A 5G AMERICAS WHITE PAPER

EVOLVING 5G SECURITY FOR THE CLOUD

SEPT 2022

Contents

Executive Summary

Security is an important topic for the mobile communications industry as 5G enables new applications and use cases. The mobile communications industry continues to consider security as a foundational pillar for each generation of our technology. It is essential to continue the progress in security innovations as there are increasing threats from nation-state and other sophisticated actors threaten critical infrastructure and present material risks to mobile network operators (MNO) and their suppliers.

5G security continues to improve as security controls, tools, and standardization evolve and the 5G ecosystem extends to include the virtualized and cloud-based Radio Access Network (RAN). 5G evolution to cloud hosting for Radio Access Network (RAN) and Core deployments brings both additional security benefits and security risks. Cloud deployments present an expanded attack surface with internal and external threats to 5G networks, requiring a zero trust mindset to secure those networks.

While the MNO can delegate responsibility for security controls to the cloud service provider (CSP), the MNO is accountable for the security posture of the deployment. Hybrid Cloud deployments, such as Multi-Access Edge Compute (MEC), pose additional security risk due to the responsibilities retained by the MNO in the Cloud Shared Responsibility Model. The MNO is always responsible for configuration of CSP provided security controls, including firewalls and access management, data protection from exposure and leakage, and scheduling and execution of software patches and upgrades. The MNO must validate configurations, use secure versions of APIs and protocols, and assign least privilege to access workloads and data.

A secure 5G cloud deployment must be built upon a secure 5G supply chain that includes software vendors and cloud service providers. The cloud can potentially introduce increased supply chain risk due to virtualization, increased use of open-source software, and a larger array of third-party vendors. MNOs must ensure 5G software vendors implement secure software assurance with a shift-left philosophy that integrates security into the software development process, continuous integration/continuous delivery, and DevSecOps early in the software development lifecycle.

The Software Bill of Materials (SBOM) provides a comprehensive view of the third-party commercial and open-source components which are incorporated in a product. The SBOM can be utilized to identify known critical vulnerabilities inherited from third parties and affected products when new vulnerabilities emerge. The GSMA association's Network Equipment Security Assurance Scheme (NESAS) assessment is a valuable tool to ensure the 5G software vendor is following industry best security practices. Third-party applications in the O-RAN ecosystem, called rApps and xApps, could introduce additional risk to the supply chain. The Service Management and Orchestration (SMO) platform vendor and MNO must practice due diligence to ensure rApps and xApps are trusted, securely on-boarded, and designed with proper security controls for integration into the ecosystem.

The cloud has great promise for 5G use cases, which can be realized when the software products have security built in and deployments are securely configured to establish a foundation for secure 5G use cases. A step-wise approach should be taken to achieve a Zero Trust Architecture for 5G deployments in the cloud so that network functions, interfaces, and data are protected from external and internal threats.

1. Introduction

The mobile communications industry continues to prioritize security advancements and specifications for each generation of technology. Mobile communications security continues to be imperative in our technological wireless advancements. 5G is the first generation of mobile technology designed for the cloud. The cloud computing characteristics of multi-tenancy, virtualization, broad device access, resource pooling, and rapid elasticity promise advantages of enhanced mobility, performance, service agility and security.

The cloud, however, has inherent security risks that increase the attack surface of the 5G Radio Access Network (RAN) and Core. The SolarWinds attack[1] was the inflection point that changed the way security professionals think about securing 5G cloud deployments. This attack highlighted the need to implement a Zero Trust Architecture (ZTA) to prevent lateral movement by adversaries already inside the 5G network.

In addition to Advanced Persistent Threats (APTs) used to conduct reconnaissance attacks, the cloud can increase risk due to misconfigurations and weak security implementations, introducing vulnerabilities that can be exploited by any malicious actor, such as a nation-state or cybercriminal. There is further risk from Hybrid Cloud deployments due to multiple stakeholders, Mobile Network Operators (MNO), Cloud Service Providers (CSP) and others sharing responsibility for security. The Cloud Shared Responsibility Model commonly used in the cloud industry is an important tool to ensure security governance is followed in the cloud. The cloud also increases risk for 5G Supply Chain Security as the cloud service provider and third-party software products become partners in the ecosystem, along with potential of increased dependence upon open-source software.

This paper builds upon prior 5G Americas work on 5G cloud security in the 2021 white paper Security for 5G[2] to examine the risks associated with 5G Hybrid Cloud deployments and recommends risk mitigations and security controls. The value of striving towards a Zero Trust Architecture for 5G deployments is discussed, along with recommendations for securing the 5G supply chain, to ensure a strong security posture for 5G networks that is protected from external and internal threats.

NOTE: Terms of malicious actor, threat actor, bad actor, and adversary are terms that have been used recently to describe the same type of threats and are used interchangeably throughout the document.

2. Secure 5G Deployments in Hybrid Cloud Environments

2.1 Introduction

Mobile services are a part of everyday life and are considered critical infrastructure for national security. 2G networks were released in the 1990s and introduced a new vocabulary set of open standards and specifications that defined a complex set of network infrastructures, protocols and interfaces. The equipment for these networks were purpose-built hardware platforms that would perform a specific function. Ten years later 3G was released and it, too, had a set of purpose-built infrastructure. 10 years after that 4G was released and required mobile network operators (MNOs) to simultaneously maintain three generations of mobile networks. MNOs began deploying solutions on both purpose-built and Commercial Off the Shelf (COTS) hardware that was still dedicated to specific software applications.

At the same time the information technology (IT) industry was pioneering compute platforms that could run multiple applications. As compute, memory, and storage capacities and performance continued to increase, server virtualization became a reality. While the MNOs were layering purpose-built infrastructure, the IT environment was running multiple applications in segmented compute space on the same infrastructure. This movement continued and gave birth to the era of virtualization.

As IT organizations embraced virtualization and participated in the open-source development community, that digital transformation allowed organizations to reduce cost, accelerate feature development and provide greater business insights and analytics to help them be more competitive. Some organizations took that even further with entities such as Amazon Web Services, Microsoft Azure, and Google Cloud Platforms offering multi-tenant environments on shared resources in the cloud.

The mobile industry collectively embraced these IT trends and advancements in virtualization to take advantage of its cost savings and deployment flexibility. 5G standards were developed that enabled separation of the core and edge compute network functions (NFs) from the hardware layer to enable virtualization of the NFs. The move to virtualization for the MNOs started in the 4G development cycle, with some virtualization occurring prior to 5G Non-Standalone (NSA) deployments. This virtualization allowed for a smoother transition from 4G to 5G since the same network function virtualization infrastructure (NFVi) could run 4G and 5G functions simultaneously.

Virtualization first used virtual machines (VMs) for virtual network functions (VNFs) and has since evolved to containers for cloud-native network functions (CNFs). With this shift to CNFs, MNOs can efficiently leverage cloud computing at large scale. This has introduced private, public, and Hybrid Cloud deployment models when designing and deploying core networks, edge computing, network slicing, private networks and more. Security for 5G cloud deployments is discussed further in this paper.

2.2 Stakeholders

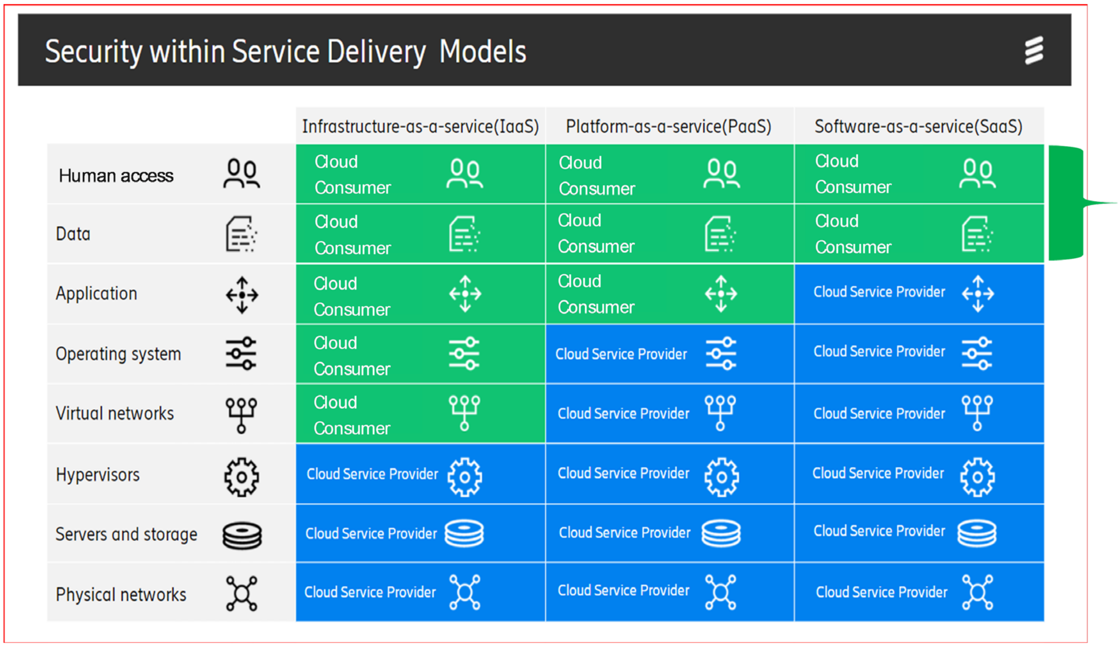
While the cloud can introduce many security benefits, it also introduces new security risks to be addressed by its stakeholders. As 5G networks are evolving to the cloud for RAN and Core deployments consideration must be made for stakeholders to protect the expanded attack surface. Cloud deployments have the following stakeholders:

Cloud Consumer: The CSP's customer, a person or organization, requesting and using resources. A Mobile Network Operator (MNO) deploying 5G networks in the cloud is a Cloud Consumer.

Cloud Service Provider: A company that offers some component of cloud computing resources delivered to a Cloud Consumer.

Figure 2.1 Cloud Shared Responsibility Mode

Source: 5G Americas Member Company



Security within Service Delivery Models

	Infrastructure-as-a-service(IaaS)	Platform-as-a-service(PaaS)	Software-as-a-service(SaaS)
Human access	Cloud Consumer	Cloud Consumer	Cloud Consumer
Data	Cloud Consumer	Cloud Consumer	Cloud Consumer
Application	Cloud Consumer	Cloud Consumer	Cloud Service Provider
Operating system	Cloud Consumer	Cloud Service Provider	Cloud Service Provider
Virtual networks	Cloud Consumer	Cloud Service Provider	Cloud Service Provider
Hypervisors	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Servers and storage	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider
Physical networks	Cloud Service Provider	Cloud Service Provider	Cloud Service Provider

Cloud Consumer is always accountable for data security and access to software applications and the node

Hyperscaler Cloud Provider (HCP): A cloud service provider with massive global scale. Some examples are Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. The security roles and responsibilities of the stakeholders in 5G cloud deployments are discussed further in this document.

2.3 Shared Responsibility Model

The key stakeholders in a cloud deployment are the cloud service provider and its customer, the Cloud Consumer. The Cloud Consumer consumes cloud service provider services in any one of three cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), and/or Infrastructure as a Service (IaaS). The responsibilities of the Cloud Consumer and cloud service provider to provide security at each layer of the cloud varies with the three service models.

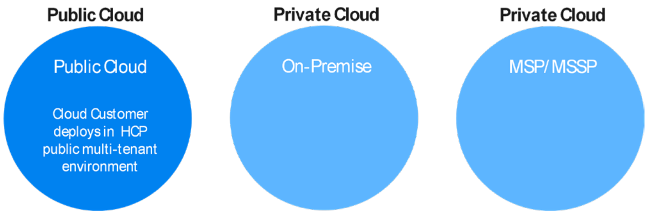
The two related terms used in cloud security are **responsibility** and **accountability:**

- ***Responsibility*** *can be outsourced or delegated*
- ***Accountability*** *cannot be outsourced nor delegated*

In the IaaS and PaaS service models, the Cloud Consumer is the Mobile Network Operator (MNO), which is selling consumer mobile and enterprise mobile services. The MNO is accountable for the security of its cloud service, including data and network functions, at all layers of the cloud stack.

Figure 2.2 Public and Private Cloud Deployment Model

Source: 5G Americas Member Company



The “Cloud Shared Responsibility Model”, as shown Figure 2.3 below, provides security guidance for the responsible stakeholder at each layer of the cloud for each of the service models. The cloud service provider is responsible for *securing the cloud* and the Cloud Consumer is responsible for the *security of the cloud*, which always includes data, devices, and people.

The cloud service provider is responsible for securing its infrastructure while the Cloud Consumers may be responsible for securing the higher layers of the cloud stack, including operating system, applications, and data.

The Cloud Consumer is always responsible for ensuring data is protected from unauthorized access that can result in internal or external threat actors viewing, modifying, or transferring the data. Ultimately, the Cloud Consumer, as the Data Owner/Controller, is always accountable for the security posture of the cloud deployment. The Cloud Consumer must ensure the cloud service agreement clearly articulates the security responsibilities for each stakeholder.

2.4 Cloud Deployment Models

Cloud Deployment Models are Private Cloud, Public Cloud, Community Cloud and Hybrid Cloud as defined by National Institute of Standards and Technology (NIST) SP 800-145,[3] published in 2011 and still referenced globally today. 5G cloud deployments have conformed to the Private, Public, and Hybrid Cloud deployment models.

2.4.1 Private and Public Cloud Deployments

- *Private Cloud*
  - » *Infrastructure is provisioned for exclusive use of services/solutions, run in a single organization comprising multiple consumers (for example, business units) within that organization.*
  - » *The service may be owned, managed and operated by the organization, a third-party (such as managed service provider (MSP)) or combination—on or off the organization premises.*
  - » *MNO deploys its 5G cloud-native network on-premises or with an MSP or managed security service provider (MSSP).*

- *Public Cloud*
  - » *Infrastructure is provisioned by a cloud provider that is intended for open use by the public (for example, any organization globally).*
  - » *The service may be owned, managed and operated by a business, academic, government or combination—on the premises of the cloud service provider.*
  - » *MNO, as Cloud Consumer, deploys in the HCP public multi-tenant environment.*

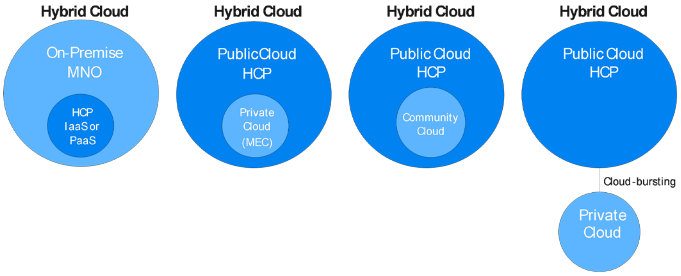
2.4.2 Hybrid Cloud Deployments

National Institute of Standards and Technology (NIST) defines the Hybrid Cloud as:

> **Infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability.[4]**

Figure 2.3 Hybrid Cloud Deployment Models

Source: 5G Americas Member Company



The Hybrid Cloud deployment options for 5G cloud are shown in Figure 2.3 below. Many 5G deployments are Hybrid Cloud deployments in which the HCP may deploy its infrastructure on-premises at the MNO facility, the MNO may deploy a Private Cloud in the HCP's Public Cloud or a Community Cloud may deploy in the HCP's Public Cloud. Traditionally, the Hybrid Cloud allows a Cloud Consumer to cloud-burst to the Public Cloud when resources are fully utilized in the on-premises Private Cloud.

5G cloud deployments for RAN and Core will use the Hybrid Cloud deployment model to enable low latency, mission critical use cases. Multi-Access Edge Compute (MEC) is an example of a Hybrid Cloud deployment in which the MNO deploys its network functions and applications in the HCP Public Cloud at the mobile network edge. The MNO may also deploy a Hybrid Cloud in which the HCP deploys its infrastructure on-premises at the MNO.

The Hybrid Cloud provides deployment advantages for the MNO as the Cloud Consumer, as follow:

- *Cloud Consumer (operator) has better control and understanding on how various government rules, laws and regulations apply to them*

- *Cloud Consumer can architect the Hybrid Cloud deployment to ensure regulatory compliance of most sensitive data, while less sensitive data is accessed, stored and processed in the Public Cloud. The Cloud Consumer (operator) must practice due diligence to assess the regulatory compliance of the cloud service provider's environment.*

- *Cloud Consumer can transfer part of the cloud operation to the CSP, which already has the necessary cloud expertise, infrastructure and systems*

2.5 Securing Hybrid Cloud For 5G Deployments

The cloud expands the 5G attack surface due to lack of clear definition of roles and responsibilities between stakeholders, lack of due diligence to determine the security posture of selected cloud service providers and inconsistent security posture in a multi-cloud environment.

There are many security and privacy challenges to consider when transitioning from a private, on-premises deployment to a hybrid or Public Cloud deployment:

- *Geographical overlap of jurisdictions may require compliance to multiple data privacy regulations*
- *Multi-tenancy introduces a shared pool of resources*
- *Misconfigurations of security for applications deployed in the cloud*
- *Slow or missing software patches and upgrades*
- *Use of Free Open-Source Software (FOSS), including use by third-party commercial software suppliers*
- *Untrusted third-party applications and administration*
- *Use of insecure APIs with known vulnerabilities*
- *Use of insecure third-party hardware*

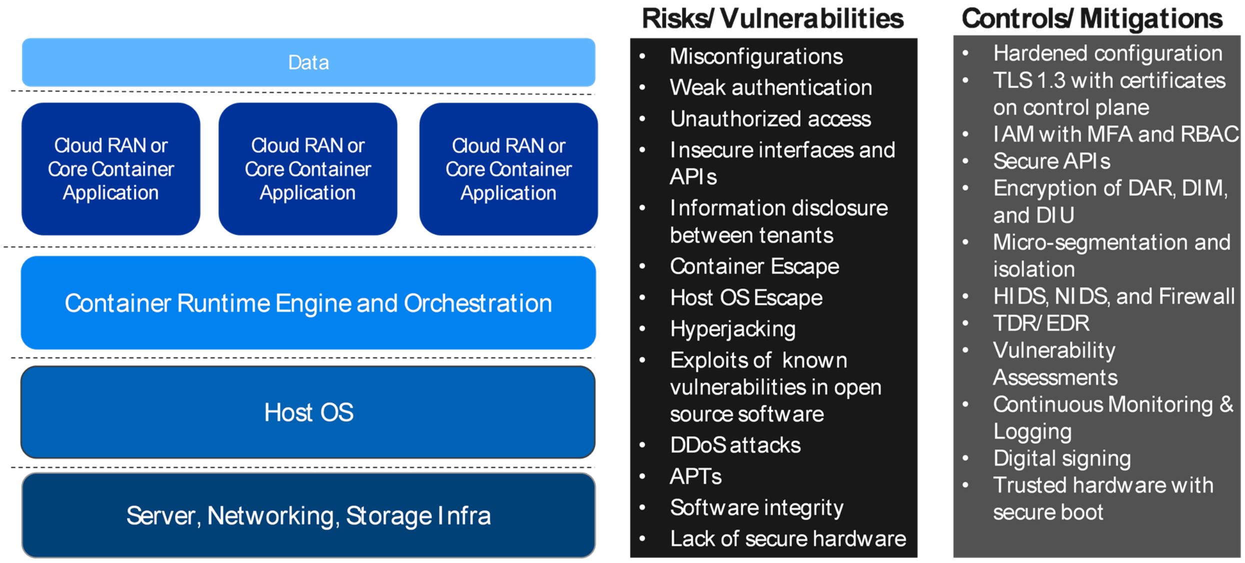
The Cloud Security Alliance (CSA) Hybrid Cloud Security Working Group[5] bases its activities on the following identified challenges:

- *There are different security risks the hybrid clouds pose, bringing on challenges to security protection*
- *For hybrid clouds, special attention must be paid to areas such as compliance and data security, which are of concern due to the interconnection between the public and private clouds*

The multi-party relationship between the vendor, operator, cloud provider and system integrator requires that security roles and responsibilities be clearly defined. The US Cybersecurity and Infrastructure Security Agency (CISA) has advised that "Cloud service providers and mobile network operators may share security responsibilities in a manner that requires the operators to take responsibility to secure their tenancy in the cloud."[6] A multi-lateral agreement should address the security controls to be deployed to protect assets, including data, and which stakeholder is responsible to implement it. Changes to risk due to evolving threats, attack vectors and security control technologies should be periodically reassessed by all stakeholders.

Cloud service providers have varying levels of security capabilities and service offerings. Typically, infrastructure security is provided at no charge, but security of the upper layers of the cloud stack, as shown in Figure 2.4, is considered the Cloud Consumer's responsibility. When the cloud service provider is delegated to provide selected security features via the cloud service agreement, the Cloud Consumer is responsible for the security configuration and accountable for the security posture of the deployment. For 5G deployments, the MNO as Cloud Consumer, is accountable for the security posture of the deployment. The operator must perform proper due diligence of cloud service providers to ensure deployments are secure and security responsibilities clearly delegated. Multi-cloud requires additional diligence to ensure the MNO deploys a consistent security posture across multiple cloud service provider partners while managing sensitive communication on the control plane for scheduling, monitoring and routing.

Figure 2.4 Cloud Risks and Mitigations[59]


Data
Cloud RAN or Core Container Application
Cloud RAN or Core Container Application
Cloud RAN or Core Container Application
Container Runtime Engine and Orchestration
Host OS
Server, Networking, Storage Infra

Risks/ Vulnerabilities

- Misconfigurations
- Weak authentication
- Unauthorized access
- Insecure interfaces and APIs
- Information disclosure between tenants
- Container Escape
- Host OS Escape
- Hyperjacking
- Exploits of known vulnerabilities in open source software
- DDoS attacks
- APTs
- Software integrity
- Lack of secure hardware

Controls/ Mitigations

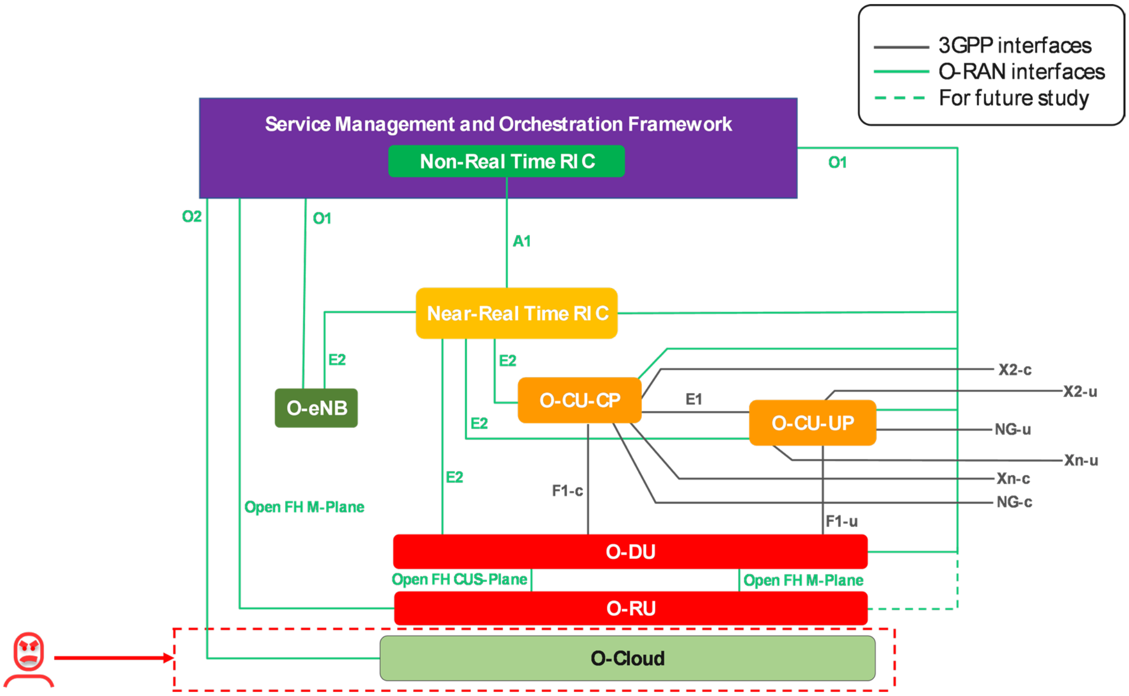
- Hardened configuration
- TLS 1.3 with certificates on control plane
- IAM with MFA and RBAC
- Secure APIs
- Encryption of DAR, DIM, and DIU
- Micro-segmentation and isolation
- HIDS, NIDS, and Firewall
- TDR/ EDR
- Vulnerability Assessments
- Continuous Monitoring & Logging
- Digital signing
- Trusted hardware with secure boot

2.6 Risk Mitigation in the Cloud

As the cloud expands the 5G attack surface, it is necessary for MNOs and their supply chain partners, including cloud service providers and network function vendors, to mitigate risk in the cloud. Vulnerabilities due to misconfigurations, weak authentication and insecure APIs can be exploited to compromise confidentiality, integrity and availability. Well known attacks in the cloud include container escape, host escape, hyperjacking, Distributed Denial of Service (DDoS) and supply chain attacks. Defense in depth mitigation throughout the cloud stack should be implemented to ensure containerized applications, container run time and orchestration, and host operating systems are secure. References for recommended best cloud security practices from the CSA,[7] Center for Internet Security (CIS),[8] US DoC NIST,[9] and US DHS CISA.[1011] Recommended controls for secure cloud deployments include:

- *Tenant isolation and container isolation*
- *Digital signatures of images to ensure trustworthiness*
- *Configuration validation and hardening to ensure unused ports are closed, unused protocols are disabled, default passwords are changed*
- *Multi-Factor Authentication (MFA) for users*
- *Transport Layer Security (TLS) 1.3 with Public Key Infrastructure (PKI) and X.509 Certificates for automated mutual authentication of software systems*
- *TLS 1.3 for confidentiality and integrity protection of data in motion (DIM)*
- *Confidentiality and integrity protection of data at rest (DAR) using strong cipher suites*
- *Access Controls with Principle of Least Privilege using Role-Based Access Controls (RBAC), Task-Based Access Controls (TBAC), or Policy-Based Access Control (PBAC)*
- *Hardware Root of Trust (HRoT), such as provided by a Hardware Security Module (HSM)*
- *Availability of systems and services with volumetric and application DDoS protection*
- *Continuous Monitoring, Logging, and Alerting with automated Threat Detection and Response (TDR)*

Figure 2.5 O-RAN Architecture with Attacker targeting O-Cloud (Adapted from O-RAN Alliance architecture diagram)[60]



Some of these controls, listed above and shown in Figure 2.4, are exclusive for cloud, but are recommended for a secure 5G cloud deployment built for a ZTA.

2.7 O-Cloud Security

While the cloud introduces threats that expand the 5G attack surface, MNOs must also consider threats introduced by O-Cloud, an O-RAN Alliance specified cloud computing platform that meets O-RAN requirements to host O-RAN's functions, management and orchestration and operating system. O-Cloud specifications from the O-RAN Alliance should provide industry best security practices to ensure O-RAN cloud implementations, including Hybrid Cloud deployments, are secure.[12] The cloud introduces security risks that are not exclusive to O-RAN, but additional security controls should be implemented to secure O-RAN deployments classified as critical infrastructure. For example:

- *O2 interface[13] for Service Management and Orchestration of the O-Cloud must be secure*
- *APIs for the Acceleration Abstraction Layer (AAL)[14] and O-Cloud infrastructure must be secure*
- *O-RAN deployments should follow cloud security best practices, such as those advised by NIST, CISA, CSA and CIS*
- *Hardware must be secure with HSM/TPM*

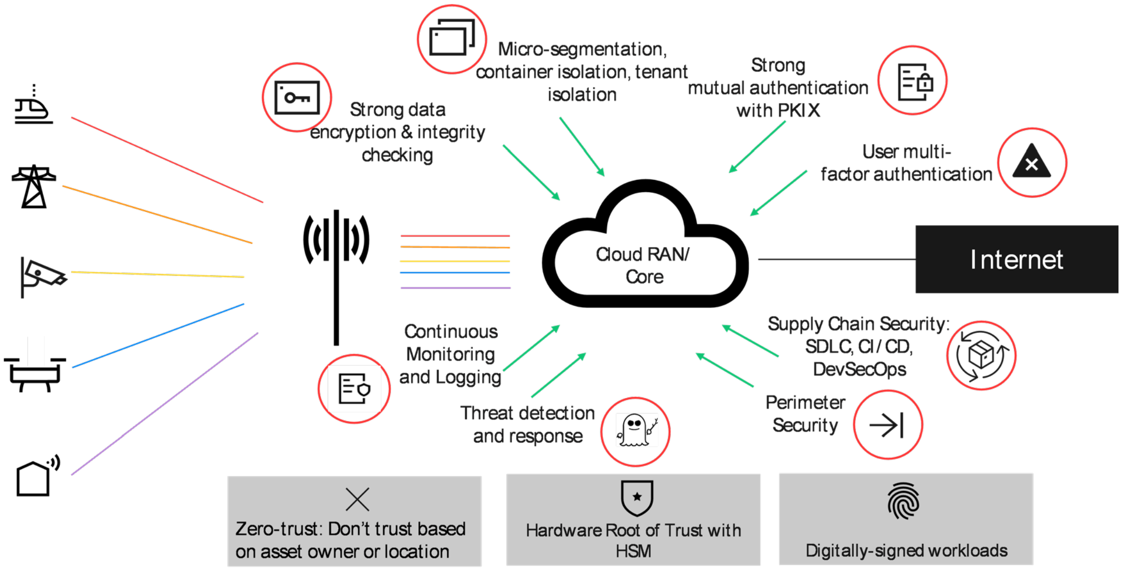
2.8 Zero Trust Architecture for Cloud Deployments

The concept of zero trust was first introduced in 2010 by John Kindervag of Forrester Research.[15] He theorized that digital systems cannot earn trust as humans do and proposed "zero trust" in digital systems based on the principle that no network user, packet, interface or device should be trusted.

Zero Trust Network Access (ZTNA) was the next evolution in zero trust in which the level of external and internal access to a digital resource (asset or application) is permitted only for trusted and authorized identities. This zero trust permission level (view, modify, copy or delete) is authorized through policies evaluated for each access request. Attribute based access control rules making up this authorization policy allow control based on such attributes as user roles, tasks, policy and security factors.

The Zero Trust Architecture (ZTA) is the evolution of the zero trust concept to enable application of zero trust for digital systems and networks for which legacy perimeter defenses are no longer sufficient. While this legacy approach has been effective against external threats, internal threats including APTs, require an evolved security paradigm with finer grained controls, particularly for cloud deployments. ZTA is based upon applying access security controls where authorization is explicitly granted for all access to sensitive resources in all cases eliminating access based on implicit trust such as through ownership, physical location or network location.[16] This increases the level of threat detection and mitigation regardless of where the attack is initiated by an external or internal threat actor.

Figure 2.6 Cloud Risks and Mitigations[61]


Micro-segmentation, container isolation, tenant isolation
Strong data encryption & integrity checking
Strong mutual authentication with PKIX
User multi-factor authentication
Cloud RAN/ Core
Internet
Continuous Monitoring and Logging
Threat detection and response
Supply Chain Security: SDLC, CI/CD, DevSecOps
Perimeter Security
Zero-trust: Don't trust based on asset owner or location
Hardware Root of Trust with HSM
Digitally-signed workloads

In 2021, multiple US agencies have provided guidance for zero trust in the cloud, as directed by the President's Executive Order "EO 14028 on *Improving the Nation's Cybersecurity*".[17] US DHS CISA on Oct 28, 2021, published Security Guidance for 5G Cloud Infrastructures. CISA's Security Guidance for 5G Cloud Infrastructures[18] brings together a single security posture for 5G cloud deployments based upon a ZTA protecting workloads, cloud platforms, and network connectivity. This 4-volume set includes:

Part I: Prevent and Detect Lateral Movement
Part II: Securely Isolate Network Resources
Part III: Protect Data in Transit, In Use and at Rest
Part IV: Ensure Integrity of Infrastructure

CISA's stated main drivers for this work were:

- *Cloud-native 5G is a lucrative target for cyber threat actors*
- *Cloud providers & MNOs share security responsibilities requiring* ***operators to take responsibility to secure*** *their tenancy "in the cloud"*
- *Strive to bring a* ***Zero Trust*** *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*

ZTA is an implementation plan for zero trust. While ZTA supports fine grained controls to sensitive resources through defined perimeters and micro-perimeters, it also provides defense in depth security building upon numerous security controls including strict authorization, micro-segmentation, cryptographic protection of data at rest and in motion, hardware root of trust, automated threat detection and response and continuous logging and monitoring, as shown in Figure 2.6 below. Supply chain security has also become a component of 5G ZTA with vendors practicing secure software development processes using continuous integration/continuous delivery (CI/CD) and DevSecOps best practices, as discussed in the Supply Chain Security section of this document.

Security controls for a ZTA should be implemented through a risk-based approach. A risk analysis calculates risk levels by assessing the threat's likelihood of attack and the impact from the attack. Impact scores can be lowered with consideration of existing security controls. Likelihood scores may be higher when the goal is a ZTA, because external and internal threats must be considered. When likelihood scoring during a risk analysis, it is necessary to consider internal threats performing reconnaissance attacks impacting confidentiality and privacy and attacks causing damage or degrading performance impacting availability. Internal threat actors are less likely to perform damaging attacks that are quickly and easily detected and blocked, but more likely to attempt reconnaissance attacks to collect information. For example, APTs, such as the SolarWinds attack, typically engage in lateral movement as an anonymous or elevated authorized privileged user, preventing detection while providing reconnaissance over a long period of time.

2.9 Evolving Technologies for Securing 5G Hybrid Cloud Deployments

Securing the Hybrid Cloud in 5G will require the software vendors and MNOs to evolve their security detection and response capabilities. Malicious actors are continuously introducing novel Tactics, Techniques, and Procedures (TTPs) in their attack campaigns, which are increasingly becoming more complex. Vendors and MNOs need to be vigilant in their defense in depth strategies and threat detection capabilities. As industry shifts-left cybersecurity in the software development process, there must be continued focus on the entire application lifecycle in the 5G network. The industry is collaborating broadly to expand the capabilities to include Software Bill of Materials (SBOM), software ID tags, software composition analysis (SCA), and interactive application security testing (IAST). This collaboration is producing capabilities that enhance Supply Chain Security by mitigating the adversary's ability to inject malicious software code into the final software products delivered to the cloud.

Industry needs to continue collaboration to evolve defense in depth strategies and adopt new capabilities that can provide advanced intelligence to detect malicious software and/or misbehaving software in 5G cloud deployments. Runtime security that can be deployed with the vendor's products provides a great opportunity to enhance defense in depth strategies. Runtime security is discussed in this subsection with focus on Runtime Application Self-Protection (RASP), Threat Detection and Response (TDR) and Endpoint Detection and Response (EDR). The 5G Core Service Based Architecture (SBA) uses HTTP 2.0 for inter-network function communications, which enables RASP to be effective in detecting misbehaving vendor code. TDR/EDR can be effective at detecting system related attacks on platforms at risk of attacks from internal and external threat actors.

The increase in number and sophistication of data breaches poses a challenge to the 5G ecosystem and its promise of greater connectivity and evolving use cases to benefit society. MNOs and cloud service providers can meet the challenge with new security architectures and data protection methods. MNOs deploying critical infrastructure in the cloud must provide end-to-end data protection with advanced security models to protect sensitive data in 5G networks. Confidential Computing is an emerging security model for data-in-processing protection, the most challenging leg of end-to-end data protection. Cost and performance are key factors in designing Confidential Computing solutions for 5G networks.

2.9.1 Runtime Security

Industry has begun implementing additional layers of security controls and capabilities, such as SCA, SBOM, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), CI/CD Pipelines, etc.) which will all play a critical role in the defense in depth strategies for securing 5G cloud deployments. It will take a few more years to mature and combine these individual layers into a solid end-to-end defensive posture for some organizations. Even with this solid end-to-end defensive posture, the software code could still be compromised in the supply chain, as demonstrated by SolarWinds.

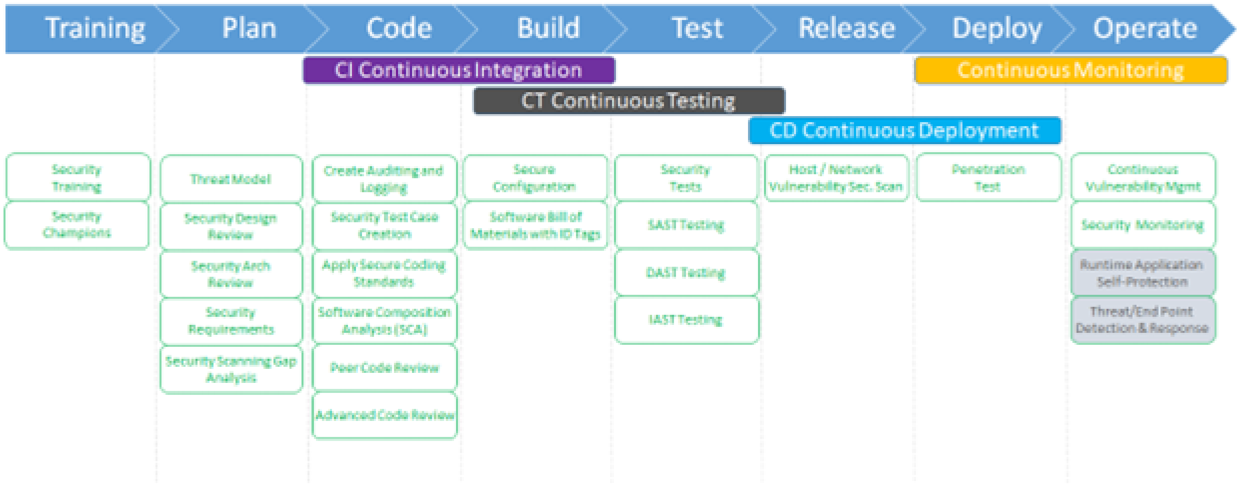
The goal of an effective cybersecurity strategy is to detect the security event as rapidly as possible so the attack can be detected and mitigated to minimize the potential damage. The application providers know their software and the behaviors of that code best. When that code is compiled and delivered to the cloud, the MNO and cloud service provider do not have the code behavior knowledge that the software vendor has. If a software package were to be compromised in the supply chain and eventually deployed into a production network, the MNO and cloud service provider may not be able to quickly detect the exploitation of a vulnerability, such as Log4Shell.[19] This ushers in runtime security, which is essentially the last line of defense. This section focuses specifically on RASP and TDR/EDR, which provide complementary levels of runtime security that can be extremely valuable to secure 5G cloud deployments. Figure 2.7 below shows the phases of the software development lifecycle (SDLC) and the use of RASP and TDR/EDR in the Operate Phase.

2.9.1.1 Runtime Application Self-Protection (RASP)

RASP capability should be embedded into the delivered software packages by software vendors, whose software development teams have the most knowledge of the code, API calls and expected behaviors. This knowledge may not be within the MNO's or cloud service provider's tooling, instrumentation or staff training. RASP can be integrated into software packages that when deployed into a production network, alert the MNO in real-time when a component in the software is exhibiting abnormal behavior.

Figure 2.7 The Phases of the SDLC Program

Source: 5G Americas Member Company



Developing and embedding the RASP functions and capabilities into a software package is quite complex. This challenging undertaking requires considerable resources from any 5G network function vendor that is delivering software packages for the Access Stratum, Non-Access Stratum, SBA, IMS and other applications. As we have seen over the past few years, malicious actors are using novel approaches such as APTs exploiting multiple vulnerabilities. RASP is a critical capability that needs to be incorporated into the telecom infrastructure to protect against these attacks. Many enterprises today are already using RASP for internally developed software and this evolution will progress into the mobile industry as well.

2.9.1.2 Threat Detection & Response and Endpoint Detection & Response (TDR/EDR)

TDR/EDR is a last line of defense capability that provides system level protection, unlike the RASP that provides only application-level protection. TDR/EDR solutions can scale to provide system level protection on a wide array of platforms and operating systems. Since they are a runtime security control, they provide high detection accuracy which should help the MNO, software vendor and cloud service provider size and scale their security operations center (SOC) teams. Commercial TDR/EDR solutions may have the following capabilities:

- *Artificial intelligence (AI) and machine learning (ML) capabilities that improve accuracy by reducing false positives and adjusting to threat environments as adversaries continuously evolve their TTPs.*

- *Integrate with threat intelligence feeds to keep current with newly published common vulnerabilities and exposures (CVEs) and coordinated vulnerability disclosures (CVDs).*

- *Data export to provide the SOC, cyber risk and threat intel teams with a broad range of data analytics that can feed into other cyber strategy programs.*

2.9.2 Confidential Computing

2.9.2.1 Why Confidential Computing now, for 5G?

MNOs are migrating to cloud-native network functions (CNFs) to increase flexibility and scalability. However, cloud technology opens new threats rendering the legacy network perimeter security insufficient. Sensitive data, including data in transit (network), data at rest (storage) and data in use (processing) requires end-to-end and life cycle protection. MNOs traditionally implement data protection assuming perimeter secured networks. Confidential Computing[20] is a well known technology for protecting data in use from external and internal threats consistent with a ZTA approach.

Confidential Computing protects sensitive data in use by performing computations in a hardware based Trusted Execution Environment (TEE). ZTA in 5G cloud deployments assumes a sensitive data processing boundary that extends to a trusted execution environment. These secure and isolated environments prevent unauthorized access or modification of applications and data while in use, thereby increasing the security assurances for organizations that manage sensitive and regulated data. This approach can work for protecting service based 5G networks in the cloud's multi-tenant environment.[21]

Confidential Computing is evolving, and periodic reassessment is required to address changes in the computing ecosystem and related laws and regulations, such as General Data Protection Regulation (GDPR). Data at rest protection mechanisms in the cloud may be implementation specific and further study may be needed to identify an industry preferred solution. In cloud-based models, it is important to protect data in use, but the evolving technology space makes it necessary to go further to ensure the separation of the processing of user data from the platform owner or administrator. The main premise behind this vision is that those controlling the infrastructure, and those that own and process the data within the infrastructure, are two separate stakeholders with different responsibilities and level of accountability for security.

MNOs use TEEs to help meet challenges associated with protecting data in use by highly distributed 5G services in functional areas such as the following:

- ***Service based architecture** using web-based integration of network functions, protected using transport layer security (TLS)*

- ***Key management for secure network access** extended to industry partners and customers*

- ***Authentication** with the Authentication Server Function (AUSF) and unified data management (UDM)*

- ***Distributed user plane**, including to non-secure physical locations*

- ***LI (Lawful Interception) sensitive data:** target list protection within the LI processing unit.*

In addition to isolation, TEEs provide assurance to outside entities that the executing code has not been corrupted or tampered with through the process of attestation. By attesting to the authenticity of its workload, a TEE can provide confidence to MNO's remote partners and customers that the destination to which they are connecting is legitimate and trustworthy, while being protected from interception by third parties.

2.9.2.2 Practical Solutions to Balance Cost and Performance

Cloud Service Providers do not accept security solutions that are too costly and disrupt other workloads. The MNO and data processor balance performance and cost with the security risk (potential severity and impact) to pragmatically determine the appropriate business requirements and investment in security. Cloud service providers and independent software vendors (ISVs) therefore provide different levels of TEE offerings for Confidential Computing to meet the business requirements.

Depending on the trusted environment boundary, a TEE can be within a chip, an entire Virtual Machine (VM), or an entire server node. A TEE within a chip often refers to a dedicated enclave as part of the chip silicon where trusted execution of code and memory access is guaranteed. Expanding the trust execution boundary to include the entire virtual machine within a virtualized system is the next level TEE. It can be an enclave of a virtual machine secured by the hypervisor layer of the virtualized system. The node level TEE usually sets the trusted execution boundary of a server where all communications in and out of the server are secured. This includes all data exchange including via Network Interface Cards (NIC), storage, and serial interface for server configuration and bootstrap.

In general, the smaller the security boundary, the more inherently secure the TEE. For example, an enclave within a chip is the safest given its embedded-in-chip access. Virtual machine (VM) level TEE relies on hypervisors to secure the execution boundary. It often leverages the memory encryption to prevent attacks from via the memory access. Node level TEE has the entire server boundary which exposes a larger attack surface. It is best used in a standalone server use case with minimum or no risk from adjacent multi-tenanted hardware.

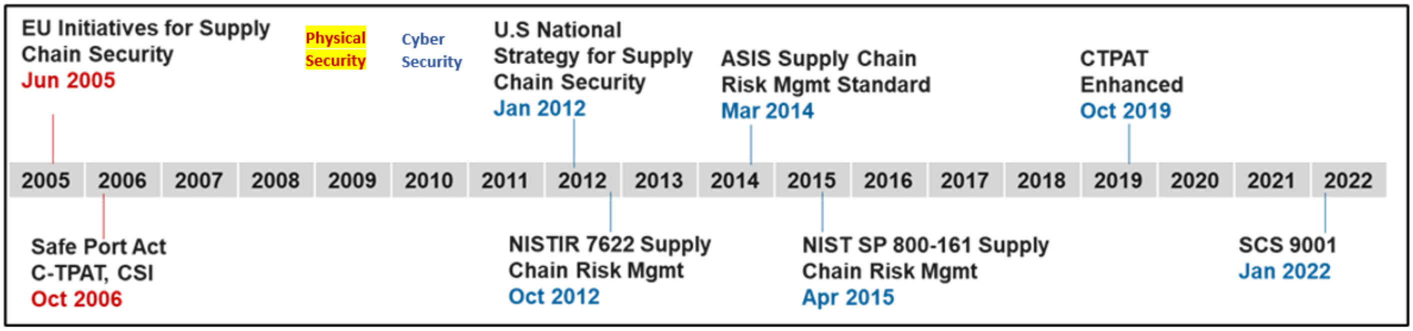
Ease of use for the TEE is a key factor in TEE selection. Trusted execution is part of a software system where all software should be developed and built under a consistent software development process. Boundaries based on the VM or Node level match the common software stacks, so no additional programming effort is needed to introduce VM or Node level TEEs. Programming towards TEEs within the chip requires coding with new pragmas and building with supported compilers.

3. 5G Supply Chain Security

Supply chain for the telecommunications industry has always been a critical component of business strategy especially during the infrastructure refresh cycles. Supply chain security has evolved from a focus on physical security to incorporate cyber security. The recently introduced SCS 9001 Supply Chain Security standard[22] brings additional focus. The progression in regulations and standards is shown in Figure 3.1 below.

Figure 3.1 Supply Chain Security – Regulatory and Standards Timeline

Source: 5G Americas Member Company


EU Initiatives for Supply Chain Security
Jun 2005
Physical Security
Cyber Security
U.S National Strategy for Supply Chain Security
Jan 2012
ASIS Supply Chain Risk Mgmt Standard
Mar 2014
CTPAT Enhanced
Oct 2019
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
Safe Port Act C-TPAT, CSI
Oct 2006
NISTIR 7622 Supply Chain Risk Mgmt
Oct 2012
NIST SP 800-161 Supply Chain Risk Mgmt
Apr 2015
SCS 9001
Jan 2022

5G Americas introduced 5G Supply Chain Security in the 2021 white paper, Security for 5G. With high visibility cybersecurity breaches such as SolarWinds and vulnerabilities such as the recent Log4j exploit, securing the supply chain in the telecom domain has become a high priority worldwide. The White House Executive Order 14028[23] pushed the need for transparency on all aspects of supply chain. It called for standards for transmitting and verifying provenance, authenticity and integrity for all components and vendors.

While network virtualization started several years ago, 5G architecture takes greater advantage of this paradigm shift in network deployment. Virtualization brings more complexity to the supply chain as more and more functionality is implemented in software. This allows for flexible deployments, but it also requires more complex validation processes with regards to deployed systems.

For 5G, Open RAN is another shift in the way the infrastructure is sourced, configured, and deployed. With projects such as O-RAN it is expected that open-source components are going to take a central role in the 5G ecosystem, therefore the need is elevated for automated and consistent upstream lineage validation. And if there is any lesson to be learned from Log4j, knowing what software is deployed in production to efficiently mitigate the security risks associated with known vulnerabilities is paramount.

Progress is being made, led by government agencies such as US NIST, US National Telecommunications and Information Administration (NTIA) and industry consortia such as ATIS (Alliance for Telecommunications Industry Solutions) and Telecommunications Industry Association (TIA). Others are working on requirements and specifications focused on securing the supply chain and defining standard processes and data formats such as the Software Bill of Materials (SBOM).

3.1 Software Supply Chain Risks

The concept of Software Supply Chain consists of the whole process of software development and deployment in the customer's environment, as shown in Figure 3.2 below. In the agile cloud-based service environment, software updates are continuously made and deployed in an automated manner through a continuous integration and continuous deployment (CI/CD) pipeline.

A typical CI/CD pipeline includes the stages of:

- *Code stage where intended features are implemented*
- *Build stage where the software components are compiled with libraries and packaged including open-source and/or 3rd party software*
- *Test stage where unit and integration test are performed*
- *Release stage where the software is delivered to the customer/consumer (e.g., at a private repository)*
- *Deploy stage where software is put into production*

Each stage of the CI/CD pipeline may entail potential risks unless appropriate security controls are employed. During the development, malicious code may be injected at the code repository, or the build tool could be exploited to include vulnerable/malicious components. Such risks can be introduced by malicious actors who have access to source code or have compromised an access credential(s) to the source code repository. Malicious code can also be injected to the software libraries/components supplied by 3rd parties or to open-source software components integrated into the software package. In the meantime, malicious software can be distributed during the distribution stage via a legitimate channel or during the deployment to production by the consumer. Potential vulnerabilities exist at different stages of software supply chain and even in cases where most of the stages employ security controls such as code inspection, static/dynamic analysis, code signing and application of security best practices, attackers may target the weakest link in the CI/CD pipeline.

Recent global high-profile cybersecurity attacks[24] were a result of insufficient security controls in the vendor's software development lifecycle or delivery framework. This includes SolarWinds,[25] Kaseya VSA,[26] Log4Shell,[27] WannaCry,[28] and NotPetya.[29] These attacks exploited one or more of loopholes in the software management channel (such as SolarWinds Orion), zero-day software/protocol vulnerabilities (such as, Kaseya, WannaCry, NotPetya) and misuse of software features (such as, Log4j). They also highlight the challenges with the security monitoring for the Indicators of Compromise (IoC) as the adversaries used complex and multi-phased attack vectors that made detection very difficult.

Supply chain risks must be addressed to ensure reliable and secure 5G network cloud deployment. Industry fora and government organizations, such as CISA,[30] have conducted threat analyses to be considered when safeguarding 5G cloud infrastructure. Considering the wide variety of suppliers participating in the global 5G ecosystem, a systematic approach to maintaining a list of trusted suppliers who follow industry best security practices for secure software development of their products/components would mitigate potential supply chain risks.

3.1.1 Virtualization

Flexibility and agility of system deployment leveraging advanced cloud technology enables security advantages such as resilience against DDoS attacks, advanced threat detection and response based upon data analytics using

Figure 3.2 Software supply chain

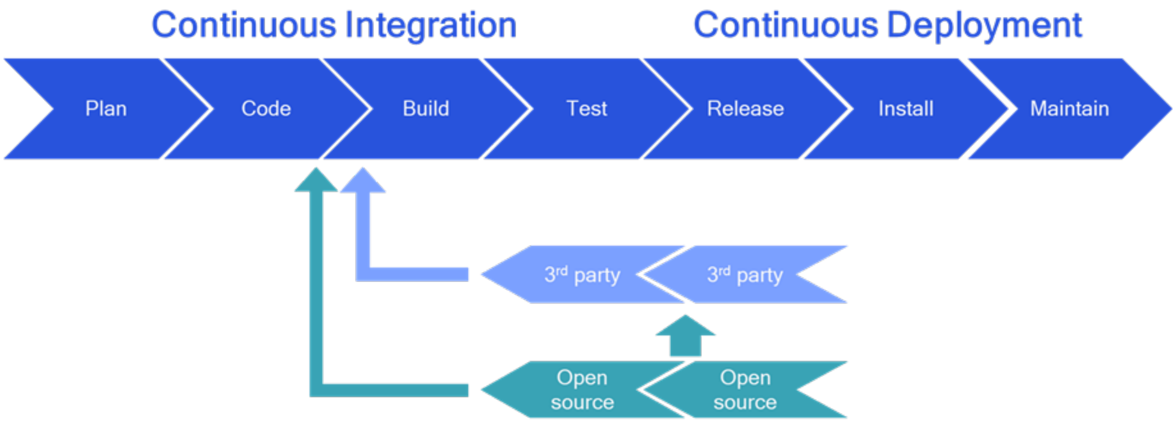
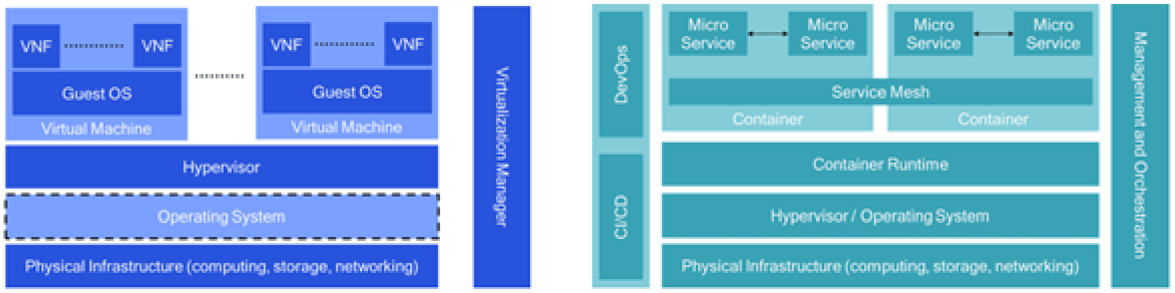


Figure 3.3 Network Function Virtualization vs Cloud-native architecture



AI/ML, and maintenance of software updates and patches, all of which are the responsibility of the MNO deploying 5G in the cloud. At the same time, software components enabling cloud-native architecture and/or network function virtualization introduce additional threat vectors as compared to the traditional systems based on physical network functions.

In the virtualized/cloud-based environment, a virtualized network function (VNF) is instantiated in a virtual machine which abstracts the physical hardware based on software technologies. Individual virtual machines are isolated via a hypervisor which may run on top of another operating system that abstracts the physical cloud infrastructure. Furthermore, such virtualized network functions as well as the entire software components comprising the cloud architecture are managed by the virtualization manager orchestrating, controlling and scheduling the VNFs as well as the virtual infrastructure—the most critical component in the virtualized systems.

This virtualization architecture has evolved into a cloud-native architecture for better agility, scalability, and flexibility of service deployment as well as failure resiliency, via containerization of microservices. Evolution of the cloud architecture expands the constituent software landscape[31] as it requires native software components including, but not limited to, hypervisor, operating system, management and orchestration framework, container runtime and service mesh, each of which may be incorporated into an automated CI/CD pipeline and expose itself to software supply chain risks.

Telecommunication networks considered critical national infrastructure require comprehensive threat analysis and proper security control for Network Functions Virtualization (NFV) and/or cloud-native architecture. The following documents should be referenced for securing 5G cloud deployments:

- *NIST's National Cybersecurity Center of Excellence (NCCoE) has recently published a draft guide to 5G cybersecurity that explains how a combination of 5G security features and third-party security controls can be leveraged to implement the security capabilities organizations needed to protect 5G networks.*[32]

- *US DHS CISA and NSA have provided guidance for securing 5G cloud deployments by preventing and detecting lateral movement, securely isolating network resources, protecting data in transit, in use, and at rest and ensuring integrity of the cloud infrastructure, as discussed in the previous section of this document addressing security of 5G Hybrid Cloud deployments.*[33]

- *US DoD and US DHS CISA have recently published guidance to assess security of 5G deployments.*[34]

3.1.2 Open-Source Software

The transparent nature of open-source software has security advantages as the software can be carefully and thoroughly examined by domain experts before its use. This is especially true for security libraries to avoid potential implementation errors or implementation specific vulnerabilities. Examples of open-source software development for telecommunication systems include O-RAN Software Community (OSC)[35] and OpenAirInterface Software Alliance (OSA).[36]

Wide use of open-source software, however, can also possibly lead to security threats, as shown in Figure 3.4 below. The recent Log4Shell vulnerability[37] has shown the impact open-source has on various industries. Considering the growing number of open-source software attacks exploiting the supply chain vulnerabilities,[38] care must be taken to strengthen the security of the open-source software supply chain for 5G cloud deployments.

Figure 3.4 Open-Source Software Benefits and Risks[62]

Benefits		Risks
Developers behave as "good citizens" in which consumers also contribute, provide useful feedback, and share fixes.	↔	Intentional backdoors can be inserted by malicious developers.
Transparency of code. Many expert eyeballs reduces software complexity and the number of bugs. This crowdsourcing approach effectively produces quality software at low cost.	↔	Attackers can review code to identify vulnerabilities.
Open source provides a platform for talented coders to openly collaborate and build software.	↔	Developers do not spend sufficient time on security. Vulnerabilities can propagate through reuse.
Open source also reduces fragmentation and increases interoperability among different products by producing components and protocols that become the de facto standard.	↔	'Trees of dependencies' make it difficult to ensure all uses of the code are patched.

3.1.3 3rd-Party Applications

Cloud-based or cloud-native 5G systems are expected to include a plethora of software components supplied by well-established and trusted vendors that have proven track records and reliable open-source software components for the essential operations. In the meantime, they may leverage third-party applications for specific purposes, such as performance enhancements, mobility optimization, energy savings to gain competitive advantages or accommodate differentiating use cases for private 5G networks. Examples include applications in the Non-Real-Time Radio Intelligent Controller (Non-RT Radio Intelligent Controller (RIC)), called rApps, and in the Near-Real-Time RIC (Near-RT RIC), called xApps, introduced in the O-RAN architecture[39] and those in the NetWork Data Analytics Function (NWDAF) of the 5G Core Network introduced by 3GPP.[40]

A motivation for rApps and xApps is to provide greater vendor diversity in which smaller, best of breed vendors can contribute third-party applications to the O-RAN ecosystem, potentially enabling a marketplace for RAN applications. This introduces supply chain security risks which must be mitigated to enable a trustworthy ecosystem of rApps and xApps vendors. The following recommendations are provided for industry to establish a trusted supply chain of secure third-party rApps and xApps:

- *Produce guidelines for secure application software development.*

- *Produce a certification process for independent third-party evaluators to provide certification of rApps and xApps.*

- *Conduct third-party vulnerability assessment (VA) to ensure rApps/xApps do not have known vulnerabilities reported in the National Vulnerability Database (NVD).*

- *Include Software Bill of Materials (SBOM), in accordance with US NTIA guidelines, with each software delivery. The SBOM must include free and open-source software modules and libraries.*

- *Provide digital signatures with each application software package to ensure software integrity.*

- *Establish a standard for secure on-onboarding of third-party rApps/xApps.*

Additional considerations should be made for the implementation of a secure RAN application marketplace and the standardization of rApps and xApps functions as the maturity of the ecosystem and deployments evolve.

The intelligence and operational logic incorporated in a third-party application is likely to include proprietary information, which by its nature cannot be easily validated. When using such third-party applications, it is extremely important to verify the integrity of the software before being deployed to production whereby interacting with other software and hardware components. In addition, these third-party applications may also include open-source software and/or another third-party software components. Providing transparency for use of and vulnerabilities assessments for such components is important to assess the potential risks introduced by upstream suppliers. Furthermore, an appropriate application on-boarding process into the ecosystem, as well as limiting authorized actions, is required to mitigate risks that third-party applications may bring into the system.

3.2 Software Supply Chain for The Cloud

The previous sections highlighted the following:

- *Securing open-source software is important. Nearly all code bases scanned by Synopsis (97%) use open-source components, and 78% of the code was open-source.*[41]
- *Consequently, to secure the software supply chain, there must be an increasing movement towards the point of software creation in modern software development methods to secure software from vulnerabilities (typically referred to "shift-left" or "shifting left")*
- *We also saw that in a virtualized cloud environment, not only is the application likely to be using open-source software, but the cloud infrastructure on which it is running will also likely be using open-source software, further expanding the 5G attack surface.*

3.2.1 SBOM/HBOM

The complex supply chain and the number of systems comprising the 5G cloud deployment are steadily expanding, which makes tracking the provenance, license, and security attributes of systems more challenging. Third-party solutions are being created to help track software and/or hardware bill of materials, which will help standardize the current methods which are often vendor-specific and difficult to efficiently share between suppliers and customers.

Many suppliers already have trusted channels with their downstream users, including software update notices, although not all of these are automated. Several promising standards have emerged that might be well-suited to enable the discovery, access, and automated ingestion of SBOM data, including:

- *Software Package Data eXchange (SPDX) is an open standard for communicating software information including components, licenses, copyrights, and security references. It is a standard that is developed by the SPDX workgroup, which is hosted by The Linux Foundation.*
- *Software Identification (SWID) tags record information about an installed software application, such as its name, edition, version, and whether it is part of a bundle, among other things. SWID tags help with software asset management and inventories. The structure of SWID tags is defined by the ISO/IEC 19770-2:2015 international standard.*
- *CycloneDX is a Software Bill of Materials (BOM) standard designed specifically for software security and supply chain component analysis. The CycloneDX Core working group maintains the specification, which has its roots in the OWASP community.*

From a 5G cloud perspective, there is no standard for creation, delivery, and consumption of SBOMs. The consumption of the SBOMs is key in the case of 5G cloud because of potential scaling requirements. The SBOM will require cloud-based real-time collaboration and data management software for managing different parts, catalogs, bill of materials, inventories, and purchase orders. The software is used in all stages of engineering, manufacturing, and supply chain. The SBOMs should have data fields for 5G Cloud elements including the cloud service provider name, vendor name, element name, and version. The support for automation is also important to ensure the data can be produced and consumed at scale using various standard data formats, including the previously discussed three leading file formats known as SPDX, SWID and CycloneDX. The US DoC NTIA has provided SBOM guidelines, which 5G Americas assessed in a previous white paper, Security for 5G.[42]

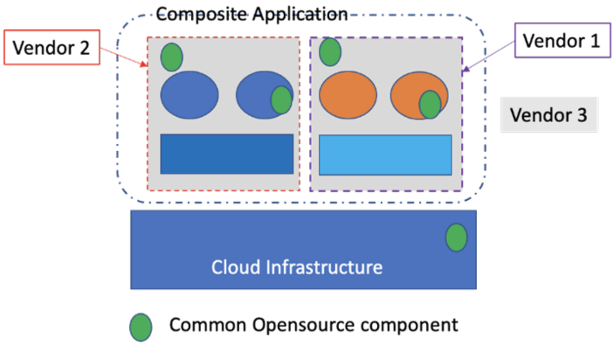
In a 5G cloud environment, you must have network functions and interfaces developed using DevSecOps and CI/CD processes. Integration of SBOM into these methods is necessary throughout the software lifecycle to achieve secure 5G cloud deployments.

3.2.2 Increased complexity with the cloud

The cloud acts a common denominator, it provides a common infrastructure on which to run applications and services. In effect, the cloud presents itself as a homogenous service on which to run applications.

From an infrastructure and application perspective, the impact of perceived homogeneity is that we are seeing increasing levels of disaggregation. Meaning that a previous monolithic application and network function is replaced with a distributed application or network function in which the components may not be coming from a single vendor. The functionality once given by an isolated monolithic function is now provided by an integrated composite function with potentially multiple vendors supplying sub-components, as shown in Figure 3.5 below.

Figure 3.5 Composite Application – same Open-source component reused multiple times



This raises the prospect that each subcomponent, as indicated by the green circles in Figure 3.5, may use different versions of the same open-source software in its release, and hence even if an SBOM is disclosed, the levels of vulnerability may be different.

3.2.3 Bad Actors Are Very Patient

Attacks can happen long after the seed has been planted. This means there is the prospect of a vulnerability being placed unintentionally or intentionally into open-source software that can travel from one development project to another, known as the tree of dependencies. This is important to consider for 5G deployments in the cloud, which is a multi-tenant environment that can be exploited for lateral movement and data exposure between tenants.

The net result is that just checking the SBOM, or only checking to a certain level of the SBOM, may not be enough, especially when the cloud is acting as a homogenizer across various applications. Runtime security using RASP and TDR/EDR are valuable tools for additional defense in depth, as discussed earlier in this paper.

3.2.4 "Shifting Left"—Early Vulnerability Identification and Resolution

Software security checks are often performed only later in the development life cycle, after the vulnerability has been introduced and code committed and, in the case of SBOMs, only against known vulnerabilities in known vulnerability data bases such as the National Vulnerability Database used with software composition analysis (SCA) tools. For a current list of such SCA tools Startup Stash has a software composition analysis tool.[43] Runtime checks can also be performed on operating software by increasing the visibility into the containerized software. The issue here is that the code is already running by the time a zero-day vulnerability may be detected.

A better approach is to perform a two-fold check: check the identity of the developer as well as the quality of the code, forming a chain of trust for that open-source contribution. If the contributions are recorded into an independent ledger, changes to the code can be observed and monitored. Then, if there is no record in the ledger associated with a change or version update, this would imply a malicious change has occurred. An example method for applying ledger records could be attached to Self-Sovereign Identities utilizing the Key Event Receipt Infrastructure (KERI)[44] Decentralized Identity (DID) method. This kind of approach would move the security of the open-source software all the way to the "left" of the process so that security of software begins at its inception, helping generate attestable SBOMs.

Multi-vendor cloud-native integration can be challenging since large interacting systems are made up of multiple components themselves. Some of those components can be the same, but the versioning and parameterization could be very different. Hence, from a security perspective, it becomes hard to normalize the security consistency across the integrated system. Moreover, increasing the SBOM levels of inspection may not be sufficient since inspecting the SBOM to any arbitrary depth across such an unnormalized security view may not provide full insight.

The SBOM gives you a vertical tree view of the CNFs/VNFs of all rolled-up components, providing a vertical snapshot view of what is currently used. However, this does not provide a horizontal historical view of the componentry. A system that can present the vertical and horizontal views is needed. To achieve both vertical and horizontal views we need a system that can practically provide levels of attestation and trust into the software supply chain. This could be achieved by instantiating a trusted model at the inception of all software component development. This requires both an authorship and content perspectives:

- *Authorship view - in effect we would be irrefutably identifying the authorship of the code component. Overtime a known profile of the author is built up (trust established).*

- *Content view - in effect we are irrefutably identifying the development phases and release component of the code. Overtime a known profile of the component is built up (trust is again established).*

Multi-vendor cloud-native integration can be enabled through the level of trust established in the authors and the components. Differences in versioning between different vendors does not become a problem from a security point of view, because trust in the different component versions has been established. This can be implemented through adaptations of the self-sovereign identity DID approaches mentioned above.

3.3 Network Equipment Security Assurance

3.3.1 Security Assurance

Security Assurance as defined by NIST is the measure of confidence that the security features, practices, procedures, and architecture of an organization are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements of the system.[45] Security assurance cannot guarantee that a product is completely risk-free, but a 5G vendor practicing due diligence should implement a security assurance program to provide confidence that its products are secured up to a certain level.

Security assurance requires more than a one-time attempt. The approach should encompass the complete system lifecycle. At any given time, what is considered an appropriate security posture may change with time, dependent on new threats or changes to system utilization. The security and success of the 5G system is dependent on continuous threat and risk analysis.

DevSecOps is an approach that utilizes automation to integrate security at every phase. One of the key processes is CI/CD to enable the automated development, delivery and deployment of software. Each stage provides feedback that can be used as a loop for continuous improvement. The automation of CI/CD increases efficiency and reduces risk. This provides up to date security, removing the risks of manual processes as well as zero touch deployment and testing.[46]

3.3.2 GSMA Network Equipment Security Assurance Scheme (NESAS)

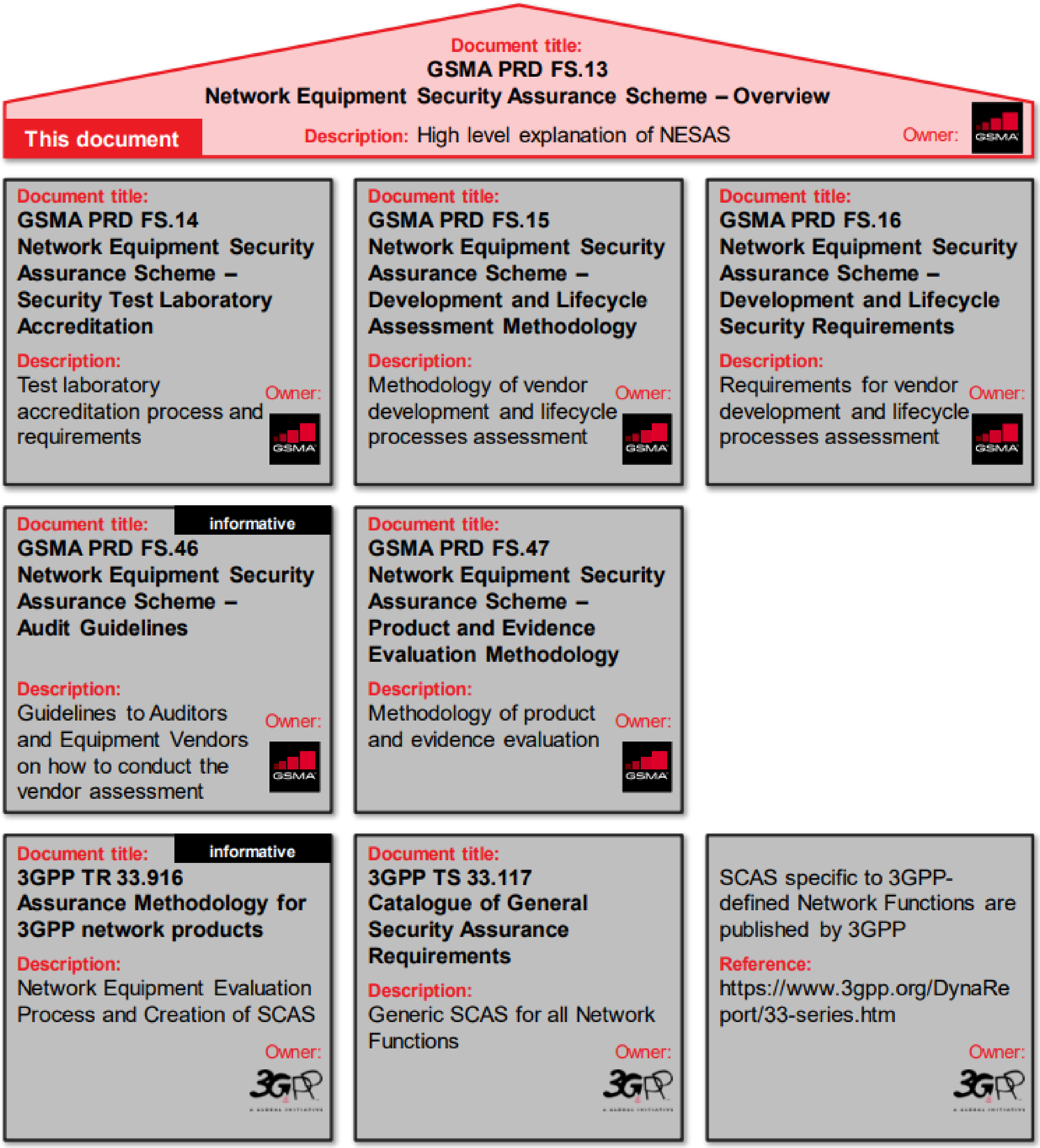
The GSMA association, in partnership with 3GPP, defined a NESAS[47] to address the global concerns relating to 5G equipment security and/or the perceived new security threats that 5G will introduce. This security scheme was described in 5G Americas white paper Security for 5G.[48]

GSMA has wide participation from operators, vendors, auditors, and governmental entities to evolve and ensure NESAS remains valuable to the 5G ecosystem. In doing so, GSMA defines and maintains the NESAS specifications, which cover assessment of the Vendor Development and Product Lifecycle Processes, NESAS Security Test Laboratory accreditation, and security evaluation of network equipment. The GSMA also defines a NESAS Dispute Resolution Process. All these elements combine to form the NESAS specifications which are detailed in Figure 3.6. 3GPP defines security requirements and test cases for network equipment implementing one or more 3GPP network functions – specified in Security Assurance Specifications (SCAS).

GSMA NESAS follows ISO/IEC 17025 by requiring an independent an accredited third-party security audit and an accredited test laboratory to perform security tests on the vendor equipment/platforms. To assist vendors with demonstrating compliance during the audit process, GSMA recently created the Audit Guidelines.[49] GSMA also recently created the Product Evidence and Methodology[50] document to further define vendor conformance during the test evaluation process. The current release, NESAS 2.1, was published in January 2022.

Most recently, GSMA created the NESAS Oversite Board responsible for the quality assurance of NESAS and the governance of the vendor development and product lifecycle process assessments. The oversight board is currently focused on expanding NESAS to include a certification process that will be acceptable to regional governmental agencies for 5G equipment.

Figure 3.6. NESAS Documents Overview[63]



This document

Document title:
GSMA PRD FS.13
Network Equipment Security Assurance Scheme – Overview
Description: High level explanation of NESAS
Owner: GSMA

Document title:
GSMA PRD FS.14
Network Equipment Security Assurance Scheme – Security Test Laboratory Accreditation
Description:
Test laboratory accreditation process and requirements
Owner: GSMA

Document title:
GSMA PRD FS.15
Network Equipment Security Assurance Scheme – Development and Lifecycle Assessment Methodology
Description:
Methodology of vendor development and lifecycle processes assessment
Owner: GSMA

Document title:
GSMA PRD FS.16
Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements
Description:
Requirements for vendor development and lifecycle processes assessment
Owner: GSMA

Document title: informative
GSMA PRD FS.46
Network Equipment Security Assurance Scheme – Audit Guidelines
Description:
Guidelines to Auditors and Equipment Vendors on how to conduct the vendor assessment
Owner: GSMA

Document title:
GSMA PRD FS.47
Network Equipment Security Assurance Scheme – Product and Evidence Evaluation Methodology
Description:
Methodology of product and evidence evaluation
Owner: GSMA

Document title: informative
3GPP TR 33.916
Assurance Methodology for 3GPP network products
Description:
Network Equipment Evaluation Process and Creation of SCAS
Owner: 3GPP

Document title:
3GPP TS 33.117
Catalogue of General Security Assurance Requirements
Description:
Generic SCAS for all Network Functions
Owner: 3GPP

SCAS specific to 3GPP-defined Network Functions are published by 3GPP
Reference:
https://www.3gpp.org/DynaReport/33-series.htm
Owner: 3GPP

4. Inter-PLMN Security

Connectivity is critical for globally connected societies. Interconnectivity naturally exposes the mobile network to additional risk and attack vectors. This exposure drives the need for secure deployment methods that allow networks to interconnect for support of roaming, without revealing confidential information or facilitating fraud/abuse.

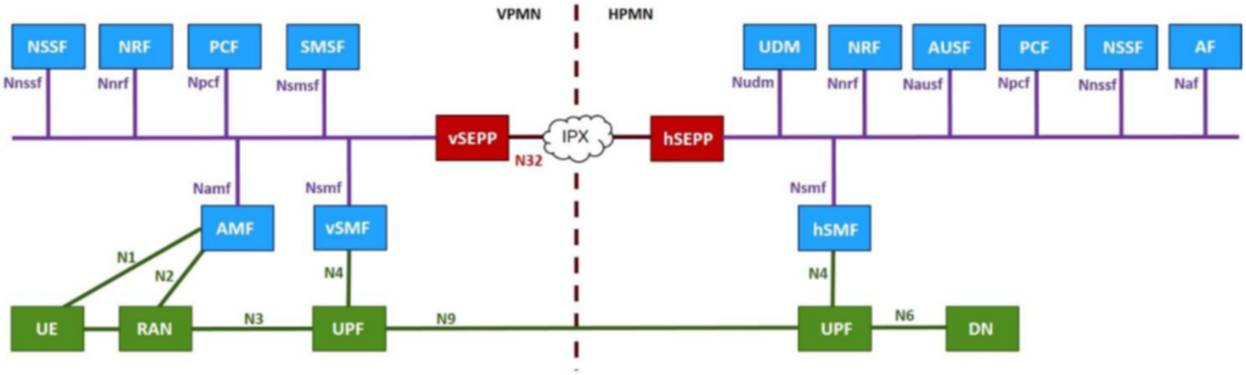
As outlined in previous 5G America's security publications, 3GPP addresses many of these interconnectivity risks in 5G SA by introducing new security controls and defining new secure inter-operator communications. For Inter-PLMN signaling security across the N32 interface, 3GPP standards include the Security Edge Protection Proxy (SEPP) with the security model using either direct TLS for end-to-end communication or PRINS (Protocol for N32 Interconnect Security) to secure the roaming interconnection when intermediaries are needed.[51] The Service Based Interfaces in a home routed roaming scenario are shown in Figure 4.1 below. The GSMA is defining the Inter-PLMN security deployment models to be used for roaming uses cases in 5G SA utilizing the baseline of 3GPP Release 16 standards as referenced above. The goal of the work is to define scalable, usable and secure 5G solutions that meet both the business and technical needs of the industry. Once completed, the resulting deployment models will be documented in a white paper GSMA NG.132[52] and subsequently in GSMA PRD NG.113 5GS Roaming Guidelines.[53]

Given the complexities and differing needs within the roaming ecosystem, it is no surprise that the requirements across the business, technical and security focused groups do not always align. To meet the near-term deployment timelines for the initial roaming use cases, the 3GPP defined deployment models are currently being addressed by the specific use case.[54]

Phase I specified the guidelines for the bilateral Inter-PLMN connection deployment scenarios along with SEPP Outsourcing and Mobile Operator Group with a shared SEPP. The deployment model for Phase I utilizes direct TLS. It makes use of the Internet Packet Exchange (IPX) network for transport, routing and end-to-end QoS.

Phase II, currently under discussion within the GSMA, will focus on deployment when a roaming partner outsources some or most of their roaming responsibilities or needs to intermediaries, focusing on outsourced security responsibilities. Roaming Hubs (RH) are a unique case that are not accounted for within the current 3GPP specifications. Documenting the full scope of

Figure 4.1 Service Based Interfaces in Home Routing (HR) Roaming Architecture[64]



their role in the roaming ecosystem, particularly in 5G SA, and their role's impact on security is vital in communicating back to 3GPP for solution assessment.

The IPX Providers scope can range from transport to more comprehensive in transit and cascaded IPX services. The services beyond transport are typically seen as business operating models and often value-added services. Both RHs and IPX Providers play a key role in the roaming ecosystem and operators expect to employ these intermediaries in 5G SA. Supporting the requested services utilizing the new 5G security controls is vital and will require compromise and innovation.

Finally, provision of Roaming Value-Added Services (RVAS), from welcome SMS to steering of roaming, will be addressed in a way that aligns with the 5G SA service based architecture and minimizes any interconnect risks.

Another critical component of Inter-PLMN security is the use of certificates and key management. To achieve the defined peer authentication, message integrity and confidential communication, 5G Inter-PLMN roaming security requires the use of cryptographic keys.[55] Key management refers to how mobile operators and roaming intermediaries (for example, RH and IPX provider) exchange certificates and how the trust relationship is established and managed between roaming partners. Keys will need to be exchanged between the different stakeholders involved in roaming and represents a new burden for the roaming ecosystem and operations teams.

While 3GPP defines the security controls, the GSMA is responsible for defining these methods and procedures for implementing the security controls. A manual method for certificate exchange has been defined within the GSMA and work is ongoing to define and develop an automated method. The details of key and certificate management in 5GS can be found in GSMA PRD FS.34.[56] The increased emphasis and need for security controls is leading to the expanded use of certificates across multiple areas of our industry. This proliferation of certificate use may lead to the 3GPP addressing certificate security in later 3GPP releases.

There is little argument that while the Inter-PLMN services offered today are valuable and needed by the ecosystem to support a robust roaming environment, the method for delivery of these services will need to change to support secure inter-operator communications going forward. It is expected that all the needed use cases and deployment models for initial 5G SA roaming will be addressed and defined within the GSMA by the end of 2022.

5. Considerations

5G is the first generation of mobile technology designed for the cloud. MNOs are accountable for the security posture of 5G cloud deployments, and the following actions should be considered for a strong security posture:

1. *Implement a Zero Trust Architecture (ZTA) to protect 5G cloud deployments from external and internal threats. NIST SP 800-207*[57] *and CISA Guidelines for a Secure 5G Cloud Infrastructure*[58] *are good references. Recommended security controls include micro-segmentation, resource isolation, continuous monitoring and logging, TLS 1.3 with PKI-based X.509 certificates, MFA, IAM, and data protection. Security controls for a ZTA should be decided using a risk-based analysis.*

2. *Ensure the cloud deployment aligns with the MNO's security governance. Perform security configuration validation and ensure industry best practices are implemented.*

3. *While the Cloud Shared Responsibility Model provides a guideline for delegation of security responsibilities to the CSP, the MNO should ensure that their cybersecurity organizations are positioned accordingly to address the related security challenges.*

4. *Use only industry approved and non-deprecated, secure versions of APIs, protocols and cipher suites.*

5. *Implement and operate a robust software patch and update program that includes the operating system software.*

6. *The cloud can introduce additional supply chain risks. Treat cloud service provider partners as third-party vendors and leverage mature Supply Chain Risk Management (SCRM) and Third-Party Risk Management (TPRM) programs to ensure alignment with the organization's security governance.*

7. *Ensure 5G software vendors implement secure software assurance with a shift-left philosophy built upon secure software development, continuous integration/continuous delivery and DevSecOps early in the software development lifecycle.*

8. *Cloud service providers, product vendors and software providers should provide the MNOs with a Software Bill of Materials (SBOM) so the MNOs can perform risk and vulnerability assessments on the delivered and/or underlying operational software to confirm it does not contain known critical vulnerabilities inherited from third parties, free and/or open-source software.*

9. *Require cloud service providers, product vendors and software providers to perform independent 3rd-party certification for penetration testing and vulnerability assessments.*

10. *The GSMA's NESAS assessment is a valuable tool to ensure the 5G software vendor is following industry best security practices in their product development lifecycle including DevSecOps and Supply Chain. That tool or other approved assessment tools could be used.*

11. *Third-party applications in the O-RAN ecosystem, called rApps and xApps, could introduce additional risk. The SMO platform vendor and MNO must practice due diligence to ensure these applications are trusted, securely on-boarded, and designed with proper security controls.*

Conclusions

5G deployments are migrating to the cloud to achieve low latencies, enabling new use cases, and greater network efficiencies and resource optimization by leveraging automation, orchestration, and intelligence in the cloud. Traditionally, mobile networks have been deployed on the Mobile Network Operator (MNO) premises, providing inherent security advantages. While the cloud can also provide security advantages, it also introduces new security risks that expand the 5G attack surface. The success of 5G deployments in the cloud will depend upon the security posture of those deployments, for which the MNO is accountable. The MNO may delegate responsibility for security based upon the Cloud Shared Responsibility Model, but the MNO is always responsible for selection and configuration of security controls to protect network functions and data at rest, in motion and in use.

A strong 5G cloud security posture is based upon a Zero Trust Architecture (ZTA), which provides security controls to mitigate attacks from external and internal threats. The ZTA approach to protect 5G networks from internal threats is a shift in security philosophy, which traditionally has considered perimeter security protecting against external threats to be sufficient. With the pursuit of a ZTA, 5G cloud deployments will leverage existing security controls provided in 3GPP standards and implement additional security controls to protect from cloud risks due to lateral movement, multi-tenancy, shared resources and Hybrid Cloud. Continuous monitoring for threat detection and response, identity and access management, and data protection is advised. Recommended security controls include micro-segmentation, resource isolation, continuous monitoring and logging, TLS 1.3 with PKI-based X.509 certificates, MFA, IAM, and data protection.

Secure 5G cloud deployments are built through software supply chain security. 5G vendors are working to secure their supply chains. Key attributes of a viable program are:

- *Clear visibility to the full supply chain including global partners and upstream suppliers*
- *Instituting and implementing Software Bill of Materials (SBOM)*
- *Ensuring proper Supply Chain Security program scope*
- *Identifying and implementing comprehensive test, metrics, and audit processes*

The US President's Executive Order 14028 on Improving the Nation's Cybersecurity emphasized the need for ZTA and robust software supply chain protections for federal agencies but are also relevant to 5G cloud deployments as critical infrastructure. Future phases of this paper series on 5G security could extend focus 5G cloud security by reviewing recent guidance from US agencies and examining the necessary security controls for specific 5G use cases. Topics such as network slicing, self-healing network services and recoverable data for various use cases running in a 5G cloud infrastructure are under consideration.

Acronyms

AAL: Acceleration Abstraction Layer

AI: Artificial intelligence

APT: Advanced Persistent Threats

ATIS: Alliance for Telecommunications Industry Solutions

AUSF: Authentication Server Function

AWS: Amazon Web Services

BOM: Bill of Materials

CISA: Cybersecurity and Infrastructure Security Agency

CNF: Cloud-native network functions

COTS: Commercial Off the Shelf

CSA: Cloud Security Alliance

CSP: Cloud service provider

CVD: Coordinated vulnerability disclosures

CVE: Common vulnerabilities and exposures

DAR: Data at rest

DDoS: Distributed Denial of Service

DID: CHECK TEXT / EXISTING GLOSSARY FOR DEFINITION

EDR: Endpoint Detection and Response

FOSS: Free Open-Source Software

GDPR: General Data Protection Regulation

HCP: Hyperscaler Cloud Provider

HR: Home Routing

HRoT: Hardware Root of Trust

IaaS: Infrastructure as a Service

IAST: Interactive application security testing

IoC: Indicators of Compromise

ISV: Independent software vendors

IT: Information technology

KERI: Key Event Receipt Infrastructure

LI: Lawful Interception

MEC: Multi-Access Edge Compute

MFA: Multi-Factor Authentication

ML: Machine learning

MNO: Mobile Network Operator

MSP: Managed service provider

MSSP: Managed security service provider

NCCoE: National Cybersecurity Center of Excellence

NESAS: Network Equipment Security Assurance Scheme

NF: Network functions

NFV: Network Functions Virtualization

Acronyms

NIC: Network Interface Cards

NIST: National Institute of Standards and Technology

NTIA: National Telecommunications and Information Administration

NVD: National Vulnerability Database

OSC: O-RAN Software Community

OWASP: CHECK TEXT / EXISTING GLOSSARY FOR DEFINITION

PaaS: Platform as a Service

PKI: Public Key Infrastructure

PRINS: CHECK TEXT / EXISTING GLOSSARY FOR DEFINITION

RAN: Radio Access Network

RASP: Runtime Application Self-Protection

RBAC: Role-Based Access Controls

RH: Roaming Hubs

RIC: Radio Intelligent Controller

RVAS: Roaming Value-Added Services

SaaS: Software as a Service

SAST: Static Application Security Testing

SBA: Service Based Architecture

SBOM: Software Bill of Materials

SCA: Software composition analysis

SCAS: Security Assurance Specifications

SCRM: Supply Chain Risk Management

SDLC: CHECK TEXT / EXISTING GLOSSARY FOR DEFINITION

SEPP: Security Edge Protection Proxy

SMO: Service Management and Orchestration

SOC: Security operations center

SPDX: CHECK TEXT / EXISTING GLOSSARY FOR DEFINITION

SWID: CHECK TEXT / EXISTING GLOSSARY FOR DEFINITION

TBAC: Task-Based Access Controls

TDR: Threat Detection and Response

TEE: Trusted Execution Environment

TIA: Telecommunications Industry Association

TLS: Transport Layer Security

TPRM: Third-Party Risk Management

TTP: Tactics, Techniques, and Procedures

VA: Vulnerability assessment

VM: Virtual Machine

VNF: Virtual network functions

ZTA: Zero Trust Architecture

ZTNA: Zero Trust Network Access

Acknowledgments

5G Americas' Mission Statement: 5G Americas facilitates and advocates for the advancement and transformation of LTE, 5G and beyond throughout the Americas.

5G Americas' Board of Governors members include Airspan Networks, Antel, AT&T, Ciena, Cisco, Crown Castle, Ericsson, Intel, Liberty Latin America, Mavenir, Nokia, Qualcomm Incorporated, Samsung, Shaw Communications Inc., T-Mobile USA, Inc., Telefónica, VMware and WOM.

5G Americas would like to recognize the significant project leadership and important contributions of group leader Scott Poretsky of Ericsson, and Mike Barnes of Mavenir, along with many representatives from member companies on 5G Americas' Board of Governors who participated in the development of this white paper.

The contents of this document reflect the research, analysis, and conclusions of 5G Americas and may not necessarily represent the comprehensive opinions and individual viewpoints of each particular 5G Americas member company. 5G Americas provides this document and the information contained herein for informational purposes only, for use at your sole risk. 5G Americas assumes no responsibility for errors or omissions in this document. This document is subject to revision or removal at any time without notice. No representations or warranties (whether expressed or implied) are made by 5G Americas and 5G Americas is not liable for and hereby disclaims any direct, indirect, punitive, special, incidental, consequential, or exemplary damages arising out of or in connection with the use of this document and any information contained in this document.

References

1 https://www.wsj.com/articles/solarwinds-microsoft-hacks-prompt-focus-on-zero-trust-security-11619429402

2 5G Security, 5G Americas, pp 8-11, December 2022, https://www.5gamericas.org/security-for-5g/

3 The NIST Definition of Cloud Computing, NIST SP 800-145, US NIST, 2011, https://csrc.nist.gov/publications/detail/sp/800-145/final.

4 The NIST Definition of Cloud Computing, NIST SP 800-145, US NIST, 2011, https://csrc.nist.gov/publications/detail/sp/800-145/final

5 Cloud Security Alliance (CSA), Hybrid Cloud Security Working Group, https://cloudsecurityalliance.org/research/topics/hybrid-cloud-security/, last viewed May 17, 2022.

6 Security Guidance for 5G Cloud Infrastructures, Volumes 1 thru 4, US DHS Cybersecurity and Infrastructure Security Agency (CISA), October 28, 2021, https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures

7 CSA Security Guidance for Critical Areas of Focus in Cloud Computing, v4.0, Cloud Security Alliance (CSA), July 2017.

8 Center for Internet Security (CIS) Benchmarks, Center for Internet Security. https://www.cisecurity.org/cis-benchmarks

9 NIST SP 800-190, Application Container Security Guide, Souppaya, M., Morello, J., Scarfone, K., U.S. NIST, September 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf

10 CISA Cloud Security Technical Reference Architecture, v1.0, US DHS Cybersecurity and Infrastructure Security Agency (CISA), August 2021, https://www.cisa.gov/sites/default/files/publications/CISA%20Cloud%20Security%20Technical%20Reference%20Architecture_Version%201.pdf

11 Kubernetes Hardening Guide, Cybersecurity Technical Report, U.S. National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), v1.1, March 2022, https://media.defense.gov/2021/Aug/03/2002820425/-1/-1/0/CTR_Kubernetes_Hardening_Guidance_1.1_20220315.PDF

12 O-Cloud Security Analysis Technical Report, O-RAN Alliance Security Focus Group, O-RAN.SFG.O-CLOUD-Security-Analysis-TR-v01.00.docx, March 2022.

13 O-RAN O2 Interface General Aspects and Principles, O-RAN Working Group 6, O-RAN.WG6.O2-GA&P-v01.02, March 2022.

14 Acceleration Abstraction Layer (AAL)Common API, O-RAN Working Group 6, O-RAN.WG6.AAL Common API v01.0, March 2022.

15 No More Chewy Centers: Introducing The Zero Trust Model Of Information Security", J. Kindervag, Forrester, September 2010

16 Zero Trust Architecture, NIST SP 800-207, US NIST, August 2020.

17 "Executive Order on Improving the Nation's Cybersecurity", The White House, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

18 Security Guidance for 5G Cloud Infrastructures, Volumes 1 thru 4, US DHS CISA, October 2021, https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures

19 Mitigating Log4Shell and Other Log4j-Related Vulnerabilities, Alert AA21-356A, US DHS CISA, https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

20 Confidential Consortium Website, https://confidentialcomputing.io

21 Confidential Computing: Hardware-Based Trusted Execution for Applications and Data, July, 2020, 30. https://confidentialcomputing.io/wp-content/uploads/sites/85/2020/06/ConfidentialComputing_OSSNA2020.pdf

22 About SCS 9001: Supply Chain Security Standard", TIA, https://tiaonline.org/what-we-do/scs-9001-supply-chain-security-standard/

[23] “Executive Order on Improving the nation’s Cybersecurity”, EO 14028, The White House, May 2021.

[24] An exhaustive list of incidences is available at Supply Chain Compromise, Technique T1195 - Enterprise | MITRE ATT&CK®.

[25] https://www.mandiant.com/resources/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor

[26] CVE-2021-30116: https://nvd.nist.gov/vuln/detail/CVE-2021-30116

[27] Mitigating Log4Shell and Other Log4j-Related Vulnerabilities, Alert AA21-356A, US DHS CISA, https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

[28] https://www.csoonline.com/article/3227906/what-is-wannacry-ransomware-how-does-it-infect-and-who-was-responsible.html

[29] https://www.csoonline.com/article/3233210/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html

[30] Security Guidance for 5G Cloud Infrastructures, Volumes 1 thru 4, US DHS CISA, October 2021, https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures

[31] https://landscape.cncf.io/

[32] 5G Cybersecurity, NIST SP 1800-33B, preliminary draft, US NIST, April 2022, https://csrc.nist.gov/publications/detail/sp/1800-33/draft

[33] Security Guidance for 5G Cloud Infrastructures, Volumes 1 thru 4, US DHS CISA, October 2021, https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures

[34] “5G Security Evaluation Process Investigation”, v1.0, US DoD and US DHS CISA, May 2022, 5G Security Evaluation Process Investigation: Version 1, May 2022 (cisa.gov).

[35] https://wiki.o-ran-sc.org/

[36] https://openairinterface.org/

[37] Mitigating Log4Shell and Other Log4j-Related Vulnerabilities, Alert AA21-356A, US DHS CISA, https://www.cisa.gov/uscert/ncas/alerts/aa21-356a

[38] https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021

[39] O-RAN Architecture Description, v6.00, O-RAN Alliance, O-RAN.WG1.O-RAN-Architecture-Description-v06.00, Nov 2021.

[40] TS 23.288 Architecture enhancements for 5G System (5GS) to support network data analytics services

[41] Open Source Security and Risk Analysis Report, Synopsys, 2022, https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html?cmp=pr-sig

[42] “Security for 5G”, 5G Americas, Dec 2021, https://www.5gamericas.org/security-capabilities-are-a-critical-element-to-5g-success/

[43] https://startupstash.com/software-composition-analysis-tools/

[44] Samuel M. Smith https://arxiv.org/abs/1907.02143

[45] Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53, Revision 5, US NIST, Sept 2020, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[46] Security in OpenRAN, Jan 2021, https://www.mavenir.com/resources/security-in-open-ran/

[47] GSMA Network Equipment Security Assurance Scheme (NESAS), https://www.gsma.com/security/network-equipment-security-assurance-scheme/

[48] “Security for 5G”, 5G Americas, Dec 2021, https://www.5gamericas.org/

security-capabilities-are-a-critical-element-to-5g-success/

49 Network Equipment Security Assurance Scheme – Audit Guidelines, PRD FS.46, GSMA, January 2022.

50 Network Equipment Security Assurance Scheme – Product and Evidence Evaluation Methodology, PRD FS.47, GSMA, January 2022.

51 Release 16 - 3GPP TS 33.501 - Security architecture and procedures for 5G System, V16.7.0, June -2021[2] GSMA PRD NG.132 Report 5G Mobile Roaming Revisited (5GMRR)

52 GSMA PRD NG.132 Report 5G Mobile Roaming Revisited (5GMRR)

53 GSMA PRD NG.113 5GS Roaming Guidelines

54 Release 16 - 3GPP TS 33.501 - Security architecture and procedures for 5G System, V16.7.0, June -2021

55 Release 16 - 3GPP TS 33.501 - Security architecture and procedures for 5G System, V16.7.0, June -2021

56 GSMA PRD FS.34 Key Management for 4G and 5G inter-PMN Security

57 Rose, S., Borchert, O., Mitchell, S., and Connelly, S., NIST SP 800-207: “ZeroTrust Architecture”, U.S. NIST, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final.

58 https://www.cisa.gov/uscert/ncas/current-activity/2021/10/28/nsa-cisa-series-securing-5g-cloud-infrastructures

59 “Intelligent Security for Open RAN”, S. Poretsky. J. Jardal, and M. Scanlon, Ericsson, June 2022. https://www.ericsson.com/assets/local/core-network/doc/intelligent-security-guide.pdf.

60 O-RAN Minimum Viable Plan and Acceleration towards Commercialization, O-RAN Alliance, June 2021, https://www.o-ran.org/resources.

61 “Evolving 5G Security for the Cloud”, S. Poretsky, Ericsson blog, January 2022. https://www.ericsson.com/en/blog/6/2022/evolving-5g-security-for-the-cloud

62 “Open-source software in an ICT context”, Ericsson, blog, Jan 2021, https://www.ericsson.com/en/blog/2021/1/open-source-security-software

63 GSMA FS.13, version 2.1, GSMA

64 5G Roaming Guidelines, GSMA PRD NG.113, v2.0, GSMA, May 2020.