OPEN RAN TECHNICAL PRIORITIES

Focus on Security

UNDER THE OPEN RAN MOU

by Deutsche Telekom, Orange, Telefónica, TIM and Vodafone

This document provides a high-level description of the MoU signatories' technical requirements on Security.

For the avoidance of doubt, the technical requirements set out in this document are those that the signatories of the Open RAN MoU consider priorities for Open RAN solutions. They serve as guidance to the RAN supplier industry on where to focus to accelerate market deployments in Europe.

1. New security section within the MoU Technical priorities

Open RAN is driving a paradigm shift in the way that the Radio Access Network (RAN) is designed, built, and operated. It introduces new technologies and vendors to the RAN ecosystem. Security risks are always present in new systems, and Open RAN is no exception.

This new release of the MoU Technical priorities focuses in more detail on security topics and various challenges introduced by the disaggregation promoted by the O-RAN architecture. Indeed, it contains a more comprehensive set of security requirements then the previous release.

Specifically, the security requirements are now contained within a dedicated section of the MoU Technical Priorities document. It is recommended that all Open RAN vendors refer to this new security section, and consider the relevant security requirements for their solutions in addition to the functional requirements.

2. Security Work within Release 3

The security requirements in this new G5-MoU Technical Priorities document are based on the security requirements that were present in the previous release, augmented with new requirements coming from the latest O-RAN Alliance specifications (November 2022). The complete set of security requirements was then consolidated and rationalised.

The security requirements within the MoU Technical Priorities document are expected to evolve further in future Releases, in line with the O-RAN Alliance specifications.

3. Overview of the included security requirements

Concerning priorities, the five operators agree that security is not to be put at stake, and there's unanimity and high priority for the included requirements.

3.1 O-Cloud

Release 3 has refined and extended considerably the requirements for the O-Cloud, mainly, as discussed previously, due to the specifications update. The new security areas addressed have been:

a. **Software package protection**, which includes the need to have the packages certified by testing suites, signed, and validated, to name a few.

b. **Secure update** of the O-Cloud software at the infrastructure layer, covering areas as validation of software images, digital signature verification, and even to have a fallback scenario.
c. **Secure storage** of cryptographic keys and sensitive data, as well as its secure deletion, and dealing with de-allocated resources in VM or containers.
d. **Chain of trust**, to validate hardware and software (O-RAN App/VNF/CNF) up to the hardware root of trust.
e. **O2** (O2dms, O2ims) interface protection, for the communication with the SMO.

3.2 Service Management and Orchestration (SMO)

The entity responsible for managing the entire RAN domain is currently under an intense specification phase (decoupled SMO, RAN-Core data sharing). For this Release 3, the following aspects have been covered:

a. **Event logs**: recording, forwarding, integrity and confidentiality protection. Logging is fundamental to any defense-in-depth strategy and capacitates to detect undesirable behavior.
b. **Interface protection**: security controls are mandated for internal communications and external interfaces, in terms of authorization, authentication, integrity and confidentiality.

3.3 RAN Intelligent Controllers

For the Near-RT RIC, requirements are focused on the security of the interfaces and APIs, and xApp authentication and authorization:

a. **Interface security** for transactional and time critical APIs: authentication must be performed with PKI certificates, for either mTLS or IPsec transport. Authorization must be performed using OAuth 2.0.
b. **xApps security**: the interface between xApps and the Non-RT RIC platform APIs requires mutual authentication using mTLS and authorization using OAuth 2.0

For the Non-RT RIC, center of attention has been put on the authorization requirements for the Non-RT RIC framework, rApps and interfaces, such as A1-EI, A1-P, or R1. These interfaces require mutual authentication using mTLS, and authorization using OAuth 2.0.

3.4 Open FrontHaul interface

Devices must use the IEEE 802.1x protocol to authenticate using EAP-TLS, in order to be authorized to access the O-FH LAN. The O-RU must support the 802.1x supplicant functionality, and the O-Cloud infrastructure and TNEs must support the 802.1x supplicant and authenticator functionality.

O-FH M-Plane functionality will be protected by making use of TLS and/or SSH protocols.

There is ongoing analysis on the use of MACSec for protecting the C-Plane and the U-Plane, and for the protection of the S-Plane using IEEE1588v2 protocol. Requirements may be updated accordingly in the future.

3.5 O1 interface

Management Service providers and consumers shall use the following set of tools/protocols:

a. NETCONF: to manage network devices, retrieve configuration data information and upload and manipulate new configuration data.
b. NACM: to enable operators need to integrate both authentication and authorization with a centralized access management platform.
c. TLS: to provide confidentiality to the communication.

3.6 Software Bill Of Materials (SBOM)

Security, per nature, is a recurrent task, where risks are to be evaluated periodically.

As the NTIA defines, a "Software Bill of Materials" (SBOM) is a nested inventory for software, a list of ingredients that make up software components. Its main goal is to handle safely, across the installed customer base, vulnerability notifications and updates.

The requirements included for the SBOM mandate the need to provide a SBOM with every software delivery package, the minimum data fields, and its depth, according to the software type (OSC, open source software, commercial software). Security requirements for authenticity, integrity and confidentiality protection, as well as for authorization are included.