   O-RAN.WG11.Threat-Modeling.O-R003-v03.0

Technical Report

Copyright © 2024 by the O-RAN ALLIANCE e.V.

The copying or incorporation into any other work of part or all of the material available in this specification in any form without the prior written permission of O-RAN ALLIANCE e.V. is prohibited, save that you may print or download extracts of the material of this specification for your personal use, or copy the material of this specification for the purpose of sending to individual third parties for their information provided that you acknowledge O-RAN ALLIANCE as the source of the material and that you inform the third party that these conditions apply to them and that they must comply with them.

O-RAN ALLIANCE e.V., Buschkauler Weg 27, 53347 Alfter, Germany

Register of Associations, Bonn VR 11238, VAT ID DE321720189

O-RAN Work Group 11 (Security Work Group)

O-RAN Security Threat Modeling and Risk Assessment

Contents

List of figures 8

List of tables 9

Intellectual Property Rights (IPR) 10

Foreword 10

Modal verbs terminology 11

1 Scope 11

2 References 11

3 Definition of terms, symbols and abbreviations 13

3.1 Definition of terms 13

3.2 Symbols 13

3.3 Abbreviations 13

4 Overview 15

4.1 Objective and structure 15

4.2 Methodology 16

4.3 Perimeter 17

4.3.1 Scope regarding architecture 17

4.3.2 Out of scope components 18

5 Statement of compatibility with 3GPP 19

5.1 Assets and Threats 19

5.2 Security requirements 19

6 Roles-Assumptions-Assets 20

6.1 Stakeholders roles and responsibilities 20

6.2 Assumptions and prerequisites 23

6.3 Critical assets 24

7 Threat model 35

7.1 Threat surface 35

7.2 Threat agent 35

7.3 Potential vulnerabilities 35

7.4 Threats 36

7.4.1 Threats against O-RAN system 37

7.4.2 Threats against O-CLOUD 56

7.4.3 Threats to open source code 70

7.4.4 Physical Threats 71

7.4.5 Threats against 5G radio networks 71

7.4.6 Threats against ML system 72

7.4.7 Protocol Stack Threats 73

7.4.8 SMO Threats 74

7.4.9 Threats against Shared O-RU 82

7.5 Coverage matrix of threats 94

8 Security principles 109

8.1 Principles (SP) 109

8.1.1 SP-AUTH Mutual Authentication 109

8.1.2 SP-ACC Access Control 109

8.1.3 SP-CRYPTO Secure cryptographic, key management and PKI 109

8.1.4 SP-TCOMM Trusted Communication 109

8.1.5 SP-SS Secure storage 110

8.1.6 SP-SB Secure boot and self-configuration 110

8.1.7 SP-UPDT Secure Update 110

8.1.8 SP-RECO Recoverability & Backup 110

8.1.9 SP-OPNS Security management of risks in open-source components 110

8.1.10 SP-ASSU Security Assurance 111

8.1.11 SP-PRV Privacy 111

8.1.12 SP-SLC Continuous security development, testing, logging, monitoring and vulnerability handling 111

8.1.13 SP-ISO Robust Isolation 111

8.1.14 SP-PHY Physical security 111

8.1.15 SP-CLD Secure cloud computing and virtualization 112

8.1.16 SP-ROB Robustness 112

8.1.17 SP-IDM O-Cloud ID secure management 112

8.2 Coverage Threats - Security principles 112

9 Risk assessment 116

9.1 Determination of severity level process 116

9.2 Determination of likelihood level process 119

9.3 Evaluation of the risks process 120

9.4 Risk assessment output 120

Revision history 144

History 144

# List of figures

[**Figure 4‑1 : Logical Architecture of O-RAN system [6]** 18](#_Toc161747992)

[Figure 7‑1 : Threats and Vulnerabilities for O-RAN LLS 7-2x 40](#_Toc161747993)

[Figure 7‑2 : UE Identification in Near-RT-RIC 45](#_Toc161747994)

[Figure 7‑3 : Near-RT-RIC and xApps conflict with gNB 48](#_Toc161747995)

[**Figure 7‑4 : A1 interface between the Non-RT RIC and the Near-RT RIC** 52](#_Toc161747996)

[**Figure 7‑5 : RAN analytics information (RAI) services via Y1 service interface** 55](#_Toc161747997)

[Figure 7‑6 : Illustration of the VM/Container escape attack 59](#_Toc161747998)

[Figure 7‑7 : Illustration of the migration flooding attack 61](#_Toc161747999)

[Figure 7‑8 : Illustration of the false resource advertising attack 61](#_Toc161748000)

[Figure 7‑9 : Illustration of the migration MITM attack 61](#_Toc161748001)

[Figure 7‑10 : Illustration of the Theft-of-Service/DoS Attack 62](#_Toc161748002)

[Figure 7‑11 : Illustration of the VM/Container hyperjacking attack 64](#_Toc161748003)

[Figure 7‑12 : Illustration of a cross VM/Container side channel attack 66](#_Toc161748004)

[**Figure 7‑13 : REST Protocol Stack for the A1 and R1 Interfaces** 73](#_Toc161748005)

[Figure 9‑1 : Main concepts of risk assessment 116](#_Toc161748006)

# List of tables

[Table 5‑1 : Statement of compatibility with 3GPP – Assets and Threats 19](#_Toc161748007)

[Table 5‑2 : Statement of compatibility with 3GPP – Security requirements 19](#_Toc161748008)

[Table 6‑1 : Roles and responsibilities 20](#_Toc161748009)

[Table 6‑2 : Critical assets 26](#_Toc161748010)

[Table 7‑1 : O-RAN Threat Inventory 95](#_Toc161748011)

[Table 8‑1 : Coverage Security principles-Threats (1/2) 113](#_Toc161748012)

[Table 8‑2 : Coverage Security principles-Threats (2/2) 114](#_Toc161748013)

[Table 9‑1 : Severity rating 116](#_Toc161748014)

[Table 9‑2 : Likelihood rating 119](#_Toc161748015)

[Table 9‑3 : Risk assessment matrix 120](#_Toc161748016)

[Table 9‑4 : Risk Assessment 121](#_Toc161748017)

# Intellectual Property Rights (IPR)

This Intellectual Property Rights Policy (“IPR Policy”) will apply to documents or code developed by the O-RAN ALLIANCE for the purpose of describing key components of a Radio Access Network and their interconnections and performance, including in particular, but not limited to, the functions, behaviors, and requirements for systems, subsystems, software modules, and hardware modules, and the details of the interfaces and APIs that interconnect these components to each other or to external systems and components as well as future amendments or revisions thereto, if any. Except as otherwise defined, all capitalized terms will have the meaning defined for them in the O-RAN Constitution

# Foreword

This Technical Report (TR) has been produced by O-RAN Alliance.

The content of the present document is subject to continuing work within O-RAN and may change following formal O-RAN approval. Should the O-RAN Alliance modify the contents of the present document, it will be re-released by O-RAN with an identifying change of version date and an increase in version number as follows:

version xx.yy.zz

where:

xx: the first digit-group is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc. (the initial approved document will have xx=01). Always 2 digits with leading zero if needed.

yy: the second digit-group is incremented when editorial only changes have been incorporated in the document. Always 2 digits with leading zero if needed.

zz: the third digit-group included only in working versions of the document indicating incremental changes during the editing process. External versions never include the third digit-group. Always 2 digits with leading zero if needed.

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the O-RAN Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in O-RAN deliverables except when used in direct citation.

# Scope

The contents of the present document are subject to continuing work within O-RAN and may change following formal O-RAN approval. Should the O-RAN Alliance modify the contents of the present document, it will be re-released by O-RAN with an identifying change of version date and an increase in version number as follows:

version xx.yy.zz

where:

xx: the first digit-group is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc. (the initial approved document will have xx=01). Always 2 digits with leading zero if needed.

yy: the second digit-group is incremented when editorial only changes have been incorporated in the document. Always 2 digits with leading zero if needed.

zz: the third digit-group included only in working versions of the document indicating incremental changes during the editing process. External versions never include the third digit-group. Always 2 digits with leading zero if needed.

This technical report describes the O-RAN Security Threat Modeling and Risk Assessment. It identifies assets to be protected, analyzes the O-RAN components for vulnerabilities, examines potential threats associated with those vulnerabilities, provides security principles which stakeholders should adress when building a secure end-to-end O-RAN system and assesses the risks of the identified threats based on impact and likelihood factors.

NOTE: The present document is transformed from a Technical Specification (TS) to a Technical Report (TR) as it doesn’t containe normartive requirements. Instead, it is an informative document that serves as a vital resource for understanding the potential risks within O-RAN and defining appropriate requirement/controls to mitigate them effectively.

# References

References are either specific (identified by date of publication and/or edition number or version number) or non‑specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

**NOTE**: While any hyperlinks included in this clause were valid at the time of publication, O-RAN cannot guarantee their long-term validity.

1. 3GPP TR 21.905: Vocabulary for 3GPP Specifications
2. 3GPP TS 33.511: Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class
3. 3GPP TS 33.501: Security architecture and procedures for 5G system
4. 3GPP TR 33.926: Security Assurance Specification (SCAS) threats and critical assets in 3GPP network product classes
5. 3GPP TS 33.117: Catalogue of general security assurance requirements
6. ORAN ALLIANCE TS “O-RAN Architecture Description”
7. ISO 27005: Information security, cybersecurity and privacy protection — Guidance on managing information security risks
8. O-RAN ALLIANCE TS “Near-RT RIC Architecture”
9. O-RAN ALLIANCE TS “O-RAN Acceleration Abstraction Layer General Aspects and Principles”
10. O-RAN ALLIANCE: O-RAN WG4 “Control, User and Synchronization Plane Specification”
11. O-RAN ALLIANCE TR “Cloud Architecture and Deployment Scenarios for O-RAN Virtualized RAN“
12. ERICSSON ‘Security Considerations of Open RAN’ whitepaper and slides.
13. NIST Special Publication 800-154 2 Guide to Data-Centric System Threat Modeling
14. Resource Allocation Scheme in 5G Network Slices
15. 3GPP TR 33.818: “Security Assurance Methodology (SECAM) and Security Assurance Specification (SCAS) for 3GPP virtualized network products”.
16. Fraunhofer AISEC - threat analysis of container-as-a-service for network function virtualization
17. Ecology-Based DoS Attack in Cognitive Radio Networks
18. AN ARCHITECTURAL RISK ANALYSIS OF MACHINE LEARNING SYSTEMS: Toward More Secure Machine Learning
19. 5G Americas Whitepaper October 2018 “The Evolution of Security in 5G”
20. 3GPP TR 33.845: Study on security aspects of the 5G Service Based Architecture (SBA)
21. OWASP API Security Top 10
22. MITRE ATT&CK containers matrix
23. 3GPP TR 33.848: Study on security impacts of virtualisation
24. Graz University of Technology (2018), Meltdown and Specter
25. O-RAN ALLIANCE TS: "Near-Real-time RAN Intelligent Controller and E2 interface; E2 General Aspects and Principles"
26. NIST Special Publication 800-207, “Zero Trust Architecture,” <https://csrc.nist.gov/publications/detail/sp/800-207/final>
27. O-RAN ALLIANCE TS: "Management Plane Specification".
28. CWE-524, "Use of Cache Containing Sensitive Information", <https://cwe.mitre.org/data/definitions/524.html>
29. CAPEC-204, “Lifting Sensitive Data Embedded in Cache”, <https://capec.mitre.org/data/definitions/204.html>
30. Infiltrating Corporate Intranet Like NSA, <https://i.blackhat.com/USA-19/Wednesday/us-19-Tsai-Infiltrating-Corporate-Intranet-Like-NSA.pdf>

# Definition of terms, symbols and abbreviations

## Definition of terms

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1], O-RAN [6], [9], [11] and the following apply:

**O-Cloud instance ID**: The O-Cloud instance ID is a unique identifier assigned to components within the O-Cloud platform, including VMs, pods, containers, nodes, and compute pools (i.e., a cluster in Kubernetes). This ensures uniqueness across the entire O-Cloud environment, irrespective of the component type. For instance, a VM, a pod, a container, a node, and a cluster will each have a distinct O-Cloud instance ID within the platform, ensuring that there is no ambiguity in identification.

**Radio jamming** is the deliberate jamming, blocking or creating interference with authorized wireless network. A radio jammer is a transmitter that tunes to the same frequency as the opponents’ receiving equipment and with the same type of modulation, with enough power to override any signal at the receiver.

**Radio Sniffing** technique helps to decode all sorts of essential network configuration details easily with low-cost software radios. Sniffing information can aid attackers in optimizing and crafting attacks.

**RF spoofing** refers to transmitting a fake signal meant to pretense as an actual signal.

**Y1**: An interface over which RAN analytics services are exposed by the Near-RT RIC to be consumed by Y1 consumers.

**Y1 consumers**: A role played by entities within or outside of the PLMN trust domain that consumes the Y1 services produced by the Near-RT RIC.

## Symbols

For the purposes of the present document, the symbols apply: none

## Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 and the following apply:

|  |  |
| --- | --- |
| AAL | Acceleration Abstraction Layer |
| AALI | Acceleration Abstraction Layer Interface |
| AALI-C | Acceleration Abstraction Layer Interface-Common |
| AALI-C-App | Acceleration Abstraction Layer Interface-Common-Application |
| AALI-C-Mgmt | Acceleration Abstraction Layer Interface-Common-Management |
| AALI-P | Acceleration Abstraction Layer Interface-Profile |
| AI/ML | Artificial Intelligence/Machine Learning |
| DL | Down Link |
| DoS | Denial of Service |
| eNB | eNodeB (applies to LTE) |
| FH | Front haul |
| FTP | File Transfer Protocol |
| FTPS | File Transfer Protocol Secure |
| GM | Grand Master |
| gNB | gNodeB (applies to NR) |
| IPSEC | Internet Protocol Security |
| KPI | Key Performance Indicator |
| KQI | Key Quality Indicator |
| L1 | Layer 1 |
| LAA | Licensed-Assisted Access |
| LBT | Listen Before Talk |
| LLS | Lower Layer Split |
| MIMO | Multiple Input, Multiple Output |
| MITM | Man In The Middle |
| MNO | Mobile Network Operator |
| NETCONF | Network Configuration Protocol |
| NF | Network Function |
| NFV | Network Function Virtualisation |
| NR-U | New Radio Unlicensed |
| O-DU | O-RAN Distributed Unit |
| O-RU | O-RAN Radio Unit |
| PDCP | Packet Data Convergence Protocol |
| PRB | Physical Resource Block |
| PTP | Precision Timing Protocol |
| QoE | Quality of Experience |
| RBAC | Role-based Access Control |
| RIC | O-RAN RAN Intelligent Controller |
| RU | Radio Unit |
| SDN | Software Defined Network |
| SINR | Signal-to-Interference-plus-Noise Ratio |
| SMO | Service Management and Orchestration |
| SSH | Secure Shell |
| T-TC | Telecom Transparent Clock |
| TC | Transparent Clock |
| TLS | Transport Layer Security |
| UAV | Unmanned Aerial Vehicle |
| UL | Up Link |
| V2X | Vehicle to Everything |
| VM | Virtual machine |
| VNF | Virtualised Network Function |
| ZT | Zero Trust |
| ZTA | Zero Trust Architecture |

# Overview

## Objective and structure

O-RAN architecture [6] differs significantly from the architecture of 3GPP RAN. It involves introducing new components, interfaces, and technologies, which give rise to new actors (stakeholders) and enable novel business models. Consequently, the attack surface expands considerably, and we anticipate that O-RAN design and deployment will present numerous security challenges and associated risks. These challenges primarily stem from various factors, such as the inclusion of O-RAN specific interfaces and components, the utilization of virtualization/containerization techniques, the incorporation of open-source code, and the capability to support AI/ML models, among other considerations.

Additionally, the O-RAN architecture is being developed using zero trust (ZT) and zero trust architecture (ZTA) principles as described in the NIST Zero Trust Architecture Special Publication [26]. Zero trust is an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned). Zero trust also assumes that an adversary can always be in the network. According to the publication [26], zero trust is based on the following tenets that can be adapted to the O-RAN architecture. Full descriptions of each tenet can be found in [26].

* [ZT-1] All data sources and computing services are considered resources.
* [ZT-2] All communication is secured regardless of network location.
* [ZT-3] Access to individual enterprise resources is granted on a per-session basis.
* [ZT-4] Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
* [ZT-5] The enterprise monitors and measures the integrity and security posture of all owned and associated assets. No asset is inherently trusted.
* [ZT-6] All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
* [ZT-7] The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

Therefore, the security analysis and the threat model for O-RAN must be carefully studied and relevant assets/stakeholders/vulnerabilities/threats/requirements/countermeasures/recommendations must be identified to reduce risk exposure, mitigate any harmful effects, and drive to a ZTA.

The material presented in this analysis aims at supporting various O-RAN stakeholders understanding the relevant threats resulting to an exposure of O-RAN assets by exploiting the vulnerabilities.

The objective is to give a comprehensive and high-level view on how security is organized in O-RAN system. In this document, we assume that 3GPP security requirements are met. Unless explicitly stated, features relate to O-RAN specifications.

This analysis is consolidated from various relevant sources, including main 5G standardization documents and telecommunication best practices (e.g., 3GPP, ETSI, NIST, ENISA).

The first main part outlines the main stockholder roles involved in managing and using O-RAN system. Further, it addresses the prerequisites and assumptions needed to securely implement and run O-RAN systems. It also identifies the list of critical assets to be protected in integrity, availability, confidentiality, replay and authenticity.

The second main part addresses the threat model. It identifies the threat agents, determines the threat surface, identifies vulnerabilities, and lists the threats for each O-RAN component or interface. For each threat, the description, threatened asset(s), vulnerabilities, threat agents and affected components are given.

The third main part describes the security principles to be achieved to counter the identified threats. In addition, it illustrates the coverage between threats and security principles.

The fourth main part is the risk assessment of the identified threats in terms of severity and likelihood.

**NOTE 1**: The present document document focuses only on the components, interfaces and protocols specified by O-RAN alliance. Components, interfaces and protocols specified by 3GPP are only referenced where needed but are not within the scope of this specific O-RAN security analysis.

**NOTE 2**: The present document is a working document with the need to update the content on a regular basis following the risk evaluation.

**NOTE 3**: In this document, the term NF (Network Function) is used to designate either VNF (Virtual Network Function), CNF (Cloud-native Network Function) or PNF (Physical Network Function).

**NOTE 4**: Terms “Containers” and “Virtual Machines” are used interchangeably in this document as the implementation of O-RAN SW components could either be container-based, VM-based or hybrid (Containers and VMs together).

## Methodology

The methodology adopted in this document is based on the standard ISO 27005 [7] which provide a detailed and flexible structure to release a risk assessment.

Refer to NIST SP 800-154 [13] for the definition of Attack, Attack Surface, Attack Vector, Controls, Risk, Risk Mitigation, Threat, and Vulnerability.

The methodology followed in this document comprises three stages:

1. Identification
   1. **Identify stakeholders:** First, we need to identify the stakeholders involved in the implementation, management, operation and maintenance of the O-RAN system. Roles and responsibilities of each stakeholder are given.
   2. **Define assumptions:** The list of minimum prerequisites and assumptions need to be defined for the operational environment (not under the control of the O-RAN system) required to successfully operate the O-RAN system.
   3. **Identify assets:** First, we need to locate relevant assets the O-RAN system hold and give details about the type (Data, component, etc.), the security properties (CIA) at rest and in transit and location.
   4. **Identify threats:** We need to identify the relevant threats associated with the new O-RAN components, interfaces and technologies. In addition, the threat surface and agents are given.
   5. **Identify vulnerabilities:** O-RAN system may have weaknesses in its new O-RAN components, interfaces and technologies which need to be identified.
   6. **Define security principles:** We need to define security principles to be achieved in order to reduce risk exposure.
   7. **Elaborate and refine security principles:** Each security principle needs to be detailed and refined into requirements, recommendations and countermeasures.
   8. **Identify existing/ongoing countermeasures:** We need to identify all of O-RAN existing/ongoing controls and to take into account the protection provided by these controls before applying any new ones.
2. Risk assessment

The value for *Risk* is defined by the following equation:

*Risk = (the probability of a threat exploiting a vulnerability) x (total impact of the vulnerability being exploited)*

1. Risk treatment
   1. Now that we know the level of risk that each threat poses, we need to decide how we’ll treat them. There are four options:
      1. **Modify the risk** by implementing a control to reduce the likelihood of it occurring.
      2. **Avoid the risk** by ceasing any activity that creates it. This response is appropriate if the risk is too big to manage with a security control.
      3. **Share the risk** with a third party. There are two ways: by outsourcing the security efforts to another organization or by purchasing cyber insurance to ensure the funds to respond appropriately in the event of a disaster.
      4. **Retain the risk**. This means that the organization accepts the risk and believes that the cost of treating it is greater than the damage that it would cause.

## Perimeter

This clause comprises the architecture in the scope of the security analysis. The architecture includes the list of O-RAN components, interfaces and protocols manipulating critical assets and implementing security functions.

### Scope regarding architecture

As specified in [6], the logical architecture of O-RAN includes the following components, interfaces and protocols:

**O-RAN components:**

* Network functions and applications
  + Service Management and Orchestration (SMO)
  + Non-RT RIC and rApps
  + Near-RT RIC and xApps
  + O-CU-CP/UP
  + O-DU
  + O-RU
  + O-eNB
* Cloud computing platform
  + O-Cloud comprising a collection of physical infrastructure nodes that meet O-RAN requirements to host the relevant O-RAN functions (such as Near-RT RIC, O-CU-CP, O-CU-UP, and O-DU), the supporting software components (such as Operating System, Virtual Machine Monitor, Container Runtime, etc.) and the appropriate management and orchestration functions.

**O-RAN specific interfaces:**

* A1 Interface between Non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications/functions, and support AI/ML workflow.
* O1 Interface connecting the SMO to the Near-RT RIC, one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs.
* O2 Interface between the SMO and the O-Cloud.
* E2 Interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, one or more O-DUs, and one or more O-eNBs.
* Open Fronthaul CUS-Plane Interface between O-RU and O-DU.
* Open Fronthaul M-Plane Interface between O-RU and O-DU as well as between O-RU and SMO.
* Y1 Interface over which RAN analytics services exposed by the Near-RT RIC to be consumed by Y1 consumers.

**Relevant Protocols used by O-RAN system for enforcing security**:

* TLS
  + Should be used to protect the traffic between the O-RAN system and other network elements. It establishes a secure channel and provides CIA (Confidentiality, Integrity, Authenticity) features.
  + Should be used in O1 interface for NETCONF over TLS and JSON/REST over TLS
  + Should be used in A1 interface
* SSH
  + Should be used in O1 interface and Fronthaul M-Plane for NETCONF over SSH
* IPSEC
  + Should be used to protect E2 traffic
* FTP and FTPS
  + Should be used to protect file transfers over O1 and Fronthaul M-Plane interfaces
* PTP (Precision Timing Protocol, IEEE 1588-2019)

Une image contenant texte, capture d’écran, diagramme, conception

Description générée automatiquement

**Figure 4‑1 : Logical Architecture of O-RAN system [6]**

### Out of scope components

The following components are not in the perimeter of the O-RAN system defined by the alliance; therefore, they are considered out of scope of this study:

* 3GPP interfaces are already studied and maintained by 3GPP,
* UE,
* MEC,
* Core,
* Antennas.

# Statement of compatibility with 3GPP

This chapter gives the statement of compatibility with 3GPP/SCAS security Assets, Threats and Requirements. The statement of compatibility shows that 3GPP Assets/Threats/Requirements are applicable and that there is no conflict affecting the security of O-RAN components.

## Assets and Threats

Table 5‑1 : Statement of compatibility with 3GPP – Assets and Threats

|  |  |  |  |
| --- | --- | --- | --- |
| **3GPP/SCAS document reference/clause** | **Description** | **Applicable to O-RAN** | **Rationale** |
| TR 33.926 [4], clauses 5 and 6 | It describes the generic assets and threats of 3GPP network products | Yes | Since these assets/threats are for generic 3GPP (virtualized) network products, they are also applicable to O-RAN. It means that there is no need to repeat those assets/threats in this document. |
| TR 33.818 [15], clause 5.2.4 | It describes the generic assets, threats and requirements of 3GPP/ETSI NFV virtualized network products. | Yes |
| TR 33.848 [23], clause 5 | It considers the consequences of virtualization on 3GPP architectures, in order to identify threats and subsequent security requirements relating to ETSI-defined interfaces and Security functional requirements related to Virtualization layer, hardware and resource isolation. | Yes |

In addition, the assets/threats related to the additional specific O-RAN interfaces and components are considered. As a result, clauses 6.3 and 7.4 elaborates the O-RAN specific assets and threats respectively.

## Security requirements

Table 5‑2 : Statement of compatibility with 3GPP – Security requirements

|  |  |  |  |
| --- | --- | --- | --- |
| **3GPP/SCAS document reference/clause** | **Description** | **Applicable to O-RAN** | **Rationale** |
| TS 33.117 [5], clauses 4.3 and, 4.42 | It describes the general approach taken towards security functional requirements deriving from 3GPP specifications and the corresponding test cases, independent of a specific network product class. | Yes | Since these requirements are for generic 3GPP (virtualized) network products, they are to be fulfilled by O-RAN. It means that there is no need to repeat those requirements in this document. |
| TR 33.818 [14], clauses 5.2.5 and 5.3 | It describes the generic assets, threats and requirements of 3GPP/ETSI NFV virtualized network products. | Yes |
| TR 33.848 [23], clause 5 | It considers the consequences of virtualization on 3GPP architectures, in order to identify threats and subsequent security requirements relating to ETSI-defined interfaces and Security functional requirements related to Virtualization layer, hardware and resource isolation. | Yes |
| TS 33.501 [3] | It describes the security architecture and procedures for 5G system including gNodeB | Yes |
| TS 33.511 [2] | It describes the security requirements for the next generation Node B (gNodeB) network product class | Yes |

In addition, O-RAN also needs to consider the security requirements related to the additional specific O-RAN interfaces and components. As a result, clause 8 focus on the O-RAN security principles.

# Roles-Assumptions-Assets

## Stakeholders roles and responsibilities

The main stakeholders managing and using the O-RAN system are the following:

Table 6‑1 : Roles and responsibilities

|  |  |
| --- | --- |
| Role | Description |
| Mobile Network Operator (MNO) | Who offers network services and has a license to operate in allocated spectrum. |
| Orchestrator | Who is in charge of operating and orchestrating the O-RAN services.  The MNO could be the orchestrator. |
| HW/ Network vendor | Who is in charge of:   * Providing the network infrastructure including servers to run SDN controller, switches, routers, gateways, radio hardware, etc. * Installation, maintenance or replacement of the hardware/network device * Providing capability and procedures to securely configure the hardware/network device * Providing capability for the hardware/network device to generate log events * Providing capability for log files to be sent to an externalized log analysis system provided by the MNO * Providing a process for users, including security researchers, to submit bug reports (e.g., using an issue tracker or a mailing list) * Testing according to 3GPP and O-RAN test plans. Testing should include security tests of the device and its interfaces * Setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the hardware/network device including firmware * Maintenance of the firmware that includes providing patches for bugs and vulnerabilities |
| HW/ Network administrator | Who is in charge of:   * Configuration of the hardware/network device * Enabling collection of log events * Collection and analysis of log events generated by the hardware/network device * Deploying firmware patches in compliance with HW/ Network vendors deployment guidance * Monitoring, identifying and notifying HW/ Network vendors on discovered vulnerabilities * Regular testing of hardware/network configuration   The MNO could be the HW/ Network administrator. |
| NF vendor | Who is in charge of:   * Developing and providing NFs (e.g. VNF, CNF, PNF) for Near-RT RIC, O-CU-CP, O-CU-UP, O-DU, etc. * Providing capability and procedures to securely configure the NF * Setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the NF * Setting up a patch development, testing and delivery processes * Maintenance of the NF that includes providing patches for bugs and vulnerabilities * Providing capability for NF to generate log events * Providing capability for log files to be sent to an externalized log analysis system provided by the MNO * Testing according to 3GPP and O-RAN test plans. Testing should include security tests of the NF and its interface * Providing a process for users, including security researchers, to submit bug reports (e.g., using an issue tracker or a mailing list) |
| NF administrator | Who is in charge of:   * Deploying patches in compliance with NF vendors deployment guidance * Monitoring, identifying and notifying NF vendors on discovered vulnerabilities * Securely configuring the NF * Regular testing of the NF configuration * Enabling collection of log events * Analyzing log events generated by the software   The MNO could be the NF administrator. |
| Virtualization/Containerization hardware infrastructure provider | Who is in charge of:   * Provides virtualized/containerized infrastructure comprising computing resources (e.g., from computing platforms), storage and network. * Providing capability to securely configure the virtualization/containerization hardware infrastructure * Setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the virtualization/containerization hardware infrastructure * Maintenance of the security of hardware infrastructure * Providing capability for the hardware infrastructure to generate log events * Providing capability for log files to be sent to an externalized log analysis system provided by the MNO * Providing a process for users, including security researchers, to submit bug reports (e.g., using an issue tracker or a mailing list) |
| Virtualization/Containerization hardware infrastructure administrator | Who is in charge of:   * Deploying the Virtualization/Containerization hardware infrastructure in compliance with providers deployment guidance * Monitoring, identifying and notifying Virtualization/Containerization hardware infrastructure providers on discovered vulnerabilities * Securely configuring the Virtualization/Containerization hardware infrastructure * Regular testing of the Virtualization/Containerization hardware infrastructure configuration * Enabling collection of log events * Analyzing log events generated by the Virtualization/Containerization hardware infrastructure   The MNO could be the Virtualization/Containerization hardware infrastructure administrator. |
| Virtualization/Containerization software infrastructure provider | Who is in charge of:   * Provides virtualized/containerized infrastructure services and designs, builds, and operates virtualization/containerization infrastructure(s). The infrastructure comprises software of compute nodes such as hypervisors, host operating systems, and container run-time systems. * Providing capability to securely configure the virtualization/containerization software infrastructure * Setting up a vulnerability management process of monitoring, identifying, evaluating, treating and reporting on security vulnerabilities in the virtualization/containerization software infrastructure * Setting up a patch development, testing and delivery processes * Maintenance of the software infrastructure that includes providing patches for bugs and vulnerabilities * Providing capability for the software infrastructure to generate log events * Providing capability for log files to be sent to an externalized log analysis system provided by the MNO * Providing a process for users, including security researchers, to submit bug reports (e.g., using an issue tracker or a mailing list) |
| Virtualization/Containerization software infrastructure administrator | Who is in charge of:   * Deploying patches in compliance with Virtualization/Containerization software infrastructure providers deployment guidance * Monitoring, identifying and notifying Virtualization/Containerization software infrastructure providers of discovered vulnerabilities * Securely configuring the Virtualization/Containerization software infrastructure * Regular testing of the Virtualization/Containerization software infrastructure configuration * Enabling collection of log events * Analyzing log events generated by the Virtualization/Containerization software infrastructure   The MNO could be the Virtualization/Containerization software infrastructure administrator. |
| System integrator | Who is in charge of:   * Appropriately integrating O-RAN HW and SW components. SW components are integrated, in most cases remotely. * Ensuring that those components function together as expected * Securely configuring (system level) the O-RAN system * Testing patches after deployment to ensure that they don’t break other parts of O-RAN system or even expose new vulnerabilities   The MNO could be the integrator. |
| System tester | Tester of the O-RAN system to ensure quality, security, functionality and performance.  The MNO could be the system tester. |
| Other administrators | Identity Admin:   * Manages (Add, Modify, Delete) administrator accounts * Configures general settings for administrator accounts (password policy, etc.)   RBAC Admin   * Generates RBAC policies and permissions on admin access   System Admin   * Monitors network traffic for any suspicious activity * Performs risk assessment and defends against zero-day malware * Audits the O-RAN system * Triggers the update of O-RAN components on the latest security patches * Runs regular backups * Regularly performs analysis of log data   PKI Admin   * Manage and secure private keys and certificates |

**NOTE 1**: The operation, administration and orchestration of the O-RAN system can be split across multiple companies or roles.

**NOTE 2**: A trust management mechanism becomes crucially important to realize trustworthy collaboration among the O-RAN stakeholders.

## Assumptions and prerequisites

This section contains the list of minimum prerequisites and assumptions for equipment, software vendors, users and the physical environment to successfully operate the O-RAN system.

* The operational environment of the O-RAN system provides reliable timestamps for the generation of audit records, etc.
* Administrators, integrators, operators and orchestrators are trustworthy, and trained such that they are capable of securely managing the O-RAN system and following the instructions provided by O-RAN Alliance as well as the provided guidance by vendors and service providers.
* Log files, secrets and credentials stored in external systems and related to O-RAN are protected. They are access controlled so only privileged users have access to those secrets/credentials.

## Critical assets

The following table gives the list of critical assets to be protected within the O-RAN system.

An asset in this context may encompass data, interface or component deemed valuable for the O-RAN system. A component is defined as an O-RAN network function or architectural element.

Here's an explanation of each column, along with guidance on how to fill out the table:

* **Asset ID:** It identifies each asset uniquely. It helps in cataloging and referencing specific assets systematically.
* **Asset Description:** A brief description of what the asset is, including its purpose, contents, and any relevant attributes.
* **Component**: It specifies the O-RAN element(s) the asset is associated with, such as O-DU, O-RU, SMO, etc. This clarifies the asset's location within the O-RAN architecture.
* **Interface**: It indicates the interface through which the asset communicates or interacts with other elements. This could be internal interfaces or external interfaces.

NOTE: Assets can either be confined to a component (for those not shared with other O-RAN elements) or be present within a component and also transmitted to other O-RAN elements over interfaces. The way in which the 'Component' and 'Interface' columns are filled out will vary based on these situations.

* **When**: It is a categorization of the asset's state in terms of its lifecycle or operational phase, like "at rest" or "in transit". It is used to indicate when certain protection levels should be applied.
  + **When (At rest):** Marks with an 'x' if the asset needs protection while it is at rest (stored and not actively being used or transmitted).
  + **When (In transit):** Marks with an 'x' if the asset needs protection during transit (being transmitted or moved).
* **Protection level (Confidentiality, Integrity, Availability, Replay, Authenticity)**: These columns specify the type of protection or security measure required for the asset. An 'x' in any of these sub-columns indicates a need for measures to ensure:
* **Confidentiality:** The asset should be accessible only to authorized entities.
* **Integrity:** The asset should be protected from unauthorized changes.
* **Availability:** The asset should be accessible to authorized entities when needed.
* **Replay:** Protection against replay attacks, ensuring that repeated or delayed transmissions are identified and prevented.
* **Authenticity:** The asset should be verifiable as genuine.

Instructions for completing the table:

* **Asset ID**: Assign a unique identifier to each asset.
* **Asset Description**: Provide a detailed description of the asset, including its nature, purpose, and any other relevant details.
* **Component**: Specify the component associated with the asset, if applicable.
* **Interface**: Indicate the interface(s) related to the asset.
* **When (At rest/In transit)**: Mark with an 'x' if the asset requires protection either at rest or in transit.
* **Protection level**: Mark with an 'x' in the appropriate sub-columns to indicate the types of protection required for the asset.

The categories "Data" and "Components" are defined as follows:

* **Data:** It refers to the information that is processed, stored, and transmitted through the O-RAN architecture.
* **Components:** It involves the physical (Hardware), logical and virtual (Software) parts of the O-RAN system.

Table 6‑2 : Critical assets

| Asset ID | Asset Description | Component | Interface | When | | Protection Level | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| At rest | In transit | Confidentiality | Integrity | Availability | Replay | Authenticity |
| **Data & Interfaces** | | | | | | | | | | |
| **ASSET-D-01** | Critical S-Plane data such as:   * Data flow for synchronization and timing information between nodes * PTP (e.g. ANNOUNCE message) transported over Fronthaul that interconnects multiple O-RUs and O-DUs. * Timing configuration (LLS C1, C2, C3, C4) and topology | O-DU, O-RU | Fronthaul CUS-Plane |  | x |  | x |  | x | x |
| x |  |  | x | x |  |  |
| **ASSET-D-02** | Critical Management-Plane data transported over the Fronthaul interface such as: maintenance and monitoring signals, data collected related to O-RU operations, logs (troubleshooting, trace) | O-DU, O-RU, SMO | Fronthaul M-Plane |  | x | x | x |  | x | x |
| x |  | x | x | x |  |  |
| **ASSET-D-03** | Critical Management-Plane data transported over the O1 interface such as:   * Observables (events and counters) and network status provided over O1 to non-RT RIC from Near-RT RIC, O-CU and O-DU. * The non-RT RIC uses the O1 observables (Feedback on the fulfilment of A1 policies in the near-RT RIC) to continuously evaluate the impact of the A1 policies towards fulfillment of the RAN Intent. * Managed Element Telemetry to monitor the application behavior (from O-Cloud). | Near-RT RIC, Non-RT RIC, O-CU, O-DU, SMO | O1 |  | x | x | x |  | x | x |
| x |  | x | x | x |  |  |
| **ASSET-D-04** | Critical C-Plane data such as:   * Scheduling information, FFT size, CP length, Subcarrier spacing, UL PRACH scheduling * DL and UL Beamforming commands (e.g., beam index) and scheduling * LBT Configuration parameters such as lbtHandle, lbtDeferFactor, lbtBackoffCounter, lbtOffset, MCOT, lbtMode, sfnSf, lbtCWconfig\_H, lbtCWconfig\_T, lbtTrafficClass. * LBT DL indication parameters such as lbtHandle, lbtResult, initialPartialSFs, bufferError, lbtCWR\_Result | O-DU, O-RU | Fronthaul CUS-Plane |  | x | x | x |  | x | x |
| x |  |  | x | x |  |  |
| **ASSET-D-05** | Critical Fronthaul U-Plane data such as:   * Use data (i.e. DNS, PUSCH, PDSCH, etc.), * Control channel data (PDCCH, PUCCH, etc.), * PRACH data | O-DU, O-RU | Fronthaul CUS-Plane |  | x | x | x |  | x | x |
| x |  | x | x | x |  |  |
| **ASSET-D-06** | Reference signals, synchronization signal and channels in downlink and uplink between O-RU and UE | O-RU | Radio |  | x | x | x |  | x | x |
| **ASSET-D-07** | A1 policies that are provided to the near-RT RIC over the A1 interface to guide the RAN performance towards the overall goal expressed in RAN Intent. The A1 policies are declarative policies that contain statements on policy objectives and policy resources applicable to UEs and cells. A1 policies are created, modified and deleted by the non-RT RIC. | Near-RT RIC, Non-RT RIC | A1 |  | x | x | x |  |  | x |
| **ASSET-D-08** | A1 Enrichment Information that is collected or derived at SMO/non-RT RIC either from non-network data sources or from network functions themselves and provided over the A1 interface to be utilized by near-RT RIC, e.g. an ML model, to improve its performance.  Discovery and request of A1 Enrichment Information from near-RT RIC to non-RT RIC  External Enrichment Information that is provided by an O-RAN external information source to near-RT RIC over A1 | Near-RT RIC, Non-RT RIC | A1 |  | x | x | x |  |  | x |
| **ASSET-D-09** | Data transported over the E2 interface such as:   * Near real-time information (e.g. UE basis, 2Cell basis). * The persistent configuration used by the near-RT RIC to control the RAN. * Identifiers of E2 nodes. * xApp-related messages. * Control signaling information. * Policies used by the Near-RT RIC to monitor, suspend/stop, override or control the behavior of E2 node. * NEAR-RT RIC services messages (REPORT, INSERT, CONTROL and POLICY). * Interface Management messages (E2 Setup, E2 Reset, E2 Node Configuration Update, Reporting of General Error Situations). * Near-RT RIC Service Update messages. | O-DU, O-CU, Near-RT RIC | E2 |  | x | x | x |  | x | x |
| **ASSET-D-10** | Database holding data from xApp applications and E2 Node | Near-RT RIC | **-** | x |  | x | x | x |  | x |
| **ASSET-D-11** | E2 Node data (e.g. configuration information (cell configuration, supported slices, PLMNs, etc.), network measurements, context information, etc.) | E2 nodes | **-** | x |  |  | x | x |  |  |
| **ASSET-D-12** | It consists of   * The Physical Infrastructure (O-Cloud Node Identifier, Pool Identifier, Pool Location Identifier, and Use Identifier) used to create the O-Cloud, * The logical Clouds which it provides as interfaces for deployments, and the inventory of deployments (deployment ID and descriptor) on the cloud * O-Cloud ID, IP address, IMS address, the IP address endpoint or url of the SMO and any necessary security keys or passwords for communication using O2 * DMS capabilities * O-Cloud (IMS): List of All Resource Pools in the O-Cloud, Attributes of a specific O-Cloud, List of all resources of an O-Cloud Pool, Attributes of each O-Cloud Resource, List of all DMS * **O-Cloud (DMS): List of Locations Supported For a given location the Capabilities supported (e.g. Descriptor types, Technology types, Accelerator types), For a given location the Capacity of the location, For a given location the Availability of the location** | SMO, O-CLOUD | O2, O-CLOUD internal interfaces | x | x | x | x | x | x | x |
| **ASSET-D-13** | It includes:   * Telemetry information of O-Cloud deployments in the network for analyzing the O-Cloud’s state and health, and for delivering on service monitoring goals. It consists of fault, performance and configuration data: * Deployment Telemetry to monitor the number of deployment instances an O-Cloud has at that moment and how many were expected, how the on-progress deployment is going, and health checks. Additional Deployment Telemetry metrics like CPU, network, and memory usage can also be collected. * - Infrastructure Telemetry to monitor the health of the O-Cloud Infrastructure components. Network Operations are interested in discovering if all the components in the O-Cloud Infrastructure are working properly and at what capacity, how many deployments are running on each node, and the resource utilization of the O-Cloud Infrastructure. | SMO, O-CLOUD | O2, O-CLOUD internal interfaces | x | x | x | x | x | x | x |
| **ASSET-D-14** | O-Cloud Provisioning information (Affinity, Anti-Affinity, Quorum Diversity Rules, capabilities, capacity and availability)  O-Cloud software management information: catalog of authorized software and its version, list of authorized VNF/CNF, VNF/CNF description files | SMO, O-CLOUD | O2, O-CLOUD internal interfaces |  | x | x | x |  | x | x |
| **ASSET-D-15** | Package: O-RAN Cloudified Network Function Software Image including the underlying software executable image, image properties/metadata such as descriptors, image signature(s), LCM scripts, data files, SoftwareImageId, Vendor, and version, secrets, configuration files.  Application data: Subscriber data, Policy data, UE context, etc.  NF location, time clock  NF instance: Application software, guest OS, host OS, Libs, instance identity, crypto keys, namespaces, virtual resources instance states, physical hardware, etc. | O-CLOUD | - | x |  |  | x | x |  |  |
| **ASSET-D-16** | X.509 certificates in O-RAN network such as those used for SMO, O-CU-CP, O-CU-UP, O-DU, O-RU, Near-RT RIC, Non-RT RIC, O-CLOUD, NetCONF (O1, Fronthaul) | All | O1, Fronthaul, O2, E2, A1 | x |  |  | x | x |  | x |
| **ASSET-D-17** | Security private keys in O-RAN network such as those used for SMO, O-CU-CP, O-CU-UP, O-DU, O-RU, Near-RT RIC, Non-RT RIC, O-CLOUD, NetCONF (O1, Fronthaul) ), for authentication, encryption, signing (e.g. for TLS and similar protocols, image signing) | All | O1, Fronthaul, O2, E2, A1 | x |  | x | x | x |  | x |
| **ASSET-D-18** | O-RAN components associated and configuration data, such as:   * Software version information, identifier, IP address, port number, network layer parameters, time of request, previous behavior, etc. * The security related parameters (such audit records, lists of algorithms which are allowed for usage, file management, hash values, etc.). | All | - | x |  | x | x | x |  |  |
| **ASSET-D-19** | Cryptographic keys: KgNB, KRRC-enc, KRRC-int, KUP-int, and KUP-enc (Hierarchy of cryptographic key derived from Anchor Key. (as defined in ETSI TS 133 501 clause 6.2.) | O-CU | - | x |  | x | x | x |  |  |
| **ASSET-D-20** | Credentials (Administrators): account information and passwords on SMO, O-CU-CP, O-CU-UP, O-DU, O-RU, Near-RT RIC, Non-RT RIC, O-Cloud used in O-RAN network | All |  | x |  | x | x | x |  |  |
| **ASSET-D-21** | 3GPP application related data such as subscription data, session data, call control related information etc. | O-CU |  | x | x | x | x | x | x | x |
| **ASSET-D-22** | Inter- and intra-slice UE priority [14] | O-CU, O-DU | - | x | x |  | x | x |  |  |
| **ASSET-D-23** | Patches for vulnerable SW components | All | - |  | x |  | x | x |  | x |
| **ASSET-D-24** | NETCONF Configuration Access Control Model datastores | All |  | x |  | x | x | x |  | x |
| **ASSET-D-25** | Training or test data and associated labels: data sets collected externally or internally from the Near-RT RIC, O-CU and O-DU and passed to the ML training hosts in a ML system. | Near-RT RIC, Non-RT RIC, xAPPs, rAPPs | A1, O1, E2 |  | x | x | x |  | x | x |
| x |  | x | x | x |  | x |
| **ASSET-D-26** | The trained ML model which includes the configured hyperparameters, inference algorithm, and learned parameters. | Near-RT RIC, Non-RT RIC, xAPPs, rAPPs |  | x |  | x | x | x |  |  |
| **ASSET-D-27** | The ML prediction results built into the model (e.g. expected outcomes) | Near-RT RIC, Non-RT RIC, xAPPs, rAPPs |  |  |  | x | x | x |  |  |
| **ASSET-D-28** | The behavior of the ML system including tasks for data collection, data wrangling, pipeline management, model retraining, and model deployment. | Near-RT RIC, Non-RT RIC, xAPPs, rAPPs |  | At runtime |  | x | x | x |  |  |
| **ASSET-D-29** | Security event log files generated by O-RAN components | All |  | x | x |  | x | x |  | x |
| **ASSET-D-30** | O-RAN specific several UE IDs | Near-RT RIC, Non-RT RIC, SMO | A1, E2, O1 |  | x | x | x |  | x | x |
| x |  | x | x | x |  |  |
| **ASSET-D-31** | Security telemetry from the NFV system for detecting threats and anomalies | All | O2, O-CLOUD internal interfaces | x | x | x | x | x | x | x |
| **ASSET-D-32** | Cryptographic keys used during secure boot, for encryption/decryption, etc. | All | - | x |  | x | x | x |  |  |
| **ASSET-D-3**3 | Data transported over the AALI-C-Mgmt interface |  | AALI-C-Mgmt |  | x | x | x |  | x | x |
| **ASSET-D-34** | Data transported over the AALI-C-App & AALI-P interfaces |  | AALI-C-App & AALI-P |  | x |  | x |  | x | x |
| **ASSET-D-35** | Data transported over the vendor specific interface |  | vendor specific interface |  | x |  | x |  |  | x |
| **ASSET-D-36** | AAL profiles | AAL |  | x |  |  | x | x |  |  |
| **ASSET-D-37** | AAL-LPU | AAL |  | x |  |  | x | x |  |  |
| **ASSET-D-38** | Stored AAL data (e.g., logs, configuration data) | AAL |  | x |  |  | x | x |  |  |
| **ASSET-D-39** | xAppID | Near-RT RIC, xApps |  | x | x |  | x |  |  |  |
| **ASSET-D-40** | ML models that have not been trained yet, i.e., Initial Models and their associated learning algorithm. | Non-RT RIC, Near-RT RIC, SMO |  | x | x |  | x | x |  |  |
| **Components (logical, virtual, physical)** | | | | | | | | | | |
| **ASSET-C-01** | Logical module: Service Management and Orchestration (SMO) |  |  | x |  |  | x | x |  | x |
| **ASSET-C-02** | Near-RT RIC software |  |  | x |  |  | x | x |  | x |
| **ASSET-C-03** | O-CU-CP software |  |  | x |  |  | x | x |  | x |
| **ASSET-C-04** | O-CU-UP software |  |  | x |  |  | x | x |  | x |
| **ASSET-C-05** | O-DU software |  |  | x |  |  | x | x |  | x |
| **ASSET-C-06** | O-RU software |  |  | x |  |  | x | x |  | x |
| **ASSET-C-07** | O-eNB |  |  | x |  |  | x | x |  | x |
| **ASSET-C-08** | O-Cloud |  |  | x |  |  | x | x |  | x |
| **ASSET-C-09** | xApps |  |  | x |  |  | x | x |  | x |
| **ASSET-C-10** | rApps |  |  | x |  |  | x | x |  | x |
| **ASSET-C-11** | Non-RT RIC software |  |  | x |  |  | x | x |  | x |
| **ASSET-C-12** | ML components deploying machine learning such as: ML training and interference hosts, ML applications (xAPPS, rAPPs) |  |  | x |  |  | x | x |  | x |
| **ASSET-C-12** | PNF NF equipment |  |  | x |  |  | x | x |  | x |
| **ASSET-C-13** | A1 termination |  |  |  | x | x | x | x |  | x |
| **ASSET-C-14** | A1 interface, including protocol stack |  |  |  | x | x | x | x | x | x |
| **ASSET-C-15** | R1 termination |  |  |  | x | x | x | x |  | x |
| **ASSET-C-16** | R1 interface, including protocol stack |  |  |  | x | x | x | x | x | x |
| **ASSET-C-17** | SMO Framework/Platform | x |  |  |  |  |  | x |  | x |
| **ASSET-C-18** | SMO Functions | x |  |  |  |  |  | x |  | X |
| **ASSET-C-19** | R1 Service Exposure Functions | x |  |  |  |  |  | x |  | x |
| **ASSET-C-20** | A1 Functions | x |  |  |  |  |  | x |  | x |
| **ASSET-C-21** | Data Management and Exposure Functions | x |  |  |  |  |  | x |  | x |
| **ASSET-C-22** | O1, including protocol stack |  | x |  | x | x | x | x | x | x |
| **ASSET-C-23** | O2, including protocol stack |  | x |  | x | x | x | x | x | x |
| **ASSET-C-24** | OFH M-Plane, including protocol stack |  | x |  | x | x | x | x | x | x |
| **ASSET-C-25** | OFH CUS-Plane, including protocol stack |  | x |  | x | x | x | x | x | x |
| **ASSET-C\_26** | External interfaces |  | x |  | x | x | x | x | x | x |
| **ASSET-C\_27** | External interfaces termination at SMO Framework/Platform |  | x |  | x | x | x | x |  | x |
| **ASSET-C-28** | External interfaces termination at Non-RT RIC Framework |  | x |  | x | x | x | x |  | x |
| **ASSET-C-29** | AAL software including software, libraries, drivers, etc. | AAL |  | x |  |  | x | x |  |  |
| **ASSET-C-30** | The hardware accelerator device firmware | Hardware accelerator device |  | x |  |  | x | x |  |  |
| **ASSET-C-31** | Shared O-RU | x |  |  |  | x | x | x |  | x |
| **ASSET-C-32** | O-RU Host | x |  |  |  | x | x | x |  | x |
| **ASSET-C-33** | O-RU Tenant (Shared Resource Operator) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-34** | O-DU Host | x |  |  |  | x | x | x |  | x |
| **ASSET-C-35** | O-DU Tenant (Shared Resource Operator) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-36** | O-CU Host, includes O-CU-CP and O-CU-UP software | x |  |  |  | x | x | x |  | x |
| **ASSET-C-37** | O-CU Tenant (Shared Resource Operator), includes O-CU-CP and O-CU-UP software | x |  |  |  | x | x | x |  | x |
| **ASSET-C-38** | SMO Host | x |  |  |  | x | x | x |  | x |
| **ASSET-C-39** | SMO Tenant (Shared Resource Operator) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-40** | E2 interface, including protocol stack |  | x |  | x | x | x | x | x | x |
| **ASSET-C-41** | E2 Functions | x |  |  |  |  |  | x |  | x |
| **ASSET-C-42** | Y1 interface, including protocol stack |  | x |  | x | x | x | x | x | x |
| **ASSET-C-43** | Y1 Functions | x |  |  |  |  |  | x |  | x |
| **ASSET-C-44** | Service Management and Exposure (SME) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-45** | Data Management and Exposure (DME) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-46** | Topology Exposure and Inventory Management (TE&IM) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-47** | rApp Management | x |  |  |  | x | x | x |  | x |
| **ASSET-C-48** | R1 Services | x |  |  |  | x | x | x |  | x |
| **ASSET-C-49** | Network Function Orchestrator (NFO) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-50** | Federated O-Cloud Orchestration and Management (FOCOM) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-51** | RAN NF Fault Management (FM) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-52** | RAN NF Configuration Management (CM) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-53** | RAN NF Performance Management (PM) | x |  |  |  | x | x | x |  | x |
| **ASSET-C-54** | A1 Enrichment Information Management | x |  |  |  | x | x | x |  | x |
| **ASSET-C-55** | A1 Policy Management | x |  |  |  | x | x | x |  | x |
| **ASSET-C-56** | A1 E1 Management | x |  |  |  | x | x | x |  | x |
| **ASSET-C-57** | SW Package Onboarding | x |  |  |  | x | x | x |  | x |
| **ASSET-C-58** | Service Orchestration | x |  |  |  | x | x | x |  | x |
| **ASSET-C-59** | Service Assurance | x |  |  |  | x | x | x |  | x |
| **ASSET-C-60** | RAN Analytics | x |  |  |  | x | x | x |  | x |
| **ASSET-C-61** | AI/ML Workflow | x |  |  |  | x | x | x |  | X |
| **ASSET-C-62** | SMOS Communication |  | x |  | x | x | x | x | x | x |

# Threat model

## Threat surface

The O-RAN architecture [6] introduces new functions and interfaces. The introduction of additional interfaces and nodes, and the decoupling of hardware and software, expands the threat and attack surface of the network. For the purposes of this document, threat surfaces are divided into six (6) main groups:

* Additional functions: SMO, Non-Real-Time RIC, Near-Real-Time RIC
* Additional open interfaces: A1, E2, O1, O2, Open Fronthaul
* Modified architecture: Lower Layer Split (LLS) 7-2x
* Decoupling increases threat to Trust Chain
* Containerization and Virtualization: Disaggregation of software and hardware
* Exposure to public exploits may be increased due to use of Open Source Code

The following entry points are considered:

* API between planes which facilitate the propagation of threats
* Threats coming from inside the O-RAN system
* Threats coming from outside the O-RAN system

## Threat agent

For the purposes of this document, threat agents are categorized as follows:

* Cyber-criminals: Represents individuals who commits cybercrimes, where he/she makes use of the computer either as a tool or as a target or as both.
* Insiders: Represents malicious attacks perpetrated on a network or computer system by a person with authorized system access.
* Hacktivists: Represents actors that perform cyber-attacks to achieve political or social gains.
* Cyber-terrorists: Represents actors that their sole aim of violence against clandestine agents and subnational groups through the compromise of O-RAN infrastructures.
* Script kiddies: Represents actors that do not poses deep technical expertise or resources to perform sophisticated attacks.
* Nation-State: actors aggressively target and gain persistent access to public and private sector networks to compromise, steal, change, or destroy information.

## Potential vulnerabilities

This document addresses the following potential security vulnerabilities that are exploitable through attacks against Confidentiality, Integrity, and Availability:

* O-RAN specific vulnerabilities
  + Unauthorized access to O-DU, O-CU-CP, O-CU-UP and RU to degrade RAN performance or execute broader network attack (Availability)
  + Unprotected synchronization and control plane traffic on Open Fronthaul Interface (Integrity and Availability)
  + Disable over-the-air ciphers for eavesdropping (Confidentiality)
  + Near-RT RIC conflicts with O-gNB (Availability)
  + x/rApps conflicts (Availability)
  + x/rApps access to network and subscriber data (Confidentiality)
  + Unprotected management interface (Confidentiality, Integrity, Availability)
  + CP UL or DL messages can be injected for attack on UP (Availability)
* General vulnerabilities
  + Decoupling of functions without hardware root of trust and software trust chain (Integrity)
  + Exposure to public exploits from use of Open Source code (Confidentiality, Integrity, Availability)
  + Misconfiguration, poor isolation or insufficient access management in the O-Cloud platform (Confidentiality, Integrity, Availability)

## Threats

For the purposes of this document, threats are grouped in eight categories:

* Threats against O-RAN system
* Threats against O-CLOUD
* Threats to open source code
* Physical threats
* Threats against 5G radio networks
* Threats against ML system
* Protocol stack threats
* SMO threats

The threat analysis is carried out using a well-defined structure to present each threat cases and simplify the risk analysis associated with each threat. In the following subsections, only a unique ID, title and description of each threat are given:

|  |  |
| --- | --- |
| Threat ID | Unique identification per Threat (e.g. T-XX-01) |
| **Threat title** | Title of the threat |
| **Threat description** | Description of the Threat |

At the end of this chapter a matrix is provided depicting the mapping between threats and the following elements:

|  |  |
| --- | --- |
| Threat agent | An individual or group that can manifest a threat |
| **Vulnerability** | What vulnerabilities can the threat exploits? |
| **Threatened Assets** | Impacted Asset(s) |
| **Affected Components** | The list of Components impacted by that Threat |

The template of the matrix is as follows:

| Threat ID | Threat title | Threat agent | Vulnerability | Threatened Asset | Affected Components |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |

### Threats against O-RAN system

#### Common among O-RAN components

The O-RAN system architecture introduces the following common threats among its components:

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-01 |
| **Threat title** | An attacker exploits insecure designs or lack of adoption in O-RAN components |
| **Threat description** | Unauthenticated/unauthorized access to O-RAN components could possibly be achieved via the different O-RAN interfaces, depending upon the design of the hardware-software O-RAN system and how different functions are segregated within the O-RAN system.  O-RAN components might be vulnerable if:   * Outdated component from the lack of update or patch management, * Poorly design architecture, * Missing appropriate security hardening, * Unnecessary or insecure function/protocol/component.   An attacker could, in such case, either inject malwares and/or manipulate existing software, harm the O-RAN components, create a performance issue by manipulation of parameters, or reconfigure the O-RAN components and disable the security features with the purpose of eavesdropping or wiretapping on various CUS & M planes, reaching northbound systems, attack broader network to cause denial-of-service, steal unprotected private keys, certificates, hash values, or other type of breaches.  In addition, O-RAN components could be software providing network functions, so they are likely to be vulnerable to software flaws: it could be possible to bypass firewall restrictions or to take advantage of a buffer overflow to execute arbitrary commands, etc. |

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-02 |
| **Threat title** | An attacker exploits misconfigured or poorly configured O-RAN components |
| **Threat description** | Unauthenticated/unauthorized access to O-RAN components could possibly be achieved via the different O-RAN interfaces, depending upon the configuration of the hardware-software O-RAN system.  O-RAN components might be vulnerable if:   * Errors from the lack of configuration change management, * Misconfigured or poorly configured O-RAN components, * Improperly configured permissions, * Unnecessary features are enabled (e.g. unnecessary ports, services, accounts, or privileges), * Default accounts and their passwords still enabled and unchanged, * Security features are disabled or not configured securely.   An attacker could, in such case, either inject malwares and/or manipulate existing software, harm the O-RAN components, create a performance issue by manipulation of parameters, or reconfigure the O-RAN components and disable the security features with the purpose of eavesdropping or wiretapping on various CUS & M planes, reaching northbound systems, attack broader network to cause denial-of-service, steal unprotected private keys, certificates, hash values, or other type of breaches. |

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-03 |
| **Threat title** | Attacks from the internet exploit weak authentication and access control to penetrate O-RAN network boundary |
| **Threat description** | Web servers serving O-RAN functional and management services should provide adequate protection.  An attacker that have access to the uncontrolled O-RAN network could:   * Bypass the information flow control policy implemented by the firewall, * And/or attack O-RAN components in the trusted networks by taking advantage of particularities and errors in the design and implementation of the network protocols (IP, TCP, UDP, application protocols), * Use of incorrect or exceeded TCP sequence numbers, * Perform brute force attacks on FTP passwords, * Use of improper HTTP user sessions, * Etc.   The effects of such attacks may include:   * An intrusion, meaning unauthorized access to O-RAN components, * Blocking, flooding or restarting an O-RAN component causing a denial of service, * Flooding of network equipment, causing a denial of service, * Etc. |

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-04 |
| **Threat title** | An attacker attempts to jam the airlink signal through IoT devices |
| **Threat description** | DDoS attacks on O-RAN systems: The 5G evolution means billions of things, collectively referred to as IoT, will be using the 5G O-RAN. Thus, IoT could increase the risk of O-RAN resource overload by way of DDoS attacks. Attackers create a botnet army by infecting many (millions/billions) IoT devices with a “remote-reboot” malware. Attackers instruct the malware to reboot all devices in a specific or targeted 5G coverage area at the same time. |

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-05 |
| **Threat title** | An attacker penetrates and compromises the O-RAN system through the open O-RAN’s Fronthaul, O1, O2, A1, and E2 |
| **Threat description** | O-RAN’s Fronthaul, O1, O2, A1, and E2 management interfaces are the new open interfaces that allow software programmability of RAN. These interfaces may not be secured to industry best practices.  O-RAN components might be vulnerable if:   * 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, * Improper implementation, * Improperly validate inputs, respond to error conditions in both the submitted data as well as out of sequence protocol steps.   An attacker could, in such case, cause denial-of-service, data tampering or information disclosure, etc.  **NOTE**: O-RAN interfaces allow use of TLS or SSH. Industry best practices mandate the use of TLS (v1.2 or higher) or SSH certificate-based authentication. An implementation that implements TLS version lower than 1.2 or a SSH password authentication, may become the key source of vulnerability that a malicious code will exploit to compromise the O-RAN system. |

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-06 |
| **Threat title** | An attacker exploits insufficient/improper mechanisms for authentication and authorization to compromise O-RAN components |
| **Threat description** | O-RAN management and orchestration should not be used without appropriate authentication and authorization and authorization checks.  O-RAN components might be vulnerable if:   * 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.   An attacker could, in such case, either inject malwares and/or manipulate existing software, harm the O-RAN components, create a performance issue by manipulation of parameters, or reconfigure the O-RAN components and disable the security features with the purpose of eavesdropping or wiretapping on various CUS & M planes, reaching northbound systems, attack broader network to cause denial-of-service, steal unprotected private keys, certificates, hash values, or other type of breaches. |

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-07 |
| **Threat title** | An attacker compromises O-RAN monitoring mechanisms and log files integrity and availability |
| **Threat description** | Improper / missing controls for protection of security event log files generated by O-RAN components and the lack of security events logged together with a unique system reference (e.g. host name, IP or MAC address) and the exact time the incident occurred do not allow a correct and rapid audit in case of security incident occurrence. Security restoration is delayed. Compromise of availability and integrity of security event log files could conduct to delays, wrong audit results, delays in security restoration, threats persistence. |

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-08 |
| **Threat title** | An attacker compromises O-RAN data integrity, confidentiality and traceability |
| **Threat description** | O-RAN components may not be secured to industry best practices. Adequate security controls are needed for protecting sensitive data stored, processed and transferred by O-RAN components.  O-RAN components might be vulnerable if:   * 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 confidential internal data in the clear to administrators. Such functions could be, for example, local or remote OAM CLI or GUI, logging messages, alarms, configuration file exports etc. * No traceability (logging) of access to personal data.   An attacker could, in such case, cause denial-of-service, data tampering, information disclosure, spoofing identity, elevation of privilege, etc. |

|  |  |
| --- | --- |
| Threat ID | T-O-RAN-09 |
| **Threat title** | An attacker compromises O-RAN components integrity and availability |
| **Threat description** | Overload situation could appear in the case of DoS attack or increased traffic. Inability to deal with such events affects availability of information or security functionalities of O-RAN components.  O-RAN components may boot from unauthorized memory devices. Inability to deal with such events affects integrity of information or security functionalities of O-RAN components.  Insufficient assurance of O-RAN software package integrity could affect CIA of data, services, hardware and policies during installation or upgrade phases for O-RAN components.  An attacker could, in such case, cause denial-of-service, data tampering, information disclosure, spoofing identity, etc. |

#### Threats against the fronthaul interface and M-S-C-U planes

The LLS architecture and the fronthaul interface introduce the following threats:



Figure 7‑1 : Threats and Vulnerabilities for O-RAN LLS 7-2x

|  |  |
| --- | --- |
| Threat ID | T-FRHAUL-01 |
| **Threat title** | An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface [12] |
| **Threat description** | When having two different vendors, the O-RU and the O-DU needs to be managed as different entities and may have heterogeneous security levels. Instead, the O-DU will have to bridge the management traffic between the management system and the O-RU. Hence the possibilities to reach the northbound systems beyond the O-DU through the Open Fronthaul interface become a possible attack vector in this split architecture. |

|  |  |
| --- | --- |
| Threat ID | T-FRHAUL-02 |
| **Threat title** | Unauthorized access to Open Front Haul Ethernet L1 physical layer interface(s) |
| **Threat description** | The Open Front Haul Ethernet L1 physical interface comprises one or more coaxial cables, twisted pairs, or optical fibers. Each end of the Open Front Haul Ethernet L1 physical interface comprises a physical connection (colloquially known as an Ethernet Port) to physical O-RAN network elements, e.g., O-DU, O-RU, etc.  Unauthorized access to the Open Front Haul Ethernet L1 physical layer interface (cables and connections) provides a means to launch attacks on the availability, integrity, and confidentiality of the Open Front Haul system.  Potential loss of availability on the Open Front Haul interface can occur from one or more of the following threats:   * An unauthorized device on the Ethernet L1 Interface can flood the L1 interface with unintended network traffic causing disruption or degradation of authorized network elements on the Open Front Haul interface. * An unauthorized device on the Ethernet L1 Interface can send L2 messages to authorized network devices causing disruption, denial, or degradation of the Open Front Haul interface. * An attacker (person) gains access to the Open Front Haul Ethernet L1 interface(s) and denies the Open Front Haul services by disabling a physical connection to a network element either by removing an Ethernet port connection or cutting the physical interface (coaxial cable, twisted pair, or optical fiber).   Potential loss of availability, confidentiality, and/or integrity on the Open Front Haul interface can occur from one or more of the following threats:   * An unauthorized device on the Ethernet L1 Interface has access to U-Plane traffic on the Open Front Hall Interface. * An unauthorized device on the Ethernet L1 Interface has access to S-Plane traffic on the Open Front Hall Interface. * An unauthorized device on the Ethernet L1 Interface has access to C-Plane traffic on the Open Front Hall Interface. * An unauthorized device on the Ethernet L1 Interface has access to M-Plane traffic on the Open Front Hall Interface. |

|  |  |
| --- | --- |
| Threat ID | T-MPLANE-01 |
| **Threat title** | An attacker attempts to intercept the Fronthaul (MITM) over M Plane |
| **Threat description** | The High bit rate Fronthaul interface impose strict performance requirements ((bandwidth, latency, fronthaul transport link length, etc.) that limit the use of some security features, due to the increased processing delay. This opens the risk of Man-in-the-Middle (MITM) attacks over the fronthaul interface or O1 to intercept the M plane.  For the transported Management-Plane data over the fronthaul interface or O1, an Attacker could potentially do threats, such as passive wiretapping and denial of service, but would need to break M-Plane Security prior to gain OAM access. |

|  |  |
| --- | --- |
| Threat ID | T-SPLANE-01 |
| **Threat title** | DoS attack against a Master clock |
| **Threat description** | A denial of service (DoS) attack towards a Master clock of the timing network used by the open Fronthaul to maintain the availability and accuracy of the Master clock. An attacker can attack a master clock by sending an excessive number of time protocol packets or impersonate a legitimate clock, a slave, or an intermediate clock, by sending malicious messages to the master, thus degrading the victim’s performance.  The attacker may be residing either within the attacked network (insider) or on an external network connected to the attacked network.  This attack results in a situation where the clock service is interrupted completely or the timing protocol is operational but slaves are being provided inaccurate timing information due the degraded performance of the Master clock.  This clock service disruption or degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell.  A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. |

|  |  |
| --- | --- |
| Threat ID | T-SPLANE-02 |
| **Threat title** | Impersonation of a Master clock (Spoofing) within a PTP network with a fake ANNOUNCE message |
| **Threat description** | An attacker within the PTP network can impersonate the master clock’s grandmasterIdentity value and propose himself as a grandmaster candidate by sending fake ANNOUNCE messages declaring him to be the best clock in the network. The attacker may be residing either within the attacked network (insider) or on an external network connected to the attacked network.  This attack results in a situation where the attacker clock becomes a GM, PTP is operational, all clocks are synchronized, but the malicious GM provides intentionally inaccurate timing information.  This degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell.  A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. |

|  |  |
| --- | --- |
| Threat ID | T-SPLANE-03 |
| **Threat title** | A Rogue PTP Instance wanting to be a Grand Master |
| **Threat description** | An attacker can propose himself as a grandmaster candidate by sending manipulated/malicious ANNOUNCE messages declaring him to be the best clock in the network. The attacker causes other nodes in the network to believe it is a legitimate master. The attacker is internal to the attacked PTP network and could launch this attack by either modification of in-flight protocol packets or injecting fake ANNOUNCE messages to the PTP network. It is assumed that an MITM attacker has physical access to a segment of the network or has gained control of one of the nodes in the network. This attack results in a situation where the time protocol is operational but slaves are being provided intentionally inaccurate timing information.  This degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell.  A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. |

|  |  |
| --- | --- |
| Threat ID | T-SPLANE-04 |
| **Threat title** | Selective interception and removal of PTP timing packets |
| **Threat description** | An attacker can position himself in such way that allows him to intercept and remove valid synchronization packets. This leads to clock synchronization errors of all clocks downstream or makes them go into free-running mode.  Attacks may be launched close to the GM by tapping the egress line of an active GM clock. This impacts a larger set of slaves who depend on this GM for timing synchronization.  Attacks may also target a one or more slaves. This is done by tapping the ingress line of a particular slave(s). The impact is confined to the targeted slaves.  Alternatively, a MiTM attacker can reside in an intermediate node such as TCs, routers and switches to launch this attack. The attacker has physical access to a node of the PTP n/w or has gained full control of one device in the network. This requires additional capability to tap the h/w where PTP timing is implemented.  Selective interception and removal can impact timing packets and cause clock degradation in attacked nodes. Removing all packets or random packets may push the clocks in attacked nodes into free running mode  This attack results in a situation where the time protocol is operational, but slaves are being provided intentionally inaccurate timing information.  This degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell.  A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. |

|  |  |
| --- | --- |
| Threat ID | T-SPLANE-05 |
| **Threat title** | Packet delay manipulation attack |
| **Threat description** | IEEE 1588 requires symmetric delays between GM and slaves. In packet delay manipulation attacks, the attacker is positioned such a way that allows him to delay the transmission of legitimate time synchronization protocol packets to the indended destination.  An attacker launches this attack by either tapping the transmission network or by taking control of an intermediate nodes such as routers, switches and T-TCs.  This attack results in a situation where the time protocol is operational, but slaves are being provided intentionally inaccurate timing information.  This degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell.  A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. |

|  |  |
| --- | --- |
| Threat ID | T-CPLANE-01 |
| **Threat title** | Spoofing of DL C-plane messages |
| **Threat description** | The lack of authentication could allow an adversary to inject own DL C-plane messages that falsely claiming to be from the associated O-DU.  As a result, it would block the O-RU from processing the corresponding U-Plane packets, leading to temporarily DoS. (Dropping the entire DL C-plane messages achieves the same goal). |

|  |  |
| --- | --- |
| Threat ID | T-CPLANE-02 |
| **Threat title** | Spoofing of UL C-plane messages |
| **Threat description** | The lack of authentication could allow an adversary to inject own UL C-plane messages that falsely claiming to be from the associated O-DU.  As a result, temporarily limited cell performance (or even DoS) on cells served by the O-RU and in addition a consequential DoS threat to all O-RUs served by that O-DU will exist. (Dropping the entire UL C-plane messages achieves the same goal). |

|  |  |
| --- | --- |
| Threat ID | T-UPLANE-01 |
| **Threat title** | An attacker attempts to intercept the Fronthaul (MITM) over U Plane |
| **Threat description** | The High bit rate Fronthaul interface impose strict performance requirements ((bandwidth, latency, fronthaul transport link length, etc.) that limit the use of some security features, due to the increased processing delay. This opens the risk of Man-in-the-Middle (MITM) attacks over the fronthaul interface to intercept the U-Plane.  For the transported U-Plane data an attacker could potentially do threats, such as passive wiretapping and denial of service, but would need to break PDCP Security prior to any content access.  3GPP defines UP integrity protection algorithms in their specifications but many of the OEMs have not implemented them because of impact on the user experience (e.g. download and upload data throughputs). Enabling UP integrity protection requires considerable compute resources and adds overhead that directly impacts the maximum throughputs that can be measured on the user device. The integrity protection is enabled on the Control Plane messages but that still leaves the user’s data traffic vulnerable because the Control Plane and User Plane are segregated. For example, the lack of UP integrity could enable a rogue base station to manipulate the user data messages (i.e. DNS) and redirect a user to a malicious website. |

#### Threats against O-RU

The O-RU introduces the following threats:

|  |  |
| --- | --- |
| Threat ID | T-ORU-01 |
| **Threat title** | An attacker stands up a false base station attack by attacking an O-RU |
| **Threat description** | A false base station attack occurs when an attacker masquerades as a legitimate mobile network to facilitate a Man-in-The-Middle (MiTM) attack between a subscriber’s user equipment (UE) and the mobile network.  There are three attack scenarios on an O-RU that enable an attacker to realize a false base station attack:   1. Hijack fronthaul to realize a false base station attack: Attacker disables an operational O-RU’s access to the open fronthaul, plugs a false base station system into the operational O-RU’s fronthaul interface, and launches a false base station attack with the O-RU providing the air interface. 2. Recruit a standalone O-RU to realize a false base station attack: The stand-alone O-RU is an O-RU that is not operational but is available to an attacker to incorporate into a false base station system. The attacker plugs a false base station system into the standalone O-RU’s fronthaul interface and launches a false base station attack with the O-RU providing the air interface. 3. Gain unauthorized physical access to O-RU to realize a false base station attack: An attacker gains access to external and internal components of an O-RU (other than the open fronthaul interface), connects the O-RU under attack to a false base station system, and launches a false base station attack with the O-RU providing the air interface.   Successful attacks may cause:   1. For a subscriber’s UE in attack scenarios 1, 2, and 3: the false base stations, also known as SUPI/5G-GUTI catchers, retrieves a subscriber identity by forcing a UE to attach to the false base station systems. This opens the door to subscriber identity interception/disclosure and unauthorized subscriber tracking attacks. These attacks include stealing subscriber information, tampering with transmitted information, tracking subscribers, and compromising subscriber privacy. 2. For the operator network: in attack scenario 1, the attacker removes the operational O-RU from providing service to UEs in the coverage area served by the operational O-RU. 3. For operators and vendors in attack scenarios 1, 2, and 3, the attacker recruits legitimate operator/vendor equipment for the purpose of creating a false base station attack on subscribers, possibly harming the reputation of the operator and vendor whose O-RU was used in the attack.   **NOTE**: The false base station threat has existed since GSM networks and continued to evolve and persist with the evolution of mobile networks. 5G networks are expected to introduce several security enhancements over 4G and legacy networks. Despite these security enhancements, 5G networks could still be a target of false base station attacks [19]. |

#### Threats against Near-RT RIC

Near-Real-Time (RT) RIC introduces the following threats:



Figure 7‑2 : UE Identification in Near-RT-RIC

|  |  |
| --- | --- |
| Threat ID | T-NEAR-RT-01 |
| **Threat title** | Malicious xApps can exploit UE identification, track UE location and change UE priority [12] |
| **Threat description** | xApps in the Near-RT-RIC have the capability to manipulate behavior of a certain cell, a group of UEs, and a specific UE. A malfunctioning or unavailable root of trust could potentially cause issues on the network and compromise RAN performance, privacy, etc. For example, the xApp could track a certain subscriber or impact service for a subscriber or a dedicated area. In addition, an xApp can receive order via A1 to control a certain UE and if a malfunctioning xApp receives an order to prioritize this UE, then the owner of the malfunctioning xApp knows a VIP that they want to track is in a certain area. With this command exposure, the attacker can obtain a rough location of a very important person and change the order from prioritize to deprioritize for a UE.  Further, E2 interface exposes UE identification that can be exploited by a malicious xApp. As the E2 interface (similar to A1 interface) can point out a certain UE in the network, this will create a correlation between the randomized (anonymized) UE identities between the RAN nodes. For example, a xApp can potentially be used as a “sniffer” for UE identification. The additional challenge for the Near-RT RIC / E2 compared to the Non-RT RIC / A1 is that more frequent signaling is expected over the E2 interface to enable near-real-time operation. Therefore, the UE identifier will be exchanged more frequently over the E2 than over the A1. |

|  |  |
| --- | --- |
| Threat ID | T-NEAR-RT-02 |
| **Threat title** | Risk of deployment of a malicious xApp on Near-RT RIC |
| **Threat description** | The security threats associated with the onboarding and deployment of malicious xApps include:  • Malicious xApps attaining unauthorized access to the Near-RT RIC and E2 Nodes  • Malicious xApps abusing radio network information and control capabilities over RAN functions  • Malicious xApp impacting service for a subscriber or a dedicated area  • Malicious xApp exploiting UE identification, tracking UE location and changing UE slice priority |

|  |  |
| --- | --- |
| Threat ID | T-NEAR-RT-03 |
| **Threat title** | Attackers exploit non authenticated, weakly or incorrectly authenticated Near-RT RIC APIs |
| **Threat description** | Not mutually authenticating xApps and Near-RT RIC platform APIs could potentially allow attackers to perform the following type of attacks [20]:   * Operating malicious xApp claiming to be genuine in order to request certain services (theft of services) or information (data leakage) * Man in the middle attacks between a genuine xApp and a Near-RT RIC platform API * Querying network or UE information from a compromised xApp to Near-RT RIC platform (e.g. database via SDL API), thereby leaking potentially sensitive data about network and/or UE (potential privacy issues) * Subscribing a malicious xApp to services provided by the Near-RT RIC platform, such as API-related events notifications, discovery of APIs, E2SM, etc.   The use of weak credentials in the process of API authentication can compromise the overall system. The user/password combination isn’t considered safe, not only for password related attacks (e.g., brute-force), but also it would represent a high risk to allow xApps, especially 3rd party xApps, to store the user/password combo. This approach would extend the attack surface into xApps side.  As a reference, OWASP API Security Top 10 report [21] indicates that authentication mechanisms are often implemented incorrectly, allowing attackers to compromise authentication tokens or to exploit implementation flaws to assume other user's identities temporarily or permanently. Compromising system's ability to identify the client/user, compromises API security overall. |

|  |  |
| --- | --- |
| Threat ID | T-NEAR-RT-04 |
| **Threat title** | Attackers exploit non authorized Near-RT RIC APIs to access to resources and services which they are not entitled to use. |
| **Threat description** | If the API consumers are not authorized by the API producers, attackers (e.g, malicious xApps) would potentially be able to perform the following types of attacks:   * Abuse and/or theft of services or information (data leakage), requesting and successfully obtaining them from the platform, e.g, in order to extract potentially sensitive information from the network and/or UEs * Negatively impacting the network performance due to malicious policies over E2 Nodes * Flooding the platform with resource demanding operations that may lead to a Denial of Service attack   As a reference, OWASP API Security Top 10 report [21] indicates that ‘Broken Object Level Authorization’ has been the most common and impactful attack on APIs. Even if the application implements a proper infrastructure for authorization checks, developers might forget to use these checks before accessing a sensitive object. Unauthorized access can result in data disclosure to unauthorized parties, data loss, or data manipulation.  In the actual context of Near-RT RIC [8], the platform as API producer is responsible to specify those rights/privileges for the platform services as resources to the xApps as consumers. In general, an xApp should only have the required set of permissions to perform the actions for which they are authorized, and no more.  **NOTE**: The investigation of services for which the API producer is the xApp is for further study |

|  |  |
| --- | --- |
| Threat ID | T-NEAR-RT-05 |
| **Threat title** | Attackers exploit non uniquely identified xApps using a trusted xAppID to access to resources and services which they are not entitled to use. |
| **Threat description** | Not uniquely identifying xApps using a trusted xAppID potentially entails certain threats and potential attacks:   * A non-unique xAppID might cause misidentification of an xApp, possibly allowing a potentially malicious xApp to request certain services (theft of services), information (data leakage), or alter existing information * A malicious xApp might use the xAppID assigned to a legitimate xApp to request services or information from Near-RT RIC platform * A non-unique xApp ID could make it impossible to accurately assign actions to the correct xApp * A non-unique xApp ID could make it difficult to recognize that a malicious xApp is in the environment |

#### Threats against Non-RT RIC

Threats against Non-RT RIC include:

|  |  |
| --- | --- |
| Threat ID | T-NONRTRIC-01 |
| **Threat title** | An attacker penetrates the Non-RT RIC to cause a denial of service or degrade the performance |
| **Threat description** | An attacker penetrates the Non-RT RIC through the SMO and attempts to trigger a Denial of Service or degrade the performance of non-RT RIC so that non-RT RIC would not be liable for ensuring:   * The monitoring or tracing of the network to understand the effect of the A1 policy on performance in Near-RT RIC * The update of A1 policy * The exposure and secure delivery of A1 Enrichment Information to near-RT RIC * The setup of access control rules and the selection of which Enrichment Information ID (EiId) are exposed to a near-RT RIC |

|  |  |
| --- | --- |
| Threat ID | T-NONRTRIC-02 |
| **Threat title** | UE tracking in the Non-RT RIC |
| **Threat description** | An attacker gains access to the Non-RT RIC through the SMO for UE tracking. |

|  |  |
| --- | --- |
| Threat ID | T- NONRTRIC-03 |
| **Threat title** | Data Corruption/Modification |
| **Threat description** | An attacker gains access to the Non-RT RIC through the SMO to cause Data Corruption/Modification. |

|  |  |
| --- | --- |
| Threat ID | T-NONRTRIC-04 |
| **Threat title** | Attacker exploits non-uniquely identified rApp instances |
| **Threat description** | An attacker can exploit non-uniquely identified rApp instances using a trusted rAppID to gain unauthorized access to services and data. Potential threats and attacks include:   * A non-unique rAppID might cause misidentification of an rApp instance, possibly allowing a potentially malicious rApp instance to request certain services (theft of services), information (data leakage), or alter existing information * A malicious rApp instance might use the rAppID assigned to a legitimate rApp instance to request access to R1 services or data * A non-unique rApp ID could make it impossible to accurately assign actions to the correct rApp instance * A non-unique rApp ID could make it difficult to recognize that a malicious rApp instance is in the environment |

#### Threats against xApps

xApps introduce the following threats:



Figure 7‑3 : Near-RT-RIC and xApps conflict with gNB

|  |  |
| --- | --- |
| Threat ID | T-xApp-01 |
| **Threat title** | An attacker exploits xApps vulnerabilities and misconfiguration |
| **Threat description** | Vulnerabilities can potentially exist in any xApp if it stems from an untrusted or unmaintained source. If attackers can find exploitable xApp, they can disrupt the offered network service and potentially take over another xApp or the whole near-RT RIC.  The actual consequences may vary. For example, an attacker may gain the ability to alter data transmitted over A1 or E2 interfaces, extract sensitive information, etc.  Malicious xApps impact near-RT RIC functions in the purpose of performance degradation, DoS, etc.  xAPPs have the capability to manipulate behavior of a certain cell, a group of UEs, and a specific UE. A malfunctioning xApp could potentially track a certain subscriber or impact service for a subscriber or a dedicated area [12]. |

|  |  |
| --- | --- |
| Threat ID | T-xApp-02 |
| **Threat title** | Conflicting xApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS [12] |
| **Threat description** | Conflicting xApps unintentionally or maliciously impact O-RAN system functions such as mobility management, admission controls, bandwidth management and load balancing in the purpose of performance degradation.  There is no clear functional split between the Near-RT RIC and the O-gNB. The functional split depends on the available xApps and the capabilities exposed by the O-gNB. This creates possible conflicts between the decisions taken by the Near-RT RIC and the O-gNB that could lead to instability in the network, which introduces vulnerabilities that could be exploited by threat actors. For example, a threat actor can utilize a malicious xApp that intentionally triggers RRM decisions conflicting with the O-gNB internal decisions to create denial of service. |

|  |  |
| --- | --- |
| Threat ID | T-xApp-03 |
| **Threat title** | An attacker compromises xApp isolation |
| **Threat description** | An attacker can exploit weaknesses and vulnerabilities to compromise xApp isolation and to break out of xApp confinement. For example, attacker can use the underlying system vulnerabilities to easily breach isolation and confinement.  Adversary can use side effects resulting from a shared resource usage to deduce information from co-hosted xApps.  Gaining unauthorized access to the underlying system provides new opportunities to exploit vulnerabilities in other xApps or O-RAN components to intercept and spoof network traffic, to degrade services (DoS), etc. |

|  |  |
| --- | --- |
| Threat ID | T-xApp-04 |
| **Threat title** | False or malicious A1 policies from the Non-RT RIC inform behavior of xApps to trigger a DoS, affect performance, or locate a subscriber. |
| **Threat description** | Unauthorized access to the Non-RT RIC enables the creation of ‘false policies’ that can be issued to the Near-RT RIC for enforcement. Existing Near-RT RIC policies could also be modified to achieve a false policy. False policies passed to the Near-RT RIC would be persistent until they were modified or deleted by the Non-RT RIC or the Near-RT RIC power cycles.  False policies can be created to have numerous impacts to the normal performance of the RAN. A single false A1 policy can target a specific UE, groups of UEs, or an entire cell. A false policy could influence the Near-RT RIC to configure the O-DU and O-RU functions to support Denial of Service (DoS) attacks by using feedback data to degrade RAN performance.  False policies could also be used for the purpose of locating a subscriber or group of subscribers. In this case, the false policy would cause the Near-RT RIC to isolate a subscriber in the O-CU. The Near-RT RIC could also use MIMO beamforming in the O-DU and O-RU to isolate a user onto a single beam. The data feedback from the RAN can include UE location or trajectory information from GPS data. The subscriber location would be attained from access to the Non-RT RIC in the SMO function.  The Near-RT RIC is capable of steering traffic to achieve optimal QoS or QoE performance. A false policy could notionally cause the Near-RT RIC to steer user data to isolate the data in order to facilitate a cyber-attack. |

#### Threats against rApps

Threats against rApps include:

|  |  |
| --- | --- |
| Threat ID | T-rAPP-01 |
| **Threat title** | Conflicting rApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS |
| **Threat description** | rApps in the Non-RT RIC can be provided by different vendors. For example, one vendor can provide the rApp for Carrier license scheduling and another vendor provide the rApp for energy saving, etc.  This creates the risk that different rApps will take conflicting decisions at the same instance in time for the same user. Such conflicts between rApps include:   * Direct conflicts: different rApps request change for the same parameter. * Indirect conflicts: different rApps request change to different parameters that will create opposite effects. * Implicit conflicts: different rApps request change to different parameters that are not creating any obvious opposite effect but result in an overall network performance degradation, instabilities, etc.   These conflicts are difficult to mitigate since dependencies are impossible to observe. |

|  |  |
| --- | --- |
| Threat ID | T-rAPP-02 |
| **Threat title** | An attacker exploits rApp vulnerabilities |
| **Threat description** | Vulnerabilities can potentially exist in any rApp. If attackers can find exploitable rApp, they can potentially force a data breach, disrupt the offered network service. and take over another rApp or the non-RT RIC.  The actual consequences may vary. For example, an attacker may gain the ability to alter data transmitted over A1 interface, extract sensitive information, etc. |

|  |  |
| --- | --- |
| Threat ID | T-rAPP-03 |
| **Threat title** | An attacker exploits rApps misconfiguration |
| **Threat description** | Security misconfiguration, such as open ports or enabled unused protocols, can potentially exist in an rApp. If attackers can find exploitable rApp, they can disrupt the offered network service and potentially take over another rApp or the whole non-RT RIC.  The actual consequences may vary. For example, an attacker may gain the ability to alter data transmitted over A1 interface, extract sensitive information, etc. |

|  |  |
| --- | --- |
| Threat ID | T-rAPP-04 |
| **Threat title** | An attacker bypasses authentication and authorization |
| **Threat description** | An Attacker can exploit an rApp that has weak or misconfigured authentication and authorization to gain access to the rApp and pose as a tenant. |

|  |  |
| --- | --- |
| Threat ID | T-rAPP-05 |
| **Threat title** | An attacker deploys and exploits malicious rApp |
| **Threat description** | An untrusted source may intentionally provide a malicious rApp. A trusted source may have a backdoor intentionally inserted in the rApp. If attackers can find exploitable rApp, they can disrupt the offered network service and potentially take over another rApp or the whole non-RT RIC.  Malicious rApps could impact non-RT RIC functions such as AI/ML model training, A1 policy management, Enrichment information management, Network Configuration Optimization in the purpose of performance degradation, DoS, enrichment data sniffing (UE location, trajectory, navigation information, GPS data, etc.), etc. |

|  |  |
| --- | --- |
| Threat ID | T-rAPP-06 |
| **Threat title** | An attacker bypasses authentication and authorization using an injection attack |
| **Threat description** | It is possible that an attacker to submit requests without prior authentication and authorization by executing an injection attack to manipulate configurations, access logs, perform remote code execution, etc. |

|  |  |
| --- | --- |
| Threat ID | T-rAPP-07 |
| **Threat title** | rApp exploits services |
| **Threat description** | A malicious rApp or a trusted but compromised rApp can exploit services across the R1 interface |

#### Threats against PNF

NFs could be either VNF, CNF or PNF. Vulnerabilities of a PNF could be used as a starting point for an attack against VNFs/CNFs.

|  |  |
| --- | --- |
| Threat ID | T-PNF-01 |
| **Threat title** | An attacker compromises a PNF to launch reverse attacks and other attacks against VNFs/CNFs |
| **Threat description** | A lack of security policies to protect mixed PNF-VNF/CNF deployments could be used to perform attacks against VNFs/CNFs, potentially taking advantage of legacy security used by PNFs and not provided by the virtualization/containerization layer.  Attackers could use insecure interfaces as injection points and for reverse attack. |

#### Threats against R1 interface

The R1 interface facilitates inter-connection between rApps and Non-RT RIC framework supplied by different vendors, and provides a level of abstraction between rApps and Non-RT RIC framework/SMO that can be the consumers and or producers of R1 services.

|  |  |
| --- | --- |
| Threat ID | T-R1-01 |
| **Threat title** | An attacker gains unauthorized access to R1 services |
| **Threat description** | “Service management and exposure services Producer” determines whether the Service Producer is authorized to produce the service. An attacker can perform a spoofing attack to gain unauthorized access to R1 services. |

|  |  |
| --- | --- |
| Threat ID | T-R1-02 |
| **Threat title** | Attacker modifies Service Heartbeat message to cause Denial of Service |
| **Threat description** | Attacker can exploit the Service Heartbeat on the R1 by modifying or inserting heartbeat messages to cause denial of service |

|  |  |
| --- | --- |
| Threat ID | T-R1-03 |
| **Threat title** | Malicious actor bypasses authentication to Request Data |
| **Threat description** | Attacker can exploit password-based authentication on the R1 to request unauthorized data. Weak password management can easily be exploited. (Certificate-based mutual authentication using TLS and PKI X.509 certificates is recommended). |

|  |  |
| --- | --- |
| Threat ID | T-R1-04 |
| **Threat title** | An attacker bypasses authorization to discover data |
| **Threat description** | “Data registration and discovery service producer” determines whether the Data Producer is authorized to produce the data types. An attacker can perform a spoofing attack to bypass authorization to discover available data. |

|  |  |
| --- | --- |
| Threat ID | T-R1-05 |
| **Threat title** | An attacker gains unauthorized access to data |
| **Threat description** | An attacker can perform a spoofing attack to exploit the Data request and subscription service for the purpose to gain unauthorized access to data. |

|  |  |
| --- | --- |
| Threat ID | T-R1-06 |
| **Threat title** | An attacker modifies a Data Request |
| **Threat description** | Data Consumers consume the “Data request and subscription service” to request data instances or subscribe to them. An attacker can modify a request to force the consumer to receive a different data set then that intended. Without checks, the received data could be processed, leading to erroneous decisions or triggers. |

|  |  |
| --- | --- |
| Threat ID | T-R1-07 |
| **Threat title** | A malicious actor snoops Data Delivery to the Data Consumer |
| **Threat description** | Data delivery messages relate to a particular data request or subscription. The data can be delivered to the Data Consumer in different ways, including:  • as part of the payload of a data delivery message,  • as a data stream,  • from e.g., a REST endpoint, a message bus or object store location.  An attacker can perform snooping, injection, or modification attacks in the Delivery of Data process. |

#### Threats against A1 interface

A1 interface enables the Non-RT RIC function to provide policy-based guidance, ML model management and enrichment information to the Near-RT RIC function for RAN can optimization. The Non-RT RIC can provide enrichment information over the A1 interface to support the policy enforcement in the Near-RT RIC. The A1 interface is used for discovery, request and delivery of A1 Enrichment Information and discovery of External Enrichment Information.



**Figure 7‑4 : A1 interface between the Non-RT RIC and the Near-RT RIC**

|  |  |
| --- | --- |
| Threat ID | T-A1-01 |
| **Threat title** | Untrusted peering between Non-RT-RIC and Near-RT-RIC |
| **Threat description** | Malicious Non-RT-RIC peers with a Near-RT-RIC over the A1 interface, or a malicious Near-RT-RIC peers with a Non-RT-RIC over the A1 interface, due to weak mutual authentication. |

|  |  |
| --- | --- |
| Threat ID | T-A1-02 |
| **Threat title** | Malicious function or application monitors messaging across A1 interface |
| **Threat description** | Internal threat actor can gain access to the messaging across the A1 interface for a MiTM attack to read policy. |

|  |  |
| --- | --- |
| Threat ID | T-A1-03 |
| **Threat title** | Malicious function or application modifies messaging across A1 interface |
| **Threat description** | Internal threat actor can gain access to the messaging across the A1 interface for a MiTM attack to modify or inject policy. This can result in the Near-RT RIC receiving malicious policy. |

#### Threats against application life cycle

|  |  |
| --- | --- |
| Threat ID | T-AppLCM-01 |
| **Threat title** | Compromise of App/VNF/CNF update package integrity prior to onboarding |
| **Threat description** | Attackers gains access to the SMO to modify the App/VNF/CNF update package to enable a malicious application. |
| **Threat type** | Tampering; Denial of Service |
| **Impact type** | Integrity; Availability |
| **Affected Asset** | ASSET-D-15: App/VNF/CNF software package |

|  |  |
| --- | --- |
| Threat ID | T-AppLCM-02 |
| **Threat title** | Compromise of App/VNF/CNF update image integrity during instantiation |
| **Threat description** | Attacker gains access to the O-Cloud platform to modify the App/VNF/CNF update image to enable a malicious application. |
| **Threat type** | Tampering; Denial of Service |
| **Impact type** | Integrity; Availability |
| **Affected Asset** | ASSET-D-15: App/VNF/CNF software package |

|  |  |
| --- | --- |
| Threat ID | T-AppLCM-03 |
| **Threat title** | Downgrade attack to vulnerable application version |
| **Threat description** | A software version downgrade attack is a form of attack on a system that makes it abandon a more recent version of a software package in favor of an older, possibly vulnerable, version.  Malicious actor downgrades an application to enable exploitation of application vulnerabilities. |
| **Threat type** | Denial of Service; Tampering |
| **Impact type** | Availability; Integrity |
| **Affected Asset** | ASSET-D-15: App/VNF/CNF software package |

|  |  |
| --- | --- |
| Threat ID | T-AppLCM-04 |
| **Threat title** | Attacker exploits missing or improperly defined elements of application’s SecurityDescriptor |
| **Threat description** | Proper and comprehensive definition of the App/VNF/CNF package SecurityDescriptor helps ensure elements of security needed for the App/VNF/CNF package are present. If attackers can find missing or improperly defined elements of an App/VNF/CNF package SecurityDescriptor, they can exploit that to gain unauthorized access to data and services. |
| **Threat type** | Elevation of Privilege; Denial of Service |
| **Impact type** | Authorization; Availability |
| **Affected Asset** | ASSET-D-15: App/VNF/CNF software package |

|  |  |
| --- | --- |
| Threat ID | T-AppLCM-05 |
| **Threat title** | Malicious actor modifies application’s SecurityDescriptor |
| **Threat description** | Malicious actor modifies fields of an App/VNF/CNF package SecurityDescriptor to change security elements of the App/VNF/CNF, which could include information on encryption, algorithms, key requirements, firewall rules, etc. An attacker can modify the SecurityDescriptor to cause service disruption and gain unauthorized access to data and services. |
| **Threat type** | Tampering; Elevation of Privilege; Denial of Service |
| **Impact type** | Integrity; Authorization; Availability |
| **Affected Asset** | ASSET-D-15: App/VNF/CNF software package |

|  |  |
| --- | --- |
| Threat ID | T-AppLCM-06 |
| **Threat title** | Improper decommissioning of application |
| **Threat description** | The improper decommissioning of an application can lead to excessive or conflicting resource usage, accidental deletion of pertinent data (such as application data, cryptographic keys, etc.), and misallocation of resources to a malicious application. Credentials or other trust relationships may not be revoked or removed, which leaves an exposure. |
| **Threat type** | Denial of Service, Information Disclosure |
| **Impact type** | Availability, Confidentiality |
| **Affected Asset** | ASSET-C-02: Near-RT RIC software, ASSET-C-11: Non-RT RIC software, ASSET-C-09: xApps, ASSET-C-10: rApps, ASSET-C-03: O-CU-CP software, ASSET-C-04: O-CU-UP software, ASSET-C-05: O-DU software |

|  |  |
| --- | --- |
| Threat ID | T-AppLCM-07 |
| **Threat title** | Improper deletion of application sensitive data |
| **Threat description** | Adversary can gain access to sensitive data and secrets if an application’s data is not securely deleted. This can include access to secure artifacts such as certificates and keys. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | ASSET-D-16: X.509 certificates, ASSET-D-17: Private keys, ASSET-D-32: Cryptographic keys used during secure boot |

#### 7.4.1.12 Threats against E2 interface

E2 is a logical interface connecting the Near-RT RIC with an E2 Node as defined in [25]. The E2 functions are grouped into the following categories:

* Near-RT RIC Services
* Near-RT RIC support functions

|  |  |
| --- | --- |
| Threat ID | T-E2-01 |
| **Threat title** | Untrusted Near-RT-RIC and/or E2 Nodes |
| **Threat description** | A malicious E2 Node communicates with a Near-RT-RIC over the E2 interface, or a malicious Near-RT-RIC communicates with an E2 Node over the E2 interface, due to weak mutual authentication. |

|  |  |
| --- | --- |
| Threat ID | T-E2-02 |
| **Threat title** | Malicious actor monitors messaging across E2 interface |
| **Threat description** | Threat actor can gain access to the messaging across the E2 interface for a MiTM attack to read messages. |

|  |  |
| --- | --- |
| Threat ID | T-E2-03 |
| **Threat title** | Malicious actor modifies messaging across E2 interface |
| **Threat description** | Threat actor can gain access to the messaging across the E2 interface for a MiTM attack to modify or inject messages. This can result in the Near-RT RIC and/or the E2 Nodes receiving malicious messages. |

#### 7.4.1.13 Threats against Y1 interface

The Near-RT RIC provides RAN analytics information (RAI) services via Y1 service interface. These services can be consumed by Y1 consumers by subscribing to or requesting the RAN analytics information via the Y1 service interface. Y1 consumers may be Application Functions (AFs) which are within an O-RAN trusted domain. AFs outside the O-RAN trusted domain may use Y1 services, too. Further details are available in the O-RAN Architecture Description [6], clauses 5.1 and 5.4.18.

Near-RT RIC

RAI producer xApp

Y1T

Y1 Consumers

Y1 API(s)

RAI API(s)

**Figure 7‑5 : RAN analytics information (RAI) services via Y1 service interface**

Malicious Y1 consumers may use their access through the Y1 interface with the intent of accessing, manipulating or negatively impacting the privacy of subscribers, the RAN or the core network.

|  |  |
| --- | --- |
| Threat ID | T-Y1-01 |
| **Threat title** | Untrusted Near-RT-RIC and Y1 consumers |
| **Threat description** | A Malicious Y1 consumer communicates with a Near-RT-RIC over the Y1 interface, or a malicious Near-RT-RIC communicates with a Y1 consumer over the Y1 interface, due to weak mutual authentication. |

|  |  |
| --- | --- |
| Threat ID | T-Y1-02 |
| **Threat title** | Malicious actor monitors messaging across Y1 interface |
| **Threat description** | Threat actor can gain access to the messaging across the Y1 interface for a MiTM attack to read messages. |

|  |  |
| --- | --- |
| Threat ID | T-Y1-03 |
| **Threat title** | Malicious actor modifies messaging across Y1 interface |
| **Threat description** | Threat actor can gain access to the messaging across the Y1 interface for a MiTM attack to modify or inject messages. This can result in the Near-RT RIC and/or the Y1 consumers receiving malicious messages. |

### Threats against O-CLOUD

Virtualization and containerization technologies in O-RAN introduce the following relevant threats:

#### Generic Threats

|  |  |
| --- | --- |
| **Threat ID** | T-GEN-01 |
| **Threat title** | Software flaw attack |
| **Threat description** | Code of host OS, Hypervisor/Container Engine and VNF/CNF can include flaws that an attacker can exploit if they are present.  As O-RAN software components relies on opensource software, opensource libraries, 3rd party components. Vulnerability in any of these software components likely to allow attacker to exploit O-CLOUD environment. This could lead attacker to carry out to malicious activities, such as:   * Compromise of the underlying VM/Container * Exploit host access via Escape to Host * Take advantage of weak identity and access management policies to attempt to elevate privileges * Execute adversary-controlled code * Enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host |

|  |  |
| --- | --- |
| **Threat ID** | T-GEN-02 |
| **Threat title** | Malicious access to exposed services using valid accounts |
| **Threat description** | Access to valid accounts to use the O-Cloud services is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the network.  Adversaries may obtain and abuse credentials of existing accounts as a means of gaining initial access, persistence, privilege escalation, or defense evasion. Compromised credentials may be used to bypass access controls placed on various resources on O-Cloud.  Compromised credentials may also grant an adversary increased privilege to specific O-Cloud services or access to restricted areas of the O-Cloud network.  Access may be also gained through an exposed service that doesn’t require authentication. In containerized environments, this may include an exposed Docker API, Kubernetes API server, kubelet, or web application such as the Kubernetes dashboard. |

|  |  |
| --- | --- |
| **Threat ID** | T-GEN-03 |
| **Threat title** | Untrust binding between the different O-Cloud layers |
| **Threat description** | One major challenge in virtualized architectures and especially in O-Cloud is to prove that a particular VM/Container runs on top of a specific Hypervisor/Container Engine. More specifically, it is necessary to assure that a trusted VM/Container is executed on a particular trusted Hypervisor/Container Engine, whereas the Hypervisor/Container Engine's trust state relies on an attestation that considers the entire corresponding hard and software stack. More precisely, this includes all hardware chips, firmware, OS and Hypervisor/Container Engine components that are relevant for the Hypervisor/Container Engine's trust state determination.  If it is not possible to establish a correlation between VM/Container and Hypervisor/Container Engine, an attacker is able to make use of a trusted VM/Container that runs on top of an untrusted Hypervisor/Container Engine and it would be impossible to detect any interference made by the malicious Hypervisor/Container Engine, e.g. intercepting communication, replacing strong or using weak cryptographic keys, etc. Similarly, trustworthiness in the service-layer might only be established if there is a mechanism to determine that only trusted VNFs/CNFs, w.r.t trusted VM/Container's, are running on specific trusted Hypervisors/Container Engines that are part of the service-provisioning-chain. |

|  |  |
| --- | --- |
| **Threat ID** | T-GEN-04 |
| **Threat title** | Lack of Authentication & Authorization in interfaces between O-Cloud components |
| **Threat description** | O-Cloud deploys CNF applications as containers in a cluster of physical nodes which may be spanned across geographical locations. Owing to the Service Based Architecture of CNFs, this introduces several service endpoints communicating across each other over the network (container to container, container to cloud infrastructure component) and it is fairly difficult to distinguish between a service terminating an external interface and a service exposing only an internal interface.  Multi-tenant deployments and deployments in public cloud also require the CNF applications to run alongside unknown entities. In such deployment scenarios, CNF service endpoints with no authentication/weak authentication expose risk of attack that can impact the availability of service and the CNF.  Lack of proper authentication in interfaces exposed by CNF services, introduces threats of lateral movement where a compromised container/rogue container   * can compromise the availability of internal service by bringing down the internal service and perform lateral movement of attack by exploiting the availability of other such services * can compromise the confidentiality of the internal service by extracting critical application data |

|  |  |
| --- | --- |
| **Threat ID** | T-GEN-05 |
| **Threat title** | Unsecured credentials and keys |
| **Threat description** | Adversaries may search compromised O-RAN NFs, VL, orchestration layer or hardware to find and obtain insecurely stored credentials. These credentials can be stored and/or misplaced in many locations on the O-cloud platform, including plaintext files (e.g. Bash History), operating system or application-specific repositories (e.g. Credentials in Registry), or other specialized files/artifacts (e.g. Private Keys) [22].  **Bash History**: Adversaries may search the bash command history on compromised systems for insecurely stored credentials.  **Credentials in registry**: Adversaries may search the Registry on compromised systems for insecurely stored credentials.  **Private Keys**: Adversaries may search for private key certificate files on compromised systems for insecurely stored credentials. Private cryptographic keys and certificates are used for authentication, encryption/decryption, and digital signatures; Common key and certificate file extensions include: .key, .pgp, .gpg, .ppk., .p12, .pem, .pfx, .cer, .p7b, .asc.  Adversary tools have been discovered that search compromised systems for file extensions relating to cryptographic keys and certificates. |

|  |  |
| --- | --- |
| **Threat ID** | T-GEN-06 |
| **Threat title** | Sensitive application data cache exploitation |
| **Threat description** | Most of the applications use data that is sensitive in nature which needs to be secured. And it is common for these applications to cache such sensitive data, after retrieving the data from a secure storage. This caching occurs in various forms: within application memory, in persistent file systems, or in ephemeral file systems (For example, non-persistent container file system).  For a VNF, the application can cache the sensitive data in its memory which is non-persistent (erased when the application ceases to exist) or in the persistent virtual machine file system.  For a CNF, the application can store the sensitive data in its memory which is non-persistent (erased when the application/microservice ceases to exist) or in the non-persistent container file system, or in the persistent host file system, provided the application has the necessary privileges to access host file system.  The sensitive data components that are cached by applications could be of different types which are used as authentication keys, session keys, passwords, tokens, etc.  The storage of sensitive data in the application cache is used to improve performance of the applications and keeping the sensitive information readily available to the applications for faster initialization, re-initialization or recovery.  An example of faster recovery/re-initialization is a scenario where a TLS client establishes a TLS session with a server and stores the client certificate and corresponding private key in the application cache. If the TLS session is terminated unexpectedly (For example, due to network error conditions), the TLS client uses the cached client certificates and private key for recovering / re-establishing the TLS session, instead of retrieving the information from a more secure, but slower, storage solution.  While leveraging application cache is indispensable for significant performance gains, it also presents a notable security risk [28], [29]. The sensitive data stored in application cache would be a primary target from attackers/threat actors [30], who can exploit this information to penetrate deeper into O-RAN network functions.  To counter this threat, a “Defense in depth” approach is essential. This approach encompasses multiple security layers designed to mitigate risks associated with application caches, focusing on strong encryption, strict access management and anomaly detection to protect sensitive data effectively. |

#### Threats concerning VMs/Containers

|  |  |
| --- | --- |
| **Threat ID** | T-VM-C-01 |
| **Threat title** | Abuse of a privileged VM/Container |
| **Threat description** | It’s possible to run VMs/Containers with unintended configurations. Such misconfigurations can help the adversaries to compromise even strongest of VM/Container isolation measures.  Such misconfigurations scenarios include:   * A VMs/Containers can be configured to have more privileges than what is actually required (e.g. settings that give it unnecessary, and perhaps unplanned, privileges). For example, an attacker with access to such a container, can use it to gain higher privileges on host, perform un-authorized operations and get to anything that the host, or any of the containers running on that host, can reach. * A VMs/Containers have unintended read/write access to a directory on host filesystem. This could allow an attacker to perform unauthorized modifications to the contents, create symbolic links to any directories or files not directly exposed by the hostPath, install SSH keys, read secrets mounted to the host, and take other malicious actions. |

|  |  |
| --- | --- |
| **Threat ID** | T-VM-C-02 |
| **Threat title** | VM/Container escape attack |
| **Threat description** | VNF/CNF deployed on the same physical machine as tenants share the same host kernel and host OS resources. Lack of strong isolation between the VMs/Containers and the host allows for a potential risk of a rogue VM/Container escaping the VM/Container confinement and impacting other co-hosted VMs/Containers. In others, an attacker may deploy a new malicious VM/Container configured without network rules, user limitations, etc. to bypass existing defenses within O-Cloud infrastructure.  Attacker deploys malicious VM/Container to escapes the host (Hypervisor/Container Engine/Host OS) and reaches the server’s hardware, then the malicious VM/Container can gain root access to the whole server where it resides. This gives the malicious VM/Container full control on all the VMs/Containers hosted on the same hacked server. This could allow an attacker to undermine the confidentiality, integrity and/or availability of VNFs/CNFs resources.  Containers can be deployed by various means, such as via Docker's create and start APIs or via a web application such as the Kubernetes dashboard or Kubeflow. Adversaries may deploy containers based on retrieved or built malicious images or from benign images that download and execute malicious payloads at runtime.  When a malicious VM/Container escapes isolation, it can gain full control over the underlying host and cause any of the below serious threats:   * Attacker would gain the ability to mount attacks on the host or compromise the host functionalities * Compromise the confidentiality & integrity of co-hosted VMs/Containers and tenants * Launch DDOS attacks on co-hosted VMs/Containers and host services thereby degrading their performance * Introduce new vulnerabilities in host to be used for future attacks * Lack of network segmentation could potentially expose other VMs/Containers in the environment to attack. An example of this could be reconnaissance, exploitation and subsequent lateral movement to another host within the cluster. |

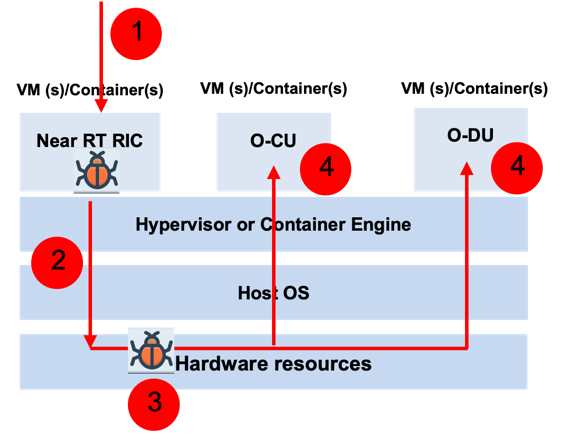


Figure 7‑6 : Illustration of the VM/Container escape attack

|  |  |
| --- | --- |
| **Threat ID** | T-VM-C-03 |
| **Threat title** | VM/Container data theft |
| **Threat description** | The VNF/CNF remotely stores sensitive data (e.g. passwords, private keys, subscription data, logs) on the logical volume that the IMS/DMS allocates to the VNF/CNF. An attacker can retrieve/manipulate these data if they have been stored in an insecure way (e.g. clear text, unsalted hashes) or a malware is installed on the logical volume that the VIM allocates to the VNF/CNF.  Container example: Adversaries may attempt to discover containers and other resources that are available locally within O-Cloud. Other resources may include images, deployments, pods, nodes, and other information such as the status of a cluster. These resources can be viewed within web applications such as the Kubernetes dashboard or can be queried via the Docker and Kubernetes APIs. In Docker, logs may leak information about the environment, such as the environment’s configuration, which services are available, and what cloud provider the victim may be utilizing. The discovery of these resources may inform an adversary’s next steps in the environment, such as how to perform lateral movement and which methods to utilize for execution. |

|  |  |
| --- | --- |
| **Threat ID** | T-VM-C-04 |
| **Threat title** | VM/Container migration attacks |
| **Threat description** | The attacks that exploit VM/Container migration can be divided into two subcategories based on the target plane:   1. **Control Plane Attacks**: These attacks target the module that is responsible for handling the migration process on a server which is called the migration module that is found in the host. By exploiting a bug in the migration module software, the attacker can hack the server and take full control over the migration module. This gives the attacker the ability to launch malicious activities including the following:    1. **Migration Flooding**: The attacker moves all the VMs/Containers that are hosted on the hacked server to a victim server that does not have enough resource capacity to host all the moved VMs/Containers. This causes a denial of service for the VNFs/CNFs running in the VMs/Containers of the victim server as there will not be enough resources to satisfy the demands of all the hosted VMs/Containers leading into VM/Container performance degradation and VM/Container crashes.    2. **False Resource Advertising**: The hacked server claims that it has a large resource slack (a large amount of free resources). This attracts other servers to off-load some of their VMs/Containers to the hacked server so that the O-Cloud workload gets distributed over the O-Cloud servers. After moving VMs/Containers from other servers to the hacked server, the attacker can exploit other vulnerabilities to break into the offloaded VMs/Containers as now these VMs/Containers are placed on a server that is under the control of the attacker. 2. **Data Plane Attacks**: These constitute the second type of VM/Container migration attacks and those attacks target the network links over which the VM/Container is moved from a server to another. Such data plane attacks include the MitM where an attacker sniffs the packets that are exchanged between the source and destination servers and reads the migrated memory pages. The attacker can monitor and/or modify the received packets while continuing to forward them to victim VM/Container resides so that the victim does not detect that any malicious activity is going on. |

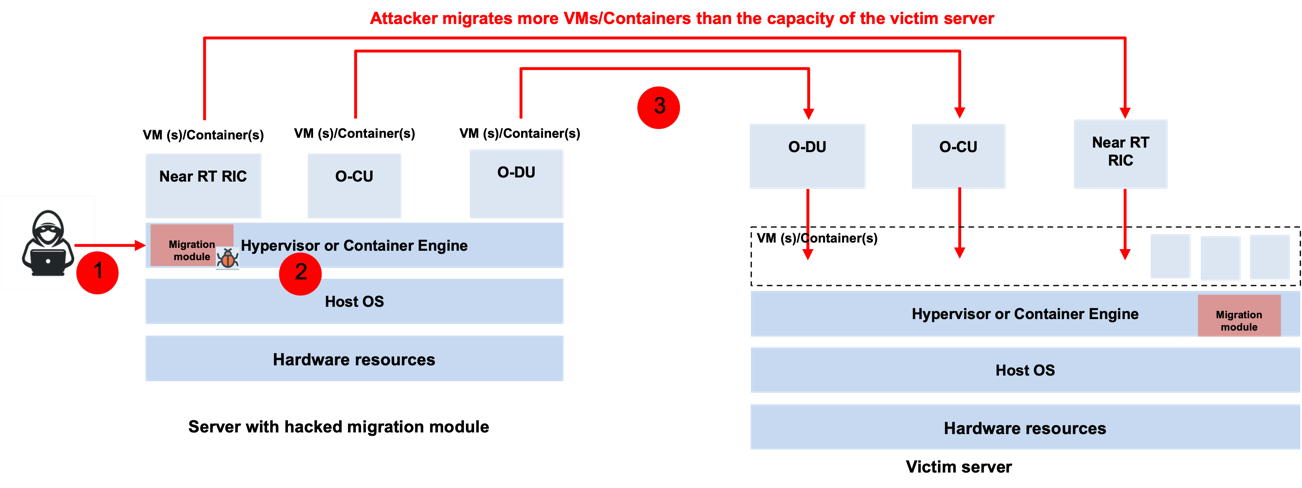


Figure 7‑7 : Illustration of the migration flooding attack

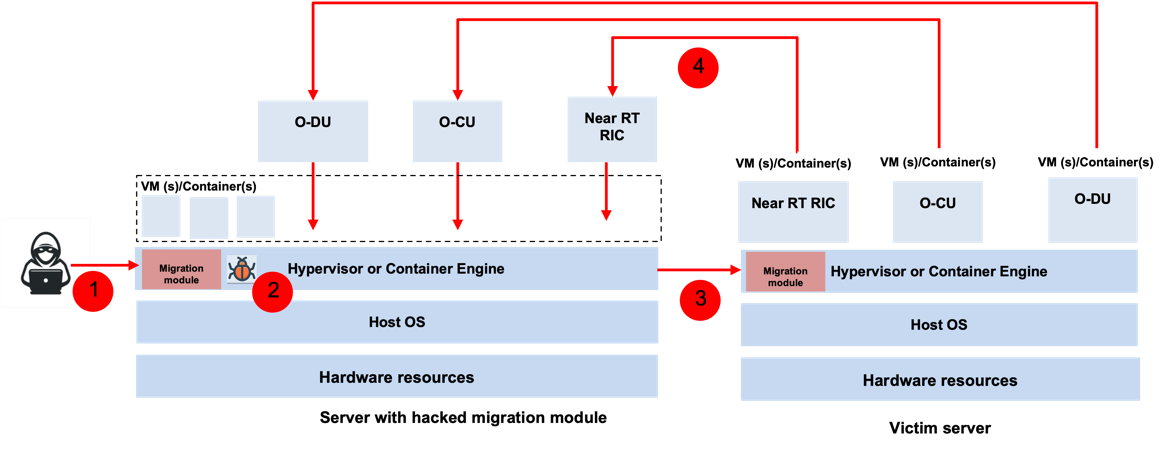


Figure 7‑8 : Illustration of the false resource advertising attack

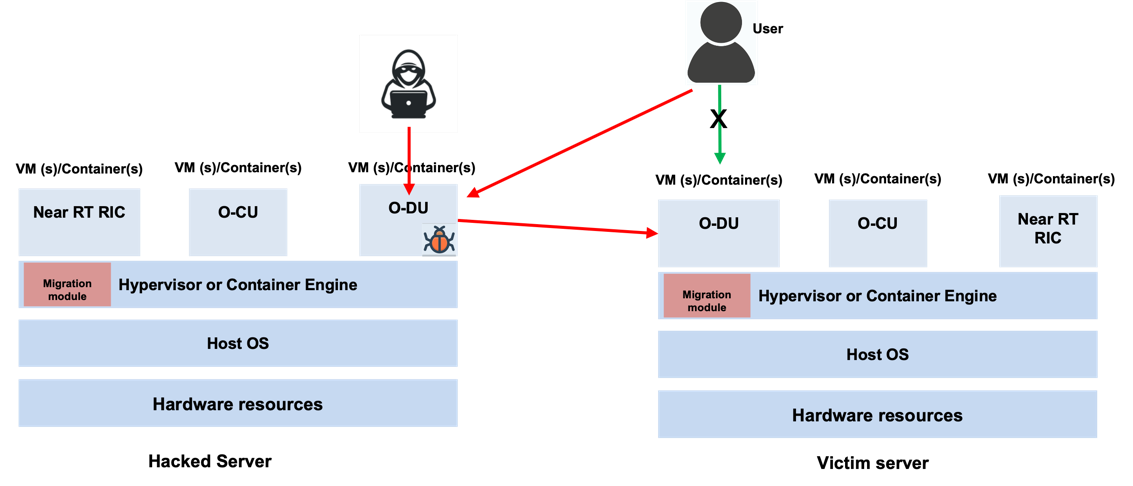


Figure 7‑9 : Illustration of the migration MITM attack

|  |  |
| --- | --- |
| **Threat ID** | T-VM-C-05 |
| **Threat title** | Changing virtualization resource without authorization |
| **Threat description** | IMS/DMS which manage the Virtualization layer is responsible for assigning virtualized resource as requested.  There are several ways to cause a DoS attack for the VNFs/CNFs:   * If IMS/DMS are compromised or the O2 interface is not securely protected, an attacker who compromised the IMS/DMS or breached the O2 interface can change the virtualized resource used by a VNF/CNF by manipulating the allocation of virtualized resource. For example, when an instantiated VNF/CNF is running, adversaries having access to a compromised IMS/DMS or adversaries breaching the insecure O2 interface can misguide the Virtualization layer to reduce the resource of or delete a VM/Container on which a VNF/CNF is running. This can result in the reliability, availability or even illegal termination of a VNF/CNF and hence the denial of service. * Hardware resource configuration and state information (e.g. events) exchange is performed through O2 interface. If the IMS is compromised or the O2 interface is not securely protected, an attacker who compromised the IMS or breached the O2 interface can tamper the hardware configuration and state information so that the virtualized resource supported by the hardware layer becomes unreliable. For example, adversaries having access to a compromised IMS or adversaries breaching the insecure O2 interface can misguide the O-Cloud platform to detach a hardware accelerator from a VNF/CNF. * Adversaries having access to a compromised virtualization layer can change the virtualization resource used by the instantiated VNF/CNF without authorization, * A malicious VM/Container deployed for one instance of a VNF/CNF on a host can illegally occupy the resources of the instantiated VNF/CNF deployed on the same host, resulting in resource limitation of the instantiated VNF/CNF   In this type of attacks, the extra allocation of resources for the malicious VM/Container comes at the expense of the other VMs/Containers that share the same server as the malicious VM/Container, where these victim VMs/Containers get allocated less share of resources than what they should actually obtain, which in turn degrades their performance. |

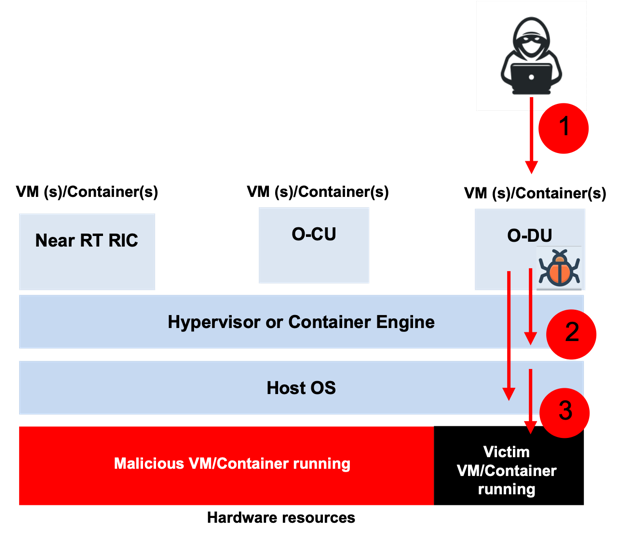


Figure 7‑10 : Illustration of the Theft-of-Service/DoS Attack

|  |  |
| --- | --- |
| **Threat ID** | T-VM-C-06 |
| **Threat title** | Failed or incomplete VNF/CNF termination or releasing of resources |
| **Threat description** | A malicious VNF/CNF is instantiated in the O-Cloud infrastructure to access to data not erased from a terminated VNF/CNF or any VNF/CNF that has released resources. Data could include application data, cryptographic keys...  Abuse of resources allocation in the O-Cloud infrastructure to allocate to a malicious VNF/CNF the virtual resources released from a terminated VNF/CNF or from a VNF/CNF that has released resources after a move or a scaling process.  Inclusion of concealed software in the O-Cloud infrastructure to prevent the deletion/erasure of data and states of the VNF/CNF that has been terminated. |

#### Threats concerning VM/Container images

|  |  |
| --- | --- |
| **Threat ID** | T-IMG-01 |
| **Threat title** | VM/Container images tampering |
| **Threat description** | An attacker can inject malicious code or tamper the information inside the unprotected image during on boarding. Then after the instantiation of the VNF/CNF, the tampered code can cause DoS, information stealing, frauds and so on. There are several attacks categories belonging to this threat. Such attacks include:   * Build machine attacks: If an attacker can modify or influence the way a VM/Container image is built, they could insert malicious code that will subsequently get run in the production environment. * Supply chain attacks: Once the VM/Container image is built, it gets stored in a registry, and it gets retrieved or “pulled” from the registry at the point where it’s going to be run. An attacker who can replace an image or modify an image between build and deployment could run arbitrary code on your deployment. |

|  |  |
| --- | --- |
| **Threat ID** | T-IMG-02 |
| **Threat title** | Insecure channels with images repository |
| **Threat description** | Images often contain sensitive components like an organization’s proprietary software, and embedded secrets and administrator credentials. If connections to registries are performed over insecure channels, man-in-the-middle attacks could intercept network traffic and therefore the contents integrity and confidentiality of images may be compromised. There is also an increased risk of man-in-the-middle attacks that could intercept network traffic intended for registries and steal developer or administrator credentials within that traffic. Thus, could be used to provide fraudulent or outdated images to orchestrators, etc. |

|  |  |
| --- | --- |
| **Threat ID** | T-IMG-03 |
| **Threat title** | Secrets disclosure in VM/Container images |
| **Threat description** | There are scenarios which benefit from including configuration and secrets, such as passwords or credentials in VNFs/CNFs images. For e.g. VMs/Containers require to be able to connect to other VMs/Containers within the deployment as well as with external entities. All these connections need to be authenticated and secured. One way of achieving this is to provide the requisite secrets or keys to the VMs/Containers which allow them to authenticate, be authenticated, secure the communication channel and signature. A common but in-secure means of providing secrets to the VMs/Containers is by packaging the secrets or the keys with the image itself. There is the risk that the same can be extracted, read or manipulated before the VM/Container is deployed and the secret used.  With a long supply chain, VM/Container images are vulnerable to outside scrutiny. With VM/Container images containing secrets or keys, this becomes a serious threat vector. Adversaries can extract them by obtaining a copy of the image and they can be potentially shared with third parties for illicit gain.   * Secrets embedded within a VM/Container image can be stolen. * Secrets embedded within a VM/Container image can be modified   Compromised private keys and algorithms used for image signing due to poor key protection/management/design could undermine the security of image signing process. |

|  |  |
| --- | --- |
| **Threat ID** | T-IMG-04 |
| **Threat title** | Build image on VL |
| **Threat description** | Adversaries may build a VM/Container image directly on the VL to bypass defenses that monitor for the retrieval of malicious images from a registry.  Container example: A remote build request may be sent to the Docker API that includes a Dockerfile that pulls a vanilla base image, such as alpine, from a public or local registry and then builds a custom image upon it.  An adversary may take advantage of that build API to build a custom image on the host that includes malware downloaded from their C2 server, and they then may deploy container using that custom image. If the base image is pulled from a public registry, defenses will likely not detect the image as malicious since it’s a vanilla image. If the base image already resides in a local registry, the pull may be considered even less suspicious since the image is already in the environment. |

#### Threats concerning the virtualization layer (Host OS-Hypervisor/Container engine)

|  |  |
| --- | --- |
| **Threat ID** | T-VL-01 |
| **Threat title** | VM/Container hyperjacking attack |
| **Threat description** | VMs/Containers run on host machines, and it is needed to ensure that those hosts (Hypervisor/Container Engine/Host OS- are not running vulnerable code (for example, old versions of components with known vulnerabilities).  Hyperjacking is an attack in which adversaries gain control over the host of a server or install a malicious Hypervisor/Container Engine/Host OS and exploit that to run malicious applications on the VM/Container that run on top of the host. This would enable the attacker to control all the VMs/Containers running on the host.  Hyperjacking involves installing a malicious, fake the Hypervisor/Container Engine/Host OS that can manage the entire server system. If the attacker gains access to the Hypervisor/Container Engine/Host OS, everything that is connected to that server can be manipulated. The Hypervisor/Container Engine/Host OS represents a single point of failure when it comes to the security and protection of sensitive information.  For a hyperjacking attack to succeed, an attacker would have to take control of the Hypervisor/Container Engine/Host OS by the following methods:   * Injecting a rogue Hypervisor/Container Engine or Host OS beneath the original hypervisor or on top of an existing Hypervisor/Container Engine/Host OS * Directly obtaining control of the original Hypervisor/Container Engine or Host OS * Running a rogue hypervisor on top of an existing hypervisor |



Figure 7‑11 : Illustration of the VM/Container hyperjacking attack

|  |  |
| --- | --- |
| **Threat ID** | T-VL-02 |
| **Threat title** | Boot tampering |
| **Threat description** | The bootloader of the virtualization layer (Host OS, Hypervisor, Container Engine) for VNF/CNF may be maliciously tampered by an attacker, e.g. the attacker compromises hypervisor or host OS to tamper the bootloader of guest OS (in case of VM) or Container.  In a O-Cloud environment any failure during the boot sequence can result in a number of situations that need to be handled by the NFO/FOCOM:  • failure of the physical machine to start at all  • physical machine entering a safe-mode  • physical machine continuing boot regardless of the integrity measurements |

|  |  |
| --- | --- |
| **Threat ID** | T-VL-03 |
| **Threat title** | Attack internal network services |
| **Threat description** | In addition to attacking the network between containers, adversaries can also attack supporting services such as DNS service, which is only reachable from within the cluster network. The highly distributed nature of containers requires shared services for example for coordination and service discovery. An attacker can target these services to degrade services. For example, a denial-of-service against the service discovery infrastructure could prevent O-Cloud to react to changing resource requirements properly. Thus, O-Cloud may no longer be able to scale appropriately to sudden demand spikes [16]. |

#### Threats concerning O-Cloud interfaces

##### O2 interface

Two main interfaces are defined in O-RAN WG6 specification and identified as critical assets of O-Cloud, i.e. interfaces O2 between O-Cloud and SMO. The threats on these interfaces are as follows.

|  |  |
| --- | --- |
| **Threat ID** | T-O2-01 |
| **Threat title** | MitM attacks on O2 interface between O-Cloud and SMO |
| **Threat description** | If the interface O2 interface is not protected, an attacker can attack all the requests/responses sent between the O-Cloud and the SMO (FOCOM and NFO).  For example, the attacker can tamper/alter/disclose requests and services (See ‘Critical services’ in 2.3) sent over O2 between O-Cloud and SMO, hence the virtualized resource or relevant status information is not as requested. This affects the normal operation of the O-Cloud, and even causes DoS attacks, information leakage.  An attacker can tamper the specific assignment of virtualized resources to cause resource assignment errors or an attacker can intercept virtualized resources state information leading to information disclosure.  An attacker can compromise IMS to tamper with the hardware state information (e.g. deleting hardware alarm information) to affect the hardware's operation or to result in information disclosure (e.g. an attacker can get the hardware configuration from the compromised IMS. Then, the attacker can attack the hardware according to the configuration such as CPU type, memory size etc.). An attacker can also tamper or intercept the hardware resource configuration and state information if the configuration and state information are transmitted using an insecure protocol on the O2 interface. |

##### O-Cloud API

|  |  |
| --- | --- |
| **Threat ID** | T-OCAPI-01 |
| **Threat title** | MitM attacks on O-Cloud interface between VNFs/CNFs and the virtualization layer |
| **Threat description** | An attacker can attack an instantiated VNF/CNF through a compromised virtualization layer. For example, cryptographic keys or other security critical data of an instantiated VNF/CNF could be stolen by an attacker with access to the virtualization layer, or the virtualized resource provided by the Virtualization layer to the instantiated VNF/CNF can be manipulated or the bootloader of Guest OS (in case of VM) or Container of an instantiated VNF/CNF can be tampered by an attacker via a compromised virtualization layer. |

#### Threats concerning hardware resources

|  |  |
| --- | --- |
| **Threat ID** | T-HW-01 |
| **Threat title** | Cross VM/Container side channel attacks |
| **Threat description** | In a typical cross-VM/Container side channel attack scenario, an adversary places a malicious VM/Container co-resident to the target VM/Container so that they share the same hardware resources. Then, the attacker extracts useful information such as cryptographic keys from the target VM/Container to use them for traffic eavesdropping and man-in-the-middle attacks. Through the side channel attack, an attacker sharing the same cache as the victim can monitor the cache access behavior of the victim. For example, the attacker is able to monitor cache timing information by measuring the execution of different operations on the victim’s VM/Container. Generally, the attacker exploits timings in the shared high-level cache memory. However, power consumption or electromagnetic leaks can also be used as a vector to launch side channel attacks.  In the virtual environment, prior to the cross-VM/Container side channel attack, the attacker needs to identify the target VM/Container’s location and place a malicious VM/Container co-resident with the target. Later, that attacker may use the maliciously placed VM/Container to extract information from the target VM/Container with the side channel attack.  Hardware vulnerabilities in processors can also have a large impact on O-Cloud security. Flaws in chip design can result in the compromise of tenant information in the cloud through side-channel attacks [24]. |

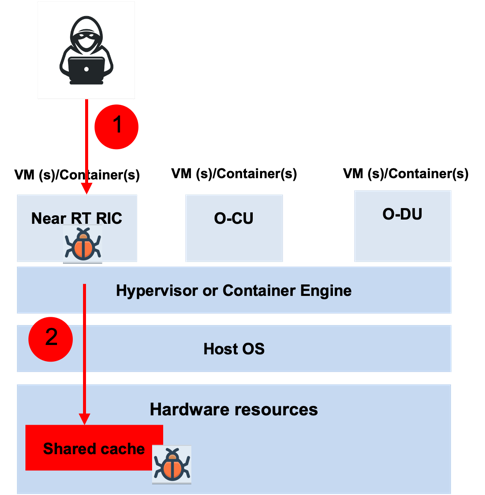


Figure 7‑12 : Illustration of a cross VM/Container side channel attack

|  |  |
| --- | --- |
| **Threat ID** | T-HW-02 |
| **Threat title** | MitM attacks on the interface between virtualization layer and hardware |
| **Threat description** | An attacker can utilize the vulnerabilities of hardware (e.g. Meltdown and Specter of CPU in host) to attack virtualization layer and/or VNFs/CNFs through this interface, resulting in tampering, information disclosure or DoS. |

#### Threats concerning O-Cloud management (SMO, NFO, FOCOM)

|  |  |
| --- | --- |
| **Threat ID** | T-ADMIN-01 |
| **Threat title** | Denial of service against NFO/FOCOM |
| **Threat description** | A denial-of-service attack against the NFO/FOCOM can interfere with the ability of operators to control and maintain their deployments. This can lead to the inability to react to changing resource requirements. In addition, the NFO/FOCOM is the external API to interact with the O-Cloud platform. Thus, other services may become inaccessible as well. For example, operators may be unable to retrieve logs, telemetry data. An attacker could use this opportunity to hide additional attacks on VM/Container instances.  In addition, an attacker on the NFO/FOCOM could prevents the O-Cloud software update (VNFs/CNFs, VL) to exploit a known security flaw in the O-Cloud software. |

|  |  |
| --- | --- |
| **Threat ID** | T-ADMIN-02 |
| **Threat title** | Abuse a O-Cloud administration service |
| **Threat description** | Usually, the SMO including NFO/FOCOM is exposed to the tenant in a web front-end or REST API. In case these interfaces contain software vulnerabilities or implement authentication and authorization insufficiently, an adversary would be able to gain access to the VM/Container management and pose as a tenant. It is also possible that an adversary gains the ability to submit requests without prior authentication and authorization.  The NFO/FOCOM interfaces encompasses a great deal of privileges because anyone gaining sufficient access is able to deploy new instances and disrupt existing O-Cloud services. It may also be possible for an adversary to submit compromised VM/Container images that unsuspecting tenants then use to initiate O-Cloud services. Moreover, adversaries can use the same access to extract business data, configuration data, user data and possibly credentials. For example, they may be able to create backups of VM/Container instances or they can export VM/Container images. The impact of compromised credentials is exacerbated by the fact that weak and insufficient safeguarding of credentials is recognized as one of the top threats in cloud computing [38].  Container example: Adversaries may abuse a container administration service to execute commands within a container. A container administration service such as the Docker daemon, the Kubernetes API server, or the kubelet may allow remote management of containers within an environment.  Container example: In Docker, adversaries may specify an entrypoint during container deployment that executes a script or command, or they may use a command such as *docker exec* to execute a command within a running container. In Kubernetes, if an adversary has sufficient permissions, they may gain remote execution in a container in the cluster via interaction with the Kubernetes API server, the kubelet, or by running a command such as *kubectl exec*. |

#### Threats concerning Acceleration Abstraction Layer (AAL)

|  |  |
| --- | --- |
| **Threat ID** | T-AAL-01 |
| **Threat title** | Attacker exploits insecure API to gain access to hardware accelerator resources |
| **Threat description** | Insecure AAL API allows an attacker to tamper the requests/responses sent between the AAL components, the O-Cloud platform and O-RAN APPs/VNFs/CNFs.  For example, the attacker can tamper requests and services sent over AALI-C-Mgnt between IMS and the hardware accelerator manager, hence capability of the hardware accelerator device, fault information, logs, performance information and others are not as requested. This affects the normal operation of the O-Cloud, and even causes tampering.  An attacker can tamper application (e.g. O-DU) requests sent over AALI-C-App to an AAL implementation for allocation of buffers. This affects the normal operation of the applications, and even causes tampering.  An attacker can tamper application (e.g. O-DU) requests sent over AALI-P for configuring and managing the AAL-LPU(s). This affects the normal operation of the applications, and even causes tampering. |

|  |  |
| --- | --- |
| **Threat ID** | T-AAL-02 |
| **Threat title** | Internal Overload DoS attack targeting AAL services |
| **Threat description** | Overload situation could appear in the case of DoS attack or increased traffic on AAL interfaces. Inability to mitigate traffic volumetric attacks on AAL affects availability of AAL data and services.  DoS attacks on the AALI-C interface affect the different services provided by the hardware accelerator manager and the transport abstraction framework.  DoS attacks on the AALI-P interface affect the configuration and management of AAL-LPU (Acceleration Abstraction Layer Logical Processing Unit) by an application (e.g. O-DU) in addition to acceleration functionality. |

|  |  |
| --- | --- |
| **Threat ID** | T-AAL-03 |
| **Threat title** | Fail to clear resources |
| **Threat description** | Fail to clear accelerator resources after a process termination. This causes an information leakage and incorrect results for computations. Further, failure to release accelerator resources may prevent other processes from running.  This threat is relevant to accelerator resources either inside the hardware accelerator device (internal memories, registers, cache) or in the O-Cloud memories used by accelerators. |

|  |  |
| --- | --- |
| **Threat ID** | T-AAL-04 |
| **Threat title** | HAM compromise |
| **Threat description** | A malicious actor can gain access to HAM to gain unauthorized access and control of the hardware accelerator device. This can result in the disruption of services (DoS) and tampering of accelerator components, such as firmware, drivers which can cause the accelerator to behave abnormally or crash altogether. |

|  |  |
| --- | --- |
| **Threat ID** | T-AAL-05 |
| **Threat title** | Malicious memory accesses |
| **Threat description** | AAL that allows one process running on the hardware accelerator device to access memory owned by another process running on the hardware accelerator device can leak information (impact on confidentiality).  Similarly, AAL allowing concurrently executing processes to write to one another’s memory may have correctness errors (impact on integrity).  If multiple processes are running concurrently and one is allowed to dominate accelerator resources, the other may suffer from degraded performance. For example, if one process can evict all cache entries belonging to the other, the victim will suffer performance penalties (impact on availability). |

|  |  |
| --- | --- |
| **Threat ID** | T-AAL-06 |
| **Threat title** | Firmware attacks |
| **Threat description** | Hardware accelerators often have their own firmware, which can be targeted by attackers. This could include modifying the firmware to introduce vulnerabilities (e.g., malware) or installing a malicious firmware to extract/modify sensitive information or execute unauthorized actions (e.g., control the device remotely). |

#### Threats concerning O-Cloud instance ID

|  |  |
| --- | --- |
| **Threat ID** | T-O-CLOUD-ID-01 |
| **Threat title** | ID reuse in O-Cloud's object lifecycle |
| **Threat description** | In O-Cloud, objects such as Containers, Pods, Nodes, and Services are identified by their IDs within a given compute pool (e.g., cluster in Kubernetes). When an object is deleted, its ID becomes available for reuse. This means that a new object can be created with the same ID as a previously deleted object. If an object gets deleted but all its associated data isn't properly isolated or cleaned, the ID, if reused, could lead to unintended data associations or leaks.  Potential consequences:   * Data Residue: A new object, reusing an ID, may inherit residual data or configurations from its predecessor, leading to potential misconfigurations and incorrect data associations. This can result in sensitive data exposure. * Data Overwrite: Automated processes unaware of the deletion and subsequent recreation might mistakenly write or read data from the new object, thinking it's the old one. * Monitoring Ambiguities: Monitoring tools might combine metrics from the old and new objects, resulting in confusing data. * Operational Disruptions: The new object might operate based on the residual configurations of the old object, potentially leading to system inefficiencies or failures. |

|  |  |
| --- | --- |
| **Threat ID** | T-O-CLOUD-ID-02 |
| **Threat title** | Node redundancy in O-Cloud deployments |
| **Threat description** | Nodes in O-Cloud often represent physical or virtual machines. If a machine fails and is replaced without deleting its corresponding Node object, and the new machine is given the same ID or the hostname, O-Cloud might treat the new machine as if it were the original.  Potential consequences:   * Resource Mismatch: The new host might have different resources (CPU, memory, storage) than the old one, leading to scheduling issues or resource constraints. * Stale Data: The new node might inherit data or configurations from the old node, leading to potential security or operational risks. * Network Issues: Network configurations or IP address assignments might be inconsistent or conflicting. |

|  |  |
| --- | --- |
| **Threat ID** | T-O-CLOUD-ID-03 |
| **Threat title** | O-Cloud ID mismanagement |
| **Threat description** | IDs are crucial for uniquely identifying objects within the O-Cloud. Mismanagement occurs when these IDs are not properly assigned, tracked, or validated, leading to potential overlaps or inconsistencies.  Potential consequences:   * ID Collision: Due to system glitches or bugs, two distinct objects could inadvertently be allocated the same ID. Such an occurrence is termed an ID collision. This can result in operations meant for one object inadvertently affecting the other. * Resource Overwrite: If two objects share the same ID, updates or modifications intended for one might overwrite the data of the other, leading to data inconsistencies or loss. * ID-Based Permissions: Many security protocols and access controls in O-Cloud can be tied to object IDs. If an attacker can predict, guess, or manipulate the ID generation process, they might gain unauthorized access to resources. * Log Merging: Monitoring tools and logging systems use IDs to track events and operations related to specific objects. If two objects share an ID, their logs might get merged, making it challenging to trace events back to their source. * RBAC Anomalies: Role-Based Access Control (RBAC) regulations attached to specific object IDs could unintentionally approve or restrict access to the novel object due to misidentification. |

### Threats to open source code

Open source introduces the following threats:

|  |  |
| --- | --- |
| Threat ID | T-OPENSRC-01 |
| **Threat title** | Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack |
| **Threat description** | The O-RAN Software Community is a Linux Foundation project, supported and funded by O-RAN to lead the implementation of the O-RAN specifications in Open Source. Industry has recognized that Open Source code introduces security risks. Open Source vulnerabilities are publicly available on the National Vulnerability Database (NVD). While this is intended for developers to disclose vulnerabilities, it is also used by hackers to exploit those vulnerabilities. Vulnerabilities frequently propagate as developers re-use free open source code enabling backdoors to attacks. There have been notable vulnerabilities from downloading open source libraries and dependencies, as well as supply chain risks when downloading Open Source code from untrusted repositories.  Some O-RAN vendors and operators may not have accurate inventories of open-source software dependencies used by their different applications, or a process to receive and manage notifications concerning discovered vulnerabilities or available patches from the community supporting the open-source.  Some O-RAN vendors may not have a lack of consistent Supply Chain traceability and security, and a lack of coding best practices conflicts with Security-by-Design principles.  Developers may use modules with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack.  Attackers can exploit a vulnerability on the open source code and infects a hypervisor, operating system, VM or container with a malware. |

|  |  |
| --- | --- |
| Threat ID | T-OPENSRC-02 |
| **Threat title** | A trusted developer intentionally inserts a backdoor into an open source code O-RAN component |
| **Threat description** | A trusted developer intentionally inserts a backdoor by injecting a few lines of malicious code into an open source code component to be used within the O-RAN system. A software project team picks up and uses the infected open source code and the development team’s tools for vetting and testing the component do not detect the malicious code. Unknowingly they have introduced a vulnerability into their O-RAN software code.  The vulnerability has gone undetected and the threat actor is able to compromise the software through the inserted vulnerability. The resulting effect on the O-RAN system can take a variety of forms, from being annoying to impacting system performance (DoS) to the loss of sensitive data. |

### Physical Threats

|  |  |
| --- | --- |
| Threat ID | T-PHYS-01 |
| **Threat title** | An intruder into a site gains physical access to O-RAN components to cause damage or access sensitive data |
| **Threat description** | Physical attacks on the O-RAN deployment that stores or processes keys, user plane data, control plane data and management data in cleartext.  O-RAN physical components might be vulnerable if:   * Improper physical security protection of data centers, PNFs, operation areas, etc. * Improper protection to power outages (power supply) * Improper protection against environmental disasters * Improper maintenance and monitoring of hardware parameters * Hardware backdoor   Attackers try to modify the O-RAN components settings and configurations via local access.  Physical access to O-RAN components thanks to unsecured management ports and consoles (such as JTAG, serial consoles or dedicated management ports), relaxed administrator credentials management, unsecured HW and SW configuration/management could allow an attacker to inject malwares and/or manipulate existing software, steal unprotected private keys, certificates, hash values, disable security features, create a performance issue by manipulation of parameters with the purpose of eavesdropping or wiretapping on various CUS & M planes, reaching the network beyond the O-RAN or with the purpose of gaining access to the O-RAN components, denial of service, intrusion and replay attacks or other type of breaches. |

|  |  |
| --- | --- |
| Threat ID | T-PHYS-02 |
| **Threat title** | An intruder into the exchange over the Fronthaul cable network attempts to gain electronic access to cause damage or access sensitive data |
| **Threat description** | O-RU and O-DU may be located at different premises and connected through a cable network to support the fronthaul link. Attackers can gain access to, or control over, data traffic through breaching terminals in the cable landing sites (O-RU or O-DU). |

### Threats against 5G radio networks

Threats against 5G radio networks include:

|  |  |
| --- | --- |
| Threat ID | T-RADIO-01 |
| **Threat title** | Disruption through radio Jamming, Sniffing and Spoofing |
| **Threat description** | Like for any wireless technology, disruption through radio jamming is possible by analyzing the physical downlink and uplink control channels and signals. 5G radio network is vulnerable to:   * Jamming Vulnerability of Reference Signals * Jamming Vulnerability of Synchronization Signal * Jamming Vulnerability of the PBCH * Sniffing and Spoofing Vulnerability of the PBCH * Jamming Vulnerability of PDCCH * Jamming Vulnerability of Physical Uplink Control Channel * Jamming Vulnerability of Physical Random-Access Channel   **NOTE 1**: The O-RAN OEMs need to develop new intelligence that can proactively alert the operator when this attack is initiated so that the operator can take appropriate actions to mitigate.  **NOTE 2**: In the scenario of RF spoofing, the UE needs to be able to validate the legitimacy of the O-RU as being one owned and operated by the operator. 3GPP has proposed in a study to use Digital Signatures to mitigate this threat but there has been no agreement on this to date. The O-RAN OEMs need to develop new intelligence that can proactively alert the operator when this attack is initiated so that the operator can take appropriate actions to mitigate. |

|  |  |
| --- | --- |
| Threat ID | T-RADIO-02 |
| **Threat title** | DoS attacks on cognitive radio networks [17] |
| **Threat description** | Cognitive radio (CR) technology, which is designed to enhance spectrum utilization, depends on the success of opportunistic access, where unlicensed secondary users (SUs) exploit spectrum void unoccupied by primary users (PUs) for transmissions. To realize DoS attacks, malicious users (MUs) target the critical functionalities for CR ecosystems, including spectrum sensing, agile radio, and light-handed regulation since once these functionalities fail, SUs are not able to communicate effectively. For example, MUs can directly jam the victim by injecting interference or deceive SUs into believing that there is a PU by emulating the signal characteristics of the PU, thereby evacuating the occupied spectrum. Moreover, the liability rule is vulnerable to the selfish and greedy users aiming to maximize their own private benefits. Since complying with the rule results in less transmission opportunities, such SUs may not want to invest efforts to follow the rule and thus will transmit simultaneously with Pus. |

### Threats against ML system

This section provides the relevant threats against the ML system implemented in O-RAN architecture. The threats listed here below are generic to cover the ML model and not refined at ML components (training and inference hosts) due to the various deployment scenarios that are considered for ML architecture/framework in O-RAN. For the purposes of this document, the deployment scenarios are:

1. Scenario 1.1: SMO/Non-RT RIC acts as both the ML training and inference host.
2. Scenario 1.2: Non-RT RIC acts as the ML training host and the Near-RT RIC as the ML inference host
3. Scenario 1.3: Non-RT RIC acts as the ML training host and the O-CU/O-DU as the ML inference host

The involved components and interfaces within each scenario are:

* Scenario 1.1: SMO/Non-RT RIC, Near-RT RIC, O-CU, O-DU, O-RU, SMO internal/O1/A1 interfaces
* Scenario 1.2: SMO/Non-RT RIC, Near-RT RIC, O-CU, O-DU, O-RU, O1/O2/A1/E2 interfaces
* Scenario 1.3: SMO/Non-RT RIC, O-CU, O-DU, O-RU, O1/O2 interfaces

|  |  |
| --- | --- |
| Threat ID | T-ML-01 |
| **Threat title** | Poisoning the ML training data (Data poisoning attacks) |
| **Threat description** | An attacker gains access to the training set of a machine learning model and alters the data (e.g. datasets that are assembled to train, test, and validate an ML system) before the training begins without the knowledge of the machine learning engineers. The training data will already be tampered with and has lost its original quality which will result in modeling on wrong data. Hence, the ML model will no longer be a reliable one since it was trained on bad data and therefore modelling, decisions, predictions, model classifications, detections, etc. will surely not be appropriate.  Also, another scenario can be in a situation where a model is online and continues to learn during operational use, modifying its behavior over time. In this case, an attacker can feed the model with bad data and the model can learn from this bad data, and as a result, negatively impact its performance and retrain the ML system to do the wrong thing. |

|  |  |
| --- | --- |
| Threat ID | T-ML-02 |
| **Threat title** | Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy) |
| **Threat description** | An attacker can illegally access a machine learning model and alter its parameters and thereby influence how it produces results. This can lead to wrong prediction and might result in catastrophic decisions if the results of the predictions were being used to make key business decisions.  Also, an attacker can extract sensitive or confidential data that, through training, are built right into the ML model. |

|  |  |
| --- | --- |
| Threat ID | T-ML-03 |
| **Threat title** | Transfer learning attack |
| **Threat description on** | A transfer learning attack is a risk when an ML system is built by fine-tuning a pretrained model that is widely available. An attacker could use the public model as a cover for their malicious ML behavior. |

For more information about ML security risks and controls, see the risk analysis of ML systems released by BIML [18].

### Protocol Stack Threats

The A1 and R1 interfaces use the REST protocol stack shown in the figure below. The transport network layer is built on IP transport. TCP provides the communication service at the transport layer. HTTP is the application-level protocol used providing reliable transport of messages. TLS provides secure HTTP connections for secure transport of messages. The application layer protocol is based on a RESTful approach with transfer of JSON formatted policy statements. Each of these protocols has known vulnerabilities that can be exploited by a malicious actor.

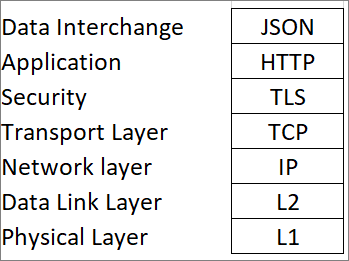


Figure. REST Protocol Stack for the A1 and R1 Interfaces

**Figure 7‑13 : REST Protocol Stack for the A1 and R1 Interfaces**

|  |  |
| --- | --- |
| Threat ID | T-ProtocolStack-01 |
| **Threat title** | REST API Exploits |
| **Threat description** | REST API common attacks include injection, cross site scripting, and DoS attacks that can exploit common vulnerabilities if proper controls are not used to protect against vulnerabilities. |

|  |  |
| --- | --- |
| Threat ID | T-ProtocolStack-02 |
| **Threat title** | REST API – Broken Object Level Authorization |
| **Threat description** | The REST API can be exploited to expose object identifiers without proper authorization checks. |

|  |  |
| --- | --- |
| Threat ID | T-ProtocolStack-03 |
| **Threat title** | JSON Exploits |
| **Threat description** | JSON attacks include injection, deserialization, web token, and cross site scripting attacks that can exploit common vulnerabilities if proper controls are not used to protect against vulnerabilities. |

|  |  |
| --- | --- |
| Threat ID | T-ProtocolStack-04 |
| **Threat title** | HTTP Exploits |
| **Threat description** | DDoS attacks include HTTP GET Flood, Garbage Flood, and Reverse Bandwidth Floods. Other well known HTTP attacks include injection attacks, such as Cross-Site Scripting (XSS) and SQL injection. |

|  |  |
| --- | --- |
| Threat ID | T-ProtocolStack-05 |
| **Threat title** | TCP Volumetric DDoS |
| **Threat description** | TCP DDoS attacks include TCP SYN Flood, ACK Flood, and RST Flood. |

### SMO Threats

#### General SMO Threats

|  |  |
| --- | --- |
| Threat ID | T-SMO-01 |
| **Threat title** | External attacker exploits authentication weakness on SMO |
| **Threat description** | An external attacker can exploit the improper/missing authentication weakness on SMO functions. If the authentication of O-RAN subjects on A1, O1, O2, and External interfaces on SMO is not supported or not properly implemented, those interfaces without proper credentials could be exploited to gain access to the SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-02 |
| **Threat title** | External attacker exploits authorization weakness on SMO |
| **Threat description** | An external attacker can exploit the improper/missing authorization weakness on SMO functions. A malicious external entity on A1, O1, O2, and External interfaces without authorization or with an incorrect access token may invoke the SMO functions. The data at rest related to that function will be leaked to the attacker. In addition, an attacker can be able to perform certain actions, e.g. disclose O-RAN sensitive information or alter O-RAN components. |
| **Threat type** | Elevation of Privilege, Information Disclosure |
| **Impact type** | Authorization. Confidentiality |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-03 |
| **Threat title** | External Overload DoS attack targeted at SMO |
| **Threat description** | Overload situation could appear in the case of DoS attack or increased traffic on externally facing interfaces. Inability to mitigate traffic volumetric attacks on an external interface affects availability of SMO data and functions. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-04 |
| **Threat title** | Internal attacker exploits authentication weakness on a SMO function |
| **Threat description** | An internal attacker can exploit the improper/missing authentication weakness on SMO functions. If the authentication of internal interfaces (e.g. Internal Message Bus and R1) on SMO is not supported or not properly implemented, those interfaces without credentials could exploited to gain access to the SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-05 |
| **Threat title** | Internal attacker exploits authorization weakness on a SMO function |
| **Threat description** | An internal attacker can exploit the improper/missing authorization weakness on SMO functions. Malicious internal entities without authorization or with an incorrect access token may invoke the SMO functions. The data at rest related to these functions will be leaked to the attacker. In addition, an attacker can be able to perform certain actions, e.g. disclose O-RAN sensitive information or alter O-RAN components. |
| **Threat type** | Elevation of Privilege, Information Disclosure |
| **Impact type** | Authorization |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-06 |
| **Threat title** | Internal Overload DoS attack targeted at SMO functions |
| **Threat description** | Overload situation could appear in the case of DoS attack or increased traffic on internal SMO interfaces. Inability to mitigate traffic volumetric attacks on an external interface affects availability of SMO data and functions. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-07 |
| **Threat title** | Internal DoS attack disables internal SMO function(s) or process(es) |
| **Threat description** | Internal malicious actor exploits a vulnerability or escalates privilege to execute a DoS attack by disabling one or more SMO processes or functions. Inability to detect and report such events affects availability of SMO functions. |
| **Threat type** | Denial of Service, Escalation of Privilege |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-08 |
| **Threat title** | Attacker exploits insecure API to gain access to SMO |
| **Threat description** | An insecure API may allow access to a system for an attacker to conduct remote code execution or an advanced persistent threat |
| **Threat type** | Tampering, Information Disclosure, Escalation of Privilege |
| **Impact type** | Integrity, Confidentiality, Authorization |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-09 |
| **Threat title** | Sensitive data in transit is exposed to an internal attacker |
| **Threat description** | Unprotected data transferred between internal SMO functions is disclosed to an internal threat actor |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-10 |
| **Threat title** | Sensitive data at rest is exposed to an internal attacker |
| **Threat description** | Unprotected data stored on the SMO is disclosed to an internal threat actor that has gain authorized access through privilege escalation |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-11 |
| **Threat title** | AI/ML poisoning by internal attacker |
| **Threat description** | Internal attacker gains authorized access exploited to poison AI/ML training data,or the AI/ML models, stored in the SMO to influence insights. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-12 |
| **Threat title** | AI/ML exposure on external entity |
| **Threat description** | An external attacker can gain access to external entities to view or modify sensitive data AI/ML data, or models, transferred between the external function and SMO via external interfaces(e.g., EI, Human-Machine, A1, O1) |
| **Threat type** | Information disclosure, Tampering |
| **Impact type** | Confidentiality, Integrity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-13 |
| **Threat title** | Malicious actor views local logs |
| **Threat description** | Malicious actor accesses locally stored logs in the SMO to perform reconnaissance to collect sensitive or private information. |
| **Threat type** | Information disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-14 |
| **Threat title** | Malicious actor modifies local log entries |
| **Threat description** | Malicious actor accesses locally stored logs in the SMO to modify entries to hide presence or cause confusion. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-15 |
| **Threat title** | Malicious actor deletes local log entries |
| **Threat description** | Malicious actor accesses locally stored logs in the SMO to delete entries to hide presence or cause confusion. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-16 |
| **Threat title** | Malicious actor intercepts exports of local logs |
| **Threat description** | Malicious actor gains access to an external interface to intercept data in transit as logs are transferred from the SMO to a remote server/external entity. |
| **Threat type** | Information disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-17 |
| **Threat title** | Malicious external actor gains unauthorized access to logs |
| **Threat description** | Malicious external actor gains unauthorized access to stored logs to view, modify, and delete |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Confidentiality |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-18 |
| **Threat title** | Malicious internal actor gains authorized access to logs |
| **Threat description** | Malicious internal actor gains authorized access to stored logs to view, modify, and delete. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | SMO |

#### SMO Threats at O2 interface

|  |  |
| --- | --- |
| Threat ID | T-SMO-19 |
| **Threat title** | Internal attacker exploits O2 interface to view data in transit between SMO and O-Cloud |
| **Threat description** | If the O2 interface is not properly confidentiality protected, an internal attacker can perform a man-in-the-middle attack to view data in transit. |
| **Threat type** | Information disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | O2 interface |

|  |  |
| --- | --- |
| Threat ID | T-SMO-20 |
| **Threat title** | Internal attacker exploits O2 interface to modify data in transit between SMO and O-Cloud |
| **Threat description** | If the O2 interface is not properly integrity protected, an internal attacker can perform a man-in-the-middle attack to modify data in transit. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | O2 interface |

|  |  |
| --- | --- |
| Threat ID | T-SMO-21 |
| **Threat title** | Internal attacker uses O2 interface via SMO to exploit API vulnerability to gain access to O-Cloud infrastructure |
| **Threat description** | If the O2 interface uses an API with a known vulnerability that is not properly protected or patched, an attacker can exploit it to gain access to the O-Cloud infrastructure from the SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-Cloud |

|  |  |
| --- | --- |
| Threat ID | T-SMO-22 |
| **Threat title** | Internal attacker floods O2 interface via SMO to cause DDoS on O-Cloud infrastructure |
| **Threat description** | If the O2 interface is not protected, an internal attacker on the SMO can flood the O2 interface to overload the O-Cloud. This can prevent legitimate messages from reaching the O-Cloud or cause heavy processing at the O-Cloud, resulting in performance degradation. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | O-Cloud |

|  |  |
| --- | --- |
| Threat ID | T-SMO-23 |
| **Threat title** | External attacker uses O2 interface via O-Cloud to exploit API vulnerability to gain access to SMO |
| **Threat description** | If the O2 interface uses an API with a known vulnerability that is not properly protected or patched, an attacker can exploit it to gain access to the SMO from the O-Cloud infrastructure. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-24 |
| **Threat title** | External attacker floods O2 interface via O-Cloud to cause DDoS on SMO |
| **Threat description** | If the O2 interface is not protected, an external attacker in the O-Cloud can flood the O2 interface to overload the SMO. This can prevent legitimate messages from reaching the SMO or cause heavy processing at the SMO, resulting in performance degradation or outage of the SMO. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-25 |
| **Threat title** | External attacker uses O2 interface via O-Cloud to gain authorized access to sensitive data-at-rest at the SMO |
| **Threat description** | If the SMO is not protected, an external attacker at the O-Cloud can use the O2 interface to gain authorized access to the SMO to view data-at-rest. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | SMO |

#### SMO Threats at External interfaces

|  |  |
| --- | --- |
| Threat ID | T-SMO-26 |
| **Threat title** | External attacker exploits External interface to view data in transit between SMO and external service |
| **Threat description** | If an External interface is not properly confidentiality protected, an external attacker can perform a man-in-the-middle attack to view data in transit. |
| **Threat type** | Information disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | External interface |

|  |  |
| --- | --- |
| Threat ID | T-SMO-27 |
| **Threat title** | External attacker exploits External interface to modify data in transit between SMO and external service |
| **Threat description** | If an External interface is not properly integrity protected, an external attacker can perform a man-in-the-middle attack to modify data in transit. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | External interface |

|  |  |
| --- | --- |
| Threat ID | T-SMO-28 |
| **Threat title** | External attacker uses External interface to exploit API vulnerability to gain access to SMO |
| **Threat description** | If an External interface uses an API with a known vulnerability that is not properly protected or patched, an attacker can exploit it to gain access to the SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-29 |
| **Threat title** | External attacker floods External interface to cause DDoS at SMO |
| **Threat description** | If the External interface is not protected, an external attacker can flood an External interface to overload the SMO. This can prevent legitimate messages and data from reaching the SMO or cause heavy processing at the SMO, resulting in performance degradation or outage of the SMO. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-30 |
| **Threat title** | External attacker uses External interface to gain access to sensitive data-at-rest at the SMO |
| **Threat description** | If the SMO is not protected, an external attacker can use the External interface to gain authorized access to the SMO to view data-at-rest. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-31 |
| **Threat title** | External attacker poisons External AI/ML data to corrupt SMO |
| **Threat description** | External data sources may be outside the control of the stakeholder(s) responsible for the O-RAN deployment. The stakeholder for an External data source could fail to provide proper security controls to protect data consumed by the SMO. If an external attacker were to gain access to AI/ML data, it could be corrupted and then be used at the SMO. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

|  |  |
| --- | --- |
| Threat ID | T-SMO-32 |
| **Threat title** | External attacker poisons External Enrichment Information data sources to corrupt SMO |
| **Threat description** | External data sources may be outside the control of the stakeholder(s) responsible for the O-RAN deployment. The stakeholder for an External data source could fail to provide proper security controls to protect data consumed by the SMO. If an external attacker were to gain access to External Enrichment Information, it could be corrupted and then be used at the SMO. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO |

### Threats against Shared O-RU

Threat Analysis tables are provided for each of the identified Shared O-RU threats in the clauses below. The Shared O-RU Threats are classified into 6 threat groups:

* Lateral Movement Between Network Functions
* Physical Port Access Threats
* Data Access Threats
* Availability Threats
* Configuration Threats
* Resiliency Threats

Use of the term “MNO Tenant” or “Tenant” refers to a “Shared Resource Operator (SRO)” as defined in [27].

#### Lateral Movement Between Network Functions

This clause provides threat analysis tables for threats to access between Shared O-RU network functions.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-01 |
| **Threat title** | O-DU Tenant accesses O-DU Host |
| **Threat description** | The O-DU Tenant accesses the O-DU Host through the Shared O-RU. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Host |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-02 |
| **Threat title** | O-DU Host accesses O-DU Tenant |
| **Threat description** | The O-DU Host accesses the O-DU Tenant through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-03 |
| **Threat title** | O-DU Tenant accesses O-DU Tenant |
| **Threat description** | An O-DU Tenant accesses another O-DU Tenant through the Shared O-RU supporting multiple tenants. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-04 |
| **Threat title** | Password Attack on OFH M-Plane |
| **Threat description** | Use of single-factor authentication with password on the Open Fronthaul M-Plane can be exploited by an internal malicious actor to gain access to the Shared O-RU. The attack can be a brute-force attack or stolen password. There is increased risk of password attack in a multi-tenant environment. The internal malicious actor may be the Host MNO, a Tenant MNO, or a 3rd-party. [9] |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | Shared O-RU, O-DU Host, O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-05 |
| **Threat title** | Untrusted peering to O-DU |
| **Threat description** | Attacker exploits weak authentication on the O-DU to establish a session with a malicious app masquerading as a Shared O-RU. From the O-DU, a malicious actor can move laterally across Shared O-RUs and northbound to the O-CU and SMO. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Host, O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-06 |
| **Threat title** | Untrusted peering to the Shared O-RU |
| **Threat description** | Attacker exploits weak authentication on the Shared O-RU to establish session with a malicious app masquerading as a O-DU Host or O-DU Tenant |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-07 |
| **Threat title** | Untrusted peering to the SMO |
| **Threat description** | Attacker exploits weak authentication on the SMO to establish session with a malicious app masquerading as a Shared O-RU. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-08 |
| **Threat title** | SMO Tenant accesses SMO Host |
| **Threat description** | The SMO Tenant accesses the SMO Host through the Shared O-RU. Weak authentication can be exploited by a tenant to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO Host |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-09 |
| **Threat title** | SMO Host accesses SMO Tenant |
| **Threat description** | The SMO Host accesses the SMO Tenant through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-10 |
| **Threat title** | O-DU Host accesses O-CU Tenant |
| **Threat description** | The O-DU Host accesses the O-CU Tenant through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-11 |
| **Threat title** | O-DU Tenant accesses O-CU Host |
| **Threat description** | The O-DU Tenant accesses the O-CU Host through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Host |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-12 |
| **Threat title** | O-DU Tenant accesses O-CU Tenant |
| **Threat description** | The O-DU Tenant accesses another O-CU Tenant through the Shared O-RU supporting multiple tenants. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-13 |
| **Threat title** | SMO Host accesses O-CU Tenant |
| **Threat description** | The SMO Host accesses the O-CU Tenant through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-14 |
| **Threat title** | SMO Tenant accesses O-CU Host |
| **Threat description** | The SMO Tenant accesses the O-CU Host through the Shared O-RU. Weak authentication can be exploited by a host to move laterally across the deployment. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Host |

#### Physical Port Access Threats

This clause provides threat analysis tables for physical port access threats to Shared O-RU.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-15 |
| **Threat title** | Physical port access to Shared O-RU Host/Tenant |
| **Threat description** | A host, tenant, or third-party gains physical port connectivity to the Shared O-RU. With this physical access the actor exploits weak physical layer authentication to gain access to the Shared O-RU. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-16 |
| **Threat title** | Physical port access to O-DU Host/Tenant |
| **Threat description** | A host, tenant, or third-party gains physical port connectivity to a O-DU Host or O-DU Tenant. With this physical access the actor exploits weak physical layer authentication to gain access to the O-DU. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Host, O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-17 |
| **Threat title** | Physical port access to O-CU Host/Tenant |
| **Threat description** | A host, tenant, or third-party gains physical port connectivity to a O-CU Host or O-CU Tenant. With this physical access the actor exploits weak physical layer authentication to gain access to the O-CU. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Host, O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-18 |
| **Threat title** | Malicious User Login Attempt to SMO Host/Tenant |
| **Threat description** | The attacker attempts to access the SMO Host or SMO tenant though a management interface. The attacker may be an internal or external actor. Weak account management and/or authentication can be exploited to gain access to move laterally across the deployment for nefarious purposes such as reconnaissance or damage. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-19 |
| **Threat title** | Malicious User Login Attempt to O-CU Host/Tenant |
| **Threat description** | The attacker attempts to access the O-CU Host or O-CU Tenant though a management interface. The attacker may be an internal or external actor. Weak account management and/or authentication can be exploited to gain access to move laterally across the deployment for nefarious purposes such as reconnaissance or damage. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-CU Host, O-CU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-20 |
| **Threat title** | Malicious User Login Attempt to O-DU Host/Tenant |
| **Threat description** | The attacker attempts to access the O-DU Host or O-DU Tenant though a management interface. The attacker may be an internal or external actor. Weak account management and/or authentication can be exploited to gain access to move laterally across the deployment for nefarious purposes such as reconnaissance or damage. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | O-DU Host, O-DU Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-21 |
| **Threat title** | Malicious User Login Attempt to Shared O-RU Host/Tenant |
| **Threat description** | The attacker attempts to access the O-RU Host or O-RU Tenant though a management interface. The attacker may be an internal or external actor. Weak account management and/or authentication can be exploited to gain access to move laterally across the deployment for nefarious purposes such as reconnaissance or damage. |
| **Threat type** | Spoofing |
| **Impact type** | Authenticity |
| **Affected Asset** | Shared O-RU |

#### Data Access Threats

This clause provides threat analysis tables for threats to Shared O-RU data access.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-22 |
| **Threat title** | Unauthorized internal threat actor gains access to data in Shared O-RU |
| **Threat description** | Malicious internal threat actor exploits compromised credentials or weak or misconfigured authorization to gain access to view or modify sensitive data-at-rest or data-in-use in the Shared O-RU. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-23 |
| **Threat title** | Unauthorized external threat actor gains access to data in Shared O-RU |
| **Threat description** | Malicious external threat actor exploits compromised credentials or weak or misconfigured authorization to gain access to view or modify sensitive data-at-rest or data-in-use in the Shared O-RU. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-24 |
| **Threat title** | Data exposure at Shared O-RU |
| **Threat description** | Data-at-rest on the Shared O-RU is exposed to a tenant. Attacker exploits weak confidentiality protection to view data owned by the MNO Host or a MNO Tenant. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-25 |
| **Threat title** | Shared O-RU data exposure at SMO |
| **Threat description** | Data-at-rest on the SMO related to a Shared O-RU is exposed to an unauthorized tenant / SMO user. Attacker exploits weak confidentiality protection to view data owned by the MNO Host or a MNO Tenant of a shared O-RU. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-26 |
| **Threat title** | Shared O-RU data exposure at O-DU |
| **Threat description** | Data-at-rest on the O-DU related to a Shared O-RU is exposed to an unauthorized tenant. Attacker exploits weak confidentiality protection to view data owned by the MNO Host or a MNO Tenant of a shared O-RU. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-27 |
| **Threat title** | Exposed data in transit between Shared O-RU and O-DU Host/Tenant |
| **Threat description** | Data-in-transit between the Shared O-RU and an O-DU Host or O-DU Tenant could be exposed to another MNO or malicious threat actor. Weak confidentiality protection of data-in-transit allows the host, tenant, or actor to view intercepted data owned by the MNO Host or a MNO Tenant. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU, M-Plane, CUS-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-28 |
| **Threat title** | Exposed data in transit between Shared O-RU and SMO Host/Tenant |
| **Threat description** | Data-in-transit between the Shared O-RU and a SMO Host or SMO Tenant could be exposed to another MNO or malicious threat actor. Weak confidentiality protection of data-in-transit allows the host, tenant, or actor to view intercepted data owned by the MNO Host or a MNO Tenant. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU, O1 |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-43 |
| **Threat title** | Eavesdropping of unprotected CUSM-plane data within shared O-RU |
| **Threat description** | The SMO assigns the role of Host and MNO SRO(s). The tenant maliciously or intended is obtaining access to transport protocol stack and is therefore able to eavesdrop sensitive data from neighbor tenants and the host. The tenant may have capability for sniffing/capturing of CUSM-plane data. |
| **Threat type** | Information Disclosure |
| **Impact type** | Confidentiality |
| **Affected Asset** | Shared O-RU |

#### Availability Threats

This clause provides threat analysis tables for availability threats to Shared O-RU.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-29 |
| **Threat title** | Modify/Delete OFH C-Plane messages |
| **Threat description** | A Host MNO, Tenant MNO, or 3rd-party, modifies or deletes control plane messages on the OFH C-Plane between the Shared O-RU and Host O-DU or Tenant O-DU. This type of integrity attack can also result in an availability attack. |
| **Threat type** | Tampering |
| **Impact type** | Integrity, Availability |
| **Affected Asset** | Shared O-RU, O-DU Host, O-DU Tenant, CUS-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-30 |
| **Threat title** | Clock hijacking on OFH S-Plane |
| **Threat description** | A Host MNO, Tenant MNO, or 3rd-party takes the role of Grand Master clock on the S-Plane to degrade performance on the U-Plane. This type of authorization exploit can also result in an availability attack. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization, Availability |
| **Affected Asset** | Shared O-RU, O-DU Host, O-DU Tenant, CUS-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-31 |
| **Threat title** | Parameter conflicts at Shared O-RU |
| **Threat description** | O-DU Host and O-DU Tenants may force conflicting parameter settings at the Shared O-RU that can degrade performance or cause an outage. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-32 |
| **Threat title** | Volumetric DDoS attack from O-DU targeting Shared O-RU |
| **Threat description** | An O-DU Host or O-DU Tenant maliciously or unintentionally sends a high-rate of malformed, mis-sequenced, invalid, or valid packets over the Open Fronthaul interface to the Shared O-RU. This kind of attack can cause a Denial of Service on the Shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU, M-Plane, CUS-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-33 |
| **Threat title** | Volumetric DDoS attack from SMO targeting Shared O-RU |
| **Threat description** | The SMO Host maliciously or unintentionally sends a high-rate of malformed, mis-sequenced, invalid, or valid packets over the Open Fronthaul interface to the Shared O-RU. This kind of attack can cause a Denial of Service on the Shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU, O1 |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-34 |
| **Threat title** | Volumetric DDoS attack targeting O-DU |
| **Threat description** | Shared O-RU maliciously or unintentionally sends a high-rate of malformed, mis-sequenced, invalid, or valid packets over the Open Fronthaul interface to the O-DU Host or O-DU Tenant. This kind of attack can cause a Denial of Service on the O-DU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | O-DU Host, O-DU Tenant, CUS-Plane, M-Plane |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-35 |
| **Threat title** | Shared O-RU initialization hijacking by DHCP compromise |
| **Threat description** | Shared O-RU bootup and initialization sequence depends on parameters passed to it via DHCP options. An attacker can compromise DHCP server and use it to hijack the O-RU and prevent Shared O-RU from reaching carrier-active state. This kind of attack can cause a Denial of Service on the shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-36 |
| **Threat title** | Shared O-RU M-plane hijacking by DNS compromise |
| **Threat description** | Shared O-RU M-plane initialization depends on DNS, if FQDN is returned as the NETCONF controller of shared O-RU during its initialization. The name resolution of FQDN can be manipulated by an attacker using a compromised DNS server and prevent Shared O-RU from reaching carrier-active state due to unavailability of carrier configuration. This kind of attack can cause a Denial of Service on the shared O-RU. |
| **Threat type** | Denial of Service |
| **Impact type** | Availability |
| **Affected Asset** | Shared O-RU |

#### Configuration Threats

This clause provides threat analysis tables for configuration threats to Shared O-RU.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-37 |
| **Threat title** | Misconfiguration of MNO Host Role |
| **Threat description** | The SMO assigns the role of MNO Host and MNO SRO(s). The assignment of Host role to the wrong SRO can expose data. A threat actor could exploit an incorrectly assigned role of Host to control function of the Shared O-RU |
| **Threat type** | Information Disclosure, Denial of Service |
| **Impact type** | Confidentiality, Availability |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-38 |
| **Threat title** | Incorrect Assignment of Spectrum Resources |
| **Threat description** | Shared O-RU is responsible for assignment and control of spectrum resources, including component carrier and frequencies within a carrier. Tenant access to the wrong resources, due to malicious intent or could be exploited to gain access to information. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-39 |
| **Threat title** | Chain of Trust in a Multi-Tenant Environment |
| **Threat description** | The Chain of Trust is a certificate-based chain used to authenticate an entity. The Chain of Trust is established by validating the hardware and software for the entity up to the root certificate as the trust anchor. The Shared O-RU mutually authenticates O-DU Hosts and O-DU Tenants. Certificates from O-DU tenants must be validated as trustworthy. Malicious actors can exploit untrustworthy certificates to gain access to the Shared O-RU. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | Shared O-RU, O-DU Host, O-DU Tenant, O-CU Host, O-CU Tenant, SMO Host, SMO Tenant |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-40 |
| **Threat title** | Hijack of MNO Host Role |
| **Threat description** | The SMO assigns the role of MNO Host and MNO SRO(s). A tenant may maliciously or unintentionally obtain the host role. The elevation of privilege would enable the tenant, acting as host, to have authorized access on the Shared O-RU to sensitive data, credentials, and system privileges. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-41 |
| **Threat title** | Not Released Host Role (Host Role resume) |
| **Threat description** | The SMO assigns the role of Host and MNO SRO(s). The tenant maliciously or intended is obtaining the host role, and implicit has obtained elevated privileges which could be used to drive wrong things, like obtaining of sensitive data and/or driving DoS. The tenant is not releasing the host role and/or the tenant is reusing known sensitive information and is driving wrong things. How to avoid that a tenant who has become once in his/her life a host is obtaining information that could be misused now and in the future. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-42 |
| **Threat title** | Misuse of “sudo” privileges |
| **Threat description** | The SMO assigns the role of Host and MNO SRO(s). The tenant maliciously or intended is obtaining the host role, and implicit has obtained elevated privileges which could be used to drive wrong things, like obtaining of sensitive data and/or driving DoS. How to avoid that any of the tenants can misuse the “sudo” privileges. This includes the default credentials of a shared O-RU. |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-55 |
| **Threat title** | Set Incorrect Array-Carrier configuration on O-DU (Standby) |
| **Threat description** | Threat actor spoofs SMO to set or modify the pre-configured array-carrier configuration on the O-DU in Standby state. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | O-DU, O1 interface |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-56 |
| **Threat title** | Modify Array-Carrier pre-configuration on Shared O-RU |
| **Threat description** | Threat actor can gain access to Shared O-RU to modify its pre-configured array-carrier |
| **Threat type** | Elevation of Privilege |
| **Impact type** | Authorization |
| **Affected Asset** | Shared O-RU |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-57 |
| **Threat title** | Modify/Inject M-Plane messages with Array-Carrier configuration |
| **Threat description** | Threat actor Modifies/Injects M-Plane messages with Array-Carrier configuration sent to the Shared O-RU. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | Shared O-RU, M-Plane |

#### Resiliency Threats

This clause provides threat analysis tables for threats introduced by the O-DU Resiliency use case.

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-52 |
| **Threat title** | Thrashing O-DU Failovers |
| **Threat description** | Threat actor spoofs SMO to cause O-DU-1 and O-DU-2 to thrash between Active state and Standby state |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | O-DU, O1 interface |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-53 |
| **Threat title** | Dual (Dueling) Active O-DUs |
| **Threat description** | Threat actor spoofs SMO to cause O-DU-1 and O-DU-2 to both be in Active state. |
| **Threat type** | Spoofing |
| **Impact type** | Authentication |
| **Affected Asset** | O-DU, O1 interface |

|  |  |
| --- | --- |
| Threat ID | T-SharedORU-54 |
| **Threat title** | Modify/Inject O1 messages at the SMO |
| **Threat description** | Threat actor spoofs O-DU to modify, inject, flood O1 messages to the SMO to prevent SMO detection of O-DU failure. |
| **Threat type** | Tampering |
| **Impact type** | Integrity |
| **Affected Asset** | SMO, O1 interface |

## Coverage matrix of threats

From the above threats, a threat inventory is developed to provide a mapping between threats, vulnerabilities and assets. For the purposes of this document, threats have been grouped into two categories:

1. ‘O-RAN specific’ comprises threats directly relating to O-RAN components and interfaces
2. ‘General’ covers threats relating to physical, open source, virtualization, IoT and radio aspects

The threat inventory provides details of each individual threat: threat agents, vulnerabilities, threatened assets and affected components.

Table 7‑1 : O-RAN Threat Inventory

| Threat ID | Threat title | Threat agent | Vulnerability | Threatened Asset | Affected Components |
| --- | --- | --- | --- | --- | --- |
| **O-RAN specific threats** | | | | | |
| T-O-RAN-01 | An attacker exploits insecure designs or lack of adaption in O-RAN components | All | * Outdated component from the lack of update or patch management * Poorly design architecture * Missing appropriate security hardening * Unnecessary or insecure function/protocol/component | All | All |
| T-O-RAN-02 | An attacker exploits misconfigured or poorly configured O-RAN components | All | * Errors from the lack of configuration change management * Misconfigured or poorly configured O-RAN components * Improperly configured permissions * Unnecessary features are enabled (e.g. unnecessary ports, services, accounts, or privileges) * Default accounts and their passwords still enabled and unchanged * Security features are disabled or not configured securely | All | All |
| T-O-RAN-03 | Attacks from the internet to penetrate O-RAN network boundary | All | Errors in the design and implementation of the network protocols (HTTP, P, TCP, UDP, application protocols) | All | All |
| T-O-RAN-04 | An attacker attempts to jam the airlink signal through IoT devices | All | Failure to address overload situations | ASSET-D-06, ASSET-D-18 | O-RU, airlink with UE, O-DU |
| T-O-RAN-05 | An attacker penetrates and compromises the O-RAN system through the open O-RAN’s Fronthaul, O1, O2, A1, and E2 | All | * 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 | All | rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC |
| T-O-RAN-06 | An attacker exploits insufficient/improper mechanisms for authentication and authorization to compromise O-RAN components | All | * 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 | All | All |
| T-O-RAN-07 | An attacker compromises O-RAN monitoring mechanisms and log files integrity and availability | All | * Lack of security event logging * Insufficient protection of log files | ASSET-D-29 | All |
| T-O-RAN-08 | An attacker compromises O-RAN data integrity, confidentiality and traceability | All | * 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 confidential internal data * No traceability (logging) of access to personal data | ASSET-D-01 to ASSET-D-29 | All |
| T-O-RAN-09 | An attacker compromises O-RAN components integrity and availability | All | * Improper handling of overload situations * Unrestricted boot memory devices * Lack of / improper mechanisms for Network Product software package integrity validation | ASSET-C-01 to ASSET-C-12 | All |
| T-FRHAUL-01 | An attacker penetrates O-DU and beyond through O-RU or the Fronthaul interface | All | Heterogeneous security levels between O-RU and O-DU provided by different vendors | ASSET-D-01, ASSET-D-02, ASSET-D-04, ASSET-D-05 | rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC |
| T-FRHAUL-02 | Unauthorized access to Open Front Haul Ethernet L1 physical layer interface(s) | All | Lack of authentication and access control to the Open Front Haul Ethernet L1 physical layer interface | ASSET-D-01, ASSET-D-02, ASSET-D-04, ASSET-D-05 | rApps, xApps, O-RU, O-DU, O-CU, Near-RT RIC, Non-RT RIC |
| T-MPLANE-01 | An attacker attempts to intercept the Fronthaul (MITM) over M Plane | All | Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements | ASSET-D-02, ASSET-D-03 | Near-RT RIC, Non-RT RIC, O-CU, O-DU, SMO |
| T-SPLANE-01 | DoS attack against a Master clock | All | * Improper process to monitor and manage the performance of the Master clock * ANNOUNCE messages can be sent publicly in clear text | ASSET-D-01 | O-DU, O-RU |
| T-SPLANE-02 | Impersonation of a Master clock (Spoofing) within a PTP network with a fake ANNOUNCE message | All | * Inaccurate timing information * Improper synchronization between clocks * ANNOUNCE messages can be sent publicly in clear text | ASSET-D-01 | O-DU, O-RU |
| T-SPLANE-03 | A Rogue PTP Instance wanting to be a Grand Master | All | * Inaccurate timing information * Improper synchronization between clocks * ANNOUNCE messages can be sent publicly in clear text | ASSET-D-01 | O-DU, O-RU |
| T-SPLANE-04 | Selective interception and removal of PTP timing packets | All | * Inaccurate timing information * Improper synchronization between clocks * ANNOUNCE messages can be sent publicly in clear text | ASSET-D-01 | O-DU, O-RU |
| T-SPLANE-05 | Packet delay manipulation attack | All | * Inaccurate timing information * Improper synchronization between clocks * ANNOUNCE messages can be sent publicly in clear text | ASSET-D-01 | O-DU, O-RU |
| T-CPLANE-01 | Spoofing of DL C-plane messages | All | Lack of authentication could allow an adversary to inject own DL C-plane messages | ASSET-D-04 | O-DU, O-RU |
| T-CPLANE-02 | Spoofing of UL C-plane messages | All | Lack of authentication could allow an adversary to inject own UL C-plane messages | ASSET-D-04 | O-DU, O-RU |
| T-UPLANE-01 | An attacker attempts to intercept the Fronthaul (MITM) over U Plane | All | Lack of sufficient security measures in the Fronthaul due to the negative impact on the performance requirements | ASSET-D-05 | O-DU, O-RU |
| T-ORU-01 | An attacker stands up a false base station attack by attacking an O-RU | All | False O-RUs | ASSET-D-01, ASSET-D-02, ASSET-D-03, ASSET-D-04, ASSET-D-05, ASSET-D-06 | O-RU |
| T-NEAR-RT-01 | Malicious Apps can exploit UE identification, track UE location and change UE priority | All | Malicious xApps may be used to gain access to UE identification location and priority | ASSET-D-21, ASSET-D-22, ASSET-D-41, ASSET-D-43 | Near-RT RIC, UE, xApps |
| T-NEAR-RT-02 | Risk of deployment of a malicious xApp on Near-RT RIC | All | Improper or missing authentication and authorization of xApps | ASSET-D-10, ASSET D-11, ASSET D-21, ASSET-D-22 | Near-RT RIC, UE, xApps |
| T-NEAR-RT-03 | Attackers exploit non authenticated, weakly or incorrectly authenticated Near-RT RIC APIs | All | Non authenticated, weakly or incorrectly authenticated Near-RT RIC APIs | ASSET-D-09, ASSET-D-10, ASSET D-11, ASSET D-20, ASSET-D-21, ASSET-D-25, ASSET-D-26, ASSET-D-29, ASSET-D-30, ASSET-C-02, ASSET-C-09, ASSET-D-41, ASSET-D-43 | Near-RT RIC, UE, xApps |
| 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. | All | Non-authorized RT RIC APIs | ASSET-D-09, ASSET-D-10, ASSET D-11, ASSET D-20, ASSET-D-21, ASSET-D-25, ASSET-D-26, ASSET-D-29, ASSET-D-30, ASSET-C-02, ASSET-C-09, ASSET-D-41, ASSET-D-43 | Near-RT RIC, UE, xApps |
| T-NEAR-RT-05 | Attackers exploit non uniquely identified xApps using a trusted xAppID to access to resources and services which they are not entitled to use. | All | Not uniquely identifying xApps using a trusted xAppID | ASSET-D-39, ASSET-C-02, ASSET-C-09 | Near-RT RIC, xApps |
| T-NONRTRIC-01 | An attacker gains access to the Non-RT RIC through the SMO to cause a denial of service or degrade the performance of the Non-RT-RIC | All | Improper or missing authentication and authorization processes on the Non-RT RIC or SMO | ASSET-D-03, ASSET-D-07, ASSET-D-08, ASSET-C-11 | Non-RT RIC, rApps |
| T-NONRTRIC-02 | An attacker gains access to the Non-RT RIC through the SMO for UE tracking | All | Malicious rApps may be used to gain access to UE identification | ASSET-D-21, ASSET-D-22, ASSET-C-11 | Non-RT RIC, rApps, UE |
| T-NONRTRIC-03 | An attacker gains access to the Non-RT RIC through the SMO to cause Data Corruption/Modification | All | Improper or missing authentication and authorization processes on the Non-RT RIC or SMO | ASSET-C-11 | Non-RT RIC |
| T-NONRTRIC-04 | An attacker exploits non uniquely identified rApp instances using a trusted rAppID to access R1 services and data which they are not entitled to use | All | Not uniquely identifying rApp instances using a trusted rAppID | ASSET-C-10, ASSET-C-11 | Non-RT RIC, rApps |
| T-xAPP-01 | An attacker exploits xApps vulnerabilities and misconfiguration | All | xApp stems from an untrusted or unmaintained source | ASSET-C-03, ASSET-C-07, ASSET-C-08, ASSET-C-09, ASSET-C-10 | O-CU, Near-RT RIC, xApps |
| T-xAPP-02 | Conflicting xApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS | All | * xApps may be misconfigured or compromised * Failing or misconfigured authentication and authorization in xApp | ASSET-C-03, ASSET-C-07, ASSET-C-08, ASSET-C-09, ASSET-C-10 | O-CU, Near-RT RIC, xApps |
| T-xAPP-03 | An attacker compromises xApp isolation | All | Vulnerabilities in the underlying system hosting xApps | ASSET-C-03, ASSET-C-07, ASSET-C-08, ASSET-C-09, ASSET-C-10 | O-CU, Near-RT RIC, xApps |
| T-xApp-04 | False or malicious A1 policies modify behavior of xApps | All | xApp functionality exploited by malicious A1 policies | ASSET-D-07, ASSET-D-11, ASSET-C-09 | O-CU, O-DU, Near-RT RIC, xApps |
| T-rAPP-01 | Conflicting rApps impact O-RAN system functions to degrade performance or trigger a DoS | All | rApp stems from an untrusted or unmaintained source | ASSET-C-10 | rApps, Non-RT RIC |
| T-rAPP-02 | An attacker exploits rApp vulnerability for data breach or denial of service | All | rApp management is exposed to the tenant in a web front-end or REST API. These interfaces may contain software vulnerabilities or implement authentication and authorization insufficiently. | ASSET-C-10 | rApps, Non-RT RIC |
| T-rAPP-03 | An attacker exploits rApps misconfiguration | All | Vulnerabilities in the underlying system hosting rApps | ASSET-C-10 | rApps, Non-RT RIC |
| T-rAPP-04 | An attacker bypasses authentication and authorization | All | * rApps may be misconfigured or compromised * Failing or misconfigured authentication and authorization in rApp | ASSET-C-10 | rApps, Non-RT RIC |
| T-rAPP-05 | An attacker deploys and exploits malicious rApp | All | * rApps may be misconfigured or compromised * Failing or misconfigured authentication and authorization in rApp | ASSET-C-10 | rApps, Non-RT RIC |
| T-rAPP-06 | An attacker bypasses authentication and authorization using an injection attack | All | * rApps may be misconfigured or compromised * Failing or misconfigured authentication and authorization in rApp | ASSET-C-10 | rApps, Non-RT RIC |
| T-rAPP-07 | rApp exploits services | All | * rApps may be misconfigured or compromised * Failing or misconfigured authentication and authorization in rApp | ASSET-C-10 | rApps, Non-RT RIC |
| T-PNF-01 | An attacker compromises a PNF to launch reverse attacks and other attacks against VNFs/CNFs | All | Mixed PNF-VNF/CNF deployments | All | All |
| T-SMO-01 | External attacker exploits authentication weakness on SMO | All | Missing or improperly configured authentication | ASSET-C-11, ASSET-C-17 | Non-RT RIC, SMO Framework |
| T-SMO-02 | External attacker exploits authorization weakness on SMO | All | Missing or improperly configured authorization | ASSET-C-11, ASSET-C-17 | Non-RT RIC, SMO Framework |
| T-SMO-03 | External Overload DoS attack targeted at SMO | All | Lack of overload protection and rate-limiting | ASSET-C-11, ASSET-C-17 | Non-RT RIC, SMO Framework |
| T-SMO-04 | Internal attacker exploits authentication weakness on a SMO function | All | Missing or improperly configured authentication | ASSET-C-11, ASSET-C-17, ASSET-C-18, ASSET-C-19, ASSET-C-20, ASSET-C\_21 | All |
| T-SMO-05 | Internal attacker exploits authorization weakness on a SMO function | All | Missing or improperly configured authorization | ASSET-C-11, ASSET-C-17, ASSET-C-18, ASSET-C-19, ASSET-C-20, ASSET-C\_21 | All |
| T-SMO-06 | Internal Overload DoS attack targeted at SMO functions | All | Lack of overload protection and rate-limiting | ASSET-C-11, ASSET-C-17, ASSET-C-18, ASSET-C-19, ASSET-C-20, ASSET-C\_21 | All |
| T-SMO-07 | Internal DoS attack disables internal SMO function(s) or process(es) | All | Privilege escalation or improperly configured authorization | ASSET-C-11, ASSET-C-17, ASSET-C-18, ASSET-C-19, ASSET-C-20, ASSET-C\_21 | All |
| T-SMO-08 | Attacker exploits insecure API to gain access to SMO | All | API vulnerability | ASSET-C-11, ASSET-C-17, ASSET-C-18, ASSET-C-19, ASSET-C-20, ASSET-C\_21 | All |
| T-SMO-09 | Sensitive data in transit is exposed to an internal attacker | All | Missing or weak confidentiality protection of data in transit | ASSET-C-11, ASSET-C-17, ASSET-C-18, ASSET-C-19, ASSET-C-20, ASSET-C\_21 | All |
| T-SMO-10 | Sensitive data at rest is exposed to an internal attacker | All | Missing or weak confidentiality protection of data at rest | ASSET-C-11, ASSET-C-17, ASSET-C-18, ASSET-C-19, ASSET-C-20, ASSET-C\_21 | All |
| T-SMO-11 | AI/ML poisoning by internal attacker | All | Missing integrity protection of data at rest | ASSET-C-11, ASSET-C-17 | Non-RT RIC, SMO Froamework |
| T-SMO-12 | AI/ML exposure on external entity | All | Missing or weak confidentiality protection of data at rest | ASSET-C-11, ASSET-C-17 | Non-RT RIC, SMO Framework |
| T-SMO-13 | Malicious actor views local logs | All | Missing or weak confidentiality protection of data at rest | ASSET-C-17, ASSET-C-18 | SMO Framework, SMO Functions |
| T-SMO-14 | Malicious actor modifies local log entries | All | Missing integrity protection of data at rest | ASSET-C-17, ASSET-C-18 | SMO Framework, SMO Functions |
| T-SMO-15 | Malicious actor deletes local logs | All | Missing integrity protection of data at rest | ASSET-C-17, ASSET-C-18 | SMO Framework, SMO Functions |
| T-SMO-16 | Malicious actor intercepts exports of local logs | All | Missing or weak confidentiality protection of data in transit | ASSET-C-17, ASSET-C\_18, ASSET-C-26 | SMO Framework, SMO Functions, External interfaces |
| T-SMO-17 | Malicious external actor gains unauthorized access to logs | All | Missing or improperly configured authorization | ASSET-C-17, ASSET-C-18 | SMO Framework, SMO Functions |
| T-SMO-18 | Malicious internal actor gains authorized access to logs | All | Missing or improperly configured authorization | ASSET-C-17, ASSET-C-18 | SMO Framework, SMO Functions |
| T-SMO-19 | Internal attacker exploits O2 interface to view data in transit between SMO and O-Cloud | All | Missing or weak confidentiality protection of data in transit | ASSET-C\_08, ASSET-C-17, ASSET-C-23 | O-Cloud, SMO, O2 interface |
| T-SMO-20 | Internal attacker exploits O2 interface to modify data in transit between SMO and O-Cloud | All | Missing integrity checking for data in transit | ASSET-C\_08, ASSET-C-17, ASSET-C-23 | O-Cloud, SMO, O2 interface |
| T-SMO-21 | Internal attacker uses O2 interface via SMO to exploit API vulnerability to gain access to O-Cloud infrastructure | All | API vulnerability | ASSET-C\_08, ASSET-C-17, ASSET-C-23 | O-Cloud, SMO, O2 interface |
| T-SMO-22 | Internal attacker floods O2 interface via SMO to cause DDoS on O-Cloud infrastructure | All | Lack of overload protection and rate-limiting | ASSET-C-08, ASSET-C-17, ASSET-C-23 | O-Cloud, SMO, O2 interface |
| T-SMO-23 | External attacker uses O2 interface via O-Cloud to exploit API vulnerability to gain access to SMO | All | API vulnerability | ASSET-C\_08, ASSET-C-17, ASSET-C-23 | O-Cloud, SMO, O2 interface |
| T-SMO-24 | External attacker floods O2 interface via O-Cloud to cause DDoS on SMO | All | Lack of overload protection and rate-limiting | ASSET-C\_08, ASSET-C-17, ASSET-C-23 | O-Cloud, SMO, O2 interface |
| T-SMO-25 | External attacker uses O2 interface via O-Cloud to gain authorized access to sensitive data-at-rest at the SMO | All | Missing or improperly configured authorization | ASSET-C\_08, ASSET-C-17, ASSET-C-23 | O-Cloud, SMO, O2 interface |
| T-SMO-26 | External attacker exploits External interface to view data in transit between SMO and external service | All | Missing or weak confidentiality protection of data in transit | ASSET-C\_11, ASSET-C-17, ASSET-C-26 | Non-RT RIC, SMO, External interfaces |
| T-SMO-27 | External attacker exploits External interface to modify data in transit between SMO and external service | All | Missing integrity checking for data in transit | ASSET-C\_11, ASSET-C-17, ASSET-C-26 | Non-RT RIC, SMO, External interfaces |
| T-SMO-28 | External attacker uses External interface to exploit API vulnerability to gain access to SMO | All | API vulnerability | ASSET-C\_11, ASSET-C-17, ASSET-C-26 | Non-RT RIC, SMO, External interfaces |
| T-SMO-29 | External attacker floods External interface to cause DDoS at SMO | All | Lack of overload protection and rate-limiting | ASSET-C\_11, ASSET-C-17, ASSET-C-26, ASSET-C\_27, ASSET-C-28 | All |
| T-SMO-30 | External attacker uses External interface to gain access to sensitive data-at-rest at the SMO | All | Missing or improperly configured authorization | ASSET-C\_11, ASSET-C-17, ASSET-C-26 | Non-RT RIC, SMO, External interfaces |
| T-SMO-31 | External attacker poisons External AI/ML data to corrupt SMO | All | Missing integrity checking for data at rest | ASSET-C\_11, ASSET-C-17, ASSET-C-26 | Non-RT RIC, SMO, External interfaces |
| T-SMO-32 | External attacker poisons External Enrichment Information data sources to corrupt SMO | All | Missing integrity checking for data at rest | ASSET-C\_11, ASSET-C-17, ASSET-C-26 | Non-RT RIC, SMO, External interfaces |
| T-R1-01 | A malicious actor gains unauthorized access to R1 services | All | weak mutual authentication | ASSET-C-16 | R1 interface |
| T-R1-02 | Attacker modifies Service Heartbeat message to cause Denial of Service | All | weak mutual authentication | ASSET-C-16 | R1 interface |
| T-R1-03 | Malicious actor bypasses authentication to Request Data | All | weak mutual authentication | ASSET-C-16 | R1 interface |
| T-R1-04 | Malicious actor bypasses authorization to Discover Data | All | weak mutual authentication | ASSET-C-16 | R1 interface |
| T-R1-05 | A malicious actor gains unauthorized access to data | All | weak mutual authentication | ASSET-C-16 | R1 interface |
| T-R1-06 | Malicious actor modifies a Data Request | All | weak mutual authentication | ASSET-C-16 | R1 interface |
| T-R1-07 | Malicious actor compromises Data Delivery to the Data Consumer | All | weak mutual authentication | ASSET-C-16 | R1 interface |
| T-A1-01 | Untrusted peering between Non-RT-RIC and Near-RT-RIC | All | weak mutual authentication | ASSET-C-14 | A1 interface |
| T-A1-02 | Malicious function or application monitors messaging across A1 interface | All | weak mutual authentication | ASSET-C-14 | A1 interface |
| T-A1-03 | Malicious function or application modifies messaging across A1 interface | All | weak mutual authentication | ASSET-C-14 | A1 interface |
| T-AppLCM-01 | Compromise of App/VNF/CNF update package integrity during onboarding | All | Lack of integrity verification | ASSET-D-15 | Apps/VNFs/CNFs |
| T-AppLCM-02 | Compromise of App/VNF/CNF update image integrity during instantiation | All | Lack of integrity verification | ASSET-D-15 | Apps/VNFs/CNFs images |
| T-AppLCM-03 | Downgrade attack to vulnerable application version | All | Lack of integrity verification | ASSET-D-15 | Apps/VNFs/CNFs |
| T-AppLCM-04 | Attacker exploits missing or improperly defined elements of application’s SecurityDescriptor | All | Misconfiguration | ASSET-D-15 | Apps/VNFs/CNFs |
| T-AppLCM-05 | Malicious actor modifies application’s SecurityDescriptor | All | Lack of authentication, lack of integrity verification | ASSET-D-15 | Apps/VNFs/CNFs |
| T-AppLCM-06 | Improper decommissioning of application | All | Improper release of resources and secrets | ASSET-D-15 | Apps/VNFs/CNFs |
| T-AppLCM-07 | Improper deletion of application sensitive data | All | Missing or weak confidentiality protection | ASSET-D-16, ASSET-D-17, ASSET-D-32 | Apps/VNFs/CNFs |
| T-SharedORU-01 | O-DU Tenant accesses O-DU Host | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-34 | O-DU Host |
| T-SharedORU-02 | O-DU Host accesses O-DU Tenant | All | Weak authentication can be exploited by a host to move laterally across the deployment. | ASSET-C-35 | O-DU Tenant |
| T-SharedORU-03 | O-DU Tenant accesses O-DU Tenant | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-35 | O-DU Tenant |
| T-SharedORU-04 | Password Attack on OFH M-Plane | All | The attack can be a brute-force attack or stolen password. There is increased risk of password attack in a multi-tenant environment. | ASSET-C-31, ASSET-C-34, ASSET-C-35 | Shared O-RU, O-DU Host, O-DU Tenant |
| T-SharedORU-05 | Untrusted peering to O-DU | All | Attacker exploits weak authentication on the O-DU to establish a session with a malicious app masquerading as a Shared O-RU. From the O-DU, a malicious actor can move laterally. | ASSET-C-34, ASSET-C-35 | O-DU Host, O-DU Tenant |
| T-SharedORU-06 | Untrusted peering to the Shared O-RU | All | Weak authentication can be exploited to establish session with a malicious app masquerading as a O-DU Host or O-DU Tenant | ASSET-C-31 | Shared O-RU |
| T-SharedORU-07 | Untrusted peering to the SMO | All | Weak authentication on the SMO can be exploited to establish session with a malicious app masquerading as a Shared O-RU. | ASSET-C-31 | Shared O-RU |
| T-SharedORU-08 | SMO Tenant accesses SMO Host | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-38 | SMO Host |
| T-SharedORU-09 | SMO Host accesses SMO Tenant | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-39 | SMO Tenant |
| T-SharedORU-10 | O-DU Host accesses O-CU Tenant | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-37 | O-CU Tenant |
| T-SharedORU-11 | O-DU Tenant accesses O-CU Host | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-36 | O-CU Host |
| T-SharedORU-12 | O-DU Tenant accesses O-CU Tenant | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-37 | O-CU Tenant |
| T-SharedORU-13 | SMO Host accesses O-CU Tenant | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-37 | O-CU Tenant |
| T-SharedORU-14 | SMO Tenant accesses O-CU Host | All | Weak authentication can be exploited by a tenant to move laterally across the deployment. | ASSET-C-36 | O-CU Host |
| T-SharedORU-15 | Physical port access to Shared O-RU Host/Tenant | All | Weak physical layer authentication can be exploited to gain access. | ASSET-C-31 | Shared O-RU |
| T-SharedORU-16 | Physical port access to O-DU Host/Tenant | All | Weak physical layer authentication can be exploited to gain access. | ASSET-C-34, ASSET-C-35 | O-DU Host, O-DU Tenant |
| T-SharedORU-17 | Physical port access to O-CU Host/Tenant | All | Weak physical layer authentication can be exploited to gain access. | ASSET-C-36, ASSET-C-37 | O-CU Host, O-CU Tenant |
| T-SharedORU-18 | Malicious User Login Attempt to SMO Host/Tenant | All | Weak account management and/or authentication can be exploited to gain access. | ASSET-C-38, ASSET-C-39 | SMO Host, SMO Tenant |
| T-SharedORU-19 | Malicious User Login Attempt to O-CU Host/Tenant | All | Weak account management and/or authentication can be exploited to gain access | ASSET-C-36, ASSET-C-37 | O-CU Host, O-CU Tenant |
| T-SharedORU-20 | Malicious User Login Attempt to O-DU Host/Tenant | All | Weak account management and/or authentication can be exploited to gain access | ASSET-C-32, ASSET-C-33 | O-DU Host, O-DU Tenant |
| T-SharedORU-21 | Malicious User Login Attempt to Shared O-RU Host/Tenant | All | Weak account management and/or authentication can be exploited to gain access | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-22 | Unauthorized internal threat actor gains access to data in Shared O-RU | All | Compromised credentials or weak or misconfigured authorization to gain access to view or modify sensitive data | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-23 | Unauthorized external threat actor gains access to data in Shared O-RU | All | Compromised credentials or weak or misconfigured authorization to gain access to view or modify sensitive data | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-24 | Data exposure at Shared O-RU | All | Weak confidentiality protection exploited to view sensitive data | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-25 | Shared O-RU data exposure at SMO | All | Weak confidentiality protection exploited to view sensitive data | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-26 | Shared O-RU data exposure at O-DU | All | Weak confidentiality protection exploited to view sensitive data | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-27 | Exposed data in transit between Shared O-RU and O-DU Host/Tenant | All | Weak confidentiality protection exploited to view sensitive data | **ASSET-C-31, ASSET-C-24, ASSET-C-25** | Shared O-RU, M-Plane, CUS-Plane |
| T-SharedORU-28 | Exposed data in transit between Shared O-RU and SMO Host/Tenant | All | Weak confidentiality protection exploited to view sensitive data | **ASSET-C-31, ASSET-C-22** | Shared O-RU, O1 |
| T-SharedORU-29 | Modify/Delete OFH C-Plane messages | All | Weak integrity protection exploited to modify or delete control messages | **ASSET-C-31, ASSET-C\_34, ASSET-C-35, ASSET-C-25** | Shared O-RU, O-DU Host, O-DU Tenant, CUS-Plane |
| T-SharedORU-30 | Clock hijacking on OFH S-Plane | All | Weak authorization exploit can also result in spoofing of the Grand Master clock for an availability attack | **ASSET-C-31, ASSET-C\_34, ASSET-C-35, ASSET-C-25** | Shared O-RU, O-DU Host, O-DU Tenant, CUS-Plane |
| T-SharedORU-31 | Parameter conflicts at Shared O-RU | All | Conflicting parameter settings degrade performance or cause an outage. | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-32 | Volumetric DDoS attack from O-DU targeting Shared O-RU | All | High-rate of malformed, mis-sequenced, invalid, or valid packets to cause a Denial of Service | **ASSET-C-31, ASSET-C-24, ASSET-C-25** | Shared O-RU, M-Plane, CUS-Plane |
| T-SharedORU-33 | Volumetric DDoS attack from SMO targeting Shared O-RU | All | High-rate of malformed, mis-sequenced, invalid, or valid packets to cause a Denial of Service | **ASSET-C-31, ASSET-C-22** | Shared O-RU, O1 |
| T-SharedORU-34 | Volumetric DDoS attack targeting O-DU | All | High-rate of malformed, mis-sequenced, invalid, or valid packets to cause a Denial of Service | **ASSET-C\_34, ASSET-C-35, ASSET-C-24, ASSET-C-25** | O-DU Host, O-DU Tenant, M-Plane, CUS-Plane |
| T-SharedORU-35 | Shared O-RU initialization hijacking by DHCP compromise | All | Compromise DHCP server and use it to prevent Shared O-RU from reaching carrier-active state causing a Denial of Service | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-36 | Shared O-RU M-plane hijacking by DNS compromise | All | The name resolution of FQDN can be manipulated by an attacker using a compromised DNS server and prevent Shared O-RU from reaching carrier-active state causing a Denial of Service | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-37 | Misconfiguration of MNO Host Role | All | A threat actor could exploit an incorrectly assigned role of Host to control function of the Shared O-RU | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-38 | Incorrect Assignment of Spectrum Resources | All | Tenant access to the wrong resources, due to malicious intent or could be exploited to gain access to information. | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-39 | Chain of Trust in a Multi-Tenant Environment | All | Untrustworthy certificates can be exploited to gain access to the Shared O-RU | **ASSET-C-31, ASSET-C-34, ASSET-C-35, ASSET-C-36, ASSET-C\_37, ASSET-C-38, ASSET-C-39** | Shared O-RU, O-DU Host, O-DU Tenant, O-CU Host, O-CU Tenant, SMO Host, SMO Tenant |
| T-SharedORU-40 | Hijack of MNO Host Role | All | Elevation of privilege enables the tenant, acting as host, to have authorized access to sensitive data, credentials, and system privileges | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-41 | Not Released Host Role (Host Role resume) | All | Elevation of privilege enables the tenant, acting as host, to have authorized access to sensitive data, credentials, and system privileges | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-42 | Misuse of “sudo” privileges | All | Elevation of privilege enables the tenant, acting as host, to have authorized access to sensitive data, credentials, and system privileges | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-43 | Eavesdropping of unprotected CUSM-plane data within shared O-RU | All | Eavesdrop sensitive data between neighbor tenants and the host | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-44 through T-SharedORU-51 are Void | | | | | |
| T-SharedORU-52 | Thrashing O-DU Failovers | All | Threat actor spoofs SMO to cause O-DU-1 and O-DU-2 to thrash between Active state and Standby state | **ASSET-C-34, ASSET-C-22** | O-DU, O1 |
| T-SharedORU-53 | Dual (Dueling) Active O-DUs | All | Threat actor spoofs SMO to cause O-DU-1 and O-DU-2 to both be in Active state. | **ASSET-C-34, ASSET-C-22** | O-DU, O1 |
| T-SharedORU-54 | Modify/Inject O1 messages at the SMO | All | Threat actor spoofs O-DU to modify, inject, flood O1 messages to the SMO to prevent SMO detection of O-DU failure. | **ASSET-C-38, ASSET-C-22** | SMO, O1 |
| T-SharedORU-55 | Set Incorrect Array-Carrier configuration on O-DU (Standby) | All | Threat actor spoofs SMO to set or modify the pre-configured array-carrier configuration on the O-DU in Standby state. | **ASSET-C-34, ASSET-C-22** | O-DU, O1 |
| T-SharedORU-56 | Modify Array-Carrier pre-configuration on Shared O-RU | All | Threat actor can gain access to Shared O-RU to modify its pre-configured array-carrier | **ASSET-C-31** | Shared O-RU |
| T-SharedORU-57 | Modify/Inject M-Plane messages with Array-Carrier configuration | All | Threat actor Modifies/Injects M-Plane messages with Array-Carrier configuration sent to the Shared O-RU. | **ASSET-C-31, ASSET-C-24** | Shared O-RU, M-Plane |
| **General threats** | | | | | |
| T-GEN-01 | Software flaw attack | All | Vulnerable code exploits, Design Weakness | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-GEN-02 | Malicious access to exposed services using valid accounts | All | Lack of authentication | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-GEN-03 | Untrust binding between the different O-Cloud layers | All | Lack of integrity verification during boot or runtime | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-GEN-04 | Lack of Authentication & Authorization in interfaces between O-Cloud components | All | Lack of authentication, Insecure interfaces | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs, O2 |
| T-GEN-05 | Unsecured credentials and keys | All | Insecure O-Cloud APIs, Lack of integrity verification during boot or runtime | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud |
| T-GEN-06 | Sensitive application data cache exploitation | All | Sensitive information disclosure, Privilege escalation in Applications | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-VM-C-01 | Abuse of a privileged VM/Container | All | Misconfiguration or Insecure VM/Container configurations | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-VM-C-02 | VM/Container escape attack | All | Shared tenancy vulnerabilities (multitenant environment), Lack of strong VM/Container isolation, lack of authentication, Insecure networking, Unrestricted communication between VMs/Containers | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-VM-C-03 | VM/Container data theft | All | Lack of authentication, insecure data storage | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-VM-C-04 | VM/Container migration attacks | All | Host misconfiguration, lack of authentication, memory pages copied in clear, vulnerable code exploits | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-VM-C-05 | Changing virtualization resource without authorization | All | Insecure O1/O2 interfaces, Lack of authentication/access control on IMS/DMS | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-VM-C-06 | Failed or incomplete VNF/CNF termination or releasing of resources | All | Lack of authentication, misconfigurations (VNF/CNF, Host OS, Hypervisor/Container Engine) | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-IMG-01 | VM/Container images tampering | All | Compromised VM/Container images (Build machine attacks, Supply chain attacks) at rest, lack of authentication, misconfiguration or Insecure VM/Container images configurations | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs images |
| T-IMG-02 | Insecure channels with images repository | All | Compromised VM/Container images in transit | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs images |
| T-IMG-03 | Secrets disclosure in VM/Container images | All | Secret exposure in VNF/CNF images | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs images |
| T-IMG-04 | Build image on VL | All | Host misconfiguration, lack of authentication | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs images |
| T-VL-01 | VM/Container hyperjacking attack | All | Host misconfiguration, lack of authentication | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-VL-02 | Boot tampering | All | Host misconfigurations, lack of authentication | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-VL-03 | Attack internal network services | All | Insecure O-Cloud APIs, Lack of authentication | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud |
| T-O2-01 | MitM attacks on O2 interface between O-Cloud and SMO | All | Insecure O2 interface, lack authentication | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O2 |
| T-OCAPI-01 | MitM attacks on O-Cloud interface between VNFs/CNFs and the virtualization layer | All | Insecure O-Cloud APIs, lack of authentication | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-HW-01 | Cross VM/Container side channel attacks | All | Flaws in chip design, use of shared hardware, Lack of isolation, lack of authentication | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud, Apps/VNFs/CNFs |
| T-HW-02 | MitM attacks on the interface between virtualization layer and hardware | All | Insecure interfaces between HW and VL layers, lack of authentication, misconfiguration | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | O-Cloud |
| T-ADMIN-01 | Denial of service against NFO/FOCOM | All | Lack of authentication, vulnerable code exploits, design weakness, insecure O2 interface | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | NFO/FOCOM, O-Cloud, Apps/VNFs/CNFs |
| T-ADMIN-02 | Abuse a O-Cloud administration service | All | Lack of authentication, secret exposure (insufficient safeguarding of credentials), vulnerable code exploits, design weakness | ASSET-D-12, ASSET-D-13, ASSET-D-14, ASSET-D-15, ASSET-D-16, ASSET-D-17, ASSET-D-18, ASSET-D-19, ASSET-D-20, ASSET-D-29, ASSET-D-31, ASSET-D-32 | NFO/FOCOM, O-Cloud, Apps/VNFs/CNFs |
| T-AAL-01 | Attacker exploits insecure API to gain access to hardware accelerator resources | All | Insecure AAL APIs and interfaces  Lack authentication and authorization | ASSET-D-33 to ASSET-D-38 | ASSET-C-29, ASSET-C-30 |
| T-AAL-02 | Internal Overload DoS attack targeting AAL services | All | Insecure AAL APIs and interfaces  Lack authentication and authorization | ASSET-D-33 to ASSET-D-38 | ASSET-C-29, ASSET-C-30 |
| T-AAL-03 | Fail to clear resources | All | Insecure AAL APIs  Flaws in AAL design  Lack of secure deletion of data after process termination | ASSET-D-33 to ASSET-D-38 | ASSET-C-29, ASSET-C-30 |
| T-AAL-04 | HAM compromise | All | Insecure HAM APIs  Flaws in HAM design  Lack of access control | ASSET-D-33 to ASSET-D-38 | ASSET-C-29, ASSET-C-30 |
| T-AAL-05 | Malicious memory accesses | All | Insecure AAL APIs  Flaws in AAL design  Unrestricted memory access  Lack of access control | ASSET-D-33 to ASSET-D-38 | ASSET-C-29, ASSET-C-30 |
| T-AAL-06 | Firmware attacks | All | Weak accelerator design  Misconfiguration  Insecure AAL/HAM APIs | ASSET-D-33 to ASSET-D-38 | ASSET-C-29, ASSET-C-30 |
| T-O-CLOUD-ID-01 | ID reuse in O-Cloud's object lifecycle | All | Insufficient data cleanup  Weak isolation mechanisms  Inadequate monitoring and Logging  Lack of ID randomization  Inefficient access controls  No Timestamping or Versioning  Lack of notification mechanisms | ASSET-D-14, ASSET-D-15, ASSET-D-18, ASSET-D-29 | ASSET-C-08 |
| T-O-CLOUD-ID-02 | Node redundancy in O-Cloud deployments | All | Inadequate decommissioning procedures  Weak identity management  Insufficient data cleanup  No state verification  Lack of Resource Auditing  Lack of notification mechanisms  Inadequate monitoring and Logging | ASSET-D-14, ASSET-D-15, ASSET-D-18, ASSET-D-29 | ASSET-C-08 |
| T-O-CLOUD-ID-03 | O-Cloud ID mismanagement | All | Predictable ID Generation  Lack of ID validation  Inefficient synchronization  No ID revocation mechanism  Inadequate access controls  Lack of Namespace Segregation | ASSET-D-14, ASSET-D-15, ASSET-D-18, ASSET-D-29 | ASSET-C-08 |
| T-OPENSRC-01 | Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack | All | * 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 | All | All |
| T-OPENSRC-02 | A trusted developer intentionally inserts a backdoor into an open source code O-RAN component | All | Bugs in open source software caused by mistakes and human error | All | All |
| T-PHYS-01 | An intruder into a site gains physical access to O-RAN components to cause damage or access sensitive data | All except Script kiddies | * Improper physical security protection of data centres, PNFs, operation areas, etc. * Improper protection to power outages (power supply) * Improper protection against environmental disasters * Improper maintenance and monitoring of hardware parameters * Hardware backdoor | All | All |
| 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 | All except Script kiddies | Physical access to the open Fronthaul cable network | ASSET-D-01, ASSET-D-02, ASSET-D-04, ASSET-D-05 | O-RU, O-DU |
| T-RADIO-01 | Disruption through radio jamming, sniffing and spoofing | All except Script kiddies | Weakness of wireless cellular communications | ASSET-D-06 | UE, O-RU, O-DU |
| T-RADIO-02 | DoS attacks on cognitive radio networks | All except Script kiddies | Weakness of wireless cellular communications | ASSET-D-06 | UE, O-RU, O-DU |
| T-ML-01 | Poisoning the ML training data (Data poisoning attacks) | All | Lack of or improper access control to the ML model | ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28 | Near-RT RIC, Non-RT RIC, xAPPs, rApps |
| T-ML-02 | Altering a machine learning model (System manipulation and compromise of ML data confidentiality and privacy) | All | Lack of or improper access control to the ML model | ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28 | Near-RT RIC, Non-RT RIC, xAPPs, rApps |
| T-ML-03 | Transfer learning attack | All | Use of pretrained public ML model | ASSET-D-25, ASSET-D-26, ASSET-D-27, ASSET-D-28 | Near-RT RIC, Non-RT RIC, xAPPs, rApps |
| T-E2-01 | Untrusted Near-RT-RIC and E2 Nodes | All | weak mutual authentication | ASSET-C-40 | E2 interface |
| T-E2-02 | Malicious actor monitors messaging across E2 interface | All | Missing or weak confidentiality protection | ASSET-C-40 | E2 interface |
| T-E3-03 | Malicious actor modifies messaging across E2 interface | All | Lack of integrity verification | ASSET-C-40 | E2 interface |
| T-Y1-01 | Untrusted Near-RT-RIC and Y1 consumers | All | weak mutual authentication | ASSET-C-42 | Y1interface |
| T-Y1-02 | Malicious actor monitors messaging across Y1 interface | All | Missing or weak confidentiality protection | ASSET-C-42 | Y1 interface |
| T-Y1-03 | Malicious actor modifies messaging across Y1 interface | All | Lack of integrity verification | ASSET-C-42 | Y1 interface |

# Security principles

This clause elucidates security principles that an O-RAN system should achieve. They provide high level and abstract statement of the intended solution to countering potential Threats. Each security principle references applicable ZT tenets.

## Principles (SP)

### SP-AUTH Mutual Authentication

* Mutual authentication SHOULD be established to allow the O-RAN system verifying who performs what, thus possible to detect fake base stations, unauthorized or malicious components, malicious applications and malicious users/administrators.
* ZT Tenets: ZT-2, ZT-3, ZT-4, ZT-6

### SP-ACC Access Control

* The O-RAN system SHOULD forbid unauthorized administrators or components to access O-RAN resources or services anytime and anywhere. Access controls are required for:
  + Network Access Controls for filtering unauthorized/unexpected traffic in the O-RAN components over their interfaces.
  + Access controls to restrict access to component configurations.
  + Access controls for hardware to maintain the trust chain.
* ZT Tenets: ZT-3, ZT-4, ZT-6

### SP-CRYPTO Secure cryptographic, key management and PKI

* Well-known, standardized, secure and unbroken cryptographic schemes and protocols SHOULD be used. Proprietary schemes and protocols SHOULD be avoided.
* A secure key management of O-RAN keys (KgNB, KRRC-enc, KRRC-int, KUP-int, and KUP-enc, ksn) SHOULD be implemented to manage all the steps of key lifecycle: key generation using an appropriate level of entropy from a reliable source, secure key storage, key rotation and revocation, secure key destruction, etc.
* Reliable PKI for authentication and data encryption SHOULD be used. Public CAs SHOULD be supported. The certificates SHOULD be issued by a trusted or rooted Certificate Authority (CA). The CA implements the Certificate Policy which specifies the rules and policies about who may or may not receive a Certificate. Relying parties can access the Certificate Policy to determine what validation/verification checks were performed prior to certificate issuance.
* Each O-RU SHOULD be configured with lists of algorithms which are allowed for usage. There SHOULD be one list for integrity algorithms, and one for ciphering algorithms. These lists SHOULD be ordered according to a priority decided by the operator.

### SP-TCOMM Trusted Communication

* Integrity, confidentiality, availability, authenticity and replay protection of resources SHOULD be ensured in transit (see ‘Critical Assets’, clause 6.3) over O-RAN interfaces.
* ZT Tenets: ZT-2

### SP-SS Secure storage

* Integrity, confidentiality, availability protection of O-RAN resources SHOULD be ensured at rest (see ‘Critical Assets’, clause 6.3).

### SP-SB Secure boot and self-configuration

* O-RAN components SHOULD secure their firmware and configuration to provide the opportunity for trust to be extended higher in the software stack. Verified platform firmware can, in turn, verify the operating system (OS) boot loader, which can then verify other software components all the way up to the OS itself, the hypervisor or container runtime layers and O-RAN components. The transitive trust SHOULD be consistent with the concept of the chain of trust (CoT)-a method where each piece of code in the boot process measures and checks the signature of the next stage of the boot process before the software boots.
* The secure boot process, signature verification and self-configuration SHOULD be securely implemented for all O-RAN components to authenticate them before loading.

### SP-UPDT Secure Update

* A secure update management process SHOULD be implemented for introducing a new component or software change into the O-RAN system. The process SHOULD consider the ability to update the cryptographic algorithms and to adapt to upcoming O-RAN security challenges. A timely update cycles if vulnerabilities are discovered SHOULD be in place.
* ZT Tenets: ZT-5

### SP-RECO Recoverability & Backup

* A recoverability process to recovery in case of denial of service SHOULD be implemented. An approach for detecting and mitigating DoS attacks SHOULD be in place.
* O-RAN vendors SHOULD define a recovery plan that resets the O-RAN components to a trustworthy state in case of a malfunction or an attack (e.g. DoS).
* Backup systems SHOULD be in place to allow data or component on the O-RAN to be secured. Backup systems SHOULD ensure a suitable level of data or component availability and reliability.
* ZT Tenets: ZT-7

### SP-OPNS Security management of risks in open-source components

* Vendors using open-source code SHOULD enhance its security by applying industry coding best practices. It is recommended that vendors practice a higher level of due diligence for exposure to public exploits when using Open-Source code.
* A Software Bill of Materials (SBOM) SHOULD be maintained to track which open-source components are in use and where.
* Security Analysis (Audit, vulnerability scan, etc.) SHOULD be performed to ensure all identified components are free of security vulnerabilities.
* A proper policy and process SHOULD be in place for identifying and patching known issues with the open-source components. Open-source software components SHOULD be kept up to date and patched.
* ZT Tenets: ZT-5

### SP-ASSU Security Assurance

* Mobile networks are classified as critical infrastructure making security assurance especially more than relevant:
  + Vendors SHOULD ensure and prove that its software or hardware meets 3GPP Security Assurance Specifications (SCAS).
  + Vendors SHOULD ensure and prove that its software or hardware fulfils O-RAN security tests, requirements and recommendations provided by O-RAN alliance.
  + Vendors SHOULD ensure and prove that their software or hardware meets the needs of many national and international cybersecurity regulations, such as the Cyber Act, GDPR, etc.
  + Vendors SHOULD provide risk assessment, secure code review, penetration testing, vulnerability analysis and hardening guidelines for their O-RAN components.

### SP-PRV Privacy

* In O-RAN, the privacy of end users SHOULD be considered. The privacy of end users can be divided into data privacy, identity privacy and personal information privacy. Most Communication services are to gather data and personal information around end users, which may reveal information sensitive to their privacy. Adversaries would further extract more personal information about end users, such as UE priority, location information, trajectory, and preference.

### SP-SLC Continuous security development, testing, logging, monitoring and vulnerability handling

* Continuous development and continuous integration (CD/CI) with continuous regression testing and software security auditing SHOULD be implemented.
* Relevant activities events SHOULD be logged and logs collected SHOULD be analyzed in real time for the identification of potential security attacks and for security auditing.
* Continuous monitoring SHOULD be implemented to verify that the wanted security state is maintained throughout the lifecycle of deployed O-RAN components.
* Vulnerability management SHOULD be in place with intelligence to continuously track, identify and remediate vulnerable applications. Vendors SHOULD keep track of any new vulnerabilities discovered and is ready to act on customer product security incidents and reported security issues affecting O-RAN components.
* ZT Tenets: ZT-7

### SP-ISO Robust Isolation

* In a multi-vendor environment, intra-domain host isolation SHOULD be enforced. In the same host, VMs, CNs, virtualization/container layer, CPU, storage, and network security isolation of resources SHOULD be ensured by implementing system security orchestration, segmentation, lifecycle management, time scheduling, monitoring and audit on the management, signaling, control and data planes, and the execution of virtualized O-RAN components.

### SP-PHY Physical security

* The O-RAN system SHOULD be located at physically secure environment in a way that minimizes the risk of resource theft and destruction. It SHOULD support secure storage of sensitive data (cryptographic keys and configuration data), execution of sensitive functions (encryption/decryption, authentication), and execution of boot and update processes.
* Special attention SHOULD be paid to the site intrusion and physical access threats against O-RU sites. Consequently O-RU equipment SHOULD disable all unnecessary physical and logical ports, protocols and interfaces. In addition, secure physical connections to O-RU for O&M operations SHOULD be implemented (e.g. secure laptop with secure credentials).

### SP-CLD Secure cloud computing and virtualization

* Defense methods SHOULD be implemented: virtual machine-based intrusion detection, virtual machine-based isolation, virtual machine-based kernel protection, virtual machine-based access control, and virtual machine-based trusted computing.

### SP-ROB Robustness

* The O-RAN system SHOULD not only ensure the robustness of software or hardware resources, but also guarantee the robustness of the cognitive radio channel for meeting the QoS of communication services required by users. In some scenarios, the robustness of spectrum sensing SHOULD be enhanced when some sensing nodes (e.g., O-RU) easily malfunction. Robustness is an essential consideration for overcoming the security threats caused by jamming, DoS or DDoS attacks.

### SP-IDM O-Cloud ID secure management

* To counter threats associated with ID reuse, mismanagement, and redundancy, the O-Cloud should employ robust strategies for ID generation, validation, and lifecycle management. Properly managed IDs reduce risks of data inconsistencies, unauthorized access, and operational inefficiencies.

## Coverage Threats - Security principles

The table below illustrates how threats are covered by security principles. It outlines the list of security principles contributing to counter threats.

Table 8‑1 : Coverage Security principles-Threats (1/2)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SP |  |  |  |  | Threats | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|  | T-O-RAN-01 | T-O-RAN-02 | T-O-RAN-03 | T-O-RAN-04 | T-O-RAN-05 | T-O-RAN-06 | T-O-RAN-07 | T-O-RAN-08 | T-O-RAN-09 | T-FRHAUL-01 | T-FRHAUL-02 | T-MPLANE-01 | T-SPLANE-01 | T-SPLANE-02 | T-SPLANE-03 | T-SPLANE-04 | T-SPLANE-05 | T-CPLANE-01 | T-CPLANE-02 | T-UPLANE-01 | T-ORU-01 | T-NEAR-RT-01 | T-NEAR-RT-02 | T-NEAR-RT-03 | T-NEAR-RT-04 | T-NONRTRIC-01 | T-NONRTRIC-02 | T-NONRTRIC-03 | T-xAPP-01 | T-xAPP-02 | T-xAPP-03 | T-xAPP-04 | T-rAPP-01 | T-rAPP-02 | T-rAPP-03 | T-rAPP-04 | T-rAPP-05 | T-rAPP-06 | T-rAPP-07 | T-PNF-01 | T-SMO-01 | T-SMO-02 | T-SMO-03 |
| SP-AUTH |  |  | x |  |  | x |  |  |  | x | x | x | x | x | x | x | x | x | x |  |  |  | x | x | x | x |  |  | x | x | x | x | x | x | x | x | x | x | x |  | x |  |  |
| SP-ACC |  |  | x |  |  | x |  |  |  | x | x | x | x | x | x | x | x | x | x |  |  |  |  | x | x | x |  |  | x | x | x | x | x | x | x | x | x | x | x |  |  | x |  |
| SP-CRYPTO |  | x | x |  | x | x |  | x |  | x | x | x | x | x | x | x | x | x | x |  | x |  | x | x | x | x |  |  | x | x | x | x | x | x | x | x | x | x | x |  |  |  |  |
| SP-TCOMM |  |  |  |  | x |  |  | x |  | x | x | x | x | x | x | x | x | x | x |  | x |  |  | x | x |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |
| SP-SS |  |  |  |  |  |  | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| SP-SB |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  | x | x |  |  |  | x | x | x | x | x | x | x | x | x | x | x | x | x | x |  |  |  |
| SP-UPDT | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  | x | x | x | x | x | x | x | x | x | x | x |  | x | x | x |
| SP-RECO |  |  |  | x |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | x | x | x | x | x | x | x | x | x | x |  |  |  | x |
| SP-OPNS |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  | x |  | x | x |  |  |  | x | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| SP-ASSU | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |  |  | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| SP-PRV |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  | x |  | x | x | x | x |  | x | x |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |
| SP-SLC | x |  |  |  |  |  | x |  | x |  |  |  |  |  |  |  |  |  |  | x |  | x | x |  |  | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x | x |
| SP-ISO |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  | x | x |  |  |  | x | x | x | x | x | x | x | x | x | x | x | x | x |  |  |  |  |
| SP-PHY |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x |  |  |  |
| SP-CLD |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | x | x |  |  |  | x | x | x | x | x |  | x | x | x | x | x | x | x |  |  |  |  |
| SP-ROB |  |  |  | x |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

Table 8‑2 : Coverage Security principles-Threats (2/2)

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SP | | | | | |  | |  | | | | | |  | | | | | | |  | | | | | |  | | | | | |  | | | | | | |  | | | | | | Threats | | | | | |
|  | T-GEN-01 | T-GEN-02 | T-GEN-03 | T-GEN-04 | T-GEN-05 | | T-GEN-06 | | T-VM-C-01 | T-VM-C-02 | T-VM-C-03 | T-VM-C-04 | T-VM-C-05 | | T-VM-C-06 | T-IMG-01 | T-IMG-02 | T-IMG-03 | T-IMG-04 | T-VL-01 | | T-VL-02 | T-VL-03 | T-O2-01 | T-OCAPI-01 | T-HW-01 | | T-HW-02 | T-ADMIN-01 | T-ADMIN-02 | T-AAL-01 | T-AAL-02 | | T-AAL-03 | T-AAL-04 | T-AAL-05 | T-AAL-06 | T-O-CLOUD-ID-01 | T-O-CLOUD-ID-02 | | T-O-CLOUD-ID-03 | T-OPENSRC-01 | T-OPENSRC-02 | T-PHYS-01 | T-PHYS-02 | | T-RADIO-01 | T-RADIO-02 | T-ML-01 | T-ML-02 | T-ML-03 | |
| SP-AUTH | x | x | x | x | x | |  | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  |  |  |  |  | |  |  | x | x | x | |
| SP-ACC | x | x | x | x | x | | x | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  |  |  |  |  | |  |  | x | x | x | |
| SP-CRYPTO | x | x | x | x | x | | x | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x |  |  | |  |  |  |  |  |  | |  |  |  |  |  | |  |  | x | x | x | |
| SP-TCOMM |  |  |  |  |  | |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |
| SP-SS | x | x | x | x | x | | x | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  |  |  |  |  | |  |  |  |  |  | |
| SP-SB | x | x | x | x | x | |  | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  |  |  |  |  | |  |  | x | x | x | |
| SP-UPDT | x | x | x | x | x | |  | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  | x | x |  |  | |  |  | x | x | x | |
| SP-RECO | x | x | x | x | x | |  | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  |  |  |  |  | |  |  | x | x | x | |
| SP-OPNS | x | x | x | x | x | | x | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x |  |  | |  |  |  |  |  |  | |  | x | x |  |  | |  |  |  |  |  | |
| SP-ASSU | x | x | x | x | x | |  | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  | x | x | x | x | | x | x | x | x | x | |
| SP-PRV |  |  |  |  |  | |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |
| SP-SLC | x | x | x | x | x | |  | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  | x | x |  |  | |  |  | x | x | x | |
| SP-ISO | x | x | x | x | x | | x | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  |  |  |  |  | |  |  | x | x | x | |
| SP-PHY |  |  |  |  |  | |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  | x | x | |  |  |  |  |  | |
| SP-CLD | x | x | x | x | x | | x | | x | x | x | x | x | | x | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x | x | | x | x | x | x |  |  | |  |  |  |  |  | |  |  | x | x | x | |
| SP-ROB |  |  |  |  |  | |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  | | x | x |  |  |  | |
| SP-  IDM |  |  |  |  |  | |  | |  |  |  |  |  | |  |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  | x | x | | x |  |  |  |  | |  |  |  |  |  | |

# Risk assessment

After identifying the list of assets, threats and vulnerabilities, the next step is the risk assessment. The main concepts of risk assessment are illustrated in the following figure.



Figure 9‑1 : Main concepts of risk assessment

The criticality of the identified threats in clause 7.4 were assessed based on the severity (consequence) and the likelihood of occurrence. Indications of severity level for each threat are given whether they are considered as high, medium, or low. This severity is a global perception of the risk based on its impacts. In practice, it varies strongly depending on the use cases and deployment/configuration models of the O-RAN system.

Moreover, the type of loss (availability, integrity and/ or confidentiality) has been assessed for each threat.

## Determination of severity level process

The process followed to determine the severity level resulting from threats that successfully exploit vulnerabilities is based on Table 9-1 which includes the definition in terms of Privacy, Confidentiality, Integrity, Availability of the three severity levels ‘Low’, ‘Medium’ and ‘High’ shown here as green, yellow and red.

Table 9-1 defines what “low,” “medium” and “high” means.

The severity of an impact is expressed as follows:

* Level of impact for various threats on the properties Privacy, Confidentiality, Integrity, and Availability
* Scale of impact, depending on the number of affected O-RUs and /or O-DUs.
* Scale of impact depending on the Clock Model and Synchronization Topology configurations LLS-C1, LLS-C2, LLS-C3 and LLS-C4 [10].
* Adverse impacts depending on whether or not existing requirments and controls are already defined in the O-RAN requirments specifications.

Table 9‑1 : Severity rating

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Severity level** | **Privacy** | **Confidentiality** | **Integrity** | **Availability** | **Number of affected O-RUs/O-DUs (Only for Threats on O-RU, O-DU, FH interface)** | **Clock Model and Synchronization Topology configurations (only for Threats on S-PLANE)** | **Adverse impacts** |
| Low | Disclosure of personal data which, with aggregation or processing, is unlikely to reveal unique subscriber’s identity. | Disclosure of information for internal use. No specific impact on its disclosure | Minor/Unnoticeable effect on system behavior/output | Brief Interruption in operations. (Estimated in secs/mins/hours) | One O-DU is affected with its related O-RU | DoS attacks on LLS-C2  DoS attacks on LLS-C4 | Already existing requirements and controls are defined in the O-RAN specifications to prevent, or at least significantly impede, the vulnerability from being exercised. Existing requirements and controls are only efficient to protect from both internal and external threats. |
| Medium | Disclosure of personal data (according to GDPR) which CAN be processed or aggregated to uniquely identify subscribers.  **NOTE**: Personal data in GDPR means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. | Disclosure of privileged information Access credentials/ configuration data, etc. | Alteration of some system functionality and features/output. | Short-term Interruption in operations. (Estimated in hours/Days) | One O-DU is affected with its related multiple O-RUs | DoS attacks on LLS-C1 | Already existing requirements and controls are defined in the O-RAN specifications to prevent, or at least significantly impede, the vulnerability from being exercised. Existing requirements and controls are only efficient to protect from external threats. |
| High | Disclosure of sensitive personal data (GDPR special category).  **NOTE**: Special data category in GDPR: data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation. | Disclosure of high value information, trade secrets, IP, mission critical data, master-keys, etc. | Complete change in normal System functioning | Prolonged interruption of operations. (Estimated in days/Weeks) | Several O-DUs and O-RUs are affected | DoS attacks on LLS-C3 | No existing requirements and controls in the ORAN specifications yet to protect from internal and/or external threats |

**NOTE 1**: The severity level depends on the number of affected RUs and O-DUs. The severity level is consequently 'Low' in case of one affected O-RU, 'Medium' in case of one affected O-DU with its related multiple O-RUs, and 'High' for multiple affected O-DUs-O-RUs. Operators conducting a full risk analysis according to this report should conduct a use case-based analysis taking into account the likelihood and the real deployment of the O-RAN system.

**NOTE 2**:

**Configuration LLS-C1**

In LLS-C1, the network timing is distributed from O-DU to O-RU via direct connection between O-DU site and O-RU site. O-DU is acting as a master and directly synchronizes O-RU.

* DoS attacks against the master clock: There are two scenarios:

1.     Scenario 1: One O-RU is served by O-DU, therefore only one O-RU is affected. Consequently, the severity level is ‘Low’.

2.     Scenario 2: Multiple O-RUs are served by O-DU, therefore all those O-RUs are affected as the connection between O-DU and O-RU is point-to-point. Consequently, the severity level is ‘Low’.

**Configuration LLS-C2**

In LLS-C2, the network timing is distributed from O-DU to O-RU between O-DU sites and O-RU sites. One or more Ethernet switches are allowed in the fronthaul network. O-DU acting as master to distribute network timing toward O-RU.

* DoS attacks against the master clock within the O-DU may affect one or multiple O-RUs. In this configuration, a neighbor O-DU could act a backup and play the role of a master to distribute network timing to all the RUs belonging to the affected O-DU by reconfiguring the network of switches. Consequently, the severity level is ‘Low’.

**Configuration LLS-C3**

Frequency and time distribution is made by the fronthaul network itself (not by the O-DU). One or more PRTC/T-GM are implemented in the fronthaul network to distribute network timing toward O-DU and O-RU.

* DoS attacks against the master clock within the fronthaul network may affect multiple O-DUs with their related O-RUs. Consequently, the severity level is ‘High’.

**Configuration LLS-C4**

Local PRTC timing that provides time synchronization to the O-RU (it could be embedded in the O-RU).

* DoS attacks against the master clock may affect only one O-RU. Consequently, the severity level is ‘Low’.

According to what we described in the here above two notes, T-SPLANE-01 has been split in Table 9-4 according to the Clock Model and Synchronization Topology configurations C1, C2, C3, and C4.

**NOTE**: Adverse impacts: This factor depends on the normative O-RAN security requirements in the security requirements specification. For a threat without any requirement in front of it, the adverse impacts level is High. It is Medium or Low for a threat with related security requirements (see column ‘Assupltions’) helping in reducing its impact.

## Determination of likelihood level process

The process followed to determine the likelihood level resulting from threats that successfully exploit vulnerabilities is based on Table 9-2 which includes the relevant factors that are considered. For each factor, three levels ‘Low’, ‘Medium’ and ‘High’ are shown in Table 9-2 as green, yellow and red.

Table 9-2 defines what “low,” “medium” and “high” means.

The likelihood level is expressed by four factors as follows:

* Adverse impacts: This factor depends on the existing normative O-RAN security requirements and controls. For example, the level is high in case no available O-RAN security requirements and controls in the O-RAN security specifications. In the risk assessment Table 9-4 in the column ‘Assumptions’, some of the agreed security controls by the O-RAN alliance have been stated for some threats as arguments for justifying the likelihood levels ‘Low’ or ‘Medium. This means that the likelihood level is estimated at Low’ or ‘Medium’, provided that the security controls are in place.

**NOTE**: This factor is used to determine the likelihood level for the most categories of threats. It is also used as a relevant factor for severity for some categories of threats, in particular the O-Cloud threats category.

* Threat event initiation: This factor takes into consideration the capabilities that attackers possess and the potential entry points to exploit a vulnerability and initiate an attack. For example, it is high if an attack can be initiated from internet or untrusted network.
* Exposure: This factor is related to the number of external interfaces and/or services that are exposed to an attacker.
* Zero Trust Approach: Likelihood scoring considers a zero-trust architecture which protects against internal threat actors. Likelihood scores are higher for a zero-trust architecture (ZTA) because internal threats should be considered in addition to external threats. In a ZTA it cannot be assumed that perimeter defense is sufficient. As a result, scored Likelihood = Medium, at a minimum. Reconnaissance type attacks can be scored Likelihood = High while damaging/availability attacks can be scored Likelihood = Medium. The reason is that threat actors are less likely to perform damaging attacks that are quickly and easily detected. Advanced Persistent Threats (APTs) typically move laterally in anonymous fashion to prevent detection while providing reconnaissance (see O-RAN.SFG.Non-RT-RIC-Security-TR-v01.00).

Table 9‑2 : Likelihood rating

|  |  |  |
| --- | --- | --- |
| **Scale** | **Factors** | **Measure of Likelihood** |
| **High** | **Adverse impacts** | **No existing requirements and controls in the ORAN specifications yet to protect from internal and/or external threats** |
| **Threat event initiation** | **Attack can be launched from the internet or untrusted network** |
| **Exposure** | **System has a large amount of exposed interfaces (e.g. ORAN interfaces, multiple O-DU, multiple O-RU, multi administrators/customers)** |
| **ZTA** | **Reconnaissance type attacks** |
| **Open-source/COTS support** | * **No vulnerability handling and patch management in place: Several CVE have already been discovered; no regular patches provided to fix the detected vulnerabilities** * **Use of open-source module not supported by a broader community** * **Use of non popular COTS product** |
| **Medium** | **Adverse impacts** | **Already existing requirements and controls are defined in the O-RAN specifications to prevent, or at least significantly impede, the vulnerability from being exercised. Existing requirements and controls are only efficient to protect from external threats.** |
| **Threat event initiation** | **Malicious user needs to have direct access to the target system** |
| **Exposure** | **System has a medium amount of exposed interfaces (e.g. ORAN interfaces, one O-DU, multiple O-RU)** |
| **ZTA** | **Damaging/availability type attacks** |
| **Open-source/COTS support** | * **Vulnerability handling and patch management in place but not efficient: Several CVE have already been discovered; no timely patches provided to fix the discovered vulnerabilities** * **Use of open-source module moderately supported by a broader community** |
| **Low** | **Adverse impacts** | **Already existing requirements and controls are defined in the O-RAN specifications to prevent, or at least significantly impede, the vulnerability from being exercised. Existing requirements and controls are only efficient to protect from both internal and external threats.** |
| **Threat event initiation** | **The malicious user needs to have administrative or elevated privileges in the target system (external having internal privileges or internal having internal privileges)** |
| **Exposure** | **Slightly exposed to external systems (e.g. one O-DU, one O-RU) (least privilege approach)** |
| **ZTA** | **Perimeter defenses are sufficient. No potential for internal threats** |
| **Open-source/COTS support** | * **Component supporting open-source module: a broader community is investing in** * **COTS modules are popular and widely used in critical infrastructure** |

## Evaluation of the risks process

The following risk assessment matrix is used to assess the risk score. The matrix takes as input two estimated qualitative inputs: (i) likelihood and (ii) the severity. One axis representing the probability of a risk scenario occurring and the other representing the damage it will cause (Severity). In the middle, you have scores based on their combined totals.

Using this formula RISK= Severity x Likelihood by a simple multiply the severity and likelihood scores to obtain the final risk score as shown in Table 9-3.

For example, if the estimated likelihood of a threat is low and the corresponding severity is high, then the risk is medium.

Table 9‑3 : Risk assessment matrix

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Severity** | 3-High | 3-Medium | 6-High | 9-High |
| 2-Medium | 2-Low | 4-Medium | 6-High |
| 1-Low | 1-Low | 2-Low | 3-Medium |
|  |  | 1-Low | 2-Medium | 3-High |
|  |  | **Likelihood** | | |

## Risk assessment output

The following is the risk assessment output table which illustrates the different threats along with their impacts, the type of loss, the perceived severity/likelihood levels and the risk scoring.

Table 9‑4 : Risk Assessment

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **THREAT ID** | **RISK DESCRIPTION** | **IMPACT DESCRIPTION** | **CIA** | **SEVERITY LEVEL** | **Likelihood LEVEL** | **Applied factors** | **Rationale** | **Considered Assumptions** | **Risk Score** |
| T-O-RAN-01(NEAR RT RIC) | An attacker exploits insecure designs or lack of adoption of security controls (e.g. hardening) in O-RAN components causing: - Loss of service - Privacy issues - Performance issues in the system in O-RAN components | Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data | C, I, A | High | High | • Exposure (High): A1, O1, E2, xApps, rApps • Adverse impacts (High) | O-Cloud security hardening requirements have not been specified yet and it is unclear whether the industry practices sufficiently cover the threats outlined.  O-RAN Alliance has specified security for O-RAN interfaces at the transport layers thereby mitigating access to O-RAN functions through the interfaces. The O-RAN Alliance has not yet specified security for protecting the platforms that host the O-RAN functions from physical or remote access. |  | High |
| T-O-RAN-01 (Non RT RIC + SMO) | An attacker exploits insecure designs or lack of adoption of security controls (e.g. hardening) in O-RAN components causing: - Loss of service - Privacy issues - Performance issues in the system in O-RAN components | Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data | C, I, A | High | High | • Exposure (High): A1, O1, O2, rApps • Adverse impacts (High) | O-Cloud security hardening requirements have not been specified yet and it is unclear whether the industry practices sufficiently cover the threats outlined.  O-RAN Alliance has specified security for O-RAN interfaces at the transport layers thereby mitigating access to O-RAN functions through the interfaces. The O-RAN Alliance has not yet specified security for protecting the platforms that host the O-RAN functions from physical or remote access. |  | High |
| T-O-RAN-01 (O-CU) | An attacker exploits insecure designs or lack of adoption of security controls (e.g. hardening) in O-RAN components causing: - Loss of service - Privacy issues - Performance issues in the system in O-RAN components | Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data | C, I, A | High | High | • Exposure (High): O1, E2, administration interfaces • Adverse impacts (High) | O-Cloud security hardening requirements have not been specified yet and it is unclear whether the industry practices sufficiently cover the threats outlined.  O-RAN Alliance has specified security for O-RAN interfaces at the transport layers thereby mitigating access to O-RAN functions through the interfaces. The O-RAN Alliance has not yet specified security for protecting the platforms that host the O-RAN functions from physical or remote access. |  | High |
| T-O-RAN-01 (O-DU) | An attacker exploits insecure designs or lack of adoption of security controls (e.g. hardening) in O-RAN components causing: - Loss of service - Privacy issues - Performance issues in the system in O-RAN components | Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data | C, I, A | High | High | • Exposure (High): E2, O1, FH • Adverse impacts (High) | O-Cloud security hardening requirements have not been specified yet and it is unclear whether the industry practices sufficiently cover the threats outlined.  O-RAN Alliance has specified security for O-RAN interfaces at the transport layers thereby mitigating access to O-RAN functions through the interfaces. The O-RAN Alliance has not yet specified security for protecting the platforms that host the O-RAN functions from physical or remote access. |  | High |
| T-O-RAN-01 (O-RU) | An attacker exploits insecure designs or lack of adoption of security controls (e.g. hardening) in O-RAN components causing: - Loss of service - Privacy issues - Performance issues in the system in O-RAN components | Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data | C, I, A | High | High | • Exposure (High): FH, O1, physical • Adverse impacts (High) | O-Cloud security hardening requirements have not been specified yet and it is unclear whether the industry practices sufficiently cover the threats outlined.  O-RAN Alliance has specified security for O-RAN interfaces at the transport layers thereby mitigating access to O-RAN functions through the interfaces. The O-RAN Alliance has not yet specified security for protecting the platforms that host the O-RAN functions from physical or remote access. |  | High |
| T-O-RAN-02 | An attacker exploits misconfigured or poorly configured O-RAN components causing: - Loss of service - Privacy issues - Performance issues in the system | Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data | C, I, A | High | High | • Threat event initiation (High) • Adverse impacts (High) | O-Cloud security hardening requirements have not been specified yet and it is unclear whether the industry practices sufficiently cover the threats outlined. |  | High |
| T-O-RAN-03 | Attacks from the internet exploit weak authentication and access control to penetrate O-RAN network boundary, causing: - Flooding of the network - loss of service, performance issues - Unauthorized access to ORAN components | Denial of service for component access and/or function/service offered; Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data; | C, I, A | High | Medium | • Threat event initiation (High) • Adverse impacts (Medium) | O-RAN Alliance has not specified yet any xApp security measures around the Onboarding onto SMO and deployment onto Near RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for xApps yet. This attack to be performed requires multiple steps to be achieved by an attacker. | The O-RAN network elements should not be exposed to untrusted/ internet end points without network access control. | High |
| T-O-RAN-04 | An attacker attempts to flooding the airlink signal (legitimate communications) through IoT devices causing: - Loss of service | Denial of service for component access and/or function/service offered | A | Medium | High | • Threat event initiation (High) • Adverse impacts (High) | O-RAN Alliance has not specified yet any security measures on flooding attacks through IoT devices. |  | High |
| T-O-RAN-05 | An attacker penetrates and compromises the O-RAN system through the open O-RAN’s Fronthaul, O1, O2, A1, and E2 | Data tampering and information disclosure; Denial of service from within for component access and/or function/service offered; Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data; | C, I, A | High | Medium | • Threat event initiation (Medium) • Adverse impacts (Medium) | Existing controls are in place (moderately satisfactory), Malicious user needs to have direct (physical) access to the target system |  | High |
| T-O-RAN-06 | An attacker exploits insufficient/improper mechanisms for authentication and authorization to compromise O-RAN components | Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data | C, I, A | High | High | • Threat event initiation (High) • Adverse impacts (Medium) | Existing controls are in place (moderately satisfactory), Attack can be launched from the internet or untrusted network | Authentication procedures are in place | High |
| T-O-RAN-07 | An attacker compromises O-RAN monitoring mechanisms and log files integrity and availability | Compromise of availability and integrity of security event log files could conduct to delays, wrong audit results, delays in security restoration, threats persistence. | I, A | Medium | Medium | • Threat event initiation (Medium) • Adverse impacts (Medium) | Existing controls are in place (moderately satisfactory), Malicious user needs to have administrative or elevated privileges in the target system. It is a likely scenario after initial compromise of network elements. | Authentication procedures , patch management regular programmed update, vulnerability handling/regular scanning, SBOM are in place | Medium |
| T-O-RAN-08 | An attacker compromises O-RAN data integrity, confidentiality and traceability | An attacker could, in such case, data tampering, information disclosure, spoofing identity, elevation of privilege, etc. | C, I | Medium | Medium | • Threat event initiation (Medium) • Adverse impacts (Medium) | Existing controls are in place (moderately satisfactory). Likely scenario after initial compromise of network elements with local data storage. | Protection at rest (e.g. HSM) is in place (operator decision), | Medium |
| T-O-RAN-09 | An attacker compromises O-RAN components integrity and availability | An attacker could, in such case, cause denial-of-service, data tampering, information disclosure, spoofing identity, etc. | I, A | High | Medium | • Threat event initiation (Medium) • Adverse impacts (Medium) | Existing controls are in place (moderately satisfactory), Malicious user needs to have direct access to the target system |  | High |
| T-FRHAUL-01 | An attacker penetrates O-DU and beyond through O-RU (bidding-down attack) | Data tampering and information disclosure; Denial of service from within for component access and/or function/service offered; Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data; | C, I, A | High | Medium | • Threat event initiation (Medium) • Adverse impacts (Medium) • Exposure (Medium) | System has an amount of exposed interfaces: multiple O-DU, multiple O-RU, FH interface. It is a possible attack, however needs physical access and sophistication to execute |  | High |
| T-FRHAUL-02 | Unauthorized access to the Open Front Haul Ethernet L1 physical layer interface (cables and connections) | It provides a means to launch attacks on the availability, integrity, and confidentiality of the Open Front Haul system. | C, I, A | High | Low | • Threat event initiation (Low) • Adverse impacts (Medium) | It is a possible attack, however needs physical access and sophistication to execute |  | Medium |
| T-MPLANE-01 | An attacker attempts to intercept the Fronthaul (MITM) over M Plane | Passive wiretapping and denial of service | C, A | Medium | Low | • Threat event initiation (Low) • Adverse impacts (Medium) | It is a possible attack, however needs physical access and sophistication to execute | TLS with PKI is supported, it is up to MNO, the likelihood is low provided that MNOs use TLS over the M-Plane | Low |
| T-SPLANE-01-C1 (one O-RU scenario) | DoS attack on an O-DU acting as master to distribute network timing toward O-RU based on point-to-point connection in LLS-C1. In this scenario, only one O-RU is connected to O-DU, therefore only that O-RU is affected. | This attack may cause performance degradation or interruption of services to only one O-RU that rely on accurate time from the affected O-DU. The severity level is consequently 'Low'. | A | Low | Low | • Exposure (Low) • Threat event initiation (Medium) | Slightly exposed to external systems: one O-RU. It is a possible attack, however needs physical access and sophistication to execute | Access control on the CUSM-Plane that mitigates unauthorized access by an insider are in place. 802.1x protocol is supported it can reduce the likelihood of this attack. | Low |
| T-SPLANE-01-C1 (multiple O-RUs scenario) | DoS attack on an O-DU acting as master to distribute network timing toward O-RU based on point-to-point connection in LLS-C1. In this scenario, multiple O-RUs are connected to O-DU, therefore those O-RUs are affected. | This attack may cause performance degradation or interruption of services to all the RUs that rely on accurate time from the affected O-DU. The severity level is consequently 'Medium'. | A | Medium | Medium | • Exposure (Medium) • Threat event initiation (Medium) | System has a medium amount of exposed interfaces: multiple O-RUs. It is possible attack, however needs physical access and sophistication to execute |  | Medium |
| T-SPLANE-01-C2 | DoS attack on an O-DU acting as master to distribute network timing toward O-RU in LLS-C2. One or more Ethernet switches are allowed between the central site (hosting O-DUs) and the remote sites (hosting O-RUs). | This attack may cause performance degradation or interruption of services to all the RUs that rely on accurate time from the affected O-DU. In this configuration, a neighbor O-DU could act a backup and play the role of a master to distribute network timing to all the RUs belonging to the affected O-DU by reconfiguring the network of switches. The severity level is consequently 'Low'. | A | Low | Medium | • Exposure (Medium) • Threat event initiation (Medium) | System has a medium amount of exposed interfaces. It is a possible attack, however needs physical access and sophistication to execute | Access control on the CUSM-Plane that mitigates unauthorized access by an insider are in place. 802.1x protocol is supported it can reduce the likelihood of this attack. | Low |
| T-SPLANE-01-C3 | DoS attack against a Master clock in the LLS-C3 configuration | In this configuration, the frequency and timing distribution is made by the fronthaul network (not by O-DU). DoS attack against a master clock may cause performance degradation or interruption of services to all the RUs and DUs that rely on accurate time from the affected master clock in the fronthaul network. The severity level is consequently 'High'. | A | High | Medium | • Exposure (Medium) • Threat event initiation (Medium) | System has a medium amount of exposed interfaces. It is a possible attack, however needs physical access and sophistication to execute |  | High |
| T-SPLANE-01-C4 | DoS attack against a Master clock in the LLS-C4 configuration | In this configuration, the time source could be locally embedded in the RU itself. DoS attack in the time source may cause performance degradation or interruption of services to only one O-RU where the time source is embedded. The severity level is consequently 'Low'. | A | Low | Low | • Exposure (Low) • Threat event initiation (Medium) | Slightly exposed to external systems: one O-RU. It is a possible attack, however needs physical access and sophistication to execute | Access control on the CUSM-Plane that mitigates unauthorized access by an insider are in place. 802.1x protocol is supported it can reduce the likelihood of this attack. | Low |
| T-SPLANE-02 | Impersonation of a Master clock (Spoofing) within a PTP network with a fake ANNOUNCE messages | Degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell. A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. | A | High | Low | • Threat event initiation (Medium) • Adverse impacts (Low) | Existing controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. It is a possible attack, however needs physical access and sophistication to execute | Access control on the CUSM-Plane that mitigates unauthorized access by an insider are in place. 802.1x protocol is supported it can reduce the likelihood of this attack. | Medium |
| T-SPLANE-03 | A Rogue PTP Instance wanting to be a Grand Master by sending manipulated/malicious ANNOUNCE messages declaring him to be the best clock in the network | Degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell. A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. | A | High | Low | • Threat event initiation (Medium) • Adverse impacts (Low) | Existing controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. It is a possible attack, however needs physical access and sophistication to execute | Access control on the CUSM-Plane that mitigates unauthorized access by an insider are in place. 802.1x protocol is supported it can reduce the likelihood of this attack. | Medium |
| T-SPLANE-04 | Selective interception and removal of PTP timing packets | Clock degradation in attacked nodes. Removing all packets or random packets may push the clocks in attacked nodes into free running mode. Degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell. A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. | A | High | Low | • Threat event initiation (Medium) • Adverse impacts (Low) | Existing controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. It is a possible attack, however needs physical access and sophistication to execute | Access control on the CUSM-Plane that mitigates unauthorized access by an insider are in place. 802.1x protocol is supported it can reduce the likelihood of this attack. | Medium |
| T-SPLANE-05 | Packet delay manipulation attack | Degradation in the accuracy of time may cause DoS to applications on all the RUs that rely on accurate time, potentially bringing down the cell. A cell outage caused by misaligned time, may further impact performance in connected neighboring cells. | A | High | Medium | • Threat event initiation (Medium) • Adverse impacts (Medium) | Existing controls are in place to prevent (moderately satisfactory). It is a possible attack, however needs physical access and sophistication to execute | 802.1x protocol is supported it can reduce the likelihood of this attack. | High |
| T-CPLANE-01 | Spoofing of DL C-plane messages | The lack of authentication could allow an adversary to inject own DL C-plane messages that falsely claiming to be from the associated O-DU.  As a result, it would block the O-RU to process the corresponding U-Plane packets, leading to temporarily DoS. (dropping the entire DL C-plane messages would achieve same goal) | A | Medium | Low | • Threat event initiation (Medium) • Adverse impacts (Low) | Existing controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. It is a possible attack, however needs physical access and sophistication to execute | 802.1x at the ethernet level ensures authentication and authorization for communication over FH interface, not sure that this control reduce the risk of spoofing of c-plane at a low level. Mitigations related to monitoring and configuration of network nodes are in place | Low |
| T-CPLANE-02 | Spoofing of UL C-plane messages | The lack of authentication could allow an adversary to inject own UL C-plane messages that falsely claiming to be from the associated O-DU. As a result, temporarily limited cell performance (or even DoS) on cells served by the O-RU and in addition a consequential threat to all O-RUs parented to that O-DU might exist. (dropping the entire UL C-plane messages would achieve same goal) | A | Medium | Low | • Threat event initiation (Medium) • Adverse impacts (Low) | Existing controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. It is a possible attack, however needs physical access and sophistication to execute | 802.1x at the ethernet level ensures authentication and authorization for communication over FH interface, not sure that this control reduce the risk of spoofing of c-plane at a low level. Mitigations related to monitoring and configuration of network nodes are in place | Low |
| T-UPLANE-01 | An attacker attempts to intercept the Fronthaul (MITM) over U Plane (PDCP protocol is used) | For the transported U-Plane data an attacker could potentially do threats, such as passive wiretapping , but would need to break PDCP Security prior to any content access. | C | Low | Low | • Threat event initiation (Medium) • Adverse impacts (Low) | Existing controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. It is a possible attack, however needs physical access and sophistication to execute | 802.1x protocol is supported it can reduce the likelihood of this attack. | Low |
| T-ORU-01-a | An attacker stands up a rogue O-RU (standalone) - a false base station | This opens the door to subscriber’s identity interception/disclosure and unauthorized user tracking attacks (privacy breach). | C, I | High | Medium | • Threat event initiation (Medium) • Adverse impacts (Medium) | Existing controls are in place to prevent (moderately satisfactory). It is a possible attack, however needs physical access and sophistication to execute | Security measures already defined by 3GPP, monitoring/detection mechanisms of a rogue ORU are in place | High |
| T-ORU-01-b | An attacker stands up a rogue O-RU attacking O-DU and beyond (core network) | It provides a means to launch attacks on the availability, integrity, and confidentiality of the Open Front Haul system, ODUs and beyond in the core network. | C, I | High | Low | • Threat event initiation (Medium) • Adverse impacts (Low) | Existing controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised. It is a possible attack, however needs physical access and sophistication to execute | 802.1x protocol is supported it can reduce the likelihood of this attack. | Medium |
| T-NEAR-RT-01 | Malicious xApps can exploit UE identification, track UE location and change UE priority | An xApp can receive order via A1 to control a certain UE and if a malfunctioning xApp receives an order to prioritize this UE, then the owner of the malfunctioning xApp knows a VIP that they want to track in a certain area. With this command exposure, the attacker can obtain a rough location of a very important person and change the order from prioritize to deprioritize for a UE; Interception of UE identifier | C, I | High | High | • Threat event initiation (High) • Adverse impacts (High) • Exposure (High) | O-RAN Alliance has not specified yet any xApp security measures around the Onboarding onto SMO and deployment onto Near RT-RIC. Further, there is no testing framework in place for xApps yet. |  | High |
| T-NEAR-RT-02 | Risk of deployment of a malicious xApp on Near-RT RIC | Deployment of malicious xApps may allow unauthorized access to E2 Nodes, abuse of radio network information, impact service, or exploit UE identification, location, and slice priority. | C, I | High | High | • Threat event initiation (High) • Adverse impacts (High) • Exposure (High) | O-RAN Alliance has not specified yet any xApp security measures around the Onboarding onto SMO and deployment onto Near RT-RIC. Further, there is no testing framework in place for xApps yet. |  | High |
| T-NEAR-RT-03 | Near-RT RIC APIs can be compromised and manipulated due to lack, incorrect or weak authentication mechanism | Near-RT RIC data around services and UEs can be eavesdropped. Unauthenticated APIs can be manipulated causing services disruptions in RAN network | C, A | High | High | • Threat event initiation (High) • Adverse impacts (High) • Exposure (High) | O-RAN Alliance has not specified yet any Near-RT RIC APIs measures. |  | High |
| T-NEAR-RT-04 | Resources and services provided by Near-RT RIC platform and xApps via APIs can be abused and/or misused | Near-RT RIC data around services and UEs can be eavesdropped by xApps without proper permissions. Abuse of resources and misuse of services can produce disruptions and/or outages in the network. | C, A | High | Medium | • Threat event initiation (High) • Adverse impacts (High) • Exposure (High) | O-RAN Alliance has not specified yet any Near-RT RIC APIs measures. |  | High |
| T-NONRTRIC-01 | An attacker gains access to the Non-RT RIC through the SMO to cause a denial of service or degrade the performance of the Non-RT-RIC | Non-RT RIC would not be able to: •monitor or trace the network to understand the effect of policy on performance in Near-RT RIC  •update A1 policy •provide exposure and secure delivery of A1 Enrichment Information to Near-RT RIC •setup access control rules and the selection of which Enrichment Information ID (EiId) is exposed to a near-RT RIC | A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any security measures around the authentication and access control to the Non RT-RIC. |  | High |
| T-NONRTRIC-02 | An attacker gains access to the Non-RT RIC through the SMO for UE tracking | Attacker has access to sensitive data and is able to track a UE | C | High | High | • ZTA (High) • Adverse impacts (High) | O-RAN Alliance has not specified yet any security measures around the authentication and access control to the Non RT-RIC. |  | High |
| T-NONRTRIC-03 | An attacker gains access to the Non-RT RIC through the SMO to cause Data Corruption/Modification | A malicious actor who gains unauthorized access to the Non-RT-RIC can modify policy to pass a “False Policy” to the Near-RT-RIC to degrade performance or cause an outage. | C | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any security measures around the authentication and access control to the Non RT-RIC. |  | High |
| T-xAPP-01 | An attacker exploits xApps vulnerabilities and misconfiguration | If attackers can find exploitable xApp, they can disrupt the offered network service and potentially take over another xApp or the whole near-RT RIC.  The actual consequences may vary. For example, an attacker may gain the ability to alter data transmitted over A1 or E2 interfaces, extract sensitive information, etc. | C, I, A | High | High | • Threat event initiation (High) • Adverse impacts (High) • Exposure (High) | O-RAN Alliance has not specified yet any xApp security measures around the Onboarding onto SMO and deployment onto Near RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for xApps yet. |  | High |
| T-xAPP-02 | Conflicting xApps unintentionally or maliciously impact O-RAN system functions to degrade performance or trigger a DoS | An attacker can utilize a malicious xApp that intentionally triggers RRM decisions conflicting with the O-gNB internal decisions to create denial of service or performance degradation. | A | High | Medium | • Threat event initiation (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any xApp security measures around the Onboarding onto SMO and deployment onto Near RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for xApps yet. |  | High |
| T-xAPP-03 | An attacker compromises xApp isolation | Gaining unauthorized access to the underlying system provides new opportunities to exploit vulnerabilities in other xApps or O-RAN components to intercept and spoof network traffic, to degrade services (DoS), etc. | C, I, A | High | Medium | • Threat event initiation (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any xApp security measures around the Onboarding onto SMO and deployment onto Near RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for xApps yet. |  | High |
| T-xApp-04 | False or malicious A1 policies modify behavior of xApps | A malicious A1 policy can exploit xApp functionality to trigger a DoS, affect performance, or locate a subscriber. | I, A | High | Medium | • Threat event initiation (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any xApp security measures around the Onboarding onto SMO and deployment onto Near RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for xApps yet. This attack to be performed requires multiple steps to be achieved by an attacker. |  | High |
| T-rAPP-01 | Conflicting rApps impact O-RAN system functions to degrade performance or trigger a DoS | rApps in the Non-RT RIC performing different functions can be provided by different vendors. This creates the risk that different rApps will take conflicting decisions to set conflicting policies. This can result in performance degradation or outage. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any rApp security measures around the Onboarding onto SMO and deployment onto Non RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for rApps yet. |  | High |
| T-rAPP-02 | An attacker exploits rApp vulnerability for data breach or denial of service | Vulnerabilities can potentially exist in any rApp. If attackers can find exploitable rApp, they can disrupt the offered network service and potentially take over another rApp or the non-RT RIC. The consequences may vary. For example, an attacker may gain the ability to alter data transmitted over A1 interface, extract sensitive information, etc. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any rApp security measures around the Onboarding onto SMO and deployment onto Non RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for rApps yet. |  | High |
| T-rAPP-03 | An attacker exploits rApps misconfiguration | Security misconfiguration, such as open ports or enabled unused protocols, can potentially exist in an rApp. If attackers can find exploitable rApp, they can disrupt the offered network service and potentially take over another rApp or the whole non-RT RIC. The actual consequences may vary. For example, an attacker may gain the ability to alter data transmitted over A1 interface, extract sensitive information, etc. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any rApp security measures around the Onboarding onto SMO and deployment onto Non RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for rApps yet. |  | High |
| T-rAPP-04 | An attacker bypasses authentication and authorization | An Attacker can exploit an rApp that has weak or misconfigured authentication and authorization to gain access to the rApp and pose as a tenant. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any rApp security measures around the Onboarding onto SMO and deployment onto Non RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for rApps yet. |  | High |
| T-rAPP-05 | An attacker deploys and exploits malicious rApp | An untrusted source may intentionally provide a malicious rApp. A trusted source may have a backdoor intentionally inserted in the rApp. If attackers can find exploitable rApp, they can disrupt the offered network service and potentially take over another rApp or the whole Non-RT RIC. Malicious rApps could impact Non-RT RIC functions such as AI/ML model training, A1 policy management, Enrichment information management, Network Configuration Optimization in the purpose of performance degradation, DoS, | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any rApp security measures around the Onboarding onto SMO and deployment onto Non RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for rApps yet. |  | High |
| T-rAPP-06 | An attacker bypasses authentication and authorization using an injection attack | It is possible that an attacker to submit requests without prior authentication and authorization by executing an injection attack to manipulate configurations, access logs, perform remote code execution, etc. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any rApp security measures around the Onboarding onto SMO and deployment onto Non RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for rApps yet. |  | High |
| T-rAPP-07 | rApp exploits services | A malicious rApp or a trusted but compromised rApp can exploit services such as O1 services across the R1 interface | A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any rApp security measures around the Onboarding onto SMO and deployment onto Non RT-RIC, authentication and access control, secure configuration, etc. Further, there is no testing framework in place for rApps yet. |  | High |
| T-PNF-01 | An attacker compromises a PNF to launch reverse attacks and other attacks against VNFs/CNFs | Data tampering and information disclosure; Denial of service from within for component access and/or function/service offered; Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data; | C, I, A | High | Medium | • Threat event initiation (Medium) • Adverse impacts (Medium) | This is a likely attack but may need physical access to the PNF. |  | High |
| T-SMO-01 | An attacker can exploit the misconfigured/poorly implemented authentication mechanism on SMO functions | The data stored in the SMO may be exposed/manipulated to an attacker. | C, I | High | High | • ZTA (High) • Threat event initiation (High) | O-RAN Alliance has not specified yet any SMO security measures around authentication, access control, secure configuration, etc. |  | High |
| T-SMO-02 | An attacker can exploit the misconfigured/poorly implemented authorization on SMO functions | An attacker can be able to perform certain actions, e.g. disclose O-RAN sensitive information or alter O-RAN components. | C, I, A | High | High | • ZTA (High) • Threat event initiation (High) | O-RAN Alliance has not specified yet any SMO security measures around authentication, access control, secure configuration, etc. |  | High |
| T-SMO-03 | Overload DoS attacks at SMO | Inability to deal with such events affects availability of SMO data and functions. | A | Medium | Medium | • ZTA (Medium) • Threat event initiation (High) | O-RAN Alliance has not specified yet any SMO security measures around authentication, access control, secure configuration, etc. |  | Medium |
| T-OPENSRC-01 | Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack | Attackers can exploit a vulnerability on the open source code and infects a hypervisor, operating system, VM or container with a malware. | C, I, A | High | High | Open-source/COTS support (High) | Vulnerability handling and patch management are not yet defined by O-RAN Alliance. Several CVE have already been discovered on open source software. |  | High |
| T-OPENSRC-02 | A trusted developer intentionally inserts a backdoor into an open source code O-RAN component. | Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data; | C, I, A | High | Medium | Open-source/COTS support (High) | Vulnerability handling and patch management are not yet defined by O-RAN Alliance. Several CVE have already been discovered on open source software. |  | High |
| T-PHYS-01 | An intruder into a site gains physical access to O-RAN components to cause damage or access sensitive data | Data tampering and information disclosure; Denial of service from within for component access and/or function/service offered; Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data; | C, I, A | High | Medium | Exposure (Medium) | O-RAN system has many external interfaces. Different O-Cloud deployment models can be used to implement O-RAN. Several scenarios to implement O-RUs and O-DUs are supported by O-RAN. |  | High |
| 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 | Data tampering and information disclosure; Denial of service from within for component access and/or function/service offered; Unauthenticated/unauthorized access of the O\_RAN component leads to compromised performance and/or function/service, lateral attack towards other O-RAN system component(s) from inside, and loss/stolen/tampering of sensitive data; | C, I, A | High | Medium | Exposure (Medium) | O-RAN system has many external interfaces. Different O-Cloud deployment models can be used to implement O-RAN. Several scenarios to implement O-RUs and O-DUs are supported by O-RAN. |  | High |
| T-RADIO-01 | Disruption through radio Jamming , Sniffing and Spoofing | Service disruption and information exposure | C, I, A | High | High | Exposure (High) | These attacks are common and not specific to O-RAN. They are likely to occur, hence they need more investigation and consideration. Mitigations to reduce these types of attacks should be defined by O-RAN Alliance. |  | High |
| T-RADIO-02 | DoS attacks on cognitive radio networks | Service disruption | A | Medium | High | Exposure (High) | These attacks are common and not specific to O-RAN. They are likely to occur, hence they need more investigation and consideration. Mitigations to reduce these types of attacks should be defined by O-RAN Alliance. |  | High |
| T-R1-01 | A malicious actor gains unauthorized access to R1 services | “Service management and exposure services Producer” determines whether the Service Producer is authorized to produce the service. An attacker can perform a spoofing attack to gain unauthorized access to R1 services. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any R1 security measures. |  | High |
| T-R1-02 | Attacker modifies Service Heartbeat message to cause Denial of Service | Attacker can exploit the Service Heartbeat on the R1 by modifying or inserting heartbeat messages to cause denial of service | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any R1 security measures. |  | High |
| T-R1-03 | Malicious actor bypasses authentication to Request Data | Attacker can exploit password-based authentication on the R1 to request unauthorized data. Weak password management can easily be exploited. (Certificate-based mutual authentication using TLS and PKI X.509 certificates is recommended). | C, I, A | High | High | • ZTA (High) • Adverse impacts (High) | O-RAN Alliance has not specified yet any R1 security measures. |  | High |
| T-R1-04 | Malicious actor bypasses authorization to Discover Data | “Data registration and discovery service producer” determines whether the Data Producer is authorized to produce the data types. An attacker can perform a spoofing attack to discover available data. | C, I, A | High | High | • ZTA (High) • Adverse impacts (High) | O-RAN Alliance has not specified yet any R1 security measures. |  | High |
| T-R1-05 | A malicious actor gains unauthorized access to data | An attacker can perform a spoofing attack to exploit the Data request and subscription service for the purpose to gain unauthorized access to data. | C, I, A | High | High | • ZTA (High) • Adverse impacts (High) | O-RAN Alliance has not specified yet any R1 security measures. |  | High |
| T-R1-06 | Malicious actor modifies a Data Request | Data Consumers consume the “Data request and subscription service” to request data instances or subscribe to them. An attacker can modify a request to force the consumer to receive a different data set then that intended. Without checks, the received data could be processed, leading to erroneous decisions or triggers. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any R1 security measures. |  | High |
| T-R1-07 | Malicious actor snoops Data Delivery to the Data Consumer | Data delivery messages relate to a particular data request or subscription. The data can be delivered to the Data Consumer in different ways, including:  • as part of the payload of a data delivery message, • as a data stream,  • from e.g., a REST endpoint, a message bus or object store location. An attacker can perform snooping, injection, or modification attacks in the Delivery of Data process. | A | High | High | • ZTA (High) • Adverse impacts (High) | O-RAN Alliance has not specified yet any R1 security measures. |  | High |
| T-A1-01 | Untrusted peering between Non-RT-RIC and Near-RT-RIC | Malicious Non-RT-RIC peers with a Near-RT-RIC over the A1 interface, or a malicious Near-RT-RIC peers with a Non-RT-RIC over the A1 interface, due to weak mutual authentication. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any A1 security measures. |  | High |
| T-A1-02 | Malicious function or application monitors messaging across A1 interface | Attacker gains access to A1 messaging for reconnaissance | C, I, A | High | High | • ZTA (High) • Adverse impacts (High) | O-RAN Alliance has not specified yet any A1 security measures. |  | High |
| T-A1-03 | Malicious function or application modifies messaging across A1 interface | Internal threat actor can gain access to the messaging across the A1 interface for a MiTM attack to modify or inject policy. This can result in the Near-RT RIC receiving malicious policy. | C, I, A | High | Medium | • ZTA (Medium) • Adverse impacts (High) | O-RAN Alliance has not specified yet any A1 security measures. |  | High |
| T-GEN-01-a | A successful attack could: - Compromise the deployed VNF/CNF | Spoofing, Tampering, Information disclosure, Elevation of Privilege | C, I | Medium | High | • Adverse impacts (Medium),  • ZTA (High) | Adverse impacts (Medium) - Only one VNF/CNF might be affected, Existing requirements and controls are defined in the O-RAN specifications that may impede successful exercise of the vulnerability.  ZTA (High): Reconnaissance and availability type attacks | SBOM requirements  REQ-SEC-SYS-1 | High |
| T-GEN-01-b | A successful attack could: - Deployment of malicious VM/Container (Lack of isolation) - Exploit host access to escape the host and reach hardware server then the malicious VM/Container can gain root access to the whole server where it resides | Spoofing, Tampering, Information disclosure, Elevation of Privilege | C, I | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) - Multiple VNFs/CNFs might be affected  ZTA (High): Reconnaissance and availability type attacks | SBOM requirements  REQ-SEC-SYS-1 | High |
| T-GEN-02 | A successful attack could: - Bypass access controls placed on various resources on O-Cloud - Gain increased privilege to specific O-Cloud services - Access to restricted areas of the O-Cloud network | Spoofing, Tampering, Information disclosure, Elevation of Privilege | C, I | Medium | High | • Adverse impacts (Medium),  • ZTA (High) | Adverse impacts (Medium) - Requirements are in place for user authentication and authorization  ZTA (High): Reconnaissance type attacks | REQ-SEC-PASS-1  REQ-SEC-OCLOUD-1  REQ-SEC-OCLOUD-2 | High |
| T-GEN-03-a | A successful attack could: - Make use of a untrusted VM/Container that runs on top of a trusted Hypervisor/Container Engine | Tampering, Information disclosure | C, I | Medium | High | • Adverse impacts (Medium),  • ZTA (High) | Adverse impacts (Medium) - Only one VNF/CNF might be affected  ZTA (High): Reconnaissance type attacks |  | High |
| T-GEN-03-b | A successful attack could: - Make use of a trusted VM/Container that runs on top of an untrusted Hypervisor/Container Engine to intercept communication, replace strong or use weak cryptographic keys, etc. | Tampering, Information disclosure | C, I | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) - Multiple VNFs/CNFs might be affected  ZTA (High): Reconnaissance and availability type attacks |  | High |
| T-GEN-03-C | A successful attack could: - Make use of a trusted VM/Container that runs on top of a trusted Hypervisor/Container Engine that runs on top of an untrusted hardware to intercept communication, replace strong or use weak cryptographic keys, etc. | Tampering, Information disclosure | C, I | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) - Multiple VNFs/CNFs might be affected  ZTA (High): Reconnaissance and availability type attacks |  | High |
| T-GEN-04 | A successful attack could: - Compromise the availability of O-Cloud services - Compromise the confidentiality/integrity of O-Cloud services by extracting/modifying critical application data | Information disclosure, Denial of Service | C, A | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) – No existing controls for interfaces in O-Cloud  ZTA (High): Reconnaissance and availability type attacks |  | High |
| T-GEN-05 (a) | A successful attack could: - view insecurely stored credentials and cryptographic materials | Information disclosure, Elevation of Privilege | C | Medium | High | Adverse impacts (Medium),  ZTA (High) | Adverse impacts (Medium) – Requirements are defined for sensitive data protection in the O-RAN security specifications  ZTA (High): Reconnaissance type attacks | REQ-SEC-OCLOUD-SS-1  REQ-SEC-OCLOUD-SS-2  REQ-SEC-OCLOUD-SS-3  SEC-CTL-OCLOUD-SS-1  SEC-CTL-OCLOUD-SS-2  SEC-CTL-OCLOUD-SS-3 | High |
| T-GEN-05 (b) | A successful attack could: - modify insecurely stored credentials and cryptographic materials | Tampering, Elevation of Privilege | I | Medium | Medium | Adverse impacts (Medium),  ZTA (Medium) | Adverse impacts (Medium) – Requirements are defined for sensitive data protection in the O-RAN security specifications  ZTA (Medium): Integrity type attacks | REQ-SEC-OCLOUD-SS-1  REQ-SEC-OCLOUD-SS-2  REQ-SEC-OCLOUD-SS-3  SEC-CTL-OCLOUD-SS-1  SEC-CTL-OCLOUD-SS-2  SEC-CTL-OCLOUD-SS-3 | Medium |
| T-GEN-06 | A successful attack could: - Gain access to the sensitive information  - Escalate privileges in Applications | Information disclosure, Elevation of Privilege | C | Medium | Medium | Adverse impacts (Medium),  ZTA (High) | Adverse impacts (Medium) – Requirements are defined for sensitive data protection in the O-RAN security specifications  ZTA (High): Reconnaissance type attacks |  | Medium |
| T-VM-C-01 | A successful attack could: - Compromise VM/Container isolation measures - Gain higher privileges on host or any of the containers running on that host - Perform unauthorized modifications to the contents of host filesystem e.g. install SSH keys, read secrets mounted to the host, and take other malicious actions | Spoofing, Tampering, Information disclosure, Denial of Service and Elevation of privilege | C, I, A | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) – No existing requirements  ZTA (High): Reconnaissance and availability type attacks |  | High |
| T-VM-C-02 | A successful attack could: - Deploy a new malicious VM/Container configured without network rules, user limitations, etc. to bypass existing defenses within O-Cloud infrastructure - Compromise the confidentiality & integrity of co-hosted VMs/Containers and tenants - Launch DDOS attacks on co-hosted VMs/Containers and host services thereby degrading their performance | Spoofing, Tampering, Information disclosure, Denial of Service and Elevation of privilege | C, I, A | High | Medium | • Adverse impacts (High),  • ZTA (Medium) | Adverse impacts (High) – No existing requirements  ZTA (Medium) - Availability type attacks |  | High |
| T-VM-C-03 | A successful attack could: - Retrieve/manipulate VNF/CNF sensitive data (e.g. passwords, private keys, subscription data, logs) | Tampering, Information disclosure | C, I | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) – No existing requirements  ZTA (High): Reconnaissance type attacks |  | High |
| T-VM-C-04-a | A successful attack could: - Cause migration Flooding: VM/Container performance degradation and VM/Container crashes | Tampering, Information disclosure, Denial of Service | C, I, A | High | Medium | • Adverse impacts (High),  • ZTA (Medium) | Adverse impacts (High) – No existing requirements  ZTA (Medium): Availability type attacks |  | High |
| T-VM-C-04-b | "A successful attack could: - Sniff the packets that are exchanged between the source and destination servers - Read the migrated memory pages - Monitor and/or modify the received packets while continuing to forward them to victim VM/Container" | Tampering, Information disclosure, Denial of Service | C, I, A | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) – No existing requirements  ZTA (High): Reconnaissance type attacks |  | High |
| T-VM-C-05 | A successful attack could: - Misguide the Virtualization layer to reduce the resource of or delete a VM/Container on which a VNF/CNF is running. This can result in the reliability, availability or even illegal termination of a VNF/CNF and hence the denial of service - Misguide the O-Cloud platform to detach a hardware accelerator from a VNF/CNF | Denial of Service | A | High | Medium | • Adverse impacts (High),  • ZTA (Medium) | Adverse impacts (High) – No existing requirements  ZTA (Medium): Availability type attacks |  | High |
| T-VM-C-06 | A successful attack could: - Access to data not erased from a terminated VNF/CNF or any VNF/CNF that has released resources | Information disclosure | C | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) – No existing requirements  ZTA (High): Reconnaissance and availability type attacks |  | High |
| T-IMG-01 | A successful attack could: - Insert malicious code that will subsequently get run in the production environment | Tampering, Information disclosure | C, I | Medium | High | • Adverse impacts (Medium),  • ZTA (High) | Adverse impacts (Medium) – Requirements are defined for image protection in the O-RAN security specifications  ZTA (High): Reconnaissance and availability type attacks | REQ-SEC-ALM-PKG-1 to REQ-SEC-ALM-PKG-15  SEC-CTL-ALM-PKG-1 to SEC-CTL-ALM-PKG-4 | High |
| T-IMG-02 | A successful attack could: - Intercept network traffic intended for registries and steal developer or administrator credentials within that traffic. Thus, could be used to provide fraudulent or outdated images to orchestrators, etc. | Tampering, Information disclosure | C, I | Medium | High | • Adverse impacts (Medium),  • ZTA (High) | Adverse impacts (Medium) – Requirements are defined for image protection in the O-RAN security specifications  ZTA (High): Reconnaissance and availability type attacks | REQ-SEC-ALM-PKG-1 to REQ-SEC-ALM-PKG-15  SEC-CTL-ALM-PKG-1 to SEC-CTL-ALM-PKG-4 | High |
| T-IMG-03 | A successful attack could: - Secrets embedded within a VM/Container image can be stolen  - Secrets embedded within a VM/Container image can be modified | Spoofing, Tampering, Information disclosure | C, I | Medium | High | • Adverse impacts (Medium),  • ZTA (High) | Adverse impacts (Medium) – Requirements are defined for image protection in the O-RAN security specifications  ZTA (High): Reconnaissance and availability type attacks | REQ-SEC-ALM-PKG-1 to REQ-SEC-ALM-PKG-15  SEC-CTL-ALM-PKG-1 to SEC-CTL-ALM-PKG-4 | High |
| T-IMG-04 | A successful attack could: - Build a custom image on the host that includes malware and then may deploy container using that custom image | Spoofing, Tampering, Information disclosure, Denial of Service and Elevation of privilege | C, I, A | Medium | High | • Adverse impacts (Medium),  • ZTA (High) | Adverse impacts (Medium) – Requirements are defined for image protection in the O-RAN security specifications  ZTA (High): Reconnaissance and availability type attacks | REQ-SEC-ALM-PKG-1 to REQ-SEC-ALM-PKG-15  SEC-CTL-ALM-PKG-1 to SEC-CTL-ALM-PKG-4 | High |
| T-VL-01 | A successful attack could: - Gain control over the host of a server or install a malicious Hypervisor/Container Engine/Host OS and exploit that to run malicious applications on the VM/Container that run on top of the host. This would enable the attacker to control all the VMs/Containers running on the host. | Spoofing, Tampering, Information disclosure, Denial of Service and Elevation of privilege | C, I, A | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (High) - No existing requirements  ZTA(High) - Reconnaissance and availability type of attacks |  | High |
| T-VL-02 | A successful attack could cause: - Failure of the physical machine to start at all - Physical machine entering a safe-mode - Physical machine continuing boot regardless of the integrity measurements | Tampering | I | High | Medium | • Adverse impacts (High),  • ZTA (Medium) | Adverse Impact (High) - No existing requirements  ZTA(Medium) - Availability type attacks |  | High |
| T-VL-03 | A successful attack could: - cause denial-of-service against the service discovery infrastructure to prevent O-Cloud to react to changing resource requirements properly | Denial of Service | A | Medium | Medium | Adverse impacts (Medium),  ZTA (Medium) | Adverse impacts (Medium) – Requirements are defined for O-Cloud authentication and authorization in the O-RAN security specifications.  ZTA (Medium): Availability type attacks | REQ-SEC-OCLOUD-O2dms-1  REQ-SEC-OCLOUD-O2dms-2  REQ-SEC-OCLOUD-O2dms-3  REQ-SEC-OCLOUD-O2dms-4  REQ-SEC-OCLOUD-O2ims-1  REQ-SEC-OCLOUD-O2ims-2  REQ-SEC-OCLOUD-O2ims-3  REQ-SEC-OCLOUD-O2ims-4  REQ-SEC-O-CLOUD-NotifAPI-1  REQ-SEC-O-CLOUD-NotifAPI-2  SEC-CTL-O-CLOUD-INTERFACE-1  SEC-CTL-O-CLOUD-INTERFACE-2  SEC-CTL-O-CLOUD-INTERFACE-3  REQ-SEC-OCLOUD-ISO-1  REQ-SEC-OCLOUD-ISO-2  REQ-SEC-OCLOUD-ISO-3  REQ-SEC-OCLOUD-ISO-4 | Medium |
| T-O2-01 | A successful attack could: - Tamper/alter/disclose requests and services sent over O2 between O-Cloud and SMO, hence the virtualized resource or relevant status information is not as requested - Affect the normal operation of the O-Cloud, and even causes DoS attacks, information leakage. | Tampering, Information disclosure, Denial of Service | C, I, A | Low | High | • Adverse impacts (Low),  • ZTA (High) | Adverse impacts (Low) – Requirements are defined for the protection of O2 interface in the O-RAN security specifications  ZTA (High): Reconnaissance and availability type attacks | REQ-SEC-O2-1  SEC-CTL-O2-2  REQ-SEC-DOS-1 | Medium |
| T-OCAPI-01 | A successful attack could: - Cryptographic keys or other security critical data of an instantiated VNF/CNF could be stolen by an attacker with access to the virtualization layer - The virtualized resource provided by the Virtualization layer to the instantiated VNF/CNF can be manipulated | Tampering, Information disclosure, Denial of Service | C, I, A | Low | High | • Adverse impacts (Low),  • ZTA (High) | Adverse impacts (Low) – Requirements are defined for the protection of O-Cloud API in the O-RAN security specifications  ZTA (High): Reconnaissance and availability type attacks | REQ-SEC-O2-1  SEC-CTL-O2-2  REQ-SEC-DOS-1 | Medium |
| T-HW-01 | A successful attack could: - Maliciously placed VM/Container extracts information from the target VM/Container with the side channel attack | Tampering, Information disclosure, Denial of Service | C, I, A | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse Impact (High) - No existing requirements  ZTA (High): Reconnaissance and availability type attacks |  | High |
| T-HW-02 | A successful attack could: - Extract useful information such as cryptographic keys from the target VM/Container to use them for traffic eavesdropping and man-in-the-middle attacks. | Tampering, Information disclosure, Denial of Service | C, I, A | High | High | • Adverse impacts (High),  • ZTA (High) | Adverse Impact (High) - No existing requirements  ZTA (High): Reconnaissance and availability type attacks |  | High |
| T-AAL-01 | A successful attack could: - tamper the requests/responses sent between the AAL components, the O-Cloud platform and O-RAN APPs/VNFs/CNFs | Tampering | I | High | Medium | Adverse impacts (Medium),  ZTA (High) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (Medium): Integrity type attacks |  | High |
| T-AAL-02 | A successful attack could: - cause DoS attack or increased traffic on AAL interfaces | Denial of Service | A | High | Medium | Adverse impacts (Medium),  ZTA (High) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (Medium): Availability type attacks |  | High |
| T-AAL-03 (a) | Fail to clear resources | Information disclosure | C | High | High | Adverse impacts (High), ZTA (High) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (High): reconnaissance type attacks |  | High |
| T-AAL-03 (b) | Fail to clear resources | Denial of service | A | High | Medium | Adverse impacts (High), ZTA (Medium) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (Medium): Availability type attacks |  | High |
| T-AAL-04 (a) | HAM compromise | Tampering | I | High | Medium | Adverse impacts (High),  ZTA (Medium) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (Medium): Integrity type attacks |  | High |
| T-AAL-04 (b) | HAM compromise | Denial of service | A | High | Medium | Adverse impacts (High), ZTA (Medium) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (Medium): Availability type attacks |  | High |
| T-AAL-05 (a) | Malicious memory accesses | Information disclosure | C | High | High | Adverse impacts (High), ZTA (High) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (High): reconnaissance type attacks |  | High |
| T-AAL-05 (b) | Malicious memory accesses | Tampering | I | High | Medium | Adverse impacts (High), ZTA (Medium) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (Medium): Integrity type attacks |  | High |
| T-AAL-05 (c) | Malicious memory accesses | Denial of service | A | High | Medium | Adverse impacts (High), ZTA (Medium) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (Medium): Availability type attacks |  | High |
| T-AAL-06 (a) | Software attacks | Information disclosure | C | High | High | Adverse impacts (High), ZTA (High) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (High): reconnaissance type attacks |  | High |
| T-AAL-06 (b) | Software attacks | Tampering | I | High | Medium | Adverse impacts (High), ZTA (Medium) | Adverse impacts (High) – Not security requirements yet for AAL in O-RAN security specifications  ZTA (Medium): Integrity type attacks |  | High |
| T-O-CLOUD-ID-01 | In the O-Cloud environment, the reuse of IDs from deleted objects for new objects can lead to unintended data associations, leaks, and operational disruptions. | Tampering, Information disclosure | C, I | High | High | Adverse impacts (High), ZTA (High) | Adverse impacts (High) – Not security requirements yet for O-Cloud ID in O-RAN security specifications  ZTA (High): reconnaissance and integrity type attacks |  | High |
| T-O-CLOUD-ID-02 | In O-Cloud deployments, replacing failed machines without proper management of their corresponding Node objects can lead to resource mismatches, stale data inheritance, and network inconsistencies. | Spoofing, Tampering, Information disclosure, Denial of Service | C, I, A | High | High | Adverse impacts (High), ZTA (High) | Adverse impacts (High) – Not security requirements yet for O-Cloud ID in O-RAN security specifications  ZTA (High): reconnaissance, integrity, and availability type attacks |  | High |
| T-O-CLOUD-ID-03 | In the O-Cloud environment, improper management of object IDs can lead to overlaps, inconsistencies, unauthorized access, and operational disruptions. | Spoofing, Tampering, Information Disclosure, Repudiation, Elevation of Privilege, Denial of Service | C, I, A | High | High | Adverse impacts (High), ZTA (High) | Adverse impacts (High) – Not security requirements yet for O-Cloud ID in O-RAN security specifications  ZTA (High): reconnaissance, integrity, and availability type attacks |  | High |
| T-ADMIN-01 | A successful attack could: - Lead to the inability to react to changing resource requirements - Operators may be unable to retrieve logs, telemetry data - Prevents the O-Cloud software update (VNFs/CNFs, VL) to exploit a known security flaw in the O-Cloud software | Denial of Service | A | Medium | Medium | • Adverse impacts (Medium),  • ZTA (Medium) | Adverse impacts (Medium) – Requirements are defined for the protection against DoS attacks and for the protection of O-Cloud API and O2 interface in the O-RAN security specifications  ZTA (Medium): Availability type attacks | REQ-SEC-DOS-1 | Medium |
| T-ADMIN-02 | A successful attack could: - Deploy new instances and disrupt existing O-Cloud services - Submit compromised VM/Container images that unsuspecting tenants then use to initiate O-Cloud services - Extract business data, configuration data, user data and possibly credentials - Create backups of VM/Container instances or export VM/Container images | Tampering, Information disclosure, Denial of Service and Elevation of privilege | C, I, A | Medium | High | • Adverse impacts (High),  • ZTA (High) | Adverse impacts (Medium) – Requirements are defined for the protection of O-Cloud API and O2 interface in the O-RAN security specifications  ZTA (High): Reconnaissance and availability type attacks | REQ-SEC-PASS-1  REQ-SEC-O2-1  SEC-CTL-O2-2  REQ-SEC-DOS-1 | High |

# Revision history

|  |  |  |
| --- | --- | --- |
| Date | Revision | Description |
| 2024.03.20 | 03.00 | Final version 03.00 |
| 2024.03.19 | 03.00.02 | Minor update |
| 2024.03.15 | 03.00.01 | Implemented CRs ERI CR0103, MTR CR0081, SYM CR0040, NEC CR0007, NEC CR0011, WG11 CR0029 |
| 2023.11.22 | 02.00 | Final version 02.00 |
| 2023.11.21 | 02.00.02 | Update according to received notes from November train review |
| 2023.11.03 | 02.00.01 | Implemented CRs WG11 CR0015, MTR CR0004 |
| 2019.01.31 | 01.00 | Final version 01.00 |
| 2019.01.24 | 01.00.02 | Implemented CRs ERI-0011, NOK-0032 and DCM-0008 |
| 2019.01.22 | 01.00.01 | Create initial O-RAN version, with change-marks from previous content. |

# History

|  |  |  |
| --- | --- | --- |
| Date | Revision | Description |
| 2024.03.20 | 03.00 | Published as final version 03.00 |
| 2023.11.22 | 02.00 | Published as final version 02.00 |
| 2023.07.31 | 01.00 | Published as final version 01.00 (Sucessor of O-RAN.WG11.Threat-Model.O-R003-v06.00) |