Open RAN Security Report

May 2023

Outcome from
Quad
Critical and Emerging Technology Working Group

Table of Contents

Introduction

Background

Mobile communication systems and other information and communication infrastructures are an essential part of the social economy and people's lives. 5G networks, which are currently being deployed globally, differ from conventional mobile communication systems in that, in addition to ultra-high speed and high capacity, they are equipped with requirements such as ultra-low latency and multiple simultaneous connections, and are expected to be used as a platform for improving efficiency and convenience in industry and society and creating new added value. The importance of these systems in society and the economy is increasing, and it is important to ensure their security. Traditionally, base stations necessary for the deployment of mobile communication systems were designed by vendors using their proprietary technologies and standards and were provided as a single solution. Therefore, if a telecommunications operator adopts a certain vendor's base station and builds a network, it will be forced to continue building its network with that same vendor's base station from then on, resulting in so-called vendor lock-in. This has made it difficult for new entrants, even those with superior technology, to enter the base station market, leading to market oligopoly and vendor lock-in, and the global market for mobile communication system base stations has become an oligopoly dominated by a small number of vendors. In addition, if the vendor lock-in situation persists for a long time, it is assumed that the specifications and operational methods of base stations may become increasingly black boxed. Furthermore, as the procurement of products is dependent on a specific vendor, if procurement from that vendor stagnates or is disrupted for some reason, there is a potential for so-called supply chain risk, where the entire service may become inoperable.

In response to this situation, worldwide efforts are underway to open up the interfaces between the devices that make up the base station, beginning with Open RAN. The Open Radio Access Network (O-RAN) Alliance, an international association for open and intelligent Radio Access Networks (RANs), was launched in 2018. As of May 2023, nearly 330 carriers and vendors belong to this organization, which has grown into a global and large industry association.

The O-RAN Alliance is developing open technical specifications for signal interfaces between the devices that make up the 5G base station. In addition, studies are being conducted on the certification and interoperability testing of Open RAN components and interfaces through Open Testing and Integration Centres (OTICs), which are open and neutral interoperability verification centres. Currently, several OTICs are established in Europe, the USA and Asia, including Japan. Open RAN allows for the free choice of the equipment that makes up the base station, making it possible to develop a highly scalable and flexible base station. Vendors will also be able to introduce high-demand and differentiated products to the market that use their own specialist technologies, and mobile network operators (MNOs) will be able to adopt better products without

being locked into existing vendors. The widespread use of O-RAN specifications is expected to break the telecoms base station oligopoly, and market competition between vendors is expected to improve the performance of individual devices and reduce the cost of equipment considering increased market competition.

On the other hand, reports published by government organizations in some countries have pointed out that Open RANs have security issues due to the inclusion of interfaces such as Open fronthaul and components such as O-Cloud, SMO (Service Management and Orchestration) and RIC (RAN Intelligent Controller).

Objectives of this research study

Given the above background, it is envisaged that in the future, vendors will actively develop O-RAN equipment, number of 5G base stations compliant with the O-RAN Alliance specifications will increase, and networks consisting of a diverse range of base stations provided by various vendors are expected to be formed.

On the other hand, reports published by government organizations in some countries have pointed out that Open RANs have security issues.

In response to these points, this study will firstly develop a categorization of security risks for 5G networks, review existing expert reports, and consider how to set conditions in a neutral and non-biased manner. A comparative study of Open RAN and traditional vertically integrated networks is then carried out to identify the security advantages and challenges of Open RAN. For the issues identified as security challenges for Open RAN, risk mitigation measures are studied for each issue, and laboratory experiments are conducted for items considered necessary or beneficial. With such attention to security in Open RANs, it is necessary to assess issues pointed out in those reports and possibilities for the mitigation in an objective manner.

Summary

5G network faces multifaceted risks such as market oligopoly of base stations, the rising cost of fossil fuel-based energy resources and increased complexity associated with technological evolution. Among them, in this investigation, security risks for typical 5G network are categorized and compared between traditional RAN and Open RAN.

Comparison of Open RAN and traditional RAN

- Several findings are derived from the STRIDE Threat Modeling and associated risk analysis performed on the basis of the O-RAN specifications
    - In total, 10 O-RAN components and interfaces have high-rated security risks associated to them. The component with the highest number of security threats according to the analysis is the O-Cloud

- However, it can be considered a virtualization-related security threat that is not limited to Open RAN. A total of 4% of the analyzed security threats are considered unique to Open RAN
- Compared to non-disaggregated, non-virtualized RAN, Open RAN has potential security advantages, incl. openly specified, verifiable security controls and capabilities associated to virtualization and cloudification that can help to improve operational security tasks

• Mitigation measures based on O-RAN specifications are evaluated as follows:
  - Analysis of the technical specifications shows that defined security controls mainly focus on the Analysis & design phase of the Open RAN lifecycle
  - Supplementary mitigation measures are provided to cover the entire Open RAN life cycle beyond Analysis & design
    - Analysis & design : Open RAN vendor to ensure compliance with relevant technical specifications (incl. O-RAN, 3GPP) and follow best practices for secure solution design
    - Implementation & test : Open RAN vendor to enforce secure development practices, perform security testing, and confirm interoperability using O-RAN test specifications
    - Sourcing & procurement : MNO, Open RAN vendor, and other involved parties to contractually agree security requirements, roles and responsibilities, e.g., by signing SLAs and utilizing RFPs/ RFQs/ SBOMs
    - Integration & deployment : Involved parties to perform network integration, security configuration and hardening tasks
    - Operations & maintenance : MNO to leverage operational security and automation capabilities of O-Cloud and SMO to enforce established best practices for identifying and mitigating security incidents
  - A security checklist attached as an Appendix to this report is also beneficial for mitigation of security risk
  - With these mitigation measures, it is possible to ensure equivalent security level compared to traditional RAN

Lab Verification and Analysis

• For lab verification purpose, Open Fronthaul is selected as a representative interface as it includes all CUS + M-Plane components and was the first interface to be opened up. This interface is an appropriate representative test subject due to its maturity and advanced implementation
• The tests conducted here were based on the O-RAN specification, and it was confirmed

that the risk of Open Fronthaul can be addressed by adhering to the standard specification

- Furthermore, Open Fronthaul includes typical connection types (Ethernet L2 connections, TCP/IP connections) and security controls Open FH, which means that it can be estimated that the risk of other interfaces can also be reduced by adhering to the standard specifications, leading to security assurance

In addition, from aspects unrelated to security, Open RAN can be expected to have the following effects:

- Improvement of the performance and reducing the cost of equipment by stimulating competition in the base station market;
- Mitigating supply chain risks (diversifying suppliers) according to the multi-vender configuration;
- Optimizing energy efficiency through intelligence (Energy saving);
- Improvement of monitoring and maintenance functions by SMOs.

So, in 5G network deployment, MNOs will be able to make comprehensive decisions based on these aspects as well as security.

Finally, A security checklist summarizing the security requirements to be met by Open RAN is also attached as an Appendix to this report. This checklist is mainly intended to be used to check whether the security measures for Open RAN networks are sufficient in the following two situations.

- For MNOs currently operating Open RAN: use the checklist to assess if the current Open RAN network deployment meets the necessary security requirements.
- For MNOs considering new Open RAN deployments: use the checklist as a reference to evaluate, eliminate or reduce security concerns prior to deploying Open RAN in the future.

1 Categorizing security risks of 5G networks

Mobile networks are subject to a plethora of security risks throughout their lifetime. 5G adopts many technologies and architectural concepts from the domain of IT and thus, it needs to take those potential risks into account, for example, related to the increased adoption of cloud computing and AI. These developments are not just constrained to the Core Network, but also affect the Radio Access Network (RAN).

For the purposes of identifying and appropriately mitigating these risks, it is useful to categorize them. One approach is to distinguish the life cycle phase in which each risk commonly occurs. Both 5G deployments and Open RAN deployments share a system life cycle that is typically comprised of the following phases:

1. Analysis & design
2. Implementation & test
3. Sourcing & procurement
4. Integration & deployment
5. Operations & maintenance

Throughout these life cycle phases, different security threats have the potential to affect individual network components or even the entire network deployment. Table 1 illustrates the different categories in relation to the system life cycle outlined above. In the remainder of this report, these categories will be leveraged to analyze Open RAN security risks further and identify associated controls.

	Design flaw	Implementation vulnerabilities	Supply chain / dependency vuln.	Misconfiguration / Lack of hardening	Intentional cyber attack
Analysis & design	●				
Implementation & test		●			
Sourcing & procurement			●		
Integration & deployment				●	
Operations & maintenance				●	●

Table 1: Categorization of security threats

2 Scope and method of research

2.1 Introduction

Globally, mobile network connections have continued to increase ever since mobile networks were introduced, and they are expected to increase further. At the same time, the use cases for mobile networks are expected to expand and mobile networks will become increasingly essential for daily life.

The Radio Access Network (RAN) is responsible for providing the access stratum. Said differently, the RAN's primary task within a mobile network is to provide coverage to mobile devices and using that coverage, enable data communications between connected devices and the core network. Within that system, it is the core network's responsibility to handle that data and to route it to an external party, either directly or through the internet.

Due to its distributed nature of deployment, the RAN accounts for a considerable part of the investment in mobile network deployments. Therefore, it is understandable that mobile network operators would like to understand what the security risks are associated with this investment and how those security risks can be addressed.

This chapter describes a threat modeling and risk analysis approach to Open RAN. It defines the scope of Open RAN, our method, and the key assumptions underpinning the assessment. Finally, it contains a summary of reports previously published by third parties on the topic of Open RAN security and how the present report further extends on this work.

2.2 Scope and limitations

The following chapter describes the threat modeling and risk analysis performed on the Open RAN system. This theoretical exercise is performed to assess the threat surface presented by Open RAN system components and derive appropriate security controls.

Basis for the analysis described in this document are the technical specifications developed by the O-RAN Alliance. Since these O-RAN specifications build on the work done by the 3rd Generation Partnership Project (3GPP), the relevant security specifications for Next Generation Radio Access Network (NG-RAN) are also taken into account. Hence, throughout this document, the term "Open RAN" is understood to mean "Open RAN as per O-RAN and 3GPP NG-RAN specifications". From both of these sources, the latest available document versions as of March 2023 are utilized. Part of this analysis is also a comparison between security risks unique to Open RAN and those that affect RAN deployments in general, incl. traditional RAN. This distinction is intended to help mobile network operators identify genuinely new threats that need to be managed when transitioning to Open RAN.

The high-level architectural diagram in Figure 1 illustrates all network components and interfaces of Open RAN that fall within the scope of this analysis. This diagram, which is created based on

the logical architecture diagram of O-RAN [1], provides a high-level overview of how individual components and interfaces are connected within the RAN, as well as specifies which of them are defined and standardized by 3GPP and O-RAN.

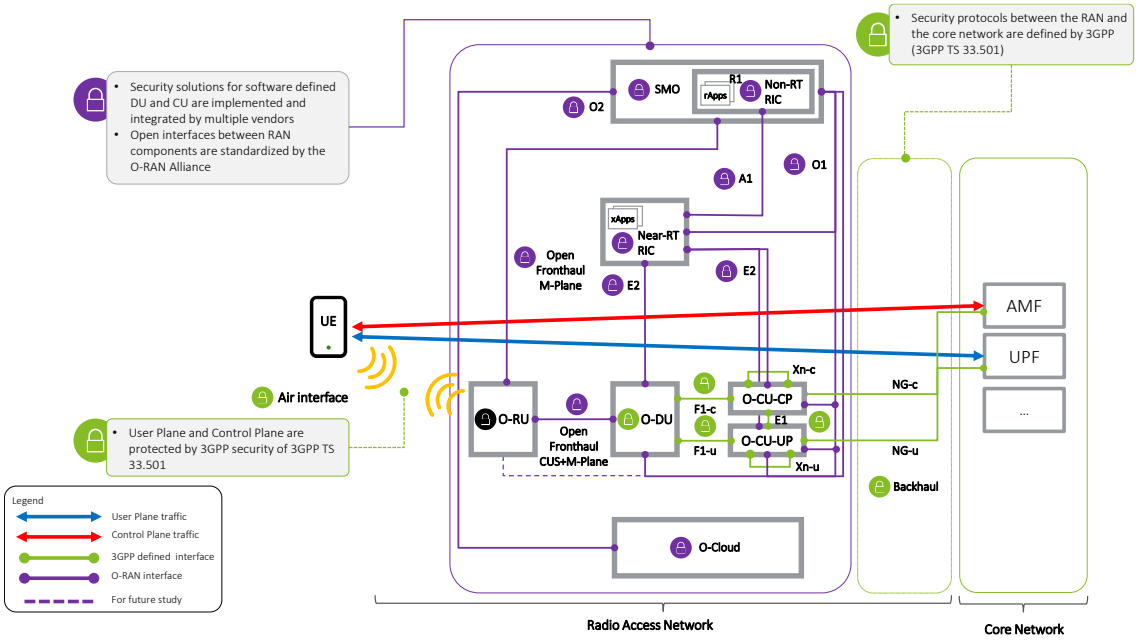

Figure 1: High-level architectural diagram of Open RAN deployments

Out of scope of this analysis are system components outside of NG-RAN (e.g., eNB, 5G Core, User Equipment), system components and interfaces of previous mobile generations (e.g., 4G/LTE), and any proprietary components outside the scope of 3GPP and O-RAN specifications (e.g., specific cloud implementations).

2.3 Assumptions on the Radio Access Network

Open RAN deployments can vary greatly between use cases and therefore, security controls differ as well. The problem this poses, is that the likelihood of a risk will be affected by the type of deployment that is selected. For example, the likelihood of an attack on an isolated deployment within the perimeter of a factory is different than the likelihood of an attack on a public network that leverages public cloud resources. To address that problem, a risk assessment for each type of deployment would need to be performed. Even then, the variation between deployments would limit the value of such a risk assessment.

As such, the first underlying assumption of the risk assessment in this document is as follows.

1. *The Open RAN deployment is assumed to be part of a public mobile network.*

Another assumption has been made on the security controls already present in the network. Specifically, it is assumed that minimum security controls necessary are already in place. Examples for minimum security controls include such fundamental capabilities such as a system inventory, secrets management, and public key infrastructure. The reason for this assumption is that without it, the risk assessment will rate many risks as high, whereas in practice, mitigating measures will be in place (and in some cases mitigating measures themselves are subject to additional risks). As such, the assumption of 'reasonable security' is made to avoid long lists of threats that may be theoretically relevant, but in practice are always mitigated. This assumption is based on expert opinions as well as public data, where available.

2. *Minimum security controls are already present in the mobile network integrating the Open RAN deployment.*

In the following, it is described in more detail what these assumptions mean specifically.

2.3.1 Deployment assumptions

Mobile network operator deployments are far from homogeneous, even within one mobile network. For example, shopping malls, tunnels, remote areas can all have different deployments depending on the local situation. This report focuses on public network deployments that are expected to be most commonly used.

Domain	Assumption
O-RU	- deployed in physically accessible locations, such as on poles, or on roof tops - physically accessible by an attacker by relatively simple means
O-DU	- deployed in a local data center, such as a dedicated building station or in the basement of a building - access to local data centers restricted, but shared with other tenants
O-CU	- deployed in physically secured data centers - only authorized personnel can access premises - data center assets separated for each client
SMO	- deployed in large, physically secured data centers

Table 2: Deployment assumptions of Open RAN components

The risk assessment also includes a comparison between Open RAN and traditional RAN. Because

the term “traditional RAN” is not clearly defined, it is assumed that traditional RAN deployments are comprised of Base Band Units (BBU) and Radio Remote Units (RRU), also called Radio Remote Heads (RRH). The architectural diagram in Figure 2 illustrates the network components in traditional RAN deployments. While this type of deployment implements a non-disaggregated RAN as specified by 3GPP, individual RAN components are often provided by a single vendor, tightly coupled, and rely on proprietary security controls.

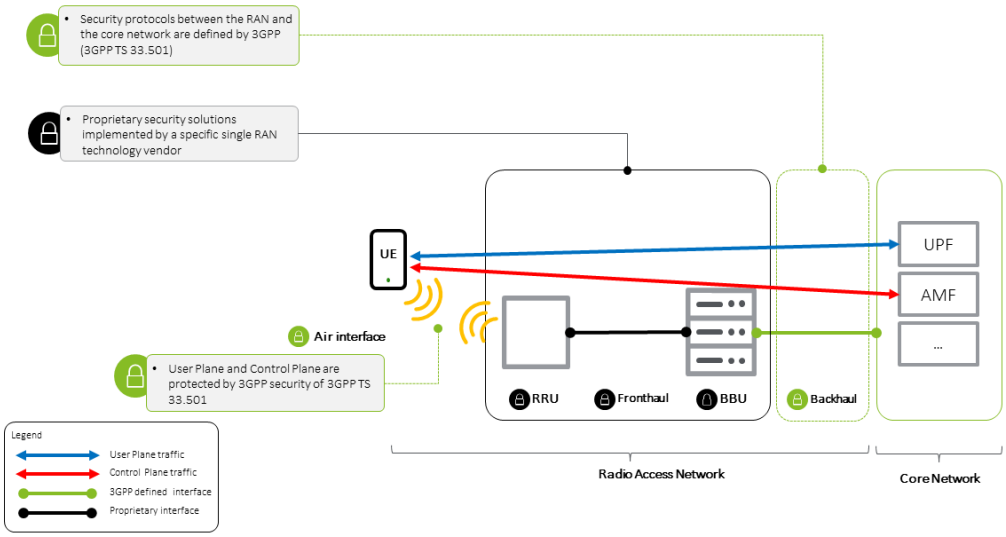

Figure 2: High-level architectural diagram of traditional RAN deployments

With regard to traditional RAN components, the following assumptions have been made. Traditional RAN interface specification is not openly published. So, third parties in the industry cannot proactively discover and address security issues in the interface specification.

Domain	Assumption
RRU/RRH	- deployed in physically accessible locations close to the radio antenna, such as on poles, or on roof tops - connected to the BBU via unsecured Ethernet or Fiber link
BBU	- deployed in physically accessible locations, such as roof tops or separate room inside a building - physically accessible by an attacker by relatively simple means

Table 3: Deployment assumptions of traditional RAN components

2.3.2 Security assumptions

Both 3GPP specifications and O-RAN specifications come with security controls that operators can choose to employ. The reason behind the optionality is that the standards need to work across different geographies, including those that may prohibit or limit the use of encryption or other cryptographic protocols. As such, technical specifications are defined in a way that security can be enabled or disabled, so that standard equipment can be used across the globe. At the same time, this does not mean that each operator will always enable all of the security functionality available in the 3GPP and O-RAN specifications. Operators may opt to not include security features if they find that it hampers performance or that it may not mitigate a significant risk, in their view. For this analysis, the following assumptions are made.

Domain	Assumption
3GPP User Plane	- AS Encryption: Assumed to be turned on - AS Integrity: Assumed to be turned off - Backhaul (NG-U, NG-C) security: Assumed to be turned off
3GPP Control Plane	- NAS Encryption: Assumed to be turned on - NAS Integrity: Assumed to be turned on - SUCI: Assumed to be plain text SUPI - IMSI paging: Assumed to not be used - GUTI: Assumed to be rotated
O-Cloud	- O-CUs are assumed to be deployed on a public cloud
Physical security	- O-RUs are not physically secure - O-DUs are deployed in shared facilities - O-CUs are deployed in a shared data center

Table 4: Security assumptions

As said before, operators do not always turn on all security features of 3GPP for various reasons. As a result, in the table above, AS Integrity protection, Backhaul security, and SUCI are assumed to be turned off. It is the authors view that these security features are the most likely ones not to be used by operators even in developed countries. However, for 5G networks designed and used for critical communications, security can be further enhanced by turning these specific security procedures on.

For the physical security of the O-RAN components assumptions were made based on both physical and design limitations. For example, an RU is more likely to be found on a roof of a building or a pole in a field, or just attached to a ceiling and is therefore assumed to be not physically secure. For the O-DU a slightly more secure shared facility like a locked cabinet in a

building was assumed. Finally, for the CU, the assumption was made that it sits in a larger data center on a public cloud and is therefore reasonably physically secured. For the O-Cloud, the assumption of a public cloud was made for O-CUs only as this seemed reasonable and a reflection of operators teaming up with cloud providers for building out their networks. The important aspect for the analysis, though, is the fact that the O-CU is located in a physically secured environment.

2.4 Risk analysis

Risk is commonly defined as the product of *impact* and *likelihood* of an adverse event, i.e., a threat. Therefore, to get to a risk rating that allows for prioritization, these two variables need to be determined first. For this study, a qualitative assessment is utilized for both impact and likelihood, assigning high-level values LOW, MEDIUM, and HIGH. A quantitative assessment is not feasible due to a lack of available data. Therefore, the assessment is bound to be subjective to an extent. Readers are encouraged to use this document as a general guideline, and make necessary adjustments based on the specific operating environment when determining the security risk of their Open RAN deployment.

2.4.1 Threat identification

First, previously published reports on Open RAN security are reviewed and summarized. Given that the security of Open RAN has been subject of active debate, this initial step helps to establish an overview of security expectations and potential security risks associate to this new deployment approach. Since some of the selected reports also comment on the O-RAN specifications, this review also allows for a comparison of these previous findings with the technical specifications in their current form.

The O-RAN Threat Modeling and Remediation Analysis [2] is the basis for the threat modeling and risk analysis described in this document. It focuses on an analysis of the O-RAN security threat modeling and its remediation measures based on the ISO 27005 standard which provides guidance for risk management. It has also identified relevant security stakeholders, critical assets that include the O-RAN components and interfaces to be protected within the O-RAN system, and threats against the O-RAN components considering threat agents who may manifest a threat and potential vulnerabilities that may be exploited.

In the current version of the O-RAN Threat Modeling and Remediation Analysis, the threats against the O-RAN components are classified into eight categories with consideration to the expanded threat surface from additional functions and interfaces, as well as the Lower Layer Split (LLS) introduced by the O-RAN architecture. In these categories, the decoupling of hardware and software, leveraging virtualization, and the use of open-source components are also considered.

1. Threats against O-RAN system
2. Threats against O-CLOUD
3. Threats to open-source code
4. Physical Threats
5. Threats against 5G radio networks
6. Threats against ML system
7. Protocol stack threats
8. SMO threats

Each threat category contains several threats with unique IDs and threat descriptions that describe how specific vulnerabilities in the O-RAN components can compromise Confidentiality, Integrity, and Availability with specific threats. As an extension of the classification of relevant threats against each O-RAN component, a threat inventory is also developed to provide a mapping between threats, vulnerabilities, and targeted critical assets.

The afore-mentioned eight threat categories consist of a well-defined set of descriptions for individual O-RAN components. However, a number of duplicates are identified. To be specific, the common threat section under the category of threats against the O-RAN system covers a wider range of threats and may also include threats that are covered in other categories. In turn, the result of the threat analysis may be skewed as some threats will weigh heavier because of this duplication. The duplicates should be removed in order to conduct the risk analysis with the underlying skew corrected. To address this issue, deduplication was carried out as following:

- First, based on the O-RAN Threat Modeling and Remediation Analysis, a list of affected O-RAN components and associated threats is compiled to confirm the completeness of the associated threats.
- Second, the list is reviewed to check if duplicate or overlapping threats are mapped to any of the O-RAN components.
- Finally, the specific threats that found to be duplicate or overlapping are removed if they do not describe a unique threat scenario not covered in more general threats.

Next, the STRIDE framework is used to categorize the security threats that have been deduplicated in the previous step. STRIDE is a mnemonic for six fundamental types of security threats a system may be subject to. Each of these security threats relates to a protection goal that it violates, as illustrated in Table 5 below.

Security threat	Protection goals
Spoofing	Authentication
Tampering	Integrity

Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privilege	Authorization

Table 5: Overview of the STRIDE mnemonic

Leveraging a framework such as STRIDE helps to ensure a structured way of identifying security threats and contributes to a better coverage of the resulting model. STRIDE is generally well-suited for performing threat modeling on a (technical) system level making it an appropriate choice for analyzing Open RAN. Alternative approaches exist for performing threat modeling in different scenarios, for example, at an organizational scope.

As noted previously, Open RAN builds on, and extends, the radio access network as specified by 3GPP. For this reason, there may be security threats relevant to Open RAN deployments that do not apply to traditional RAN. As part of this step, it is therefore also assessed whether an identified threat is specific to Open RAN or not.

2.4.2 Risk rating

In order to create a prioritized lists of security risks, it is required to determine impact and likelihood of the threats identified. Given the afore-mentioned dependencies to individual deployment scenarios and the use cases supported by a given Open RAN system, a qualitative assessment is performed. Both impact and likelihood are classified in the generic categories HIGH, MEDIUM, and LOW. Eventually, both impact and likelihood ratings are combined into one risk rating that follows the same classification. The following sections outline how impact and likelihood ratings have been determined.

Impact

The O-RAN Threat Modeling and Remediation Analysis [2] considers the following five factors in determining the severity rating of a security threat:

- Impact on privacy of network subscribers;
- Impact on the basic security properties confidentiality, integrity, and availability;
- Scale of impact, depending on the number of affected O-RUs and/or O-DUs;
- Impact on the Clock Model and Synchronization Topology configurations;
- Adverse impacts depending on whether existing requirements and controls are already defined in the O-RAN requirements specifications.

This approach to determining threat impact poses two issues. Firstly, risk assessments should not

take into account security requirements or controls. Ideally, they are determined as a result of the risk assessment. Even if security controls are considered, they may be able to reduce the likelihood of a given threat, but they cannot affect its impact. Secondly, impacts on privacy and synchronization data are treated as separately from confidentiality, integrity, and availability threats. Privacy is indeed distinct from security, as it concerns not just data protection, but also aspects such as the legality of data processing and the data owner's rights. However, from a purely technical point of view, a privacy impact occurs where the security of personal-identifiable information –such as user data, user location data, or user identifiers – is breached. Therefore, analysis in this report will assume privacy risks as being directly related to threats on network components processing personal-identifiable information. Similarly, any risks to synchronization data are also directly related to threats against components which provide clock and synchronization functionalities.

Considering the above, for the purposes of the risk assessment described in this document, the threat impact rating is determined only by the following ratings:

- Service impact, describing the impact on a single subscriber's session if a threat of confidentiality, integrity, or availability materializes against a given component; and
- Scale of impact, describing the impact on the overall network deployment or subscriber base when a given component is compromised.

These two ratings are distinguished because the compromise of an individual network component may not necessarily have a significant effect on the overall deployment. It is assumed that the primary concern of mobile network operators is to ensure security at the service layer, rather than preventing the compromise of every single component. Due to this fact, more weight is placed on the Scale of impact than on the Service impact rating.

Table 6 illustrated how these two ratings are leveraged to derive one consolidated impact rating per threat.

Impact		Scale of Impact		
		High	Medium	Low
Service Impact	High	High	Medium	Medium
	Medium	High	Medium	Low
	Low	Medium	Medium	Low

Table 6: Impact rating scheme

Likelihood

The O-RAN Threat Modeling and Remediation Analysis [2] determines the likelihood rating of a

threat based on the following four factors:

- Threat event initiation, depending on the capabilities that attackers possess and the potential entry points to exploit a vulnerability to initiate an attack;
- Exposure, which is related to the number of external interfaces and/or services that are exposed to attackers;
- Zero Trust Approach (ZTA), depending on the implementation of a zero trust architecture protecting against attackers; and
- Adverse impacts depending on whether existing requirements and controls are already defined in the O-RAN requirements specifications.

As noted previously, security requirements and controls should not be considered as part of a risk assessment, rendering Zero Trust Approach and Adverse impacts as unsuitable. Instead, the likelihood rating is determined by the following two factors:

- Attacker value, characterized by the assumed value of compromising a given component/interface based on the associated functionality and data; and
- Exposure, characterized by the number of components/interfaces in a typical network deployment

Both Exposure and Attacker value are assumed to have approximately the same influence on the likelihood of a threat. Table 7 shows how the two ratings are combined to determine the overall likelihood rating.

Likelihood		Attacker Value		
		High	Medium	Low
Exposure	High	High	High	Medium
	Medium	High	Medium	Low
	Low	Medium	Low	Low

Table 7: Likelihood rating scheme

Risk

The overall risk rating is determined by impact and likelihood of a given threat. The formula used can be expressed as follows: *Risk= Impact x Likelihood*. The resulting classification is shown in Table 8 below.

Risk		Likelihood		
		High	Medium	Low
Impact	High	High	High	Medium

	Medium	High	Medium	Low
	Low	Medium	Low	Low

Table 8: Risk rating scheme

2.4.3 Risk mitigation

Following the analysis and prioritization of security risks is the documentation of mitigating measures. In a first step, the technical specifications of 3GPP and O-RAN are reviewed to identify essential security controls required for interoperability. These security controls are mapped to the collection of security risks created in the previous stage. For risks that are not addressed by the technical specifications, generic security standards and best practices published by reputable organizations are leveraged, such as NIST or CIS.

2.4.4 Mitigation owners

The present document distinguishes different mitigation owners, i.e., stakeholders responsible for implementing mitigating measures. Specifically, the following roles are assumed based on a life cycle view on the Open RAN system: Open RAN vendor, Infrastructure provider, Network operator (i.e., internal threat actors). Note that these roles can be associated to the same or different stakeholders, depending on the operating model of a given deployment.

	Design flaw, etc.	Implementation vulnerabilities, etc.	Supply chain / dependency vuln., etc.	Misconfiguration / Lack of hardening, etc.	Intentional cyber attack
Analysis & design	OV, MNO				
Implementation & test		OV			
Sourcing & procurement			OV, MNO		
Integration & deployment				IP, OV, MNO	
Operations & maintenance				IP, OV, MNO	*

Table 9: Categorization of security threats, incl. associated mitigation owners

2.5 Previously published views on Open RAN security

2.5.1 BSI – Open RAN Risk Analysis (5GRANR)

In February 2022, Germany's Federal Office for Information Security (BSI) published an Open RAN risk analysis [3]. The authors examine the security risk of Open RAN implementations along five central protection goals (confidentiality, integrity, accountability, availability, privacy) and from the perspective of three different stakeholders (end user, network operator, state/society). The risk analysis performed is based on a qualitative assessment of the likelihood of occurrence (high, medium, low) and does not take into account impact. Different attacker types are considered. Security safeguards that may reduce the identified risks are based on the technical specifications by 3GPP and the O-RAN Alliance. The authors account for optionality of certain security controls in the specifications by considering the best-case, i.e., all optional controls are implemented, and worst-case, i.e., no optional controls are implemented.

The study finds that, at the time of its creation, 3GPP and O-RAN specifications are not sufficiently developed according to "security/privacy by design/default" and "zero trust" best practices, thus exhibiting multiple security risks. In particular, the authors point out the optionality of security controls and ambiguity regarding the mandatory use of security mechanisms. On the O-RAN specifications specifically, it is noted that there are multiple areas of the system that are underspecified with regard to security, incl. system interfaces, O-RAN apps, and the underlying O-Cloud. The authors provide recommendations for improvement.

2.5.2 NIS Group – Report on the cybersecurity of Open RAN

In May 2022, NIS Cooperation Group published a report on cybersecurity implications of Open RAN [4]. The report focuses primarily on two points: security risks with an estimation on the impact Open RAN will have on each of them (Both identified security risks currently associated with traditional RAN, as well as new risks introduced by Open RAN) and potential security opportunities that will be increased by utilizing Open RAN solutions.

The impact of Open RAN on identified security risks is classified by whether the risks are somewhat similar, amplified, or reduced, depending on how the impact changes relative to Traditional RAN. In addition, a new risk classification is also presented in the report, but the potential impact is not identified at the time of its publication.

The authors point out that the concept of Open RAN is still uncertain and under development including its specifications. Specifically, the attack surface is increased due to its new approach, new interfaces, and new types of RAN components that are potentially supplied from multiple vendors. Beyond the security issues, there is also mention of increased dependency on specific stakeholders such as cloud service/infrastructure providers, as Open RAN deployment relies on virtualization and cloudification.

The key areas of opportunity to be improved by Open RAN are analyzed based on the level of potential benefit (high, medium, low), enabling factors, such as the maturity of open interfaces and robust standardization, and associated counter-risks, i.e., conditions that could threaten the potential benefit. It is mentioned that the nature of Open RAN could present opportunities for mobile network operators. For instance, functional disaggregation and interoperability allow the RAN to be customized for specific needs without replacing the entire RAN. Additionally, openly specified interfaces provide visibility and transparency that help with auditing. These opportunities can be realized when certain conditions are met, such as the maturity of open interfaces and robust standardization.

Based on the security risk analysis, the authors highlight the need to take appropriate measures against potential risks. For this purpose, they provide guidance on Open RAN risk mitigations based on the EU 5G toolbox [5], consisting of measures for strategic, technical, and supportive actions.

2.5.3 CISA – Open Radio Access Network Security Considerations

In September 2022, the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) published a white paper on Open Radio Access Network Security Considerations [6]. The authors mainly discuss the benefits of Open RAN and the security considerations associated with implementing Open RAN as specified by the O-RAN Alliance. The authors identify four security considerations associated to Open RAN, specifically:

- Multi-vendor management: While traditional proprietary RANs are single-vendor, the Open RAN architecture will lead to more complexity due to the increased number of vendors.
- Open Fronthaul security: Since the Open Fronthaul is a key element for operating 5G base stations, its security aspects such as Confidentiality and Integrity of data, Availability of interfaces, and Authenticity for the Fronthaul should be considered.
- rApps/xApps security: The introduction of xApps and rApps bring vendor diversity, but at the same time the increased vendor diversity also increases the risk of supply chain issues associated to rApps/xApps vendors.
- AI/ML hardening: AI/ML algorithms in Open RAN components should be continually hardened since they can behave unpredictably or maliciously when be under to data poisoning attacks.

In addition to the above considerations, it is noted that the security concerns for Open RAN regarding applications, open-source software, supply chain, zero-trust, etc., are the same as those found in the industrial sector of information and communications technology (ICT).

The authors conclude that these security considerations can be overcome with continuing efforts

by the Open RAN ecosystem, specifically:

- Operators should be conscious of Open RAN components and functions from different vendors and diagnose and prevent problems in the earliest time.
- Each communication between components should be encrypted and protected properly.
- Secure peering between xApps/rApps should be provided with mutual authentication for confidentiality and integrity while using secure AI and ML data sets and models.
- Open RAN needs to adopt ICT best practices to mitigate the same security concerns as ICT.

2.5.4 IFRI – "Open" Telecom Networks (Open RAN)

In October 2022, The French Institute of International Relations (IFRI) published a white paper [7] which covers both technical aspects of Open RAN, as well as geopolitical considerations. Regarding the technical aspects, the author identifies that the distinguishing factors of Open RAN, namely virtualization, automation, disaggregation, and openness offer benefits that could not be found with traditional closed RAN solutions. For example, the author notes that the benefits of combining virtualization and automation are reduced risks of human error, easier maintenance, faster adaptation, improved network resilience, etc. In addition to the benefits of virtualization and automation, the disaggregation of RAN functionalities promotes a more diverse ecosystem, which reduces the risks of over dependency on a single vendor and allows for a mix of solutions from multiple suppliers. The concept of openness, which consists of three traits –open interfaces, the use of open-source components, and open standards–, may have the potential to increase transparency of network operations and the trust between RAN components as opposed to closed interfaces.

However, regardless of these benefits, the author points out that Open RAN may increase security risks, especially those associated with disaggregation and openness of the system. The disaggregation of RAN functionalities may result in lower-quality performance due to components provided by multiple suppliers. Because not all suppliers are trusted, the performance of the components compared to proprietary solutions and their inherent security vulnerabilities remain in question. Integrating components from different suppliers may also increase configuration complexity and the risks of misconfiguration. Moreover, the attack surface of Open RAN deployments is increased due the introduction of new interfaces and the increased adoption of open-source software. The latter may allow untrusted actors to access and perhaps even modify the source code to introduce security vulnerabilities. Even more uncertainty is created by the fact that its specification body, the O-RAN Alliance, does not disclose publicly the process of how the O-RAN specifications are developed.

2.5.5 NTT Docomo – 5G Open RAN Ecosystem White paper

In June 2021, NTT Docomo published a white paper on the 5G Open RAN Ecosystem [8]. The document discusses the distinguishing factors of Open RAN –namely, open interfaces, virtualization, and intelligence–, and expected benefits from the perspective of mobile network operators. In addition, a brief outlook on NTT Docomo's Open RAN Ecosystem (OREC) project is provided.

Security is only featured in a short section of the report. The authors identify several security issues associated to Open RAN, specifically:

- security risks of open-source software and off-the-shelf technologies;
- increased attack surface due to disaggregated/modular system architecture;
- functional security concerns with newly introduced RAN functions;
- physical attacks, amplified due to distributed network deployments; and
- cloud security risks.

Beyond these technical considerations, process related challenges are also mentioned, such as the increased complexity of multi-vendor management and the security life cycle management of heterogenous Open RAN deployments.

The white paper contains recommendations to mitigate these challenges. These include establishing a holistic security life cycle, from design to operations, that incorporates security by design and zero trust paradigms. This life cycle is expected to be supported by automation capabilities, such as for automated monitoring, response and operations. Because the ecosystem may comprise a number of different stakeholders, the need for a clear separation of roles and security responsibilities is emphasized. The authors further mention opportunities for security improvements due to the nature of Open RAN that should help address the afore-mentioned challenges. Specifically:

- increased control over RAN security for mobile network operators;
- opportunity to mix-and-match security solutions;
- potential for fixing security issues quicker with less overall system impact;
- increased operational visibility;
- greater automation potential; and
- ability to streamline security processes/resources between Open RAN and IT.

The authors conclude that these could achieve an "overall security level far beyond anything existing today".

2.5.6 Summary of previously published views

Contents

Publication	Summary
BSI – Open RAN Risk Analysis (5GRANR)	- Examines the security risk of Open RAN considering five protection goals of confidentiality, integrity, accountability, availability, and privacy and three stakeholders, such as end user, network operator, and state/society - Outlines worst-case and best-case scenario to account for optionality in the specifications - Notes that O-RAN specifications should contain less optionality and more concrete provisions on what is required or not allowed
NIS Group – Report on the cybersecurity of Open RAN	- Outlines common security risks associated to traditional RAN in addition to new security risks of Open RAN and its potential security opportunities - Points out that Open RAN specifications still under development and need to mature further; especially security considerations at an early stage - Highlights the need to take cautious approach to Open RAN transition and provides guidance on Open RAN risk mitigations based on the EU 5G toolbox
CISA – Open Radio Access Network Security Considerations	- Outlines security considerations related to Open RAN component and associated technology, e.g., virtualization and open-source software (OSS), but also looks at Open RAN from multi-vendor management aspect - Identifies security concerns related to applications, OSS, supply chain, and zero trust which are similar concerns as those in the industrial ICT sector - Concludes that concerns can be overcome with continuing effort, if Open RAN adopts established ICT best practices
IFRI – "Open" Telecom Networks (Open RAN)	- Identifies the distinguishing factors of Open RAN, namely virtualization, automation, disaggregation, and openness, and their security benefits - Emphasizes that security drawbacks are still beyond resulting benefits

	- Highlights challenges regarding maturity, security, performance, and transparency of the O-RAN specification process
NTT Docomo – 5G Open RAN Ecosystem White paper	- Outlines distinguishing factors of Open RAN and expected benefits from the perspective of mobile network operators, e.g., reduced TCO, increased operational efficiency, and improved security - Examines security issues associated to Open RAN in terms of technology and process; introduces recommendations to mitigate these challenges

Methodology and key findings

Publication	Identified security benefits	Identified security risks	Methodology
BSI – Open RAN Risk Analysis (5GRANR)	-	- O-RAN development process not following security/privacy by design/default approach - Lack of specification & optionality introduces considerable risks - Rights & roles concept not sufficiently defined - Selection of security protocols does not always follow best practices	- Risk assessment of technical specifications based on qualitative likelihood estimation - Considers five protection goals and three different stakeholders - Distinguishes worst-case/best-case scenarios, based on implementation of optional security controls

NIS Group – Report on the cybersecurity of Open RAN	- Increased supplier diversity (incl. greater role of EU-based suppliers) - Greater interoperability - Improved visibility and transparency - Opportunities associated to technologies that are part of, but not specific to Open RAN, such as, intelligent automation, cloudification and virtualization	- Expanded threat surface - Increased complexity for network fault management - Deficiencies in technical specifications - Increased dependency on infra providers - Impacts on network security and performance due to mix-and-match - Security risks due to resource sharing	- Builds on EU Coordinated risks assessment of 5G - Assesses Open RAN risks in relation to existing risks to traditional RAN deployments - Opportunities are analyzed based on level of potential benefit, enabling factors, and associated counter-risks
CISA – Open Radio Access Network Security Considerations	- For MNOs, Open RAN may result in a more robust supplier ecosystem and networks with increased agility, resiliency, and flexibility - For vendors, Open RAN can lower the barrier of entry & foster innovation	- Changing threat surface due to network disaggregation - Security considerations related to open-source software - Security concerns not unique to Open RAN, e.g., cloud risks, secure virtualization/ containerization, and Distributed Denial of Service (DDoS) attacks	- Considers the broader technology stack (incl. virtualization) and Open RAN life cycle - Focuses on security risks at later life cycle stages, after technical design and specification

IFRI – "Open" Telecom Networks (Open RAN)	- Summarizes technical design principles of Open RAN (i.e., virtualization, automation, dis-aggregation, openness), and resulting security benefits	- Increased risk of mis-configuration and vulnerabilities in low-quality components - Larger attack surface - Potentially greater reliance on unreliable (e.g., open-source) components & vendors - Risk of increased dependency on foreign suppliers	- Focuses on risks in the Open RAN specification development process and supply chain risks rather than detailed technical risks on each component
NTT Docomo – 5G Open RAN Ecosystem White paper	- Greater security control for network operators - Enabling mix-and-match of best security solutions - Possibility to address identified issues faster - Increased visibility, allowing for better incident response - Automation potential - Re-use of IT security processes and resources	- Security issues of open-source software and off-the-shelf technologies - Increased threat surface due to exposed interfaces - Security issues related to added RAN functions - Higher probability of physical attacks - Cloud security issues - Process vulnerabilities	- Assesses challenges and opportunities from a life cycle view on Open RAN - Considers risks related to Open RAN technical components as well as process challenges due to shift in responsibilities

3 Comparison of Open RAN and traditional RAN

3.1 Security risks associated to Open RAN

3.1.1 Result of the threat identification

Following the analysis of the O-RAN Threat Modeling and Remediation Analysis [2] as described in section 2.4.1 (Threat identification), a total of 40 threats have been determined to be duplicated while 82 threats are non-duplicate. That is, duplicate threats are already covered by general threats that may apply to the entire system, rather than individual components/interfaces only. For reference, Appendix A1 contains a list of specific threats that are removed and a mapping to the related general threats retained.

Next, the resulting list of threats has been broken down by their STRIDE categorization and the component/interface affected. Whereas the O-RAN Threat Modeling and Remediation Analysis regularly combines different threat types and affected components into a single threat, this risk assessment distinguishes these aspects. For instance, T-O-RAN-01 describes the general threat related to insecure design or lack of adoption of security controls. As per the O-RAN Threat Modeling and Remediation Analysis, T-O-RAN-01 may affect all components/interfaces and may cause security threats relating to any of the threat types in the STRIDE framework.

By contrast, for the risk assessment described in this document, a distinct threat is created for each affected component and each STRIDE category to calculate the risk rating of each component/interface in a more precise manner. This allows for a more accurate risk rating, since impact and likelihood may vary based on the component/interfaces affected and the threat type in question.

Figure 3 shows an example of how components (Near-RT RIC and O-RU) that may be affected by the general threat T-O-RAN-01 are classified by each STRIDE category. Further elaboration on how each component/interface is rated by a threat impact rating, which is determined by combining the scale of impact and the service impact, and a likelihood rating, which is determined by combining the attacker value and the exposure, will be discussed in section 3.1.2 (Result of the risk rating).

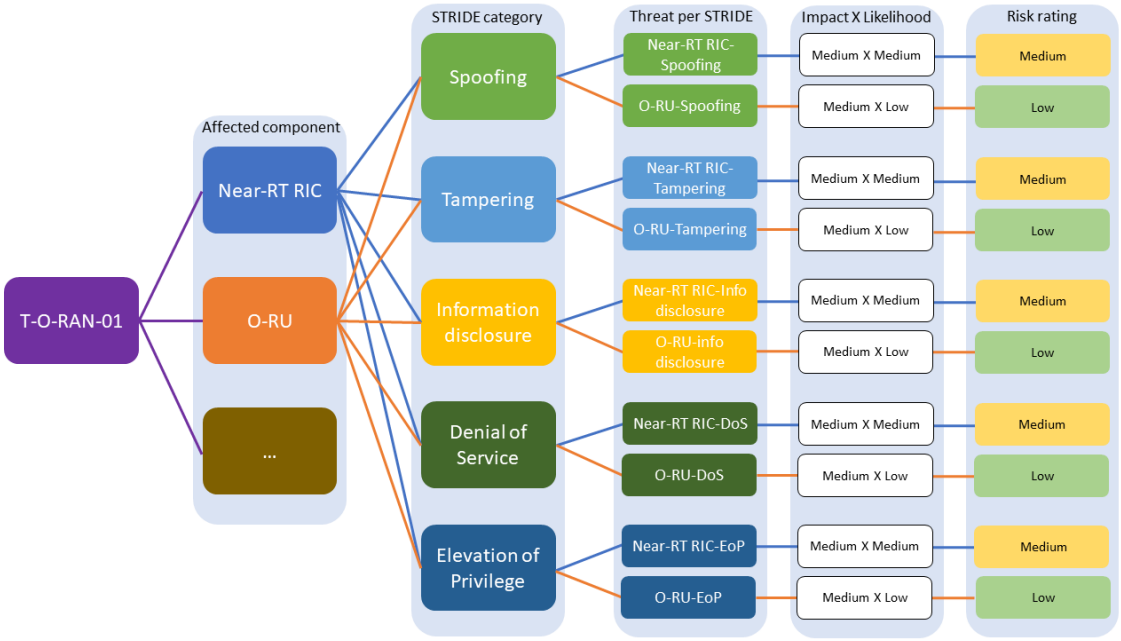

Figure 3: Overview of STRIDE category breakdown for each affected component

As a result of the deduplication and detailed classification of threats per affected component/interface and STRIDE category, a total of 1338 unique security threats have been identified. Based on this information, we can already derive valuable information about security threats that the Open RAN system is exposed to. The analysis shows that the largest percentage of threats (27%) is related to denial of service, i.e., a compromise the availability, as illustrated in Figure 4. This is followed by Tampering (20%), Elevation of privilege (19%), Information disclosure (18%), and Spoofing, which makes up the smallest percentage of identified security threats with 16% of all threats. One exception is the threat classification Repudiation, which has no threats associated to it. Non-repudiation is a legal concept describing that the validity of a fact cannot be denied. As such, its relevancy is limited in the domain of network security.

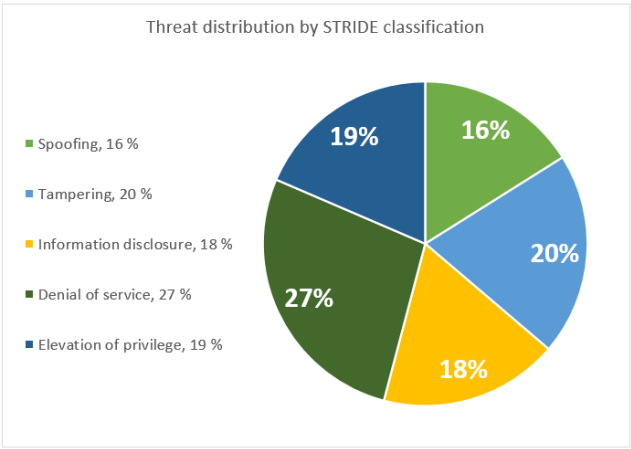

Figure 4: Distribution of threat by STRIDE classification

3.1.2 Result of the risk rating

Based on the threats identified in section 3.1.1 (Results of the threat identification), a qualitative assessment of impact and likelihood is performed for each of the threats to determine their risk. As described in section 2.4.2 (Risk rating), the impact is determined by two aspects: Service impact and Scale of impact. Service impact describes the impact of a breach of confidentiality, integrity, or availability of a given component/interface on a single subscriber's session. The base assumption is that the impact of any security breach is high, unless there is valid reason to lower the rating considering the functionality of a given component/interface and the type of data processed.

Table 10 contains the assigned Service impact ratings for each component and interface. The components/interfaces related to the O-RAN RICs and RAN Apps have been rated "Medium" in each threat category. This includes the Near-RT RIC, xApp, E2 interface, Non-RT RIC, rApp, A1 interface, and R1 interface. The reason for not rating them "High" is that their functionality is primarily related to network optimization tasks. As such, a compromise of either confidentiality, integrity, or availability may result in a potential degradation of service, but no critical service impact, such as a dropped subscriber session. In addition, a "Medium" rating was also assigned to the management components/interfaces SMO, O1, O2, and Open Fronthaul M Plane specifically for confidentiality threats. The rationale behind this rating is that a confidentiality breach of network management data (e.g., configuration parameters, log files, etc.) may reveal sensitive data about the network, but it has no direct service impact. In contrast, a breach of integrity or availability of management components/interfaces may directly degrade service, because certain information exchanges are tampered with or cannot happen at all. No component was assigned lower rating than "Medium" for either confidentiality, integrity, or availability.

Service impact	**Network component / interface**		
Threat type	Confidentiality	Integrity	Availability
High	O-RU, O-DU, OFH CUS, F1U, F1C, O-CU, O-Cloud, XnU, XnC, NgU, NgC, E1	O-RU, O-DU, OFH M, OFH CUS, F1U, F1C, O-CU, O-Cloud, O1, O2, XnU, XnC, NgU, NgC, E1, SMO	O-RU, O-DU, OFH M, OFH CUS, F1U, F1C, O-CU, O-Cloud, O1, O2, XnU, XnC, NgU, NgC, E1, SMO

Medium	Near-RT RIC, xApp, E2, Non-RT RIC, rApp, A1, R1, SMO, O1, O2, OFH M	Near-RT RIC, xApp, E2, Non-RT RIC, rApp, A1, R1	Near-RT RIC, xApp, E2, Non-RT RIC, rApp, A1, R1
Low	-	-	-

Table 10: Service impact

The second aspect affecting a threat impact rating is the Scale of impact. Table 11 shows the assigned Scale of impact ratings for each component and interface. This rating is determined based on how a breach of a single component/interfaces would affect the entire network. If a compromised component/interface has to potential to impact the service in large parts of the network, the assumed Scale of impact is high. In contrast, if the compromise of a component/interface only impacts a small, geographically limited area of the network, the Scale of impact is lower.

Because all O-RAN functions rely on central system components, such as the O-Cloud and the SMO, which are connected to essential management interfaces, these parts of the system are assigned a "High" rating. Comparatively, components such as the O-DU, O-CU, Near-RT RIC, xApp, and associated interfaces only affect a limited area of the network and thus, are rated "Medium". The least impact on the overall network is assumed when individual O-RUs and Open Fronthaul interfaces are compromised and rated "Low".

Scale of impact	Network components / interfaces
High	SMO, O1, O-Cloud, O2, E2, Non-RT RIC, rApp, R1, A1
Medium	F1U, F1C, O-CU, O-DU, Near-RT RIC, xApp, XnU, XnC, NgU, NgC, E1
Low	O-RU, Open Fronthaul M Plane, Open Fronthaul CUS Plane

Table 11: Scale of Impact

Aside from impact, the second factor affecting the risk rating is the likelihood of a threat. As outlined in section 2.4.2 (Risk rating), the aspects considered for determining the likelihood are exposure of a component/interface as well as the Attacker value.

Exposure of a given component or interface is greater for those RAN components deployed in large numbers and insecure locations, providing malicious actors with more opportunities. Table 12 shows the Exposure rating assigned to each component/interface. Fronthaul and midhaul components have been rated "High" because they are assumed to be deployed in physically accessible locations, such as on street poles or on roof tops. Components such as the O-CU and associated interfaces are rated "Medium", because they are assumed to be deployed in local data centers to which access is restricted, but potentially shared between different tenants, as

described in section 2.3.1 (Deployment Assumptions). Lastly, the SMO, Non-RT RIC, rApps and associated interfaces have been assigned a “Low” rating, as they would likely be deployed on network operator premises or in large data centers that are physically secured.

Exposure	Network components / interfaces
High	O-RU, O-DU, O1, OFH M Plane, OFH CUS Plane, E2, F1U, F1C
Medium	O-CU, O-Cloud, Near-RT RIC, xApp, XnU, XnC, NgU, NgC, E1
Low	SMO, rApp, O2, A1, Non-RT RIC, R1

Table 12: Exposure

The Attacker value is determined by the sensitivity of a given component or the sensitivity of data carried over a given interface. Central components that would allow attackers to negatively influence large parts of a network deployment, if compromised, will have a higher value for attackers than those on the far edge of the network. Similarly, interfaces carrying management traffic that potentially contains sensitive information about the network, such as O1 and O2 will be more valuable to an attacker than interfaces carrying User Plane or Control Plane traffic, such as XnU, XnC, NgU, and NgC. A special case is the fronthaul and midhaul interfaces that are assumed to be protected at a higher protocol layer. Specifically, Open Fronthaul CUS Plane, F1-U, and F1-C have been assigned the value “Mitigated”. Due to the mitigation measures described in section 2.3.2 (Security assumptions), it is assumed that information carried over those interfaces would be of no value to an attacker, even if the interface is compromised. Table 13 summarizes the assigned Attacker value ratings for each component and interface.

Attacker value	Network components / interfaces
High	SMO, O-Cloud, rApp, O1, O2, A1, E2, Non-RT RIC, R1
Medium	O-CU, Near-RT RIC, xApp, XnU, XnC, NgU, NgC, E1, OFH M Plane
Low	-
Mitigated	O-RU, OFH CUS Plane, O-DU, F1U, F1C

Table 13: Attacker value

Based on the above ratings for Service impact, Scale of impact, Exposure, and Attacker value, a consolidated risk rating is calculated for each threat previously identified as described in section 2.4.2 (Risk rating). Figure 5 illustrates the distribution of risk ratings as well as the network components/interfaces with the most high-rated threats.

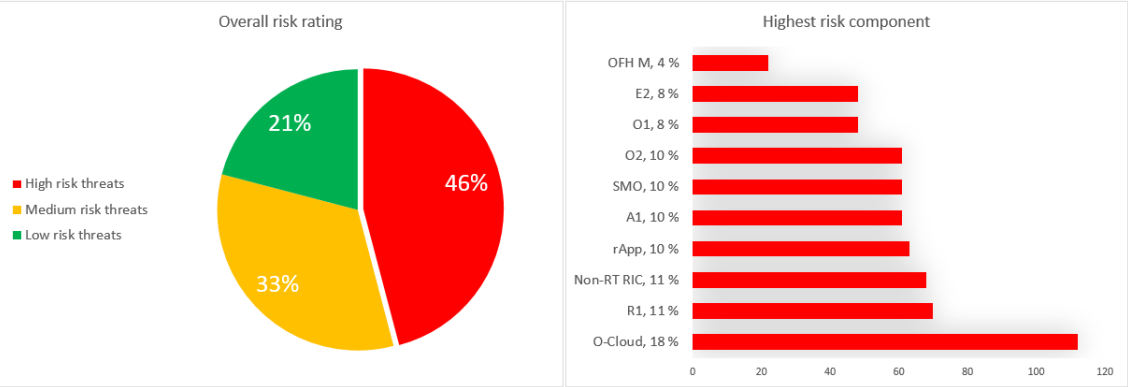

Figure 5: Overall risk rating and highest risk component

The results indicate that 46% of security threats are rated “High”, 33% are rated “Medium”, and 21% are rated “Low”. In the underlying calculations, components/interfaces associated with high-risk threats have high or medium impact and likelihood, and components/interfaces associated with medium-risk threats have medium impact and likelihood. Conversely, components/interfaces associated with low-risk threats are calculated based on low impact and medium likelihood. Importantly, this does not mean that components/interfaces with higher ratings are more important than others, only that failure to protect them is associated with a higher risk of affecting the broader network and network service.

As shown on the right-hand side of , a total of 10 components and interfaces (i.e., O-Cloud, R1, Non-RT RIC, rApp, A1, SMO, O2, O1, E2, and OFH M) are mapped to the most high-risk threats. The O-Cloud is the component connected to the most high-rated risks, accounting for 18% due to its essential role for the Open RAN system. In short, O-Cloud is the underlying infrastructure that provides cloud computing capabilities to host various RAN network functions. As such, O-Cloud is associated with a wider range of threats compared to the other components/interfaces, ranging from threats concerning hardware resources, VMs/containers, the virtualization layer, to threats that also affect other parts of O-RAN, such as software flaws and secure network communication. This is highlighted by Figure 6 which shows the distribution of threats per O-RAN component/interface. Whereas the majority of components/interfaces is affected by approximately the same number of threats, the O-Cloud has a notably higher number of threats associated to it.

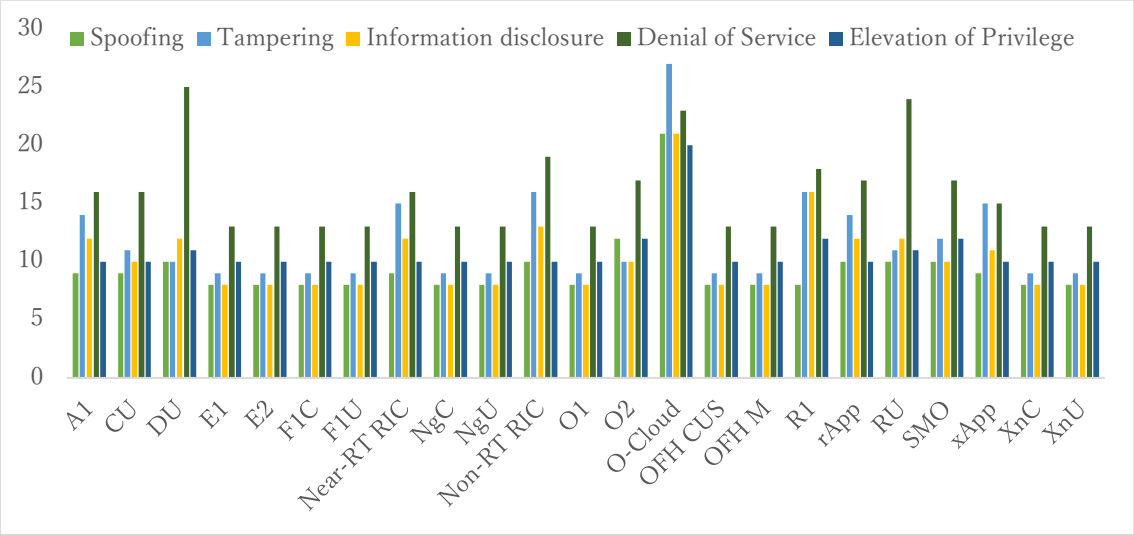

Figure 6: STRIDE distribution for each O-RAN component/interface

Security risks unique to Open RAN

Open RAN is a new approach to deploying radio access networks in a disaggregated, interoperable, and extensible manner. As established before, Open RAN as defined by the O-RAN Alliance builds on established standards defined in the 3GPP technical specifications. Its most important accomplishment is arguably that functional RAN components are clearly defined and communication between them is carried out via standardized interfaces. However, the fact that interfaces are specified in open standards does not mean that, from a technical point of view, Open RAN is truly different from traditional RAN in its internal way of working. Considering the above, determining whether a given security threat is specific to Open RAN is not entirely straightforward. Certain interfaces specified by the O-RAN Alliance may not completely new but were previously implemented by network equipment vendors in a non-standard manner (e.g., fronthaul interface, management and orchestration systems). For example, the Open Fronthaul interface was previously non-standardized. Although the interface itself is one of the key developments of the O-RAN architecture over that of traditional RAN deployments, its specification does not affect the potential security risks that the interface is subject to. Rather, the open specification allows for testing and verification of an interface that previously relied on security by obscurity. Testing and verification may be performed by the MNOs and by any other party, such as security researchers. This public review process can help to improve security. A similar approach can be observed in cryptography. For example, cryptographic algorithms are only considered trusted if their specification is publicly available (e.g., AES).

Taking into account the above, this risk analysis takes an approach in that only those risks associated to the following components and interfaces are considered unique to Open RAN

deployments:

- Near-RT RIC and Non-RT RIC;
- xApps, rApps, and associated Machine Learning (ML) models;
- Interfaces A1, E2, and R1.

In contrast, risks that are associated to the increased virtualization and disaggregation of the RAN are generic and may affect non-Open RAN deployments as well. Namely, O-Cloud, O-CU, O-DU, and related interfaces are considered not unique to this type of deployment. It can be argued that the initiatives that resulted in the O-RAN specifications were the initial driver for these RAN technology changes. However, due to other industry developments such as the proliferation of Cloud RAN and the introduction of functional splits in the 3GPP technical specifications, these are by no means unique to Open RAN. Figure 7 illustrates the percentage of Open RAN specific threats among high-rated risks as well as the overall risk rating of Open RAN specific threats.

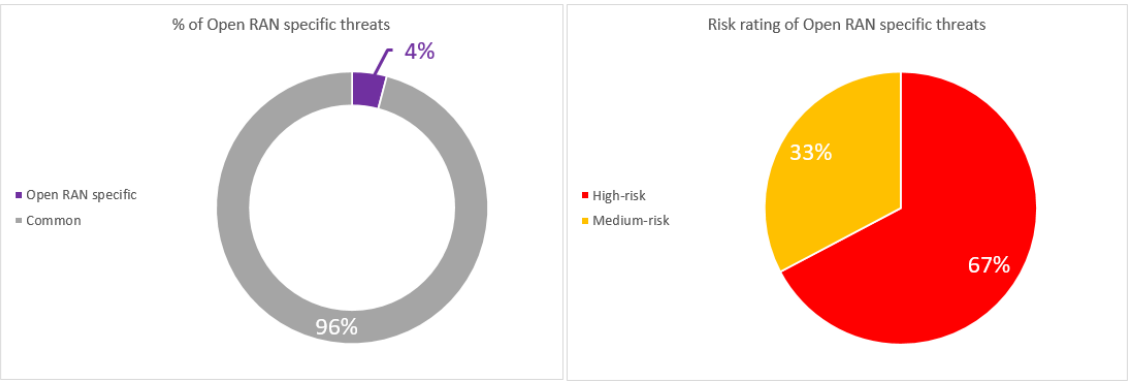

Figure 7: Percentage of high-risk threats and risk rating of Open RAN specific threats

Out of total threats only 4% are considered unique to Open RAN, while the remaining 96% of the threats are common. The total number of threats unique to Open RAN is 55. For reference, appendix A2 contains a list of Open RAN specific threats, along with their corresponding risk ratings. Out of those, 67% pose a high risk to the system, and 33% pose a medium risk. Accordingly, the risk analysis shows that five out of ten highest-risk components/interfaces are unique to Open RAN (i.e., Non-RT RIC, rApp, A1, E2, and R1).

Security risks independent of Open RAN

As an extension to the 3GPP technical specifications, Open RAN shares the majority of general security risks with traditional RAN deployments. Among others, these include design flaws, cloud security risks, network security risks, software security considerations, or risks pertaining to existing RAN components, such as O-RU, O-DU, or O-CU. By and large, none of these are particularly new to mobile network operators, but some of them may be affected by the RAN

deployment approach.

This document uses the assumption that a component or interface is not specific to Open RAN if its functionality already exists in traditional RAN, regardless of whether it was newly specified by O-RAN specifications or not. Therefore, this risk analysis considers the risks associated to the following components and interfaces are considered independent of Open RAN deployments:

- Existing RAN components, such as O-RU, O-CU, and O-DU;
- SMO;
- O-Cloud;
- Interfaces O1, O2, OFH M, OFH CUS, XnU, XnC, NgU, NgC, E1, F1U, and F1C.

Figure 8 illustrates the distribution of threats per life cycle phase, which influences the distribution of mitigation owners. The majority of threats relate to the four life cycle phases after analysis and design. Accordingly, the majority of threats is assumed to be managed by either Open RAN vendors or MNO. A smaller part falls under the responsibility of the infrastructure provider, which is primarily expected to address threats against the underlying platform the Open RAN system is deployed on. Of course, this distribution is not clearly determined and will depend on the operational model chosen by the MNO and the way it distributes security responsibility among other Open RAN stakeholders. For example, part of the mitigations assigned to the MNO may instead be outsources to a system integrator that could take fulfil certain tasks during integration & deployment and even operations & maintenance.

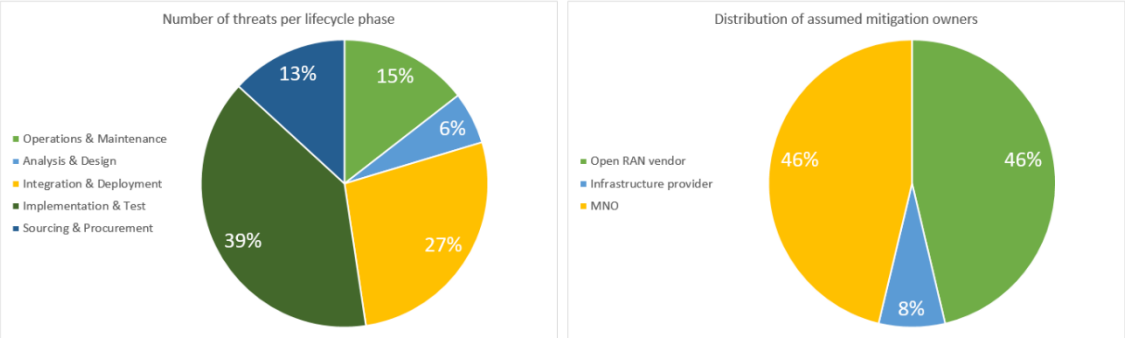

Figure 8: Distribution of mitigation owners

3.2 Potential Open RAN security challenges

Previously published reports identified certain security risks that are introduced or further increased by the introduction of Open RAN, as summarized in section 2.5 (Previously published views on Open RAN security). The detailed view of concrete security risks developed in the current chapter allows for a validation of some of these findings. In the following, previously highlighted

Open RAN threats are discussed in the context of the data obtained from the performed risk assessment.

Increased RAN attack surface

The large number of security threats (i.e., 1338) against Open RAN components and interfaces shows that the system exposes a significant attack surface to malicious actors. However, as previously outlined, very few of these threats are actually new and unique to Open RAN. While the associated components/interfaces may not have been openly specified before, the threats themselves are similar to those affecting traditional RAN deployments. Simply based on the number of Open RAN specific threats, one may conclude that Open RAN only increases the attack surface of the RAN marginally.

AI/ML related risks

The use of AI/ML in RANs for intelligent optimisation and automation is a development specific to Open RANs, which is seen as having benefits such as reducing human error in RANs and reducing TCO.

Although the number of relevant threats in this risk assessment is small (16 out of 1388) and the affected components are limited (Near-RT RICs, Non-RT RICs, xApps and rApps), depending on the scale at which these technologies are used in the network, the security risk may be considered medium to high. AI/ML has new security challenges, such as data poisoning (attacks that alter the training data used to generate deep learning models to make incorrect decisions).

What is more, best practices to address these challenges have yet to be studied and documented by the industry.

However, AI/ML is widely used in society, not only in the networking field, and research is ongoing on security risks and mitigation measures for this technology. The results of such research and best practices in other fields can also be used to mitigate security risks in RANs.

Cloud related risks

With increased centralization of components in the O-Cloud, the RAN becomes more dependent on this common platform providing compute, network, and storage resources to different RAN resources. This introduces a single point of failure that did not exist in traditional RAN deployments. A compromise of the O-Cloud affects any other O-RAN components deployed on top of it, incl. O-DU, O-CU, Near-RT RIC, xApps, and parts of the SMO. This is also reflected by the large number of O-Cloud security threats rated “High” (i.e., 112 or 18%).

While cloud computing risks may not be entirely new to MNOs, moving essential network resources like the RAN into the cloud –instead of business IT applications– could pose significant

challenges.

Unreliable vendors and open-source software related risks

Previous reports highlighted the risk of potentially untrusted vendors and the components supplied by them, particularly xApps and rApps. As third-party extensions to the RAN Intelligent Controllers, the barrier to entry for new, less mature vendors is particularly low with regard to these components. At the same time, the number of security threats associated to them is substantial, at 123 out of 1338. What is more, since the functionality of these components is not clearly defined by the O-RAN specifications, the potential impact of compromised or intentionally malicious xApps/rApps is medium to high. This emphasizes the importance for every stakeholder in the supply chain to analyze and test their technology dependencies and harden the resulting products – both Open RAN vendors as well as network operators integrating network components into a complete deployment.

Another category of untrusted components is open-source software (OSS). Given its widespread use even in commercial solutions, OSS could potentially affect almost any component in the entire Open RAN system. This is highlighted by the fact that there is a large number of threats (i.e., 230 out of 1338) connected to this topic. It is important to note that OSS is not a threat that is unique to Open RAN. Already today, network elements make use of open-source components and network vendors as well as operators have to manage the associated security threats. However, the diversification of suppliers and technology components used in the RAN may make it even more difficult to keep track of all software components, incl. OSS. This introduces additional challenges for testing and hardening in order to ensuring a consistent security posture. Whereas the technology stack of a network deployment supplied by a single vendor may be fairly homogenous, there is a chance for Open RAN deployments to contain multiple different versions of the same software which all need to be hardened appropriately.

Stakeholder management and process challenges

A component-based risk assessment as described in this document cannot yield concrete evidence about potential process challenges associated with the transition to Open RAN. However, due to the addition of new stakeholders in the Open RAN life cycle, it is fair to assume that alignment between different parties will be more complex than a single RAN vendor taking primary responsibility for the security of RAN components, as is the case with traditional RAN. For example, if the transition to Open RAN is accompanied with a move into the cloud, MNOs will likely depend on the infrastructure provider for certain security controls. If specialized service providers are used to support integration and deployment tasks, yet another external dependency is introduced into the Open RAN life cycle. While these external parties can be made responsible for

implementing appropriate security controls, it is important to note that accountability always remains with the MNO. As the party providing telecommunication services and thus, the party bound to regulatory requirements, the MNO is required to ensure that its vendors and service providers are suitable.

Beyond the expected increase in complexity due to additional stakeholders, it is difficult to make generic statements about the process related security challenges introduced by Open RAN. This is because there is no standard way of sourcing, integrating, and deploying Open RAN. Rather, it is up to the MNO to define security roles and responsibilities as part of its operating model and enforce them throughout the Open RAN life cycle.

3.3 Potential security advantages of Open RAN

Similar to the security challenges, some of the previous reports summarized in section 2.5 (Previously published views on Open RAN security) also pointed to potential security opportunities of Open RAN. These include openness and interoperability, virtualization and cloudification as well as automation. While these aspects provide the potential for improvement, it is important to note that security gains will not come automatically but require effort at every stage of the solution life cycle to come to fruition.

Openness and interoperability

Although the disaggregation of RAN functions necessarily exposes interfaces previously contained in a black box, the use of open technical specifications is what allows network operators to test and verify associated security controls. Whereas previously, MNOs had to trust that their RAN vendor to protect non-standard interfaces appropriately, the O-RAN specifications can provide a clearly defined industry standard. For the O-RAN technical specifications to facilitate improvements to RAN security, they need to be unambiguous and contain minimal optionality. In addition, the openness of the interface can make it available for inspection and monitoring in live environments as well; this provides increased opportunities for security monitoring and detecting malicious activity.

Virtualization and cloudification

As the risk analysis shows, the majority of significant security risks are associated to the O-Cloud, which includes the infrastructure, the virtualization layer, and virtual deployment units (i.e., virtual machines and containers). At the same time, addressing security threats to these lower layers of the technology stack in a centrally and in a *de-facto* standardized manner can improve the security posture of large parts of the deployment. While in traditional RAN, platform security needed to be addressed separately for each deployment site, these issues can

be taken care of much more efficiently when deploying in a cloud environment. However, doing so also requires streamlining of the technology stack. For example, if Open RAN components require different virtualization platforms, depend on specific hardware support, or a certain operating system, it may be difficult to fully leverage the cloud benefits.

Automation

With Open RAN comes the potential to automate a lot of manual tasks, in part thanks to new functions such as the RAN Intelligent Controllers and associated RAN Apps, but also due to the shared cloud platform which can help to improve operational visibility and configuration management. However, one should not expect automation to be a feature provided "out-of-the-box". Considering that Open RAN is also expected to lead to a diversified supplier ecosystem, ensuring full interoperability to the level of intelligent automation will require significant integration efforts. Without RAN technology suppliers filling this role, it will be on MNOs –or specialized system integrators on behalf of them– to manage this integration.

Mitigation of supply chain risk and cost reduction

In conventional vertically integrated RANs, it is difficult to change only some components such as CU/DU/RU to another vendor's equipment because the equipment configuration includes each vendor's own interfaces. If this vendor lock-in situation persists for a long time, it is assumed that the specifications and operational methods of base stations will become increasingly 'black boxed'. Furthermore, as the procurement of products is dependent on a specific vendor, if procurement from that vendor stagnates or is disrupted for some reason, there is a potential for so-called supply chain risk, in which the entire service may become unavailable.

Open RAN, on the other hand, not only eliminates vendor lock-in and reduces supply chain risk by making the interfaces open, but also allows operators to build networks at lower prices than vertically integrated RANs due to the price competition principle.

4 Risk mitigation measures

As discussed in the previous chapter, Open RAN is affected by many of the same security risks as traditional RAN deployments. Beyond these common security risks, there are also those which are either new or more pronounced due to Open RAN, such as AI/ML related risks and cloud security risks. The O-RAN technical specifications already provide certain security requirements to mitigate some of these risks. One example is the O-RAN Security Requirements Specification [9].

This chapter considers all identified risks, not just 4% of risks (55 risks) and describes an analysis of the O-RAN documents carried out to determine the coverage of the security requirements and controls defined by the O-RAN Alliance. Moreover, supplementary mitigating measures based on established industry standards and best practices are documented for each phase of the Open RAN life cycle.

4.1 Mitigation measures defined by O-RAN specifications

4.1.1 Specification analysis

Similar to the risk analysis described in Chapter 3, the analysis of mitigating measures is conducted based on the O-RAN specifications, specifically, the O-RAN Threat Modeling and Remediation Analysis [2] and the O-RAN Security Requirements Specification [9] . The purpose of this analysis is to assess the coverage of security requirements and controls defined by the O-RAN Alliance with regard to the threats identified in section 3.1 (Security risks associated to Open RAN). This way, potential control gaps can be identified which may need to be addressed by supplementary mitigation measures.

In the first step of this analysis, the relation between O-RAN security principles and O-RAN components/interfaces is assessed. Security principles, defined in the O-RAN Threat Modeling and Remediation Analysis, are goals to be achieved for the protection of the O-RAN system and the data processed. As such, they outline high-level security measures to address the threats discussed in section 3.1.1 (Result of the threat identification). Table 14 shows the list of security principles.

ID	Security Principle	Description
SP-AUTH	Mutual Authentication	A mutual authentication protection with a unique identifier and one or more credentials should be implemented.
SP-ACC	Access Control	An access control protection is recommended to prevent unauthorized access to the system should be implemented
SP-CRYPTO	Secure cryptographic, key management and PKI	It is recommended to use secure and unbroken cryptographic schemes and protocols, a reliable PKI for authentication, and certificates should be issued by a trusted Certificated Authority (CA). A secure key management of O-RAN keys should be also implemented to manage all steps of the key life cycle.
SP-TCOMM	Trusted Communication	Integrity, confidentiality, availability, authenticity, and replay protection of data in transit should be ensured.
SP-SS	Secure storage	Integrity, confidentiality, availability of data at rest should be ensured.
SP-SB	Secure boot and self-configuration	A secure boot process through establishing a chain of trust should be implemented to ensure the security of all layers from the underlying hardware, firmware, and configuration.
SP-UPDT	Secure Update	A secure update management process should be in place, including continuous monitoring and patching.
SP-RECO	Recoverability & Backup	A secure recoverability process and backup system should be implemented to prepare against malicious attacks.

SP-OPNS	Security management of risks in open-source components	It is recommended to apply industry coding best practices, maintain SBOMs, and perform security analysis to mitigate the risk of open-source vulnerabilities.
SP-ASSU	Security Assurance	Security assurance of hardware and software used in the Open RAN system should be pursued (e.g., 3GPP SCAS and the security requirements and test cases provided by the O-RAN Alliance).
SP-PRV	Privacy	Privacy of subscribers' information should be ensured.
SP-SLC	Continuous security development, testing, logging, monitoring, and vulnerability handling	A CI/CD process should be integrated along with continuous testing, logging, monitoring, and vulnerability management.
SP-ISO	Robust Isolation	Security isolation should be ensured for all resources used in the O-RAN system.
SP-PHY	Physical security	The O-RAN system should be housed in a physically secure environment and protected against threats from physical access.
SP-CLD	Secure cloud computing and virtualization	Protection of underlying hardware, firmware and virtualization software should be implemented.
SP-ROB	Robustness	Robustness of software or hardware resources, as well as the cognitive radio channel should be ensured.

Table 14: Security principles

The most recent version of the O-RAN Threat Modeling and Remediation Analysis contains a mapping between security principles and security threats (e.g., the general threat T-O-RAN-01 relates to SP-UPDT, SP-ASSU, and SP-SLC). The mapping appears to be incomplete, as it only covers 83 of the 122 identified security threats[1]. The document does not provide details on how

[1] The following steps of the assessment are based entirely on the contents of the most recent version of the O-RAN Threat Modeling and Remediation Analysis. The existing mapping between security threats and security principles has not been completed.

each security principles addresses the individual threats.
In order to assess the coverage of security requirements and controls defined in the O-RAN specifications per component, it is necessary to establish a connection between security principles and O-RAN components/interfaces. Although the current version of the O-RAN Threat Modeling and Remediation Analysis does not contain this information, such a mapping can still be performed via the security threats that are meant to be addressed by the security principles and that affect certain O-RAN components/interfaces.

In the second step of this analysis, the security principles are correlated to the related security requirements and security controls. The O-RAN Security Requirements Specification defines a set of security requirements and associated security controls to protect O-RAN components and interfaces. These comprise both specific requirements on O-RAN components and interfaces as well as general requirements that are applicable to the entire O-RAN system. Although the document states that the security requirements are based on security principles, no direct mapping is provided. The connection between the two was established retroactively as part of this analysis in order to assess the coverage of security requirements and security controls. The correlation with security principles was performed based on the content of the security requirements and security controls using professional judgement.
For instance, if a given component/interface is connected to the security principle “SP-AUTH”, in this analysis mutual authentication protection was derived as the relevant security requirement and implementing TLS/mTLS was determined to be the corresponding security control to address the security requirement.

In the third and final step of this analysis, the result of the previous two steps is used to determine the coverage of the security requirements and controls as they pertain to (1) security threats in different life cycle phases and (2) individual O-RAN components and interfaces.

The process described above is illustrated by Figure 9 Security threats are linked to an affected component/interface, which is in turn connected to related security principles. From security principles, security requirements are derived which are addressed by security controls. For example, the A1 interface is affected by a variety of potential security threats, as shown below:

- threats against open-source code (T-OPENSRC-01, T-OPENSRC-02, T-OPENSRC-03);
- general threats against the entire O-RAN system (T-O-RAN-01, T-O-RAN-02, T-O-RAN-03, T-O-RAN-06, T-O-RAN-07, T-O-RAN-08, T-O-RAN-09); and
- physical threats (T-PHYS-01).

The security threats affecting the A1 interface are connected to the security principles SP-AUTH, SP-ACC, and SP-TCOMM, which map to the existing security requirements REQ-SEC-A1-1 and REQ-SEC-A1-2. Finally, the security controls SEC-CTL-A1, SEC-CTL-A1-2, and SEC-CTL-A1-3 address the security requirements.

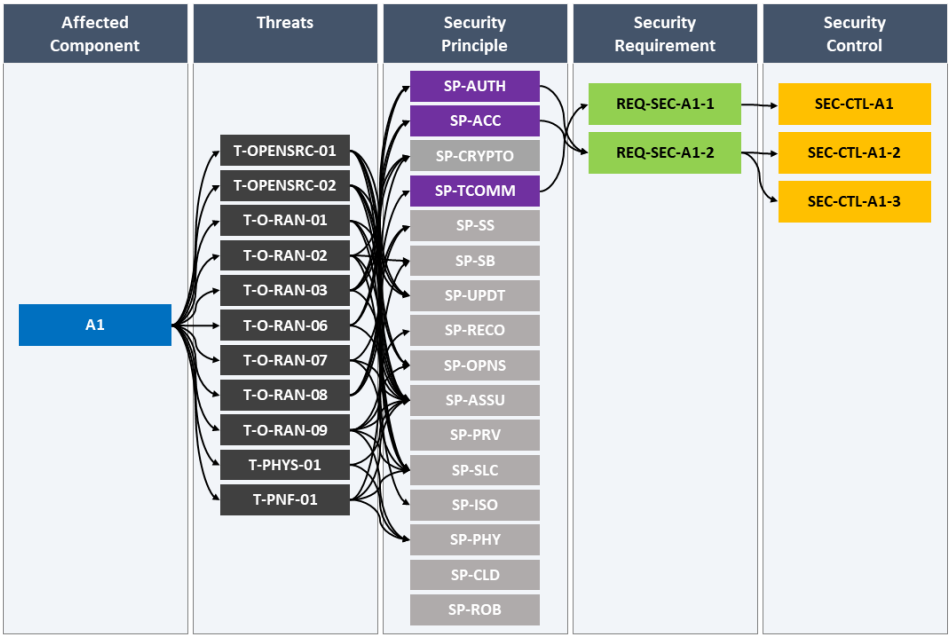

Figure 9: Mapping processes of the specification analysis

4.1.2 Analysis results

Coverage of O-RAN life cycle phases

Based on the analysis described in 4.1.1 (Specification analysis), the affected components and interfaces are found to be subject to multiple identified threats, and as a result, several security principles have been linked to these components and interfaces, with some overlap. However, not all security principles associated with these components/interfaces could be linked to relevant security requirements due to incomplete documentation of the security requirements in the O-RAN Security Requirements Specification. At this stage, the security requirements primarily focus on the following security principles: SP-SCC, SP-AUTH, SP-TCOMM, SP-SB, SP-SS, SP-CRYPTO, SP-UPDT, SP-ASSU, and SP-CLD. In particular, the majority of security requirements pertain to SP-ACC, SP-SB, SP-TCOMM, and SP-CLD. As previously mentioned in Table 14, security principles SP-ACC and SP-TCOMM aim to ensure the confidentiality, integrity, authenticity, and availability of data being transmitted between components, with SP-SB for secure boot protection, and SP-CLD for protecting the underlying O-Cloud environment. For instance, a requirement to achieve SP-TCOMM described in the O-RAN specifications is the mutual authentication of communication

between xApps and Near RT RIC platform APIs. While the listed security principles have corresponding security requirements, others such as SP-PRV on privacy aspects lack such security requirements.

Similarly, the relation between security requirements and controls appears to be incomplete. Ideally, it should be possible to trace back each security control to a specific security requirement that is addresses. However, such a clear mapping between controls and requirements is not always possible, based on the current version of the O-RAN specifications. In some scenarios, more than one control is needed to fully address a broad security requirement (e.g., Both mTLS and OAuth are needed to address the requirement for mutual authentication and authorization of an interface). Moreover, certain security requirements have no corresponding security controls at all.

As described in section 4.1.1 (Specification analysis), the security requirements are categorized into two main types: specific requirements for individual O-RAN components and interfaces, and general requirements, to which the O-RAN document refers to as transversal requirements. The focus of the specific requirements is the design of individual components and interfaces. That is, all of them relate to the Analysis & design phase of the Open RAN life cycle. In contrast, transversal requirements are phrased more broadly and apply across the entire O-RAN system. The O-RAN document in the latest version outlines seven groups of transversal requirements, including software bills of material (SBOM), network protocols and services, and robustness of common transport protocols. Each group includes a number of requirements that are applicable to later phases of the life cycle. For example, the requirements associated with the SBOM are most relevant to the Sourcing & procurement phase, while documentation of a list of protocols supported on the O-RAN components and disabling the unused protocols can be applicable to both Sourcing & procurement and Integration & deployment phases. Meanwhile, robust implementation is a requirement for the Implementation & test phase. The O-RAN Security Requirements Specification also provides a brief explanation of the importance of addressing the transversal requirements. However, the document does not specify concrete security controls in order to do so. Furthermore, no explanation is provided on the criteria used to select these requirements, or the responsibilities of different stakeholders for their enforcement.

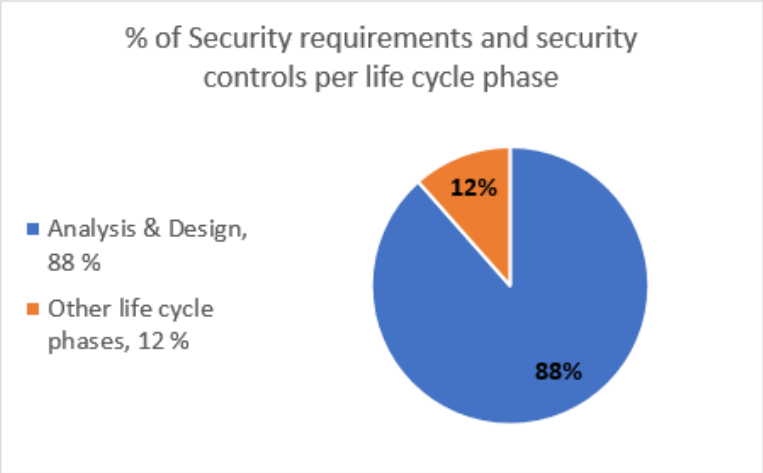

Figure 10: Percentage of Security requirements and security controls per life cycle phase

Figure 10 illustrates the distribution of security requirements and security controls over different phases of the Open RAN life cycle. With 88%, the majority relates to the Analysis & design phase. The afore-mentioned transversal requirements account for the remaining 12%, which address later life cycle phases. This finding is expected, as technical specifications –such as those developed by the O-RAN Alliance and 3GPP– are primarily concerned with ensuring an interoperable design of system components and associated security requirements and controls. Security requirements and controls beyond that, which are often deployment specific, are usually less suitable to be addressed in specifications that apply to the industry as a whole.

Coverage of O-RAN components and interfaces

Aside from the life cycle perspective, the existing security requirements and controls are further assessed based on the O-RAN components and interfaces covered. Figure 11 shows the O-RAN components and interfaces for which dedicated security requirements and security controls have been defined. Note that this view does not take into account the afore-mentioned transversal requirements, which apply across multiple components/interfaces.

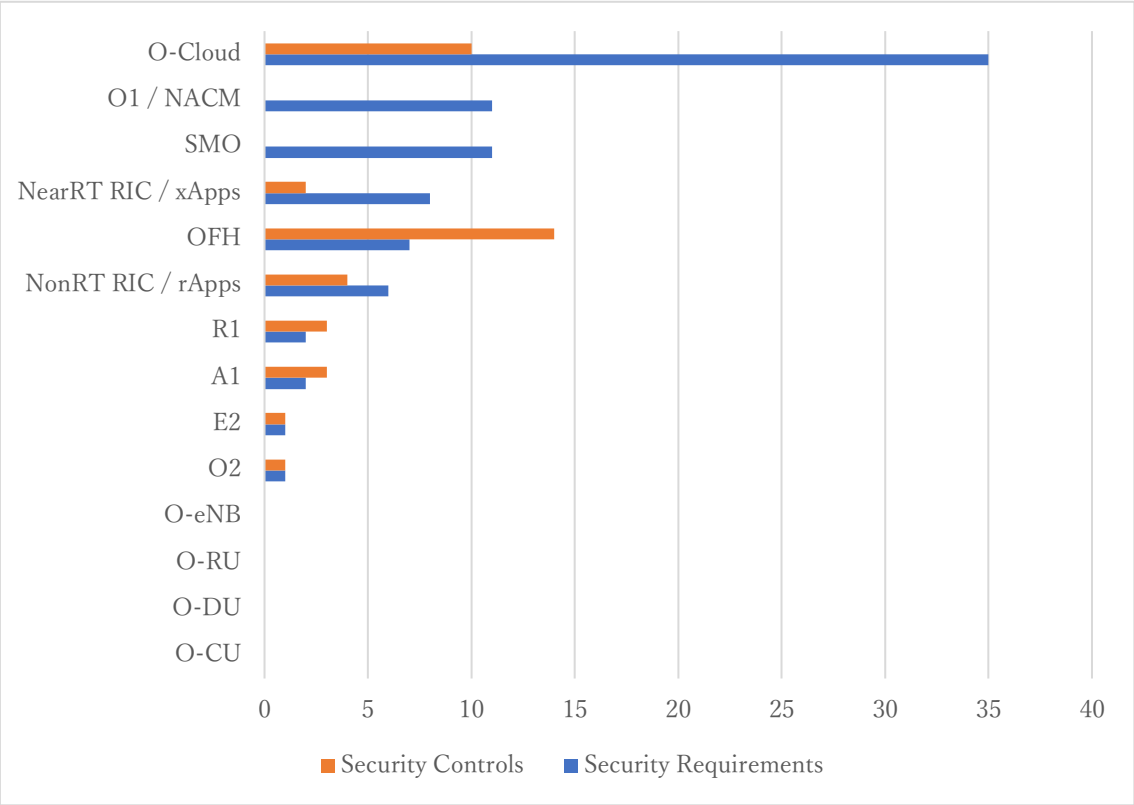

Figure 11: Number of security requirements and controls per O-RAN component/interface

The data shows that the O-RAN specifications define requirements and controls for most of components/interfaces that are affected by high-risk threats as per the risk assessment in section 3.1.2 (Result of the risk rating). This includes the O-Cloud, Non-RT RIC, rApps, and the interfaces O1, O2, R1, A1, E2, and Open Fronthaul. Aspects concerning components and interfaces defined by 3GPP are not covered by the O-RAN specifications, such as the mid-haul interfaces F1 and E1. However, the specification suggests that additional requirements and controls may be defined in the future for O-RU, O-DU, O-CU, and O-eNB.

The largest number of security requirements and controls defined so far focuses on the O-Cloud. In total, there are 35 security requirements and 10 security controls defined for this component. Just as the security threats analyzed in section 3.1 (Security risks associated with Open RAN), these apply not just to the cloud environment itself but also the virtualized workloads, for example, requirements on how to secure software images. Specifically, the O-RAN Security Requirements Specification outlines seven areas associated to the security of the O-Cloud: Generic requirements, Software Package Protection at the O-Cloud Network Functions and Applications Layer, Software Package Protection at the O-Cloud Infrastructure Layer, O-Cloud Virtualization and Isolation, Secure update, Secure storage of cryptographic keys and sensitive data, and Chain of Trust. With

the exception of Software Package Protection at the O-Cloud Infrastructure Layer, security requirements and/or controls have been defined for all of them.

Security requirements defined for the management interface O1 focus primarily on network protection at transport layer, the NETCONF protocol, and the associated network configuration access control model (NACM). While the latter two are needed to enforce access control, Transport Layer Security (TLS) ensures confidentiality, integrity, and mutual authentication. Which TLS version to use and how to profile the protocol is defined in the dedicated O-RAN Security Protocol Specifications [10].

The SMO, also identified as one of the high-risk components, is addressed by 11 security requirements in the O-RAN specifications. Notably, these requirements focus solely on securing event logs in SMO at this point. This partial coverage of SMO security aspects highlights that the O-RAN Security Requirements Specification is still under development. In fact, an Editor's Note explicitly mentions that the same section is to be updated in the future.

The 14 requirements and 6 controls defined for the RAN Intelligent Controllers and associated RAN Apps primarily relate to authentication and authorization, the protection of information exchanged between these components, and the ability to recover from DDoS attacks.

The Open Fronthaul interface is addressed by generic requirements for the point-to-point LAN segment as well as dedicated requirements and controls for each traffic plane carried over this LAN. For the Synchronization Plane, requirements and controls are defined to protect the authenticity and integrity of time information and to enable redundancy of time sources. With regards to the Management Plane, the security requirements specification points to the O-RAN Management Plane Specification [11] for security requirements and controls. No security requirements or controls are defined for the User Plane of Open Fronthaul, since it is protected by the PDCP protocol, as also described in section 2.3.2 (Security assumptions) of this document.

4.1.3 Summary of O-RAN defined mitigating measures

The following key findings have been derived from the analysis of mitigation measures defined by O-RAN specifications:

- The O-RAN specifications primarily address Analysis & design and thus, can only provide limited protection throughout the Open RAN life cycle.
- The O-RAN specifications do not contain details on how each Security Principle addresses the identified security threats.
- Several security requirements lack corresponding controls and vice versa. As a result, not all security principles are covered by security controls.

While the limited scope of industry-defined technical specifications is to be expected, the analysis

shows that the specification of O-RAN security requirements in particular is still a work in progress. Firstly, it is positive that the O-RAN Alliance utilizes a structured approach for the definition of security requirements and controls, based on high-level security principles. However, the specifications lack sufficient detail that allows readers to retrace how these elements relate to each other. Secondly, missing content in a number of document sections in the Security Requirements Specification [9] as well as corresponding Editor's Notes highlight that the current version of O-RAN specifications still contain obvious gaps. Thirdly, the security requirements and controls defined so far are not always consistently marked as such and are spread across different documents. While the Security Requirements Specification captures most security requirements and controls and highlights them explicitly, centralizing requirements and controls contained other documents (e.g., O-RAN Management Plane Specification [11]) could go a long way to further improve the specifications.

The above findings highlight the necessity to describe supplementary controls, beyond those defined in the technical specifications, to ensure a comprehensive controls framework during all stages of the Open RAN life cycle, incl., Implementation & test, Sourcing & procurement, Integration & deployment, and Operations & maintenance. In this document, the readers can secure their posture by implementing the mitigation measures in the next section 4.2 (Supplementary mitigation measures) and utilizing the checklist in the Appendix.

4.2 Supplementary mitigation measures

To supplement the security requirements and controls in the O-RAN specifications, this section provides recommendations for securing the Open RAN system beyond the technical specifications. The mitigating measures described in this section are based on industry-standards and best practices and grouped by the life cycle phase in which they would typically be used. Grouping measures by their life cycle phases allows for an estimation of the associated mitigation owners and relevant security threats. Although the roles and responsibilities in the Open RAN life cycle may shift depending on the agreement between the involved parties, as a whole, the following mitigating measures can help to establish a robust security posture for the Open RAN system.

4.2.1 Analysis & design

General statement

The Analysis & design phase is the first step in every system life cycle. It is here that requirements on functionality and security are determined, system components and interfaces are defined, and the high-level system architecture is developed. In the case of Open RAN, some of this work is done by industry stakeholders participating in the development of the O-RAN technical

specifications. However, the design work performed internally at Open RAN vendors and MNOs may also be considered part of this phase, incl. the design of specific Open RAN network products or that of security controls in the network which are usually not standardized, for example, identity management, log collection, and monitoring.

During this phase, Open RAN vendors have a primary responsibility to securely design Open RAN components that can serve as the foundation for a strong security posture in the final product that will be developed and implemented in later phases. Meanwhile, MNOs need to define their security architecture and requirements to ensure the desired security capabilities and outcome. What sets Open RAN deployments apart is an increase in flexibility, which also extends to security controls. MNOs may choose to simply utilize the security controls provided by their RAN vendors as they do in traditional RAN deployments. Alternatively, they also have the option to turn to specialized security vendors or leverage controls provided by other parties, such as the infrastructure provider. What is more, RAN (security) capabilities may further be extended using third-party xApps and rApps.

Compliance with O-RAN and 3GPP specifications

The technical specifications by 3GPP and O-RAN Alliance provide the basis for securing network components and interfaces. While O-RAN specifications focus on O-RAN components/interfaces specifically, the scope of 3GPP specifications goes beyond just the RAN. One particularly important specification is 3GPP TS 33.501 [12], which defines security aspects for the 5G System, including network security requirements, security procedures, and security protocols. 3GPP TS 33.210 [13] goes into further detail, specifying how to profile security protocols. Together, 3GPP and O-RAN technical specifications provide the foundation for securing interfaces required to ensure interoperability between Open RAN components. While the technical specifications already cover many security aspects, it is important to consider how to improve them further and to recognize that technical specifications can only ever be a starting point for a comprehensive security framework. In addition, MNOs, Open RAN vendors, and other stakeholders also need to consider more widely adopted industry standards and best practices.

Utilization of CSRIC best practices

The US Communications Security, Reliability, and Interoperability Council VIII (CSRIC VIII) [14] recently published a report on “challenges to the development of ORAN technology and recommendations on how to overcome them”, outlining recommendations both for the O-RAN industry as well as specific stakeholder groups (e.g., network operators). As far as the design of O-RAN technology is concerned, CSRIC VIII recommends the industry to strive for improvements to the technical specifications and industry standards, incl. the Open RAN security specifications and “test specifications for xApps and rApps to ensure secure integration into the RIC platforms and protection of sensitive data”. It specifically highlights the following best practices related to

the design and implementation phase of Open RAN system components:

- Open RAN implementations should be based on the principles of Zero Trust Architecture (ZTA).
- Open RAN architectures should implement defenses to prevent Adversarial Machine Learning (AML) attacks.
- Putting Security at the core of the Software Development Life Cycle (SDLC) by utilizing best practices such as NIST DevSecOps [15], NIST SSDF [16], BSA Framework for Secure Software [17], or SAFECode [18].

Utilization of NIST CSF and NIST 800-53 best practices

Other publications, such as the NIST Cybersecurity Framework (CSF) [19], can be utilized to supplement technical specifications for telecom. The CSF provides comprehensive guidelines and best practices to help organizations enhance their security posture and manage and minimize security risks effectively. The framework is designed in a way that it can easily integrate with the security processes already in place within any organization, regardless of industry. It identifies five core functions that organizations should perform to manage the cybersecurity risks, which are Identify, Protect, Detect, Respond, and Recover. Each function includes specific activities designed to achieve each function (e.g., Risk assessment under the Identify function), a set of results for each specific activity (e.g., Asset vulnerabilities are identified and documented when the risk assessment is performed), and references to other resources that are most frequently referenced during the framework development process, for example, the Controls defined by the Center for Internet Security (CIS). The CIS Controls are a comprehensive set of guidelines that outline necessary security controls an enterprise needs to put in place to protect against cyberattacks. The importance of each security control is described along with requirements, procedures, and associated tools. O-RAN Technical Reports which document studies performed on the security of individual O-RAN components also recommend the use of CIS Controls along with several security guidelines and best practices (O-Cloud [20], SMO [21], shared O-RU [22]). Alternatively, NIST 800-53 [23] may also be utilized to identify and define concrete security controls. The document, which is specifically recommended for strong security controls in the afore-mentioned O-RAN Technical Reports, outlines recommended security and privacy controls for federal information systems. Controls are classified into families (e.g., Access control) and can be viewed as description of protection capabilities appropriate for achieving the specific security and privacy objectives of the organization. The O-RAN Technical Reports highlights the following NIST 800-53 control families related to security controls for Open RAN system components:

- Access Controls;
- Risk Assessment;
- System and Communications Protection; and

- System and Information Integrity.

The O-RAN Technical Reports do not provide a rationale for how the above recommendations are derived. Given the comprehensiveness and the broad range of controls of the NIST publication, careful attention is required to determine which control families are applicable.
Open RAN vendors and MNOs can utilize NIST and CIS frameworks to assess whether sufficient security controls are in place, or as a basis for creating more specific and detailed security controls.

4.2.2 Implementation & test

General statement

In the Implementation & test phase, individual components of the Open RAN system designed previously are developed and tested to verify that they meet the identified security requirements. The purpose of testing during this stage of the system life cycle is to ensure that the individual components implement the required security controls, are developed according to secure coding practices, and are free of known vulnerabilities.
Open RAN differs from traditional RAN deployments in that it introduces new network functions, interfaces, and deployment options. In particular, new network functions Near-RT RIC and Non-RT RIC with xApps and rApps and associated interfaces, such as A1 and E2. However, the approach to securely implementing these system components remains similar. That is, Open RAN vendors are required to practice secure system engineering and software development and need to ensure that the resulting products meet the security requirements defined during Analysis & design. To do so, they may utilize established security guidelines as a reference to identify and adopt best practices for secure development and testing. These guidelines can be tailored and expanded to align with the specific security requirements of the Open RAN components under development.

O-RAN Alliance Test Cases and Specifications

The O-RAN Alliance has published a series of test cases [24] to validate the implementation of security requirements and protocols. Test cases are designed to simulate security attacks on O-RAN components, interfaces, and the system as a whole, in order to evaluate the robustness of the O-RAN system and overall impact on service, incl.:

- Security protocol validation (SSH Server & Client, TLS, DTLS, IPSec, and OAuth 2.0);
- Common network security tests for O-RAN components include service enumeration, password-based authentication, etc.; and
- System security evaluation for O-RAN components include vulnerability scanning, data and information protection, and system logging.

Currently, the O-RAN Security Test Specifications does not cover test cases for ML-related threats,

such as data poisoning and data extraction, and test cases for specific O-RAN components, with the exception of the Open Fronthaul and the O1 interface.

Utilization of NESAS best practices

To ensure a commonly agreed security baseline for network equipment, 3GPP and GSMA have jointly established the Network Equipment Security Assurance Scheme (NESAS). NESAS comprises product development and security life cycle requirements as well as product security requirements. Compliance with the NESAS indicates that the vendor has processes in place that enable it to develop secure products and that the resulting products comply with technical best practices defined by 3GPP. For the Implementation & test phase, NESAS requires vendors to implement the following security measures in their development processes (see GSMA FS.16 [25]):

- Source Code Review;
- Source Code Governance;
- Automated Build Processing;
- Build Process Management;
- Security Testing;

Additionally, FS.16 also contains general requirements which are relevant during and beyond Implementation & test, such as the implementation of a Version Control System and a Change Tracking process.

Utilization best practices from other industries

Apart from best practices specific to the telecom industry, there are several general best practices used across industries that can also be utilized by Open RAN vendors. One example is the OWASP Secure Coding Practices Quick Reference Guide [26]. The guide is independent of the concrete functionality to be developed or the programming language used and aims to provide developers with generic best practices to help them write more secure code.

As the Open RAN system is designed to be modular, one particular type of system component that is becoming increasingly important is Application Programming Interfaces (APIs). As such, it is necessary for Open RAN vendors to enforce not only common application security but also API security best practices. For this purpose, they can refer to several OWASP publications such as Top 10 Web Application Security Risks [27] and Top 10 API Security [28]. Each contains a list of the ten most critical and common security risks (e.g., Broken access control and broken user authentication) as well as guidance on how to identify and address them.

Initiatives Related to O-RAN Vendors

O-RAN vendors can also leverage reference implementations provided by the O-RAN Software Community (OSC) to develop prototypes for O-RAN solutions. The OSC is an open-source

community for O-RAN development founded by a collaboration between O-RAN and the Linux Foundation. The community aims to develop open-source software solutions for Open RAN that are in line with the O-RAN specifications, with the objective of creating deployable open-source solutions.

Utilization of Two concepts, DevSecOps and Shift Left

As far as security testing and enforcement are concerned, two related concepts that have gained lots of popularity are DevSecOps and Shift Left. Together, they try to make developers take ownership of security matters and enforce security controls as early as possible in the development life cycle. While DevSecOps may only be applicable to a limited extent to mobile network components, because the network operator is usually not implementing the individual system components, Shift Left can certainly benefit the Open RAN security life cycle. Rather than performing security checks at the end of the implementation task, various security checks are integrated from the first day of development. The fundamental idea is that the earlier a security flaw is identified, the easier and cheaper it is to rectify. Further details on these topics can be found in the NIST DevSecOps resources [15] mentioned earlier or the OWASP DevSecOps Guideline [29].

Utilization of NIST SSDF best practices

The afore-mentioned recommendation by the CSRIC VIII group to utilize the NIST Secure Software Development Framework (SSDF) [16] applies not just during design, but also implementation and test of the solution. NIST SSDF is a framework specifically focused on ensuring the secure software development. Open RAN vendors may leverage its list of high-level best practices (e.g., prevent future reoccurrence of vulnerabilities by identifying root causes of vulnerabilities) throughout the entire software life cycle.

4.2.3 Sourcing & procurement

General statement

Sourcing & procurement is a life cycle phase that concerns both Open RAN vendors as well as MNOs. On one hand, Open RAN vendors need to securely package and deliver their final products. On the other hand, MNOs assess vendors and their products to perform a selection and, once a purchasing decision has been made, validate the products received to ensure they perform as expected. For both parties, it is vital to agree clear security responsibilities and service level agreements (SLA) in binding contracts.

Utilization of RFP/RFQ and SBOM by early stage

When comparing the sourcing of third-party components in Open RAN to traditional RAN, the fundamental principles are not different, as the process itself remains unchanged. However, sourcing from multiple vendors in Open RAN can lead to increased complexity for MNOs as

opposed to a single vendor, as it may be more difficult to ensure that components from different vendors meet the expected security requirements. In order to address the increased complexity and supply chain risks, MNOs adopt a cradle-to-grave approach to effectively source and procure RAN components from multiple suppliers. This involves specifying clear security requirements during the Request for Proposal (RfP) or Request for Quotation (RfQ) processes that allows MNOs to enforce security requirements early on and helps identify suitable vendors and products. In addition, MNOs may require their vendors to provide detailed information on the vendor's security processes and the security of its products. Part of the product security documentation should be an SBOM, as mentioned in the transversal requirements of the O-RAN Security Requirements Specification [9]. Such information about subcomponents of the supplied products can be utilized to identify security vulnerabilities and increase the transparency and security of the MNO supply chain. Specifically, NTIA provides a definition of Minimum Elements For a Software Bill of Materials [30], incl. basic use cases and key security features. The document can help MNOs and Open RAN vendors understand the importance of SBOM and ensure that theirs includes the elements required to improve software supply chain security.

Utilization of NIST SP 800 best practices

To implement the best practices mentioned above, both MNOs and Open RAN vendors can refer to the existing industrial guidelines. Specifically, NIST SP 800-161 [31] provides general guidance to organizations on how manage cybersecurity risks throughout the supply chain, including information on identifying, assessing, selecting, and implementing appropriate risk management processes, as well as implementing mitigating measures. Open RAN vendors should refer to section 1.4.5, which points to recommended practices and control for system development, system engineering, and system implementation. For MNOs, section 1.4.3 is more relevant, as it introduces recommended practices and control for acquisition and procurement owners and operators. Concrete security controls, which are defined in NIST SP 800-53 [23] include the establishment of, for example:

- A Supply Chain Risk Management (SCRM) Plan;
- Processes to verify the provenance of supplied goods;
- Appropriate acquisition strategies, tools, and methods;
- Supplier assessments and reviews; and
- Notification agreements.

Utilization of NIST IR 7622 best practices

NIST IR 7622 [32] is another document that offers guidance on managing risks related to the procurement and use of ICT systems, products, and services. It provides a set of practices and considerations for managing supply chain risks specifically for federal information systems.

Although this document is primarily aimed at federal departments and agencies, other non-federal organizations can also benefit from it by implementing the high-security level of their supply chain processes. This is because many of the concepts and best practices outlined in the document are applicable to other organizations as well.

Utilization of ATIS best practices

In addition to these NIST publications, ATIS provides a more telecom-specific standard for 5G network supply chains [33]. The standard describes a number of requirements for the supply chain, each with corresponding levels of assurance. In line with the afore-mentioned cradle-to-grave approach, these requirements cover the entire life cycle of the procured software and hardware. The standard also outlines high-level controls and mitigations required to meet these requirements, such as:

- Solution design (e.g., network segregation and zero-trust mechanisms between internal resources/functions);
- Inbound supply (e.g., software scans to identify potential malware);
- Build environment (e.g., verification of the software development environment);
- Distribution (e.g., secure software packaging and storage);
- Delivery and installation (e.g., robust tracking and transit capabilities);
- Operational tasks (e.g., secure update processes);
- Post operation tasks (e.g., data clearing); and
- Management and administration (e.g., certification, accreditation, and security assessments).

4.2.4 Integration & deployment

General statement

In the Integration & deployment phase, MNOs combine, test, and roll-out the individual components that have been sourced in the previous phase. The aim is to ensure that all components and interfaces of the network are fully functional, are configured correctly, and functionality and security meet the needs of the MNO. Usually, this phase also relies on the involvement of other stakeholders, such as the Open RAN vendors and Infrastructure providers. Moreover, MNOs may also decide to outsource certain tasks during Integration & deployment to specialized service providers (e.g., System Integrators).

Given the disaggregation and newly specified components and interfaces, Open RAN introduces new challenges for MNOs. Managing the network integration in a multi-vendor environment necessarily involves more effort than sourcing a complete RAN solution from a single vendor. Additionally, although 3GPP and O-RAN technical specifications ensure basic interoperability, different vendors may still use different technologies and protocols for non-standard functionality

(e.g., access management, logging), which may cause additional compatibility issues.

Importance of roles and responsibilities regarding integration and deployment

As there is no dedicated guideline for the Integration & deployment of Open RAN, it is on MNOs to define roles and responsibilities of each party involved during this phase (e.g., System integrator for software testing, MNO for software roll-out). This is crucial to ensure that each party involved has a clear understanding of what is expected of it, and to avoid confusion that may lead to delays in the process or, at worst, control gaps.

Once responsibilities and roles are clarified, the party responsible for system integration has to configure all components in a manner that allows for the correct operation of Open RAN components and security controls. It is recommended to conduct both component testing as well as integration testing to validate end-to-end interoperability and to verify the entire Open RAN system meets performance, reliability, and security requirements. With regards to integration testing, the O-RAN Alliance has developed a set of tests to promote interoperability across different implementations of the O-RAN interfaces, in addition to afore-mentioned tests for validating each component/interface. For example, interoperability testing of O-RUs and O-DUs from different vendors connected through the Open Fronthaul interfaces[34]. Referring to the test specifications, it is specified which tests should be conducted to ensure interoperability between different components/interfaces and provided guidance on how to conduct the tests in a manner that aligns with industrial standards.

Utilization of NIST SP 800-53, NIST SP 800-161 and CIS Controls

Further, Open RAN vendors, MNOs, and Infrastructure providers need to ensure that their systems are securely hardened to minimize the attack surface, for example, by disabling unnecessary services, tightening access rights and privileges. To assist MNOs and Infrastructure providers in identifying and adopting best practices for integration and deployment, some of the afore-mentioned industry guidelines may be referred. NIST SP 800-53 [23], NIST SP 800-161 [31], and CIS Controls [35] include guidance on integration, testing, and deployment.

While the CIS Controls provide a broader framework of cybersecurity best practices, CIS Benchmarks [36] offer guidance for configuring and securing individual technology components, such as operating systems, applications, and cloud environments. Depending on the exact implementation, the following CIS benchmarks may be relevant for Open RAN technology components:

- Virtualization software (e.g., VMware, Docker, Kubernetes);
- Operating systems (e.g., Ubuntu Linux, Red Hat Enterprise Linux);
- Web servers (e.g., NGINX, Apache HTTP Server); and
- Database servers (e.g., Microsoft SQL server, PostgreSQL).

Utilization of CIS benchmarks and ETSI NFV for O-cloud services

If the Open RAN deployment utilizes cloud resources, the MNO may also refer to CIS benchmarks for cloud services by popular Infrastructure providers, such as Amazon AWS, Google Cloud, and Microsoft Azure. By following the CIS Benchmarks, the Open RAN stakeholders can effectively harden core technology components of the Open RAN system.

When it comes to integrating the Open RAN components with the underlying O-Cloud, Open RAN vendors, MNOs, and infrastructure providers can refer to the specifications by ETSI NFV. Specifically, ETSI GS NFV-SEC 021 [37] provides the security requirements for protecting the authenticity and integrity of the VNF package during onboarding onto the NFV infrastructure, incl.:

- Each individual artifact in a VNF Package shall have a cryptographic signature when it is stored in the NFV-MANO catalogue(s); and
- Before instantiation, all available signatures on the artifacts shall be verified by NFV-MANO.

Utilization of CSRIC VIII report

The CSRIC VIII report [14] also contains recommendations for this phase of life cycle, such as deploying Open RAN software on secure server hardware with encrypted and securely stored credentials and keys and using a secure boot with software signing to establish an end-to-end chain of trust.

4.2.5 Operations & maintenance

General statement

During the Operations & maintenance phase, it is on the MNO to continuously ensure the availability of network infrastructure and services. In contrast to the previous life cycle phases, this involves not just preventive, but also reactive and corrective security controls. To that end, Operations & maintenance tasks for Open RAN are not different from those for traditional RAN deployments.

Important aspects of operational security

First, a key aspect of operational security is ensuring visibility. This requires such fundamental controls such as a complete, up-to-date system inventory and identity management system, so that the MNO can know what needs to be secured. Further, information about security relevant events throughout the network should be collected, which may involve information such as log files collected at the level of network functions and the underlying infrastructure, alerts issued by network elements and security controls, and network connections and traffic flows.

Second, MNOs need to be able to identify security defects and incidents in a timely manner. This

requires capabilities to analyze the different operational data points collected as well as awareness of continuously emerging security threats. A Security Information and Event Management (SIEM) can help to correlate data points from different sources and identify individual events or anomalies. Additionally, MNOs may want to regularly scan their deployments for vulnerabilities and indicators of compromise (IOC), in order to detect known security issues.

Third, processes should be in place to take corrective action, once security issues are identified. If an incident is identified, a coordinated response process should ensure containment, the eradication of the incident, and a complete recovery from it. If a vulnerability is detected, a vulnerability management process should document, assess, prioritize, and eventually mitigate it, for example, by rolling out relevant software updates. The latter also requires a structured configuration and change management process that ensures changes to the network are properly documented, reviewed, tested, and approved before being rolled-out into the network.

Although it may seem as if the Operations & maintenance phase only depends on the MNO, all the capabilities described above require active involvement by the other Open RAN stakeholders as well. Open RAN vendors and infrastructure providers need to develop products that can be monitored effectively by implementing established industry standards for system management and monitoring. If security vulnerabilities or weaknesses are identified in Open RAN components or the cloud infrastructure, MNOs need to be informed about them. Furthermore, security updates and mitigating measures need to be provided by as contractually agreed during the Sourcing & procurement life cycle phase.

Utilization of a variety of specifications

For best practices regarding operational security measures, MNOs can refer to some of the guidelines referred to in previous sections. The CIS Controls [35] as well as the CSA Control Matrix [38] provide actionable advice on how to protect individual systems and the underlying cloud infrastructure.

While the afore-mentioned resources document generic IT security best practices, there are also those which are tailored specifically at telecom environments. One of these is MITRE FiGHT™ [39]. Modelled after the popular MITRE ATT&CK® framework [40], FiGHT™ extends the generic guidance by additional attack techniques (e.g., Registration of malicious network functions, gNodeB Component Manipulation) and mitigations that are relevant to 5G networks. Like ATT&CK®, it is structured like a typical flow of actions of a malicious actor attempting to compromise the system. By doing so, it can help to perform more realistic threat assessments, identify potential control gaps, and design defenses so that stop attackers as early as possible in the process. Some of the recommended mitigations that are also relevant to Open RAN components include:

- Enforcing resource Isolation in virtualization environments;

- Ensuring physical and environmental protection; and
- Providing for continuity of power supplied to equipment deployed in the field.

5 Lab Verification and Analysis

5.1. Purpose of Lab Verification

In the previous chapters, security risks of Open RAN described in Chapter 3 and risk mitigation measures described in Chapter 4 have been examined and compared to traditional RAN.
When MNOs deploy Open RANs, in addition to risk analysis, the actual network equipment on which the Open RAN is built should be checked to ensure that it is secure. This is an important factor in the decision-making process.
In this chapter, it is verified whether some of the identified security risks of Open RAN are addressed by implementing the measures specified by O-RAN Alliance on the network equipment.

5.2. Lab verification scope and procedure

5.2.1 Scope

The transformation of radio access with Open RAN is driven by three technology areas: Open Interfaces, Virtualization, and Intelligence. The interfaces and components included in each area are summarized in Table 15. Security risk mitigation measures will be tested against the three areas. In this report, all the test items in three areas have been examined and the open interface test was conducted among them.

Area	Interface	Component
Open Interface	Open Fronthaul CUS-Plane, Open Fronthaul M-Plane, A1, O1, O2, E2, R1	Components interconnected by Open Interfaces
Virtualization	O2	O-Cloud, SMO
Intelligence	A1, O1, O2, E2, R1	SMO, Non-RT RIC, Near-RT RIC, xApp, rApp

Table 15: Open RAN Technical Areas

The interfaces and components corresponding to the three areas (Open Interface, Virtualization, and Intelligence) in the O-RAN architecture are shown in Figure 12

.

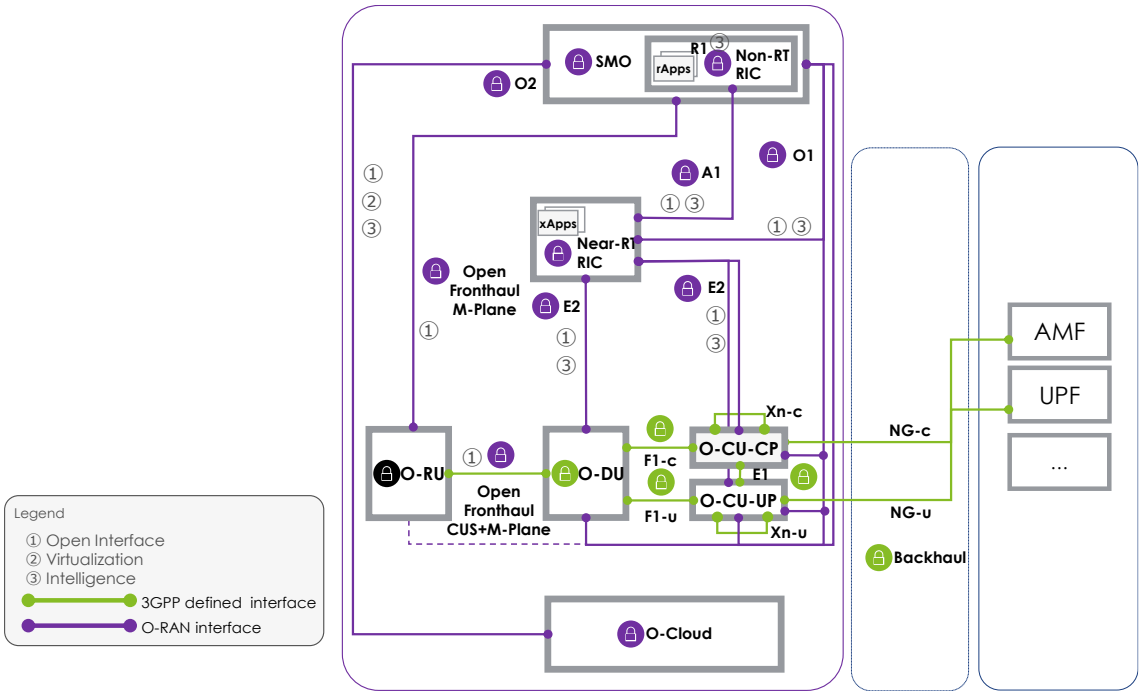

Figure 12: **Interfaces and Components in O-RAN Technical Areas**

5.2.2 Procedure

Firstly, test scenarios are defined for each targeted area to confirm the implementation of security measures. In O-RAN Alliance, Security Work Group is developing security-related test specifications, and the Test & Integration Focus Group also includes a security perspective in its end-to-end testing specification. The test scenarios are developed based on O-RAN test specifications and referencing 3GPP test specification [24] [41] [42].

Secondly, a test environment is prepared to conduct representative test scenarios. It is used to validate the test scenarios (testing to ensure that the security measures are properly implemented and functioning) and assess the effectiveness of the measures (testing to ensure that the risk is being effectively addressed by the security measures). Because typical scenarios are designed to confirm the effectiveness of risk mitigation measures, confirmation of the effectiveness of scenarios leads to confirmation of the effectiveness of measures. When conducting tests, if the number of tests that can be conducted is limited due to the constraints of the test environment or other reasons, the tests will be prioritized from cases that can cover a wider range of Open RAN issues.

When cases are found where measures have not been implemented, the measures to be implemented to avoid security risks are considered and presented in this report.

As the purpose of the actual equipment testing is not to evaluate individual devices, results that indicate vulnerabilities of specific devices will be excluded from this report.

5.3. Test scenarios

The O-RAN security test specifications verify that devices are adequately compliant with Open RAN security requirements. This chapter therefore checks whether the risks of Open RAN are addressed by specifying test scenarios based on the O-RAN and 3GPP test specifications. As mentioned in 4.1.3, in the Open RAN system life cycle, the O-RAN specification mainly covers the Analysis & design phase. In addition, testing based on the specification can cover a part of Implementation & test phase.

5.3.1 Open Interface

5.3.1.1 Characteristics of Open Interface

The O-RAN architecture specifies six open interfaces: Open Fronthaul, A1, O1, O2, E2, and R1 and Open Fronthaul has CUS + M-Plane in one interface. Some of these interfaces exist in traditional RAN systems, but opening up and standardizing them enables a strong, robust, industry-driven, evolvable, regulatable and standardized set of security measures against attackers. The security controls of each interface are summarized in Table 16 from the perspective of the security controls and features that they must achieve [43]. Open and standardized interfaces between components without the standard security measures, theoretically provide the attack surfaces to attacker. It is therefore necessary to verify that O-RAN equipment is able to address risks by implementing standard security measures based on standard specifications.

Potential Goals	Open Fronthaul				Non-Fronthaul				
	C-Plane	U-Plane	S-Plane	M-Plane	A1	O1	O2	E2	R1
Authenticity				TLS/SSH	TLS	TLS	TLS	IPsec	TLS
Confidentiality		PDCP		TLS/SSH	TLS	TLS	TLS	IPsec	TLS

Integrity		PDCP		TLS/SSH	TLS	TLS	TLS	IPsec	TLS
Authorization				NACM	OAuth	NACM	OAuth		OAuth
Data Origination				TLS/SSH	TLS	TLS	TLS	IPsec	TLS
Replay Prevention		PDCP		TLS/SSH	TLS	TLS	TLS	IPsec	TLS

Table 16: Mandatory O-RAN interface security controls

The protocol stack of Open Fronthaul is shown in Figure 13 [44] and Figure 14 [11]. The Open Fronthaul CUS-Plane is an Ethernet L2 connection, while the Open Fronthaul M-Plan other open interfaces are TCP/IP connections.

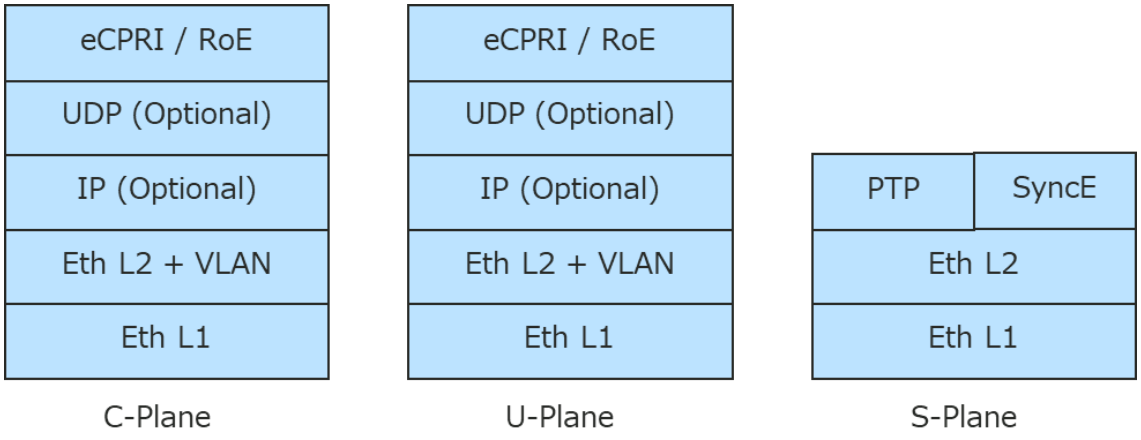

Figure 13: Open Fronthaul CUS-Plane Protocol Stack

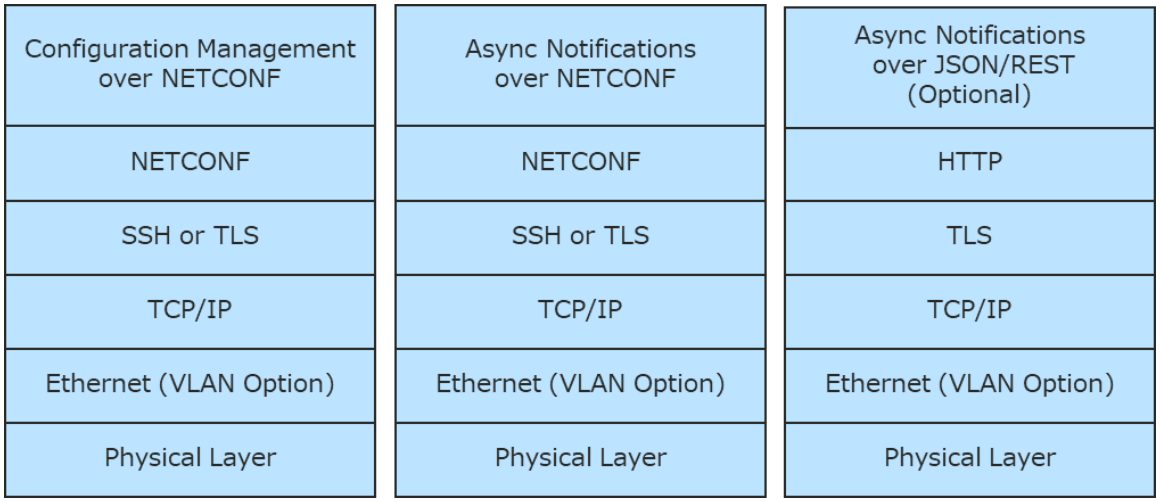

Figure 14: Open Fronthaul M-Plane Protocol Stack

5.3.1.2 Open Fronthaul Test Scenario

In developing test scenario for open interfaces, Open Fronthaul is selected as a representative interface that includes CUS + M-Plane.

As described in Section 2.3.1, it is assumed that traditional RAN deployment comprised of Base Band Units (BBU) and Radio Remote Head (RRH), and connections between components are made through closed interfaces. In the O-RAN specification, Open Fronthaul was the first interface to be opened up and is an appropriate representative test subject due to its maturity and advanced implementation.

Furthermore, Open Fronthaul includes typical connection types (Ethernet L2 connections, TCP/IP connections) and security controls, and the learnings gained by examining its differences with other interfaces can be applied to mitigate security risks of other open interfaces.

Test scenario for Open Interface is shown in Table 17.

#	Test Item	Overview	Target	Source
1	Service Enumeration/ Network Boundary Examination	Assess TCP and UDP open ports	M-Plane	O-RAN Security Test Spec 7.2.1
2	SSH Server & Client	Verify the proper implementation of the SSH protocol	M-Plane	O-RAN Security Test Spec 6.2

3	TLS	Verify the proper implementation of the TLS secure communication protocol	M-Plane	O-RAN Security Test Spec 6.3
4	Password-Based Authentication/PWDAUTH	Verify the robustness of every management plane protocol	M-Plane	O-RAN Security Test Spec 7.3.1
5	Password Policy Enforcement	Verify that policies on acceptable password values are enforced properly.	M-Plane	O-RAN Security Test Spec 7.3.3
6	Security Event Logging	Security events shall be logged together with a unique system reference	M-Plane	3GPP TS 33.117 4.2.3.6.1
7	Log Transfer to Centralized System	The element shall support forwarding of security event log to an external system.	M-Plane	3GPP TS 33.117 4.2.3.6.2
8	Protecting Session – Logout Function	The system shall have a function that allows a signed in user to logout at any time.	M-Plane	3GPP TS 33.117 4.2.3.5.1
9	Protecting sessions - inactivity timeout	An OAM user interactive session shall be terminated automatically after a specified period of inactivity.	M-Plane	3GPP TS 33.117 4.2.3.5.2
10	TCP SYN/FIN Flooding	An attack method that sends a large number of SYN packets that request TCP connections	M-Plane	O-RAN Security Test Spec 7.5.1

11	Unexpected Input (Fuzzing)	An attack method that sends unexpected (not in-line with protocol specification) input towards O-DU C-Plane and S-Plane.	C-Plane S-Plane	O-RAN E2E Test Spec.7.2.4 O-RAN E2E Test Spec.7.2.5
12	DoS	An attack method that sends a predefined volumetric pocket against O-DU C-Plane and S-Plane.	C-Plane S-Plane	O-RAN E2E Test Spec.7.2.1 O-RAN E2E Test Spec.7.2.2

Table 17: Open Fronthaul Test Scenario

5.3.1.3 Other Open Interface Test Scenarios

Open interfaces other than Open Fronthaul require testing against the security controls they are required to implement. Table 18 specifies test scenarios for each open interface.

#	Test Item	Overview	Target	Source
1	NACM Validation	Validate the NACM enforcement on the O-RAN component O1 interface for the role-based access control	O1	O-RAN Security Test 17.2
2	TLS	Verify the proper implementation of the secure communication protocol TLS	A1, O1, O2, R1	O-RAN Security Test 6.3
3	IPSec	Verify the proper implementation of the secure communication protocol IPsec.	E2	O-RAN Security Test 6.5
4	OAuth 2.0	Verify the proper implementation of the authorization of O-RAN application's (e.g. xAPP) API service request to O-RAN resource provider (e.g., Near-RT RIC) based on OAuth 2.0	A1, O2, R1	O-RAN Security Test 6.6

Table **18: Open Interface Test Scenarios**

5.3.2 Virtualization

5.3.2.1 Characteristics of Virtualization

Because O-RAN systems run on O-Cloud, the virtualization foundation, an attack on the virtualization leads to an impact on the entire O-RAN system deployed on it. While the virtualization is a key element of Open RAN, the elements used are not specific to Open RAN alone, but are widely used throughout the entire 5G system, including the 5G core. For this reason, the test items for the virtualization in the O-RAN test specification are generic.

5.3.2.1 Test scenario for virtualization

Test scenario for the virtualization is shown in Table 19.

#	Test Item	Overview	Target	Source
1	Side channel DoS attack	Verify that a noisy neighbor DoS attack against O-Cloud for resource starvation will not degrade service availability or performance	O-Cloud, MANO	O-RAN E2E Test 7.3
2	Software Image Signing	Check whether App/VNF/CNF package is digitally signed.	O-Cloud	O-RAN Security Test 9.5.1
3	Software Signature Verification	Check whether signature of App/VNF/CNF package is verified by Service provider.	O-Cloud	O-RAN Security Test 9.5.2
4	Service Enumeration/ Network Boundary Examination	Assess TCP and UDP open ports	O-Cloud, MANO, O2	O-RAN Security Test Spec 7.2.1
5	Password-Based Authentication/PWDAUTH	Verify the robustness of every management plane protocol	O-Cloud, MANO, O2	O-RAN Security Test Spec 7.3.1

6	Unauthorized Password Reset	Verify whether out-of-band mechanisms exist and exposed to circumvent, disable, or reset the password	O-Cloud, MANO, O2	O-RAN Security Test Spec 7.3.2
7	Password Policy Enforcement	Verify that policies on acceptable password values are enforced properly.	O-Cloud, MANO, O2	O-RAN Security Test Spec 7.3.3

Table 19: Virtualization Test Scenario

5.3.3 Intelligence

5.3.3.1 The Characteristics of Intelligence

Open RAN introduces RIC (RAN Intelligent Controller) and related RAN apps (rApp, xAPP) to enable autonomous and automated RAN operations by leveraging machine learning and artificial intelligence. RIC is a logical component that designs and sets parameters of base stations and automates and optimizes operations to realize intelligent network operations. There are two types of RICs, Near-RT RIC and Non-RT RIC, and their control algorithms are specified by rApp and xApp, respectively. Thus, security testing for intelligence centers on interfaces and authentication interconnecting each component.

5.3.3.2 Intelligence Testing Scenario

Intelligence Testing Scenario is listed in Table 20

#	Test Item	Overview	Target	Source
1	NACM Validation	Validate the NACM enforcement on the O-RAN component O1 interface for the role-based access control	O1	O-RAN Security Test 17.2
2	TLS	Verify the proper implementation of the secure communication protocol TLS	A1, O1, O2, R1	O-RAN Security Test 6.3

3	IPsec	Verify the proper implementation of the secure communication protocol IPsec.	E2	O-RAN Security Test 6.5
4	DDoS	Validate how handling of large amounts of requests is done. DoS/DDoS attacks will come in three forms: Protocol layer attacks, Volume based attacks and Application layer attacks.	SMO, Non-RT RIC, Near-RT RIC	O-RAN Security Test 7.5
5	Software Image Signing	Check whether App/VNF/CNF package is digitally signed.	xApp, rApp	O-RAN Security Test 9.5.1
6	Software Signature Verification	Check whether signature of App/VNF/CNF package is verified by Service provider.	xApp, rApp	O-RAN Security Test 9.5.2
7	OAuth 2.0	Verify the proper implementation of the authorization of O-RAN application's (e.g. xApp) API service request to O-RAN resource provider (e.g., Near-RT RIC) based on OAuth 2.0	A1, O2, R1	O-RAN Security Test 6.6
8	Service Enumeration/ Network Boundary Examination	Assess TCP and UDP open ports	SMO, Non-RT RIC, Near-RT RIC	O-RAN Security Test Spec 7.2.1
9	Password-Based Authentication/PWDAUTH	Verify the robustness of every management plane protocol	SMO, Non-RT	O-RAN Security Test Spec 7.3.1

			RIC, Near-RT RIC	
10	Unauthorized Password Reset	Test and verify whether any out-of-band mechanisms exist (and are exposed), which can be used to circumvent, disable, or reset the password.	SMO, Non-RT RIC, Near-RT RIC	O-RAN Security Test Spec 7.3.2
11	Password Policy Enforcement	Verify that policies on acceptable password values are enforced properly.	SMO, Non-RT RIC, Near-RT RIC	O-RAN Security Test Spec 7.3.3
12	ML data poisoning	AI/ML can be susceptible to security attacks such as data poisoning, backdoor, evasion, model stealing and data extraction.	xApp, rApp	O-RAN Security Test Spec 10.2 (To be updated in subsequent version)

Table 20: Intelligence Test Scenario

5.4. Test Environment

A test environment needs to be constructed to perform lab verification. The test environment assumes a commercial environment for MNOs, which must include a virtualized radio access network (vRAN) consisting of equipment from multiple vendors. It is first necessary to construct and integrate the multi-vendor system and establish stable end-to-end mobile communications. Secondly, a representative test scenario is selected from the test scenarios specified in the previous section, and verification tests are conducted using this test environment. Selection of test scenarios is prioritized for those that can cover a wider range of Open RAN issues and can be performed in the test environment.

5.5. Validation Results

5.5.1 Open Interface

5.5.1.1 Verification items and procedures

As mentioned above, Open FH is selected for the following lab verification because it is a representative interface which includes CUS + M-Plane components, typical connection types (Ethernet L2 and TCP/IP connections) and security controls.

Figure 15 shows the test target.

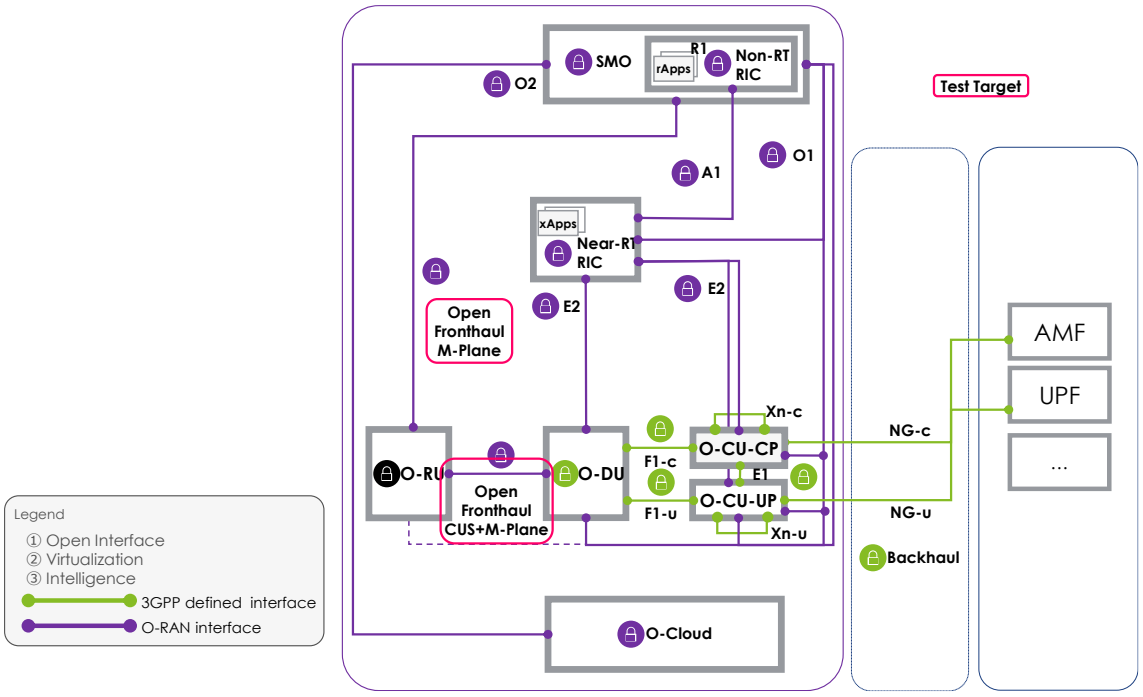

Figure 15: Test Target

Approach:

(1) Connect test PC to same VLAN as O-DU and O-RU

(2) Precondition

A) IP address and MAC address of O-DU and O-RU are provided

B) M-Plane uses Netconf/SSH profile

(3) Perform verification as black box test based on pre-information

Test procedure

1. Service Enumeration/ Network Boundary Examination

Target: O-DU and O-RU

Precondition: Access to IP addresses of target systems

Test tool: Nmap and manual validation of ports exposure

Procedure:

TCP Port Scan

(1) Send a TCP SYN packet to each port of O-DU and check if the port is open

(2) Check if the service is available for the open port

(3) Identify active services and attempt to compromise

(4) Send a TCP SYN packet to each O-RU port and check if the port is open

(5) Check if the service is available for the open port

(6) Identify active services and attempt to compromise

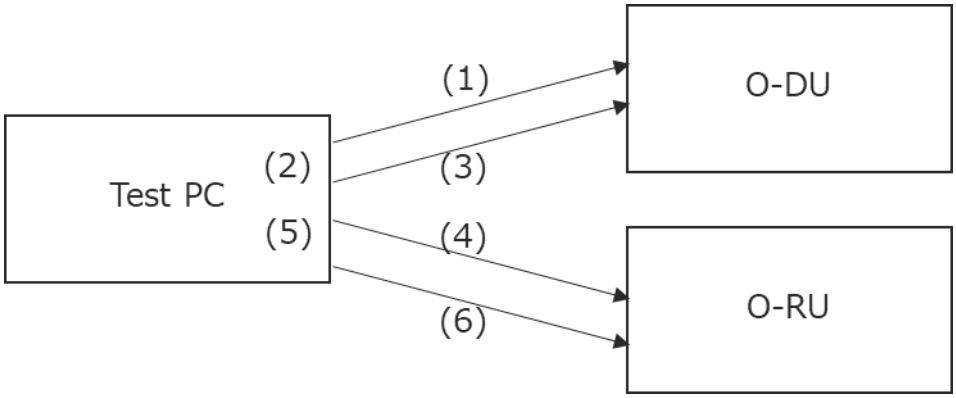

Figure 16: Service Enumeration/ Network Boundary Examination

2. SSH Server & Client

Target: O-RU

Precondition: Access to SSH interface

Test tool: BASH script and nmap test cases against encryption

Procedure:

Server-side

(1) Access and attempt to iterate over known weak/insecure cipher suites available and agreed upon from server

(2) Review the tool's output for reported vulnerabilities

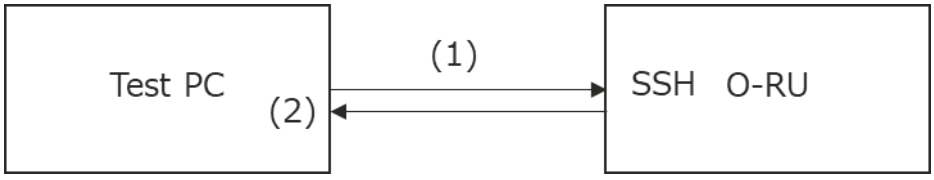

Figure 17: SSH Server & Client

Server-side (Gray box test)

(1) Retrieve credential information (username, id, authentication key)

(2) Confirm login with credential information

(3) Verify SSH protocols and algorithms (for host key, symmetric encryption, key exchange, and MACs) as defined by Security Protocol Specifications.

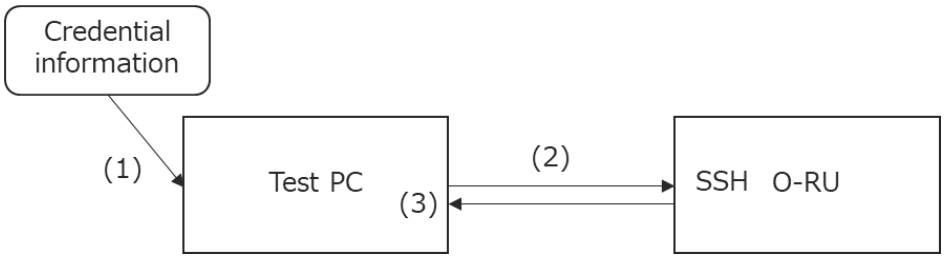

Figure 18: SSH Server & Client (Gray Box Test)

3. TLS

Target: O-RU

Precondition: Access to TLS interface

Test tool: BASH script and nmap test cases against encryption

Procedure:

(1) Access and attempt to iterate over known weak/insecure cipher suites available and agreed upon from server

(2) Review the tool's output for reported vulnerabilities

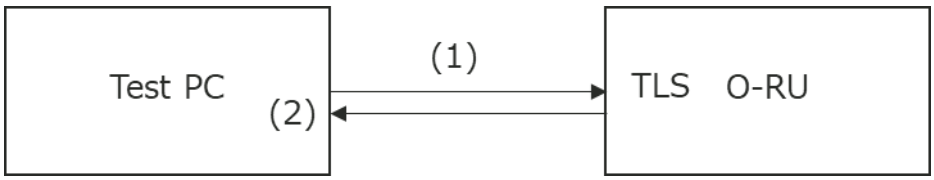

Figure 19: TLS

4. Password-Based Authentication/PWDAUTH

Target: O-RU

Precondition: Access to password policies (authenticated), access to authentication interfaces

Test tool: Manual evaluation from service (command line/browser) with proxy or other capture tools

Procedure:

(1) Using a common set of usernames and password combinations, continually connect and guess user/password.

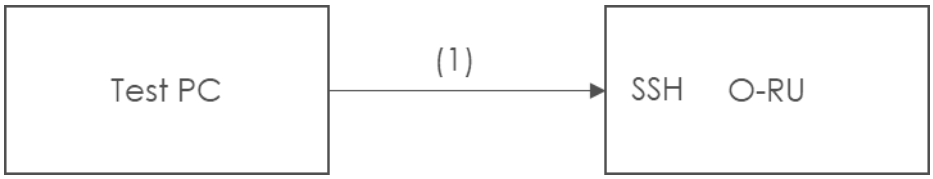

Figure 20: Password-Based Authentication/PWDAUTH

5. Password Policy Enforcement

Target: O-RU

Precondition: Access to password policies (authenticated), access to authentication interfaces

Test tool: Manual evaluation from service (command line/browser) with proxy or other capture tools

Procedure:

(1) Test the resistance of the equipment against password attack guessing using available password dictionaries by evaluating the length, complexity, reuse, change frequency, and aging requirements of passwords.

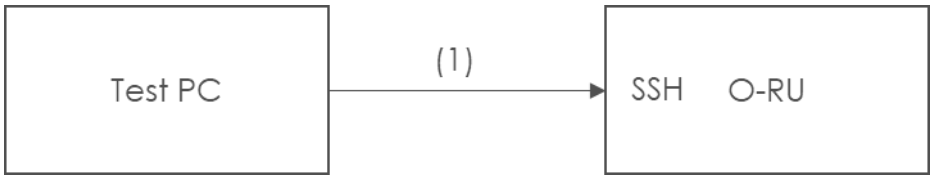

Figure 21: Password Policy Enforcement

Test 6 to Test 9 were not performed.

10. TCP SYN/FIN Flooding

Target: O-DU

Precondition: Network access to two resources on same subnet

Test tool: Tools to mass send TCP SYN packets

Procedure:

(1) Send large number of packets to target system, and evaluate service stability and resilience

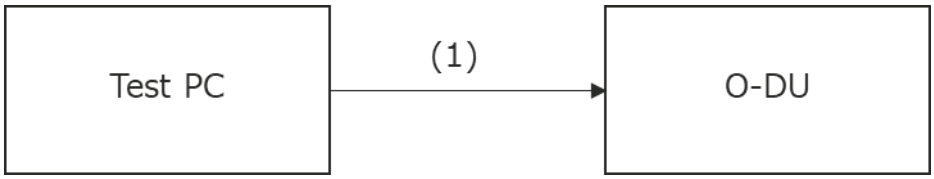

Figure 22: TCP SYN/FIN Flooding

11. Unexpected Input (Fuzzing)

Target: O-DU

Precondition: Authenticated access to the device, network access to services

Test tool: Nmap and manual validation of ports exposure, manually interacting with protocols and sending error packets

Procedure:

(1) Ensure packet communication from test PC to O-DU on C-Plane and S-Plane

(2) Use sample packet or packet made from legitimate message sent towards the O-DU

(3) Use fuzzing tool to send test packet while keeping original source/destination MAC address

(4) Observe the functional and performance impact of the target

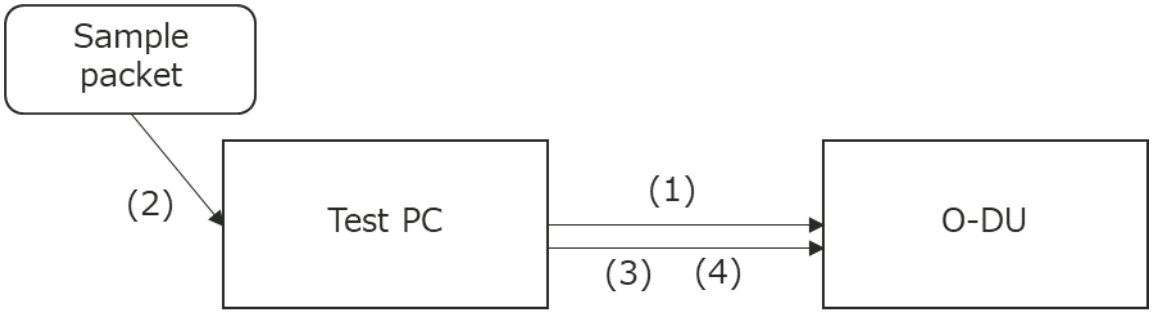

Figure 23: Unexpected Input (Fuzzing)

12. DoS

Target: O-DU

Precondition: Network access to two resources on same subnet mapping of known hosted services

Test tool: Bash and other scripts/binaries for ending large amounts of packets

Procedure:

(1) Ensure packet communication from test PC to O-DU on C-Plane and S-Plane

(2) Use test tool to generate various level of volumetric DoS attack against the MAC address of the O-DU

(3) Observe the functional and performance impact of the target

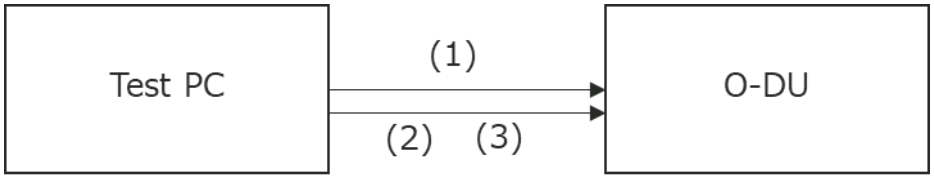

Figure 24: DoS

5.5.1.2 Test Results

Test results for each test item are shown in Table 21.

#	Test Item	Result	Remarks
1	Service Enumeration/ Network Boundary Examination	2 TCP open ports at O-RU and 3 at O-DU are found, but found no vulnerability to open ports.	
2	SSH Server & Client	SSH login failed to SSH server in O-RU (Black box test) Successful login to SSH server using credential information in O-RU, and supported algorithms are verified. (Gray box test)	In M-Plane, O-RU becomes a server using SSH + NETCONF, prevents any login to higher devices (O-DU or SMO) and is considered a safe design.
3	TLS	O-DU and O-RU used in this test does not support NETCONF/TLS 1.2, so it is not tested	Open Fronthaul M-Plane has IOT profiles of NETCONF/SSHv2 support and NETCONF/TLS 1.2 support, and this time a system that supports the former is used
4	Password-Based Authentication/PWDAUTH	Brute force attack on O-RU authentication, but login was unsuccessful	
5	Password Policy Enforcement	Confirmed that no dictionary-registered password was used in O-RU authentication	
6	Security Event Logging	Not performed	Since it is confirmation of the component function, it will be covered by the vendor hearing.
7	Log Transfer to Centralized System	Not performed	Since it is confirmation of the component function, it will be covered by the vendor hearing.

8	Protecting Session –Logout Function	Not performed	Since it is confirmation of the internal component operation, it will be covered by the vendor hearing.
9	Protecting sessions - inactivity timeout	Not performed	Since it is confirmation of the internal component operation, it will be covered by the vendor hearing.
10	TCP SYN/FIN Flooding	No abnormality occurred in O-DU condition	
11	Unexpected Input (Fuzzing)	No abnormality occurred in O-DU condition	
12	DoS	No abnormality occurred in the condition of O-DU.	

Table 21: Test Result

5.5.1.3 Analysis

As a representative of open interfaces, lab verification of Open Fronthaul was conducted.
Open Fronthaul has M-Plane over TCP/IP connections and CUS-Plane over Ethernet L2 connections, and the other open interfaces specified by O-RAN Alliance are TCP/IP connections. Since all open interface has supported TCP/IP connection, black-box and gray box test for M-Plane was conducted first.
The M-Plane risk is that by opening up and standardizing the interface without the mandatory security controls, an attacker can analyze the interface, break into the component, and perform a service outage.
For O-RU, it can be determined from the standard specification that there is an SSH server, which could be an entry point. Based on the port scan results, an attempt was made to break into the SSH Server, but no login was possible. Then, in a gray box test using credentials information, it successfully logged in to the SSH server on the O-RU and confirmed that there were no problems with the algorithms.
In M-Plane, placing a NETCONF + SSH server at the O-RU does not make it an attack surface to log in to upper devices (e.g.,O-DU,SMO). Even if it is invaded, the damage will not be expanded. It can be said that it enhances the safety of the design.

For C-Plane and S-Plane, no impact was observed on the O-DU in response to DoS/Fuzzing tests for Ethernet L2 connections.

The lab validation of Open Fronthaul included the general risks of open interfaces, and it was observed that Open Fronthaul is capable of mitigating these risks. The tests conducted here were based on the O-RAN specification, and it was confirmed that the risk of Open Fronthaul can be addressed by adhering to the standard specification. Since Open Fronthaul covers typical connection types and security controls for open interfaces, the findings from Open Fronthaul tests can be applied to other open interfaces. As with Open Fronthaul, it can be estimated that for other open interfaces, the risk can be reduced by adhering to the standard specifications, leading to security assurance.

6 Conclusion

6.1 Open RAN security risks and mitigations

6.1.1 Risk analysis findings

The latest stage of the RAN evolution, Open RAN, introduces new network components, interfaces, and features in an effort to raise operational efficiency, foster interoperability and innovation. These developments also have the potential to enhance the security RAN deployments. Meanwhile, there are also a number of security risks that are either entirely new to the RAN or more pronounced than in traditional RAN deployments. This report aims to resolve concerns about the security of Open RAN by providing structured analysis of the associated security risks and recommended mitigating measures to address them.

The analysis builds on related work performed by the O-RAN Alliance. By reviewing and further detailing their threat modelling and risk analysis work [2], it was possible to obtain a comprehensive picture of the security risk Open RAN components and interfaces are subject to. Key findings include:

- In total, 10 Open RAN components and interfaces have high-rated security risks associated to them. These are O-Cloud, R1, Non-RT RIC, rApp, A1, SMO, O2, O1, E2, and Open Fronthaul (M Plane).
- The most critical component, based on the number of high-rated security threats, is the O-Cloud. The O-Cloud is subject to a number of security threats that are not directly connected to other Open RAN components, i.e., virtualization-related security threats. Nevertheless, these threats still have the potential to affect other network components, if the underlying O-Cloud is compromised.
- A total of 55 (or 4%) of the analyzed security threats are considered unique to Open RAN. That is, they are threats that do not affect traditional RAN deployments. Out of those 4%, two-thirds are security risks rated high, while the remaining one third is rated medium.

As such, these findings substantiate the claim that Open RAN increases the attack surface as compared to traditional RAN deployments, albeit only by a small degree. Similar to traditional RAN deployments, centralized network components and interfaces that can have large impact on the overall network deployment if compromised can be considered more critical than those at the edge of the network serving a limited area and subscriber count. Specifically, the utilization of cloud resources poses a high risk to RAN deployments, as a breach of security at the infrastructure layer –be it intentionally malicious or unintentional– can have a critical impact on large parts of the network.

6.1.2 Mitigating measures

Specification gaps and inconsistencies

Previous reports on Open RAN security commented on the state of the O-RAN specifications and improvements that would be necessary to improve the security of Open RAN. As the analysis described in this report relies on the work performed by the O-RAN Alliance, it is important to recognize potential gaps and necessary shortcomings of the O-RAN specifications in their current state. During the analysis, the following points became apparent:

- The technical specifications mainly focus on Analysis & design phase, but also contain general requirements for certain aspects in other life cycle phases, for example, SBOM (see Figure 10).
- Parts of the O-RAN security specification appear to be incomplete, for example:
    - Security requirements do not cover all security principles (see section 4.1.2 (Analysis result))
    - Specified security controls do not cover all security requirements (see Figure 11)
    - Security controls do not cover all components/interfaces (see Figure 11)
- It is often unclear how guidance has been determined or how it relates to other parts of the security specification, for example:
    - No details on how security principles have been derived and how the security controls address the security threats (see section 4.1.1 (Specification analysis))
    - It is unclear how the O-RAN Alliance selected security guidelines and best practices related to Open RAN security. For example, relevant CIS controls and NIST 800-53 control families are recommended in some of the Technical Reports on individual components, such as O-Cloud, SMO, and shared O-RU (see section 4.2.1 (Analysis & design))

The first finding is to be expected. Technical specifications are limited in scope by necessity because they ensure an interoperable design of system components and associated security controls. As such, they cannot provide a holistic security framework that covers all phases for the Open RAN life cycle. For this purpose, supplementary mitigating measures that do not need to be standardized should be put in place by the relevant Open RAN stakeholders.

The second and third finding, however, can be addressed by further work to the O-RAN specifications. The O-RAN Threat Modeling and Remediation Analysis [2] provides a good foundation for defining Open RAN security requirements and controls that go beyond the current level of coverage. It may be improved even further by incorporating some of the observations

made in section 2.3 (Risk analysis). Importantly, the specifications would benefit significantly from further details on how some of the recommendations have been derived. Given the attention by industry and regulatory bodies, this could go a long way to dispel some of the concerns regarding Open RAN security.

Supplementary mitigation measures

Based on the analysis of security controls and requirements defined in the technical specifications, supplementary mitigation measures are provided to cover the entire Open RAN life cycle beyond Analysis & design. Where available, these recommendations are based on telecom-specific guidance developed by organizations such as GSMA. Alternatively, generic industry standards and best practices are referenced. It is apparent that, with the exception of the O-RAN test specifications concerning security requirements [24] and interoperability [45], few aspects require guidance specifically tailored to Open RAN or even telecommunications. Instead, it is expected that common IT security best practices can be leveraged for valuable information on securing Open RAN deployments. Further study would be required to gauge the potential benefits of closer alignment between network and IT security requirements and controls in network operators.

The large number of referenced best practices shows that relevant guidance does exist, just not yet in a consolidated form. Additional efforts from industry groups will be required to support Open RAN stakeholders identify and adopt relevant security best practices. This applies in particular to MNOs, as the absence of a single RAN vendor requires them to take on new security responsibilities in the Open RAN life cycle.

6.1.3 Comparison to traditional RAN

The findings of the Open RAN risk analysis show that Open RAN does not fundamentally change the risk landscape that also affects traditional RAN deployments. While it is true that the system design introduces components and interfaces that were previously less visible due to their proprietary nature, the risks they are subject to are hardly new. This includes fronthaul interfaces, management and orchestration systems, and cloud computing capabilities. An exception are genuinely new RAN functionalities, such as RAN Intelligent Controllers as well as xApps and rApps. The AI/ML capabilities used in these components introduce novel types of security threats, such as AI/ML poisoning or transfer learning attacks. This relatively small group of novel threats is not to be dismissed, as associated components and interfaces (i.e., Non-RT RIC, rApp, A1, E2, and R1) make up five out of ten high-risk items identified.

When comparing Open RAN to traditional RAN deployment models, more fundamental changes can be identified in the roles and responsibilities for ensuring security. As outlined in section 2.4.4 (Risk owners and mitigation owners), different stakeholders are required to implement and

enforce security controls throughout the system life cycle. With Open RAN, the responsibilities between them are not as clearly defined as in single-vendor, non-cloud RAN deployments. It is on the MNOs as ultimately accountable party to define security requirements and a controls framework aligned to their operating model and enforce those across multiple suppliers and service providers. If stakeholders follow security best practices, such as those outlined in chapter 4 (Risk mitigation measures) throughout the Open RAN life cycle, Open RAN can be built as secure as traditional RAN.

To what extent Open RAN can improve on the security posture of existing RAN deployments will depend on the extent to which implementors, integrators, and operators will be able to leverage the theoretical advantages that an openly specified and software-defined system provides over a proprietary solution that depends on specialized hardware.

6.1.4 Lab Verification and Analysis

In this lab validation, the Open Fronthaul was examined as a representative of open interfaces, on which various security breach tests were performed. The validation of Virtualization and Intelligence remains an important item for future study.

O-Cloud, which constitutes the virtualization foundation, is an essential element of the O-RAN system and has a high-risk rating. The virtualization technology used in Open RAN is generic and common across a wide range of 5G systems, and there are few elements unique to Open RAN.

Intelligence is a newly introduced field in Open RAN.

This verification was for Open Fronthaul and was sufficiently valid. Further verification will be possible by conducting the remaining test for virtualization and intelligence.

6.2 Open challenges

6.2.1 AI/ML poisoning

AI/ML security is still a topic of ongoing research. Hence, the authors are not aware of established best practices for comprehensively securing AI/ML models against poisoning and other specialized attacks. However, the industry appears to recognize this issue and work on possible mitigations. 3GPP is currently studying security aspects of AI/ML for the NG-RAN (see 3GPP TR 33.877 [46]). Aside from data poisoning, this document also discusses key issues related to secure information transfer and user privacy.

6.2.2 Privacy considerations

As described in section 2.4.2 (Risk rating), privacy involves more than just data protection. To ensure systems and services respect the privacy of individuals, aspects such as lawfulness of processing, consent, and the rights of data subjects are just as important as technical

considerations. Thus, a system-level analysis, as described in this report, cannot provide a comprehensive assessment of privacy aspects. Privacy assessments have to be performed per use case to determine the potential privacy impact and appropriate controls.

6.3 Aspects unrelated to security

6.3.1 Increased competition in the base station market

Historically, openness, i.e. standardization, has contributed to market competition and achieved cost reductions and performance improvements in various areas. (e.g. DVD, Blu-ray, SD, TCP/IP, etc.) Similarly, the widespread use of O-RAN specifications is anticipated to reduce or even eliminate the oligopoly of telecommunications base stations, and market competition between vendors is expected to improve the performance of each function while reducing the cost of equipment. In this way, an ecosystem based on O-RAN equipment offers many potential benefits for the mobile industry. Specifically, the virtualization of base stations (vRAN) enables software and hardware separation. This enables the use of general-purpose equipment instead of the expensive dedicated equipment that was previously required, which is anticipated to reduce OPEX/CAPEX. The virtualization working groups of the O-RAN Alliance, working toward its key principle of separating RAN hardware and software for all components and the deployment of software components on commodity server hardware, is helping to realize costs savings in telecommunications equipment compared to traditional vertically integrated RANs. The multi-vendor configuration of the O-RAN specification also enables the selection of best-of-breed products for various deployment scenarios. It also contributes to supply chain risk mitigation.

6.3.2 Optimizing energy efficiency through intelligence (Energy saving)

O-RAN is currently actively working on optimizing energy efficiency (Energy saving) as a means of reducing the OPEX of telecom operators, which is important in light of the rising cost of fossil fuel-based energy resources and the urgent need to reduce CO2 emissions. The optimization of O-RUs, which account for the majority of the power consumption of radio access networks, is essential for the realization of energy efficiency optimization. O-RAN Alliance standardization activities are looking at improving the overall energy consumption of radio access networks by turning off or reducing the coverage of cells with few users through Non-RT/Near-RT RIC. In addition, the use of intelligent control, such as AI/ML-based forecasting of future traffic volumes and user mobility, could further improve energy efficiency optimization.

6.3.3 Improved monitoring and maintenance functions by SMOs

In Open RAN, RIC, MANO and Slice Management support a higher level of optimization of RAN operations by using SMO. The use of a standardized interface also allows for a free choice of

applications. Automatic adjustment of RAN parameters and automation of operational settings leads to a reduction in OPEX. Furthermore, service availability can be improved by autonomous operation according to policy settings and the detection of predictive failure signs using AI/ML.

7 References

[1] O-RAN Alliance, "O-RAN Architecture Description 7.0," 2022.

[2] O-RAN Alliance, "O-RAN Security Threat Modeling and Remediation Analysis 5.0," 2022.

[3] BSI, "Open RAN Risk Analysis (5GRANR)," 2022.

[4] NIS Group, "Report on the cybersecurity of Open RAN," 2022.

[5] European Commission, "The EU Toolbox for 5G security," 2021.

[6] CISA, "Open Radio Access Network Security Considerations," 2022.

[7] IFRI, ""Open" Telecom Networks (Open RAN)," 2022.

[8] NTT Docomo, "5G Open RAN Ecosystem Whitepaper," 2021.

[9] O-RAN Alliance, "O-RAN Security Requirements Specification 5.0," 2022.

[10] O-RAN Alliance, "O-RAN Security Protocols Specifications 5.0," 2022.

[11] O-RAN Alliance, "O-RAN Management Plane Specification 11.0," 2022.

[12] 3GPP, "TS 33.501: Security architecture and procedures for 5G System; 18.0.0," 2023.

[13] 3GPP, "TS 33.210: Network Domain Security (NDS); IP network layer security; 17.1.0," 2022.

[14] CSRIC VIII, "REPORT ON CHALLENGES TO THE DEVELOPMENT OF ORAN TECHNOLOGY AND RECOMMENDATIONS ON HOW TO OVERCOME THEM," 2022.

[15] NIST, "Software Supply Chain and DevOps Security Practices: Implementing a Risk-Based Approach to DevSecOps," 2022.

[16] NIST, "SP 800-218: Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities," 2022.

[17] BSA, "The BSA Framework for Secure Software Version 1.1," 2022.

[18] SAFECode, "Managing Security Risks Inherent in the Use of Third-party Components," 2017.

[19] NIST, "Framework for Improving Critical Infrastructure Cybersecurity 1.1," 2018.

[20] O-RAN Alliance, "O-RAN Study on Security for O-Cloud 2.0," 2023.

[21] O-RAN Alliance, "O-RAN Study on Security for Service Management and Orchestration (SMO) 1.0," 2023.

[22] O-RAN Alliance, "O-RAN Study on Security for Shared O-RU (SharedORU) 1.0," 2023.

[23] NIST, "SP 800-53 Rev.5: Security and Privacy Controls for Information Systems and Organizations," 2020.

[24] O-RAN Alliance, "O-RAN Security Test Specifications 3.0," 2022.

[25] GSM Association, "FS.16 – NESAS Development and Lifecycle Security Requirements v.2.2," 2022.

[26] OWASP, "Secure Coding Practices-Quick Reference Guide," 2022.

[27] OWASP, "Top 10 Web Application Security Risks," 2021.

[28] OWASP, "Top 10 API Security," 2021.

[29] OWASP, "DevSecOps Guideline - v-0.2".

[30] NTIA, "The Minimum Elements For a Software Bill of Materials (SBOM)," 2021.

[31] NIST, "SP 800-161r1: Cybersecurity Supply Chain Risk Management Practicies for Systems and Orgnizations," 2022.

[32] NIST, "IR 7622: Notional Supply Chain Risk Management Practices for Federal Information Systems," 2012.

[33] ATIS, "ATIS Standard: 5G Network Assured Supply Chain," 2022.

[34] O-RAN Alliance, "O-RAN Fronthaul Interoperability Test Specification (IOT) 8.0," 2022.

[35] CIS, "CIS Critical Security Controls Version 8," 2021.

[36] CIS, "CIS Benchmarks".

[37] ETSI, "GS NFV-SEC 021: VNF Package Security Specification v2.6.1," 2019.

[38] CSA, "Cloud Controls Matrix and CAIQ v4," 2021.

[39] MITRE, "FiGHT™(5G Hierarchy of Threats) v1.0.0," 2022.

[40] MITRE, "ATT&CK Framework v4.0.1," 2022.

[41] O-RAN Alliance, "O-RAN TIFG, End-to-end Test Specification 4.0," 2022.

[42] 3GPP, "TS 33.117 “Catalogue of General Security Assurance Requirements” (Release 16)," 2020.

[43] O-RAN Alliance, "Security Work Group Continues Defining O-RAN Security Solutions, https://www.o-ran.org/blog/the-o-ran-alliance-security-work-group-continues-defining-o-ran-security-solutions," 2022.

[44] O-RAN Alliance, "O-RAN Control, User and Synchronization Plane Specification 11.0," 2022.

[45] O-RAN Alliance, "Security Work Group Continues Defining O-RAN Security

Solutions, https://www.o-ran.org/blog/the-o-ran-alliance-security-work-group-continues-defining-o-ran-security-solutions," 2022.

[46] 3GPP, "TR 33.877: Study on the security aspects of Artificial Intelligence (AI)/Machine Learning (ML) for the NG-RAN; 0.5.0," 2023.

Appendix

A1 Duplicate threats identified in the O-RAN Threat Modeling and Remediation Analysis

Threat ID	Title	Duplicate of	Title
T-AAL-01	Insecure API to gain access to AAL services	T-ProtocolStack-01	REST API Exploits
T-AAL-02	Internal Overload DoS attack targeting AAL services	T-O-RAN-09	Compromise of O-RAN components' integrity and availability
T-ADMIN-01	Denial of service against NFO/FOCOM	T-O-RAN-09	Compromise of O-RAN components' integrity and availability
T-FRHAUL-01	An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface	T-O-RAN-05	Penetration and compromise of the O-RAN system through the open O-RAN's Fronthaul, O1, O2, A1, and E2
T-FRHAUL-02	Unauthorized access to Open Front Haul Ethernet L1 physical layer interface(s)	T-PHYS-02	An intruder into the exchange over the Fronthaul cable network attempts to gain electronic access to cause damage or access sensitive data
T-NEAR-RT-01	Malicious xApps can exploit UE identification, track UE location and change UE priority	T-NEAR-RT-02	Risk of deployment of a malicious xApp on Near-RT RIC
T-NEAR-RT-03	Attackers exploit non authenticated, weakly or incorrectly authenticated Near-RT RIC APIs	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization

T-NEAR-RT-04	Attackers exploit non authorized Near-RT RIC APIs to access to resources and services which they are not entitled to use	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization
T-NONRTRIC-03	Data Corruption/Modification	T-O-RAN-08	Compromise of O-RAN data integrity, confidentiality and traceability
T-O-RAN-04	Jamming attack through IoT devices	T-RADIO-01	Disruption through radio Jamming , Sniffing and Spoofing
T-R1-01	Gaining unauthorized access to R1 services	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization
T-rApp-02	rApp vulnerabilities	T-GEN-01	Software flaw attack
T-rApp-03	rApps misconfiguration	T-O-RAN-02	Misconfigured or poorly configured O-RAN components
T-rApp-04	Bypassing authentication and authorization	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization
T-rApp-06	Bypassing authentication and authorization using an injection attack	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization
T-rApp-07	rApp exploits services	T-rApp-05	Malicious rApp
T-SMO-01	External attacker exploits authentication weakness on SMO	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization
T-SMO-02	External attacker exploits authorization weakness on SMO	T-O-RAN-06	Insufficient/improper mechanisms for

			authentication and authorization
T-SMO-04	Internal attacker exploits authentication weakness on a SMO function	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization
T-SMO-05	Internal attacker exploits authorization weakness on a SMO function	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization
T-SMO-09	Sensitive data in transit is exposed to an internal attacker	T-O-RAN-08	Compromise of O-RAN data integrity, confidentiality and traceability
T-SMO-10	Sensitive data at rest is exposed to an internal attacker	T-O-RAN-08	Compromise of O-RAN data integrity, confidentiality and traceability
T-SMO-11	AI/ML poisoning by internal attacker	T-ML-01	Poisoning the ML training data (Data poisoning attacks)
T-SMO-12	AI/ML exposure on external entity	T-O-RAN-08	Compromise of O-RAN data integrity, confidentiality and traceability
T-SMO-13	Malicious actor views local logs	T-O-RAN-07	Compromise of O-RAN monitoring mechanisms and log files integrity and availability
T-SMO-14	Malicious actor modifies local log entries	T-O-RAN-07	Compromise of O-RAN monitoring mechanisms and log files integrity and availability

T-SMO-15	Malicious actor deletes local log entries	T-O-RAN-07	Compromise of O-RAN monitoring mechanisms and log files integrity and availability
T-SMO-16	Malicious actor intercepts exports of local logs	T-O-RAN-07	Compromise of O-RAN monitoring mechanisms and log files integrity and availability
T-SMO-17	Malicious external actor gains unauthorized access to logs	T-O-RAN-07	Compromise of O-RAN monitoring mechanisms and log files integrity and availability
T-SMO-18	Malicious internal actor gains authorized access to logs	T-O-RAN-07	Compromise of O-RAN monitoring mechanisms and log files integrity and availability
T-SMO-19	Internal attacker exploits O2 interface to view data in transit between SMO and O-Cloud	T-O-RAN-08	Compromise of O-RAN data integrity, confidentiality and traceability
T-SMO-20	Internal attacker exploits O2 interface to modify data in transit between SMO and O-Cloud	T-O-RAN-08	Compromise of O-RAN data integrity, confidentiality and traceability
T-SMO-26	External attacker exploits External interface to view data in transit between SMO and external service	T-O-RAN-08	Compromise of O-RAN data integrity, confidentiality and traceability
T-SMO-27	External attacker exploits External interface to modify data in transit between SMO and external service	T-O-RAN-08	Compromise of O-RAN data integrity, confidentiality and traceability

T-SMO-28	External attacker uses External interface to exploit API vulnerability to gain access to SMO	T-SMO-08	Attacker exploits insecure API to gain access to SMO
T-SMO-29	External attacker floods External interface to cause DDoS at SMO	T-SMO-03	External Overload DoS attack targeted at SMO
T-SMO-30	External attacker uses External interface to gain access to sensitive data-at-rest at the SMO	T-O-RAN-06	Insufficient/improper mechanisms for authentication and authorization
T-xApp-01	xApps vulnerabilities and misconfiguration	T-GEN-01	Software flaw attack
T-xApp-03	Compromising xApp isolation	T-VM-C-02	VM/Container escape attack
T-xApp-04	False or malicious A1 policies from the Non-RT RIC inform behavior of xApps	T-O-RAN-02	Misconfigured or poorly configured O-RAN components

Threat ID	Title	STRIDE categorization	Affected component	Risk rating
T-NEARRT-02	Risk of deployment of a malicious xApp on Near-RT RIC	T	xApp	Medium
T-NEARRT-02	Risk of deployment of a malicious xApp on Near-RT RIC	I	xApp	Medium
T-NEARRT-02	Risk of deployment of a malicious xApp on Near-RT RIC	T	Near-RT RIC	Medium
T-NEARRT-02	Risk of deployment of a malicious xApp on Near-RT RIC	I	Near-RT RIC	Medium
T-NONRTRIC-01	An attacker penetrates the Non-RT RIC to cause a denial of service or degrade the performance	D	Non-RT RIC	High
T-NONRTRIC-01	An attacker penetrates the Non-RT RIC to cause a denial of service or	D	rApp	High

	degrade the performance			
T-NONRTRIC-02	UE tracking in the Non-RT RIC	I	Non-RT RIC	High
T-NONRTRIC-02	UE tracking in the Non-RT RIC	I	rApp	High
T-xApp-02	Conflicting xApps unintentionally or maliciously impact O-RAN system functions	T	xApp	Medium
T-xApp-02	Conflicting xApps unintentionally or maliciously impact O-RAN system functions	D	xApp	Medium
T-xApp-02	Conflicting xApps unintentionally or maliciously impact O-RAN system functions	T	Near-RT RIC	Medium
T-xApp-02	Conflicting xApps unintentionally or maliciously impact O-RAN system functions	D	Near-RT RIC	Medium

T-xApp-02	Conflicting xApps unintentionally or maliciously impact O-RAN system functions	T	CU	Medium
T-xApp-02	Conflicting xApps unintentionally or maliciously impact O-RAN system functions	D	CU	Medium
T-rApp-01	Conflicting rApps unintentionally or maliciously impact O-RAN system functions	D	rApp	High
T-rApp-01	Conflicting rApps unintentionally or maliciously impact O-RAN system functions	D	Non-RT RIC	High
T-rApp-05	Malicious rApp	S	rApp	High
T-rApp-05	Malicious rApp	T	rApp	High
T-rApp-05	Malicious rApp	I	rApp	High
T-rApp-05	Malicious rApp	D	rApp	High
T-rApp-05	Malicious rApp	S	Non-RT RIC	High
T-rApp-05	Malicious rApp	T	Non-RT RIC	High
T-rApp-05	Malicious rApp	I	Non-RT RIC	High
T-rApp-05	Malicious rApp	D	Non-RT RIC	High

T-R1-02	Modifying Service Heartbeat message	T	R1	High
T-R1-02	Modifying Service Heartbeat message	D	R1	High
T-R1-03	Malicious actor bypasses authentication to Request Data	I	R1	High
T-R1-04	Bypassing authorization to discover data	I	R1	High
T-R1-04	Bypassing authorization to discover data	E	R1	High
T-R1-05	Gaining unauthorized access to data	I	R1	High
T-R1-05	Gaining unauthorized access to data	E	R1	High
T-R1-06	Modifying a Data Request	T	R1	High
T-R1-06	Modifying a Data Request	I	R1	High
T-R1-06	Modifying a Data Request	D	R1	High
T-R1-07	A malicious actor snoops Data Delivery to the Data Consumer	T	R1	High
T-R1-07	A malicious	I	R1	High

	actor snoops Data Delivery to the Data Consumer			
T-A1-01	Untrusted peering between Non-RT RIC and Near-RT RIC	S	A1	High
T-A1-02	Malicious function or application monitors messaging across A1 interface	I	A1	High
T-A1-03	Malicious function or application modifies messaging across A1 interface	T	A1	High
T-ML-01	Poisoning the ML training data (Data poisoning attacks)	T	rApp	High
T-ML-01	Poisoning the ML training data (Data poisoning attacks)	T	xApp	Medium
T-ML-01	Poisoning the ML training data (Data	T	Non-RT RIC	High

	poisoning attacks)			
T-ML-01	Poisoning the ML training data (Data poisoning attacks)	T	Near-RT RIC	Medium
T-ML-02	Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy)	T	xApp	Medium
T-ML-02	Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy)	I	xApp	Medium
T-ML-02	Altering a machine learning model (System manipulation and compromise of ML data confidentiality	T	rApp	High

	and privacy)			
T-ML-02	Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy)	I	rApp	High
T-ML-02	Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy)	T	Near-RT RIC	Medium
T-ML-02	Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy)	I	Near-RT RIC	Medium
T-ML-02	Altering a machine learning model (System manipulation	T	Non-RT RIC	High

	and compromise of ML data confidentiality and privacy)			
T-ML-02	Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy)	I	Non-RT RIC	High
T-ML-03	Transfer learning attack	T	xApp	Medium
T-ML-03	Transfer learning attack	T	rApp	High
T-ML-03	Transfer learning attack	T	Near-RT RIC	Medium
T-ML-03	Transfer learning attack	T	Non-RT RIC	High

A3 Security checklist for Open RAN

A3.1 Objective of this checklist

This checklist is created as a tool with hope of the improving convenience, the security measures for Open RAN networks sufficient.

The O-RAN security requirement document is formatted as a checklist and related information (vulnerability information, threat values, etc.) is added to improve visibility and operability.

This checklist is intended to be used in the following two situations.

- For MNOs currently operating Open RAN: use the checklist to assess if the current Open RAN network deployment meets the necessary security requirements.
- For MNOs considering new Open RAN deployments: use the checklist as a reference to evaluate, eliminate or reduce security concerns prior to deploying Open RAN in the future.

In this document, we assume that 3GPP security requirements are met. Unless explicitly stated, features relate to O-RAN specifications. Therefore, the scope of this checklist is not within for the 3GPP security requirements area.

A3.2 Description of parameters in this checklist

- Number: Serial number of this checklist.
- Check Items: Security requirements to be checked.
- Check Result: Result column to be filled in by the operator/vendor.
- Rationale: An information from which the "Check Result" response filled by the operator/vendor was derived.
- Scope-Category: The classification of the check target, which is the same as the classification in the O-RAN security requirements.
- Scope-Subject: The specific name of the target component or interface. This parameter can be used to extract information for evaluation of specific components.
- Representative Threat: Typical threat information. Specific details can be found in "O-RAN Working Group 11 (Security Working Group), O-RAN Security Threat Modeling and Remediation Analysis O-R003-v05.00.01" please see the threat section in the "O-RAN Security Threat Modeling and Remediation Analysis.
- Representative Vulnerability: Typical Vulnerability Information. For specific details, please refer to the threat inventory in "O-RAN Working Group 11 (Security Working Group) O-RAN Security Threat Modeling and Remediation Analysis O-R003-v05.00.01".
- Security Baseline: Mandatory as "Basic" and enhanced as "Advanced" are assigned as security baseline of the check items.
- C.I.A: Applicable information on the security elements Confidentiality (C)/Integrity

(I)/Availability (A).

- Affected Component: Information on components that could be affected if the Check Item is not met or is insufficient.
- Service Impact: The degree of impact at the service level, expressed as High/Medium/Low.
- Scale of Impact: Network impact, expressed as High/Medium/Low.
- Impact: Impact calculated from the service level impact and network impact, expressed as High/Medium/Low.
- Source: The source document in the check items.
- Security Requirement ID: This is the security requirement ID number associated with the "Representative Threat" content of the O-RAN specification.
- Threat ID: This is the vulnerability ID number associated with the "Representative Vulnerability" content in the O-RAN specification.
- Remarks: Prepared as a free text field by the operator/vendor.

A3.3 Supplementary information

- Regarding the relationship between "Security Requirement ID" and "Threat ID".

i. For each target component name in Security Requirement ID, extract target matches by target component name in Threat ID. Associate with the security requirement content if it matches. Extract Non-RT RIC from REQ-SEC-NonRTRIC-1 as a target component element.

ii. If the content does not match the security requirement in i). Extract comprehensive Threat IDs with a higher level of abstraction that match the security requirement contents and associate them.

- Methodology for Calculating Scale of Impact.

  We use a combined evaluation of "Service Impact," which represents the impact at the service level if a threat materializes, and "Scale of Impact," which represents the impact on the network as a whole. Please see to Chapter 2.4 Risk Analysis for the calculation method regarding the calculation.

- Regarding the "Will be updated" notation of check items in this Checklist

  Check items in this Checklist are based on the security requirements established by the O-RAN Alliance, and there are some areas that are still under development as requirements. Therefore, items that are expected to be updated in the future are indicated with "n/a".

- Regarding the "n/a" notation in the "Impact" column.
  As described in Chapter 2.4 Risk Analysis, "n/a" is used for a configuration with multiple components or a wide range of targets because the impact on individual specific components unable evaluated.

- Regarding the "n/a" notation in the "Security Baseline" column.
  Check items in this Checklist are based on the security requirements established by the O-RAN Alliance, and there are some areas that are still under development as requirements. Therefore, items that are expected to be updated in the future are indicated with "n/a".

Table 22: Security checklist

Number	Check Items	Check Result	Rationale	Scope		Representative Threat	Representative Vulnerability	Security Baseline	C.I.A	Affected Component	Service Impact	Scale of Impact	Impact	Source	Security Requirement ID	Threat ID	Remarks
				Category	Subject												
1	SMO shall support forwarding of event logs to a remote location.			NFs and Apps	SMO	Malicious actor intercepts exports of local logs	Missing or weak confidentiality protection of data in transit	Basic	C	SMO Framework, SMO Functions	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-1	T-SMO-16	
2	SMO shall provide confidentiality protection for event logs over protected protocols to remote server.			NFs and Apps	SMO	Malicious actor views local logs	Missing or weak confidentiality protection of data at rest	Basic	C	SMO Framework, SMO Functions	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-2	T-SMO-13	
3	SMO may support configuration settings that allow selection of remote servers to securely transfer the event logs.			NFs and Apps	SMO	Malicious actor views local logs	Missing or weak confidentiality protection of data at rest	Advanced	C	SMO Framework, SMO Functions	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-3	T-SMO-13	
4	SMO shall be capable of logging the event logs locally on itself.			NFs and Apps	SMO	Malicious actor views local logs	Missing or weak confidentiality protection of data at rest	Basic	C	SMO Framework, SMO Functions	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-4	T-SMO-13	
5	SMO shall provide confidentiality protection for the locally stored event logs.			NFs and Apps	SMO	Malicious actor views local logs	Missing or weak confidentiality	Basic	C	SMO Framework,	Medium	High	High	O-RAN Security Requirement [9]	REQ-SEC-SMO-Log-5	T-SMO-13	

							protection of data at rest			SMO Functions				O-RAN Threat Analysis [2]			
6	SMO shall provide integrity protection for the locally stored event logs.			NFs and Apps	SMO	Malicious actor modifies local log entries	Missing integrity protection of data at rest	Basic	I	SMO Framework, SMO Functions	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-6	T-SMO-14	
7	SMO shall support access to event logs by authorized external services.			NFs and Apps	SMO	External attacker exploits authorization weakness on SMO	Missing or improperly configured authorization	Basic	C.I.A	Non-RT RIC, SMO, External interfaces	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-7	T-SMO-02	
8	SMO shall be capable of reporting to authorized external services.			NFs and Apps	SMO	External attacker exploits External interface to modify data in transit between SMO and external service	Missing integrity checking for data in transit	Basic	I	Non-RT RIC, SMO, External interfaces	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-8	T-SMO-27	
9	SMO shall be able to record all the security related log events.			NFs and Apps	SMO	External attacker exploits authentication weakness on SMO	Missing or improperly configured authentication.	Basic	C.I	Non-RT RIC, SMO Framework	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-9	T-SMO-01	
10	The security logs of SMO should be separate from other system logs.			NFs and Apps	SMO	External attacker exploits	Missing or improperly configured authentication.	Advanced	C.I	Non-RT RIC, SMO Framework	High	High	High	O-RAN Security Requirement [9]	REQ-SEC-SMO-Log-10	T-SMO-01	

						authentication weakness on SMO							O-RAN Threat Analysis [2]			
11	The SMO shall not permit configuration change to logging level(s) of any component on the SMO system without proper authorization.			NFs and Apps	SMO	Malicious internal actor gains authorized access to logs	Missing or improperly configured authorization	Basic	C	SMO Framework, SMO Functions	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SMO-Log-11	T-SMO-18	
12	The Non-RT RIC shall support authorization as a resource owner/server and client.			NFs and Apps	Non-RT RIC and rApps	An attacker penetrates the Non-RT RIC to cause a denial of service or degrade the performance.	Improper or missing authentication and authorization processes on the Non-RT RIC or SMO	Basic	A	Non-RT RIC, rApps	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NonRTRIC-1	T-NONRTRIC-01	
13	The Non-RT RIC Framework, as a resource owner/server, shall provide authorization to requests from rApps as a client.			NFs and Apps	Non-RT RIC and rApps	An attacker penetrates the Non-RT RIC to cause a denial of service or degrade the performance.	Improper or missing authentication and authorization processes on the Non-RT RIC or SMO	Basic	C.I.A	Non-RT RIC, rApps	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NonRTRIC-2	T-NONRTRIC-01	

14	rApps shall provide client authorization requests to the Non-RT RIC Framework.			NFs and Apps	rApps	An attacker bypasses authentication and authorization.	rApps may be misconfigured or compromised. Failing or misconfigured authentication and authorization in rApp.	Basic	C.I.A	rApps, Non-RT RIC	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NonRTRIC-3	T-rAPP-04	
15	rApps shall provide client authorization requests to the Non-RT RIC Framework.			NFs and Apps	rApps	An attacker bypasses authentication and authorization using an injection attack.	rApps may be misconfigured or compromised. Failing or misconfigured authentication and authorization in rApp.	Basic	C.I.A	rApps, Non-RT RIC	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NonRTRIC-3	T-rAPP-06	
16	The Non-RT RIC shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across the A1 interface, due to misbehavior or malicious intent.			NFs and Apps	Non-RT RIC and rApps	An attacker penetrates the Non-RT RIC to cause a denial of service or degrade the performance.	Improper or missing authentication and authorization processes on the Non-RT RIC or SMO	Basic	A	Non-RT RIC, rApps	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NonRTRIC-4	T-NONRTRIC-01	
17	The Non-RT RIC Framework shall be able to recover, without catastrophic failure, from a			NFs and Apps	Non-RT RIC and rApps	An attacker penetrates the Non-RT RIC to cause a	Improper or missing authentication and authorization	Basic	A	Non-RT RIC, rApps	Medium	High	High	O-RAN Security Requirement [9]	REQ-SEC-NonRTRIC-5	T-NONRTRIC-01	

	volumetric DDoS attack across the R1 interface, due to misbehavior or malicious intent.					denial of service or degrade the performance.	processes on the Non-RT RIC or SMO							O-RAN Threat Analysis [2]			
18	rApps shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across the R1 interface, due to misbehavior or malicious intent.			NFs and Apps	rApps	Conflicting rApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS	rApp stems from an untrusted or unmaintained source.	Basic	C.I.A	rApps, Non-RT RIC	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NonRTRIC-6	T-rAPP-01	
19	xApp images shall be authenticated during onboarding using a signature that is generated by the xApp Solution Provider and validated by the Service Provider.			NFs and Apps	xApps	An attacker exploits xApps vulnerabilities and misconfiguration.	xApp stems from an untrusted or unmaintained source.	Basic	C.I.A	O-CU, Near-RT RIC, xApps	Medium	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-XAPP-1	T-xAPP-01	
20	xApp instances shall be validated during Registration to the Near-RT RIC platform using signatures from both the Service Provider and the xApp Solution Provider.			NFs and Apps	xApps	An attacker exploits xApps vulnerabilities and misconfiguration.	xApp stems from an untrusted or unmaintained source.	Basic	C.I.A	O-CU, Near-RT RIC, xApps	Medium	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-XAPP-2	T-xAPP-01	

21	Near-RT RIC shall authenticate xApp access to the Near-RT RIC database(s) during SDL registration.			NFs and Apps	Near-RT RIC	Attackers exploit non authenticated, weakly or incorrectly authenticated Near-RT RIC APIs.	Non authenticated, weakly or incorrectly authenticated Near-RT RIC APIs.	Basic	C.A	Near-RT RIC, UE, xApp	Medium	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NEAR-RT-1	T-NEAR-RT-03	
22	Near-RT RIC shall provide authorized access to Near-RT RIC database(s).			NFs and Apps	Near-RT RIC	Attackers exploit non authorized Near-RT RIC APIs to access to resources and services which they are not entitled to use.	Non-authorized RT RIC APIs	Basic	C.A	Near-RT RIC, UE, xApp	Medium	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NEAR-RT-2	T-NEAR-RT-04	
23	The communication between xApps and Near-RT RIC platform APIs shall be mutually authenticated.			NFs and Apps	Near-RT RIC	Attackers exploit non authenticated, weakly or incorrectly authenticated Near-RT RIC APIs.	Non authenticated, weakly or incorrectly authenticated Near-RT RIC APIs.	Basic	C.A	Near-RT RIC, UE, xApp	Medium	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NEAR-RT-3	T-NEAR-RT-03	

24	Near-RT RIC architecture shall provide an authorization framework for the consumption of the services exposed in the platform APIs by the xApps, that takes operator policies into consideration. The framework should be used by the specified API procedures in [O-RAN.WG 3.RICARCH-v 02.01].			NFs and Apps	Near-RT RIC	Attackers exploit non authorized Near-RT RIC APIs to access to resources and services which they are not entitled to use.	Non-authorized RT RIC APIs	Basic	C.A	Near-RT RIC, UE, xApp	Medium	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NEAR-RT-4	T-NEAR-RT-04	
25	The Near-RT RIC shall support authorization as a resource owner/server (A1-P) and client (A1-EI).			NFs and Apps	Near-RT RIC	Attackers exploit non authorized Near-RT RIC APIs to access to resources and services which they are not entitled to use.	Non-authorized RT RIC APIs	Basic	C.A	Near-RT RIC, UE, xApp	Medium	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NEAR-RT-5	T-NEAR-RT-04	
26	The Near-RT RIC shall be able to recover, without catastrophic failure, from a volumetric DDoS attack across the A1 interface,			NFs and Apps	Near-RT RIC	Attackers exploit non authorized Near-RT RIC APIs to access to resources and	Non-authorized RT RIC APIs	Basic	C.A	Near-RT RIC, UE, xApp	Medium	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NEAR-RT-6	T-NEAR-RT-04	

	due to misbehavior or malicious intent.					services which they are not entitled to use.											
27	Will be updated			NFs and Apps	O-CU-CP O-CU-UP	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	n/a	C.I.A	All	High	Medium	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	-	T-O-RAN-01	
28	Will be updated			NFs and Apps	O-DU	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate	n/a	C.I.A	All	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	-	T-O-RAN-01	

							security hardening. Unnecessary or insecure function/protocol/component.										
29	Will be updated			NFs and Apps	O-RU	An attacker stands up a false base station attack by attacking an O-RU.	False O-Rus	n/a	C.I	O-RU	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	-	T-ORU-01	
30	Will be updated			NFs and Apps	O-eNB	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	n/a	C.I.A	All	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	-	T-O-RAN-01	

31	User should be authenticated and authorized.			NFs and Apps	O-Cloud/Cloud Platform Management	Abuse a O-Cloud administration service.	Lack of authentication, secret exposure (insufficient safeguarding of credentials), vulnerable code exploits, design weakness.	Advanced	C.I.A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-1	T-ADMIN-02	
32	Means of isolation of control and resources among different users shall be implemented.			NFs and Apps	O-Cloud/Cloud Platform Management	VM/Container escape attack	Shared tenancy vulnerabilities (multitenant environment), Lack of strong VM/Container isolation, lack of authentication, Insecure networking, Unrestricted communication between VMs/Containers.	Basic	C.I.A	O-Cloud, Apps/VNFs/ CNFs	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-2	T-VM-C-02	

33	The App/VNF/CNF package shall be certified by the App/VNF/CNF Provider using industry recognized software testing suites (e.g., vulnerability scanning, static and dynamic testing, penetration testing) to find any flaws and defects within the package and to eliminate them before its delivery to the Service Provider. Test results shall be shared with the Service Provider.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Software flaw attack	Vulnerable code exploits, Design Weakness.	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-1	T-GEN-01	
34	The App/VNF/CNF package shall be signed by the App/VNF/CNF Provider prior to its delivery to the Service Provider for ensuring its authenticity and integrity.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Secrets disclosure in VM/Container images.	Secret exposure in VNF/CNF images	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-2	T-IMG-03	

35	The App/VNF/CNF package shall include minimally the following artifacts according to [ETSI GS NFV-SEC 021], [ETSI GS NFV-SOL 004]: the App/VNF/CNF software image, the signing certificate, and signature(s) of App/VNF/CNF Provider.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Secrets disclosure in VM/Container images.	Secret exposure in VNF/CNF images	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-3	T-IMG-03	
36	If the App/VNF/CNF package refers to external artifacts [ETSI GS NFV-SEC 021], [ETSI GS NFV-SOL 004], those artifacts shall be signed by the App/VNF/CNF Provider.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Secrets disclosure in VM/Container images.	Secret exposure in VNF/CNF images	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-4	T-IMG-03	
37	The Service Provider shall verify the signatures on all external artifacts.			NFs and Apps	SW package protection at the O-Cloud NW functions	Untrust binding between the different O-Cloud layers.	Lack of integrity verification during boot or runtime.	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-5	T-GEN-03	

					and App layer												
38	The App/VNF/CNF package shall be validated by NFO upon its reception using the signature generated and provided by the App/VNF/CNF Provider.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Lack of Authentication & Authorization in interfaces between O-Cloud components	Lack of authentication, Insecure interfaces.	Basic	C.A	O-Cloud, Apps/VNFs/ CNFs, O2	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-6	T-GEN-04	
39	The App/VNF/CNF package shall be tested by the Service Provider for known security vulnerabilities (e.g., vulnerability scanning). All discovered vulnerabilities must be reported and remediated where possible.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack.	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-7	T-OPENSRC-01	

							vulnerabilities and untrusted libraries.										
40	The App/VNF/CNF package shall be cryptographically bound to one Telco Operator before its on-boarding to the O-Cloud images repository. This will prevent unauthorized package to be instantiated even if it has valid App/VNF/CNF certificate [ETSI GS NFV-SEC 021], [3GPP TR 33.848: Study on Security Impacts of Virtualisation], [3GPP TR 33.818].			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Untrust binding between the different O-Cloud layers.	Lack of integrity verification during boot or runtime.	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-8	T-GEN-03	
41	App/VNF/CNF packages shall be successfully authenticated and verified during instantiation to the O-Cloud Platform from the trust O-Cloud images repository			NFs and Apps	SW package protection at the O-Cloud NW	Lack of Authentication & Authorization in interfaces between	Lack of authentication, Insecure interfaces.	Basic	C.A	O-Cloud, Apps/VNFs/ CNFs, O2	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-9	T-GEN-04	

	using signatures from both App/VNF/CNF Provider and Service Provider.				functions and App layer	O-Cloud components											
42	Signatures reaching the end of their lifetime shall be renewed before the certificate times out (signatures provided by the App/VNF/CNF Provider might be ignored if the signature of the Service Provider is valid). App/VNF/CNF packages during instantiation that do not include valid certificates shall be removed from the O-Cloud images repository and from any type of O-Cloud Platform memory.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Unsecured credentials and keys	Insecure O-Cloud APIs, Lack of integrity verification during boot or runtime.	Basic	C	O-Cloud	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-10	T-GEN-05	
43	App/VNF/CNF packages stored within the O-Cloud images repository shall be protected in			NFs and Apps	SW package protection at the O-	Abuse a O-Cloud administration service.	Lack of authentication, secret exposure (insufficient safeguarding of	Basic	C.I.A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-11	T-ADMIN-02	

	terms of integrity and confidentiality.				Cloud NW functions and App layer		credentials), vulnerable code exploits, design weakness.										
44	App/VNF/CNF packages stored within the O-Cloud images repository shall be accessible to only authorized actors (e.g., authorized users and authorized systems) and over networks that enforce authentication, integrity, and confidentiality.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Abuse a O-Cloud administration service.	Lack of authentication, secret exposure (insufficient safeguarding of credentials), vulnerable code exploits, design weakness.	Basic	C.I.A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-12	T-ADMIN-02	
45	O-Cloud images repository shall be clear of vulnerable App/VNF/CNF packages and of packages with expired or missing certificates.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Abuse a O-Cloud administration service.	Lack of authentication, secret exposure (insufficient safeguarding of credentials), vulnerable code exploits, design weakness.	Basic	C.I.A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-13	T-ADMIN-02	

46	Sensitive information (e.g L1 Apps/VNFs/CNFs, keys, PII, passwords or other critical configuration data) that is needed during the lifecycle of the App/VNFs/CNFs shall be protected in terms of confidentiality at rest and in transit [CIS Benchmarks for Docker v1.4.0, Section 4.10], [ETSI GS NFV-SEC 021 NF Package Security Specification", V2.6.1 (2019-06), Section 6.4], [ETSI GS NFV-SOL 004 VNF Package and PNFD Archive specification V4.3.1 (2022-07), Section 5.5].			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Abuse a O-Cloud administration service.	Lack of authentication, secret exposure (insufficient safeguarding of credentials), vulnerable code exploits, design weakness.	Basic	C.I.A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-14	T-ADMIN-02	
47	NFO shall contain a pre-installed root certificate of trusted CA (trusted by the Telco Operator) before the on-boarding of the App/VNF/CNF package for verifying its			NFs and Apps	SW package protection at the O-Cloud NW functions	Abuse a O-Cloud administration service.	Lack of authentication, secret exposure (insufficient safeguarding of credentials), vulnerable code	Basic	C.I.A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-15	T-ADMIN-02	

	authenticity and integrity. Root certificate shall be delivered via a trusted channel separately from an App/VNF/CNF package [ETSI GS NFV-SOL 004].				and App layer		exploits, design weakness.										
48	App/VNF/CNF Packages shall contain a Change Log. Change log captures the changes from one version to another including but not limited to features added/removed, issues fixed as well as known issues not resolved [ETSI GS NFV-IFA 011].			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Denial of service against NFO/FOCOM	Lack of authentication, vulnerable code exploits, design weakness, insecure O2 interface.	Basic	A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-16	T-ADMIN-01	
49	O-Cloud Platform shall monitor stored App/VNF/CNF Packages downloaded from the O-Cloud images repository within SMO to the O-Cloud platform to determine if any unauthorized modification, deletion, or insertion has occurred.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Denial of service against NFO/FOCOM	Lack of authentication, vulnerable code exploits, design weakness, insecure O2 interface.	Basic	A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-17	T-ADMIN-01	

50	SMO and O-Cloud Platform shall support a strong protection of keys and algorithms for the code signing and encryption/decryption processes.			NFs and Apps	SW package protection at the O-Cloud NW functions and App layer	Abuse a O-Cloud administration service	Lack of authentication, secret exposure (insufficient safeguarding of credentials), vulnerable code exploits, design weakness.	Basic	C.I.A	NFO/FOCOM, O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-IMG-18	T-ADMIN-02	
51	O-Cloud shall implement means of preventing privilege escalation by Apps/VNF/CNF.			NFs and Apps	Virtualization and Isolation	Abuse of a privileged VM/Container	Misconfiguration or Insecure VM/Container configurations.	Basic	C.I.A	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-ISO-1	T-VM-C-01	
52	The communication between the different Apps/VNF/CNF shall be mutually authenticated and authorized.			NFs and Apps	Virtualization and Isolation	VM/Container hyperjacking attack	Host misconfiguration, lack of authentication.	Basic	C.I.A	O-Cloud	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-ISO-2	T-VL-01	
53	The O-Cloud consumer and provider shall together ensure that the Apps/VNF/CNF have only the minimum required capabilities and privileges as well as minimum required access to NFVI resources.			NFs and Apps	Virtualization and Isolation	VM/Container hyperjacking attack	Host misconfiguration, lack of authentication.	Basic	C.I.A	O-Cloud	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-ISO-3	T-VL-01	

54	The O-Cloud platform shall ensure that there is strict isolation between Apps/VNFs/CNFs in terms of data in transit, data in use and data at rest.			NFs and Apps	Virtualization and Isolation	Attack internal network services	Insecure O-Cloud APIs, Lack of authentication.	Basic	A	O-Cloud	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-ISO-4	T-VL-03	
55	All software within the O-Cloud platform shall be kept up to date with the last security updates for adding additional security protections and correcting vulnerabilities [49].			NFs and Apps	Secure Update	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SU-1	T-O-RAN-01	
56	Before updating O-Cloud, all O-Cloud software images shall be signed by O-Cloud Software Providers prior to their delivery to O-Cloud Service Provider for			NFs and Apps	Secure Update	Secrets disclosure in VM/Container images.	Secret exposure in VNF/CNF images	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs images	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SU-2	T-IMG-03	

	ensuring their authenticity and integrity.																
57	Before updating O-Cloud, all O-Cloud software images shall be validated by SMO upon their reception using signatures generated and provided by O-Cloud Software Providers.			NFs and Apps	Secure Update	Secrets disclosure in VM/Container images.	Secret exposure in VNF/CNF images	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs images	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SU-3	T-IMG-03	
58	The O-Cloud platform shall verify prior to the update process, the digital signature contained in the new O-Cloud software image.			NFs and Apps	Secure Update	Secrets disclosure in VM/Container images.	Secret exposure in VNF/CNF images	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs images	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SU-4	T-IMG-03	
59	In case of an incomplete update, or incident during the installation process, the O-Cloud platform shall remain in its initial working state.			NFs and Apps	Secure Update	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SU-5	T-O-RAN-01	

							Unnecessary or insecure function/protocol/component.										
60	The O-Cloud platform shall prevent the unauthorized rollback of its software to an earlier vulnerable version.			NFs and Apps	Secure Update	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SU-6	T-O-RAN-01	

61	The update of O-Cloud software should be completed with minimal disruption and downtime.			NFs and Apps	Secure Update	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Advanced	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SU-7	T-O-RAN-01	
62	All cryptographic keys and sensitive data within the O-Cloud platform shall be protected in terms of integrity and confidentiality at rest and in transit.			NFs and Apps	Secure storage of Cryptographic keys and sensitive data	An attacker compromises O-RAN data integrity, confidentiality and traceability	Improper or missing ciphering of sensitive data in storage or in transfer. Improper or missing integrity mechanisms to protect sensitive data in storage or in transfer. Presence of active function(s) that reveal	Basic	C.I	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SS-1	T-O-RAN-08	

							confidential internal data. No traceability (logging) of access to personal data.										
63	The O-Cloud platform shall delete cryptographic keys and sensitive data using a secure deletion method from both active and backup storage medias.			NFs and Apps	Secure storage of Cryptographic keys and sensitive data	VM/Container data theft	Lack of authentication, insecure data storage.	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SS-2	T-VM-C-03	

64	The O-Cloud platform shall ensure that any data contained in a resource is not available when the resource is de-allocated from one VM/Container and reallocated to a different VM/Container. This requirement requires protection for any data contained in a resource that has been logically deleted or released but may still be present within the resource which in turn may be re-allocated to another VM/Container.			NFs and Apps	Secure storage of Cryptographic keys and sensitive data	Failed or incomplete VNF/CNF termination or releasing of resources	Lack of authentication, misconfigurations (VNF/CNF, Host OS, Hypervisor/Container Engine).	Basic	C	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-SS-3	T-VM-C-06	
65	The O-Cloud platform shall support a root of trust that verifies the integrity of every relevant component in the O-Cloud platform [NIST SP 800-190 APPLICATION CONTAINER SECURITY GUIDE], [ENISA NFV SECURITY IN 5G Challenges			NFs and Apps	Chain of Trust	Abuse of a privileged VM/Container	Misconfiguration or Insecure VM/Container configurations.	Basic	C.I.A	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-COT-1	T-VM-C-01	

	and Best Practices], [IBM Securing the container platform, Build a chain of trust].																
66	It shall be possible to attest an O-RAN App/VNF/CNF through the full attestation chain from the hardware layer through the virtualization layer to the O-RAN App/VNF/CNF layer [3GPP TR 33.848: Study on Security Impacts of Virtualisation], [ETSI GR NFV-SEC 018].			NFs and Apps	Chain of Trust	VM/Container hyperjacking attack	Host misconfiguration, lack of authentication.	Basic	C.I.A	O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OCLOUD-COT-2	T-VL-01	
67	A1 interface shall support confidentiality, integrity, replay protection.			IF	A1	Untrusted peering between Non-RT-RIC and Near-RT-RIC.	weak mutual authentication.	Basic	C.I.A	A1 interface	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-A1-1	T-A1-01	
68	A1 interface shall support mutual authentication and authorization.			IF	A1	Untrusted peering between Non-RT-RIC and Near-RT-RIC.	weak mutual authentication.	Basic	C.I.A	A1 interface	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-A1-2	T-A1-01	

69	Confidentiality, Integrity and Authenticity Management Service providers and consumers that use TLS SHALL support TLS as specified in O-RAN Security Protocols Specification [O-RAN Security Protocols Specification 4.0] section 4.2.			IF	O1	An attacker penetrates and compromises the O-RAN system through the open O-RAN's Fronthaul, O1, O2, A1, and E2	Improper or missing authentication and authorization processes. Improper or missing ciphering and integrity checks of sensitive data exchanged over O-RAN interfaces. Improper or missing replay protection of sensitive data exchanged over O-RAN interfaces. Improper prevention of key reuse.	Basic	C.I.A	rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-TLS-FUN-1	T-O-RAN-05	

70	Least Privilege Access Control Management Service providers and consumers that use NETCONF SHALL support the Network Configuration Access Control Model (NACM) as specified in RFC 8341 to restrict NETCONF protocol access for users to a preconfigured subset of available NETCONF protocol operations and content.			IF	O1	An attacker exploits insufficient/improper mechanisms for authentication and authorization to compromise O-RAN components	Unauthenticated access to O-RAN functions. Improper authentication mechanisms. Use of Predefined/ default accounts. Weak or missing password policy. Lack of mutual authentication to O-RAN components and interfaces. Failure to block consecutive failed login attempts. Improper authorization and access control policy.	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-1	T-O-RAN-06	

71	The NETCONF implementation for O1 SHALL set the default values of the NACM Global Enforcement Controls as follows. • enable-nacm = true • read-default = permit • write-default = deny • exec-default = deny • enable-external-groups = true			IF	O1	An attacker exploits insufficient/improper mechanisms for authentication and authorization to compromise O-RAN components	Unauthenticated access to O-RAN functions. Improper authentication mechanisms. Use of Predefined/ default accounts. Weak or missing password policy. Lack of mutual authentication to O-RAN components and interfaces. Failure to block consecutive failed login attempts. Improper authorization and access control policy.	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-2	T-O-RAN-06	

72	Management Service providers that support NETCONF SHALL support the following pre-defined groups in NACM to restrict NETCONF protocol access for users. • O1_nacm_management: Allows changes to the /nacm objects which includes the NACM Global Enforcement Controls. • O1_user_management: Allows assignment and deletion of users and assignment of users to roles on the O1 node. o Mandatory if the network device supports a local user store. o Not provided if the network device does not support a local user store and requires all user/role information to be provided by an external			IF	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-3	T-O-RAN-01	

	authentication/authorization service. • O1_network_management: Allows read, write and execute operations on the <running> datastore and read, write, execute and commit operations on the <candidate> datastore if <candidate> is supported. All operations on the /nacm objects are prohibited. • O1_ network_monitoring: Allows read operations on configuration data in the <running> datastore, except for the /nacm objects. • O1_software_management: Allows installation of new software including new software versions.																

73	Users assigned to the O1_nacm_management group SHALL have read and write permission for the /nacm objects and attributes, which include the NACM Global Enforcement Controls.			IF	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-4	T-O-RAN-01	
74	Users assigned to the O1_user_management group SHALL have read and write permissions for the locally defined user store objects and attributes.			IF	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-5	T-O-RAN-01	

							function/protocol/component.										
75	Users assigned to the O1_network_management group SHALL have read, write and execute permissions for the <running> datastore and read, write, execute and commit permissions on the <candidate> datastore if <candidate> datastore is supported. Users assigned to the O1_network_management group SHALL NOT have any permissions for the /nacm objects.			IF	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-6	T-O-RAN-01	

76	Users assigned to the O1_network_monitoring group SHALL have read permissions for the <running> datastore. Users assigned to the O1_network_monitoring group SHALL NOT have read permissions for the /nacm objects.			IF	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-7	T-O-RAN-01	
77	Users assigned to the O1_software_management group SHALL have permissions to install new software.			IF	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-8	T-O-RAN-01	

							function/protocol/component.										
78	NETCONF endpoints SHALL support external user to group mapping via at least one of the following protocols: LDAP with StartTLS [RFC4513], OAuth 2.0, RADIUS with EAP, and TACACS/TACACS+.			IF	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Basic	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-9	T-O-RAN-01	

79	Management Service providers MAY allow the definition of users in the <groups> NACM object.			IF	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	Advanced	C.I.A	All	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-NAC-FUN-10	T-O-RAN-01	
80	O2 interface shall support confidentiality, integrity, replay protection and data origin authentication.			IF	O2	MitM attacks on O2 interface between O-Cloud and SMO	Insecure O2 interface, lack authentication.	Basic	C.I.A	O2	High	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-O2-1	T-O2-01	

81	E2 interface shall support confidentiality, integrity, replay protection and data origin authentication.			IF	E2	An attacker penetrates and compromises the O-RAN system through the open O-RAN's Fronthaul, O1, O2, A1, and E2.	Improper or missing authentication and authorization processes. Improper or missing ciphering and integrity checks of sensitive data exchanged over O-RAN interfaces. Improper or missing replay protection of sensitive data exchanged over O-RAN interfaces. Improper prevention of key reuse.	Basic	C.I.A	rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-E2-1	T-O-RAN-05	
82	The C-Plane shall support authentication and authorization of O-DUs that exchange C-plane messages with O-RUs.			IF	Open Fronthaul C-plane	Spoofing of DL C-plane messages	Lack of authentication could allow an adversary to inject own DL C-plane messages.	Basic	A	O-DU, O-RU	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OFCP-1	T-CPLANE-01	

83	Open Fronthaul U-plane transports 5G System Control Plane and User Plane messages between O-CU-CP and UE, and O-CU-UP and UE. The Packet Data Convergence Protocol (PDCP) [3GPP TS 38.323 NR] provides confidentiality and integrity protection of 5G System Control Plane and User Plane between O-CU-CP and UE, and O-CU-UP and UE.			IF	Open Fronthaul U-plane	An attacker attempts to intercept the Fronthaul (MITM) over U Plane	Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements.	Basic	C.I.A	O-DU, O-RU	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	n/a	T-UPLANE-01	
84	The S-Plane shall support authentication and authorization of PTP nodes that communicate with other PTP nodes within Configuration LLS-C1, Configuration LLS-C2, or Configuration LLS-C3. NOTE: This ensures least privilege access to the S-Plane where authenticated and authorized PTP nodes			IF	Open Fronthaul S-plane	A Rogue PTP Instance wanting to be a Grand Master	Inaccurate timing information. Improper synchronization between clocks. ANNOUNCE messages can be sent publicly in clear text.	Basic	A	O-DU, O-RU	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OFSP-1	T-SPLANE-03	

	communicate over the Open Fronthaul network. NOTE: There is no specific requirement for authentication and authorization mechanism of S-plane PTP messages.																
85	The S-Plane should provide a means to prevent spoofing of master clocks.			IF	Open Fronthaul S-plane	Impersonation of a Master clock (Spoofing) within a PTP network with a fake ANNOUNCE message	Inaccurate timing information. Improper synchronization between clocks. ANNOUNCE messages can be sent publicly in clear text.	Advanced	A	O-DU, O-RU	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OFSP-2	T-SPLANE-02	
86	For the O-DU at the Data Centre deployment model the S-Plane should protect against MITM attacks that degrade the clock accuracy due to packet delay attacks or selective			IF	Open Fronthaul S-plane	Packet delay manipulation attack	Inaccurate timing information. Improper synchronization between clocks. ANNOUNCE messages	Advanced	A	O-DU, O-RU	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OFSP-3	T-SPLANE-05	

	interception and removal attacks [RFC 7384].						can be sent publicly in clear text.										
87	The Open Fronthaul shall provide a means to authenticate and authorize point-to-point LAN segments between Open Fronthaul network elements.			IF	Open Fronthaul M-plane	An attacker attempts to intercept the Fronthaul (MITM) over M Plane	Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements.	Basic	C.A	Near-RT RIC, Non-RT RIC, O-CU, O-DU, SMO	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OFHPLS-1	T-MPLANE-01	
88	The Open Fronthaul shall provide a means to detect and report when an authorized point-to-point LAN segment is made or broken.			IF	Open Fronthaul M-plane	Unauthorized access to Open Front Haul Ethernet L1 physical layer interface(s)	Lack of authentication and access control to the Open Front Haul Ethernet L1 physical layer interface.	Basic	C.I.A	rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OFHPLS-2	T-FRHAUL-02	

89	The Open Fronthaul shall provide a means to block access to unused Ethernet ports in an Open Fronthaul network element. Open Fronthaul implementations may support IEEE 802.1X-2020 to satisfy the requirements listed above. Implementations that support optional 802.1X shall provide the security controls as specified in sections 5.2.5.5.2 and 5.2.5.5.3.			IF	Open Fronthaul M-plane	Unauthorized access to Open Front Haul Ethernet L1 physical layer interface(s)	Lack of authentication and access control to the Open Front Haul Ethernet L1 physical layer interface.	Basic	C.I.A	rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC	High	Low	Medium	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-OFHPLS-3	T-FRHAUL-02	
90	R1 interface shall support confidentiality, integrity, and replay protection.			IF	R1	An attacker gains unauthorized access to R1 services.	weak mutual authentication.	Basic	C.I.A	R1 interface	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-R1-1	T-R1-01	
91	R1 interface shall support mutual authentication and authorization.			IF	R1	Malicious actor bypasses authentication to Request Data.	weak mutual authentication.	Basic	C.I.A	R1 interface	Medium	High	High	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-R1-2	T-R1-03	

92	The Application Package shall be digitally signed by the Solution Provider.			Transversal	Common Application Lifecycle Management	Secrets disclosure in VM/Container images.	Secret exposure in VNF/CNF images	Basic	C.I	O-Cloud, Apps/VNFs/ CNFs images	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-ALM-FUN2-1	T-IMG-03	
93	The SMO shall have the capability to verify the digital signature of the Application Package.			Transversal	Common Application Lifecycle Management	Abuse a O-Cloud administration service.	Lack of authentication, secret exposure (insufficient safeguarding of credentials), vulnerable code exploits, design weakness.	Basic	C.I.A	NFO/FOCOM , O-Cloud, Apps/VNFs/ CNFs	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-ALM-FUN3-1	T-ADMIN-02	
94	A list of network protocols and services supported on the O-RAN component shall be clearly documented by its vendor. Unused protocols shall be disabled.			Transversal	Network Protocols and Services	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-NET-1	T-O-RAN-01	

							function/protocol/component.										
95	Common transport protocols (IP, UDP, TCP, SCTP, SSH, HTTP and HTTP2) used in O-RAN system should be able to handle unexpected inputs (not in-line with protocol specification) without functional compromise. The unexpected inputs include random mutations of the protocol headers and payloads, as well as targeted fuzzing with state awareness.			Transversal	Robustness of Common Transport Protocols	Attacks from the internet exploit weak authentication and access control to penetrate O-RAN network boundary	Errors in the design and implementation of the network protocols (HTTP, P, TCP, UDP, application protocols).	Advanced	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-TRAN-1	T-O-RAN-03	

96	An O-RAN component with external network interface shall be able to withstand network transport protocol based volumetric DDoS attack without system crash and returning to normal service level after the attack.			Transversal	Robustness against Volumetric DDoS Attack	An attacker penetrates and compromises the O-RAN system through the open O-RAN's Fronthaul, O1, O2, A1, and E2	Improper or missing authentication and authorization processes. Improper or missing ciphering and integrity checks of sensitive data exchanged over O-RAN interfaces. Improper or missing replay protection of sensitive data exchanged over O-RAN interfaces. Improper prevention of key reuse.	Basic	C.I.A	rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-DOS-1	T-O-RAN-05	
97	Known vulnerabilities in the OS and applications of an O-RAN component shall be clearly identified and documented by its vendor.			Transversal	Robustness of OS and Applications	Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-SYS-1	T-OPENSRC-01	

						attacker through a backdoor attack.	Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.										
98	If password is used as an authentication attribute, O-RAN component vendors shall follow security best practices to mitigate risks resulting from different password-based authentication attacks such as brute-forcing, unauthorized password resets, man-in-the-middle, and dictionary attacks.			Transversal	Password-Based Authentication	Attacks from the internet exploit weak authentication and access control to penetrate O-RAN network boundary	Errors in the design and implementation of the network protocols (HTTP, P, TCP, UDP, application protocols).	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SEC-PASS-1	T-O-RAN-03	
-	The SBOM delivery should be made under contractual agreement with specific terms that include the following items:			SBOM	-	-	-	Basic	-	-				O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	Prerequisite of SBOM	-	

99	The O-RAN vendor should provide the SBOM with every O-RAN software delivery, including patches, to the network operator.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	Advanced	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-001	T-OPENSRC-01	
100	The minimum set of data fields must be according to NTIA guidance. Additional fields may be required on a contractual basis.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-002	T-OPENSRC-01	

							vulnerabilities and untrusted libraries.											

101	Vulnerabilities must not be included as an additional data field because it would represent a static view from a specific point in time, while vulnerabilities are constantly evolving. NOTE: The SBOM should be used by vendors and operators to periodically check against known vulnerability databases to identify potential risk. NOTE: The level of risk for a vulnerability should be determined by the software vendor and operator with consideration of the software product, use case, and network environment. NOTE: The SBOM provides transparency into the use of open-source software having known vulnerabilities or			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-003	T-OPENSRC-01	

	contributions from individuals or companies in adversarial nations, but it does not protect against zero-day vulnerabilities that were unintentionally or maliciously inserted, exploited, or discovered and not reported.																
102	SBOM Depth must be provided at top-level.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-004	T-OPENSRC-01	

						attacker through a backdoor attack	Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.										
103	SBOM depth must be provided to a second-level for O-RAN Software Community (OSC) sourced software to indicate which OSC modules are used and which individual and/or company contributed the software for that module.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-005	T-OPENSRC-01	

104	SBOM depth should be provided to second-level for any used open source software.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	Advanced	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-006	T-OPENSRC-01	
105	A hash must be generated for the SBOM.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-007	T-OPENSRC-01	

							vulnerabilities and untrusted libraries.										
106	A digital signature must be provided for the SBOM.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-008	T-OPENSRC-01	

107	Access control to the SBOM must be established on a need-to-know basis to limit security risk and protection of intellectual property. Access controls should be agreed upon between the vendor and operator and contractually specified.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-009	T-OPENSRC-01	
108	The SBOM must be encrypted in transfer and storage. NOTE: As stated in the DoC/NTIA report, "…some have raised concerns that adversaries could take advantage and target those critical components for novel attacks. Further research is necessary to understand the optimal structure and incentives			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-010	T-OPENSRC-01	

	for sharing, protecting, and using SBOM data."						vulnerabilities and untrusted libraries.										
109	The SBOM must be provided in Software Package Data eXchange (SPDX), CycloneDX, or Software Identification (SWID) format. NOTE: ISO/IEC 5962:2021 - Information technology — SPDX® Specification V2.2.1, published August 2021, specifies SPDX as the standard data format for communicating the component and metadata information associated with SBOM.			SBOM		Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Inaccurate inventories of open-source software. Lack of consistent Supply Chain traceability and security. Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	Basic	C.I.A	All	n/a	n/a	n/a	O-RAN Security Requirement [9] O-RAN Threat Analysis [2]	REQ-SBOM-011	T-OPENSRC-01	

*This report was commissioned and financed by the Ministry of Internal Affairs and Communications of Japan, prepared in cooperation with industrial partners including a MNO and cybersecurity companies and reported to the Quad Critical and Emerging Technology Working Group.