Establishing a Strong Security Posture for Open RAN

A Technical Paper prepared for SCTE by

Scott Poretsky
Director of Security, North America
Ericsson
Plano, TX, USA
(508) 261-4429
scott.poretsky@ericsson.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

List of Tables

Title **Page Number**

1. Introduction

5G will deliver significant societal value as it provides critical infrastructure, mission critical applications, smart manufacturing, connected car, and other use cases. As a result, our risk tolerance must decrease due to the increased impact from a cyberattack on a 5G network. Radio Access Networks (RAN) is evolving to Open RAN, including Cloud RAN and O-RAN, characterized by a disaggregated, virtualized, cloud-native, automated, and intelligent network. Open RAN brings many security benefits, including vendor diversity, but it also introduces security risks that must be managed to ensure Open RAN deployments have a strong security posture.

Cloud security risks are not exclusive to Open RAN, but they must be considered during a risk analysis to ensure secure Open RAN deployments. Cloud deployments of Open RAN can offer many security advantages inherent from third-party cloud-based services while also expanding the RAN attack surface due to increased internal threats. Open RAN must be built upon a zero trust architecture (ZTA) to mitigate risks from internal and externals threats. This is a new paradigm for securing RAN, where traditional on-premise networks have focused primarily on protection from external threats.

The O-RAN architecture, from the O-RAN Alliance, expands the attack surface by specifying new functions and interfaces built on the 3GPP standardized architecture. The Lower Layer Split (LLS 7-2x) with the Open Fronthaul (OFH) interface, as well as RAN Intelligent Controllers (RICs), with xApps and rApps, and the Open Cloud (O-Cloud) must all be secured to protect O-RAN's network functions, interfaces, and data. The Service Management and Orchestration (SMO) can enhance the Open RAN security posture, but it must also be securely designed and implemented to prevent internal and external threat actors from gaining access and control.

The goal of this paper is to present the security risks and recommend security controls to establish a strong security posture for Open RAN deployments. Section 2 of the paper provides a baseline discussion of evolving Open RAN architectures, including O-RAN from the O-RAN Alliance. Section 3 introduces the Open RAN security posture, presenting the security tradeoffs of Open RAN and expanded attack surface of the O-RAN architecture. Section 4 discusses additional security considerations for a strong Open RAN security posture with focus on ZTA and cloud security to support deployment of 5G critical infrastructure for protection against external and internal threats. Section 5 provides a detailed technical analysis of the security risks across the O-RAN architecture and recommends security controls to mitigate those risks. Recommended security controls are provided with the goal to strive towards a ZTA that protects against internal and external threats, ensuring Open RAN deployments will be secure.

2. RAN Architectures

The 5G network is built from Radio Access Network (RAN) and Core (5GC). RAN uses radio frequencies to provide wireless connectivity to devices for delivery of applications and consists of antennas, radios, baseband (RAN compute), and RAN software enabling high data rates for innovative mobile use cases. Antennas radiate the electrical signals into radio waves and the radio converts digital information into signals that can be transmitted wirelessly while ensuring the transmitted signals are in the assigned frequency bands at the configured power levels. The baseband provides signal processing functions for efficient wireless communication and secure use of spectrum to deliver extremely high data processing speeds.

Traditionally, baseband functionality has been complex software providing intelligence to assign data bits to available frequency and time slots and prioritizing users on a millisecond (or sub-millisecond) basis, running on proprietary hardware deployed at cell sites. With the evolution to virtualization and containerization of network functions, baseband functionality can be implemented in software to operate on Commercial Off the Shelf (COTS) server hardware at edge sites, or central sites, co-located with 5GC components. This means that RAN and 5GC software may be geographically co-located, deployed on the same infrastructure, and managed as a single solution. As a result, the security of 5G RAN has evolved to be as critical and sensitive as security of the 5GC.

Open RAN, including Cloud RAN, such as [1], and O-RAN from the O-RAN Alliance [2], is a general term for open radio access network architectures defined by open and interoperable interfaces, virtualization, cloudification, and intelligence enabled through AI/ML. Open RAN solutions use the 3GPP-specified air interface that provides security features such as signaling confidentiality and integrity protection, user plane confidentiality and integrity protection, and the Subscription Concealed Identifier (SUCI) for subscriber privacy [3].

Cloud RAN is based upon the Third-Generation Partnership Project (3GPP) Release 15 (R15) Higher Layer Split (HLS) having the RAN Compute disaggregated into a Central Unit (CU) and Distributed Unit (DU). The CU and DU use the enhanced Common Public Radio Interface (eCPRI) fronthaul interface between them, as shown in Figure 1. Cloud RAN provides the advantages of open, standards-based cloud-native network functions managed by a SMO, without requiring a LLS.

The O-RAN architecture introduces a LLS disaggregating the RAN's O-DU and O-RU with the Open Fronthaul interface between them, as shown in Figure 1. The O-RAN Alliance's Open Fronthaul interface specifies a Control, User, Synchronization Plane (CUS-Plane) and Management Plane (M-Plane) running over eCPRI. The primary goal of the disaggregation to the O-DU and O-RU is to further increase vendor diversity in the RAN.

The O-RAN architecture also introduces the Near-Real-Time RAN Intelligent Controller (Near-RT RIC) and SMO, with an internal Non-RT RIC, for automation, orchestration, and optimization of RAN functions and performance. The Near-RT RIC and Non-RT RIC are specified to support RAN applications, known as xApps and rApps, respectively, with the goal to enhance RAN innovation and optimization through an ecosystem of purpose-built applications from RIC platform vendors and third-parties. O-RAN specifications also provide an O-Cloud for infrastructure upon which the O-RAN network functions run as applications.

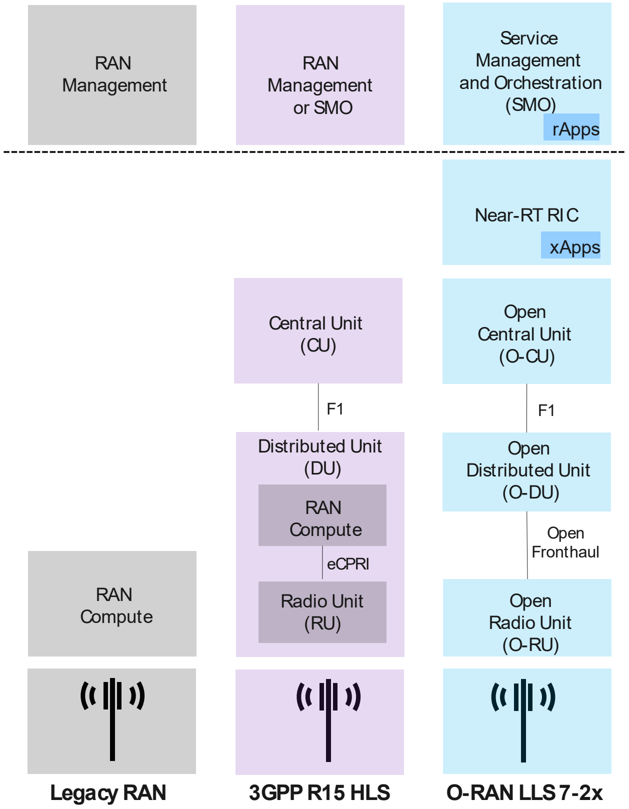


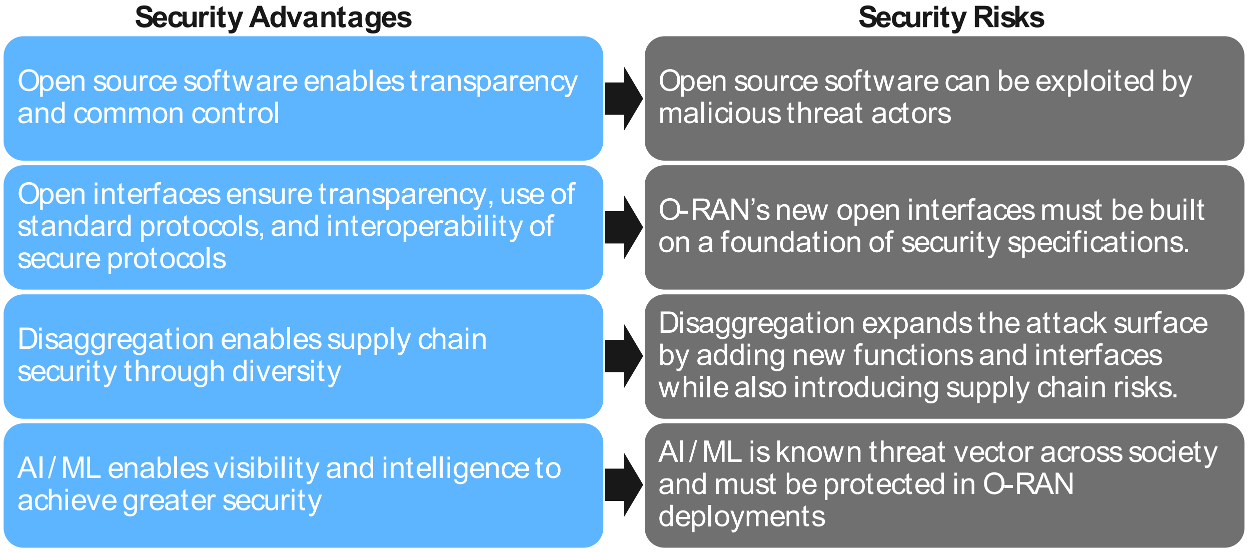
Figure 1 - RAN Splits

3. Open RAN Security Posture

Open RAN solutions and architectures, including Cloud RAN and O-RAN, share common security advantages and disadvantages. This section discusses the security tradeoffs for Open RAN and examines the expanded attack surface specific to the O-RAN architecture.

3.1. Open RAN Security Tradeoffs

A security posture of a telecommunications network is the security status of a network, information, and systems based on security controls *in place* to manage the defense and react to situational changes [4]. Open RAN, including Cloud RAN and O-RAN, provides enhanced RAN security including use of open-source software enabling transparency and common control; open interfaces ensuring transparency and use of standard, interoperable, and secure protocols; disaggregation enabling supply chain security through vendor diversity; and use of AI/ML enabling visibility and intelligence to achieve greater security [5]. However, Open RAN solutions also tradeoff introduction of security risks, such as open-source software vulnerabilities exploited by malicious threat actors, new interfaces with weak security specifications, and architectural modifications that expand the RAN attack surface. These security tradeoffs are summarized in Figure 2. Open RAN security risks were first analyzed in [6] and the O-RAN Alliance Working Group 11 (WG11) (formerly Security Focus Group – SFG) has been evolving O-RAN's security specifications to support a strong O-RAN security posture.



Security Advantages	Security Risks
Open source software enables transparency and common control	Open source software can be exploited by malicious threat actors
Open interfaces ensure transparency, use of standard protocols, and interoperability of secure protocols	O-RAN's new open interfaces must be built on a foundation of security specifications.
Disaggregation enables supply chain security through diversity	Disaggregation expands the attack surface by adding new functions and interfaces while also introducing supply chain risks.
AI / ML enables visibility and intelligence to achieve greater security	AI / ML is known threat vector across society and must be protected in O-RAN deployments

Figure 2 - Open RAN Security Advantages and Risks

3.2. O-RAN Attack Surface

O-RAN introduces architectural changes through disaggregation, opening the ecosystem for increased vendor diversity. The architectural changes that define O-RAN are the LLS 7-2x, OFH interface, RICs, and RAN applications known as rApps and xApps. However, O-RAN's new network functions and interfaces expand the O-RAN attack surface [7], [8], [9]. A strong O-RAN security posture must implement security controls at each layer of the architecture to protect the network functions, interfaces, and data from external and internal threats, as shown in Figure 3. The O-RAN Alliance's WG11 has performed a detailed threat analysis of O-RAN [10] and continues to evolve O-RAN's security specifications to meet the security baseline expected by network operators and their users. The specification effort considers a Zero Trust Architecture (ZTA) in accordance with US NIST SP 800-207 [11] to provide protection from external and internal threats.

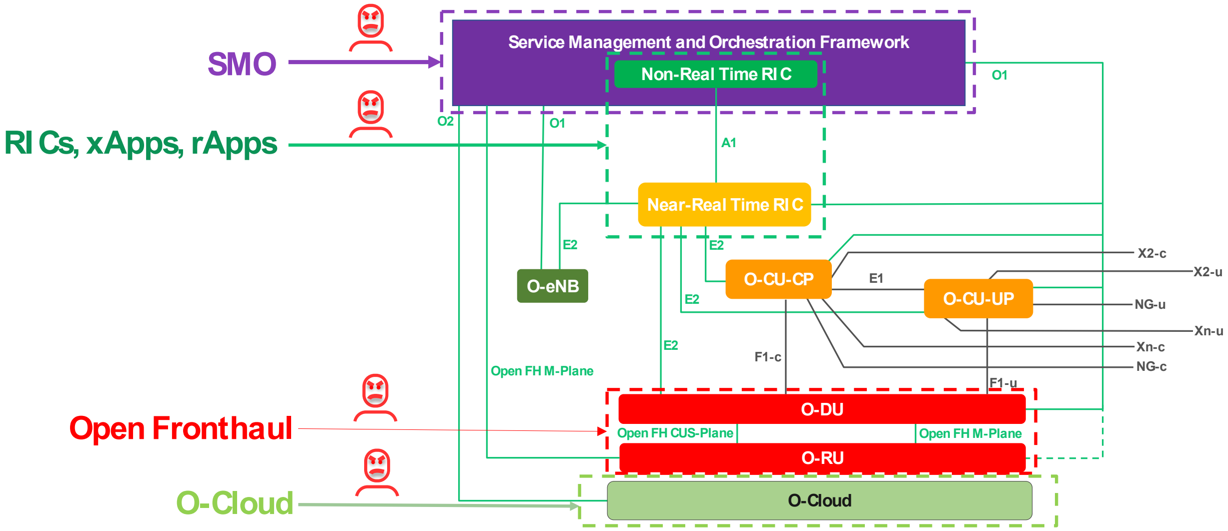


Figure 3 - O-RAN Expanded Attack Surface [adapted from 12]

4. Additional Security Considerations

Additional security considerations should be made to achieve a strong Open RAN security posture built upon a ZTA for cloud deployments. This section discusses ZTA and cloud security to support deployment of Open RAN critical infrastructure that provides defenses against internal and external threats.

4.1. Zero Trust Architecture

5G is the first generation of mobile technology designed for cloud deployments of RAN and Core. Open RAN enables cloud migration of the RAN to leverage its benefits of rapid elasticity, on-demand self-service, broad network access, and multi-tenancy. However, cloud deployments introduce an expanded threat surface due to the increased risk of internal threats, shifting the security paradigm to building a ZTA from the traditional perimeter-based security focused on protecting against external threats. In a ZTA, this is no longer sufficient because we must design for a perimeter-less network [13] that assumes the adversary is already inside the network [14]. This is a new paradigm for RAN security, as RAN has been traditionally secured at the perimeter because it has run on operator hardware in an operator managed network in an operator facility assuming internal trust. 3GPP releases 15 and 16 specify 5G with security features that align well with the NIST seven tenets of a ZTA. Some examples are provided in Table 1 below with additional examples provided in [15].

Table 1 – Alignment of 3GPP 5G Standards to NIST ZTA Tenets (Examples)

#	ZTA Tenet	5G Feature
1	All data sources and computing services are considered resources	The end-to-end 5G network, including UEs, RAN, Transport, Core, Applications, and Services are assets and data sources
2	All communication is secured regardless of network location	Subscriber identity privacy using SUCI . TLS provides confidentiality and integrity protection across the SBI .
3	Access to individual resources is granted on a per-session basis	UE access is granted using 5G-AKA, EAP-AKA’, and EAP-TLS. Authentication and authorization between NFs over SBI in the 5GC is provided with certificate-based mutual authentication using TLS
4	Access to resources is determined by dynamic policy	The PCF feeds the AMF with access and mobility policies that affect UE authorization to access 5G network resources
5	The operator monitors and measures the integrity and security posture of all owned and associated assets	NWDAF incorporates standard interfaces from the SBA to collect data and evaluate systems in terms of compliance with security policy rules
6	All resource authentication and authorization are dynamic and strictly enforced before access is allowed	Mutual authentication enables the device to authenticate the network using the AUTH (Authentication Token) returned by the network
7	The operator collects information about the current state of assets, network infrastructure and communications and uses it to improve its security posture	The MNO should have a mature supply chain risk management to ensure NFs are compliant with GSMA NESAS.

NOTE: See acronym list for acronyms used in Table 1.

While Open RAN provides opportunity to deliver an ecosystem of innovative vendors and products, mobile network operators (MNOs) are accountable to evaluate the security posture of its deployment. A threat analysis identifies potential threats, vulnerabilities, and exploits while a risk analysis determines the likelihood and impact of attacks compromising confidentiality, corrupting integrity, or degrading availability. A ZTA approach may increase risk likelihood scores due to consideration of external and internal threats, while implementation of security controls can decrease risk impact scores. The O-RAN Alliance WG 11 is evolving O-RAN's security specifications to align with industry best practices and meet the security baseline established by 3GPP for 5G, while pursuing a ZTA [16].

4.2. Security Controls for 5G Cloud Deployments

As 5G networks are critical infrastructure, it is important to properly secure cloud deployments to protect against external threat actors at the perimeter and internal threat actors exploiting zero-days, performing lateral movement for reconnaissance, and conducting advanced persistent threats (APTs). With the evolution of 5G to public cloud and hybrid cloud deployments, the 5G attack surface expands due to running on third-party infrastructure in a multi-tenant environment managed by another third-party. The cloud introduces increased internal threats from lateral movement, reconnaissance, and advanced persistent threats (APTs) from nation-state, criminal, and internal threat actors. Open RAN and 5G Core have increased risk of internal threats in the cloud due to increased dependency on cloud service providers, lack of defined security roles across stakeholders, resource sharing with other tenants, greater risk of security misconfiguration, and increased use of open-source software [17].

A risk-based approach must be taken to select the proper security controls for Open RAN deployments to mitigate internal and external threats in the cloud, or O-Cloud. Each layer of the cloud stack must be secured to reduce risk from potential vulnerabilities being exploited by internal or external threat actors. 5G cloud deployments should pursue a ZTA to align with US DHS Cybersecurity and Infrastructure Security Agency (CISA) guidance with the following capabilities [18]:

- prevent and detect lateral movement
- secure isolation of network resources
- data protection
- ensure integrity of cloud infrastructure

Common vulnerabilities, such as misconfigurations, weak authentication and use of open-source software with known vulnerabilities, can be prevented using industry best security practices. Well-known attacks in the cloud, including container escape, host escape, shared resource exhaustion, remote code execution, information disclosure between tenants, distributed denial of service (DDoS), and advanced persistent threats (APT) must be mitigated for Open RAN deployments [19]. Security controls must be provided at each layer of the cloud stack, as shown in Figure 4, to protect data, containers, container runtime engines and orchestration, operating systems, and infrastructure including servers, networks, and storage.

Recommended controls include micro-segmentation, tenant isolation and container isolation, mutual transport layer security (mTLS) 1.2, or 1.3, and X.509 certificates, Identity and Access Management (IAM), Multi-Factor Authentication (MFA), and role-based access controls (RBAC) for user access. To help ensure a secure and trusted runtime environment, Open RAN deployments should operate on a hardware root of trust using hardware security modules (HSM), a purpose-built appliance compliant with 3GPP security standards for hardware-based storage and lifecycle management of cryptographic keys. 5G critical infrastructure deployed in the cloud must have continuous monitoring, logging, and alerting with periodic vulnerability assessments and configuration validation to protect against evolving threats. Security controls for Open RAN deployments in the cloud are discussed further in [20].

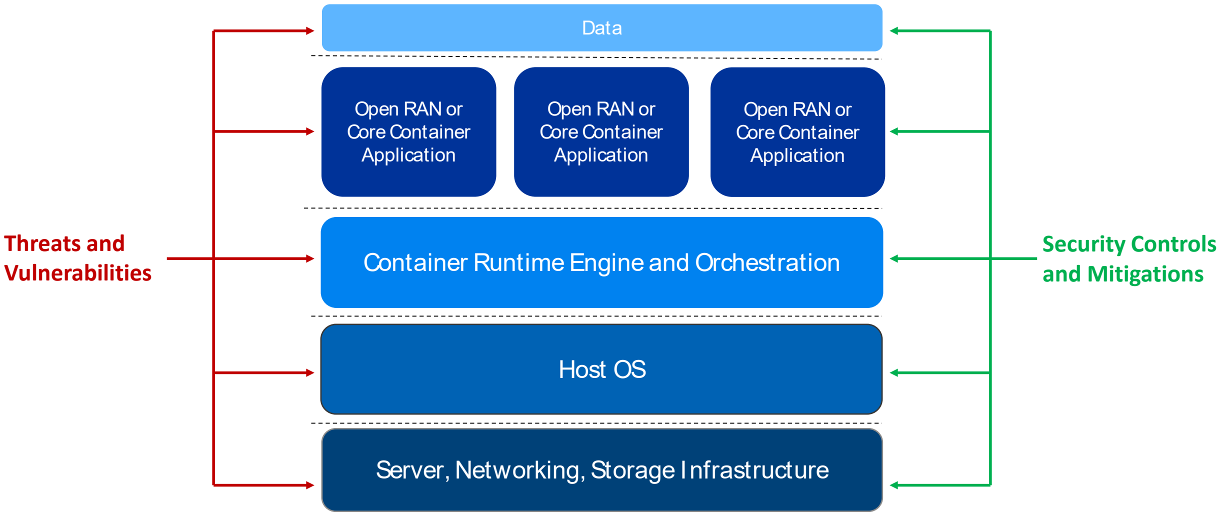

Data
Open RAN or Core Container Application
Open RAN or Core Container Application
Open RAN or Core Container Application
Container Runtime Engine and Orchestration
Host OS
Server, Networking, Storage Infrastructure
Threats and Vulnerabilities
Security Controls and Mitigations

Figure 4 – Multi-Layer Security for 5G Cloud Deployments

5. Securing the O-RAN Architecture

A strong O-RAN security posture provides security controls for protection from external and internal threats introduced by O-RAN's expanded attack surface due to the architectural changes with new network functions, interfaces, and data. This section provides analysis of the threats, risks, and controls for O-RAN's OFH, RICs and applications, SMO, and O-Cloud.

5.1. Open Fronthaul

Fronthaul carries data between the 5G radio and RAN compute nodes using eCPRI, an industry consortium interface specification that utilizes an ethernet for packet forwarding [21]. The design of eCPRI is highly resource efficient and provides the flexibility for different deployment scenarios and functional splits, while enabling use of standard secure IP-based protocols, such as mTLS 1.2, on the fronthaul. The choice of ethernet in eCPRI enables the packet-based fronthaul, COTS, and Open RAN.

O-RAN's OFH interface, using LLS 7-2x, provides O-RAN Alliance specified Control, User, and Synchronization Plane (CUS-Plane) [22] and Management Plane (M-Plane) [23] over eCPRI to provide message exchange between the O-DU and O-RU for coordination. The C-Plane runs over eCPRI to provide message exchange between the O-DU and O-RU for scheduling and beamforming, numerology, and spectrum sharing control. The U-Plane runs over eCPRI to provide uplink and downlink frequency domain IQ data samples. The S-Plane provides timing and synchronization of the O-DUs and O-RUs using Synchronous Ethernet and IEEE 1588 Precision Time Protocol (PTP) [24]. The M-Plane manages and initializes the connection between the O-RU and O-DU. The OFH should have security controls implemented to protect against external and internal threats, consistent with a ZTA. M-Plane and CUS-Plane security are discussed in the sections below.

5.1.1. M-Plane Security

The O-RAN M-Plane specification has mandatory requirement for vendors to support two methods of authentication [25]:

1. O-RU supports Secure Shell version 2 (SSHv2) with password-based authentication of the O-DU and the O-DU supports SSHv2 with simple public key based authentication of the O-RU.
2. The O-RU and O-DU support mutual authentication with TLS 1.2, or higher, and X.509 certificates.

While it is mandatory for the O-RU and O-DU vendors to support both methods of authentication, the operator has the option which to use in production. Password-based authentication is considered weak security for critical infrastructure [26] due to the efficiency in which an attacker can perform a brute force attack upon gaining access to the interface, which can be exploited for lateral movement to northbound functions of the O-RAN architecture to execute broader network attacks. Best security practice, consistent with 3GPP security standards, is for operators to use mTLS with X.509 certificates for 5G deployments [27], including O-RAN deployments for which “it is recommended that operators use NETCONF/TLS and FTPES in production networks” on the M-Plane [28]. This tradeoff for M-Plane security is shown in Figure 5 below.

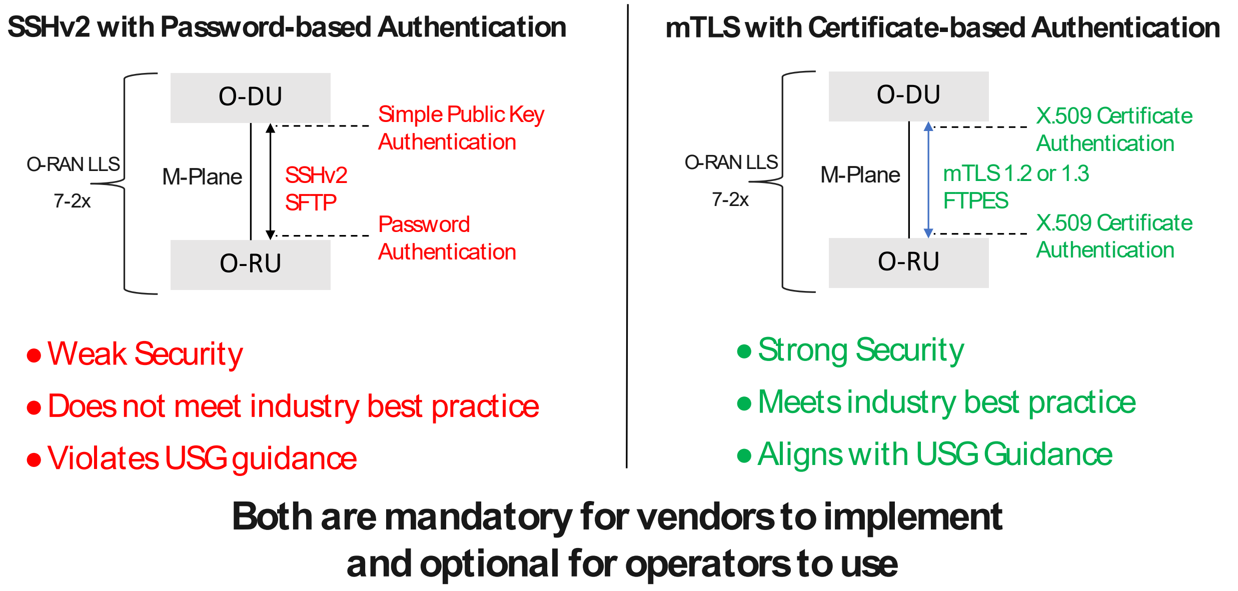

SSHv2 with Password-based Authentication
O-DU
Simple Public Key Authentication
O-RAN LLS 7-2x
M-Plane
SSHv2 SFTP
Password Authentication
O-RU
● Weak Security
● Does not meet industry best practice
● Violates USG guidance
mTLS with Certificate-based Authentication
O-DU
X.509 Certificate Authentication
O-RAN LLS 7-2x
M-Plane
mTLS 1.2 or 1.3 FTPES
X.509 Certificate Authentication
O-RU
● Strong Security
● Meets industry best practice
● Aligns with USG Guidance
Both are mandatory for vendors to implement and optional for operators to use

Figure 3 - OFH M-Plane Security

The M-Plane has two optional deployment models, Hybrid and Hierarchical, as shown in Figure 6, which influences the operator’s approach to certificate management. In the Hybrid model, the O-RU and O-DU have direct IP connectivity to Public Key Infrastructure (PKI) and management systems. The O-RU and O-DU are considered separately managed entities by the SMO platform and enroll their unique operator-signed certificates in a Certificate Authority/Registration Authority (CA/RA) server using Certificate Management Protocol version 2 (CMPv2). PKI provides full lifecycle management of certificates for the O-DU and O-RU and the unique O-RU and O-DU enrolled operator-signed certificates are used to establish the secure mTLS session between O-RU and O-DU.

In the Hierarchical model, the O-DU has direct IP connectivity to PKI and management systems, enrolls its unique operator-signed certificate in the CMPv2 capable CA/RA server, and is considered a managed entities by the SMO platform. The O-RU does not have direct IP connectivity to PKI and management systems and is not considered a managed entity. During start-up installation the O-RU optionally downloads configuration from O-DU, which includes the trust anchor (root certificate) for the O-DU operator-signed certificate used by O-RU to authenticate the O-DU. The configuration may also include identity of a CMPv2 capable CA/RA server reachable through the O-DU, if supported in the production deployment, for certificate enrollment. The O-RU establishes mTLS sessions with the O-DU by using either an enrolled operator-signed certificate in the CA/RA server reachable through the O-DU or its factory installed vendor-signed certificate when the CA/RA server is not reachable through the O-DU, as shown in Figure 6 below. The O-DU installs the O-RU vendor-signed root certificate used for authenticating the O-RU in the Hierarchical model deployment scenario that the O-DU does not provide the O-RU connectivity to a CMPv2 capable CA/RA.

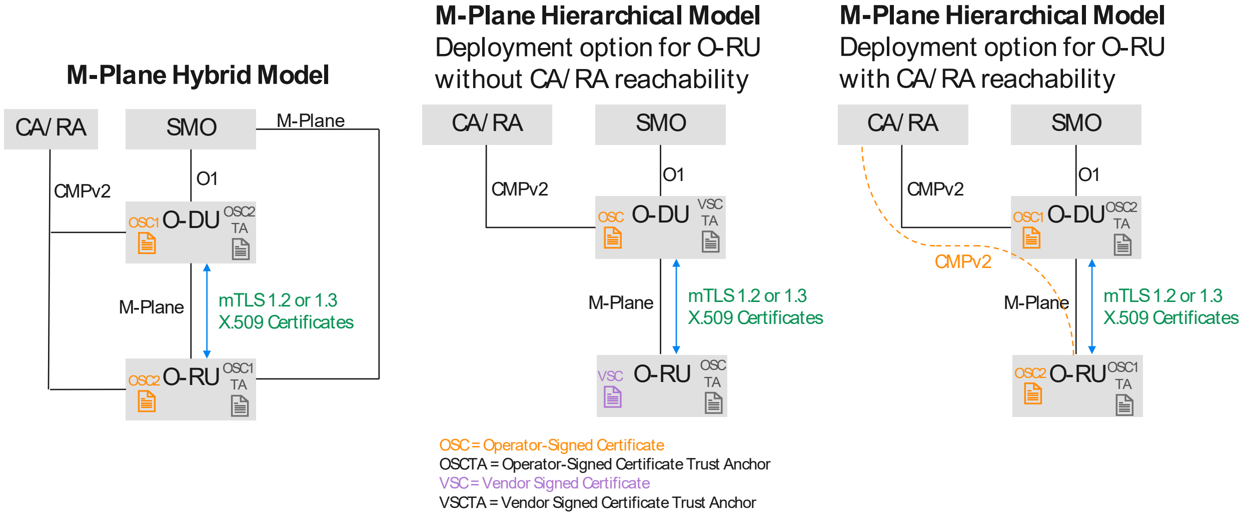

M-Plane Hybrid Model
CA/ RA
SMO
M-Plane
CMPv2
O1
OSC1
O-DU
OSC2 TA
M-Plane
mTLS 1.2 or 1.3
X.509 Certificates
OSC2
O-RU
OSC1 TA
M-Plane Hierarchical Model
Deployment option for O-RU without CA/ RA reachability
CA/ RA
SMO
CMPv2
O1
OSC
O-DU
VSC TA
M-Plane
mTLS 1.2 or 1.3
X.509 Certificates
VSC
O-RU
OSC TA
M-Plane Hierarchical Model
Deployment option for O-RU with CA/ RA reachability
CA/ RA
SMO
CMPv2
O1
OSC1
O-DU
OSC2 TA
CMPv2
M-Plane
mTLS 1.2 or 1.3
X.509 Certificates
OSC2
O-RU
OSC1 TA
OSC = Operator-Signed Certificate
OSCTA = Operator-Signed Certificate Trust Anchor
VSC = Vendor Signed Certificate
VSCTA = Vendor Signed Certificate Trust Anchor

Figure 4 - Certificates in the Optional M-Plane Models

5.1.2. CUS-Plane Security

The OFH interface C/U/S-Plane has control and synchronization messaging that is unauthenticated and in the clear, enabling the man-in-the-middle (MitM) attack vectors shown in Figure 7 and as follows:

- C-Plane - Intercept messages to learn subscriber and network information.
- C-Plane - Message spoofing to inject false information to influence network parameter settings.
- S-Plane - Impersonation of PTP Master Clock or Grand Master, which can be exploited to degrade U-Plane performance and availability.

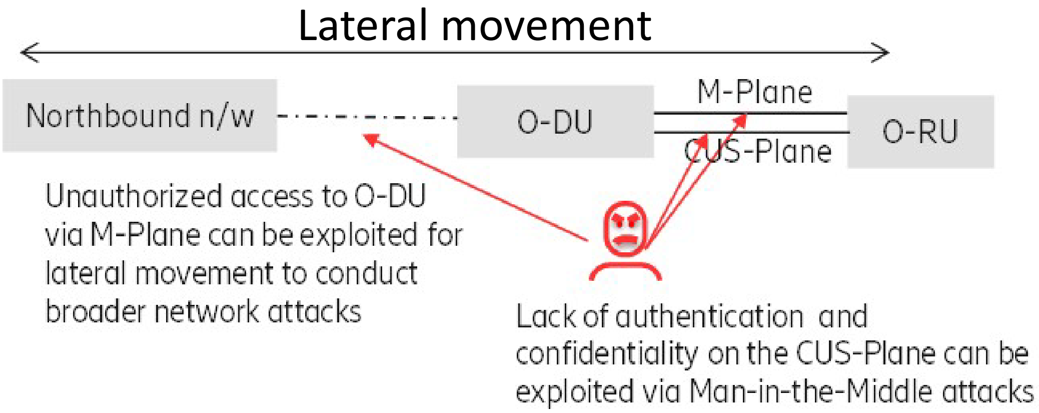

Lateral movement
Northbound n/w
O-DU
M-Plane
CUS-Plane
O-RU
Unauthorized access to O-DU via M-Plane can be exploited for lateral movement to conduct broader network attacks
Lack of authentication and confidentiality on the CUS-Plane can be exploited via Man-in-the-Middle attacks

Figure 5 - O-RAN Open Fronthaul Attack Vectors

Security controls for confidentiality and integrity of messages on the CUS-Plane have been limited due to latency requirements on the CUS-Plane [29]. Further study is needed to identify potential security solutions. IEEE 802.1X-2020 Port-based Network Access Control 0 can be configured to provide protection of OFH interfaces at the physical layer for secure network access in point-to-point LAN segments within the Open Fronthaul network [31].

5.2. RICs and RAN Applications

Open RAN architecture describes two new RIC frameworks, Non-RT-RIC and Near-RT-RIC, for hosting automation applications known as xApps and rApps, respectively, as shown in Figure 8. The xApps and rApps enhance RAN innovation and optimization through an ecosystem of purpose-built applications from RIC platform vendors and third-parties. The Near-RT RIC and xApps provide automation and management of use cases with a suggested control loop of 10 msec to 1 second, while the Non-RT RIC and rApps provide automation and management of use cases with a suggested control loop of one second or more. The Non-RT RIC uses its rApps to decide RAN policy that it pushes to the Near-RT RIC, and its xApps, across the O-RAN Alliance specified A1 interface. The R1 interface between the SMO, Non-RT RIC, and rApps enables any rApp, as a Service Producer or Service Consumer, to work with any SMO and other rApps to enable insights from one rApp to serve as input to another, forming more complex decision-making capabilities.

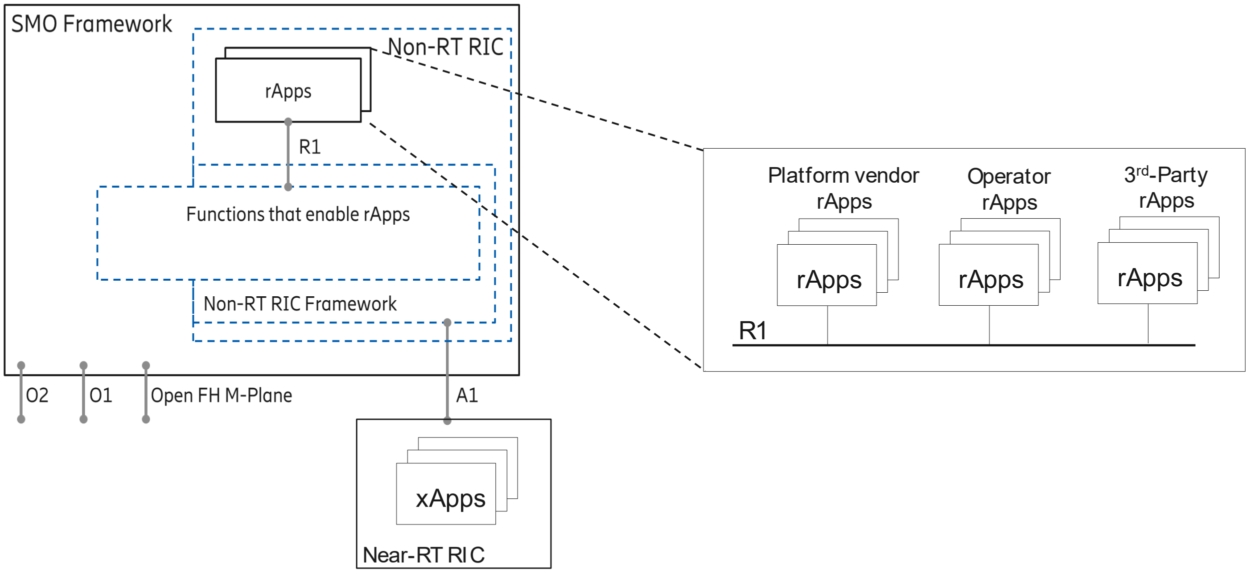


Figure 6 - Open RAN RICs and RAN Applications [adapted from 32]

A primary driver to have xApps and rApps is to broaden O-RAN innovation through smaller best of breed vendors to offer microservices leveraging AI/ML technology for use cases such as spectral efficiency, handover management, network optimization, and network healing. The specification of the A1 and R1 interfaces enables third-party xApps and rApps to efficiently integrate into an Open RAN deployment. However, considerations must be made for architectural and supply chain security risks to the RAN introduced by the RICs and their xApps/rApps. The risks and appropriate security controls are as follow:

- Risk: RICs may decide RAN parameter settings that have direct or indirect conflicts with local gNB decisions, which can degrade performance or availability. The risk of parameter conflicts increases as the number of third-party xApps vendors increases.
    - Solution: The Near-RT RIC supports a conflict mitigation function.
- Risk: Conflicts between rApps from multiple vendors could unintentionally or maliciously push conflicting RAN policies and parameter settings to degrade performance or availability. The risk of parameter conflicts increases as the number of third-party rApps vendors increases.
    - Solution: The Non-RT RIC supports a conflict mitigation function.
- Risk: Use of unsigned, untrusted, or improperly secured third-party xApps or rApps can introduce risks to deployments.
    - Solution: xApps and rApps are digitally signed, penetration tested, and vulnerability scanned prior to delivery. xApps and rApps are securely on-boarded and monitored for anomalous behavior in production. xApps and rApps must support logging and export of logs to the SMO.
- Risk: Malicious Near-RT RIC or Non-RT RIC can attempt to gain access across the A1 interface
    - Solution: The A1 interface supports mutual authentication using mTLS with X.509 certificates.

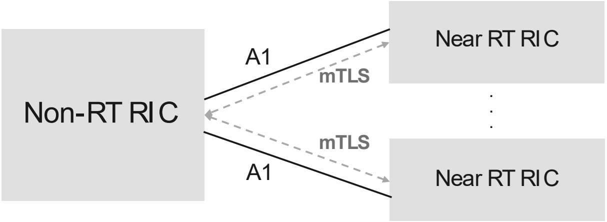


Figure 7 - Mutual authentication on the A1 interface

- Risk: Malicious rApps can attempt to gain access to other rApps through the Non-RT RIC Framework
  - Solution: The R1 interface supports mutual authentication using mTLS with X.509 certificates.

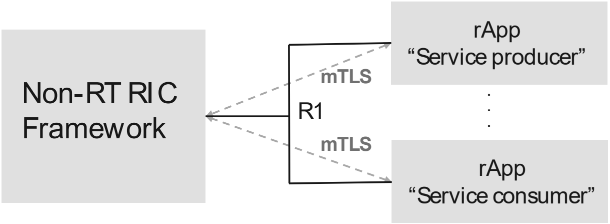


Figure 8 - Mutual authentication on the R1 interface

- Risk: xApps or rApps could be exploited by internal or external threat actors to gain access to private personal information or sensitive business information.
  - Solution: Near-RT RIC, Non-RT RIC, Non-RT RIC Framework, and rApps support authorization using OAuth 2.0. xApps and rApps provide confidentiality protection for sensitive data at rest. Data in motion across the A1 and R1 interfaces has confidentiality and integrity protection using TLS 1.2, or 1.3.

5.3. Service Management and Orchestration

The SMO is an intelligent automation platform for Open RAN, including Cloud RAN and O-RAN, radio resources that applies automation at scale to simplify the complexity of networks, improve network performance, enhance customer experience, and minimize RAN operational costs. The SMO, as a component of the operational support system (OSS), enables automation and increases the abstraction offered to users by managing Open RAN as a service and intents. The O-RAN Alliance defines technical specifications and interfaces related to the O-RAN's SMO Framework.

The SMO, through its Non-RT RIC, provides policy-based guidance and enrichment information to the Near-RT RIC. The Non-RT RIC is an automation platform that uses rApps to deliver higher layer automation policies, orchestrating the Near-RT RIC and RAN nodes. The rApps provide RAN optimization, with the potential to extend to other RAN functions such as capacity planning or security. The rApps are used in conjunction with AI and ML models, leveraging data sets from other functions in the Open RAN and external sources. A secure, standardized R1 interface enables any rApp to work with other rApps, providing the flexibility to group rApps for more complex use cases and decisions.

The visibility and intelligence of the SMO, such as [33], make it an ideal platform to enhance the security posture of Open RAN cloud deployments, aligning with a ZTA. The SMO's logging capabilities coupled with its AI/ML can provide the awareness, threat intelligence, and automated responses needed for a secure Open RAN. The SMO's intelligence and its support for rApps, as shown in Figure 8, enable an ecosystem of purpose-built security functions providing faster and deeper threat detection, helping to ensure secure Open RAN public and hybrid cloud deployments. As the SMO has network-wide visibility from internal and external data sources, its rApps can be purpose-built to provide RAN-protecting security functions, such as Open RAN anomaly detection, O-Cloud threat detection and response, security configuration validation, and security compliance monitoring [34]. The SMO also provides the flexibility to build-in rApps with Security Information and Event Management (SIEM) and Security Orchestration Automation and Response (SOAR) functionality, plus the ability to integrate with external SOAR or SIEM in the security operations center (SOC).

However, securing the SMO is critical because a vulnerability in the SMO could be exploited to serve as an entry point for attacks against Open RAN and lateral movement across Open RAN interfaces and functions. While the SMO can enhance the O-RAN security posture, the SMO must have built-in security controls implemented with a zero trust mindset, assuming the adversary is already inside the network. It is critical that the SMO implements proper controls to ensure secure access with authentication and authorization of external and internal resources. The SMO must also provide security controls for confidentiality, integrity, and availability protection of SMO functions, interfaces, and data from internal and external threats.

5.4. O-Cloud

While cloud threats and cloud security controls are not exclusive to Open RAN deployments, critical infrastructure deployed in the cloud requires a higher level of due diligence and design with built-in security. O-RAN's O-Cloud inherits the threats and vulnerabilities inherent in the cloud where RAN will run on third-party hardware in a multi-tenant environment managed by a third-party. Recent real-world security events, including Solarwinds, Kaseya, Log4Shell, have demonstrated the potential risks of operating Open RAN as critical infrastructure in the cloud due to external and internal threats, including APTs which could exploit Open RAN vulnerabilities for lateral movement and reconnaissance.

O-Cloud is the cloud computing platform specified by the O-RAN Alliance to host O-RAN network functions, including Near-RT RIC, O-CU, and O-DU. The O-Cloud is a collection of physical infrastructure nodes supporting software components, such as operating system, container runtime, and management and orchestration functions. The O2 interface between the SMO and the O-Cloud provides platform resources and workload management of the cloud infrastructure for support of O-RAN network functions, including discover and administrate, create and delete, dynamic scaling, and Fault, Configuration, Accounting, Performance, and Security (FCAPS).

A risk-based analysis, considering a ZTA to protect against internal and external threats, should be performed to secure the O-Cloud and the O2 interface used to manage it. The O-RAN Alliance WG11, O-RAN Security, has identified O-Cloud threats across the five following threat categories [35]:

- Compromise of virtual network function or cloud-native function images and embedded secrets
- Weak orchestrator configurations, access controls and isolation that can be exploited
- Misuse of a virtual machine or container to attack another virtual machine/container, hypervisor/container engine, or other hosts via shared resources such as memory, network, or storage
- Spoofing and eavesdropping on network traffic to access all O-RAN data processed in the workload

- Compromise to supporting network services

These threat categories are consistent with the Cloud Security Alliance (CSA) identification of the current eleven most important threats to cloud deployments as of 2022 [36], including:

1. Insufficient Identity, Credential, Access and Key Management, Privileged Accounts
2. Insecure Interfaces and APIs
4. Lack of Cloud Security Architecture and Strategy
6. Unsecure Third-Party Resources
9. Misconfiguration and Exploitation of Serverless and Container Workloads
11. Cloud Storage Data Exfiltration

The O-RAN Alliance WG11, O-RAN Security, has a current work item to ensure the O-Cloud and the O2 interface will be securely specified to protect against internal and external threats.

6. Conclusion

5G migration to the cloud provides great opportunity to transition the RAN from proprietary hardware to open software while increasing vendor diversity. While Open RAN, including Cloud RAN and O-RAN, provides security advantages, it also expands the RAN attack surface introducing new security risks requiring a shift in security paradigms from a perimeter-based approach to a ZTA that protects against internal and external threats. The O-RAN Alliance's WG11 continues to evolve the security posture of O-RAN's Open Fronthaul interface, RICs, SMO, and O-Cloud to align with a ZTA. Existing security protocols, including mTLS 1.2 with X.509 certificates, CMPv2, and OAuth 2.0, are valuable tools to protect against external and internal threats. The SMO, along with security rApps, can further enhance the security posture of Open RAN deployments. A secure Open RAN can help fulfill the promise of 5G use cases and ensure secure deployment of 5G critical infrastructure in the cloud.

Abbreviations

3GPP	3rd-Generation Partnership Project
AI	Artificial Intelligence
APT	Advanced Persistent Threats
CA	Certificate Authority
CMPv2	Certificate Management Protocol version 2
COTS	Commercial Off the Shelf
CU	Central Unit
DDoS	Distributed Denial of Service
DU	Distributed Unit
eCPRI	enhanced Common Public Radio Interface
FCAPS	Fault, Configuration, Accounting, Performance, and Security
FTPES	File Transfer Protocol Explicit Security
gNB	Next Generation Node B
HLS	Higher Layer Split
HSM	Hardware Security Module
IAM	Identity and Access Management
LLS	Lower Layer Split
MFA	Multi-Factor Authentication
MitM	Man-in-the-Middle
ML	Machine Learning
MNO	Mobile Network Operator
mTLS	Mutual Transport Layer Security
Near-RT RIC	Near-Real-Time RAN Intelligent Controller
Non-RT RIC	Non-Real-Time RAN Intelligent Controller
O-Cloud	Open Cloud
O-CU	Open-Central Unit
O-DU	Open-Distributed Unit
O-RU	Open-Radio Unit
OFH	Open Fronthaul
PKI	Public Key Infrastructure
PTP	Precision Time Protocol
RA	Registration Authority
RAN	Radio Access Network
RBAC	Role-Based Access Controls
RIC	RAN Intelligent Controller
SMO	Service Management and Orchestration
SSHv2	Secure Shell version 2
SUCI	Subscription Concealed Identifier
TA	Threat Analysis
TLS	Transport Layer Security
ZTA	Zero Trust Architecture

Bibliography & References

[1] Ericsson Cloud RAN, https://www.ericsson.com/en/ran/cloud

[2] O-RAN Architecture Description, v6.0, Technical Specification (TS), O-RAN Alliance, WG1, March 2022.

[3] Security architecture and procedures for 5G System, Technical Specification (TS), 3GPP TS 33.501, Release 16.

[4] Adapted from NIST Computer Security Resource Center, Glossary, https://csrc.nist.gov/glossary/term/security_posture#:~:text=Definition(s)%3A,react%20as%20the%20situation%20changes.

[5] ENSIA NIS Cooperative Group, May 11.

[6] Security Considerations of Open RAN, S. Poretsky and J. Boswell, Ericsson, Aug 2020.

[7] O-RAN Minimum Viable Plan and Acceleration towards Commercialization, White Paper, O-RAN Alliance, June 2021.

[8] Open RAN Risk Analysis, Germany BSI, Federal office of Information Security, English Translation, February 2022.

[9] Report on Open RAN Cybersecurity, ENISA NIS Cooperative Group, May 2022.

[10] O-RAN Threat Modeling and Remediation Analysis, v3.0, O-RAN Alliance, WG11, March 2022.

[11] Zero Trust Architecture, NIST SP 800-207, US NIST, Aug 2020.

[12] Adapted from O-RAN architecture diagram from O-RAN Alliance, O-RAN Architecture Description, v6.0, O-RAN Alliance, WG1, March 2022.

[13] Zero Trust Architecture, NIST SP 800-207, US NIST, Aug 2020.

[14] Security Guidance for 5G Cloud Infrastructures, US DHS CISA, Oct 2021.

[15] Security for 5G, 5G Americas, December 2021.

[16] O-RAN Minimum Viable Plan and Acceleration towards Commercialization, White Paper, O-RAN Alliance, June 2021.

[17] Report on the Cybersecurity of Open Radio Access Networks, ENISA NIS Cooperative Group, May 2022.

[18] Security Guidance for 5G Cloud Infrastructures, US DHS CISA, Oct 2021.

[19] “OpenRAN – 5G hacking just got a lot more interesting“, Karsten Nohl, MCH (May Contain Hackers), July 2022, https://www.youtube.com/watch?v=LRQsFTmWa2w&t=13s.

[20] Security Considerations for Cloud RAN, S. Poretsky and J. Jardal, Ericsson, Sept 2021.

[21] eCPRI Specification, v2.0, CPRI, May 2019, http://www.cpri.info/index.html.

[22] CUS-Plane Specification, v9.0, Technical Specification (TS), O-RAN Alliance, WG4, March 2020.

[23] M-Plane Specification, v9.0, Technical Specification (TS), O-RAN Alliance, WG4, March 2020.

[24] IEEE Std 1588-2019 "Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", November 2019.

[25] M-Plane Specification, v9.0, Technical Specification (TS), O-RAN Alliance, WG4, March 2020.

[26] https://www.cisa.gov/uscert/ncas/current-activity/2021/08/30/cisa-adds-single-factor-authentication-list-bad-practices, US DHS CISA, August 2021.

[27] Security Guidance for 5G Cloud Infrastructures, US DHS CISA, Oct 2021.

[28] M-Plane Specification, v9.0, Technical Specification (TS), O-RAN Alliance, March 2020.

[29] CUS-Plane Specification, v9.0, Technical Specification (TS), O-RAN Alliance, WG4, March 2020.

[30] IEEE Std 802.1X-2020 "IEEE Standard for Local and Metropolitan Area Networks--Port-Based Network Access Control", February 2020.

[31] O-RAN Security Protocols Specifications, v3.0, O-RAN Alliance, WG11, March 2020

[32] Adapted from O-RAN architecture diagram from O-RAN Alliance, O-RAN Architecture Description, v6.0, O-RAN Alliance, WG1, March 2022.

[33] Ericsson Intelligent Automation Platform (EIAP), https://www.ericsson.com/en/ran/intelligent-ran-automation/intelligent-automation-platform.

[34] Intelligent Security: Using the SMO to enhance the Open RAN Security Posture, S. Poretsky and J. Jardal, Ericsson, June 2022.

[35] O-RAN Threat Modeling and Remediation Analysis, v3.0, O-RAN Alliance, WG11, March 2022.

[36] Top Threats to Cloud Computing: The Pandemic 11, Cloud Security Alliance (CSA), June 2022.