CTONE

Securing Connectivity in O-RAN systems

Securing the evolving O-RAN landscape against emerging attack surfaces

The global open RAN market is projected to experience significant growth, increasing from USD 1.1 billion in 2022 to USD 15.6 billion by 2027, with a remarkable CAGR of 70.5% during the forecast period. This growth is closely tied to the transformation in O-RAN (Open RAN)) architecture, shifting from proprietary or closed radio access network structures towards open and interoperable systems.

O-RAN emphasizes the adoption of open interfaces, software-defined networking (SDN), and virtualization to enable multi-vendor interoperability and enhance flexibility in deploying and managing radio access networks. Embracing O-RAN principles empowers operators and system integrators to avoid vendor lock-in, foster innovation, and cultivate a more open and competitive telecommunications ecosystem.

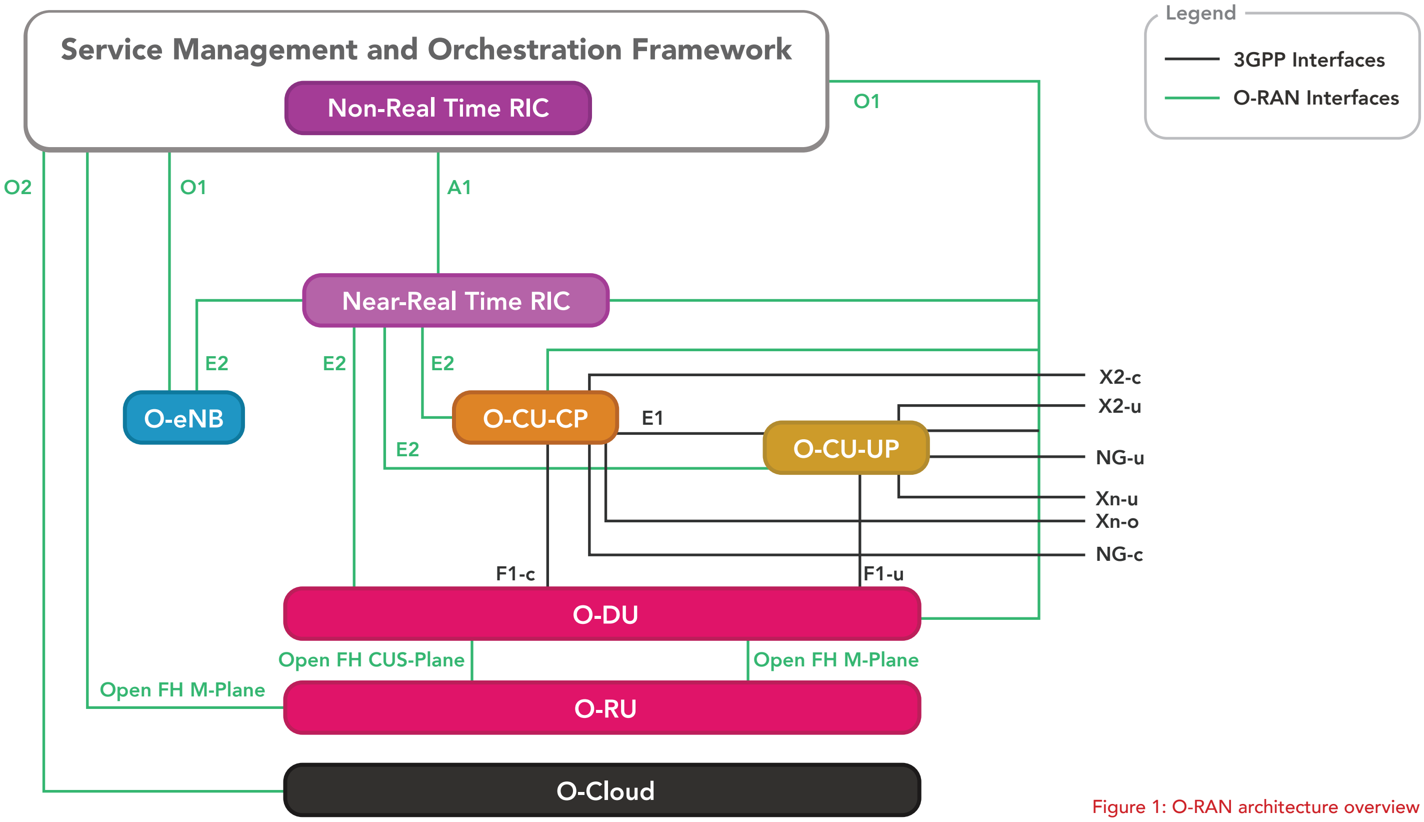


Figure 1: O-RAN architecture overview

What Does Security Mean for O-RAN?

Security in the context of O-RAN refers to the measures and practices implemented to protect the network infrastructure, components, and data from unauthorized access, malicious attacks, and potential vulnerabilities. Security measurement plays a pivotal role in ensuring the network's integrity, confidentiality, and availability, making it an essential element of O-RAN deployment. Within the realm of end-to-end mobile networks, the widespread utilization of Open Radio Access Network (O-RAN) signifies the broad implementation of open and interoperable systems. However, it is important to recognize that this approach may potentially introduce certain vulnerabilities as vendors construct the network environment for private/ public environment. Consequently, new attack surfaces may emerge, highlighting the need to consider innovative O-RAN security solutions before deploying the network. By proactively addressing these concerns, organizations can ensure the safeguarding and resilience of their mobile network infrastructure.

Emerging New Attack Surface in the O-RAN World

It is crucial to address these **challenges** to ensure the security and integrity of open RAN networks.

1 **TRANSITIONING FROM CLOSE TO OPEN SYSTEMS**
Open RAN architecture expands the potential attack vectors and pathways for hackers to target the O-RAN system, presenting increased security risks.

2 **NEW INTERFACES IN O-RAN**
Such as A1, E2, O1 etc., are emerging as the new attack surface within the OPEN structure.

3 **SUPPLY CHAIN RISK**
The shift from single-vendor reliance to a multi-vendor supply chain introduces increased risks of attacks and compromises.

4 **CT (Communication Technology) IS GRADUALLY BECOMING IT-ORIENTED**
The widespread adoption of virtualization technologies on Commercial Off-The-Shelf (COTS) servers and open-source software, leads to more security risks from IT technologies.

5 **OPEN SOURCE UTILIZATION**
The transparency and accessibility of open-source components expose O-RAN systems to vulnerabilities in unknown circumstances.

Securing Your O-RAN World: CTOne RAN Protection

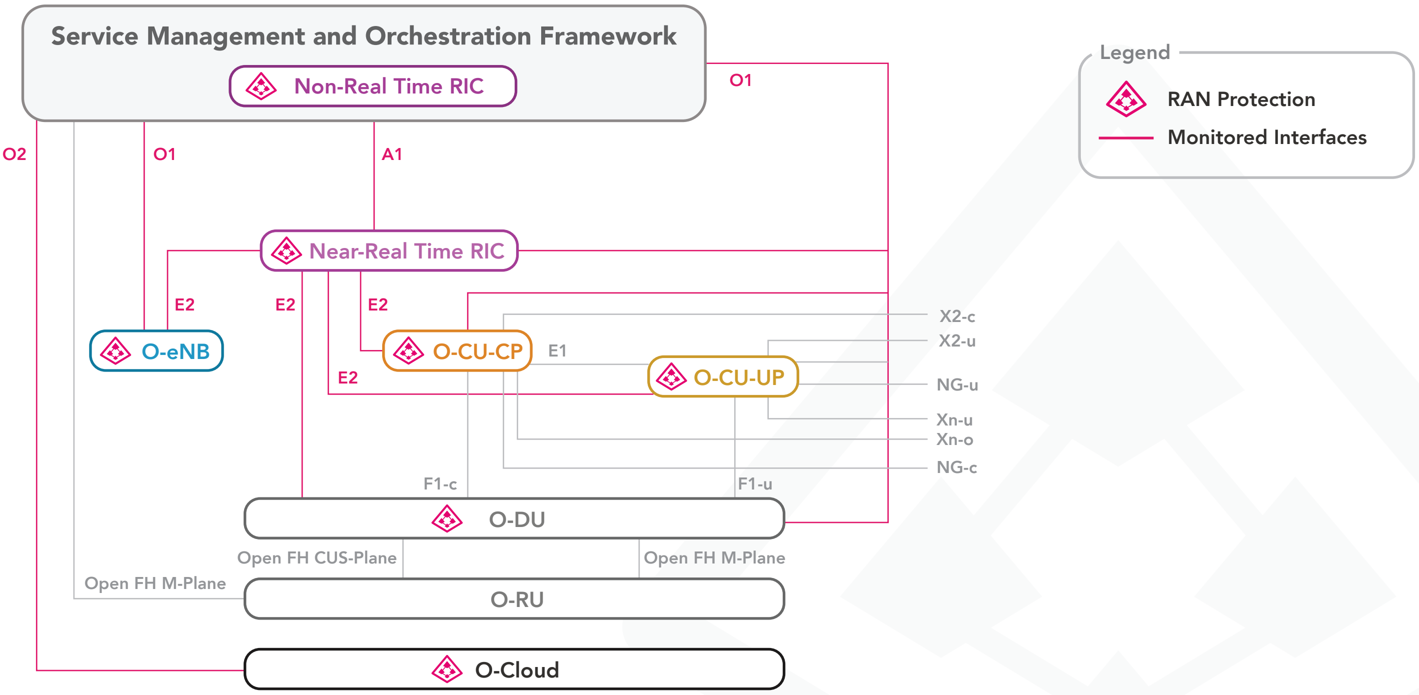
CTOne RAN Protection is a tailored cybersecurity solution that covers both IT and CT domains, specifically designed for O-RAN systems, and deployed on the O-Cloud platform to protect the key elements in O-RAN system. It monitors the host server, O-RAN interfaces, and generates SBOM (software BOM) exchangeable data, enabling seamless collaboration with third-party SBOM management systems and ensuring compliance with security regulations.

Visibility of O-RAN System

SBOM profiling is crucial for transparency, vulnerability management, compliance, incident response, and informed decision-making. It enhances software security, mitigates risks, and improves overall system resilience. CTOne RAN Protection generates SBOM exchangeable data and vulnerability exploit information, providing a comprehensive view of the O-RAN system's software landscape. It promotes visibility, facilitates collaboration with third-party SBOM management systems, and ensures compliance with security regulations.

Real-time Protection

CTOne RAN Protection provides a proactive security measure that monitors critical system files and configurations for any unauthorized changes or tampering. By continuously comparing the current state with trusted baseline values, it helps detect potential security breaches, ensuring the integrity and security of the system. Furthermore, RAN Protection encompasses the identification and mitigation of potential network exploits within O-RAN software.



Enhance Your Connectivity with Holistic Mobile Networks Security

CTOne offers a completely private 5G security solution for enterprises, protecting their entire network, including IIoT endpoint devices, O-RAN systems, edge computing applications, and core networks. This turnkey solution is designed to provide comprehensive protection without requiring substantial investments or management costs. By bridging the gap between IT and CT, CTOne ensures the security of both network and endpoint layers, addressing the evolving cyber threats faced by businesses in 4G/LTE and 5G networks.

> “Empowering Secure Connectivity in an Open World”

About CTOne

CTOne, a global cybersecurity leader in communication technology, offers enterprise cybersecurity solutions for next-generation wireless networks. A subsidiary of Trend Micro, CTOne enables digital transformation and strengthens the resilience of communication technology.

www.ctone.com