OPEN RAN SECURITY WHITE PAPER

UNDER THE OPEN RAN MOU

by Deutsche Telekom, Orange, Telefónica, TIM and Vodafone

MoU Open RAN Security White Paper

Contents

0. Executive Summary

Early in 2021, Vodafone Group, Deutsche Telekom AG, Orange S.A., Telefónica S.A., and TIM S.P.A. founded the Open RAN Memorandum of Understanding (MoU) to support the rollout of Open RAN for future mobile networks. This White Paper presents their assessment of Open RAN security.

The security of Open RAN is of vital interest to European operators as reputation, trust and legal duty demand that Open RAN systems are secure before any commercial roll-out. The MoU is supporting the O-RAN ALLIANCE Security Focus Group (SFG) to define the security architecture and helping to achieve a common vision of what the security standards required for O-RAN systems.

Open RAN systems have strong security attributes. O-RAN Alliance recognizes that the attack surface of RAN systems is expanded due to open and cloud-based architectures, but transparency of new open interfaces will increase scrutiny and monitoring of vulnerabilities and failures. Openness also brings more competition to the telecommunication industry because implementation of security solutions will not be bound to products of just one vendor but will be usable with equipment from any O-RAN compliant vendor. Mobile Network Operators (MNOs) would be free to select products and solutions that best suit their needs and diversify their vendor base (supporting recommendations from the EU 5G Toolbox).

The O-RAN ALLIANCE SFG is using a risk based approach to characterize risks in Open RAN systems according to the ISO 27005 [1] risk analysis methodology using a Zero Trust Architecture, as defined by the National Institute of Standards and Technology (NIST) [2] as underlying assumption. Threats and vulnerabilities to Open RAN systems are used to derive potential security requirements and priorities according to the impact and likelihood of attacks

The O-RAN security architecture consists of four pillars:

- The first is the “O-RAN Threat model and remediation analysis” [3] that is described above.

- The “O-RAN Security Requirements Specifications” [4] captures in a central location all O-RAN security related requirements and controls for each O-RAN function and interface. Requirements address **confidentiality, integrity, and availability** and consider key controls such as **authentication, authorization, replay protection, least privilege access control** and **zero trust.**
-The “O-RAN Security Protocols Specifications” [5] specifies the implementation, configuration and use of security protocols in O-RAN.
- The “O-RAN Security tests specifications” [6] establishes test cases and criteria for compliance with Security Requirements and Security Protocols Specifications. It’s the first step towards a verifiable set of O-RAN security requirements that can be used by third party certification bodies.

The SFG is collaborating with other O-RAN working groups on additional security enhancements. These include O-Cloud, RAN Intelligent Controllers (Near-RT-RIC & Non-RT-RIC) and their related applications (xApps and rApps), Fronthaul interface, certificate management and secure application Life Cycle Management.

With this, the O-RAN SFG and consequently the European operators participating in the MoU Group are confident that the O-RAN security specifications, as will be further developed in the O-RAN ALLIANCE, will allow vendors to develop secure products for testing, integration and deployment by operators. It will be necessary to apply the necessary security hardening and operational security processes to any commercial deployment of Open RAN systems.

The MoU will continue to liaise and work closely with European and national authorities to ensure a thorough understanding of regulatory expectations and demonstrate their security best practices. Vodafone Group, Deutsche Telekom AG, Orange S.A., Telefónica S.A., and TIM S.P.A have previously held a workshop with ENISA (November 2021) to discuss the security challenges for Open RAN. This paper builds on those discussions and aims to demonstrate why O-RAN systems can be as secure, or even more secure, as traditional proprietary RAN systems.

1. Open RAN MoU framework

Early in 2021, Vodafone Group, Deutsche Telekom AG, Orange S.A., Telefónica S.A., and TIM S.P.A. announced the formation of the MoU Group to help support the rollout of Open RAN as the technology of choice for future mobile networks, and to enable connectivity that would greatly benefit the needs of consumers and enterprises today and in the future.

The MoU collaboration aims to provide a framework that enables the creation of an ecosystem that allows for an interoperable market thanks to Open RAN and ensures the availability of solutions for timely deployments across Europe.

In line with the MoU's set objectives, a "Technical Priority Document" [7] was first released in the middle of 2021 to support new and existing vendors developing interoperable software and hardware. The document, which was published in two steps, outlined: (1) An executive summary of the technical priorities on the MoU signatories' websites, in May and (2) The complete Technical Priority Document published on Telecom Infra Project (TIP) [8] and O-RAN Alliance [9] websites, in June.

In addition, in November 2021, the five MoU operators published a report “Building an OPEN RAN Ecosystem for Europe” [10], calling policymakers, EU Member States, and industry stakeholders to collaborate and urgently prioritise OPEN RAN.

Furthermore, the five MoU operators have been working on the "MoU Action Plan" covering a number of key activities which include the promotion of the European perspective relating to the security of Open RAN. In this respect, MoU technical and policy experts have set out to create a clear understanding of how Open RAN can fit into the EU 5G Cybersecurity Framework. The way to achieve this would be to include communications with relevant stakeholders, identifying gaps between EU requirements and MoU members' priorities [7], ensuring continuous cooperation with ENISA and EU stakeholders on 5G security initiatives, and socializing MoU parties' views on Open RAN security.

2. Open RAN / O-RAN ALLIANCE

O-RAN Alliance was founded in February 2018 by five operators (AT&T, China Mobile, Deutsche Telekom, NTT DOCOMO and Orange; with TIM S.P.A joining before the end of 2018) with the aim of defining a new architecture for Radio Access Networks (RAN) to enable a more rapid and cost-efficient delivery of innovative features and services in a highly competitive market scenario. The association soon grew and now counts more than 300 contributors including major world Telecommunication operators, Equipment suppliers, Research institutions and Universities.

The Alliance aims to define a more intelligent, open, virtualized and fully interoperable radio access architecture characterized by:

- The ability to use devices, equipment and applications from different suppliers, guaranteeing interoperability through the definition of open standard interfaces
- The use of non-specialized hardware on which to install multi-vendor software modules which implement the various network functions leveraging state of the art IaaS/PaaS cloud technologies
- The exploitation of AI / ML (Artificial Intelligence / Machine Learning) to automate operations related to management, configuration and radio optimization.

Each of these points is addressed in the activities of the organization and is translated into technical specifications. The approach represents a real-world revolution as it aims to overcome current monolithic solutions in which the vendor integrates and manages all the components of the radio access network (RAN). In this way it is therefore possible to "disaggregate" the various components opening the ecosystem to new suppliers, achieving greater flexibility in deployments and operations, interoperability in multi-vendor RAN components and improved trusted supply chain diversification.

The work of the Alliance focuses on three main areas:

- Technical specifications development to define the components of the new RAN and the related interfaces, fully supporting and in a complementary way standards defined by 3GPP and other industry organizations.
- O-RAN Software Community activities (a collaboration between O-RAN Alliance and Linux Foundation) to develop open-source software based on the technical specifications.
- Testing and integration activities to verify the correct functioning, security and interoperability of O-RAN implementations and promote their adoption.

Technical specifications are constantly evolved via three deliveries during the year, both to insert new features and to update existing ones: they represent a snapshot of what the various groups produced at the time of publication. Asynchronous publication mechanisms can be accommodated as well in the case of updates to some specifications.

Based on and in compliance with the specifications, the O-RAN Software Community develops the open-source software of the radio access network nodes (e.g., for the Near-Real-Time RAN intelligent controller, virtualization and cloud platforms,etc). The challenges of this approach are related to the development of highly performing software able to operate in real time environments and to the collaborate with other open-source communities in order to leverage on existing solutions.

Finally, to facilitate and stimulate the development of solutions according to the architecture and interfaces defined in the technical groups, O-RAN Alliance has promoted the establishment of laboratories for testing and integration called OTIC (Open Testing and Integration Center). OTIC labs provide an open, collaborative and unbiased environment (i.e., independent from the O-RAN vendors) in order to pursue several objectives:

- Support for the adoption of O-RAN specifications and the development of the O-RAN ecosystem through the organization of demos, laboratory or field trials and events such as workshops.
- Organization of Plugfests, to host demonstrations of solutions and Proof of Concept based on O-RAN specifications.
- Testing and verification of the adherence of the implementations of RAN equipment to the O-RAN specifications through conformity tests and interoperability tests based on the test specifications developed in the technical groups. In this case, the goal is to issue certificates and badges by the OTIC laboratory for solutions that meet the specifications based on the tests performed.
- End-to-End setup functional and performance tests, according to the test specifications defined within the Testing and Integration Focus Group (TIFG).
- OTIC centers are also concerned about security aspects, in particular security features verification and functional and performance security tests of the RAN elements, with the starting focus on End-to-End testing.
- Feedbacks to O-RAN Alliance based on test activities and experience, in order to support the development of technical specifications.

As an open technical organization, O-RAN Alliance is the place where both incumbent as well as emerging industry players and academic institutions work together and contribute to open RAN solutions. All participants in fact can access and make technical contributions to any of the groups through a consensus-driven process.

O-RAN specifications have always been publicly accessible, as once approved by the O-RAN Board, they can be downloaded from the public website upon agreement to the O-RAN Alliance Adopter License. More recently, the Alliance updated its working procedures towards more transparency to match that of long established standardization bodies. As an example, it was decided that the technical specifications be formally recognized by European Telecommunications Standards Institute (ETSI) through a procedure called PAS (Publicly Available Specification). The process is currently underway, and the activity is expected to be taken over by the ETSI Technical Committee MSG (Mobile Standards Group).

To ensure compatibility and to avoid duplication of work, O-RAN's technical work builds on existing 3GPP specifications and standards. Specifically, one of the objectives of the Alliance is to design the unbundling of the radio access node with the addition of functional elements and related interfaces in accordance and compliance to the 3GPP architecture.

As shown in Figure 1, the O-RAN architecture extends the functional disaggregation of a 3GPP radio base station (e.g. eNB for LTE or gNB for NR) by introducing three components plus a management one:

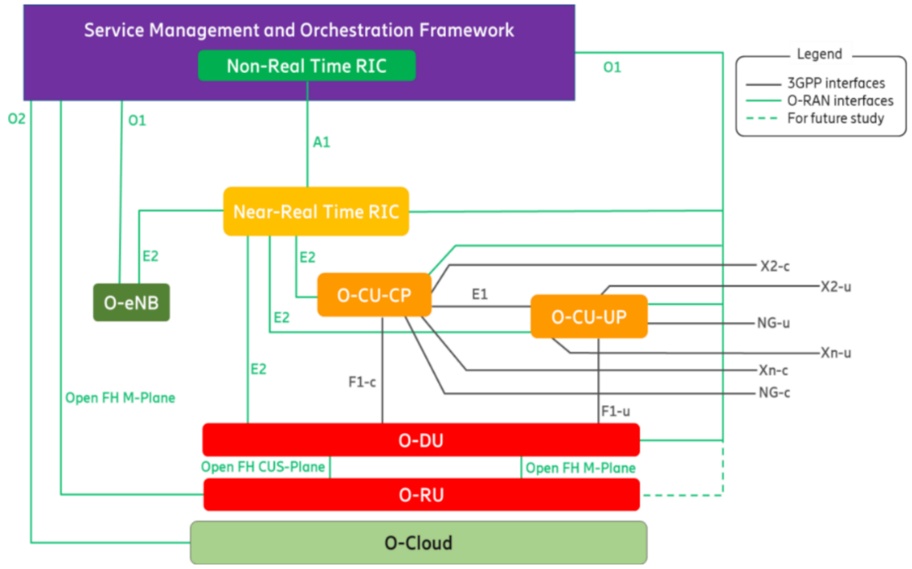

Figure 1 : O-RAN logical architecture[11]

- O-CU (O-RAN Central Unit) separated into O-CU-CP (Control Plane) and O-CU-UP (User Plane) as already foreseen in 3GPP: this is where the radio network intelligence is concentrated. It is a mini data center with high processing capacity, capable of managing multiple antennas deployed within a radius of a few tens of Kms.
- O-DU (O-RAN Distributed Unit): it is where the transmission and reception operations are managed. Also, in this case, the node can be virtualized and hosted in a centralized data center for the management and coordination of multiple radio sites or reside directly near the antennas.
- O-RU (O-RAN Remote Unit): it is the node physically mounted together with the antenna and can include the radio frequency and management components of the intelligent antennas.
- RIC (RAN Intelligent Controller), divided into Non-Real Time RIC and Near-Real Time RIC, exercises the management of radio resources and the control of the three components above (O-CU, O-DU and O-RU).

Whilst solutions that implement disaggregated radio base stations already exist on the market, they would be based on non-standard interfaces which force the operator to rely on a single supplier. The novelty introduced by the Alliance is the specification of new open interfaces between the disaggregated components, together with the interoperability specifications that enable the operator to purchase the different blocks from multiple suppliers.

Another important objective is the separation, again through interoperable interfaces, between the management network and the equipment. In this way, the applications and management algorithms come no longer as a “monolith” from a single supplier but can be developed by a third party or directly by the operator.

O-RAN Alliance technical specifications cover use cases, requirements and solutions for each component and interface depicted in Figure 1, therefore dealing with evolution of the architecture and definition of use cases, O-RAN Near-RT RIC, Non-RT RIC, Open Fronthaul Interfaces, Profiling of the

3GPP-based interfaces, O-RAN Cloud and Orchestration, White-box Hardware and Open Source SW, transport network, management network, test and integration, and security aspects.

The most updated versions of the specifications can be found in [12].

Within the Alliance, the SFG (Security Focus Group) is responsible for defining the requirements and specifying the architectures and protocols for security and privacy in O-RAN systems. SFG specifies security requirements, architectures and frameworks in support of the open interfaces defined by other O-RAN WGs. This includes security guidelines that span across the entire O-RAN architecture.

3. Security in Open RAN

Open interfaces between individual network functions with available specifications unlock traditional closed world of telecommunications to vendors from IT. Security of RAN, even though it has its own specifics, shares many risks with IT infrastructure. Thanks to its openness and transparency, O-RAN can benefit from existing as well as future security solutions initially developed for IT.

Openness also brings more competition to telecommunication industry because implementation of security solution will not be bound to products of just one vendor but will be usable with equipment from any O-RAN compliant vendor. This inherited interoperability also opens doors for specialized vendors, who provide best of breed security solutions, but do not provide entire RAN stack. Mobile network operators (MNOs) will be free to select products that best suits their needs and will avoid a risk of vendor lock in. Transparency builds ground for better monitoring and gives better visibility into the network, which leads to more effective security operations. Disaggregation also enables MNOs to replace smaller parts of RAN equipment from one vendor in case it does not meet their requirements anymore.

Security Focus Group (SFG) has adopted principles of zero trust architecture (ZTA) as defined in NIST Special Publication 800-207 [2] which is based on zero trust security model. Zero trust security models assume that an attacker can be present in internal as well as external environment and that an operator-owned environment is no different and no more trustworthy than any other environment. Its principle: “never trust, always verify”. Due to this approach, no implicit trust between O-RAN components and any other parts of the infrastructure is assumed.

Security in Open RAN is built on thorough risk analysis from which explicit requirements are created.

In March 2022, O-RAN Alliance released its first version of Security Test Specifications [6]. Target of this document is to develop the security test cases, which verifies the development and implementation of the security requirements or emulates the attacks and validates mitigation methods align with the threats and recommended security controls identified in O-RAN threat modelling and remediation analysis.

Open as well as proprietary RAN implementations must face the same technological challenges. Due to its open nature, all Open RAN specifications come under close scrutiny. They have to address security challenges and by consensus propose the best secure solution possible. This ensures that real security is achieved instead of security through obscurity.

MoU representatives in the O-RAN Alliance support development of open RAN specifications that enable compliance with security and data privacy requirements in the EU to allow MNOs to build solutions that meet security and legislative requirements.

4. The O-RAN risk-based approach to cybersecurity

O-RAN architecture adds beyond the 5G 3GPP specifications new open interfaces and functions to enable secure supplier diversity. Security concerns are similar to those of 5G networks e.g. the cloud, virtualization, containerization, edge computing, network slicing and AI/ML. Since the O-RAN architecture is built based on 3GPP specifications, it emerges and benefits from the 3GPP's security features.

Innovation and supplier diversity in an open ecosystem will bring forward additional diverse security solutions to address potential threats and mitigate risk because of the ability to monitor, detect, prevent and respond more quickly.

O-RAN Alliance recognizes cybersecurity as an essential topic on its agenda and is earnestly searching for the optimal means to improve cyber resilience of the O-RAN system.

MoU operators who will deploy and manage O-RAN infrastructure are committed to handle cybersecurity seriously with constant attention. They want to know how well cyber risks facing O-RAN are being managed in their organizations, processes, and services. They need to have a thorough understanding of cyber risks in open and interoperable networks like O-RAN systems and have to know how to leverage from security measures and mitigation techniques specified within O-RAN specifications and have to identify hardening measures for operational environments so to cope with cyber risks and regulations.

A risk-based threat modeling and remediation analysis has been conducted within the O-RAN Alliance in line with ISO 27005 [1] for building an effective security O-RAN architecture, as well as managing and continuously decreasing risks of the overall O-RAN system. The proposed risk assessment process has three parts: risk identification, risk analysis and risk evaluation. This means that one has first to identify valuable assets, then consider the threats that could compromise those assets and finally perform a risk assessment in order to estimate the actual damage generated by the realization of any threat to these assets.

The risk-based threat modeling and remediation analysis is focusing on the critical O-RAN components and interfaces to identify the true risks to the O-RAN's most valuable assets, prioritize actions to mitigate those risks to acceptable levels and deliver compliance to the national authority procedures and overall regulation framework (EU 5G toolbox, …). The concept of "zero trust" [2] networking is applied on the risk assessment meaning that anything that connects to a O-RAN network should inherently not be trusted unless it can be verified.

Following the ISO 27005 methodology [1], the O-RAN risk-based threat modeling and remediation analysis assesses and aligns security with the goals that the O-RAN Alliance has identified the following items:

- Item 1: The main stakeholders contributing to the security of O-RAN networks
- Item 2: The main assets, their degree of sensitivity and security properties
- Item 3: The main threats actors, threats and vulnerabilities posed to O-RAN networks
- Item 4: The main security principles to enforce the security of the O-RAN system
- Item 5: The main risks in terms of impact and likelihood based on risk criteria
- Item 6: Prioritization which risks need to be addressed, and in which order
- Item 7: Risk monitoring and review

MoU operators are aware that the identified risks are not static and can change abruptly. Therefore, risks will be continuously monitored, where the characteristics of each threat (e.g., likelihood, impact, vulnerabilities, and assets) will be reassessed over time to keep an up-to-date risk picture for O-RAN.

MoU operators will also keep a close eye on:

- Any new assets included within the risk management scope
- Asset values that require modification in response to changing O-RAN requirements
- New threats, whether external or internal, that have yet to be assessed
- Security incidents.

This risk-based approach enables O-RAN members to focus their efforts on the risks that are the most significant to their operations.

5. O-RAN Security Focus Group activities

The SFG work is captured in four security specifications that are the pillars of the O-RAN security architecture that cover threat modeling, security requirements, protocols and tests. Latest approved SFG specifications are accessible on the O-RAN ALLIANCE web site [12].

5.1. O-RAN Security Threat Modeling and Remediation Analysis 2.1 [3]

This document is a risk-based threat modeling and remediation analysis used for managing risks and for building an effective O-RAN security architecture. The risk assessment methodology based on ISO 27.005 standard described in previous section has been used within the "O-RAN Security Threat Modeling and Remediation Analysis" document. The version 2.1 contains description of Item 1 to 5 addressed in section 4 above:

- Main stakeholders managing, operating, and maintaining O-RAN systems with their associated responsibilities are identified. Among them, three stakeholders are of particular relevance to the cybersecurity of O-RAN networks: on one hand, mobile network operators have a central, decision-making role, giving them leverage on the overall secure operation of their networks, and on the other hand, telecom equipment suppliers and cloud providers, who are responsible for the provision of software and hardware required to operate O-RAN networks.
- O-RAN's key assets to be protected are determined together with their location in component. 42 assets are identified with their protection level in terms of Confidentiality, Integrity, Availability (CIA), Replay and Authenticity when at rest and in transit.
- Based on the critical assets coming from the previous item, their vulnerabilities, potential threats and threat agents have been characterized.

  The assessed threats are consolidated from various sources, including O-RAN specifications, main 5G standardization documents and telecommunication best practices (e.g. 3GPP, ITU, ETSI, ENISA, ISO, NIST and GSMA).

Threat ID	
Threat title	Title of the threat
Threat description	Description of the Threat
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

Figure 2: Threat template used in O-RAN Threat Model and Remediation Analysis

The threat modelling and remediation analysis identified specific O-RAN vulnerabilities. Among them, there are the unauthorized access to O-DU, O-CU-CP, O-CU-UP and RU to degrade RAN performance or execute broader network attack, the unprotected synchronization and control plane traffic on Open Fronthaul Interface, the Near-RT RIC conflicts with O-gNB, the x/rApps conflicts and the x/rApps access to network and subscriber data.

The identified threats are grouped in seven categories to cover the overall O-RAN architecture. Among of them

- Common threats related to the insecure design, misconfiguration, weak authentication, and lack of access control.
- Threats against the Fronthaul interface and M-S-C-U Planes including the MiTM attacks, unauthorized access to the FH interface, spoofing of M-S-C-U Planes messages and DoS attacks against a Master clock.
- Threats against Near RT-RIC xApps, Non-RT RIC and rApps.
- Threats against SMO such DoS attacks and improper/missing authorization weakness on SMO functions
- Threats against O-Cloud including the compromise of VNF/CNF images and embedded secrets, the weak orchestrator configurations, access controls and isolation, the misuse of a VM/Container to attack other VM/Container, hypervisor/container engine, other hosts (memory, network, storage), etc., the spoofing and eavesdropping on network traffic to access all O-RAN network data processed in the workload and the compromise auxiliary/supporting network services.
- Threats to open source including the use of SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack.
- Threats against ML including data poisoning attacks, altering a machine learning model and transfer learning attack.

The rationale between the 49 identified threats and the vulnerabilities within the O-RAN's assets are provided.

As already anticipated above, it is worth highlighting that O-RAN expanded attack surface is bounded by explicit security requirements in a Zero Trust environment. A zero-trust architecture means even in a closed proprietary implementation, interfaces between internal proprietary software modules shouldn't be trusted. Many of today's security threats come from faults in one module opening access to compromise of other critical modules. From this standpoint, even closed proprietary implementations should examine their own internal proprietary threat surfaces. Closed proprietary RAN implementations by a single vendor has similar attack surface within their own internal components, and because the implementation is proprietary there is no way to demonstrate whether they are taking a zero-trust approach to their internal interfaces because it is hidden without clear stated requirements to be tested against.

- Security principles based on the zero-trust approach are defined to adequately address the identified threats in the previous step. 16 Security Principles are identified among them, authentication and access control mechanisms, trusted communication, secure cryptographic operations, secure storage, secure boot, trusted and secure update, secure management of open-source components, robust isolation, continuous security development, testing, logging, monitoring and vulnerability handling, and security assurance. The security principles rationale is provided to trace all security principles back to threats and demonstrate that the defined security principles contribute to counter those threats. These principles are intended to drive specifications of normative security requirements (see "O-RAN Security Requirements Specifications" [4] in section 5.2 below) and provide security principles which vendors and operators should address when building a secure end-to-end O-RAN system.
- The process of risk assessment evaluates the risk for each asset-threat-vulnerability combination and then assigns it a risk score. Each identified threat is assigned to an impact level and based on the likelihood of it occurring. Taking the two values coming from the likelihood of a threat to occur and the impact it will cause a risk level for each threat is derived. Risks are categorized as high, medium, or low in relation to how likely they are to occur.
- Part of the risk assessment steps includes assessing current security controls to determine if the implemented or planned controls will minimize or eliminate risks to O-RAN. This involves reviewing the existing controls installed to protect the security of O-RAN.

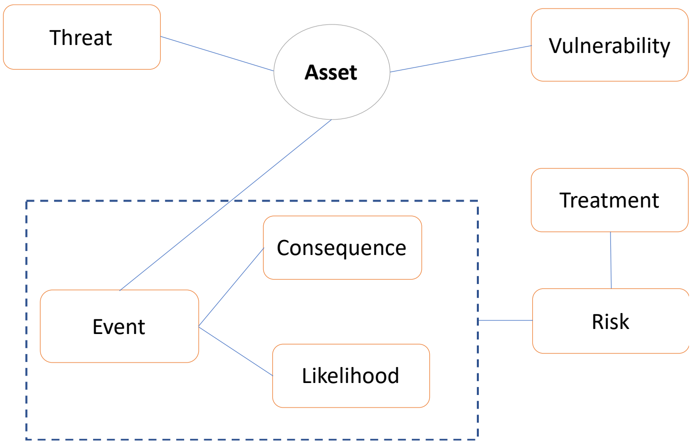

Figure 3: Risk assessment methodology

- The risk assessment study in this version of the document is the first stage and aims to assess the criticality of threats based only on their potential impacts without considering the likelihood. In future step, a full risk assessment considering the likelihood will be conducted and provided in a next version of the report. The criticality of the identified threats was assessed based on their potential impacts. Indications of severity level for each threat are given whether they are considered as high, medium, or low. This severity is seen as a global perception of the risk based on its impacts.

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)**

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
Medium	Disclosure of personal data (according to GDPR[1]) which CAN be processed or aggregated to uniquely identify subscribers.	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
High	Disclosure of sensitive personal data (GDPR special category[2]).	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

Table 1 : Severity rating

5.2. O-RAN Security Requirements Specifications v2.0 [4]

This document specifies the initial security requirements per O-RAN Interface and per O-RAN component. Requirements address confidentiality, integrity, and availability (CIA) protection by considering key controls such as authentication, authorization, replay protection, least privilege access control, and zero-trust among others. V2.0 of this document contains:

- Confidentiality, Integrity, Replay protection and Data origin authentication mandatory requirements for A1, O1, O2, E2 interfaces.
- Least Privilege Access Control on O1 interface enforcement with IETF RFC- 8341 Network Configuration Access Control Model (NACM) requirements.
- Authentication and Authorization based on IEEE 802.1x Port based Network Access Control requirements to control network access in point-to-point LAN segments across the Open Fronthaul interface.
- Mandatory support for TLS 1.2+ and Public Key Infrastructure X. 509 (PKIX) for mutual authentication on the Fronthaul M-Plane (Will be reflected in O-RAN WG4 Open Fronthaul Management Plane Specification v8.0 [13])
- Transversal requirements and tests cases (see section 5.4 below) for Networks Protocols and Services, DDoS attacks protection, password protection policies and vulnerability scanning.
- Software supply chain security support in the form of Software Bill Of Material (SBOM) requirements for every O-RAN software delivery following NTIA guidance.

[1] '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.

[2] 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.

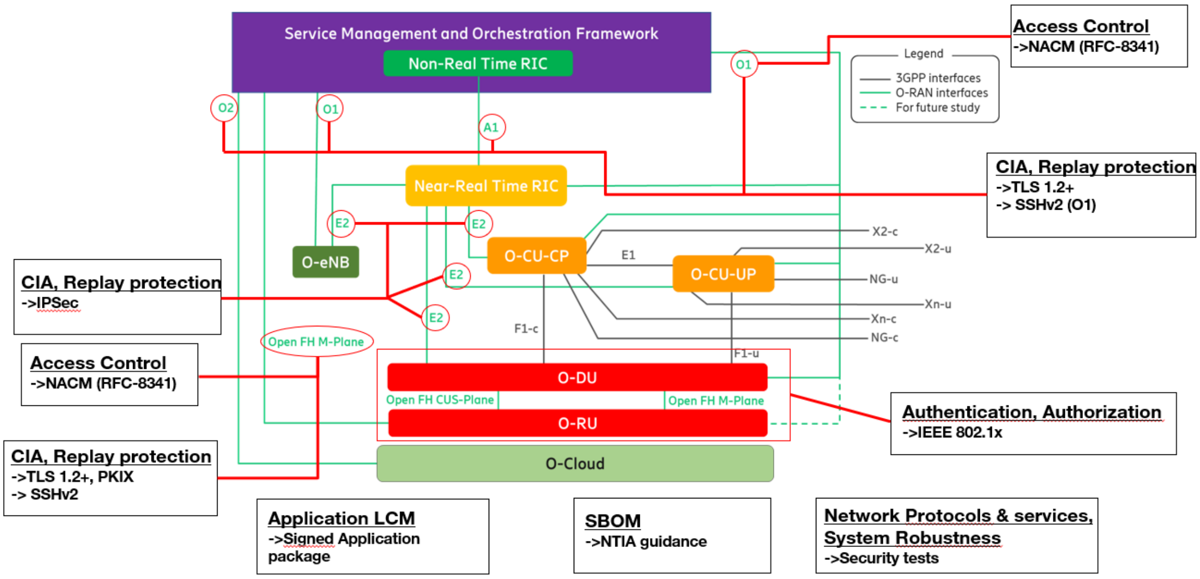

Figure 4: View of SFG specified security requirements – November 2021– O-RAN Logical architecture

5.3. O-RAN Security Protocols Specifications v3.0 [5]

This document specifies security protocols used by O-RAN compliant implementations. It defines implementation requirements for SSH, IPSec, DTLS, TLS 1.2, TLS 1.3 and NETCONF support over secure transport. Recent update adds mandatory support for TLS 1.3 to comply with National Institute of Standards and Technology's (NIST) directive to have support by January 1, 2024.

5.4. O-RAN Security Tests Specifications v1.0 [6]

This document specifies and describes security tests needed to validate security-related functions, configurations, and protocols requirements and is the first step towards verifying the security requirements of O-RAN systems. The main focus of the security test specifications is on:

- Validating the proper implementation of security protocols requirements specified in the O-RAN Security Protocols Specifications (SSH, TLS, DTLS, and IPSec).
- Emulating security attacks against the O-RAN component(s), interfaces, and the system to measure the robustness of the O-RAN system and the service impact(s).
- Validating the effectiveness of the security mitigation method(s) to protect the O-RAN system and the services it offers.

Validating transversal requirements for Networks Protocols and Services, DDoS attacks protection, password protection policies, and vulnerability scanning defined in O-RAN Security Requirements.

5.5. On-going work items and next steps

The SFG has identified risks through threat modeling and risk analysis and is collaborating with other O-RAN working groups on additional security enhancements. These include:

- Securing the O-Cloud: Work Group (WG) 6 and the SFG are tackling security challenges related to O-Cloud environments. To address the security of O-Cloud, the roles, and responsibilities of users likely to interact with the O-Cloud will be defined. The O-RAN Security Threat Model and

Risk Analysis framework will be used to provide a security risk assessment of the different O-Cloud deployment models, e.g. Private, Public, Hybrid, Community, to help O-RAN stakeholders assess the risks that they may face in different O-RAN cloud deployments. The attack vectors for exploiting vulnerabilities of O-Cloud framework will be tackled in detail in extensive groups of threats. The SFG will use the output from these efforts to security requirements, controls, and good practices for enhancing the security of O-Cloud.

- Securing the Fronthaul interface and its participating Network Elements: SFG and WG4 are tackling specific threats toward Synchronization, Control and User planes and investigating solutions to secure these planes. SFG has proposed use of IEEE 802.1X Port based Network Access Control (PNAC) protocol to protect these messages on the Fronthaul. It is also considering possible application of IEEE 1588 TLV security profiles for protecting S-plane messages, and IEEE 802.1AE MACSec for protecting Control and User plane messages.
- Securing the Near-RT RIC platform, xApps, and related interfaces: SFG and WG3 are analyzing a list of key issues and potential security solutions in the Near RT RIC and xApps including isolation compromises, malicious A1 policies, ML vulnerabilities, data compromises, the trust model for 3rd party applications, Near-RT RIC APIs authentication and authorization, and the secure onboarding of xApps.
- Securing the SMO Non-RT RIC and rApps: A work item involving SFG and WG2 experts has been created to tackle security of the Non-RT-RIC, rApps and their related interfaces. They will follow a risk-based approach with identification of threats actors, attack surface, potential exploits and their impacts. Controls will then be specified targeting PKI with X.509 certificates, multifactor authentication, Role Based Access Control, and logging strategy.
- Specifying security test strategies and test cases: A specific SFG work item is dedicated to updating the Security Test Specifications version 1.0 document with further tests cases to align with the threats and recommended security controls identified in O-RAN Threat Modelling and Remediation Analysis activities. Additionally, develop the security badging technical procedures to be adopted by Open Test Integration Center (OTIC) by leveraging on existing Test and Integration Focus Group (TIFG) OTIC certification procedures and integrating into future OTIC certification and badging processes and procedures.
- Updating the O-RAN risk analysis with likelihood scores according to ISO 27005 standard [1] with consideration of Zero Trust Architecture [2], thus providing accurate vision of risks with combination of their potential impacts and likelihood. The scoring exercise is to be periodically updated to account for mitigation provided by newly defined security specifications. Risk level scoring will then be used to identify most critical threats on which to focus specification effort.
- A certain amount of security topics is identified for further specification work. Among topics that will be developed: Certificate management, API security, Application Life Cycle Management, Security logging, AI/ML security, guidelines for secure software development…

The four specification documents listed above are regularly updated and revised to reflect evolving threats and attack vectors, and to specify new security requirements, controls, and related test cases. Along with the O-RAN SFG Work Items listed above the MoU Group of operators is confident that the O-RAN security specifications will allow vendors to develop secure products to be then tested, integrated and deployed by operators.

6. Conclusion

As presented in previous sections, O-RAN architecture, built in compliance with the standards promoted by the O-RAN Alliance, operates on the secure foundation of zero trust approach (never trust, always verify) where network elements have to authenticate mutually with each other for them to communicate. All communication between them will be transported over a secure interface per industry best practices specified by the O-RAN Alliance's security specifications. Furthermore, the standardization is based on the O-RAN risk-based threat modeling and remediation analysis following the ISO 27005 methodology.

Decoupling hardware and software, makes the system less interdependent on hardware, reducing the risk associated with upgrades or isolated security breaches. In addition, the enhanced modularity available with open interfaces makes it easier for operators to move towards a continuous integration/continuous delivery (CI/CD) operating model that enables the seamless and effective patch management needed to fix any security vulnerability.

In addition, avoiding vendor lock-in means supply chain flexibility that gives the operators a new way to prioritize secure solutions, in addition to allowing them to pick best-of-class suppliers that meet their requirements.

On the other hand, virtualization increases visibility because virtual hosts provide operational telemetry data about the functions they support. This data is isolated from the function's execution environment, which decreases its vulnerability to attack. Isolating network functions adds greater operational awareness and limits the damage that one security threat can produce in the overall network. In addition, security best practices in containerized solutions are applied, so multiple elements of security for different layers of the container solution stack and different stages of the container life cycle are defined.

So, considering the security from the design stage, following all the security standards and specifications from SFG and 3GPP, and adopting a zero-trust approach and an end-to-end security governance over the implementation, makes O-RAN systems as secure, or even more secure, as traditional proprietary RAN systems.

7. References

[1] ISO 27005 : https://www.iso.org/standard/75281.html

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

[3] O-RAN ALLIANCE, "O-RAN Security Threat Modeling and Remediation Analysis 2.1", November 2021

[4] O-RAN ALLIANCE, "O-RAN Security Requirements Specifications 2.0", November 2021

[5] O-RAN ALLIANCE, "O-RAN Security Protocols Specifications 3.0", November 2021

[6] O-RAN ALLIANCE, "O-RAN Security Tests Specifications 1.0", November 2021

[7] Open RAN Technical Priority Document, by the Open RAN MoU signatories (Deutsche Telekom, Orange, Telefónica, TIM and Vodafone) – June 2021

[8] https://telecominfraproject.com/openran-mou-group/

[9] https://www.o-ran.org

[10] Building an Open RAN ecosystem for Europe, https://www.o-ran.org/ecosystem

[11] O-RAN ALLIANCE, “O-RAN Architecture Description 6.0”, November 2021

[12] https://www.o-ran.org/specifications

[13] O-RAN ALLIANCE, “O-RAN Management Plane Specification 8.0”, November 2021

8. Acknowledgements

The MoU signatories Vodafone Group, Deutsche Telekom AG, Orange S.A., Telefónica S.A., and TIM would like to recognize the significant project leadership and important contributions of group leaders Patricia Diez Munoz, Paolo De Lutiis, Maria Pia Galante, Hector Dotse, Kyriakos Exadaktylos, Jan Balas, Roberta D’amico, Holger Erkens, Mohamad Hajj and Sébastien Jeux along with many representatives from MoU companies and Internet of Trust who participated in the development of this White Paper.