DEC 2021

A 5G Americas White Paper

SECURITY FOR 5G

5G americas

Contents

Executive Summary

Each generation of cellular technology has been more secure than the previous version and 5G is no exception. 3GPP has standardized 5G to be the most secure foundational wireless technology yet and first cellular technology designed for cloud deployments, which requires further security considerations.

5G network functions for Core and RAN are evolving to become cloud-native, enabling open interfaces, containerized applications, and cloud-based deployments. This evolution will impact the security posture of 5G networks as cloud security best practices, multi-layer security controls, zero-trust architecture (ZTA), and supply chain security must be considered. In the cloud's multi-stakeholder environment, cloud-native function (CNF) software vendors, platform vendors, mobile network operators (MNOs), hyperscale cloud providers (HCPs), and system integrators (SIs) must collaborate to clearly define roles and responsibilities for implementing security architecture and controls.

In addition to providing an update on the security enhancements introduced by 3GPP in releases 15 and 16, this paper builds upon prior 5G Americas publications addressing 5G security by providing considerations for securing 5G in Private, Public, and Hybrid cloud deployment models. Topics such as orchestration, automation, cloud-native security, and application programming interface (API) security are addressed while also discussing the transition from perimeter-based security to a zero-trust architecture to protect assets and data from external and internal threats. Recommendations for securing non-public 5G networks are provided for the vertical segments including vehicle to everything (V2X), smart manufacturing, fixed-wireless access, and critical infrastructure.

Recent cyberattacks, particularly in the US, have highlighted the importance of securing the 5G supply chain. This paper also addresses supply chain security with focus on the use of trusted suppliers, secure use of open-source software, secure software development, DevSecOps, and internal adoption of software bill of materials (SBOM) as part of a software assurance program. This paper also provides a current assessment of Open RAN security as its standards continue to mature to meet the level of security expected by 5G network operators and their users.

This paper makes the following recommendations for securing 5G networks:

- *Build 5G networks with a ZTA that is complemented with perimeter security to provide protection from internal and external threats.*
- *Implement a 3GPP Release 16 5G standalone network to benefit from security enhancements that support a zero-trust architecture and follow CSRIC VII recommendations.*
- *Follow industry best practices for secure cloud deployments, including secure CNF, orchestration, automation, APIs, and infrastructure. These best practices are applicable to private, public, and hybrid deployment models.*
- *Consider supply chain security as a component of 5G security. Use trusted suppliers that follow industry best practices for secure development processes.*

1. Introduction

Communication service providers (CSPs) are starting to realize the potential of 5G by enabling new innovative services. However, such potential will not be realized without building and maintaining a secure 5G network. Deployment of 5G networks is well underway, but the work to ensure these networks are secure is ongoing. Given the recent cyberattacks on non-mobile networks in the United States, from the SolarWinds breach to the pipeline ransomware attack to the Kaseya ransomware attack, security of critical infrastructure including information and communications technology (ICT) networks is front and center. Security is a critical component of 5G architecture for Standards Development Organizations (SDOs), industry forums, vendors of network functions, and MNOs. Focus on security threats and controls will continue to be necessary to gain the trust of enterprises, manufacturing, critical infrastructure providers, and governments that are exploring opportunities to leverage 5G for improved communications, operations, and new revenue streams.

Past 5G Americas papers have provided an overview of 5G security standards developed at 3GPP. Those papers addressed the attack surface and identified potential security risks with use of 4G in the Non-Standalone Architecture (NSA), Internet of Things (IoT) devices, User Equipment (UE) with limited security capabilities, roaming, and internetworking. Security controls to mitigate risk in the Radio Access Network (RAN), 5G Core (5GC), and interconnects were discussed, including mutual authentication between UEs and the network, identity management, volumetric Distributed Denial of Service (DDoS) mitigation, application DDoS mitigation, and 5G network slicing for traffic segmentation and tailored security controls.

A subsequent 5G Americas paper[1] took a deeper look into the cloud native and software-controlled threats and vulnerabilities. That paper differentiated between non-standalone (NSA) and standalone (SA) issues with a focus on disaggregation, virtualization, network function virtualization (NFV), and software-defined networks (SDN) areas of 5G architecture. Other topics such as data security at the edge, private 5G and specific RAN concerns were addressed. Recommended mitigations to secure 5G networks were proposed, including zero-trust, cyber threat intelligence, and network slicing.

This paper builds upon that prior work and focuses on evolving 5G security considerations, such as 3GPP Release 16 security enhancements, 5G use cases, zero-trust architecture (ZTA), supply chain security, secure 5G vertical segments and open RAN security. The goal of this paper is to address these security topics in the context of the evolution to cloud-based and distributed 5G networks. The authors aim to promote better security practices in which the organization's security posture is periodically re-assessed to address changes in risk from evolving threats, attack vectors, risk tolerance, and security control technologies.

2. 3GPP Security Enhancements in 5G

3GPP has standardized 5G in releases 15 and 16. 3GPP release 15 introduced the following security improvements:

- *Subscriber authentication: secure mutual authentication using 5G Authentication and Key Agreement (5G-AKA), Extensible Authentication Protocol Authentication and Key Agreement Prime (EAP-AKA'), and Extensible Authentication Protocol – Transport Layer Security (EAP-TLS), Home Control of authentication for roaming devices, and non-SIM card-based authentication for IoT devices*
- *Subscriber privacy: Stronger False Base Station (FBS) protection and Subscription Permanent Identifier/Subscription Concealed Identifier (SUPI/SUCI) for encrypted long-term subscriber identifiers. CSRIC VII recommends that the SUCI feature is mandatory for U.S. deployments, except when the UE is requesting emergency services.*
- *Secure service-based architecture (SBA): TLS and OAuth 2.0 on all mandatory functions*
- *Secure roaming interconnects: introduction of the Security Edge Protection Proxy (SEPP) at the application layer*

3GPP release 16 introduced additional 5G security enhancements including:

- *Inter-PLMN User Plane Security (IPUPS): The role of the User-Plane Function (UPF) is expanded to include traffic protection with a "common firewall" between two roaming PLMNs.*
- *Full-rate User Plane Integrity Protection: CSRIC VII recommends that this feature is mandatory for Release 16 U.S. deployments.*
- *Network Slice Specific Authentication and Authorization (NSSAA): provides separate authentication and authorization per network slice.*
- *Non-Public Networks (NPN): 5G Private networks to provide security and privacy on dedicated resources that are independently managed.*
- *Use case specific security enhancements for cellular IoT and URLLC services.*

3GPP security enhancements in release 16 are covered further in a later section.

3. 5G Security Considerations

3GPP has standardized each generation of mobile technology to be more secure than its predecessor and 5G is the most secure yet. Nevertheless, our risk tolerance has decreased because of the increased impact a cyberattack on a 5G network could pose as society increasingly relies upon it for critical infrastructure, mission critical applications, public safety, smart manufacturing, connected car, and other real-time, low latency use cases.

5G is the first cellular technology designed for the cloud. The cloudification of the 5G RAN and Core leverages cloud security best practices to protect networks, applications, and data, while also introducing new security risks associated with the cloud that must be considered for 5G deployments. Cloud deployments of RAN and Core should be built upon a foundation of zero-trust with a strong security posture based upon industry best practices and standards for cloud security, Cloud-Native Function (CNF) security, and secure use of open-source software.

This section further describes evolving security considerations for 5G, including 3GPP security enhancements in 5G releases 15 and 16, cloud deployment models, orchestration, automation, cloud-native security, and application programming interface (API) security. Zero-trust is discussed further in a dedicated section later in this document.

3.1 Deployment Models

U.S. National Institute for Standards and Technology (NIST) defines three cloud service models: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). For service delivery, NIST has defined four cloud deployment models: Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud. The Cloud Security Alliance (CSA), which provides guidance to support business goals while managing and mitigating the risks associated with the adoption of cloud computing technology, uses the NIST defined cloud service and deployment models. 5G RAN and Core can be deployed using the NIST cloud deployment models in which vendors of CNFs and hardware, network operators, and cloud providers are stakeholders who must establish a multi-party relationship with defined roles and responsibilities for security controls. There are also further 3GPP studies ongoing regarding security for on-premises and off-premises deployment models.

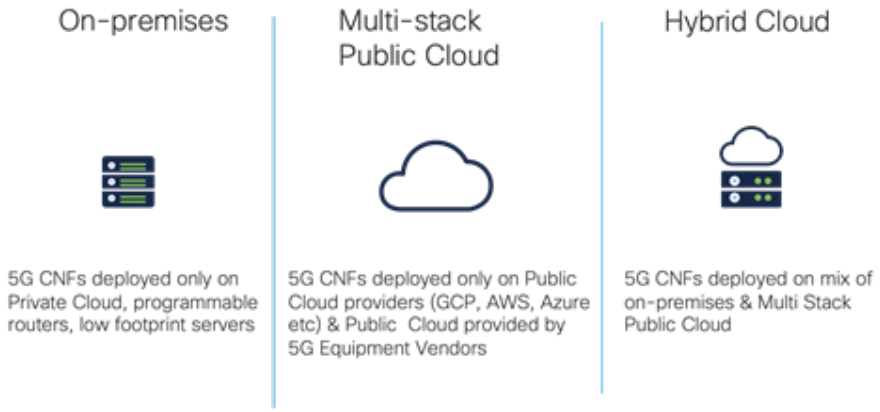
5G networks can be virtualized, software-driven with open, flexible deployment models that leverage cloud technologies and software-defined platforms in which networking functionality is managed through software rather than hardware. 5G networks can create software-defined subnetwork constructs known as network slices which enables network operators to create an isolated end to end network consisting of both virtualized and physical components. Network slices can be tailored using automated provisioning and proactive management of traffic and services to fulfill diverse service level QoS and security requirements requested for a particular application or customer.

Advancements in virtualization, cloud-based technologies, adoption of APIs, IT and business process automation enable 5G architecture to be agile and flexible and to provide anytime, anywhere user access. An example is the flexible control of multi stacks within the public cloud. Each stack is a cluster of CNFs and 3rd party applications grouped together for enabling particular use case. Having control over each of the individual stacks allows tighter security control in public cloud deployments. 5G RAN and Core CNFs can be deployed using the following options:

1. **On-premises (Private Cloud) Deployments: 5G CNFs deployed within the private data center with programmable access and aggregation routers. NIST refers to this as the Private Cloud deployment model.**

2. **Public Cloud Deployments: 5G CNFs deployed within the multi stack public cloud of Hyperscale Cloud Providers (HCPs) or a public cloud provided by Managed Service Providers (MSPs).**

Figure 1. 5G Deployment Models[54]



3. **Hybrid Deployments: 5G CNFs deployed as a composition of both the multi stack public cloud and on-premises.**

Most security controls would be similar across all deployment models illustrated in Figure 1, but the priority of the security controls would differ in each model. For example, for on-premises deployments perimeter security needs to be carefully planned and configured, while in public cloud deployments certain perimeter security controls, such as firewalls, although necessary, would be lower priority than other security controls such as granular application to user mapping due to greater risk from internal threats.

5G multi-stack public cloud deployments present additional security challenges, especially where the enterprise may control the information systems security policies in a manner not consistent with MNOs. To deal with these cases, Cloud Access Security Brokers (CASB) can provide insight into

Definitions of Cloud-Native Applications, Stack, and Security:

1. *Cloud-native applications*: applications specifically designed to take advantage of innovations in cloud computing. These applications integrate easily with their respective cloud architectures, taking advantage of the cloud's resources and scaling capabilities. It also refers to applications that take advantage of innovations in infrastructure driven by cloud computing. Cloud native applications today include apps that run in a cloud provider's datacenter and on cloud native platforms on-premise. Source: glossary/cloud_native_apps.md at main · cncf/glossary · GitHub

2. *Cloud-native stack*: technologies used to build cloud native applications. Enabling organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds, cloud native technologies uphold the 'promise of the cloud' and leverage cloud computing benefits to their fullest. They are designed from the ground up to exploit the capabilities of cloud computing and containers, service meshes, microservices, and immutable infrastructure exemplify this approach. Source: glossary/cloud_native_tech.md at main · cncf/glossary · GitHub

3. *Cloud-native security:* an approach that builds security into cloud native applications. It ensures that security is part of the entire application lifecycle from development to production. Cloud native security seeks to ensure the same standards as traditional security models while adapting to the particulars of cloud native environments, namely rapid code changes and highly ephemeral infrastructure. Cloud native security is highly related to the practice called DevSecOps. Source: glossary/cloud_native_security.md at main · cncf/glossary · GitHub

non-compliances, which is useful for regulated industries. Furthermore, as data (such as network performance metrics, configuration files and SBI communications) needs to be exchanged between cloud vendors, an API Gateway, Integration Broker, or Web Application Firewall may be required to ensure the data is pushed/pulled securely between two or more clouds. Integration between the vendor's Role Based Access Control (RBAC) and operator's Identity and Access Management (IAM) is required to ensure granular access control for least-privilege access to specific authorized users.

3.2 Cloud-Native Security

Mobile core networks are evolving from 2G and 3G with proprietary physical hardware, to 4G running virtual machines (VMs) and virtual network functions (VNFs), to 5G running VNFs and CNFs. The term 'cloud-native' refers to building and running applications that take advantage of the distributed computing offered by a cloud delivery model. Cloud native apps are designed and built to exploit the scale, elasticity, resiliency, and flexibility of the cloud.

As defined by the Cloud Native Computing Foundation (CNCF), cloud-native technologies empower organizations to build and run scalable applications in modern, dynamic environments such as public, private, and hybrid clouds. Containers, service meshes, microservices, immutable infrastructure, and declarative APIs exemplify this approach. These techniques enable loosely coupled systems that are resilient, manageable, and observable. Combined with robust automation, they allow engineers to make high-impact changes frequently and predictably with minimal toil.[2]

Figure 2 illustrates the evolution in packet core infrastructure from physical monolith packet cores in 2G and 3G to virtualized cloud native packet core deployment in 5G. 5G introduces CNFs, which is a software implementation of network functions that can be deployed in a private or public cloud environment. CNFs communicate with each other using APIs, further extending the attack surface. This section discusses cloud-native security in 5G.

Although the system resource utilization in proprietary physical servers used in legacy cellular technologies is lower, it allows good isolation by providing physical separation of management and user plane with separate ports, line cards and CPU. Although virtualized cloud native deployment of 5G network functions such as 5GC and 5G RAN allows flexibility and scalability in deployment, it also introduces new vulnerabilities. The CNF approach for building 5G NF components allows use of an open-source software stack to develop the 5GC and 5G RAN CNFs, which increases risk in 5G deployments. Previous cellular technologies used a perimeter defense around the centralized packet core components. 5G CNFs are infrastructure agnostic and can be deployed on-premises or in the public cloud, obfuscating the perimeter and thereby making perimeter-based security less effective.

Network Function Virtualization Infrastructure (NFVI) security relates to hardening the NFVI hardware, secure east-west traffic flow between devices and the data center, and VNFs deployed as VMs. Cloud-Native Functions (CNFs) are the evolution from VMs to containers. CNF security best practices include micro-segmentation and isolation, detecting malicious behavior of the virtual functions, securing the third-party application and API, and securing and segmenting the network interfaces, roaming, and peering interfaces, and then securing the user access and the orchestration layer.

Cloud-native deployments of 5G network functions in 5GC and 5G RAN provide flexibility and scalability but may introduce new risks due to increased internal threats. The expanded attack surface with 5G CNF deployments can be split into 3 categories: container vulnerabilities, insecure container networking vulnerabilities, and hardware and host OS vulnerabilities. Example vulnerabilities for each of these categories are shown in Figure 3.

Securing 5G CNFs requires a new mindset towards securing a 5G environment. The key security controls and processes required to secure 5G CNFs can be grouped as listed below and discussed further in sections below:[3]

- *Secure CI/CD and implementing DevSecOps practices*
- *Securing 5G CNF run-time*
- *Securing 5G CNFs and traffic*
- *Securing 5G CNF orchestration and access controls*
- *Securing 5G CNFs in roaming scenarios*
- *Securing Host OS and HW*

3.3 API Security

The service-based architecture of 5G networks enables introduction of CNFs, which bring elasticity, scalability, and creation of rich services for operators to expose

Figure 2: Evolution to 5G CNFs

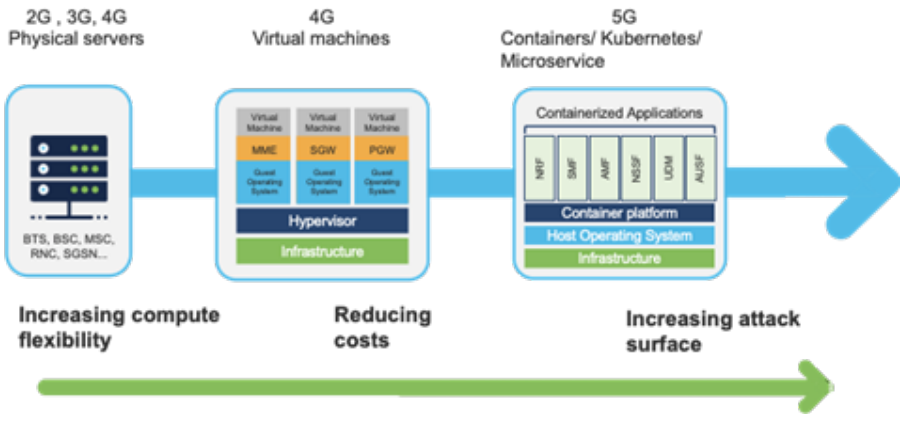


Figure 3: Security risks within the 5G CNF deployments.

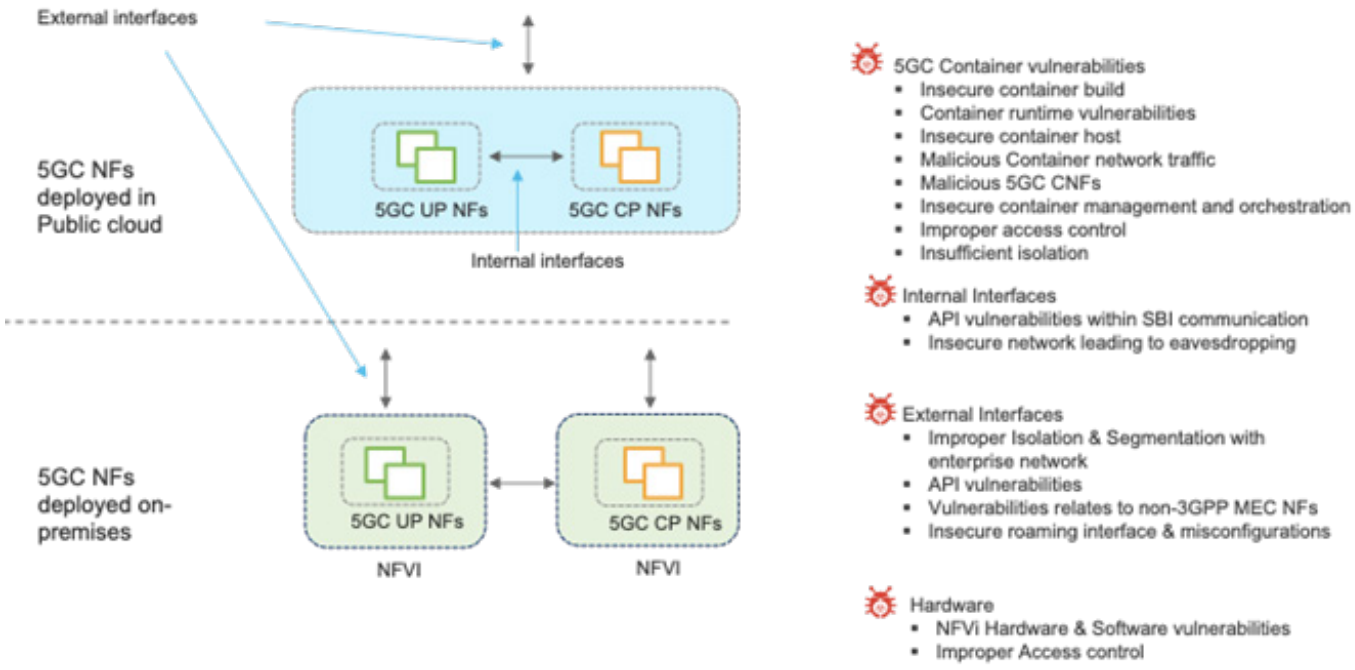
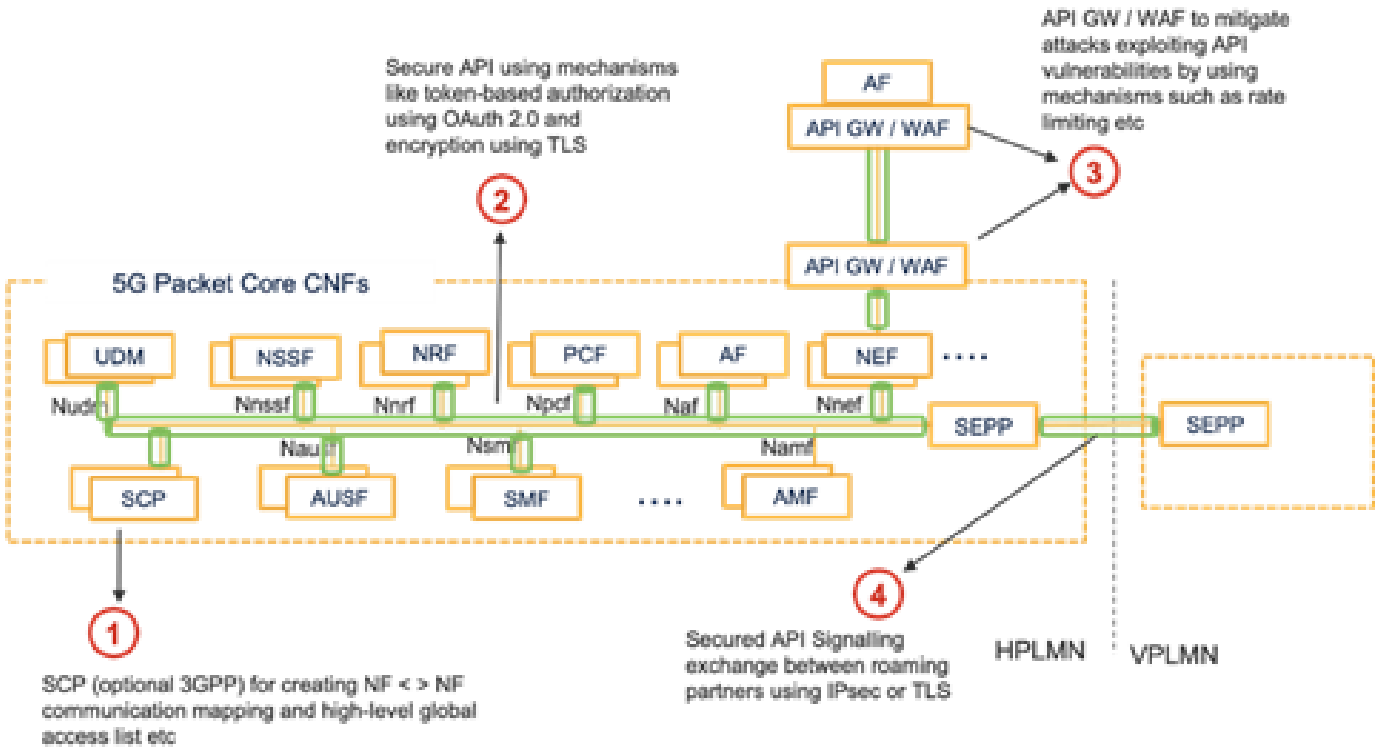


Figure 4. API Security controls in the 5G Service Based Architecture (SBA)[55]



through the cloud and RESTful APIs. Apart from communications between 5G CNFs within SBA and roaming inter-connectivity, APIs also facilitate integration between different solutions and information sharing for 3rd party applications

Multi-Access Edge Compute (MEC) is one of the key pillars for meeting the low latency demands of 5G use cases where data is processed and stored at the network edge to bring technology resources closer to the user. API introduction for 5G MEC applications also brings in the expertise of the web application developers to develop 3rd party 5G related MEC applications. The 3rd party MEC applications deployed at the edge require API integration with the MEC application server and possibly other 5GC network functions. An API that is not deployed following industry best practices can introduce attack vectors related to insecure API security risks such as user and function-level authorization, excessive data exposure, and broken object level that are more prominent in 5G MEC deployments.[4]

Figure 4 shows the following four security controls for securing API in the Service Based Architecture (SBA):

1. **Service Communication Proxy (SCP), optional for 3GPP, for creating NF to NF communication mapping, load balancing, high level global access list and so on**
2. **Secure API using mechanisms like token-based authorization and encryption using TLS (TLSv1.3 is recommended)**
3. **API Gateway or Web Application Firewall (WAF) to protect against attacks exploiting API vulnerabilities**
4. **Securing external API communications using IPsec or TLS**

API security controls includes mechanisms such as strong authentication and authorization mechanism, encryption of the message contents as the basic requirements, and strong security protocols and algorithms. End systems must be protected from unauthorized access by proper authentication as well as by allowing only the Transmission Control Protocol/User Datagram Protocol (TCP/UDP) ports used for APIs and blocking the rest. Application-level Distributed Denial of Service (DDoS) is a common type of attack that exploits systems invoking APIs to partially or completely cripple network availability. An important component of API security is API Policy enforcement of permitted connection endpoints, rate limiting, and types of APIs between specific end points.

For secure inter-NF communications within 5GC, SBA defined by 3GPP TS 33.501[5] specifies authentication, authorization, and encryption of API calls between the 5GC NFs. The authentication and transport security using encryption can be supplied by using TLS 1.2, or 1.3, and token-based authorization using OAuth 2.0 can be used for authorization of NFs. 3GPP has also taken steps in enhancing the security for the external API communication by introducing security features and security mechanisms for the common API framework (CAPIF) as specified in 3GPP TS 33.122.[6]

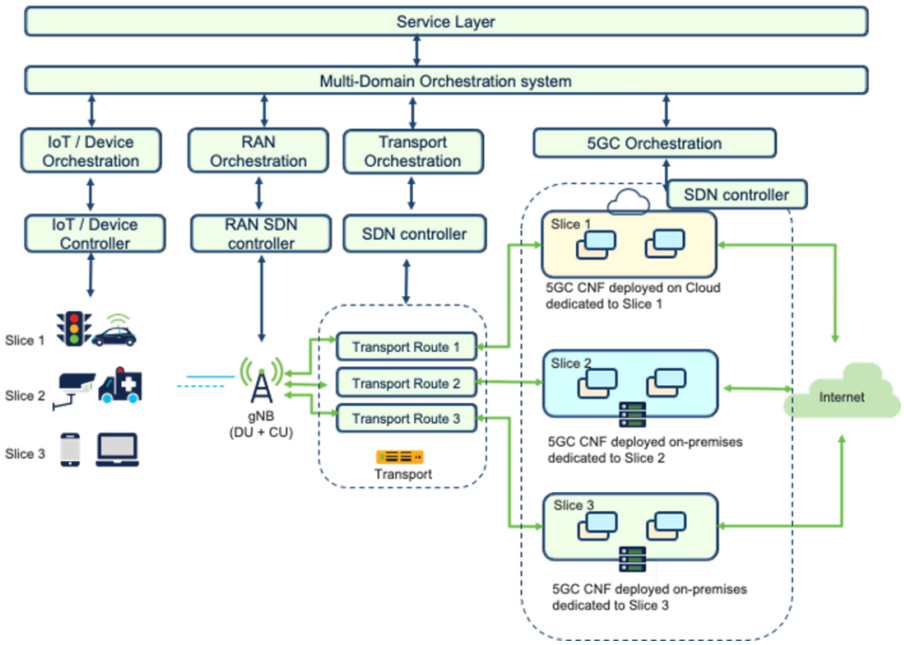
3.4 Orchestration and Automation

The wide variety of new use cases in 5G requires flexibility for deploying 5G network functions across RAN, Transport and 5GC. As illustrated in Figure 5, this flexibility is provided by multidomain network orchestration and SDN architectures, which enables the common infrastructure to efficiently deliver orchestration and automation of multiple 5G network instances with tailored services. Common abstractions allowed by SDN-enable resources such as networking, processing, and storage types to fulfill a business purpose, while open and programmable interfaces in SDN and Orchestration layers allow dynamic control and automation of network slice creation and operation.[7]

While orchestration and automation provide flexible, dynamic network configurations, these also introduce an expanded attack surface to exploit vulnerabilities from improper isolation, insecure API implementation that leads to risks such as unauthorized user and function-level access, excessive data exposure, broken object level. Risks in SDN components are data exfiltration, data hoarding and sniffing, unauthorized user access, and DoS/DDoS attacks on the SDN/ Orchestration and Automation layers, which attack network availability by degrading service creation capabilities.

Several steps can be taken to mitigate risks in orchestration and automation, including:

Figure 5: Service, Orchestration, and Automation layers in a 5G network



- *Implementation of RBAC, and more granular access controls such as microservice to user policy mapping, to authorize access to the Service Layer, Orchestration, SDN and 5G network functions that are deployed in the public cloud, on-premises, or hybrid models.*
- *The Orchestration and Automation layer should be able to integrate with an application protection and policy enforcement layer, which scans all software images before execution to enforce policy checking and validate execution permissions. Such scans should prevent the deployment of untrusted and vulnerable images, block containers that violate its runtime model based on the configured runtime rules and prevent deployment of such instances by the orchestration solution.*
- *The Orchestration and Automation layers should be closely monitored to detect any behavioral anomalies, helping to mitigate risks such as data exfiltration and data hoarding.*
- *A strong secure API strategy, including conducting penetration tests and audits on APIs and applications using APIs, helps to ensure secure APIs, thereby contributing to secure orchestration and automation communication with the network functions. API security was discussed in the previous section.*

3.5 Network Management

MNOs face operational complexities due to the scaling requirements and NFV demands introduced in the 5G Core and RAN. Network management has grown from network engineers manually logging into infrastructure to configure or troubleshoot, into a plethora of automated systems that use orchestration and APIs to enable an elastic network fabric. Historically, network availability was mostly vulnerable to user errors, such as accidental manual misconfigurations or broadcast storms after an engineer did a port down/up command. Network availability was also vulnerable to an insider who could unintentionally or maliciously cause service disruption.

These risks still exist in today's 5G network, but now MNOs are required to leverage more automation, orchestration, and software-based intelligence (e.g., Software Defined Networking) that are delivered by the infrastructure vendors. Traditionally, the network operations organizations would be able to select various automation tools, such as Simple Network Management Protocol (SNMP), and exercise full control over the dynamic routing protocols in their networks. Now much of that control is being transitioned from the bolt-on operational tools into the network functions delivered by infrastructure vendors.

MNOs have new tools to face these complexities. Advanced monitoring tools and capabilities can monitor these operational complexities to detect and mitigate misbehaving network function orchestration and automation in real-time. Behavioral analytics is one advanced capability to identify whether a network function or equipment was compromised in the supply chain, or a potential insider manipulated the logic of the tools to disrupt the network. For example, behavioral analytics can use machine learning technology to monitor a network function's control plane, user plane, and/or management traffic patterns to identify outliers and anomalies, which could signal an embedded software package, library, or binary was compromised in the supply chain or a potential insider is performing a data exfiltration attack.

5G is opening new threat surfaces and exposure points, including Network Exposure Function, Multi-Access Edge Computing, Non-Public/Private Networks, Security Edge Protection Proxy, Network Slice-Specific Authentication/Authorization, and exposed APIs. Advanced security anomaly detection capabilities are foundational for the systems providing network and cyber resiliency within these complex environments and network exposure points.

3.6 Automated Security

The increased openness of the 5G network and its exposed services requires MNOs and industry verticals deploying Non-Public Networks (NPN)/Private 5G networks to act quickly in securing mobile connectivity. The benefits of pervasive connectivity must be weighed against the increased attack surface resulting from the envisioned global connectivity of billions of users and devices. To establish automated security in these digitally delivered services, MNOs must stay ahead of the growing security issues and tackle them in an efficient and automated manner. Hence, automated security is considered more of a framework that requires the creation of well-defined build and care processes throughout its continuous lifecycle.

The complexity of various underlying cloud technologies reinforces the importance of augmenting managed security of the 5G network, and its services, with automation. Automated security in 5G includes, but is not limited to:

- *Handling the complexity and dynamicity introduced by 5G network components and services*
- *Reducing response time to security incidents by providing rapid provisioning and ability to manipulate security settings and services*
- *Creating a security feedback loop that spans multiple 5G network components, so workflows and configurations can be securely maintained, policies and rules can be dynamically applied, and the overall security service lifecycle can be continuously managed.*

3.7 5G Layered Security Controls

Securing Data Center (DC) and cloud components is critical as 5G CNFs can be deployed on premises or in the public cloud. A secure DC has perimeter security at the trust border, and zero-trust to protect against external and internal threats.

5G brings distributed deployments, dynamic workloads, and encrypted interfaces, which require end-to-end visibility to ensure proper security posture including anomalous behavior detection. Advanced threat detection and DDoS protection mechanisms should also be used to mitigate attacks from the devices deployed within the infrastructure.

5G also enables Private/NPN deployments, in which the enterprise has deployed RAN infrastructure, user plane functions of 5G, and the MEC application within the enterprise perimeter as CNFs. The network will be responsible for granting network access and the MEC application will be responsible for granting access to MEC applications, such as a robotics controller. Such deployments ensure proper isolation by using micro-segmentation between the cloud native network functions (CNFs), provide secure communication between the CNFs, and enforce granular access control between the users and the CNFs. A risk mitigation strategy using multiple layers of security, as shown in Figure 6, should be implemented to establish trust between each user, the user's device, and/or a hardware authentication device, such as a YubiKey, accessing a private 5G network and MEC application.

A solid cloud native security strategy uses innovations in cloud native industry which provides more granular security controls over the applications in the software defined perimeter scenarios. Adoption of Service Mesh, which is a transparent layer enabling flexible configuration and control of interactions between distributed CNFs across multiple CNF clusters, provides a reliable and consistent way to connect, observe and apply granular micro-segmentation to cloud native perimeter-less deployments.8 It provides other key features such as service to service authentication, policy creation, load balancing and traffic routing. Security controls such as vulnerability assessment, patch management, enhanced visibility, Anti-DDoS solution and a threat intel with artificial intelligence (AI) and machine learning (ML) should also be used to proactively detect and mitigate threats towards the 5G CNFs irrespective of where the CNFs are deployed, thereby securing the software defined perimeter.

Figure 6: Layered 5G security controls

4. Zero-Trust

Traditional networks are based on defined perimeters, where most mobile packet core functions are centralized. The evolving mobile packet core architectures create software-defined perimeters. The 5G RAN and Core may be based on a cloud-native architecture which allows 5G CNFs to be deployed as microservices in the MNO's private data center or in a public cloud. Multiple vendors will supply NFV Infrastructure (NFVI) components, VNFs, and CNFs for which there will be contractors and sub-contractors requiring access to the 5G network for support, configuration, and deployment purposes.

Perimeter security assumes that the network inside the perimeter is secure and users who have gained access to network functions and data inside that perimeter can be trusted. Perimeter security does not fully protect against threats from supply chain, internal threats, and malware infection supporting lateral movement. The Solarwinds and Kaseya supply chain attacks and other recent attacks that exploit the perimeter security approach are driving implementation of perimeter-less security based upon a zero-trust architecture (ZTA), in which there is no implicit trust granted to assets or users based on physical or network location, or ownership.[9]

Zero-trust is a security model built on the principle that no user or network function can be trusted, whether internal or external to the network. Zero-trust shifts the focus away from network perimeter security, instead restricting access by internal and external users and software components through use of strong authentication and least privilege authorization. As defined by NIST,[10] Zero-trust focuses on protecting resources, including assets, services, workflows, and accounts instead of protecting network segments. ZTA is built upon the principles of zero-trust to minimize access to resources, such as data, compute resources, applications, and services, to only those subjects and assets identified as needing access, as well as continually authenticating and authorizing the identity and security posture of each access request.

MNOs had designated certain devices, applications, and users as "trusted" and then allowed them broad access to other parts of the network. Threat actors could exploit this, which drives the need for new requirements to provide a robust ZTA for 5G networks. Zero-Trust capabilities are inherently available, by standard, in 5G to mitigate security risks. The 3GPP Release 15 and 16 standards for 5G define relevant network security features supporting a zero-trust approach that, if used, could enable MNOs to implement varied deployments of NIST (SP) 800-207 ZTA based on the operator's network deployment options. Enforcement using risk-based and adaptive access policies, while enabling secure connections to devices and applications, may then be undertaken. After access is granted, zero-trust principles demand that security teams monitor how data is used.

NIST's Seven Tenets of Zero-Trust

T1. All data sources and computing services are considered resources.

T2. All communication is secured regardless of network location.

T3. Access to individual [operator] resources is granted on a per-session basis.

T4. Access to resources is determined by dynamic policy – including the observable state of client identity, application/service, and the requesting asset – and may include other behavioral and environmental attributes.

T5. The [operator] monitors and measures the integrity and security posture of all owned and associated assets.

T6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.

T7. The [operator] collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture

5G networks, which contain cloud-based assets, along with an increasing number of users, devices and machines, could benefit from zero-trust initiatives. Zero-Trust is not a "rip and replace" model. Instead, a ZTA can augment existing architecture using three logical elements as illustrated in Figure 7. The Policy Engine (PE) and Policy Administrator (PA) together form the Policy Decision Point (PDP) that makes decisions enforced by the Policy Enforcement Point (PEP). Policy frameworks are employed in 3GPP-based systems to manage access to resources in different security domains. For example, to gain access to the 5G network services (tenet T1), the user equipment (UE) contacts an Access and Mobility Management Function (AMF) that takes a PEP role. A PDP role can be represented by multiple NFs where Unified Data Management (UDM) and the Policy Control Function (PCF).[11]

Zero-Trust can be applied in different ways and adapted for various systems, including 5G. 5G ZTA is end-to-end including RAN, Transport, and Core, and consists of multiple layers of security to establish trust in user identity, enhanced end-to-end visibility, and trustworthiness of each user device accessing the Data Control Network (DCN) using any cloud deployment model, as discussed in a previous section. The mapping of NIST's ZTA to 5G network functions[12] is shown in Figure 8. Table 1 summarizes the applicability of NIST's seven tenets of a ZTA to 5G networks. For further information about zero-trust in 5G networks, see paper "Zero trust and 5G – Realizing zero trust in networks".[13]

Figure 7. Zero-Trust Architecture Logical Elements (as defined in NIST SP 800-207)

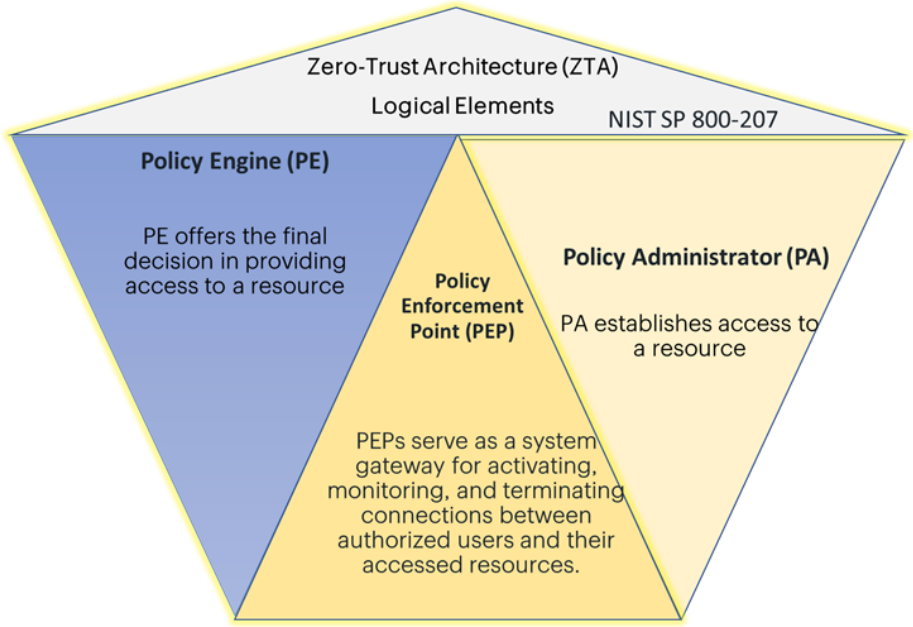


Figure 8. Overlay of NIST ZTA with 3GPP 5G Architecture

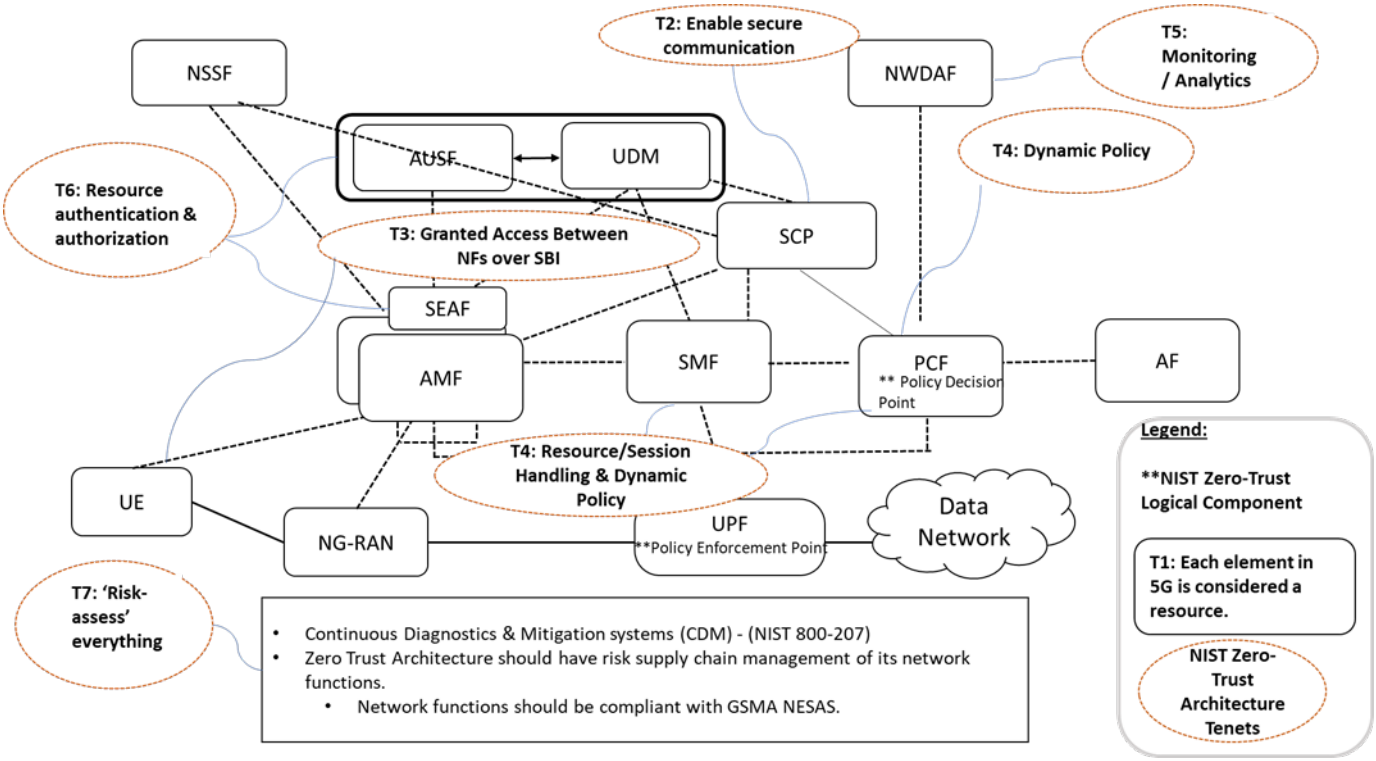


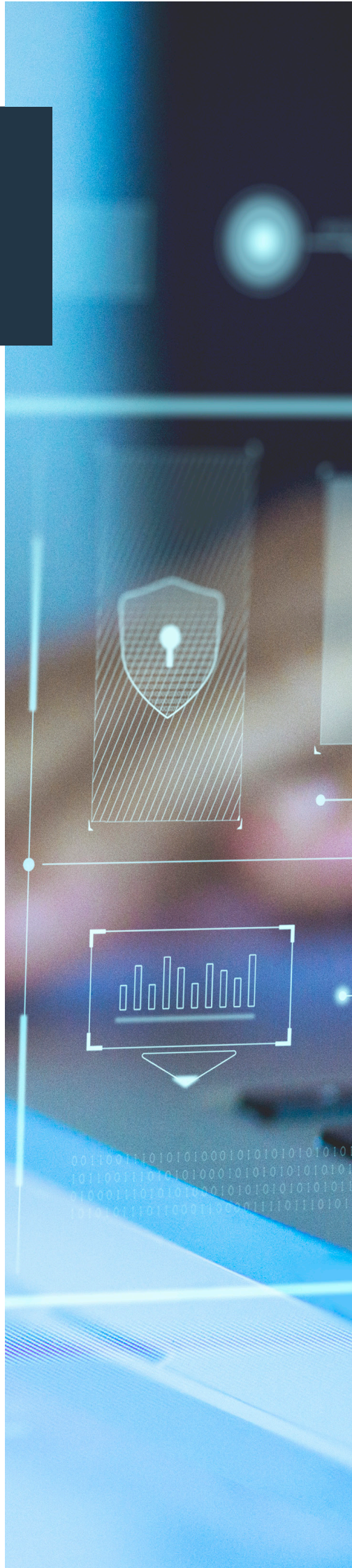
Table 1: Application of NIST Zero-Trust Architecture Tenets to 5G[56]

NIST Zero-Trust Tenets	Description	How ZTA can be applied to 5G
T1. All data sources and computing services are considered resources.	All 5G network assets and functions, including devices, computing resources, and services, are considered untrusted.	The end-to-end 5G network, including UEs, RAN, Transport, Core, Applications, and Services are assets and data sources. In the 5G SBA, NFs are identified as consumers and producers. UEs are identified using: • International Mobile Equipment Identifier (IMEI) • International Mobile Subscriber Identity (IMSI) or Subscription Permanent Identifier (SUPI)
T2. All communication is secured regardless of network location.	All communications must meet the same security requirements as third parties.	Service Communication Proxy (SCP) helps operators to efficiently secure and manage their 5G network by providing routing control, resiliency, and observability to the core network. Secure communication in 5G includes: • TLS to provide confidentiality and integrity protection across the SBI. • IPsec and DTLS to protect control messaging and user data in transport. • Subscriber identity privacy is provided with the Subscription Concealed Identifier (SUCI). • Full-rate User Plane Integrity protection • Stronger False Base Station (FBS) protection
T3. Access to individual resources is granted on a per-session basis.		UE access is granted using Shared Symmetric Key - Authentication and Key Agreement using 5G-AKA or EAP-AKA', or Public Key Certificate using EAP-TLS. Authentication and authorization between NFs over SBI in the 5GC is provided with certificate-based mutual authentication using TLS. Home Control of authentication is provided for roaming devices. RAN Slicing supports slice-specific mutual authentication for devices using the NSSAA.
T4. Access to resources is determined by dynamic policy	Trigger decisions on granting access based on various factors such as credentials, software version/patches, location, etc	The PCF feeds the AMF with access and mobility policies that affect UE authorization to access 5G network resources. Unified 5G policy allows for creating security policies for security use cases and user plane security enforcement within the session management and established security policies.
T5. The operator monitors and measures the integrity and security posture of all owned and associated assets.	The security state of all resources is monitored continuously in real-time.	5G is redefining Security Monitoring from physical probes and cables to software and virtual links. New software-based solutions include monitoring of East/West and North/South directions. Deliver analytics functions in the network for automation, maintaining security analytics and reporting. NWDAF defined in 3GPP TS 29.520 incorporates standard interfaces from the service-based architecture to collect data and evaluate systems in terms of compliance with security policy rules.

Table 1: Application of NIST Zero-Trust Architecture Tenets to 5G[56] (continued)

NIST Zero-Trust Tenets	Description	How ZTA can be applied to 5G
T6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.	Least Privilege: Any access, if granted, should be authorized with the least privileges. The access is only granted for a specific resource (depending on the sensitivity of the resource) and is not valid for a different resource.	The SBA uses OAuth 2.0 token-based authorization for any NF that wants to communicate with another NF. Mutual authentication enables the device to authenticate the network using the AUTH (Authentication Token) returned by the network and the Shared Key using Security Anchor Function (SEAF) and AUthentication Security Function (AUSF).
T7. The operator collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.	The security posture of devices, and behavioral patterns of resources are crucial to capture security baseline and maintain it. Trust evaluation and risk assessment is conducted for everything in 5G.	For the MNO, application of this tenet can be considered from two perspectives: 1. The MNO should leverage solutions that align with the continuous diagnostic and mitigation (CDM) systems as defined by NIST in Special Publication 800-207. 2. The MNO should have a mature supply chain risk management (SCRM) which should require the 5G network functions to be compliant with GSMA NESAS. NESAS includes security assessments of vendor development and product lifecycle processes and Security Assurance Specifications. In 5G, the assessment is carried out at the beginning to ensure products/solutions are evaluated against known risks. However, this will need to be automated once the products/solutions are also implemented in the network. The following could serve good reference to ‘risk-assess’ elements in 5G: • 3GPP Security Assurance Specification (SCAS) • GSMA - Network Equipment Security Assurance Scheme (NESAS)

5. 3GPP R16 Security Enhancements



5.1 Overview

Release 16 builds on the initial 5G security capabilities developed in release 15[14] covering the following areas:

- *Security additions and enhancements for new 5G functionality added in Release 16*
- *Added security capabilities for Release 16*
- *Minor security enhancements and corrections*

The following lists the major functional features or capabilities added or enhanced in Release 16 that also offered 5G security enhancements:

- *Enhanced support of vertical and LAN services*
- *Advanced vehicle-to-everything services (V2X)*
- *Enhancements for Common API Framework (CAPIF)*
- *Enhancement of network slicing*
- *Non-Public Networks (NPN)*
- *URLLC enhancements*
- *Full rate user plane integrity protection (UPIP)*

For a high-level description of the 5G Release 16 functionalities covered by the security enhancements and additions, refer to 3GPP TR 21.916.[15] Two of the more significant security focused architecture enhancements, Inter-PLMN UP Security (IPUPS) and Cellular IoT (CIOT), are described in more detail below.

5.2 Inter-PLMN User Plane Security (IPUPS)

Inter-PLMN User Plane Security was introduced in 3GPP Release 16 to provide enhanced protection of the user plane data in a roaming scenario. As the N9 interface between PLMNs can carry privacy sensitive material, such as user and subscription data, this interface was defined to be confidentiality, integrity, and replay protected. The IPUPS functionality is specified in 3GPP TS 23.501, clause 5.8.2.14[16] and 3GPP TS 33.501.[17]

IPUPS is a functionality of the UPF that enforces GTP-U security on the N9 interface between UPFs of the visited and home PLMNs. Operators can deploy UPFs supporting the IPUPS functionality at the border of their network to protect their network from invalid inter PLMN N9 traffic in home routed roaming scenarios. The UPFs supporting the IPUPS functionality in VPLMN and HPLMN are controlled by the V-SMF and the H-SMF of that PDU Session respectively. The UPF with IPUPS functionality, either as a dedicated UPF or combined with other UP functionality, is controlled by the SMF via the N4 interface

5.3 Cellular IOT (CIOT)

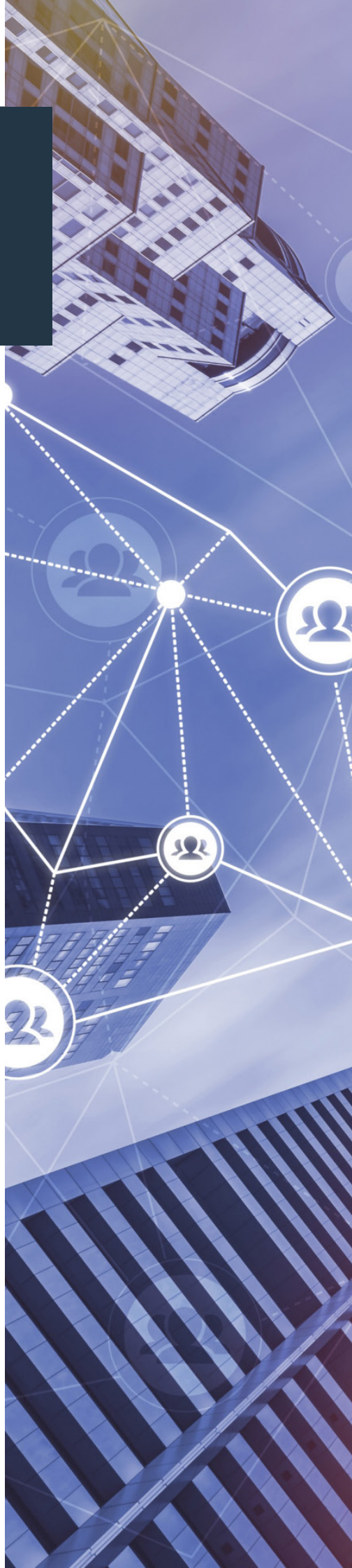
In 3GPP Release 13, CIoT was introduced to provide wireless connectivity to low-cost IoT devices with a longer battery lifetime and expanded coverage. These IoT devices typically have constraints on power consumption and device complexity, thus, they may only transfer small amounts of data infrequently. To support

such use cases, 3GPP developed two optimization features for small data transmission: Control Plane CIoT optimization and User Plane CIoT optimization.

In Release 16, the 5G System also supports the same CIoT optimization features as in LTE for small data transmission. In Control Plane CIoT optimization, the small user data is carried in Non-Access Stratum (NAS) messages – control-plane signaling messages exchanged between UE and AMF, where the user data is protected using the 5G NAS security context. This Control Plane optimization allows CIoT UEs to transfer data without establishing an Access Stratum (AS) security with the RAN node, thereby not only simplifying the data transfer procedure but reducing implantation complexity of CIoT UEs.

Meanwhile, in User Plane CIoT optimization, the small user data volume is transferred over the User Plane and protected using the AS security context established between the UE and the RAN node during the prior Radio Resource Control (RRC) connection. For the User Plane CIoT optimization, the RRC Suspend and Resume procedure was introduced to maintain the UE's AS security context (or UE's AS context in general) even when the current RRC connection is released. With such optimization, the CIoT UE does not need to perform a connection establishment procedure that would require substantial power consumption to those power-hungry CIoT devices.

6. GSMA 5G Security Recommendations



GSMA represents the interests of mobile operators worldwide, uniting them with the broader mobile ecosystem, as well as organizations in adjacent industry sectors. One of the GSMA key goals is to bring technologies to a position where they can interwork across many organizations, adding value to the overall standards environment. GSMA meets this key goal by developing standard profiles, implementation, and operational guidelines using 3GPP developed standards as the baseline. Within the GSMA, the Fraud and Security Working Group define fraud and security requirements, baseline security controls for the industry, and drive operator implementation and compliance with those recommendations.

With interconnect and roaming, the mobile network is exposed to other networks. This exposure drives the need for secure methods that allow partners to interconnect in a controlled way to be deployed, without revealing confidential information or facilitating fraud/abuse. In addition, there is an increasing demand for security by the public and by regulators. With the 5G standards, 3GPP addresses these many of these demands by introducing new security controls and defining new secure inter-operator communications. GSMA has taken these security controls and developed implementation and operational guidance for deployment for the mobile operators and value added IPX providers.

6.1 Inter-PLMN Security Enhancements

As described earlier in this paper, 3GPP has defined 5G standards with robust security controls beyond earlier generations of wireless technology. Those 5G security standards, enhanced in Rel. 16, improve the protection of 3GPP compliant networks, devices, and data to risks and threats. The security organizations in the government agencies and private enterprises welcome the expanded security enhancements to Inter-PLMN communications as many of their staff, employees and contractors travel internationally.

GSMA is defining the Inter-PLMN security deployment models to be used for roaming uses cases in 5G SA based on 3GPP Release 16 standards. The goal of the work is to define a scalable, usable, and secure 5G solution that meets both the business and technical needs of the industry. For Inter-PLMN signaling security across the N32 interface, 3GPP standards include the Security Edge Protection Proxy (SEPP) with the security model using either:[18]

- *Direct TLS for end-to-end communication or*
- *PRINS (Protocol for N32 Interconnect Security) to secure the roaming interconnection when intermediaries are needed*

As TLS and PRINS are not compatible deployment models for use between roaming partners one or the other model must be selected for use prior to establishing 5G SA roaming. This can add significant complexity to the negotiation and operational setup of global roaming relationships. To streamline that complexity and facilitate deployment, a GSMA inter-disciplinary team is actively working on defining the appropriate model to be use per use case. That work is slated to be completed in the second half of 2021 and will be documented in GSMA PRD NG.113 5GS Roaming Guidelines.[19]

A key management solution is required for 5G SEPP security. 3GPP TS 33.501[20] defines 5G inter-PLMN roaming security cryptographic keys to establish peer authentication, message integrity and confidential communication. The cryptographic keys need to be managed and exchanged between stakeholders involved in roaming. GSMA is defining the key management solution to be used across all roaming interfaces globally. The first phase is defined using manual processes to support initial 5G SA roaming implementations. For additional detail, please reference GSMA PRD FS.34.[21] Work is ongoing to operationalize the phase I key management and complete phase II which will include enhance scalability and automation.

In securing the control plane communications across the N32 interface, operators are required to secure user plane traffic across the N9 interface by establishing an IPSec secure tunnel. The IPSec tunnel will allow the operators to secure and filter the exchange of GTP-U messages over the N9 reference point with their roaming partners. 3GPP Release 16 introduces the new Inter-PLMN User Plane Security (IPUPS) functionality that can reside within the User Plane Function that will act as a GTP firewall for incoming GTP messages.

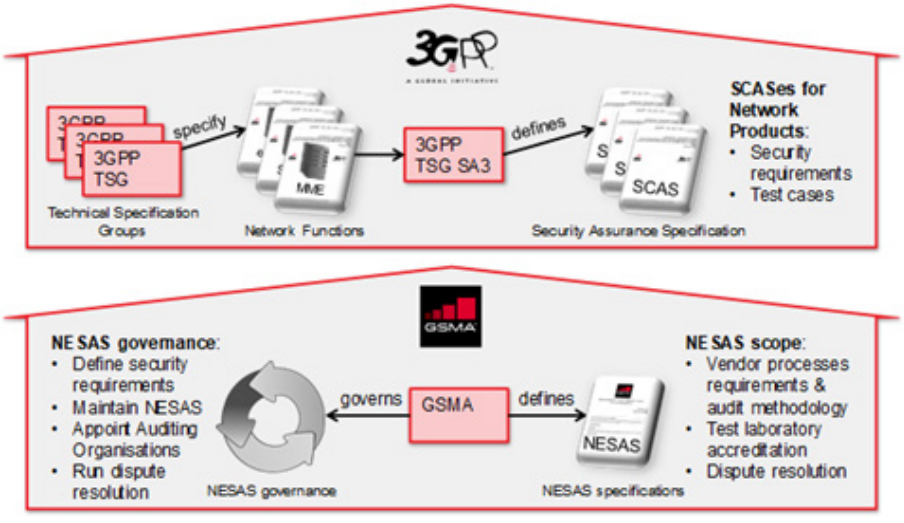
6.2 Network Equipment Security Assurance Scheme (NESAS)

GSMA, in partnership with 3GPP, defined NESAS to address the global concerns relating to 5G security and/or the perceived new security threats that 5G will introduce. NESAS provides an industry-wide security assurance framework to facilitate improvements in security levels across the mobile industry. NESAS defines a series of security requirements, a security assessment framework for secure Product Development Lifecycle (PDLC) processes by an independent auditor, and lab security testing based upon 3GPP defined specific network function security assurance specifications (e.g., security test cases) by an independent test lab facility. Figure 9 shows the roles of 3GPP and GSMA in NESAS.

NESAS is a critical industry led "shift-left" activity to guide 5G vendors to adopt industry accepted security best practices (e.g., DevSecOps, Supply Chain, etc.) in all phases of product development and delivery into the supply chain. NESAS is a volunteer audit and test exercise for the 5G vendor. An MNO should encourage their 5G vendors to submit their network equipment, or VNFs/CNFs, into the NESAS program.

That said, NESAS is an important activity to be embraced, but this should not be the only security validation exercise to be undertaken. It is critical that all parties use an appropriate set of security policies covering the whole lifecycle of a network. These policies can also include the application of other published GSMA security recommendations and participation in the GSMA's operational security services. One of the goals for developing NESAS is that the scheme helps vendors and operators avoid fragmented regulatory security requirements. NESAS should be used globally as the common baseline, with operator and/or national security measures or requirements added as enhancements.

Figure 9. Roles of 3GPP and GSMA in NESAS[57]



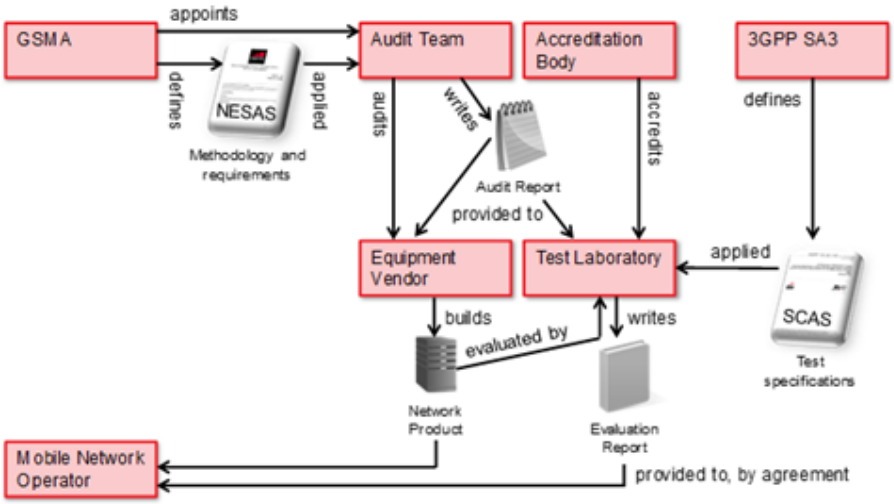
NESAS requires that an independent security accredited 3rd party perform a software development lifecycle (SDLC) security audit and security tests on the vendor platforms for GSMA and 3GPP compliance. When a vendor submits a product into the NESAS program, GSMA will assign the independent 3rd party auditor and security lab testing facility to the vendor for both stages of the program. The products that obtain full compliance by the independent 3rd party auditor will proceed to the testing phase, which the audit reports will be supplied to the independent test laboratory before testing begins. Figure 10 provides a high-level overview of NESAS.

6.3 GSMA's Coordinated Vulnerability Disclosure (CVD)

The GSMA CVD program provides researchers or practitioners a confidential method to disclose a vulnerability that impacts the mobile ecosystem. The goal of the CVD program is to allow the vulnerability to be assessed and for the impact to be mitigated before it enters the public domain. This program augments the U.S. NIST National Vulnerability Database (NVD)[22] and US-CERT[23] programs by adding a 5G focus. All are important tools for secure lifecycle management of 5G products and networks.

The GSMA CVD team is made up of individuals from member companies, along with GSMA staff. The CVD team works with mobile operators, suppliers, and standards bodies to develop fixes and mitigating actions to

Figure 10. NESAS High Level Overview[58]



protect customers' security and trust in the mobile communications industry.

The scope of GSMA's CVD Programme[24] is security vulnerabilities that impact the mobile industry, primarily open standards-based technologies. Operator or vendor specific vulnerabilities are not included in the scope of the CVD program and are best dealt with directly.

GSMA manages the CVD program and maintains an archive list of all disclosed CVD submissions. There are several recent examples of 5G Security vulnerability disclosures under the GSM CVD program, including a general submission on 5G SA Core security vulnerabilities (GSMA CVD-2021-0044x) and 5G Network Slicing vulnerabilities (GSMA CVD-2021-0047). Typically, these CVD's will lead to specific change requests to 3GPP standards and/or GSMA permanent reference documents (PRD).

7. Security for 5G Vertical Segments

5G expands the 3GPP technologies usefulness and benefits to a larger number of vertical segments beyond those support in previous 3GPP technologies. 5G security is also developed in alignment with the functional enhancements developed for each vertical segment. Each vertical segment is at risk of internal and external threat actors exploiting vulnerabilities for attacks on confidential, integrity, and availability. 5G security controls such as certificate-based mutual authentication, UPIP, Private Networks, and Network Slicing, as specified by 3GPP, can be implemented to protect 5G networks implemented by a variety of verticals. This section highlights the security risks and controls in 5G for several vertical segments. In addition, industry best practices for supply chain security, as described in the following section, should also be followed.

7.1 V2X

Vehicle to Everything (V2X) communications is a key component of the Intelligent Transportation System (ITS). On-Board Units (OBU) are installed in vehicles enabling them to communicate with other vehicles (V2V), infrastructure (V2I), pedestrians (V2P), networks (V2N), sensors (V2S), charging grid (V2G) and applications running on the edge and cloud.

5G allows convergence of 3GPP and non-3GPP networks to 5G packet core (5GC), thereby allowing co-existence of multiple technologies enabling V2X use cases. 5G enablers such as Multi-Access Edge Computing (MEC), Network Function Virtualization (NFV), Network Slicing, API enabled Service Based Architectures (SBA) and open software stack-based Cloud Native Functions (CNF) will help realize V2X use cases.[25]

5G-V2X use cases, classified as URLLC services, include safety and non-safety related use cases. Many of the use cases, specifically safety related, require low latency and high reliability, but are susceptible to risk of attacks. While safety related use cases are primarily URLLC, non-safety use cases are eMBB and MIoT oriented and provide value added services to consumers such as in-vehicle media, streaming, and identification related information. While 3GPP caters for securing V2X over NR based PC5 reference point, there are general security and privacy principles applicable outside of 3GPP scope which need to be secured by multi-layered security controls.

Early application of V2X is expected to be for traffic related use cases such as early notification/warnings foranti-collision and traffic alerts). A successful attack would therefore devalue such information and impact acceptance and consumer confidence in these systems.

Threat vectors include bogus messages, message modifications, Sybil attack, DoS, Eavesdropping, Impersonate attack, Replay attack, Black-hole attack, Grey-hole attack and location tracking. These impact the confidentiality, integrity, and availability of data. As discussed in the 5G Americas white paper “Vehicular Connectivity: C-V2X & 5G White Paper”,[26] proper certificate management framework is required to avoid privacy violation. An anomalous behavior detection and reporting system can provide a first level of defense to protect the system from attacks.

7.2 Smart Manufacturing

5G is positioning itself in factory automation and with cyber-physical systems for smart manufacturing. This is the area of industrial control systems, Industrial Internet of Things (IIoT), Supervisory Control And Data Acquisition (SCADA) systems, Operational Technology (OT) versus Information Technology (IT), all of which are all being grouped into the general term "Industry 4.0."

Two differences are key to the existing concepts of smart manufacturing and a future one envisioned with 5G:

- *Current systems are generally air-gapped from the Internet; and*
- *Current manufacturing devices rely heavily on wired systems, but are also connected using Wi-Fi and other wireless technologies. Of the wired connectivity, X.25 is in use as well as specialized industrial ethernet protocols.*

Manufacturing systems that are not connected to the Internet, known as air-gapped, have the advantage that they are not vulnerable to remote probing and scans and DDoS attacks from the Internet. However, a lack of remote connectivity also means the operators personnel of the manufacturing network must be physically present to operate it.

Smart manufacturing, and the "lights-out factory" concept of Industry 4.0, need varying degrees of connectivity outside of the factory to operate properly. Additionally, industrial control systems (ICS) typically run non-traditional operating systems with specialized applications. These systems are typically less vulnerable for attackers to exploit, but can be vulnerable to newly developed exploits that become zero-day attacks. More worrisome, though, is that air-gapped systems can suffer from a lack of patching or updates and are still vulnerable to the introduction of malware via an insider connecting an infected device, such as a USB memory stick, to a system on the network.

5G's characteristics of high bandwidth (eMBB) and low latency (URLLC) make it an ideal technology for connecting industrial devices in a factory without the constraint of wires. Like many 5G use-cases, smart manufacturing must ensure that:

- *Only authorized devices can connect to the 5G network;*
- *Only authorized devices can communicate and control the industrial devices; and*
- *The industrial equipment does not interfere with the radio frequencies of the 5G network.*

One ideal technique to accomplish this level of security in smart manufacturing is the 5G Private Network. This allows a tighter control over the access and range of the 5G network itself, however, the network remains exposed to spoofing from illegitimate devices and frequency jamming. A downside to a 5G Private Network is the skills gap of an enterprise, which may not have in-house cybersecurity skills. Therefore, a Network-as-a-Service (NaaS) offering from an MNO might be an ideal solution for enterprises.

Special care must be taken when allowing Internet connectivity to a private 5G network. In smart manufacturing applications, Internet access could easily allow an attacker to gain access to the control systems and disrupt any aspect of the manufacturing process. Therefore, any external connectivity should be strictly controlled by an architecture that ensures proper security and zero-trust.

7.3 Critical Infrastructure

According to U.S. Government's Cybersecurity and Infrastructure Security Agency (CISA), critical infrastructure can be defined as those sectors whose assets, systems, and networks, whether physical or virtual, are considered so critical to the U.S. that any disruption or destruction of this infrastructure would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.[27] Regardless of the country of origin, the definition of critical infrastructure is presumed to be synonymous. For example, the energy generation, storage, and distribution infrastructure are commonly defined as critical infrastructure as well as fresh water sources, purification, storage, and distribution infrastructure. Emergency services, financial Industry, and healthcare are just a few other examples of critical infrastructure sectors.

Historically, critical infrastructure has been deployed with limited monitoring, measurement, and asset tracking capabilities. This was primarily due to the lack of technology, intelligence and digital data transport. During the last fifteen years the electric utility industry has experienced a very large increase in the number of residential electric smart meters using cellular connectivity for very small data transmissions.

LTE ushered in this new wealth of digital data transport capabilities that has been integrated into an ever-growing Internet of Things (IoT) market that enables new technologies and intelligence for monitoring, measurement, and asset tracking in the electrical, water and other critical infrastructure sectors. Originally, LTE was not designed to support IoT, as that industry really came into being after LTE was deployed globally. More typically, the industry deployed IoT at scale in LTE using Narrowband IoT and Cat-M, which limited the data throughputs for an IoT device.

IoT was purposely built into 5G to support massive machine type communications (mMTC), also known as massive IoT. The 5G objective is to provide broadband transport to these commercial and/or industrial IoT devices. The result is that the 5G specifications are defined in a way that the critical infrastructure sectors can now implement new technologies, gain intelligence, and have access to an ultra-reliable low latency communication (URLLC) transport.

5G plays a critical role that enables many connections which are used in various settings within the critical infrastructure sectors. However, this critical role is threatened by the potential attack vectors to Policy and Standards, Supply Chain, and 5G

Systems Architecture, as described below.

The Evolution of Policy and Standard. All critical infrastructure sectors should be proactive in ensuring a healthy and unbiased development of 5G policies and standards for securing 5G's future communications infrastructure of the sectors.

The Supply Chain Threat. The universal battle over 5G dominance and the resulting rush to establish essential 5G network infrastructure that supports various critical infrastructure deployments has created a fertile ground for attackers to perform malicious activities. All the critical infrastructure sectors along with the 5G critical infrastructure that support them could be susceptible to malicious software and hardware, and unauthorized manufacturing processes. One malicious act could heavily impact any critical infrastructure that is powered by the 5G network. For example, water meter SCADA systems could be compromised, impacting the service quality and disrupting remote monitoring. Another example is a 5G enabled water quality monitoring system that could be compromised to obscure an anomalous total dissolved solids (TDS) and pH values and fail to alert of a possible water contamination event.

The 5G Systems Architecture Aspect. The evolution to supporting billions of devices will create non-traditional devices that need to have access to the 5G Core Network. 5G systems architecture is evolving to include the security of 3GPP and non-3GPP devices.

As 5G becomes widely adopted, it will quickly play an important role in the operation of critical infrastructure. 5G security for the Energy and Water and Healthcare sectors are examined further below.

7.3.1 Energy and Water

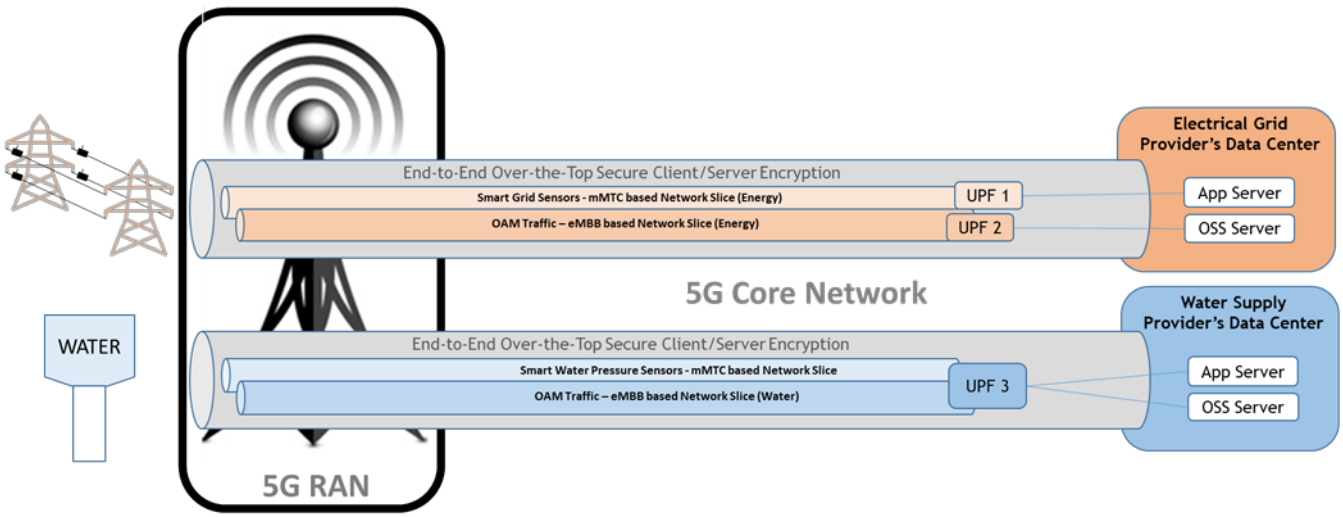
Foundationally, critical infrastructure must be designed and implemented so that it is reliable and non-disruptive. As the Energy and Water providers expand their monitoring, measurement and asset tracking capabilities using 5G based wireless communications, security must be paramount into all the data communication flows, IoT device APIs, IoT device security hygiene, and end-to-end security monitoring. Utilizing low band RF frequencies with 5G provides exceptional coverage across metro and rural areas due to its propagation and penetration characteristics which provide a reliable data communication path between the IoT device and the Energy/Water sector provider's application, security monitoring, and telemetry servers as shown in Figure 10.

By design, 5G uses built-in strong confidentiality and integrity ciphering algorithms on the air interface (e.g., between the IoT and the 5G radio). The User Plane Integrity Protection (UPIP) specifications in 3GPP Release 16 were updated to mandate the equipment manufacturers enable full rate UPIP support in the devices and radios which the mobile network operators can decide to use or not. There will be some low-end devices that do not have the compute resources to support full rate UPIP but that may be acceptable for some use cases.

For the Energy and Water sectors, 5G UPIP along with Network Slicing could be used in conjunction to provide reliability and secure connectivity by layering in strong wireless replay protection and end-to-end segmentation. Using network slices, MNOs could dedicate a network segment for each critical infrastructure provider to ensure that its services and network traffic are isolated from each other, as shown in Figure 11. By leveraging network slicing, this reduces the threat landscape of one mission critical provider negatively impacting another. For instance, a security event, such as denial of service on one network slice impacting a critical infrastructure provider, should not leak into a different network slice used by another critical infrastructure provider.

Beyond 5G UPIP and Network Slicing, the critical infrastructure providers

Figure 11. Network Slicing and Secure Tunnel



and the MNO must secure all interface points, monitor all third-party interconnections, and enable active security monitoring to detect security anomalies in near real-time. From the MNO perspective, the security health of all active links servicing critical infrastructure providers should be continuously monitored at the transport level. From the critical infrastructure provider's perspective, IoT devices and services, including application, APIs, and telemetry, must be deployed with security hygiene, strong baseline security controls, defense-in-depth strategy, and active metrics/log monitoring that are functioning properly.

The Energy and Water critical infrastructure providers should ensure that the IoT devices, applications and server infrastructure are manufactured and developed based upon industry accepted security standards around hardware and software development lifecycles and methodologies, including DevSecOps, transparent software bill of materials including any free and open-source software (FOSS) and 3rd party sourced software, completed vulnerability scans, and completed penetration testing.

MNOs will provide a secure 5G transport medium including the potential of using UPIP and Network Slicing, but the Critical Infrastructure providers are solely responsible for the broader end-to-end security of the complete technology ecosystem. 5G provides a breadth of security for the transport including high reliability and many areas of ubiquitous coverage. Optimistically, the 5G Mobile Network Operators and the Critical Infrastructure Providers can partner to protect the national interest from threats known and unknown.

In 2021, there have been a spike in ransomware attacks including the publicly disclosed Colonial Pipeline[28] and Kaseya attacks.[29] A collaborative approach to develop a defense-in-depth strategy to protect the 5G enabled IoT devices and services is paramount which includes both a secure 5G transport offered by Mobile Network Operators and end-to-end protection of the technology services offered by the critical infrastructure providers.

7.3.2 Healthcare

As healthcare providers continue to find ways to improve patient healthcare, outcomes and experience, the providers may be struggling to adopt and deploy new wireless medical devices, platforms and tools to elevate these metrics. Hospitals today feature a plethora of wireless medical devices, platforms and tools that leverage unlicensed frequency bands. The primary unlicensed bands for in-building wireless cover are the 2.4GHz to 2.5GHz and 5GHz to 6GHz frequency bands (e.g., 802.11 Wi-Fi) and 802.15 Bluetooth/WPAN).

The challenges with the application of unlicensed wireless frequencies include significant RF congestion, the broad availability of low-cost compatible compute devices that can be used for malicious activities, and significant electromagnetic interference from some imaging platforms in these bands. The providers have worked to limit the RF congestion by increasing the number of radios then reducing the transmit power levels to reduce co-channel interference. The providers have worked to shield the imaging rooms to prevent the electromagnetic energy from disrupting the in-building Wi-Fi network. Neither of these reduce the threat surface that the unlicensed bands introduce to their critical infrastructure. For less than $100 US, a bad actor can purchase a device with built in Wi-Fi that can then be used to execute passive and active attacks on the hospital's critical infrastructure.

As mentioned earlier, 5G was designed to support mMTC communications for which there is a developing ecosystem of 5G smart devices, platforms, and tools. Healthcare providers can explore leveraging in-building 5G licensed wireless coverage, instead of Wi-Fi and Bluetooth. Within the 5G framework, the mobile network operators could partner with the hospital provider to deploy a 5G standalone public network, standalone non-public network (SNPN), public network integrated non-public network (PNI-NPN), private access point names (PAPN), multi-operator core network (MOCN), or a multi-operator radio access network (MORAN).

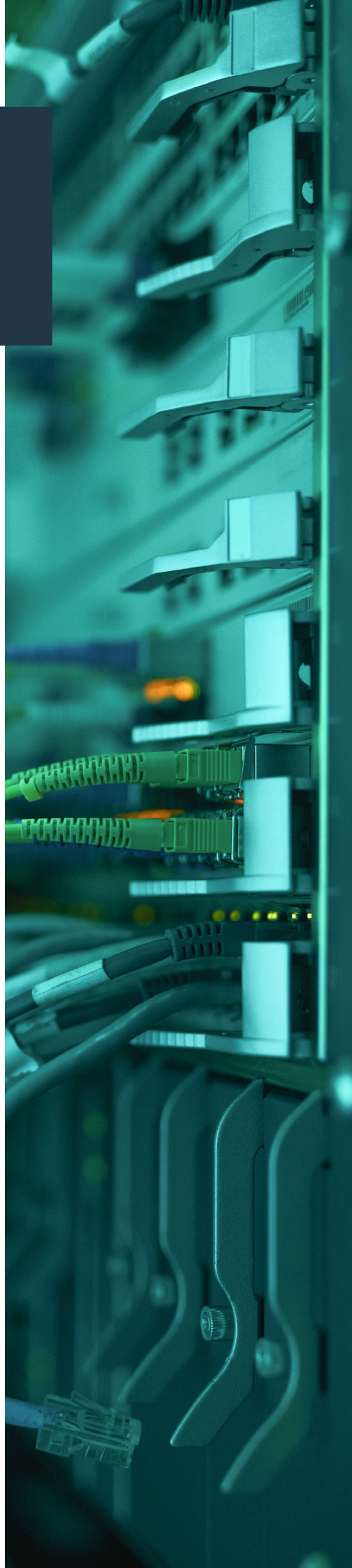
These licensed wireless solutions mitigate the availability of low-cost compute devices for a bad actor to use. There are software defined radios (SDRs) that support a wide range of RF frequency bands, but they are typically only available online and then require advanced technical skills to operate. More importantly, 5G uses industry defined security ciphering algorithms and secure communication flows that have been defined by the industry's top security engineers. A bad actor armed with a SDR is lower risk with a 5G in-building infrastructure than a bad actor equipped with a Wi-Fi enabled Windows laptop and Wireshark who can immediately start passively attacking the unlicensed network. These licensed bands would assist in mitigating the congestion in the Wi-Fi and Bluetooth bands.

As another layer of security, 5G network slicing can be leveraged to provide traffic segregation between various business, healthcare and 3rd party use cases. For instance, if the Radiology department is outsourced to a 3rd party, network slicing provides a means to separate their traffic from the rest of the hospital's traffic by creating separate end-to-end traffic isolation (e.g., UE to the Cloud).

As 5G is natively designed for network slicing, it should be difficult for bad actors to access the broader system. Network slicing also enables for better privacy which can benefit the protection of Personal Health Information (PHI), because PHI is not shared across segregated slices. Furthermore, with 5G, health organizations security operations centers can collect and analyze a huge amount of slice-specific information collected from the increasing numbers of medical devices used by medical personnel. This facilitates data insights that enable the identification of suspicious activities for detection and response early in the attack phase.

5G is a powerful tool to overcome the security challenges associated with Wi-Fi. 5G's strong security capabilities protect the confidentiality and privacy of data and the availability of the network, enabling healthcare providers to more effectively communicate and interact with the patient, staff and assets. The 5G experience can also extend beyond the hospital's facilities to provide a means to securely communicate with patients and their 5G enabled medical devices, such as heart monitor and glucose reader.

8. Supply Chain Security



Supply chain security is an integral part of 5G security. This section discusses important topics for a secure software supply chain: trusted suppliers, secure use of open-source software, secure software development, DevSecOps, and software bill of materials.

8.1 Trusted Suppliers

The global pandemic and software supply chain attacks highlighted the need to have a secure and resilient supply chain built upon a foundation of trusted suppliers. The U.S. Department of Homeland Security's CISA formed the Information and Communications Technology Supply Chain Risk Management (ICT SCRM) Task Force to provide guidance and recommendations to the ICT industry. The task force determined that trustworthiness can be applied to ICT organizations, products, and services in which trusted suppliers meet the following criteria:[30]

- *Hardware integrity*
- *Secure Software Development Lifecycle (SDLC), including the software development environment, deployment, and updates*
- *Third-Party Component Management, including Software Bill of Materials (SBOM) and secure use of open-source software*
- *Resilient supply chain with trusted upstream suppliers. The CISA ICT SCRM Task Force produced a standardized template of questions[31] for trusted suppliers to communicate ICT supply chain risk posture in a consistent way.*

The topics of secure use of open source, secure SDLC, DevSecOps, and SBOM are discussed further in the sections below.

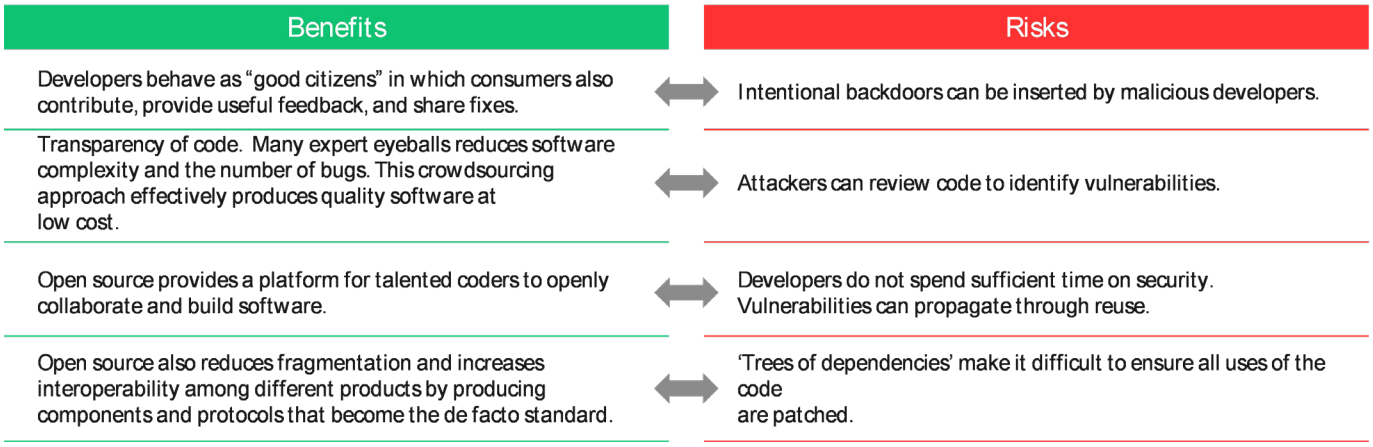
8.2 Open-source Software Security

Open-source software has many benefits for 5G software development projects but if deployed without following the best security practices, will lead to increased risks that require the vendor to implement a higher level of due diligence. Open source works optimally when developers behave as "good citizens", openly collaborate, and build software in a crowdsourcing-type approach to software development.

The transparency of code reduces software complexity, fragmentation, and bug count, while increasing interoperability. Open source also facilitates security testing by independent third parties. The benefits of open source also introduce risks, as shown in the Figure 12.

Tools and resources are available for secure use of open-source software in development projects. The tools include software composition analysis (SCA) that identifies all package dependencies (including versions, vulnerabilities, and licensing information) in a code base, static application security testing (SAST) which identifies vulnerabilities in the code base (excluding packages), and dynamic application security testing (DAST) which can be tuned and trained to detect run-time vulnerabilities.

Figure 12. Open source software security benefits and risks [source: Ericsson]



The SCA tool would be integrated into the integrated development environment. The SCA tool would alert the developer in real-time when the developer uses known vulnerable free and/or open source software including the vulnerabilities and any mitigations to the security threat(s). With safeguards in place, open source can be used effectively at low risk to realize its intended benefits. Products relying on open source must be developed using methodologies and safeguards that ensure the expected level of security is met. Open source can accelerate innovation, reduce the development timeline, speed time to market, realize cost savings, but inherent security cannot be assumed. 5G vendors must take responsibility and practice a higher level of due diligence when using OSS components.

In response to the recent cyberattacks and published CVDs, it is important for mobile network operators to request their vendors to provide a software bill of materials (SBOM), as discussed in a later section, that shows use of free and open-source software (FOSS) embedded in the shipped product. This facilitates identification of a potential vulnerability in the software product when a CVD is released for a particular open-source binary, library, or package.

8.3 Secure Software Development Lifecycle

The software development lifecycle (SDLC) is the methodology to build high-quality software in phases of the software lifecycle: requirements, planning, design, development, testing, and deployment. SDLC best practices have been established by organizations such as BSA/ The Software Alliance[32], Open Web Application Security Project (OWASP),[33] and SAFECode.[34] U.S. NIST, at the time of publication of this paper, is in the process of defining the Secure Software Development Framework (SSDF) that integrates security into the SDLC to achieve three primary goals:[35]

1. **reduce the number of vulnerabilities in released software**
2. **mitigate the potential impact of the exploitation of undetected or unaddressed vulnerabilities**
3. **address the root causes of vulnerabilities to prevent future recurrences**

The NIST SSDF is organized into four phases:

1. **Prepare the Organization**
2. **Protect the Software**
3. **Produce Well-Secure Software**
4. **Respond to Vulnerabilities.**

NIST will be further developing the SSDF in support of NIST's responsibilities under Executive Order 14028.

The DHS CISA ICT SCRM Task Force considers SDLC, due to its influence on the creation and delivery of the software product, as a category of supply chain integrity. Their report[36] provides four control areas for a secure SDLC:

1. **software development environment**
2. **third-party component management**
3. **software deployment**
4. **software updates**

Code signing, digital signatures, and software bill of materials (SBOM) provide various levels of attestation from the vendor and should be used to ensure software integrity. SBOM is discussed further in a later section.

8.4 DevSecOps

Mature DevSecOps programs are critical to ensuring that any hardware platforms and software packages are intentionally built with security in all phases of the product and/or software development lifecycle. A DevSecOps program must focus on security during the development phases as well as the deployment and operations lifecycle phases.

All hardware and software provided by the infrastructure and handset vendors includes 3rd party components, 3rd party software, open-sourced software and possibly even free pre-compiled software. This has been the evolution of technologies and infrastructure for over a decade – the move from bare metal running proprietary software to COTS hardware that leverages the open software industry to assist in the delivery of scalable products more quickly to the market. With that, the vendors must demonstrate that they are taking all the necessary steps to secure

the hardware and software before delivering them to the Mobile Network Operators.

5G cloud native architecture further increases the need for industries to adopt a new development framework with virtualization, automated deployment, instantiations, and upgrades, by leveraging open-source technology and software stacks. This affects not only new 5G services planned to be delivered by service providers, but also represents new ways for enterprise and industry verticals to utilize those services. Cloud native architectures splits the applications and 5G Network Functions (NFs) into individual microservices and focuses on decomposition to allow distributed deployments to accelerate value generation.

Accelerated application development and deployment for 5G networks requires DevOps to bring together software development and operations to shorten development cycles, allow organizations to increase agility, and maintain the pace of innovation while taking advantage of 5G cloud-native architecture. However, existing DevOps practices used to develop hardware and software platforms may be implemented without security considerations, shifting industry's interest to use DevSecOps practices.[37]

Processes such as DevSecOps, short for Development Security and Operations, bake in security at every step of software design, development, testing and quality. This enables the development of secure software with the speed of DevOps to meet the need for better security while still providing greater agility and scale.[38]

Instead of depending on various inspection algorithms to identify the security gaps within the code, DevSecOps aims to have secure software earlier in the development process. DevSecOps helps ensure that security is addressed as part of all DevOps practices by integrating security practices and automatically generating security and compliance artifacts throughout the process. DevSecOps for cloud-native applications, as currently being addressed by the NIST DevSecOps Project,[39] integrates security into the DevOps process, reducing vulnerabilities, mitigating potential impacts of vulnerabilities, and preventing recurrence of vulnerabilities

DevSecOps best practices adopted by 5G vendors and service providers help to ensure secure deployment of 5G cloud native network functions. For vendors, following the DevSecOps methodology reduces vulnerabilities, malicious code, and other security issues in hardware and software stacks being deployed in service providers 5G critical infrastructure, without slowing code production and releases. For MNOs, implementing DevSecOps methodologies helps address security issues such as vulnerabilities and malicious code before it is deployed in the production environment, improving security efficacy of the 5G network. For all deployment scenarios, since a substantial percentage of an application consists of 3rd party packages, DevSecOps teams must plan to upgrade to the latest version of these packages to reduce the number of inherited vulnerabilities in their applications. Packages that are no longer supported should be replaced efficiently.

DevOps and DevSecOps best practices are currently focused on development, integration and operational deployment or delivery within a single entity/enterprise. 5G networks require a significant system integration of multiple hardware/software systems, often from a large number of vendors to move to an operational state. The goal is to have multiple 5G vendors' Continuous Integration/Continuous Development (CI/CD) processes[40] to feed into multiple operators' automated System Integration/Operation processes in an automated and integrated fashion to reduce the time from development to operational status. Security aspects must be integrated from start to finish. However, there are several aspects which are not yet explored to any extent nor incorporated in best practices:

- *Streamlining and automating the system integration of multiple systems from multiple vendors typically performed by operators or 3rd party system integrators*
- *Integration of cross organization processes at scale (such as multiple vendors delivery of CI/CD artifacts to multiple operators).*

8.5 Software Bill of Materials (SBOM)

The software bill of materials (SBOM) is a fundamental component of a mature Software Development Lifecycle (SDLC) process. SBOMs are meta-data structures about the software and its components. They are used for multiple purposes including license management, IPR risk management and product inventory for vulnerability management. For instance, an SBOM can maintain a documented list of third-party software suppliers, including third-party commercial software and free and open-source software (FOSS), used in software projects.

SBOM is an industry best practice for secure software development to enhance the understanding of the upstream software supply chain so that vulnerability notifications and updates can be properly and safely handled across the installed customer base.

Recent cyberattacks in the U.S. prompted Executive Order 14028, "Improving the Nation's Cybersecurity",[41] with a directive to the U.S. Department of Commerce (DoC) to provide guidance for industry on SBOM. The DoC and the National Telecommunications and Information Administration (NTIA) define SBOM as "a formal record containing the details and supply chain relationships of various components used in building software." The DoC, in coordination with NTIA, published a report "The Minimum Elements for a Software Bill of Materials (SBOM)"[42] that provides guidance on the data fields, automation, and processes to be used by suppliers and customers. Some key points are provided below:

SBOM Data Fields

- *The SBOM must contain as minimum fields: Supplier Name, Component Name, Version of the Component, Other Unique Identifiers, Dependency Relationship, Author of the SBOM data, and Timestamp.*

SBOM Automation

- *The interoperable data formats used to generate and consume SBOMs must be either Software Package Data eXchange (SPDX),[43] CycloneDX,[44] or Software Identification (SWID)[45] tags.*

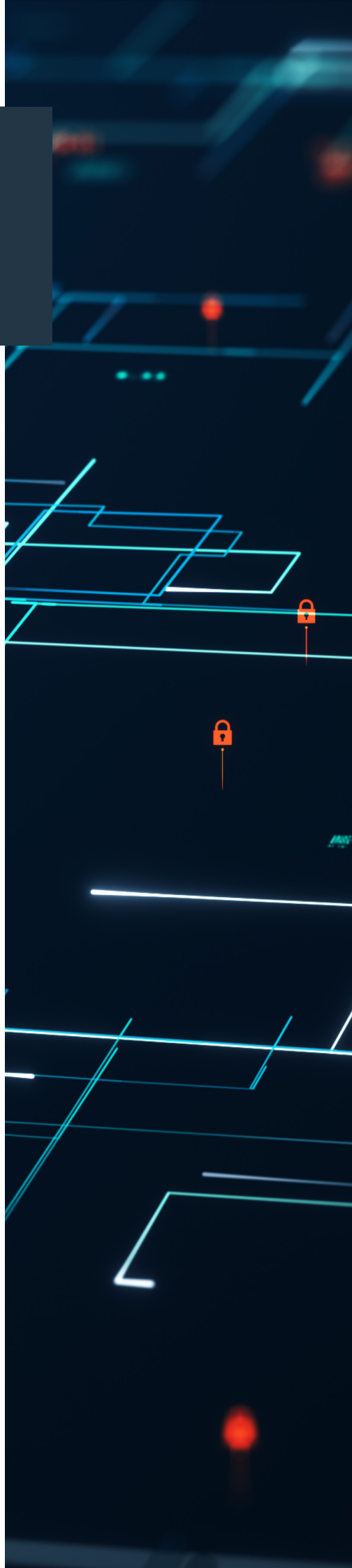
SBOM Processes

- *DoC advises that the cryptographic hash and digital signature of the SBOM may be defined in the contractual agreement between the software supplier and customer.*
- *DoC advises the terms for access control to the SBOM may be defined in the contractual agreement between the software supplier and customer.*
- *Depth is the level of upstream suppliers maintained in the SBOM. DoC advises an SBOM should contain all primary (top level) components, with all their transitive dependencies listed. At a minimum, all top-level dependencies must be listed with enough detail to seek out the transitive dependencies recursively.*
- *The commercial software supplier is not obligated to make the SBOM publicly available.*

Since there is no global naming/identity authority, a major challenge with SBOMs is proper identification of suppliers, upstream vendors, and FOSS software components used in the delivered software. This is especially true when the SBOM is generated by discovery where author of the SBOM and the supplier are not the same entity. One way to mitigate this is to require SBOMs from upstream suppliers, shifting responsibility upstream, to produce better SBOM accuracy. The upstream responsibility to produce the SBOM for FOSS needs to be resolved.

SBOM does not prevent cyber-attacks nor does SBOM protect against vulnerabilities. SBOM does provide a key piece in mapping known vulnerabilities to existing inventory for risk assessment and mitigation purposes and can provide transparency into the use of open source software with contributions from individuals or companies in adversarial nations.

9. Open RAN Security



The open RAN ecosystem is gaining momentum in the marketplace. Open RAN, with its virtualization, disaggregation, automation, and intelligence, is a complementary part of 5G's overall broader progression to greater security. Security is top-of-mind for many open RAN industry initiatives that recognize both the benefits and attack surface of an open, disaggregated RAN architecture. The combination of greater risk with reduced risk tolerance requires a zero-trust approach to securing open RAN. This section highlights the efforts of several open RAN security initiatives.

O-RAN Alliance

The O-RAN Alliance aims to make open RAN as secure by design as the 3GPP specified RAN. The Alliance sees inherent security benefits to the openness and disaggregated architecture while recognizing the expanded attack surface from additional RAN network functions and open interfaces.

The O-RAN Alliance Security Focus Group (SFG) is mitigating security risks to reduce likelihood and impact of attacks on third-party RAN applications, open fronthaul interface, network management, and UE identify privacy within the O-RAN.[46] The SFG performs continuous threat assessments across the open RAN architecture and applications, develops solutions to counter threats, and sets security requirements and protocol specifications for each O-RAN release to guide the development, deployment, and operation of an O-RAN.[47]

OpenRAN MoU Group - TIP

The Open RAN MoU Group of the Telecom Infra Project (TIP) supports "the advancement and adoption of standards-based Open RAN solutions".[48] The MoU Group signatories comprise Deutsche Telekom, Orange, Telefónica, TIM, and Vodafone.[49]

In June 2021 the MoU Group published technical priorities for the open RAN that includes security requirements.[50] Security requirements for the open Fronthaul span timing synchronization and network management. The MoU Group wants to prevent unauthorized physical access to a radio unit's DDR/ Flash memory modules and JTAG interfaces and to detect when a radio unit is moved from the intended installation location. The publication calls for IPsec for mid-haul data-in-transit confidentiality and integrity between CU and DU.

Network functions, such as the CU and DU, may operate as cloud-native functions (CNFs) workloads within a cloud infrastructure. The MoU group outlines unanimous support of several mandatory security requirements for the RAN cloud infrastructure to include container host operating system security, trusted code, and protection of data at rest and in transit.

The MoU Group sees a need for securing the O-RAN Alliance near-real-time RAN intelligent controller (near-RT RIC) and the applications running in the near-RT RIC. Priorities include protecting from malicious applications and maintaining confidentiality and integrity of RAN data.

Linux Foundation O-RAN Software Community

The O-RAN Software Community (OSC)[51] is a collaboration between the O-RAN Alliance and Linux Foundation with the mission to support the creation of software for the RAN. OSC uses O-RAN specifications while leveraging other LF network projects to address the challenges in performance, scale, and 3GPP alignment. Contributions to the OSC can be made by O-RAN Alliance members, regardless of country of origin.

The O-RAN Alliance is producing security guidelines for open-source developers to develop, contribute, and used open-source software in the OSC. These guidelines include Core Infrastructure Initiative (CII) badging for OSC projects to self-certify. CII badging[52] is an open-source secure development maturity model for vendor self-certification comprising criteria across change control, reporting, quality and security requirements. The current CII badge status of OSC open-source software development can be found in the OSC wiki.

A more secure open RAN through industry initiatives

Common approaches to securing the open RAN run through these industry initiatives. All initiatives address security concerns early through security-by-design. Software drives open RAN and allows for iterative process improvement, including security. Each initiative is evolving open RAN with learnings from early deployments. The openness of the RAN architecture enables the initiatives to find, analyze, and close new vulnerabilities through technical and security policy controls. These initiatives will continue to contribute to ensuring O-RAN achieves the level of security expected by operators and users of 5G networks. U.S. National Telecommunications and Information Agency (NTIA) recommends that the U.S. Government continue to support industry in the development of open RAN specifications to meet these goals.[53]

Conclusions

5G holds the promise of elevating society as business, public services, and citizens increasingly rely upon it for critical infrastructure, mission critical applications, public safety, smart manufacturing, connected car, and other real-time, low latency use cases. This results in greater impact from a cyberattack in 5G, decreasing our risk tolerance. The combination of greater risk with reduced risk tolerance requires a zero-trust approach. 3GPP has introduced an evolution of the trust model for standalone 5G deployments, for which trust within the network is considered to decrease as one moves further from the core. Trust in 5G can be enhanced using a zero-trust architecture (ZTA), which makes no implicit assumptions of trust based upon an asset's network location, geographic location, or ownership.

This white paper makes several recommendations for securing 5G networks. 5G operators will benefit from deploying zero-trust security controls to protect network assets and data and enhanced ability to detect attacks. 5G provides digital identities, mutual authentication between all functions, and strong cipher suites for confidentiality and integrity protection on the control and user planes. 5G is also the first cellular technology designed to be cloud-native. The cloudification of the 5G RAN and Core can leverage cloud security best practices to protect networks, applications, and data, but it also introduces new risks due to an expanded threat surface. Open RAN, with its virtualization, disaggregation, automation, and intelligence, can become a complementary part of 5G's broader progression to greater security as industry initiatives address open RAN's security risks.

Non-Public Networks / Private 5G deployments enable industry verticals to benefit from the advantages of 5G through deployment of customized use cases using third party developers, while opening the ecosystem for wider integration and operational efficiency. Although 5G brings in openness and allows closer integration with third party application developers, it also increases the threat surface. Supply chain risk management must ensure trusted suppliers use secure software development practices with transparency of upstream software components and secure use of open-source software.

Stakeholders, including hardware and software vendors, MNOs, HCPs, and SIs must establish a multiparty relationship in which security roles and responsibilities are clearly defined. 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 so secure cloud deployments can provide the foundation for use cases that deliver on 5G's promises to society and business.

Acronyms

3GPP: Third-Generation Partnership Project

5G: Fifth Generation

5GA: 5G Americas

5GC: Fifth Generation Core

5G NR: Fifth Generation New Radio

AKA: Authentication and Key Agreement

API: Application Programming Interface

CII: Core Infrastructure Initiative

CISA: Cybersecurity and Infrastructure Security Agency

CIoT: Cellular Internet of Things

CNF: Cloud Native Function

COTS: Commercial-off-the-shelf

CSRIC: Communications Security, Reliability and Interoperability Council

CVD: Coordinated Vulnerability Disclosure

DAST: Dynamic Application Security Testing

FBS: False Base Station

FCC: Federal Communications Commission

FOSS: Free and Open-Source Software

ICT: Information and Communications Technology

IoC: Indicators of Compromise

IoT: Internet of Things

IIoT: Industrial Internet of Things

IPUPS: Inter-PLMN User Plane Security

MEC: Multi-Access Edge Compute

MNO: Mobile Network Operator

MSP: Managed Service Provider

NESAS: Network Equipment Security Assurance Scheme

NF: Network Function

NIST: National Institute of Standards and Technology

NPN: Non-Public Network

NSSAA: Network Slicing Security Authentication and Authorization

NTIA: National Telecommunications and Information Agency

OSC: O-RAN Software Community

OSS: Operations Support System

OWASP: Open Web Application Security Project

OSS: Open Source Software

PLMN: Public Land Mobile Network

PAPN: Private Access Point Names

PCF: Policy Control Function

PDP: Policy Decision Point

PEP: Policy Enforcement Point

PHI: Personal Health Information

PNI: Public Network Integrated

PRINS: Protocol for N32 Interconnect Security

R15: Release 15

Acronyms

R16: Release 16

RF: Radio Frequency

SAST: Static Application Security Testing

SBA: Service Based Architecture

SBI: Service Based Interface

SBOM: Software Bill of Materials

SCA: Software Composition Analysis

SCRM: Supply Chain Risk Management

SDO: Standard Development Organization

SDLC: Software Development Lifecycle

SEPP: Security Edge Protection Proxy

SI: System Integrator

SNPN: Standalone Non-Public Network

SPDX: Software Package Data eXchange

SSDF: Secure Software Development Framework

SUCI: Subscriber Concealed Identifier

SUPI: Subscriber Permanent Identifier

TIP: Telecom Infra Project

TLS: Transport Layer Security

UE: User Equipment

UPF: User Plane Function

URLLC: Ultra Reliable Low Latency Communication

V2X: Vehicle to Everything

V2V: Vehicle to Vehicle

V2I: Vehicle to Infrastructure

V2P: Vehicle to Pedestrian

V2N: Vehicle to Network

V2S: Vehicle to Sensor

V2G: Vehicle to Grid

ZTA: Zero Trust Architecture

Endnotes

1 https://www.5gamericas.org/security-considerations-for-the-5g-era/

2 https://github.com/cncf/toc/blob/main/DEFINITION.md

3 Nair, Pramod, Securing 5G and Evolving Architectures (ISBN: 9780137457939)

4 Nair, Pramod, Securing 5G and Evolving Architectures (ISBN: 9780137457939)

5 3GPP TS 33.501, "Security architecture and procedures for 5G system", Release 16, v 16.5.0

6 3GPP TS 33.122, "LTE; 5G; Security aspects of Common API Framework (CAPIF) for 3GPP northbound APIs", 3GPP, version 16.3.0 Release 16, August 2020.

7 Nair, Pramod, Securing 5G and Evolving Architectures (ISBN: 9780137457939)

8 Nair, Pramod, Securing 5G and Evolving Architectures (ISBN: 9780137457939)

9 NIST SP 800-207, Zero-Trust Architecture, Rose, S., Borchert, O., Mitchell, S., Connelly, S., U.S. NIST, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final

10 NIST SP 800-207 Zero Trust Architecture

11 Zero trust and 5G – Realizing zero trust in networks, Olsson. J., et al, Ericsson Technology Review, Ericsson, May 12, 2021, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g.

12 Reference: Zero Trust Architecture, U.S. NIST, SP 800-207, https://csrc.nist.gov/publications/detail/sp/800-207/final

13 Zero trust and 5G – Realizing zero trust in networks, Olsson. J., et al, Ericsson Technology Review, Ericsson, May 12, 2021, https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/zero-trust-and-5g.

14 https://www.5gamericas.org/security-considerations-for-the-5g-era/

15 "Release description; Release 16", Sultan, Alan, 3GPP TR 21.916, version 16.0, June 2021.

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

17 https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

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

19 https://www.gsma.com/newsroom/resources/ng-113-5gs-roaming-guidelines-v4-0/

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

21 https://www.gsma.com/security/resources/fs-34-key-management-for-4g-and-5g-inter-plmn-security/

22 https://nvd.nist.gov/

23 https://us-cert.cisa.gov/

24 CVD Programme, GSMA, https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

25 https://www.5gamericas.org/vehicular-connectivity-c-v2x-and-5g/

26 https://www.5gamericas.org/vehicular-connectivity-c-v2x-and-5g/

27 Cybersecurity & Infrastructure Security Agency, "Critical Infrastructure Sectors". Available: https://www.cisa.gov/critical-infrastructure-sectors. [Accessed 7 July 2021].

28 A. Greenberg, "The Colonial Pipeline Hack is a New Extreme for Ransomware", Wired, 8 May 2021. [Online]. Available: https://www.wired.com/story/colonial-pipeline-ransomware-attack/. [Accessed 8 July 2021].

29 E. Moyer, "Ransomware attack on Kaseya, a software firm, threatens businesses worldwide", CNET, 4 July 2021. [Online]. Available: https://www.cnet.com/tech/services-and-software/ransomware-attack-on-kaseya-a-software-firm-threatens-businesses-worldwide/. [Accessed 8 July 2021].

30 Report on Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists: Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks, U.S. DHS CISA ICT SCRM Task Force, April 2021.

31 Vendor Supply Chain Risk Management (SCRM) Template, U.S. DHS CISA ICT SCRM Task Force, April 2021.

32 https://www.bsa.org/about-bsa

33 https://owasp.org/

34 https://safecode.org/

35 Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF), U.S. NIST, April 23, 2020, https://csrc.nist.gov/Projects/ssdf

36 Report on Mitigating ICT Supply Chain Risks with Qualified Bidder and Manufacturer Lists: Recommendations on the Use of Qualified Lists and Considerations for the Evaluation of Supply Chain Risks, U.S. DHS CISA ICT SCRM Task Force, April 2021.

37 Nair, Pramod, Securing 5G and Evolving Architectures (ISBN: 9780137457939)

38 https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/devsecops-infographic.pdf

39 NIST DevSecOps Project, https://csrc.nist.gov/Projects/devsecops

40 https://www.ericsson.com/en/blog/2021/3/your-guide-to-cicd-in-telecom-networks--for-today-and-tomorrow

41 Executive Order on Improving the Nation's Cybersecurity, The White House, EO 14028, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

42 "The Minimum Elements for a Software Bill of Materials (SBOM), Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity", U.S. DoC and NTIA, July 2021

43 SPDX, https://spdx.dev/

44 CycloneDX, https://cyclonedx.org/

45 David Waltermire et al., Guidelines for the Creation of Interoperable Software Identification (SWID) Tags (2016) (Nat'l Inst. of Standards & Tech. Internal Rep. 8060), http://dx.doi.org/10.6028/NIST.IR.8060 (SWID tags are defined by ISO/IEC 19770–2:2015).

46 O-RAN Minimum Viable Plan and Acceleration towards Commercialization, O-RAN Alliance, June 2021, https://www.o-ran.org/s/O-RAN-Minimum-Viable-Plan-and-Acceleration-towards-Commercialization-White-Paper-29-June-2021.pdf.

47 O-RAN Threat modeling and remediation analysis, v1.0, O-RAN ALLIANCE, March 2021 and O-RAN Security Protocols Specifications-V1.0, O-RAN ALLIANCE, March 2021

48 https://telecominfraproject.com/openran-mou-group/

49 I. Dvoretskyi, "Cloud Native Computing Foundation (CNCF) Charter", GitHub, 5 Aug 2019. [Online]. Available: https://github.com/cncf/foundation/blob/master/charter.md. [Accessed 23 July 2021].

50 https://cdn.brandfolder.io/D8DI15S7/at/gf2qtrc9c3tptgxh5jjf/Open-RAN-Technical-Priority-Document-Final-Version-1.xlsx

51 https://www.o-ran.org/software#:~:text=The%20O-RAN%20Software%20Community%20is%20a%20Linux%20Foundation,License.%20O-RAN%20Software%20Community%20Charter%20Apache%202.0%20License

52 https://wiki.o-ran-sc.org/display/ORAN/Core+Infrastructure+Initiative+%28CII%29+Badging

53 Comments of the National Telecommunications and Information Administration to the FCC NoI on Open RAN, Smith, K., Remaley, E., and Way, J., July 16 2021. https://www.ntia.gov/fcc-filing/2021/ntia-comments-promoting-deployment-5g-open-radio-access-networks

54 Nair, Pramod, Securing 5G and Evolving Architectures (ISBN: 9780137457939)

55 Nair, Pramod, Securing 5G and Evolving Architectures (ISBN: 9780137457939)

56 NIST SP 800-207, Zero Trust Architecture

57 GSMA PRD FS.13 Network Equipment Security Assurance Scheme – Overview, https://www.gsma.com/security/resources/fs-13-network-equipment-security-assurance-scheme-overview/

58 Network Equipment Security Assurance Scheme - Overview Version 2.0 05 February 2021 FS.13-NESAS-Overview-v2.0.pdf (gsma.com)

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 leaders Pramod Nair, Cisco and Scott Poretsky, Ericsson along with many representatives from member companies on 5G Americas' Board of Governors who participated in the development of this white paper.