POINT OF VIEW

Security Considerations in Open-RAN Environments

Introduction

Open Radio Access Network (O-RAN) represents a technological evolution in mobile Radio Access Networks (RANs) with the objective of making them open and smart. RAN openness is achieved via open interfaces, open hardware, and cloudification. A smarter RAN is enabled via deep learning and embedded intelligence within the RAN architecture.

O-RAN's major benefit lies in its ability to enable new use cases via the utilization of machine learning (ML) and artificial intelligence (AI) to empower network intelligence through open and standardized interfaces in a multivendor RAN environment. These new use cases will drive value and growth for the mobile operator.

O-RAN architecture is open and more complex compared to traditional RAN and its associated threat landscape. Therefore, attack vectors are significantly more complex and introduce more potential opportunities for attack and errors that may result in compromised service availability and integrity. It is important that O-RAN architecture's security risks are identified and the appropriate solutions are deployed to face these risks.

Main Security Considerations

The following diagram outlines O-RAN's high-level architecture, its place within the overall 5G system (5GS), and its main cybersecurity areas of consideration outlined in red and discussed throughout the document.

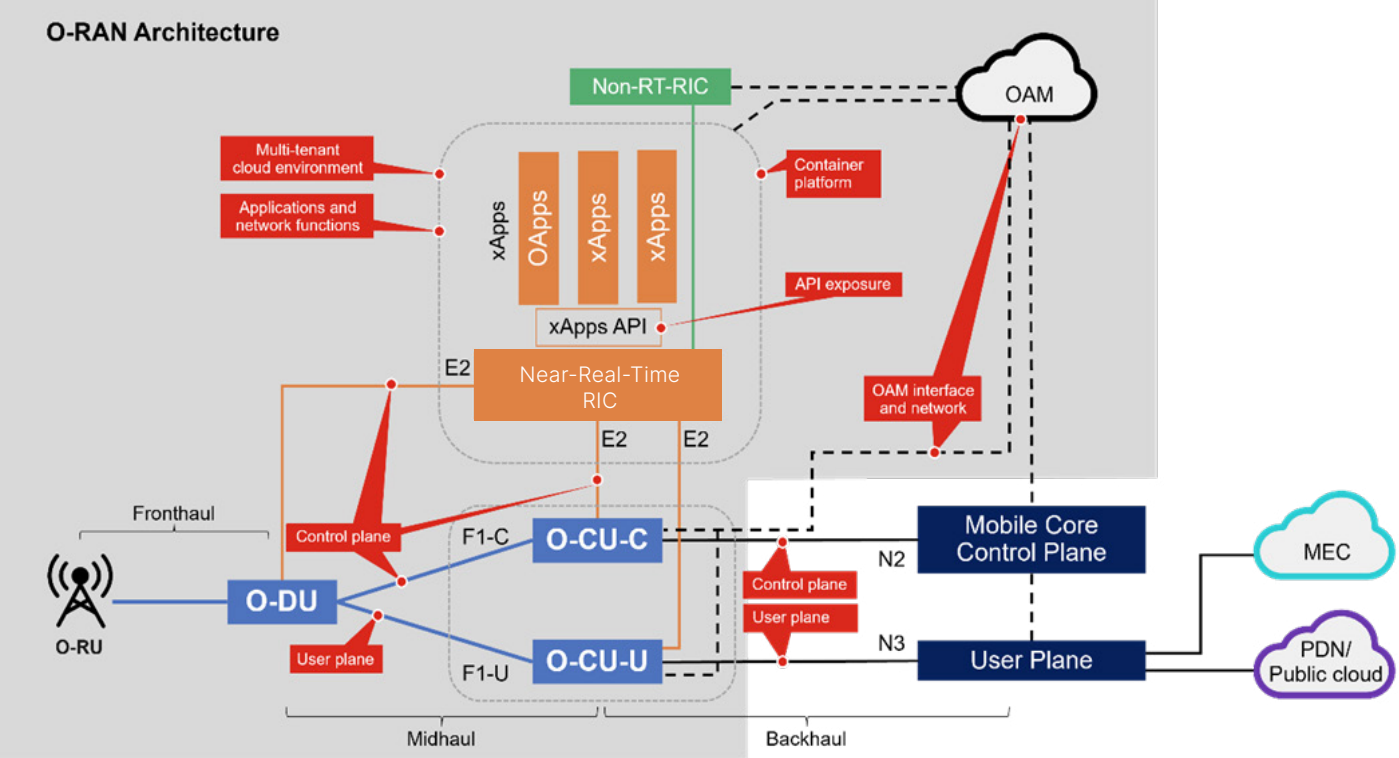

Figure 1: O-RAN Architecture diagram

Multivendor Ecosystem

Traditional RAN solutions have tended to be a proprietary ecosystem that is vendor specific. O-RAN is far more complex due to the increased number of vendors and the disaggregation of network functions. O-RAN heterogenous environments use open interfaces to enable multivendor integration. While the benefits of agility, innovation, and potential cost reduction in such an open and multivendor environment are clear, it puts a greater emphasis on integration and security considerations for operators. Each vendor integrated within the O-RAN environment is potentially expanding the cybersecurity risk via potential code vulnerabilities, the use of open source, and insufficient security hygiene in product development and overall life-cycle management.

Open Interfaces

O-RAN disaggregates the RAN into several components (like centralized RAN or C-RAN) and specifies the protocols and interfaces between them.

O-DU to O-CU components rely on existing 3GPP F1 specifications, which mandate confidentiality and integrity protection via the use of IPSec for the control plane data only, while the user data plane may be left unprotected. This leaves the user plane traffic open to cyberattack risks, which is unacceptable when critical use cases are concerned. Although the control plane data should be protected via IPSec encryption, it does not eliminate cyber risks hidden within the IPSec tunnels originating from O-DU tempering and SCTP control plane protocol-based attacks. Providing IPSec and the ability to safeguard both control and user plane traffic is required.

Open RAN adds new interfaces that are critical to the operation and use cases O-RAN enables.

The E2 interface connects the near-real-time RAN intelligent controller (near-RT RIC) to the O-RAN nodes and enables near-RT service loops through the streaming of telemetry from the RAN and the feedback with control from the near-RT RIC. Although encrypted, this critical interface is running on top of the SCTP protocol, which can be used as an attack vector to manipulate the near-RT RIC.

Embedded Intelligence

An intelligent RAN is crucial to delivering O-RAN's benefits. Intelligence is achieved via a combination of O-DU/CU capabilities and telemetry, near-RT-RIC control and its related xApps. Each O-DU/CU node can publish its capabilities, and the xApps on the near-RT RIC can subscribe to one or more of these functions. The xApps are part of the near-RT RIC. They are microservice-based applications working in a Kubernetes cloud environment and provide the capability to continuously enhance the RANs efficiency, performance, and services. xApps can receive data and telemetry from the RAN components and send back control using the xApps APIs. They can be provided by different vendors, creating a multivendor, multitenant environment.

Near-RT RIC specifications include a security subsystem whose goal is to prevent sensitive RAN data leaks and stop malicious xApps from affecting RAN performance. However, the specification for the module is still under study, and even when completed, it is expected to answer part of the cybersecurity challenges facing the near-RT RIC environment.

The neat-RT RIC is the core of O-RAN and therefore must be safeguarded: the Kubernetes environment in which it operates, the xApps, its API interworking, and any external exposure point such as the southbound E2 interfaces and the northbound A1 and O1 interfaces.

Management Network

An unprotected management interface and components provide an easily exploitable vulnerability in the RAN and the overall 5GS. Thus, the O-RAN mandates that the management interfaces must be protected using industry security best practices. O-RAN operation, administration, and orchestration (OAM) applications and interfaces are part of the overall 5GS OAM network, and every aspect must be protected from potential cyber risks and unauthorized access. Cybersecurity considerations should include zero-trust access, application-level security, API interworking, and any additional exposure.

Conclusion

Open RAN is an exciting step forward in the evolution of mobile networks and services, a step that opens doors to innovation, improved network efficiency and performance, and a more diverse and competitive RAN ecosystem. These can only be achieved via a more open and complex architecture and ecosystem, which enlarges the potential attack surface and increases cybersecurity risks.

To ensure the deployment and success of O-RAN, these cybersecurity risks must be identified, and the solutions and practices needed to mitigate them must be utilized.

January 21, 2023 3:13 AM
1912351-0-0-EN