December 2022

COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL VIII

REPORT ON CHALLENGES TO THE DEVELOPMENT OF ORAN TECHNOLOGY AND RECOMMENDATIONS ON HOW TO OVERCOME THEM

DRAFTED BY
WORKING GROUP 2: PROMOTING SECURITY, RELIABILITY, AND INTEROPERABILITY OF OPEN RADIO ACCESS NETWORK EQUIPMENT

Table of Contents

1 Executive Summary

The Federal Communications Commission (FCC) tasked CSRIC VIII "to provide recommendations to advance security, reliability, and interoperability of Open Radio Access Network (RAN) equipment in the United States, and what new actions can be undertaken to support secure and interoperable Open RAN design and deployment."[1]

Open RAN enhances the 5G mobile network by evolving the RAN architecture with open interoperable interfaces, virtualization, and big data and AI-enabled intelligence. Open RAN includes O-RAN, Virtual RAN (vRAN), Cloud RAN, and other technologies. The introduction of Open RAN enables mobile network operators to use equipment from multiple vendors while ensuring interoperability.

This report opens with background information on Open RAN technology, ecosystem, supply chain and deployment. This is followed by in-depth analysis of Open RAN architecture and cloud infrastructure, software development, operations and supply chain, including recommendations in each area. The report concludes with a comprehensive list of recommendations to the FCC and to Industry, as well as proposed future areas of investigation.

The analysis found that some concerns exist in both Open RAN and closed proprietary RAN. Open RAN security considerations with applications, open source software, supply chain, and zero trust are consistent with those from the Information and Communications Technology (ICT) sector, and Open RAN must implement the ICT best practices to address these concerns. Open RAN utilizes existing 5G Core network technologies including multi-vendor core network functions and 5G cloud infrastructures. Open RAN will benefit by adopting the ICT and 5G best practices to ensure secure, reliable and interoperable deployment and operation.

Open RAN brings new capabilities and concerns with the introduction of xApps/rApps application frameworks, AI/ML technology, and the O-RAN Alliance defined Open Fronthaul network connecting base stations and radios with real-time performance requirements. Some of these concerns are shared with the ICT sector, and both Open and proprietary fronthaul solutions are challenged to balance the security requirements with performance and cost considerations.

With the continued evolution of Open RAN, security and reliability continues to be addressed by the appropriate groups such as O-RAN Alliance and ICT and 3GPP standards evolution.

This analysis is consistent with the conclusions from the Enduring Security Framework (ESF) report on "Open RAN Security Considerations"[2]

[1] Communications Security, Reliability, and Interoperability Council VIII (CSRIC VIII), *CSRIC Working Group Tasks* (Sept. 2021), https://www.fcc.gov/about-fcc/advisory-committees/communications-security-reliability-and-interoperability-council-1.

[2]NSA Enduring Security Framework (ESF) and CISA, Open Radio Access Networks Security Considerations, 2022, http://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf.

2 Introduction

This report identifies security, reliability and interoperability challenges facing Open RAN technology in the US, and provides recommendations to the FCC, and to industry, for addressing these challenges. This work builds on earlier CSRIC recommendations, including CSRIC VII recommendations for securing 5G SA networks, and CSRIC VI recommendations for securing open-source software and digital signing of production software in 5G networks.

The three aspects of security, reliability and interoperability are in many ways related. Addressing a security aspect often touches on reliability and interoperability, which is reflected in the analysis.

The report content and recommendations were crafted using expert knowledge from industry and government, as well as collaboration with other CSRIC VIII working groups and presentations from several subject matter experts.

2.1 CSRIC Structure

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

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

Table 1 - Working Group Structure

2.2 Working Group 2 Team Members

Working Group 2 members are listed below.

Name	Company
Rob Alderfer	Charter Communications
Robert Dew	CISA
Marla Dowell	NIST
Andrew L. Drozd	ANDRO Computational Solutions
Russ Gyurek	Cisco Systems, Inc.
Javed Khan	Rakuten Symphony
Mike Loushine	AT&T, Inc.
Jennifer Manner	Hughes Communications
Martin McGrath	Nokia
Jack Nasielski	Qualcomm Technologies, Inc.
Scott Poretsky	Ericsson
Vishwanath Ramamurthi	Verizon Communications
Stefan Saroiu	Microsoft Corporation
Tom Sawanobori	CTIA
Tim Schram	NARUC
Nick Solano	Qcommunications, LLC
Eric Tamarkin	Samsung Electronics America
Jean Trakinat	T-Mobile USA
Claire Vishik	Intel
Henry Young	BSA | The Software Alliance
Tim May	NTIA

Table 2 - List of Working Group Members

Alternates for members are listed below.

Name	Company
Reza Arefi	Intel
Afeite Dadja	CTIA
Brian Daly	AT&T
Heidi Obermeyer	BSA | The Software Alliance
Anand Palanigounder	Qualcomm
Sanil Rama Chandran	Samsung Electronics America
James B. Ramsay	NARUC
Nancy Shemwell	Rural Wireless Association (RWA)
Lakhbir Singh	Charter Communications
Matthew Sneed	Hughes Communications
Ryan Stokes	Rural Wireless Association
Lap Tse	Verizon Communications
Timothy O. Woods	ANDRO Computational Solutions

Table 3 - List of Working Group Alternates

2.3 Subject Matter Expert Contributors

Name	Company
Nagendra Bykampadi	Rakuten Symphony
Dr. Ken Urquhart	Zscaler
Chris Boyer	AT&T, behalf of the Open RAN Policy Coalition.

Table 4 - List of Subject Matter Experts

3 Objective, Scope, and Methodology

3.1 Objective

The Chairwoman of the FCC directs CSRIC VIII to provide recommendations to advance security, reliability, and interoperability of Open Radio Access Network (RAN) equipment in the United States and what new efforts can be undertaken to support secure and interoperable Open RAN design and deployment. The RAN is the final link between the network and the phone. It includes the antennae on towers, buildings, and in stadiums, plus the base stations. When a consumer makes a call or connects to a remote server, the antenna transmits and receives signals to and from the consumer's mobile phone or other handheld device. The signal is then digitalized in the RAN base station and connected into the network. The introduction of Open RAN enables mobile network operators to use equipment from multiple vendors and still ensure interoperability

3.2 Scope

CSRIC has previously considered security risks in emerging 5G networks.[3]

CSRIC VIII builds on this work and expands it as one part of its exploration of the development and deployment challenges facing Open RAN technology, including the extent Open RAN technology may increase the attack surface and how best to mitigate such security challenges.

Further, CSRIC VIII will consider how the FCC can support the goals of developing and deploying secure, open and interoperable networks when the FCC participates in standards-setting bodies like 3GPP and the Alliance for Telecommunications Industry Solutions.

3.3 Methodology

The following key areas were studied with emphasis on security, reliability, and interoperability:

- O-RAN Architecture
- Open RAN Cloud Infrastructure
- Open RAN Deployments
- Open RAN Operations
- Open RAN Supply Chain
- Open RAN Software Development Process

In this report, the term "O-RAN" refers to the O-RAN Alliance, while the term "Open RAN" applies to all Open RAN technologies.

[3] CSRIC VII Report on Recommendations for Identifying Optional Security Features that can Diminish the Effectiveness of 5G Security, (10 March 2021); CSRIC VII Report on 5G from Legacy Vulnerabilities and Best Practices for Mitigation (10 June 2020).

4 Background

Open RAN is the industry term for the evolution of the RAN architecture to open interoperable interfaces, virtualization, and big data and AI-enabled intelligence. Open RAN includes O-RAN, Virtual RAN (vRAN), Cloud RAN and other technologies.

The disaggregation of RAN hardware and software, and the use of generic hardware for RAN functions is known as virtualized RAN or vRAN in short. When vRAN is designed to be cloud native that incorporates microservices, continuous integration/continuous delivery (CI/CD) and containerization, it may be referred as Cloud RAN or vRAN.

The O-RAN Alliance is an industry Open RAN initiative, launched in 2018, composed of operators, vendors, and academic researchers who define specifications for the Open Fronthaul interface and other new elements such as Service Management and Orchestration (SMO), RAN Intelligent Controllers (RICs), xApps and rApps, and O-Cloud. The primary goal of O-RAN Alliance is to broaden a supply chain that opens the RAN market for new suppliers.

The term OpenRAN, as distinct from Open RAN refers to the initiative driven by Telecom Infrastructure Project (TIP), initiated by Facebook. TIP's member organizations include operators and RAN equipment suppliers. The group creates high-level technical requirements for significant use cases, test and validate network elements, products, and configurations; and share best practices for commercial deployments of the tested technologies. The core activities of this group are to create high-level technical requirements for significant uses, test and validate the network elements, products, and configurations; and share best practices for commercial deployments of the tested technologies.

While initial Open RAN efforts began in 2016, standardization work began in 2018. Thus, the development of O-RAN standards is relatively new. The increasing dependency on cellular networks requires any/all network technology to ensure security, reliability, and interoperability. Key drivers for operators are the ability to enable new network function innovation driven by software, decoupling new network functions from hardware investment cycles. Software-driven network functions also enable greater specialization among suppliers, empowering operators to select from a more diverse suite of vendors that represent best-of-breed for a growing set of network needs.

The O-RAN Alliance is responsible for the specification of the O-RAN Architecture components and interfaces. Multiple new interfaces and profiles of existing 3GPP defined interfaces are being specified with the degree of completeness of some interfaces more than others. Completing this work such that all interfaces reach an acceptable level of maturity is an important task to ensure that there are complete and stable interface specifications available for product/solution implementations to be based upon as well as providing a baseline against which Interoperability Testing can be conducted.

This report bases the technical reasoning on the work done by the O-RAN Alliance,[4] technical discussions by industry and government subject matter experts, and publicly available information provided by standards bodies, industry organizations and other sources.

[4] O-RAN Alliance, http://www.o-ran.org (last visited October 24, 2022).

4.1 Cellular Radio Access Networks

The RAN connects end user equipment (UE) to a core network via cells sites. The key function of the RAN is to provide an air interface towards the UE and handle all aspects associated with radio signal processing and radio resource control to enable a subscriber to attach to the network and use supported services. The introduction of new access technologies in 5G allows new levels of flexibility in architecting, scaling, and deploying telecommunication networks leading to disaggregated networks.

This technology advancement, along with advances in computing platforms as well as some industry driven initiatives, have given rise to new RAN architectures such as vRAN and Open RAN. Figure 1 below shows the high-level 5G architecture. Legacy networks and the majority of 5G networks are currently being deployed using the traditional RAN architecture where all baseband processing is implemented as a single monolithic appliance called the baseband unit (BBU), RF functions are performed by a radio unit and vendor proprietary interfaces are used between the BBU and the radio unit.

At a high level any wireless network consists of following main network elements, a RAN, a Core Network and User Equipment (UE). The following diagram shows a 3GPP defined RAN architecture consisting of a gNB-CU and gNB-DU which interface via the standardized F1 interface. Although not specified by 3GPP actual implementations of a gNB-DU may consist of a DU and RU with a proprietary interface between them, known as the Front Haul interface. One of the innovations that O-RAN Alliance introduces is the formal specification of the interface between the DU and RU, referred to as the Open Front Haul (OFH) interface.

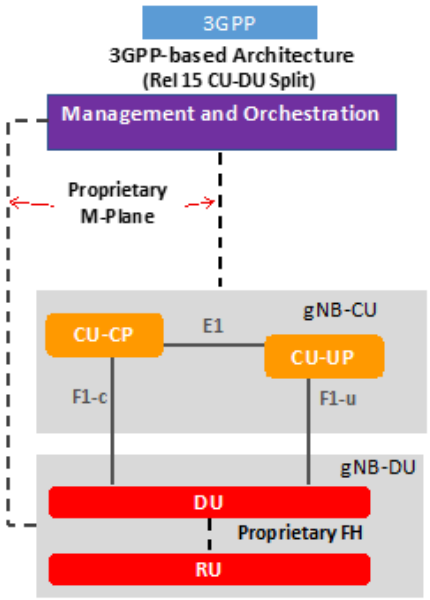

Figure 1: 5G high-level architecture[5]

[5] Adapted from O-RAN Architecture Description, v7.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

This includes the 3GPP defined higher layer Centralized Unit (CU) - Distributed Unit (DU) split using FI interface, and DU-RU split using the O-RAN Open FH interface. This innovation as well as advancements in general-purpose compute have led to the development of virtualized RAN and Open RAN systems.

From a RAN perspective, a disaggregated RAN consists of three primary components: Radio Unit (RU), DU, and CU. The RAN architecture may have the 3GPP defined higher layer split (HLS) of the CU-DU using the F1 interface and the lower layer split (LLS) of the DU-RU using the O-RAN Open Fronthaul (OFH) interface. This novel architecture and advancements in general-purpose compute led to the development of virtualized RAN and Open RAN systems. O-RAN uses the 3GPP-standardized air interface.

- The RU includes macro, micro, small cells, and indoor radios as per network requirement. These radio units host the RF and Low-PHY layers to provide for the[6] transmission, reception, amplification, and digitization of the radio frequency signals.
- The DU is generally deployed near the RU, is a logical node hosting Radio Link Control (RLC)/Medium Access Control (MAC)/High-PHY layers based on a lower layer functional split. Here the DU and Remote Radio Unit (RRU) function includes real-time Layer 2 (L2) functions, base band processing and radio frequency processing.
- The CU is a logical node hosting the Radio Resource Control (RRC) and Packet Data Convergence Protocol (PDCP) functions. It is generally deployed close to the core network and may support multiple DUs.

4.2 Open RAN Ecosystem

Current 5G deployments are largely built on the 3GPP native 5G RAN architecture. Significant development is required to realize the benefits to innovation and competition associated with Open RAN architectures. Virtualized and cloud-native functions must be standardized, developed, and integrated and then be deployed and operated.

One major driver for Open RAN is the desire is to expand the RAN supply chain. Service providers want wider vendor choice and flexibility and reliance upon secure supply chains. The introduction of RAN disaggregation and virtualization, open and interoperable interfaces and intelligent control is expected to realize more scalable and automated networks and reduction in total cost of ownership (TCO).

There are a few challenges which need to be addressed to deploy open and disaggregated networks. They include securing new attack surfaces due to the introduction of virtualization, open interfaces and new network elements such as RIC platforms and interoperability testing necessary to support the increase in vendor diversity. This report takes a closer look at these challenges and provides guidelines and recommendations to address these challenges.

[6] NSA Enduring Security Framework (ESF) and CISA, Open Radio Access Networks Security Considerations, 2022, http://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf.

4.3 O-RAN

The O-RAN architecture envisioned by O-RAN Alliance[7] is built upon 3GPP's Release 15 and beyond RAN architecture[8] that disaggregates a monolithic 5G Node B (gNB) into gNB-CU and gNB-DU as well as gNB-CU into gNB-CU-Control Plane (CP) and gNB-CU-User Plane (UP). Open RAN provides further standardized disaggregation of the RAN, introducing the Open FH interface to further disaggregate the gNB-DU into O-DU and O-RU. In addition, O-RAN introduces the Non-Real Time and Near-Real Time RICs, potentially expanding the attack surface and introducing additional security risks.[9] Figure 2 below shows the additional functions and interfaces in the disaggregated O-RAN architecture[10] relative to disaggregated 3GPP RAN architecture.[11] At the same time, Open RAN architectures, with appropriate security framework, could provide a path to more secure open networks and interfaces over what exists today by providing better visibility and control over the network.[12]

[7] O-RAN Alliance, *Specifications*, https://www.o-ran.org/specifications (last visited 17 November 2022).

[8] 3GPP TS 38.300 and 3GPP TS 38.401, http://www.3gpp.org (last visited Oct. 22, 2022).

[9] NSA Enduring Security Framework and CISA, Open Radio Access Networks Security Considerations, (2022), http://www. www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-consideration_508.pdf; Ericsson, Security Considerations of Open RAN (2020), http://www.ericsson.com/4a4b77/assets/local/security/security-considerations-open-ran.pdf; O-RAN Alliance, O-RAN Minimum Viable Plan and Acceleration towards Commercialization, (2021); Germany BSI, Open RAN Risk Analysis, (2021), https://www.bsi.bund.de/ DE/Service-Navi/Publikationen/Studien/Open-RAN/Open-RAN_node.html;jsessionid=7E6F065AA03CD6753849A31E226B8033.internet481; EC NIS Cooperation Group, Report on the Cybersecurity of Open RAN (2022), http://www.digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks.

[10] O-RAN Alliance, *Specifications*, https://www.o-ran.org/specifications (last visited 17 November 2022).

[11] 3GPP TS 38.401, http://www.3gpp.org (last visited October 24, 2022).

[12] Mavenir, *Resources*, *Security in Open RAN*, Security in Open RAN (2021). https://www.mavenir.com/resources/security-in-open-ran/ (last visited 18 November 2022); Altiostar, Intel, Cisco, RedHat, Security Benefits of Open Virtualized RAN, (2020), https://www3-realm.cisco.com/c/dam/en/us/solutions/service-provider/pdfs/5g-network-architecture/white-paper-sp-open-vran-security-benefits.pdf (last visited 18 November 2022); Qualcomm, Towards enabling Secure 5G networks with O-RAN (2022); O-RAN Alliance, The O-RAN ALLIANCE Security Task Group Tackles Security Challenges on All O-RAN Interfaces and Component (2020), https://www.o-ran.org/blog/the-o-ran-alliance-security-task-group-tackles-security-challenges-on-all-o-ran-interfaces-and-components; Deutsche Telekom, Orange, Telefonica, TIM, and Vodafone, Open RAN Security White Paper under the Open RAN MOU, (2022).

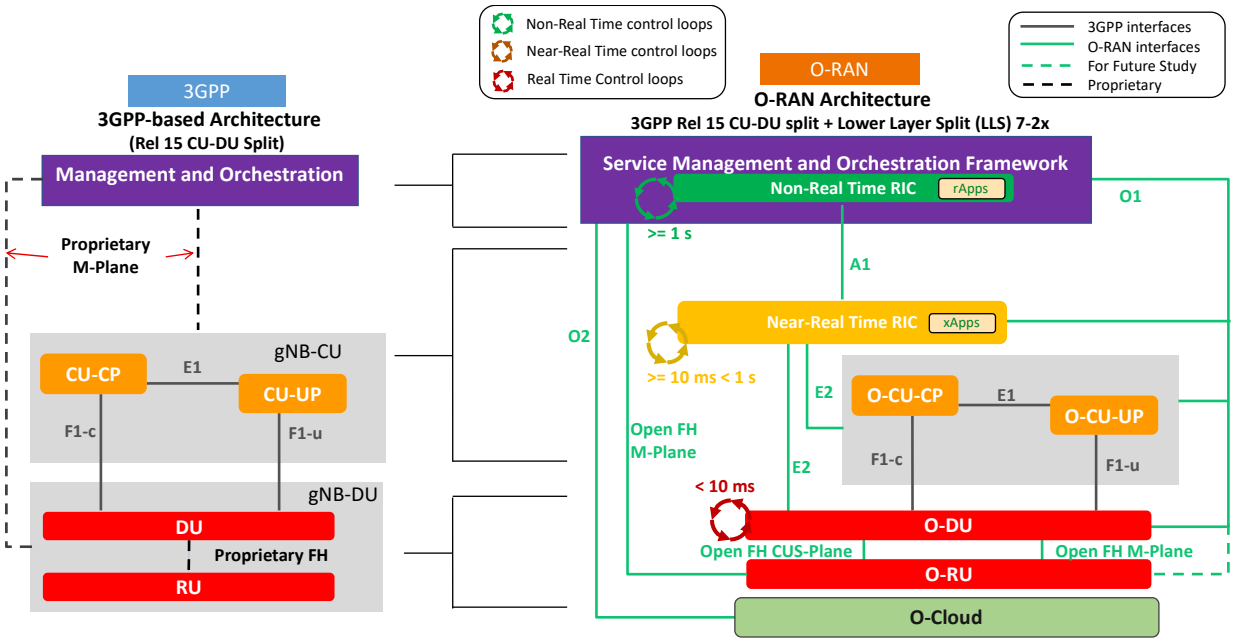

Figure 2. Comparison of 3GPP and O-RAN Architectures[13]

O-RAN standardizes the Open Fronthaul (OFH) between the Open DU (O-DU) and Open RU (O-RU) using the LLS 7-2x,[14] as shown in Figure 2. The O-RA+N OFH includes the Open FH Control User Synchronization (CUS) Plane and the OFH M-plane interfaces. The OFH CUS Plane interface specifies the Control, User and Synchronization plane aspects between the O-DU and O-RU. The OFH M-plane specifies Management plane aspects related to the O-RU. It allows the use of either a hierarchical deployment mode (O-DU manages the O-RU) or a hybrid deployment mode (O-DU and SMO together manage the O-RU), as shown in Figure 3.

[13] Adapted from O-RAN Architecture Description, v7.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

[14] O-RAN Architecture Description, v7.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

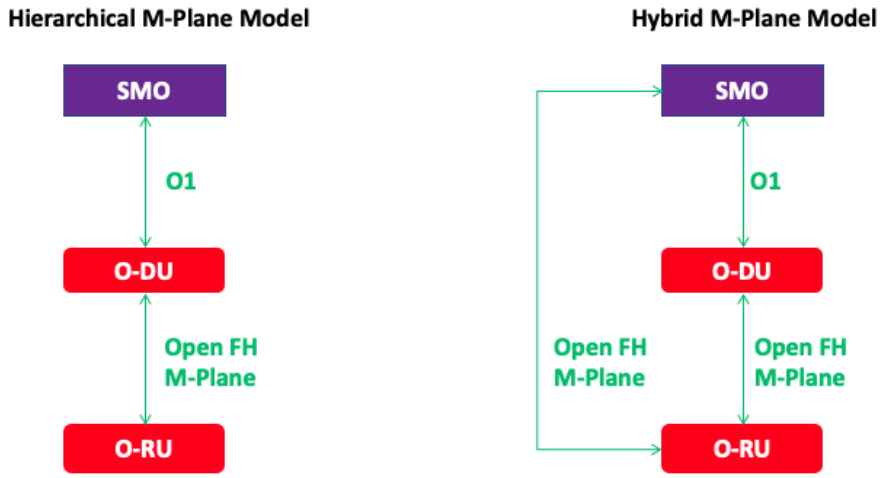

Figure 3. Comparison of Hierarchical and Hybrid M-Plane models. (CSRIC VIII)

O-RAN introduces a SMO function with standardized interfaces to O-RAN elements (O-CU, O-DU, O-RU, RICs), as well as to the Cloud platform hosting the O-RAN elements (O-Cloud). This enables operators to use a common management platform across a multi-vendor network, providing better visibility and simplified management and orchestration across the whole RAN. The SMO uses the O1 interface to manage Open-Centralized Unit-Control Plane (O-CU-CP), Open-Centralized Unit-User Plane (O-CU-UP), Near-RT RIC, and O-DU. The SMO, together with O-DU, manages the O-RU in the Hybrid deployment model using the O-RAN FH M-Plane interface. The SMO does not directly manage the O-RU in the Hierarchical deployment model, instead managing it via the O-DU. In both the Hierarchical and Hybrid models, the O-RU is managed using the Open FH M-Plane interface, as shown in Figure 3.

O-RAN also introduces specifications for two types of RICs: the Non-Real Time RIC (Non-RT RIC) and the Near-Real Time RIC (Near-RT RIC), as shown in Figure 2. The SMO includes the Non-RT RIC with rApps to provide optimization and other functions for the RAN. The Non-RT RIC provides higher layer automation policies with a control loop greater than 1 second using automation applications known as rApps. These policies can be implemented through either the Near-RT RIC, with the Non-RT RIC effectively orchestrating the Near-RT RIC, or through direct connection to the RAN nodes using open interfaces, such as the O1, O2 and A1. The Near-RT RIC provides lower-level or RAN-specific programmatic control of Open RAN O-CU and O-DU using automation applications known as xApps with a control loop of 10ms to 1s.

The O-RAN architecture is an open, adaptive, and intelligent architecture that intends to improve operational efficiencies by leveraging artificial intelligence/machine learning (AI/ML) to automatically manage network resources for use cases such as traffic steering, quality of experience prediction, and anomaly detection. The O-RAN Alliance specifications[15] provide a framework to use AI/ML in the RIC platforms to optimize radio resources in networks to improve performance and automate operations through intelligent algorithms that improve the system continuously. AI/ML-enabled closed-loop automation will help in reducing operating

[15] O-RAN Use Case Analysis Report, v9.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited 17 November 2022).

expenditures through advanced and adaptive self-managing capabilities accelerated time-to-value and reduced risk of human errors.

The O-RAN Alliance has three specification release cycles per year, typically in March, July, and November,[16] which continue to evolve the specifications with new features and enhancements.

Security continues to be at the forefront of the O-RAN Alliance's work.[17] Working Group 11 (WG11), formerly the Security Focus Group (SFG) and Security Task Group (STG), was founded in March of 2020 and is leading all O-RAN working groups to define the appropriate level of security requirements. WG11 follows a process of asset and threat identification, threat analysis using the Microsoft STRIDE model,[18] to protect Open RAN from external and internal threats.

4.4 Open RAN Supply Chain Security Risks

While the introduction of Open RAN architecture provides an opportunity for new entrants to move their products from development to deployment, network providers will need to assess security risks associated with implementing a more diversified vendor environment and take appropriate actions. While not unique to Open RAN, potential security risks include, but are not limited to:[19]

- insertion of malicious features during design.
- alteration of system behavior through illicit access points that exist due to hardware design weaknesses or architectural flaws.
- extraction of sensitive or secret information through unintended communications (side) channels.
- stolen intellectual property through reverse engineering.
- counterfeit, including recycled, cloned or remarked components or systems represented as genuine.
- modification to insert hidden malicious functionality.

4.5 Issues facing the deployment of Open RAN equipment in the US

One basic paradigm of Open RAN is that a "more competitive and vibrant RAN supplier

[16] O-RAN Alliance, *O-RAN Specifications,* https://orandownloadsweb.azurewebsites.net/specifications (last visited October 31, 2022).

[17] O-RAN Alliance, *News and Events, Statements and Announcements, The O-RAN ALLIANCE Security Work Group Continues Defining O-RAN Security Solutions (October 23, 2022).*

[18] NIST Special Publication (SP) 800-207, Zero Trust Architecture, http://www.csrc.nist.gov/publications/detail/sp/800-207/final.

[19] 5G Hardware Supply Chain Security Through Physical Measurements, NIST Special Publication 1278 (https://doi.org/10.6028/NIST.SP.1278), May 2022.

ecosystem with faster innovation"[20] will improve the user experience. Operators may have differing views on deploying Open RAN. One uncertainty is if operators committing to Open RAN technology will need to expend greater efforts to test and integrate components at various layers of network functionality to ensure security and interoperability prior to deploying it in their production networks.

While a larger vendor marketplace may initially occur, operators may select and rely upon a smaller number of vendors in order to reduce the test and integration burden and subsequent risk. This may cause the supplier marketplace to shrink and lose some robustness, as the router vendor market consolidated in the first decade of this century.

The increased complexity of the Open RAN architecture and mix-vendor platforms and networks increase the difficulties of troubleshooting and problem isolation. Operators traditionally have kept the number of vendors high enough to encourage competition but low enough so that when there are problems with a particular platform, the operator can rely on that vendor's expertise to resolve the issue. The multi-vendor network introduces an increased complexity in troubleshooting network issues.

U.S. network operators have spent billions building out their RAN, so it may be several years down the path of integrating Open RAN with their legacy networks before significant cost savings may be realized. Existing networks will retain legacy 4G and possibly earlier technologies and operators must ensure that the new Open RAN technology integrates in a stable way to avoid compromising their subscribers and their service offerings.

The security posture of Open RAN has received much attention and is a key priority for the development of the technology. Furthermore, the vendor diversity inherent in Open RAN increases the resiliency of the mobile infrastructure supply chain. However, the disaggregated and virtualized architecture may increase the attack surface, so network operators will need to perform risk management to identify and mitigate the security risks as they currently do with their existing networks.

[20] O-RAN Alliance, *Who We Are, About Us*, https://www.o-ran.org/about (last visited October 31, 2022).

5 Analysis and Recommendations

The Enduring Security Framework (ESF) report on "Open RAN Security Considerations"[21] states:

> "The deployment of Open RAN introduces new security considerations for mobile network operators (MNO). By nature, an open ecosystem that involves a disaggregated multi-vendor environment requires specific focus on changes to the threat surface area at the interfaces between technologies integrated via the architecture. In addition to addressing security considerations related to integrating components from multiple vendors, service providers will continue to deal with other considerations related to use of open source applications and new 5G network functions and interfaces whose standards are still under development."

This section further analyzes these Open RAN attack vectors.

5.1 Analysis: O-RAN Architecture Security

As discussed in Section 4 above, 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[22] OFH interface, RICs, and RAN applications known as rApps and xApps. However, O-RAN's new network functions and interfaces potentially expand the O-RAN attack surface.[23]

With the development of Open RAN architecture as described in Section 4.3, it is important to identify and address potential new threats due to new functions as well as take the opportunity of better network visibility and AI/ML capabilities to make the RAN more secure. A strong Open RAN security posture must implement security controls at each layer to protect the network functions, interfaces, and data from external and internal threats, as shown in Figure 4. The O-RAN Alliance's WG11 has performed a detailed threat analysis of O-RAN[24] and continues to evolve O-RAN's security specifications to meet the security baseline expected by network operators and their users. The specification considers Zero Trust Architecture (ZTA) as

---

[21] NSA Enduring Security Framework (ESF) and CISA, Open Radio Access Networks Security Considerations, 2022, http://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf.

[22] O-RAN Architecture Description, v7.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022). visited on 17 November 2022).

[23] NSA Enduring Security Framework (ESF) and CISA, Open Radio Access Networks Security Considerations, 2022, http://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf Germany BSI, Open RAN Risk Analysis, (2021), https://www.bsi.bund.de/ DE/Service-Navi/Publikationen/Studien/Open-RAN/Open-RAN_node.html;jsessionid=7E6F065AA03CD6753849A31E226B8033.internet481; EC NIS Cooperation Group, Report on the Cybersecurity of Open RAN (2022), http://www.digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks.

[24] O-RAN Alliance, O-RAN Security Threat Modeling and Remediation Analysis, O-RAN.SFG, O-RAN-Threat-Model-v03.00, March 2022.

described in US NIST SP 800-207[25] as an important approach fostering protection from external and internal threats.

A security analysis of the O-RAN architecture is provided in subsequent sections. The analysis is aligned with the ongoing work items in the O-RAN Alliance's WG11 to drive enhanced security specifications.[26]

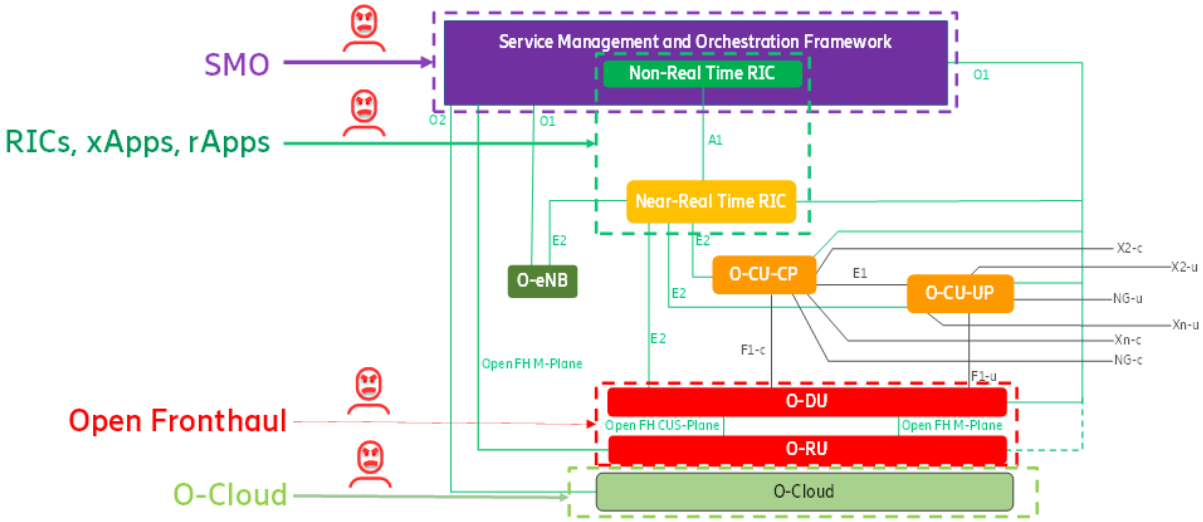

Figure 4. Threats to the O-RAN Architecture[27]

5.1.1 Securing Management and Orchestration

Current Service Management and Orchestration (SMO) functions in 5G networks rely on proprietary interfaces to provide management and orchestration to the RAN and are unique to each supplier. O-RAN introduces the SMO function to perform the 3GPP defined Network Manager functions with standardized interfaces for management and orchestration as shown in Figure 5 below. Securing the SMO and its associated interfaces is imperative because it is responsible for all service management and orchestration. A security vulnerability within the SMO could be exploited to serve as an entry point to other Open RAN components and lateral movement across Open RAN for attacks on RAN confidentiality, integrity, availability, and authenticity.

The SMO also accesses internal and external data stores through Application Programming

[25] NIST, SP 800-207, Zero Trust Architecture, (2020), http://www.csrc.nist.gov/publications/detail/sp/800-207/final

[26] O-RAN Alliance, *News and Events, Statements and Announcements, The O-RAN ALLIANCE Security Work Group Continues Defining O-RAN Security Solutions (October 23, 2022).*

[27] Adapted from O-RAN Architecture Description, v7.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

Interfaces (APIs) which must be securely implemented so that data at rest, in motion, and in use are protected. An external attacker could poison external data controlled by another third-party who has not implemented proper security controls. After the poisoned data is imported to the SMO via the External interfaces, as shown in Figure 6, the external attacker could exploit it to gain access to the O-RAN ecosystem to degrade performance or perform reconnaissance.

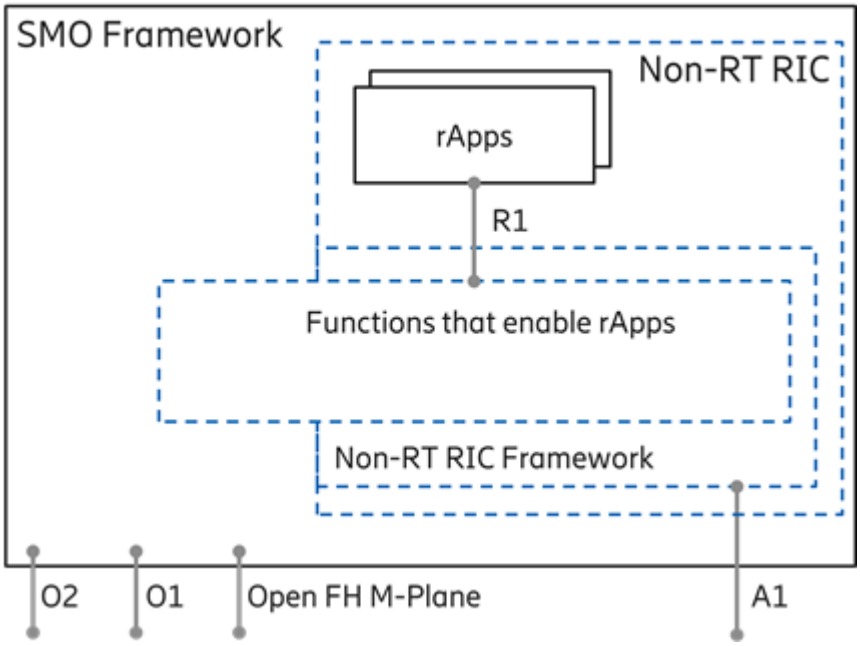

Figure 5. SMO Framework[28]

5.1.2 RAN Intelligent Controllers (RICs)

Applications known as rApps and xApps are intended to enhance RAN optimization, with the potential to extend to other RAN functions such as capacity planning, sustainability, and security. The security of rApps and xApps in Open RAN have the following characteristics

- rApps and xApps perform RAN optimization functions leveraging AI and ML. Security of AI/ML data and models is a recognized challenge across all industries that must also be addressed in Open RAN. rApps and xApps should be securely use AI/ML data sets and models.
- Each rApp can also interwork with other rApps by means of standardized R1 interfaces, as shown in Figure 5, in which the insights from one rApp serve as input to another to build a more complex automation function for more complex decisions. Secure peering between rApps must be provided with mutual authentication across the R1 interface, as

[28] O-RAN Architecture Description, v7.0, O-RAN Alliance, Specifications, https://orandownloadsweb.azurewebsites.net/specificationsorandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

shown in Figure 5. Confidentiality and integrity protection should be provided on the R1 interface to secure it against malicious rApps snooping, modifying, or injecting messages on the interface.

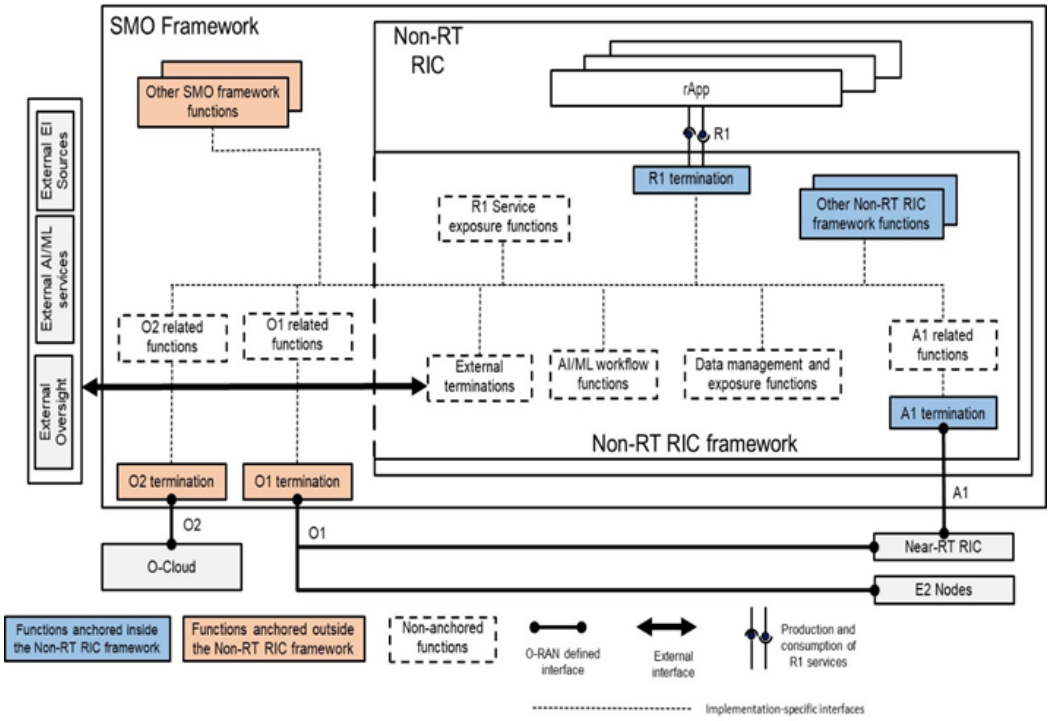

Figure 6. Non-RT RIC Framework[29]

- The risk of conflicting policies and parameter settings increases as the number of application vendors increases. Conflict mitigation is important in a multi-vendor environment in which multiple apps from different vendors could be, unintentionally or maliciously, forming and pushing conflicting RAN policies and parameter settings. Conflict mitigation prevents RAN performance degradation and outages, which are availability attacks.
- rApps used in conjunction with AI/ML can leverage internal and external data sources. Integration with these data sources is provided using open APIs, which must be interoperable and secure. Access to the data must be protected with strong authentication and multi-factor authorization. Data confidentiality, integrity, and availability should also be supported.

The A1 interface enables the Non-RT RIC to provide policy-based guidance, ML model management, and enrichment information to the Near-RT RIC. Secure peering on the A1 interface must be provided with mutual authentication. Confidentiality and integrity protection must be provided on the A1 interface to protect against a malicious actor snooping, modifying,

[29] O-RAN Non-RT RIC Architecture, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

or injecting messages on the interface. A motivation for rApps and xApps is to provide greater vendor diversity in which smaller, best of breed vendors can contribute third-party applications to the Open RAN ecosystem, potentially enabling an application marketplace for RAN applications. This direction can introduce supply chain security risks which must be mitigated to enable a trustworthy ecosystem of rApps and xApps vendors.

The following guidelines should be followed by industry to establish a trusted supply chain for secure rApps and xApps:

- Produce guidelines for secure application software development based on the NIST SSDF.[30]
- Utilize a third-party vulnerability assessment (VA) entity to ensure rApps/xApps do not have known vulnerabilities reported in the National Vulnerability Database (NVD).
- Delivery of rApps/xApps should include Software Bill of Materials (SBOM), aligned with the emerging United States Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) guidelines[31] and O-RAN Alliance specifications.[32]
- Provide digital signatures with each application software package to ensure software integrity and verifiability.
- Establish a standard for secure on-boarding of rApps and xApps.
- Additional considerations should be made for the implementation of a secure RAN application marketplace that enables innovators to contribute trustworthy applications.

5.1.3 Open Fronthaul Interface

The O-RAN Open FH M-Plane specification[33] enables O-RU controllers to manage the operation of the O-RU. It specifies the use of the NETCONF protocol together with a set of associated YANG models to enable an O-RU controller to configure the O-RU and recover operational data from the O-RU. The specifications require that NETCONF is securely transported over SSHv2 or TLS1.2 or higher. M-Plane authentication can be based on usernames and passwords or simple public key certificates or PKIX (Public Key Infrastructure with X.509 Certificates) when SSHv2 is used, or PKI X.509 certificates when TLS is used.

The M-Plane provides end to end security as a mandatory feature. M-Plane security shall support NETCONF/SSHv2 and NETCONF/TLS 1.2. TLS 1.3 may also be optionally supported in addition to TLS 1.2. The OFH M-Plane specification also requires mandatory support of SFTP over SSH and FTPES over TLS for secure file transfer. The CISA list of security bad

[30] NIST SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (2022), https://csrc.nist.gov/publications/detail/sp/800-218/final.

[31] CISA, Software Bill of Materials (SBOM), https://www.cisa.gov/sbom (last visited November 9, 2022).

[32] O-RAN Security Requirements Specification, v4.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

[33] O-RAN Open Fronthaul Management Plane Specification, v7.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

practices[34] including single-factor authentication and known/fixed/default passwords should be avoided in US production networks. OFH M-Plane allows operators to optionally configure an IEEE 802.1X PAE-Supplicant.[35]

Whether using SSHv2 or TLS, the authenticated username is used with NETCONF access control model (NACM) which defines role-based authorization of access to specific YANG models, YANG defined schema nodes, remote procedure calls and notifications with authorization policies are defined for SMO and O-DU roles.

Protocol	Certificate lifecycle management	PKIX (Public Key Infrastructure with X.509 Certificates)	Simple Public Key	Password-based Authentication
TLS 1.2	Mandatory to support CMPv2, optional to support vendor certificate lifecycle management	Mandatory to support / Optional to use	Not specified in RFCs 5246/8446	Not specified for use with NETCONF
SSHv2	Optional to support CMPv2, optional to support vendor certificate lifecycle management	Optional to support/Optional to use	Used for SSH Server authentication by SSH client. Mandatory to support / Optional to use	Used for SSH Client authentication by SSH server. Mandatory to support / Optional to use

Table 5. M-Plane Authentication – Optional and Mandatory Requirements[36]

As shown in Figure 3 above, the OFH allows the use of either a hierarchical deployment mode (where O-DU manages the O-RU) or a hybrid deployment mode (where O-DU and SMO together manage the O-RU). When OFH is deployed in hierarchical configuration, the fronthaul traffic can be fully isolated within the O-RU to O-DU interface using segmentation. Such segmentation, also commonly used in traditional 3GPP-based fronthaul, offers a primary security mechanism to isolate assets, reduce attack surfaces and simplify access control. In such a deployment, any attack launched from the fronthaul interface is protected by the access controls implemented by the O-DU.

When deployed in hybrid configuration, M-Plane traffic can reach additional centralized management systems, for which additional security measures may be warranted. In such scenarios, 802.1x NAC can be employed to authenticate the O-RU. Packet switched transport systems can also implement access control to filter traffic between O-RUs and centralized management systems to permit only the secured NETCONF signaling defined by the Open FH M Plane.

---

[34] Cybersecurity and Infrastructure Security Agency, Bad Practices, https://www.cisa.gov/BadPractices (last visited 31 October 2022).

[35] IEEE 802.1X-2020, IEEE Standard for Local and Metropolitan Area Networks, Port-Based Network Access Control, https://standards.ieee.org/ieee/802.1X/7345/ (last visited 17 November 2022).

[36] O-RAN Management Plane Specification, v10.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

For edge elements, securing point-to-point (P2P) LAN segments and implementing secure data packet designs become key to securing the OFH Interface. The M-Plane specifies optional support and use of IEEE 802.1X port-based access control in the O-RU.[37] When configured, only those network elements acting as an IEEE 802.1X supplicant and that have mutually authenticated with an IEEE 802.1X authenticator may be authorized to participate in the Open FH network.

The O-RAN OFH provides O-RAN specified CUS-Plane and M-Plane, running over the evolved Common Public Radio Interface (eCPRI)[38] or optionally over IEEE 1914.3 (RoE),[39] is also at risk of exploits. O-RAN and many existing 3GPP-based 5G deployments use eCPRI for the fronthaul between the DU and RU. 3GPP-based RAN deployments may have proprietary implementations for control and user plane, but typically use standardized protocols running over eCPRI. The O-RAN OFH specifies the CUS-Plane running over eCPRI (or optionally over IEEE 1914.3 RoE) and the M-Plane, providing an opportunity for the O-RAN Alliance to address those threats as identified[40] and discussed further below.

Lack of encryption of control messages on the C-Plane allows modification, injection, and replay attacks that can be used to degrade RAN performance or cause an outage. However, the CUS-Plane is sensitive to latency, which could inhibit or limit use of encryption. If front-door encryption is insufficient or lacking, the opportunity exists for external attacks and subsequent network degradation.

For the S-plane, attacks that are possible by an external threat are the most important ones to address. A lack of authentication on the S-plane enables an attacker to take over the role of Grand Master Clock, which can be used to exploit synchronization causing degradation in U-plane performance. An external RF-cyber-attack could affect the downstream Ethernet-based Precision Time Protocols (PTP), Master Clock, Transparent Clock, and Boundary Clock, among other synchronization and timing elements. As of the March 2022 train of O-RAN specifications,[41] specific authentication and authorization mechanism of S-plane PTP messages are not required. Authentication per IEEE 802.1X[42] is a possible solution. Threats and associated risk analysis of OFH and its planes can be found in the O-RAN Threat Modeling and

[37] O-RAN Management Plane Specification, v10.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

[38] O-RAN Specifications, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022); CPRI Forum, *Specifications*, http://www.cpri.info/spec.html (last visited October 24, 2022)

[39] Institute of Electrical and Electronics Engineers, IEEE 1914.3-2018, Standard for Radio over Ethernet Encapsulations and Mappings, https://standards.ieee.org/ieee/1914.3/6785/ (last visited October 24, 2022).

[40] O-RAN Alliance, O-RAN Security Threat Modeling and Remediation Analysis, O-RAN.SFG, O-RAN-Threat-Model-v03.00, March 2022.

[41] O-RAN Specifications, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

[42] IEEE 802.1X-2020, IEEE Standard for Local and Metropolitan Area Networks, Port-Based Network Access Control, https://standards.ieee.org/ieee/802.1X/7345/ (last visited 17 November 2022).

Remediation Analysis Specification.[43]

Although protection is provided via IEEE 1588[44] PTP Integrated Security mechanisms, this approach has inherent limitations. For instance, no normative Key Management mechanism is defined in IEEE 1588, so this needs to be addressed by the O-RAN Alliance. This includes assuring sufficient redundancy to eliminate single points of failure and to compensate for byzantine failures. Additionally, implementing IEEE 1588 PTP Integrated Security would require support for crypto operations just before the packets are put on the physical wire. This effectively rules out the use of 1-step PTP clocks in the Open Fronthaul network.

5.1.3.1.1 S-plane Guidelines

The following guidelines should be applied to S-Plane specifications to mitigate S-Plane specific vulnerabilities from external RF-cyber-attacks:

- Implement security hardening of O-DU, O-RU, and intermediary network elements.
- PTP nodes connecting to the Open Fronthaul network should be appropriately hardened following industry best security practices. This includes securing data (credentials) at rest and disabling all ports and services that are not used, using industry-standard security protocols.
- Industry-standard Identity and Access Management (IAM) control mechanisms should be put in place to ensure that only authenticated and authorized users can access the network element or critical parts of the network.
- Physically secure the Open FH transmission network to deter/minimize external attackers from becoming a Man-in-the-Middle (MiTM) and launching packet delay attacks. PHY layer security protocols (RF intrusion detection) should be incorporated at the Open FH Interface.

5.1.4 O-Cloud

While cloud security risks are not exclusive to Open RAN, such networks may be considered critical infrastructure. The Open RAN architecture includes specifications for the O-Cloud on top of which the Open RAN network functions and applications run. The O-Cloud software and interface must be hardened to prevent attacks against the cloud infrastructure that could impact confidentiality, integrity, availability, and authenticity of the Open RAN deployment. The O-

[43] O-RAN Security Threat Modeling Remediation Analysis, v4.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

[44] Institute of Electrical and Electronics Engineers, IEEE 1588-2019, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems, https://standards.ieee.org/ieee/1588/6825/ (last visited 17 November 2022).

Cloud is managed and orchestrated by the SMO using the O2 interface, which must be secure to prevent threat actors from attacking the O-Cloud infrastructure via the SMO or the SMO via the O-Cloud infrastructure. Open RAN deployments should follow industry best security practices, including secure hardware using Hardware Security Module (HSM) to establish a hardware root of trust.

CISA states "Cloud providers and MNOs share security responsibilities requiring operators to take responsibility to secure their tenancy in the cloud."[45] The cloud service provider is accountable for the security posture of the deployment. As security service offerings differ amongst cloud service providers, MNOs must perform due diligence to ensure their deployments meet security requirements. While security responsibilities can be delegated by the operator to the cloud service provider via the Cloud Agreement, the MNO retains accountability. This delegation of responsibilities in a hybrid cloud deployment must clearly define roles and responsibilities for all stakeholders.

5.1.5 O-RAN Coexistence Orchestration to Mitigate Security Vulnerabilities in Multi-RAT Environments

Heterogeneous Radio Access Technology (RAT) networks require secure RAN orchestration such that the latest O-RAN-based 5G standalone deployment can securely coexist with other types of 5G and legacy systems, referred to as multi-RAT. An O-RAN-based 5G network deployment by itself can exhibit almost ideal performance but placed in the presence of other RAT networks or devices, chaotic and unsecure performance can emerge. Multi-RAT challenges overall network security by introducing threat variables to assure optimal O-RAN orchestration performance for secure coexistence in the presence of multiple threat variables and attack surfaces.

Multi-RAT increases exposure of the network's attack surface to malicious actors. Since Open RAN decouples the software from the hardware and moves orchestration to a cloud-native environment, orchestration can become automated and easily untrusted. Additionally, the RATs are vendor agnostic, creating an unknown attack surface between multi-vendor solutions.

Many organizations have developed their own unique implementations of RAN and RATs. The Department of Defense (DoD) is also a RAN developer engaged in research and development in Open RAN through DARPA's Open, Programmable, Secure 5G (OPS-5G)[46] program. These ongoing efforts expose security and coexistence vulnerability barriers that prohibit innovation and delay the adoption of Open RAN technologies. The following lists the key challenges, from a RAN and multi-RAT perspective to coexistence and O-RAN-based 5G security:

- Open RAN software is in a developmental state of flux and implementations are still evolving and in certain cases not stabilized.

[45] Cybersecurity and Infrastructure Security Agency (CISA), *Media, CISA News Room, NSA and CISA Provide Cybersecurity Guidance for 5G Cloud Infrastructure* (October 28, 2021), https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures.

[46] US Gov Ops, *Explore Ops-5G*, https:usgovops.org/ops5g (last visited 17 November 2022).

- Open RAN developers need special RAN knowledge to use complex code bases.
- Most Open RANs have limited documentation, making them difficult to build and install.
- Many Open RANs require specific proprietary implementations, making them difficult to obtain, especially if incorporating the over-the-air device or RU.
- There is currently no standards organization which is addressing multi-RAT co-existence.
- Implement orchestration consistent with SMO

5.1.6 Broader Security Considerations for Open RAN

The following sections considers some broader security topics that are applicable to but not exclusive to Open RAN technologies

5.1.6.1 Trust

5.1.6.1.1 Zero Trust Architecture

The increased risk from cyberattacks has advanced interest in ZTA for 5G cloud-based deployments. The principles of a ZTA for 5G cloud deployments are based on perimeter-less security in which each asset implements security controls. In October of 2021, CISA released its "Security Guidance for 5G Cloud Infrastructures"[47] based on the work of the ESF's 5G Cloud Working Panel. This is the first publication from a government agency around the globe that provides guidance for a security posture that specifically connects 5G, Cloud, and ZTA. The CISA work builds upon NIST Zero Trust Architecture,[48] which defines a ZTA to have no implicit trust granted to an asset based upon ownership, physical location, or network location.

As RAN functions become virtualized and migrate to the cloud, each function must be an independently secured asset that does not rely upon perimeter protection. 5G cloud deployments may reside in a third-party's facility, such as with Multi-access Edge Compute (MEC), a 3rd-party may be managing infrastructure, and the software platform has components from other 3rd-parties with potential vulnerabilities. This requires a zero trust mindset for 5G cloud deployments. A ZTA includes the following list of security controls, also shown in Figure 7:

- Continuous monitoring and logging.
- Threat Detection and Response.
- Data encryption and integrity checking for data-at-rest, data-in-motion, and data-in-use.
- Micro-segmentation and isolation, including tenant isolation and container isolation.
- Strong authentication protocols like TLS 1.2 or 1.3 or SSHv2 for users on network

[47] Cybersecurity and Infrastructure Security Agency (CISA), *Media, CISA News Room, NSA and CISA Provide Cybersecurity Guidance for 5G Cloud Infrastructure* (October 28, 2021), https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures.

[48] NIST, SP 800-207, Zero Trust Architecture, (2020), http://www.csrc.nist.gov/publications/detail/sp/800-207/final

interfaces.

- Avoid list of security bad practices.[49]
- Multi-Factor Authentication for users accessing functions and data.
- Role Based Access Control, Task Based Authorization Controls, or Policy Based Access Controls for users and systems attempting to access data.
- Supply chain security in which vendors and upstream suppliers implement a secure software development lifecycle, DevSecOps and CI/CD.
- A chain of trust based upon a hardware root of trust using HSM.
- Plus, perimeter security, which has successfully protected networks and should continue as a component of a ZTA.

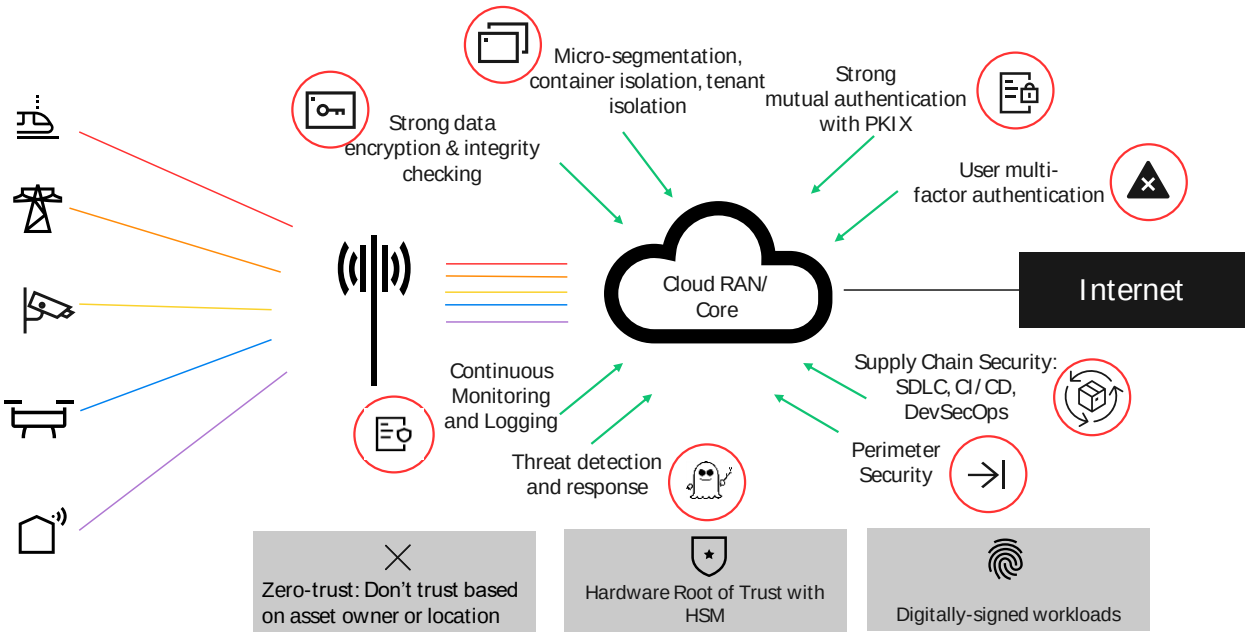

Figure 7. Zero Trust Architecture for 5G Cloud Deployments [source: Ericsson][50]

5.1.6.1.2 Trustworthiness within Open RAN ecosystem

It is important to secure the RAN for new emerging 5G use cases with Internet of Things (IoT) devices such as smart cities, smart power grids, autonomous vehicles, and smart buildings. Open RAN shares the same security vulnerabilities of IT systems using Commercial Off-the-

[49] Cybersecurity and Infrastructure Security Agency, Bad Practices, https://www.cisa.gov/BadPractices (last visited 31 October 2022).

[50] Ericsson, Ericsson Blog, Evolving 5G Security for the Cloud, (January 14, 2022), https://www.ericsson.com/en/blog/6/2022/evolving-5g-security-for-the-cloud.

Shelf (COTS) hardware, open-source software and use of international hardware and software components. These vulnerabilities are well studied and addressed through standardized remediation processes to prevent compromise to confidentiality, integrity and availability.

Active security monitoring will be required for any unexpected activity internal or external to the Open RAN system that could be harmful including denial of service, jamming, Adversarial Machine Learning (AML), and spoofing.

Common industry best practices should be followed to establish a trusted Open RAN deployment, including:

- All software components should follow a security by design process and undergo extensive testing including white box, black box and sandbox testing.
- All software components should be digitally signed using secure hash algorithms.
- Hardware and software platforms should verify the digital signatures of the software before loading and running them, as applicable.
- Establish a chain of trust built upon a hardware or firmware root of trust.
- Mechanisms should be in place to isolate and disable hardware and software components in case unwanted behavior is identified. This can be done via several techniques, for example, X.509 certificate revocation.

5.1.6.1.3 AI/ML Security and Adversarial Machine Learning

ML-based systems may suffer from a special type of logical vulnerabilities that stem from the inherent properties of the machine learning algorithms. For instance, an adversary can utilize AML, where ML models are susceptible to adversarial samples that appear as normal samples but have some imperceptible noise added to them with the intention of spoofing a trained classifier and misclassifying the input. This mechanism potentially allows an adversary to exploit the ML in a way to gain control of the network and exfiltrate information/data to degrade network performance or to gain control of the network for other malicious purposes. It is therefore necessary to consider ways of detecting and blocking adversaries in real time that could exploit ML-based vulnerabilities to their advantage.

One methodology involves the application of proven cyber-behavioral analysis models that can be used to detect and monitor possible exploits in real time and employ techniques to ensure data-to-decisions rulesets are nonmodifiable or nonfungible (i.e., cannot be retrained or reset) by external actors.

AI/ML technologies have attracted a lot of attention recently in 3GPP, O-RAN Alliance, other standards bodies, and industry associations.

3GPP has several completed and ongoing AI/ML initiatives spanning across various working groups and releases in the Core as well as RAN domains. A non-exhaustive list of these efforts follows. AI/ML related efforts in 3GPP Rel-16 include study of enablers for Network Automation for 5G,[51] architecture enhancements for 5G System (5GS) to support network data

[51] 3GPP TR 23.791, http://www.3gpp.org (last visited October 24, 2022).

analytics services in 5G Core network,[52] Network Data Analytics Function (NWDAF) services of the 5GS[53], Management Data Analytics (MDA),[54] and open & closed loop service assurance using MDA + NWDAF.[55] 3GPP Release 17 includes AI/ML management capabilities for 5GS[56] and a study on RAN intelligence enabled by AI/ML.[57] AI/ML related efforts in 3GPP Release 18 include study on traffic characteristics and performance requirements for AI/ML model transfer.[58]

The O-RAN architecture is an open, adaptive, and intelligent RAN architecture designed to drive operational efficiencies. Motivated by the success of AI in other domains, O-RAN strives to leverage ML to automatically and efficiently manage network resources for traffic steering, quality of experience prediction, and anomaly detection. O-RAN Alliance specifications provide a framework to use AI/ML to optimize radio resources in networks with the purpose to improve performance and automate operations through intelligent algorithms that improve the system continuously. This will be done through applications hosted on the RIC platforms. AI/ML-enabled closed-loop automation will help in reducing operating expenditures through advanced and adaptive self-managing capabilities accelerated time-to-value and reduced risk of human errors. Some of the intended usage applications of AI/ML are:

- Parameters tuning to optimize radio network performance.
- Identify and resolve the network issues also known as self-healing.
- Network performance data collection and analytics.

The planned AI/ML model will employ combination of supervised, unsupervised and reinforced learning. Some models are expected to interact within the platform through rApps/xApps within the RICs or over open interfaces such as A1 and E2.

Wireless and mobile networks benefit from the application of ML to detect network element and traffic anomalies. However, ML detectors themselves can be exfiltrated/evaded by the samples carefully designed by attackers, raising security concerns for ML-based network applications. Thus, it is crucial to detect such samples to safeguard the network. New AML approaches in the generation and detection of adversarial samples is required to minimize the impact.

The AML threat can originate from O-RAN application software developer, virtualization software provider, hardware infrastructure supplier or the user equipment. The attacker can potentially tamper with the network thus compromising integrity, cause availability issues with

---

[52] 3GPP TS 23.288, http://www.3gpp.org (last visited October 24, 2022).

[53] 3GPP TS 29.520, http://www.3gpp.org (last visited October 24, 2022).

[54] 3GPP TR 28.809, http://www.3gpp.org (last visited October 24, 2022).

[55] 3GPP TS 28.535, http://www.3gpp.org (last visited October 24, 2022); 3GPP TS 23.536, http://www.3gpp.org (last visited October 24, 2022).

[56] 3GPP TS 28.105, http://www.3gpp.org (last visited October 24, 2022).

[57] 3GPP TR 37.817, http://www.3gpp.org (last visited October 24, 2022).

[58] 3GPP TR 37.817, http://www.3gpp.org (last visited October 24, 2022).

denial of service or disclose or have access to private data/models in use.

Open RAN architecture should implement defenses to prevent AML attacks. For example, robust statistical analysis can be used to mitigate the influence of outliers and can reject the corrupt samples to defend against corruption.

5.1.6.1.4 Application Programming Interfaces /Protocol Security

APIs are general cloud technology re-used in O-RAN. An example is the IETF's REST API, used for web services in the cloud. While some O-RAN interfaces use REST, the known security risks with REST and other APIs could impact Open RAN deployments. Additional due diligence is recommended to ensure that APIs are securely implemented and configured.

5.1.6.1.5 Real-time security control of the RAN

In the real-time or operational context, dedicated monitoring functions should be used for the verification of operational and data security of the distributed Open RAN components. Continuous monitoring strategy and security architecture for an Open RAN system will identify the security controls that will be monitored and the monitoring frequency, and how changes to the system are monitored and risk assessments are conducted. This may require implementing security log generation and collection to an external security information and event management system. The real time monitoring of Open RAN systems should log access attempts to resources and data and the specific conditions resulting in permit or deny. All access requests should be continuously monitored and validated against the defined access context. Context is the foundation for the zero trust model. Context enables the right user, under the right conditions, to have the right access, to the right data to ensure the principle of least privilege is enforced. Security controls should not delay access grant to the right resources and may continuously analyze and improve verification for faster connection in the future.

Fast response should be provided when an anomaly is detected. Actions can include revoking access, quarantining users, creating compliance reports or an event. Security control enforcement may continuously evaluate and adjust policies, authorization actions and remediation tactics. The perimeter around each resource may be tightened to drive faster, more informed decisions, adjust context to support trustworthiness, constantly improve overall security and compliance, as well as reduce risk.

Security controls may use advanced analytics to adjust verification and remediation, adjust network segments to tighten the perimeter, adjust IAM and data security policies to determine trustworthiness, constantly improve overall security and compliance, as well as reduce risk.

Configuration controls and management are important for ensuring the operational integrity of the Open RAN system, including verifying that components from different sources/suppliers are running compatible software versions. Compatibility is an important consideration for deployment and change management.

5.1.6.2 Preparing for the Quantum Computer Threat

Present-day Cryptography, referred to here as Classical Cryptography, provides the underlying foundation on which the security of the data and communications in our digital worlds is built. Mobile telecommunication networks and devices, including those based on 3GPP and Open

RAN architectures, depend heavily on Classical Cryptography to protect the privacy, confidentiality and integrity of their users and data.

Classical Cryptography can be rendered unsecure if a large-scale Quantum Computer becomes available. The Classical Cryptography mathematical algorithms which are difficult to solve using today's digital computers could be quickly solved using a Quantum Computer which efficiently leverage quantum algorithms, such as Shor's or Grover's algorithms.[59]

Existing Quantum Computers[60] have limited capacity and not considered powerful or stable enough to threaten Classical Cryptography. A large-scale Quantum Computer may be realized in the next 20 years, the 2030~2040 timeframe.[61]

Classical Cryptography includes both Symmetric and Asymmetric Cryptography, the latter commonly referred to as Public Key Cryptography (PKC). PKC is considered to be more vulnerable to Quantum Computers. Symmetric Cryptography, while also vulnerable, may mitigate the threat by increasing the size of the cryptographic keys.

To address this impending threat to PKC, NIST has undertaken a Post-Quantum Cryptography (PQC) project[62] to study, evaluate and standardize by 2024 PKC algorithms which are resistant to threats from both Classical and Quantum Computers. These algorithms are referred to as PQC, Quantum Safe or Quantum Resistant algorithms. In 2022 NIST announced the first four PQC algorithms to be standardized as part of the PQC project.[63]

Assets secured with Classical Cryptography, such as encrypted data or communication sessions, which must remain secure many years or decades into the future may potentially be at risk from a Quantum Computer. Assets secured with Classical Cryptography may be eavesdropped and stored by an adversary today and decrypted later when a large Quantum Computer becomes available – referred to as the "Harvest Now, Decrypt Later" problem.

A paper by Michele Mosca[64] provides guidance on one approach to assess readiness for the Quantum Compute threat. It states that if Y is the amount of time required to migrate to PQC, noting that everything secured up to the end of Y relies on Classical Cryptography, and X is the time data must remain secure for, and Z is when a large Quantum Computer becomes available, then if X+Y is greater than Z there is a problem.

---

[59] NIST Report on Post-Quantum Cryptography: https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf.

[60] IBM Quantum Roadmap: https://www.ibm.com/quantum/roadmap.

[61] Quantum Threat Timeline Report 2020: https://globalriskinstitute.org/publications/quantum-threat-timeline-report-2020/.

[62] https://csrc.nist.gov/projects/post-quantum-cryptography; https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization; https://csrc.nist.gov/Projects/post-quantum-cryptography/workshops-and-timeline.

[63] https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

[64] Cybersecurity in an era with quantum computers: will we be ready? https://eprint.iacr.org/2015/1075.pdf.

The journey towards the adoption of NIST PQC algorithms is expected to be challenging and take many years, even decades, to achieve given the pervasive deployment and usage of PKC that has occurred globally over the past decades. The US White House has stated "the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography, with the goal of mitigating as much of the quantum risk as is feasible by 2035."[65]

Many challenges need to be overcome, some of which will include for example:

- Discovery of where Quantum Computer vulnerable Classical Cryptographic technologies are currently or will be used i.e., in which architectures (e.g., 3GPP, O-RAN), which products, solutions and deployments (e.g., network/cloud nodes, ender use devices).
- Enabling co-existence and interoperability of both Classical and Post-Quantum Cryptographic technologies as well as the capability to replace algorithms, referred to as Crypto-Agility, in case one becomes compromised or needs to be upgraded or fallback to a previous version.
- Ensuring security protocols, such as TLS & IPsec/IKE to mention a few, are evaluated to support PQC algorithm parameters such as larger keys, ciphertext and signature sizes as well as mechanisms to negotiate usage of Classical and/or PQC algorithms.
- Understanding the Performance of PQC algorithms e.g., processor and memory utilization and so on.
- Addressing resource constrained end-devices such as Internet of Things (IoT) devices that may not have sufficient compute/memory resources to run PQC algorithms.

Extensive research highlights the importance and suggested steps to be taken to prepare for the adoption of and migration to Post-Quantum Cryptography, the following being some references[66] worth exploring.

5.1.6.3 Border Gateway Protocol (BGP)

O-RAN Alliance WG9 defines the packet switched transport architectures for supporting front-, mid- and back-haul interfaces. The O-RAN Xhaul Packet Switched Architectures and Solutions

[65] National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems: https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/.

[66] NIST white paper: Getting Ready for Post-Quantum Cryptography https://csrc.nist.gov/publications/detail/white-paper/2021/04/28/getting-ready-for-post-quantum-cryptography/final; NIST National Cybersecurity Center of Excellence; Migration to Post-Quantum Cryptography project https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms

Specification[67] use the BGP internet routing protocol.[68] The security of BGP could impact Open RAN deployments in cloud environments, particularly hybrid cloud deployments, for which due diligence should be performed to establish BGP security [69].

5.1.6.4 Considerations for Secure Cloud Deployments

5G is the first generation of mobile technology designed for cloud deployments. The cloud offers many security advantages, while also introducing new security risks as it expands the 5G attack surface and enables internal lateral movement. These considerations are important when performing a risk analysis to ensure Open RAN deployments in the cloud are secure.

Hybrid cloud deployments, such as Multi-Access Edge Compute (MEC), introduce additional security risks due to having multiple stakeholders, evoking the need to clearly define security role and responsibilities. The primary stakeholders are the Cloud Consumer, which for 5G deployments is the MNO, and the Cloud Service Provider (CSP).

As advised by CISA, "Cloud providers and MNOs share security responsibilities requiring operators to take responsibility to secure their tenancy in the cloud,"[70] assigning accountability to the MNO. The MNO is accountable for the security posture of the deployment and may delegate responsibility as indicated in the Cloud Shared Responsibility model, as shown in the example Figure 9. The delegation of security controls varies with the type of cloud service, either Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS), as defined by NIST.[71] The MNO is always responsible for data protection and user accounts with privilege levels.

CSPs have varying, disparate security offerings and levels of security posture. In some cases, a required security control may be available from the CSP only when purchased and included in the cloud agreement. It is important for the operator to perform due diligence when selecting a CSP to ensure that the CSP's security posture aligns with the MNO's. This is an additional

---

[67] O-RAN Alliance, O-RAN XHaul Packet Switched Architectures and Solutions, v3.0, O-RAN WG9, XPSAAS-v03.00, Specifications, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

[68] Internet Engineering Task Force (IETF), A Border Gateway Protocol, (January 2006), https:///www.rfc-editor.org/info/rfc4271; *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, NIST SP 800-189 (2019) https://csrc.nist.gov/publications/detail/sp/800-189/final; CSRIC III Report on BGP Security Best Practices(March 2013); CSRIC III Report on Secure BGP Deployment (March, 2013)

[69] *MANRs for Network Operators*, Internet Society, https://www.manrs.org/netops/; *Briefing on Routing Security*, ICANN Security and Stability Advisory Committee (9 June 2022), https://www.icann.org/en/system/files/files/sac-121-en.pdf; *Routing Security: BGP Incidents, Mitigation Techniques and Policy Actions*, OECD Digital Economy Papers, Oct. 12, 2022, https://www.oecd.org/publications/routing-security-40be69c8-en.htm; *Security of the Internet's Routing Infrastructure*, Broadband Internet Technology Advisory Group, 2022, https://www.bitag.org/Routing_Security.php

[70] Cybersecurity and Infrastructure Security Agency (CISA), *Media, CISA News Room, NSA and CISA Provide Cybersecurity Guidance for 5G Cloud Infrastructure* (October 28, 2021), https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures.

[71] NIST SP 800-145, The NIST Definition of Cloud Computing (2011), https://csrc.nist.gov/publications/detail/sp/800-145/final.

challenge in a multi-cloud deployment there are two or more CSPs that may have varying service offerings and security postures. In most cases, a security offering from the CSP requires that the Cloud Consumer, in this case the MNO, is responsible for security configuration and validation, leaving the MNO accountable for any security misconfiguration.

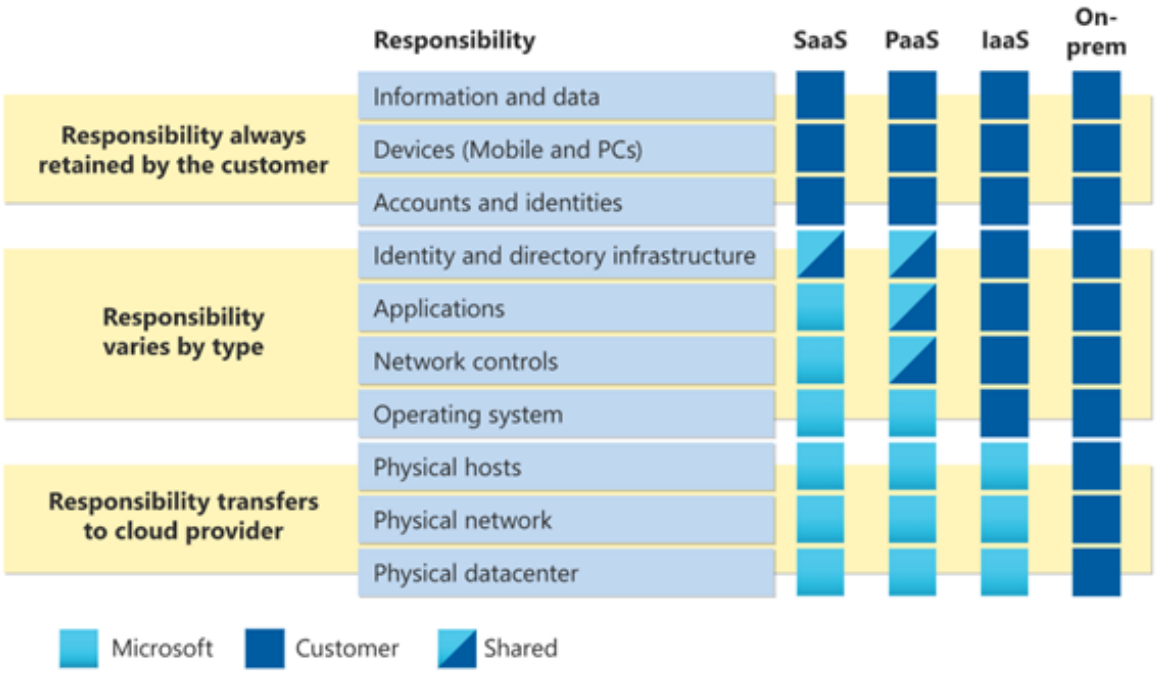

Figure 9: Cloud Shared Responsibility Model [source: Microsoft Azure][72]

5.1.6.5 Establishing Chain of Trust

Zero trust can only be achieved with the full participation of all the elements in a network's trust chain. Trusted hardware is built with a tamper resistant Hardware Root of Trust (HRoT) device. The root of trust can be implemented as an HSM storing encryption keys and credentials or as a multifunctional standard implementation of Trusted Platform Module (TPM). TPMs support broad functionality, from secure or trusted boot to attestation. The HRoT device exposes a simple user interface for the application to use when storing keys and retrieving certificates.

5.1.6.6 Uniform security profile in a heterogeneous vendor environment

Assuring a uniform security profile in a heterogeneous vendor environment requires traceability to validate root of trust and pedigree of processes, services, software applications, and data when integrating network functions and applications distributed throughout the O-RAN architecture. Multiple vendors in an approved supply chain should adhere to standards, requirements, and best practices that can be used to independently validate and verify security protocols and integration

[72] Microsoft, *Learn*, *Azure*, *Security*, *Fundamentals*, Shared responsibility in the cloud, https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility (last visited 19 November 2022).

schemes. This ensures secure operation throughout the O-RAN architecture and 5G network interoperability between all O-RAN service providers.

A uniform, maintainable "security profile" in a heterogeneous multi-vendor environment requires hardware end-item and integration standards that are traceable and verifiable. Multi-vendor traceability and accountability processes should be employed to verify the processes, services, applications, data or supplier end-item and associated quality and integrity checks to understand the source/origin of all hardware throughout their useful life cycle. In the absence of fault tolerance or failover, a traceback process should be implemented to ensure that multi-vendor artifacts are properly integrated to meet the basic security and technical performance requirements addressing[73]:

- redundancy.
- failover to validated secure systems and vendor end-items.
- verified priority services and network management protocols designed to fill any security gaps or shortfalls.

A possible method of assuring pedigree and traceability is to begin with an efficient deployment management scheme for 5G/O-RAN network system deployments using a common database for storing multi-vendor security configuration information[74]. The database system can be used for end-item or service life-cycle authentication, authorization, and accounting. This would include tracking which port-based network access control is used in combination with dynamic host configuration protocol mechanisms such as in IP address allocation. 5G wireless and Ethernet-based access technologies can be handled uniformly to identify where and when an end-item or service was implemented and what requirements and standards were met prior to or during the integration cycle. An advantage of this approach is use of standardized mechanisms in the fixed or mobile node and access networks[75].

5.1.6.7 Interoperability and Failover between O-RAN service providers for Priority Services and Emergency Communications

As 4G/5G infrastructure service providers migrate to fully virtualized, closed loop automation control, service providers will have one network able to serve a multiple consumer, enterprise, public safety, and priority communications use cases. Software Defined Networking (SDN), Network Function Virtualization (NFV), cloud computing, network slicing, and orchestration will allow service providers to dynamically provide these various use cases end to end across the 5G architecture. These use cases and services will most likely take the form of logical network slices that will traverse the core, transport, and RAN segments of the 5G architecture while

[73] Sritapan, V., Talbot, B., and Massey, D. (May 2022). "5G security evaluation process investigation, Version 1," White Paper prepared by Cybersecurity and Infrastructure Security Agency (CISA).

[74] ATIS Standard:5G Network Assured Supply Chain, ATIS-I-0000090, June 2022.

[75] Valero, J, Sánchez, P., Lekidis, A, Hidalgo, J., Pérez, M., Siddiqui, M., Celdrán A, and & Pérez, G. (2022). "Design of a security and trust framework for 5G multi-domain scenarios," *Journal of Network and Systems Management*, volume 30, article number 7.

maintaining pre-defined attributes to meet quality of service (QoS), priority, and security Key Performance Indicators (KPIs) based on the user and service type. As more of the physical infrastructure is virtualized and cloud computing becomes more prevalent, including at the edge of the network, these network slices will traverse various aggregation layers in the transport network, Backhaul (BH), Midhaul (MH), and Fronthaul (FH).

Open RAN will provide many deployment advantages to 5G infrastructure service providers including ability to mix and match RAN vendors for best price and performance, and open interfaces for more applications and services. However, this vendor diversity in the RAN places a heavier burden on the service provider and their cloud partners by introducing a more complex ecosystem to integrate and orchestrate; to implement network slicing and automation; to provide multi-vendor and inter-service provider interoperability; and to improve reliability. MNOs may be challenged to maintain a uniform security profile in a heterogeneous RAN as part of a 5G ZTA.

Deploying secure, reliable and interoperable Open RAN equipment faces many of the same challenges as deploying secure, reliable and interoperable equipment in any 5G RAN and Core. In other words, deployment issues are not exclusive to Open RAN. Open RAN adds an extra dimension to the complexity of achieving security, reliability, and interoperability when compared to a single vendor RAN deployment. The Open RAN ecosystem will now encompass many systems integrators, cloud platform providers, Open RAN software suppliers, third-party hardware suppliers, and chipset providers.

Whether Open RAN or traditional RAN, the RAN is typically where network congestion and degradation occurs due to it being the wireless access medium of the network relying on the limited resource of frequency. Frequency is a limited resource, which if compromised affects the availability pillar of cybersecurity. As a result, security, reliability, and interoperability are critical in traditional RAN and Open RAN.

Secure and prioritized interoperable emergency communications between service provider Open RANs will be critical for Public Safety, National Security and Emergency Preparedness (NS/EP) personnel and critical infrastructure stakeholders. Many of these stakeholders leverage priority emergency communications services such as Wireless Priority Service, AT&T FirstNet, Verizon Frontline, and T-Mobile Connecting Heroes or combinations of these—all of which utilize 4G/5G RAN infrastructure. In addition, these services can also complement and interoperate with Land Mobile Radio networks or wireline priority services such as the Government Emergency Telecommunications Service. These services are highly reliable and provide invaluable priority and preemption capabilities for their emergency communications stakeholders. However, these services cannot overcome interoperability issues between Open RAN vendors within a given coverage area.

In addition to interoperability support, offered solutions will need to meet other criteria that purchasers will evaluate in their decision-making process such robust security, performance and management capabilities. Priority emergency communications require certain priority mechanisms in the RAN such as access class barring and high priority access admission control. Open RAN will need to support these priority capabilities on its new interfaces and functions. A greater Open RAN vendor base will require interoperability and high resiliency of these priority mechanisms.

Future priority emergency communications will cover many use cases such as mobile broadband data, video and information services for greater situational awareness, ultra-low latency for Vehicle-to-Everything, massive IoT including sensors for situational context, and data analytics at the network edge. Prioritizing and securing these various services on the same 4G/5G infrastructure may benefit from differentiated network slices and federated network slicing to interoperate these services between service providers when needed, including roaming and disaster scenarios, such as widespread network outage, massive congestion, cyber and physical attacks. All RAN vendors within a single Open RAN deployment and interoperating between multiple service provider Open RANs may need to adhere to and honor QoS, network slice types and attributes including MultiMedia Priority Service, 5QI settings, and priority and pre-emption parameters. The actions enforced will depend upon the type of service and priority levels of the users.

Additional considerations must be made for use of Open RAN in NS/EP use cases. Within a service provider's Open RAN deployment, each vendor should adhere to orchestrated security controls, which may leverage AI/ML for real-time threat and anomaly detection. In addition, each Open RAN vendor should interact with transport and aggregation layer real-time controls within a network slice and RIC platform upon workload migration due to workload failure, infrastructure failure, or cyberattack.

5.1.7 Summary of Recommendations for Open RAN Architecture

5.1.7.1 Architectural Recommendations for the FCC.

Recommendation-Arch-FCC-1: CSRIC VIII recommends future CSRICs consider further CSRIC work on the Quantum Computer threat.

5.1.7.2 Architectural Recommendations for Industry.

Recommendation-Arch-Indust-1: CSRIC VIII recommends that CSRIC VII recommendations[76] for securing 5G SA networks should apply to Open RAN.

Recommendation-Arch-Indust-2: CSRIC VIII recommends that the CSRIC VI recommendations[77] for securely consuming open-source software for deployment in 5G production networks should apply to Open RAN.

Recommendation-Arch-Indust-3: CSRIC VIII recommends that the CSRIC VI recommendations[78] for digital signing of production software should apply to Open RAN workloads, including network functions and applications.

---

[76] CSRIC VII Report on 5G from Legacy Vulnerabilities and Best Practices for Mitigation (10 June 2020).

[77] CSRIC VI Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging Wireless Networks (September 2018).

[78]CSRIC VI Report on Best Practices and Recommendations to Mitigate Security Risks to Emerging Wireless Networks (September 2018).

Recommendation-Arch-Indust-4: CSRIC VIII recommends that ethernet based Front Haul networks be segmented to isolate FH traffic from other traffic flows and that port based authentication be used to enable authorization of network elements attached to the FH network.

Recommendation-Arch-Indust-5: CSRIC VIII recommends that secure protocols providing mutual authentication be used when deploying RUs with ethernet based FH in US production networks.

Recommendation-Arch-Indust-6: CSRIC VIII recommends that IEEE 802.1X Port-based Network Access Control[79] be implemented for all Network Elements that connect to the Open FH network deployed in hybrid mode.

Recommendation-Arch-Indust-7: CSRIC VIII recommends that RICs are enabled with conflict mitigation capability when deploying Open RAN with 3rd-party rApps or xApps.

Recommendation-Arch-Indust-8: CSRIC VIII recommends that the US telecommunications industry should establish test specifications for xApps and rApps to ensure secure integration into the RIC platforms and protection of sensitive data.

Recommendation-Arch-Indust-9: CSRIC VIII recommends that separation and isolation of applications (i.e., xApps/rApps) should be built-in to reduce the possibility of further compromise to other Open RAN components or applications if those applications become compromised.

Recommendation-Arch-Indust-10: CSRIC VIII recommends that Open RAN software be deployed on secure server hardware. The credentials and keys used as part of the Open RAN software should be encrypted and stored securely.

Recommendation-Arch-Indust-11: CSRIC VIII recommends that US industry should drive evolution of Open RAN security specifications at the relevant standards bodies and industry consortia to align with the recommendations in this report.

Recommendation-Arch-Indust-12: CSRIC VIII recommends that Open RAN implementations should be based on the principles of Zero Trust Architecture (ZTA).

Recommendation-Arch-Indust-13: CSRIC VIII recommends that Open RAN products should follow the same processes used to certify equipment, to the extent they are used for priority communications for National Security and Emergency Preparedness (NS/EP), public safety and critical infrastructure.

Recommendation-Arch-Indust-14: CSRIC VIII recommends US industry to work within ATIS to establish an Open RAN focus group for NS/EP, Public Safety and Emergency Services.

Recommendation-Arch-Indust-15: CSRIC VIII recommends that Industry should assess the need for establishing a process for accreditation of independent test laboratories for Open RAN

[79] IEEE 802.1X-2020, IEEE Standard for Local and Metropolitan Area Networks, Port-Based Network Access Control, https://standards.ieee.org/ieee/802.1X/7345/ (last visited 17 November 2022).

multi-vendor security, priority, interoperability and performance testing.

Recommendation-Arch-Indust-16: CSRIC VIII recommends that Open RAN architectures implement defenses to prevent Adversarial Machine Learning (AML) attacks. Industry should work within the O-RAN Alliance to drive security specifications that mitigate AML attacks.

Recommendation- Arch-Indust-17: CSRIC VIII recommends that the MNO use secure boot based on hardware root of trust, with credentials securely stored (e.g., in an HSM), and software signing to establish an end to end chain of trust.

5.2 Analysis – Secure Open RAN Software Development

5.2.1 Evolution of Secure Software Development

Systems normally evolve or transition to the next generation because of changing requirements or improvements in technology. System security plans should continually evolve with the system. Much of the environmental, management, and operational information for the original system should still be relevant and useful when the organization develops the security plan for the follow-on system. Secure development processes based upon the NIST Secure Software Development Framework (SSDF)[80] is a component of a secure Open RAN supply chain. Since security is the key to a successful implementation of Open RAN, adoption of security-by-design reduces risk in the Open RAN ecosystem by considering security from the early phases of development to establish product trustworthiness.

Open RAN development community's planned use of software, including open-source software and third-party proprietary components, will bring challenges as there will be hundreds of applications throughout the system lifecycle. Addressing these challenges requires a robust process that includes DevSecOps and CI/CD integrated into the development organization's software development life cycle (SDLC). It is recommended to put DevSecOps at the core of the product development to reduce vulnerabilities and minimize the impact of vulnerabilities[81, 82,83]. CI/CD enables software developers to frequently deliver code changes to respond to security threats and vulnerabilities. Organizations should define and adopt a process for managing software and the security risk of third-party components that fits into an organization's existing SDLC to ensure supply chain integrity. Putting security at the core of the SDLC enhances Open RAN system security.

---

[80] NIST, SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (2022), https:// csrc.nist.gov/publications/detail/sp/800-218/final.

[81] The President's National Security Telecommunications Advisory Committee (NTSTAC) Report, Software Assurance in the Information and Communications Technology and Services Supply Chain (November 2021, https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20Software%20Assurance.pdf.

[82] NIST, *Information Technology Laboratory (ITL), Publications, Computer Security Resource* Center, Projects,

[83] DevSecOps, https://csrc.nist.gov/projects/devsecops (last visited 19 November 2022).

5.2.2 Secure Development Phases

O-RAN development should also apply NIST special publication 800-160[84] which provides considerations for a multidisciplinary approach in the engineering of trustworthy secure systems. The Linux Foundation's white paper[85] suggests best practices described a set of "activities" that teams producing secure software should perform, with balanced guidance that is meaningful and relatively easy to implement without being overly prescriptive or rigid.

5.2.3 NIST SSDF

Open RAN development community can also benefit from NIST's SSDF,[86] which describes a set of fundamental, sound practices for secure software development. The NIST SSDF project brings together a set of secure software development practices from organizations such as BSA,[87] OWASP,[88] and SAFECode.[89] The SSDF fills in the details of security within SDLC models. Expected benefits from the SSDF include a reduction of software vulnerabilities, mitigation of undetected or unaddressed vulnerabilities, and prevention of future recurrences of vulnerabilities. Development organizations may integrate the SSDF throughout their existing software development practices, express their secure software development requirements to third-party suppliers using SSDF conventions, and acquire software that meets the practices described in the SSDF. They may also use SAFEcode' s paper[90] on managing security risks inherent in the use of third- party components. Third-party components should be consumed with due diligence that ensures responsible, disciplined evaluation. This paper proposes a lightweight and easy-to-use third-party component life cycle that can easily be aligned to an existing software development life cycle to tackle security risks due to the use of third-party components.

5.2.4 O-RAN OSC

---

[84] NIST, SP 800-160v1, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (2018), https://csrc.nist.gov/publications/detail/sp/800-160/vol-1/final.

[85] Linux Foundation, *Resources, Publications,* https://linuxfoundation.org/resources/publications/improving-trust-and-security-in-open-source-projects (last visited November 1, 2022)

[86] NIST, SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (2022), https:// csrc.nist.gov/publications/detail/sp/800-218/final.

[87] The BSA Framework for Secure Software, Sept 2020, https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf (last visited November 22, 2022).

[88] Open Web Application Security Project® (OWASP), https://owasp.org (last visited November 1, 2022).

[89] SAFEcode, *Resource: Secure Development Practices*, https:// safecode.org/category/resource-secure-development-practices/ (last visited October 31, 2022).

[90] SAFEcode, Managing Security Risks Inherent in the Use of Third-party Components, https://safecode.org/ wp-content/uploads/2017/05/SAFECode_TPC_Whitepaper.pdf (last visited October 31, 2022).

The O-RAN Alliance has collaborated with Linux Foundation to create open-source community for O-RAN development.[91] The purpose of O-RAN Software Community (OSC) is to develop software for O-RAN solutions, focusing on aligning with the O-RAN Alliance's open architecture and specifications with the goal to achieve a deployable Open RAN solution. The OSC will help develop modular, open, intelligent, and efficient disaggregated radio access networks using secure development practices within open-source communities.

The Open RAN community should ensure that Open RAN standards, software, and equipment are developed with security-by-design to facilitate successful growth of Open RAN. Open RAN software development, including OSC contributors and consumers, should follow industry best practices, including:

- US 5G networks, including Open RAN, should use the most recent and secure versions of protocols.
- Threat analysis and secure design is not a one-time process. Threat analysis should be continuously repeated by the software vendor during the development process.
- Open RAN products and networks should securely consume and maintain software using development frameworks such as the NIST SSDF.[92]
- Vendors should disable insecure security protocols and deprecated cryptographic algorithms.
- Security controls should be developed and implemented to ensure network functions and data are protected in use, during transmission and at rest.
- Protocols and interfaces must be specified, implemented, and configured to be secure.
- O-RAN applications and network functions should have clearly defined roles, permissions, and constraints using the principle of least privilege.
- O-RAN applications and network functions should be designed and developed to minimize the attack surface.
- Be aware of country of origin when consuming OSC software.

5.2.5 **Recommendations for Open RAN Software Development**

5.2.5.1 Recommendations for the FCC

Recommendation-SWDev-FCC-1: CSRIC VIII recommends that the FCC facilitate the

[91] Press Release, O-RAN Alliance, The O-RAN Alliance and Linux Foundation launch Industry-Leading O-Ran Open-source Community (April 2, 2019), https://assets-global.website-files.com/60b4ffd4ca081979751b5ed2/611976f76ada866b2df4c0ce_FINAL%2BO-RAN%2BOSC%2B190402.pdf

[92] NIST, SP 800-218, Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (2022), https:// csrc.nist.gov/publications/detail/sp/800-218/final.

establishment of a collaborative national 5G Open RAN emulation environment that is available to industry, academia, and government to evaluate and identify zero day attacks. For example, this could be accomplished by expanding the NIST NCCoE or encouraging utilization of the United States based Open Test and Interoperability Center (OTIC).

5.2.5.2 Recommendations for Industry

Recommendation-SWDev-Indust-1: CSRIC VIII recommends that the Open RAN ecosystem puts security at the core of the Software Development Life Cycle (SDLC) by utilizing best practices such as NIST DevSecOps, NIST SSDF, BSA Framework for Secure Software, or SAFECode.

5.3 Analysis: Operations

Network operations include all the monitoring and response activities carried out to maintain network availability and performance. These activities include management network equipment/functions (e.g., servers, firewalls, databases), infrastructure (e.g., connections with data networks and services, backhaul links), and devices. A cellular network may have several Network Operation Centers (NOCs) responsible for specific geographical areas or specific functions, such as security. Alternatively, a single NOC could be divided into multiple teams dedicated to specific areas of responsibility.

Main activities of the NOC are monitoring current network performance and managing network services. Activities surrounding network performance, including quality and reliability KPIs drive network optimization and faster incident response. The NOC also manages software/firmware updates and patches and ensures backups are successfully completed. The security operations team could be part of the NOC or work closely with the NOC staff.

Another aspect of network operations is testing network component upgrades and updates. This is done for reasons such as remediating known errors, performing vulnerability patches, or addressing network anomalies, or to introduce new capabilities to the network. Thorough integration testing may also reduce the risk of misconfiguration and human-induced configuration errors.

5.3.1 Challenges in multi-vendor RAN environment

As stated in the ESF report:[93]

> "While traditional RANs are inherently single-vendor, Open RAN architecture will introduce more complexity due to the increased number of vendors and disaggregation of traditional network functions."

This section further examines the challenges in a multi-vendor RAN environment.

[93] NSA Enduring Security Framework (ESF) and CISA, Open Radio Access Networks Security Considerations, 2022, http://www.cisa.gov/sites/default/files/publications/open-radio-access-network-security-considerations_508.pdf.

Open, standardized, secure and stable interface specifications are the technology enablers for an open ecosystem that attracts suppliers to build solutions and at the same time offers diversity and choice to purchasers. Even if interfaces are built based on the same O-RAN specifications, extensive testing of the interfaces with correct and aligned configurations are necessary. Interoperability testing is generally found to be time consuming and expensive and service operator generally bear the cost of this effort.

Due to Open RAN's multi-vendor environment, there is increased complexity for the network management and security operations center to determine the cause of an outage or performance degradation. Another challenge is ensuring that the trusted container or Virtual Machine is operating correctly. With the disaggregation of network functions and components, it is difficult to quickly isolate problems, which may result in lengthy network recovery from compromised or malfunctioning functions or components. Increased integration testing prior to deployment may mitigate this concern with the tradeoff that it increases the operator's time to implement any change in the network.

The multi-vendor environment in an Open RAN deployment increases the challenge to build a network to be "secure by design" and interoperable. This may require a higher degree of integration at various layers within a network to achieve the targeted security posture. Open RAN's multi-vendor ecosystem could potentially benefit from a certification process to show compliance to interoperability and security standards. Such a process could reduce integration time between multiple vendors. The need to have formal certifications is currently being discussed by industry and government. Accredited labs would need to be certified to be able to provide vendor certifications. A formal certification process has many tradeoffs that could either hurt or benefit potential stakeholders, including national operators, rural operators, large vendors, small vendors, and government agencies. Independent of the certification process, stakeholders are recommended to apply the O-RAN Alliance's test specifications as applicable.

5.3.2 Challenges for Distributed Far-Edge

Traditional security solutions have been focused on perimeter defenses keeping the attacker and malicious entities outside of the network. Sometimes attackers may be successful compromising portions of the Open RAN network. To ensure reliability, recovery from security events need to be accomplished rapidly with minimal manual effort. This is especially important in Open RAN far-edge scenarios where the large number of sites makes it prohibitively expensive to send technicians into the field for recovery.

An increasing area of interest is Open RAN's ability to self-heal and automatically recover from failures and compromises. This is relevant as malware and ransomware are being weaponized by nation-state actors whose mission is to take down critical infrastructure, including mobile networks. Disrupting communications is a prime target for nation states, and this could be accomplished by infecting Open RAN with malware with remote command and control, can take down a portion of the RAN. Ransomware is a rising type of threat for telecommunications.

5.3.3 Training

The increased network complexity in an Open RAN deployment requires an increased level of

technical expertise to ensure the network is operated and maintained in a secure and reliable way.

Deploying Open RAN solutions, which relies on disaggregation and virtualization technologies, changes the paradigm in which network equipment vendors provide dedicated telecommunications technical support to one in which network operators will require a workforce with IT engineering and system integration experience. These types of individuals are in high demand, making it a considerable challenge to find a sufficient, highly skilled workforce.

Training certifications and programs need to be established to meet the need for a qualified workforce. These activities will support workforce training needs and skilled labor immigration to address US labor skills gaps that may impede the development of Open RAN.

Initiatives include:

- The Department of Commerce, National Science Foundation, National Academies, and other agencies that have responsibility for STEM workforce development can foster such programs.
- The Departments of Homeland Security and State can specify visa and skilled worker entry requirements.
- Industry should establish programs that facilitate a talent pipeline from HBCUs.
- Virtual training ranges (or environments) can be set up to enable current and rising security professionals to quickly ramp up their skills in the areas of 5G and Open RAN.

5.3.4 Compliance

While carriers have the ultimate obligation for compliance, they rely heavily on standards developing organizations to ensure national and regional regulations can be met. Vendors also develop their products to ensure they can meet national and regional regulatory requirements. Compliance requirements may impact an operator's deployment by imposing jurisdictional constraints. US operators provide additional assistance to US law enforcement by providing cell tower location databases that enable historical location data for investigations and trials which may be used as evidence to indicate the location of a particular handset at a particular time.

Data centers supporting Open RAN equipment should meet the same physical security requirements, and provide data security to sensitive data-at-rest, data-in-transit, and data-in-use, as is implemented in legacy cellular RANs.

5.3.5 Recommendations - Operations

5.3.5.1 Operations Recommendations for the FCC

Recommendation-Ops-FCC-1: CSRIC VIII recommends that the FCC work with the Department of Commerce, National Science Foundation, National Academies, and other agencies that have responsibility for STEM workforce development, as well as the Departments of Homeland Security and State on visa and skilled worker entry requirements to support

workforce training needs and skilled labor immigration to address US labor skills gaps that may impede the development of Open RAN. Furthermore, it is recommended that the FCC work with industry to establish programs that facilitate a talent pipeline from HBCUs.

5.3.5.2 Operations Recommendations for Industry

Recommendation-Ops-Indust-1: CSRIC VIII recommends that industry determines the need for formal certifications of Open RAN solutions and the applicability of those certifications to the deployment and use cases.

Recommendation-Ops-Indust-2: CSRIC VIII recommends that all O-RAN stakeholders apply the O-RAN Alliance's test specifications as applicable.

5.4 Analysis: Supply Chain

5.4.1 Observations about the Open RAN Supply Chain

CSRIC VIII has made the following observations for Open RAN supply chain:

- Open RAN systems incorporate additional components due to disaggregation and architectural flexibility. However, the main supply chain security practices are not fundamentally different from traditional RAN.
- Supply chain diversification is more significant in Open RAN compared to traditional RAN due to the ability to have multi-vendor network components. The benefits of diversification have been recognized by industry. Diversification leads to a greater need to rely on best practices in the supply chain and may require additional protections for the supply chain.
- Greater flexibility and diversification of the supply chain puts a greater importance on interoperability between components, thus requiring greater investment in supply chain planning.
- network operators need cradle to grave approaches to qualify, test, configure, update and manage separately designed RAN components, to successfully source, integrate, deploy, and support RAN components from multiple suppliers.
- Disaggregation in Open RAN creates a virtualized software environment where resilience depends on the software supply chain. Attention to software supply chain in Open RAN environment is required.
- In planning to use disaggregated components in a virtual RAN, network operators may need their procurement and supply chain organizations to plan for managing requirements for subsystems and components such as ASICs, GPUs, accelerators and FPGAs.
- Disaggregation within a complex global supply chain requires careful planning due to differences in export controls and trade rules, to avoid potential obstacles.

5.4.2 Current RAN supply chains

Deploying, maintaining, and optimizing proprietary networks is time consuming and costly,

with heavy reliance on a few vendors. "RANs are traditionally vendor-locked, vertically integrated telecommunications architectures that enable wireless communications, such as 4G, 5G, and subsequent generations of communications technologies."[94]

Supply chain diversification is an important issue associated with Open RAN and frequently understood in terms on national security. The US Executive Order on America's Supply Chains[95] identified additional characteristics of a resilient supply chain, including the ability to revitalize and rebuild domestic manufacturing capacity, maintain America's competitive edge in research and development, and support small businesses.

5.4.3 Telecommunications supply chain

In October 2018, CISA launched the ICT Supply Chain Risk Management (SCRM) Task Force,[96] a public-private partnership to provide advice and recommendations to CISA and its stakeholders on means for assessing and managing risks associated with the ICT supply chain. Recommendations include discussions about challenges of single source and single region suppliers that could be addressed through Open RAN.[97] Within the context of the critical issue of supply chain security risk management, Open RAN supports increased supply chain supplier diversity. Network disaggregation creates market opportunities to introduce diversification of RAN components available to the market, including potential new suppliers. A longer list of potential suppliers would support national security by increasing redundancy and resilience in supply chains.

Various components of the supply chain in Open RAN environment operate in different ways. Improving resilience requires attention to all areas throughout the lifecycles. When supply chain issues in 5G and Open RAN are discussed, hardware and software supply chain plays an important role in improving supply chain resilience. Moreover, supply chain activities persist throughout the lifecycle. Finally, collaboration with the stakeholders engaged in the development, deployment, procurement, maintenance and other parts of the equipment, software, and infrastructure lifecycle are important to ensure efficiency and resilience of the Open RAN supply chain. NSTAC report on software assurance and supply chain provides a useful framework addressing some of these issues.[98]

---

[94] Department of Defense, *News, Press Products, Releases*, DoD and National Spectrum Consortium Team for Open RAN Acceleration (June 3, 2022), https://www.defense.gov/News/Releases/Release/Article/3052013/dod-and-national-spectrum-consortium-team-for-open-ran-acceleration/.

[95] The White House, *Briefing Room*, US Executive Order on America's Supply Chain (Feb 24, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/

[96] https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Tak%20Force%20Interim%20Report%20(FINAL)_508.pdf.

[97] Assessment of the Critical Supply Chains Supporting the U.S. ICT Industry, https://www.dhs.gov/publication/assessment-critical-supply-chains-supporting-us-ict-industry (2022).

[98] https://www.cisa.gov/sites/default/files/publications/NSTAC%20Report%20to%20the%20President%20on%20So

Open RAN system enables the service provider to use COTS hardware, open-source software and applications developed by multiple sources. In an Open RAN system, all the hardware and software components are expected to work together seamlessly since all interfaces will be open and standardized. This poses a major challenge in interoperability and compatibility of various hardware and software components along with security concerns. For the success of Open RAN ecosystem, it is important that one to one replacement of all hardware and software components is possible to create healthy competition among suppliers, prevent vendor lock in situations, and offer more choices for sourcing based on needs.

The following guidelines should be implemented to have a robust supply chain:

- Available components have demonstrated interoperability amongst themselves based on open interfaces.
- One to one replacement of components should be possible and replacement component should meet the technical requirements.
- It should be possible for operators to manage all components using a common management platform and open management interfaces.
- All hardware software components should be from a trusted source and certified to be free from any known security vulnerabilities.
- All hardware and software components should have established root of trust with all sources well documented in an SBOM that contains the source of each software component used.

5.4.4 Elements of software/firmware (SBOM and software inventory)

The growth in the use of third-party code may complicate software developer's ability to maintain an accurate inventory of the code used and its source. Suppliers need to know where their code uses a specific vulnerable third-party library and the status of remediating those instances.

Obtaining an accurate, much less complete, software inventory is difficult. It is not a simple "list of ingredients," because third-party code may include components within other components (e.g., fourth- and fifth-party inclusions in the third-party code). In some cases, developers download a third-party component that may include hundreds of incorporated components, though they intend to integrate only a single component.

An especially complicated problem is obtaining an inventory of all components used in a cloud service. Even defining such an inventory is difficult: should a "cloud service software inventory" include merely the code elements in the "direct" cloud service application (e.g., a human capital management application)? Or should it include the components in all the auxiliary elements of the cloud (e.g., load balancers, firewalls, routers, etc.)? Another challenge is the frequency of changes in cloud services, where code may change multiple times a day. Any inventory, including a published SBOM, becomes stale almost as soon as it is completed, even

ftware%20Assurance.pdf.

with automated SBOM generation.

In many cases, cloud-based transactions involve multiple entities. For example, a transaction submitted to a cloud server may traverse many services prior to completion. Even simple transactions, such as transferring funds from an account in one bank to another bank, may include notices to multiple government and consumer credit agencies. With respect to an inventory, should it include all elements of all services the transaction affects, or a subset? Each application involved in such transactions may be updated independently of the other applications, to the extent that a similar and subsequent transaction a few minutes later might involve newly updated code.

Lastly, an inventory, particularly in generating SBOMs, is not meaningful without standard nomenclature. If supplier and component names are not standardized, it is hard to identify where the code uses a vulnerable third-party library and the status of remediating those vulnerable versions. The criticality of addressing these considerations reinforces the need for standardization to maintain the benefits of an SBOM. However, it is important to prevent fragmented SBOM standards across multiple standards bodies. The O-RAN Alliance has specified SBOM requirements[99] based upon the NTIA's guidelines.[100]

The CSRIC VIII report on "Recommended best practices to improve the communications software supply chain security" addresses and provides SBOM recommendations.[101]

5.4.5 Open-source Software (OSS)

Open-source software (OSS) is commonly used in Open RAN projects, as discussed in section 5.2.4. This section discusses the advantages and disadvantages of utilizing OSS.

NIST defines open source software as:

> "Software that can be accessed, used, modified, and shared by anyone. Open source is often distributed under licenses that comply with the definition of "Open Source" provided by the open source initiative and/or that meet the definition of "Free Software" provided by the Free Software Foundation."[102]

OSS pervades the ICT environment. Virtually all commercial codebases contain open-

[99] O-RAN Security Requirements Specification, v4.0, O-RAN Alliance, Specifications, https://orandownloadsweb.azurewebsites.net/specificationsorandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

[100] National Telecommunications and Information Administration, The Minimum Elements For a Software Bill of Materials (SBOM), (July 2021), https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom.

[101] CSRIC VIII Report on Recommended Best Practices to Improve Communications Supply Chain Security (September 2022), https://www.fcc.gov/file/23839/download

[102] National Institute of Standards and Technology, NIST Suborder 6106.01 Version 1 (December 2018), https://www.nist.gov/system/files/documents/2019/02/19/final_s_6106.01_ver_1.pdf.

source components,[103] of which forty-nine percent (49%) contain high-risk vulnerabilities.[104] Programmers like the ability to "crowd-source" code that performs a function that their application needs, however only 2.27% of their time is spent on security. This creates a need to incentivize developers to improve effort to follow secure software development best practices.[105] Technology companies have incentives to contribute to open-source code, as it often advances the adoption of their own products.

OSS is a powerful tool that can be used by organizations to accelerate innovation while reducing the development timeline, product time to market, and overall cost. OSS also reduces fragmentation and increases interoperability among different products by producing components and protocols that become the de facto standard. OSS provides a platform for talented coders to openly collaborate and build software. Open source works optimally when developers behave as "good citizens" in which consumers also contribute, provide useful feedback, and share fixes. The transparency of code reviewed by many expert eyeballs reduces software complexity and the number of bugs. This crowdsourcing approach to software development has effectively produced quality software at low cost.

As experienced with recent security incidents, there is a tradeoff as OSS's advantages can be exploited as disadvantages and its strengths can be exploited as weaknesses. While the community approach benefits OSS, it also provides an attack surface. As with all software, OSS has many attack vectors, including intentional backdoors made by malicious developers, propagation of vulnerabilities through reuse, exploitation of publicly disclosed vulnerabilities, and human error. The tradeoffs with OSS security are outlined in Figure 11 and discussed further.[106] SBOM and Software Composition Analysis (SCA) are valuable tools to understand the use of OSS components with reported vulnerabilities in Open RAN projects.

[103] Synopsys, "Synopsys Study Shows Uptick in Vulnerable, Outdated, and Abandoned Open-source Components in Commercial Software," April 13, 2021, https://news.synopsys.com/2021-04-13-Synopsys-Study-Shows-Uptick-in-Vulnerable-Outdated-and-Abandoned-Open-source-Components-in-Commercial-Software

[104] Synopsys, Open source Security and Risk Analysis Report (2020) https://ttpsc.com/wp3/wp-content/uploads/2020/10/2020-ossra-report.pdf

[105] The Linux Foundation, *Resources, Publications*, Report on the 2020 FOSS Contributor Survey, https://www.linuxfoundation.org/resources/publications/foss-contributor-survey-2020?hsLang=en (last visited on 18 November 2022).

[106] Ericsson, Ericsson Blog, Open source software security in an ICT context – benefits, risks, and safeguards, (January 14, 2021), https://www.ericsson.com/en/blog/2021/1/open-source-security-software.

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

Figure 11. Open-source software security tradeoffs [source: Ericsson]

5.4.6 Supply Chain Recommendations

5.4.6.1 Supply Chain Recommendations for the FCC

None

5.4.6.2 Supply Chain Recommendations for Industry

Recommendation-Supply-Indust-1: CSRIC VIII recommends that US O-RAN community members develop and complete the O-RAN specifications to ensure a baseline exists for Interoperability testing.

Recommendation-Supply-Indust-2: CSRIC VIII recommends that industry facilitate the evaluation of Open RAN technologies for interoperability, performance, and security for different use cases and deployment scenarios.

Recommendation-Supply-Indust-3: CSRIC VIII recommends that optional fields, whose usage could potentially jeopardize interoperability, be minimized.

Recommendation-Supply-Indust-4: CSRIC VIII recommends that the Open RAN Industry adopts Software Bill of Materials (SBOMs), e.g., O-RAN Alliance Working Group 11 Security requirements.[107]

5.5 Policy Discussions

5.5.1 Policy Recommendations

[107] O-RAN Security Requirements Specification, v4.0, O-RAN Alliance, *Specifications*, https://orandownloadsweb.azurewebsites.net/specifications (last visited on 17 November 2022).

5.5.1.1 Policy Recommendation for the FCC

Recommendation-Policy-FCC-1: CSRIC VIII recommends that the FCC encourages innovation and the development of Open RAN solutions that address market-driven use cases, rather than mandating Open RAN requirements.

Recommendation-Policy-FCC-2: CSRIC VIII recommends that the FCC promotes global economies of scale in the Open RAN ecosystem through industry-led, collaborative standards and interoperability efforts, and encourage US industry leadership in standards via clear exemptions from export controls for these standards efforts. To this end, CSRIC VIII recommends that the FCC should consult with the Departments of Commerce, State, Treasury, and Defense as the Administration considers export controls or other sanctions that may impact Open RAN standards development and interoperability.

Recommendation-Policy-FCC-3: CSRIC VIII recommends the FCC accelerate the growth of the Open RAN ecosystem through incentives, including consulting with the Commerce Department as it makes funding available through the Public Wireless Supply Chain Innovation Fund, as well as other available programs, toward the following purposes: 1) Research and development of Open RAN hardware and software solutions; 2) multi-vendor interoperability and system integration efforts, such as the OTIC program as well as such efforts undertaken in MNO and Vendor Labs ; 3) Application development for the RIC to drive Open RAN system performance, visibility, and automation; and, 4) Technologies that enable Open RAN ecosystem development and growth, including semiconductor innovation and integration with diverse transport networks.

Recommendation-Policy-FCC-4: CSRIC VIII recommends that the FCC not create new certification requirements on Open RAN products beyond current and existing requirements for RAN equipment. See related Recommendation-Ops-Indust-1.

5.5.1.2 Policy Recommendations for Industry

None

6 Recommendations To the FCC and Industry

This report describes Open RAN architectures, security considerations, and challenges to the development of a secure Open RAN ecosystem. These challenges include the growing maturity of the technology, the desire to grow the pool of vendor solutions, the need for multi-vendor solution integration, and a variety of specific technical choices to be made as Open RAN systems develop.

Recommendations to the FCC and to industry are listed below. The recommendation heading shows the recommendation area (Architecture, Operations, SW Development, Supply Chain, Policy) and whether to the FCC or Industry. Each page number links to the section within this report which has additional information on the recommendation.

7 Conclusions

This analysis of Open RAN security, reliability and interoperability considerations produced seven (7) recommendations to the FCC and twenty-four (24) recommendations to industry.

The analysis found that some concerns exist in both Open RAN and closed proprietary RAN. Open RAN security considerations with applications, open source software, supply chain, and zero trust are consistent with those from the Information and Communications Technology (ICT) sector, and Open RAN must implement the ICT best practices to address these concerns. Open RAN utilizes existing 5G Core network technologies including multi-vendor core network functions and 5G cloud infrastructures. Open RAN will benefit by adopting the ICT and 5G best practices to ensure secure, reliable and interoperable deployment and operation.

Open RAN brings new capabilities and concerns with the introduction of xApps/rApps application frameworks and AI/ML technology, and the O-RAN Alliance specified Open Fronthaul network connecting base stations and radios with real-time performance requirements. Some of these concerns are shared with the ICT sector, and both Open and proprietary fronthaul solutions are challenged to balance the security requirements with performance and cost considerations.

With the continued evolution of Open RAN, security and reliability continues to be addressed by the appropriate groups such as O-RAN Alliance and ICT and 3GPP standards evolution.

CSRIC recommends that the FCC and industry act on the recommendations by leveraging existing best practices to address common concerns and implement new processes to mitigate new attack vectors.

8 Appendix A – Glossary

8.1 Acronyms

AI	Artificial Intelligence
AML	Adversarial Machine Learning
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BBU	Baseband Unit
BGP	Border Gateway Protocol
CI/CD	Continuous Integration/Continuous Deployment
CMP	Certificate Management Protocol
CP	Control Plane
CPRI	Common Public Radio Interface
eCPRI	Enhanced CPRI
CSP	Cloud Service Provider
CU	Centralized Unit
CUS	Control User Synchronization
DDoS	Distributed Denial-of-Service
DoS	Denial-of-Service
DU	Distributed Unit
EMOE	Electromagnetic Operational Environment
eNB	Enhanced Node B or E-UTRAN Node B
FH	Fronthaul (or Front Haul)
FPGA	Field Programmable Gate Array
HLS	Higher Layer Split
GPU	Graphics Processing Unit
HRoT	Hardware root of trust
HSM	Hardware Security Module
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IoT	Internet of Things
LLS	Lower Layer Split
MAC	Medium Access Control
MEC	Multi-access Edge Compute
MITM or MiTM	Man-in-the Middle
ML	Machine Learning
MNO	Mobile Network Operator
NACM	NETCONF access control model

Near-RT RIC	Near-Real Time RIC
NFV	Network Function Virtualization
NOC	Network Operation Center
Non-RT RIC	Non-Real Time RIC
NS/EP	National Security and Emergency Preparedness
O-CU	Open RAN Open CU
O-DU	Open RAN Open DU
O-RAN	Open RAN specified by O-RAN Alliance
OSC	O-RAN Software Community
PaaS	Platform as a Service (PaaS)
PDCP	Packet Data Convergence Protocol
PHY	Physical (layer), also called Radio Layer 1
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PQC	Post Quantum Cryptographic
PTP	Precision Time Protocols
RAN	Radio Access Network
RAT	Radio Access Technology
RF	Radio Frequency
RIC	RAN Intelligent Controller
RLC	Radio Link Control
RRC	Radio Resource Control
RRU	Remote Radio Unit
RT	Real Time
SaaS	Software as a Service
SCA	Software Composition Analysis
SBOM	Software Bill of Materials
SDN	Software Defined Networking
SDLC	Software Development Life Cycle
SIM	Subscriber Identity Module
SMO	Service Management and Orchestration
SSH	Secure Shell
UP	User Plane
ZTA	Zero Trust Architecture

8.2 Definitions

Cloud RAN: A cloud-native solution for radio access networks (RAN) that enables large-scale deployment, deployment flexibility, and open RAN architectures.

Database attack: A type of Cyber-attack against the 5G-enabled network's database managed through different servers, i.e., fog server, cloud server, etc. Examples include Structured Query Language attack, Cross-Site Scripting attack, and Cross-Site Request Forgery.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks: Types of Cyber-attacks where an adversary conducts malicious tasks to prevent the legitimate parties from accessing the resources of the network or system, and coded packets are sent under these attacks to rapidly consume bandwidth resources of the targeted system (e.g., in 5G-enabled IoT communication networks, DoS attacks can also be performed through other types of routing attacks such as sinkhole, wormhole, blackhole and misdirection attacks; in such attacks, the physically deployed attacker nodes disturb the ongoing routing process to drop, delay, or modify the exchanged packets; also, in the presence of such attacks data messages [packets] may be altered, delayed or dropped before reaching their intended recipient, causing an increment in the end to end delay, reduced throughput, and other deleterious effects on other network performance parameters).

Eavesdropping, sniffing or snooping attacks: Types of Cyber-attacks where an attacker eavesdrops on exchange messages among the communicating parties to launch further attacks.

Electronic jamming attack: A type of Cyber-attack when electronic signals used to overpower the functionality and performance of 5G systems.

Impersonation attack: A type of Cyber-attack where an attacker successfully determines the identity of a genuine communicating party and then creates a message and sends it to the recipient on behalf of the ``authorized communicating party'' (also called primary user emulation attack).

Injector traffic analysis attack: A form of passive Cyber-attack in which an attacker intercepts and examines exchanged messages to devise further attack strategies.

Insider or byzantine attack: A type of Cyber-attack where a privileged insider user of the trusted authority penetrates the RF/PHY layer and exploits stored information to introduce other severe attacks such as session key computation, password guessing attack, etc.

Malware attack: A type of Cyber-attack where an adversary executes a malicious script in a remote system to perform various unauthorized activities, for example, stealing, deletion, updating, and encryption of important information. Malware may be inserted in the process of different types, for example, viruses, worms, keyloggers, spyware, ransomware, and Trojan horses. They are also used to monitor the activities of the users without their consent. These attacks may also harm the functionality of 5G-enabled systems or networks. For instance, a smart IoT device can be hijacked (controlled) remotely by exploiting malware.

Man-in-the-middle attack (MITM): A type of Cyber-attack where an attacker exfiltrates transmitted messages and then attempts to update or delete the messages before forwarding them to the intended receiver.

Man-in-the-Cloud (MITC): A type of Cyber-attack which is caused because of the successful data synchronization of the attacker's device with the victim's information.

Open Fronthaul: An O-RAN Alliance specified interface that forms a link between an O-RAN Distributed Unit (O-DU) and O-RAN Radio Unit (O-RU), enabling interoperability between

different vendors. Also known as the Lower Layer Split (LLS) 7-2x.

Open RAN: A RAN concept based on virtualization of RAN elements and interoperability using open interfaces.

Physical capture of deployed devices: A type of Cyber-attack in which continuous physical monitoring of O-RAN/5G networks and IoT devices can be impractical, giving an adversary the chance to physically capture these devices and extract sensitive information (i.e., identities, secret keys, etc.) from the device memory when monitoring is disabled.

RAN Layer 1 (PHY): Defines the physical radio interface from the UE to the RAN.

RAN Layer 2: Includes four sub layers (i.e., Service Data Adaptation Protocol (SDAP), Packet Data Convergence Protocol (PDCP), Radio Link Control (RLC), and Medium Access Control (MAC).

RAN Layer 3 (RRC) Layer: Responsible for radio resource control (e.g., RRC connection establishment, maintenance and release, and establishment, configuration, maintenance and release of point-point radio bearers.

Side-channel attack: A type of Cyber-attack where the device signatures (such as power, electronic emanations, memory usage, timing, and fault response) can be monitored during operation by an attacker to recover sensitive data. An adversary may utilize this information to conduct other undesired exploits (e.g., impersonation, password guessing, session key computation, MITM, and other attacks) in an O-RAN/5G-enabled IoT environment.

Software Composition Analysis (SCA): An automated process that identifies the open source software in a codebase. This analysis is performed to evaluate security, license compliance, and code quality.

vRAN or V-RAN: Virtualized RAN moves the control functions of hardware base stations to centralized servers, bringing them closer to the network edge.

rApps: Modular applications that leverage the functionality exposed via the Non-RT RIC Framework's R1 interface to provide added value services relative to RAN operation. The rApp functionality within the Non-RT RIC enables non-real-time control and optimization of RAN elements and resources and policy-based guidance to the applications/features in Near-RT RIC.[108]

Replay attack: A type of Cyber-attack when an attacker intercepts exchanged messages and deceitfully delays or retransmits them to confound the receiving entity.

Software Composition Analysis (SCA) : An automated process that identifies license compliance and evaluates security compliance.

xApps: An application designed to run on the Near-RT RIC.[109]

---

[108] O-RAN Alliance, Specifications, O-RAN Architecture Description, v7.0, O-RAN.WG1.O-RAN-Architecture-Description-v07.00, https://orandownloadsweb.azurewebsites.net/specifications

[109] O-RAN Alliance, Specifications, O-RAN Architecture Description, v7.0, O-RAN.WG1.O-RAN-Architecture-Description-v07.00, https://orandownloadsweb.azurewebsites.net/specifications.

Zero trust (ZT): An evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.

Zero trust architecture (ZTA):[110] Uses zero trust principles and assumes no implicit trust is granted to assets or user accounts based solely on their ownership, physical location, or network location.

[110] NIST, Publications, Zero Trust Architecture, NIST SP 800-207, August 2020, https://www.nist.gov/publications/zero-trust-architecture (last visited October 2022).

9 Appendix B – Government Actions: ICT Supply Chain

Executive Orders, legislative actions, and federal policies to address security issues related to the ICT supply chain are listed here.

- Executive Order (E.O. 13873)[111] on Securing the Information and Communications Technology and Services Supply Chain.
- Executive Order (E.O. 14017)[112] on America's Supply Chains, directs Departments of Commerce and Homeland Security to conduct one-year assessment of supply chains for critical sectors and subsectors of the U.S. Information and Communications Technology (ICT) base.
- U.S. Dept. Commerce and Homeland Security's Assessment of the Critical Supply Chains Supporting the U.S. Information and Communications Technology Industry[113] .
- Office of Management and Budget Federal Source Code Policy[114] requires federal agencies to release at least 20 percent of new custom code as Open Source.
- NTIA Report to Congress on Competitiveness and Sustainability of Trusted Suppliers in the Wireless Supply Chain.[115]
- The International Trade Administration provides market intelligence reports on the Information and Communication Technology (ICT) market[116]. These reports provide insights into ICT policies of foreign entitles.
- Public Law 116-124, Secure and Trusted Communications Networks Act of 2019.[117]

---

[111] Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, (May 15, 2019), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

[112] Executive Order 14017, America's Supply Chain, (February 24, 2021), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain

[113] Department of Homeland Security, *Publication Library, Assessment of the Critical Supply Chairs Supporting the U.S. Information and Communications Technology Industry*,https://www.dhs.gov/sites/default/files/2022-02/ICT%20Supply%20Chain%20Report_2.pdf (last visited October 31, 2022).

[114] Office of Management and Budget, Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open-source Software (8 August 2016), https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m_16_21.pdf.

[115] E. Remaley in response to reporting requirement in Section 9202(a)(1)(G) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (August 5, 2021), https://www.ntia.doc.gov/files/ntia/publications/ndaa_pwscif_response.pdf.

[116] Official Website of the International Trade Administration, *Market Intelligence*, https://www.trade.gov/market-intelligence-search/1299 (last viewed October 27, 2022).

[117] Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 133 Stat. 158 (2020) (codified as amended at 47 U.S.C. §§ 1601-1609 (https://www.govinfo.gov/content/pkg/COMPS-15677/pdf/COMPS-15677.pdf).