SecurityGen

Telecom Security. Transcending Generations.

RAN/O-RAN ARCHITECTURE: NEW OPPORTUNITIES AND SECURITY CHALLENGES

Author: Paolo Emiliani, Co-Founder & Global Head of Operations

Past two decades, the telecom sector has witnessed a massive transformation - from 3G to 4G and now the emergence and accelerated adoption of 5G technology. All through this time, the primary focus of MNOs has been on offering augmented services and secure elevated experiences while striving for efficiency and business agility to address new revenue streams. This continues with 5G, which is set to change our life further in the coming times.

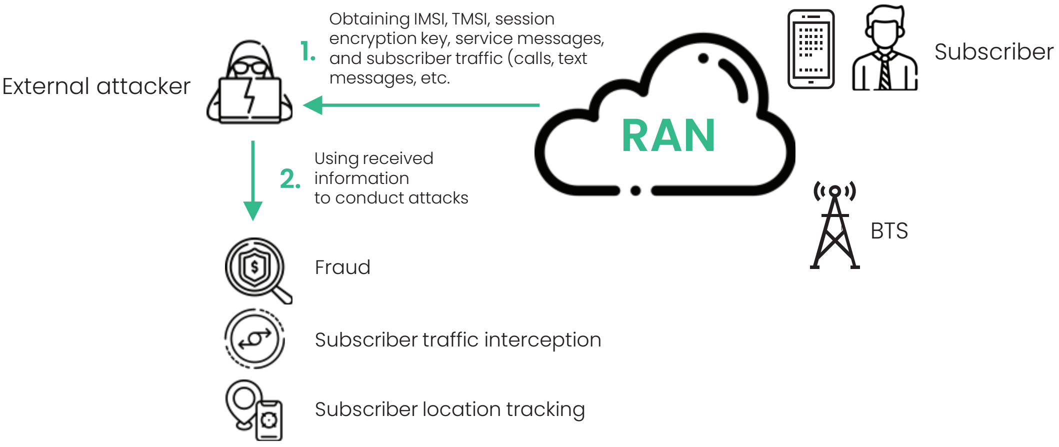
To unleash the full potential of 5G – faster speed (enhanced bandwidth), massive machine type connections, and more reliable low latency communication, there is an urgent need to build the right and secure telecom ecosystem. Security, performance, interoperability, and auditable compliance will be the bedrock of a robust 5G system roll-out.

But this evolving telecom landscape, replete with numerous connected devices, virtualisation techniques, and open networks, has also resulted in and will continue to expand the attack surface—a significant security concern for the MNOs.

Complex telecom ecosystem: Rising security vulnerabilities

The new radio generation of threats via new interfaces, growing API/applications, virtualisation & containerisation have compounded the existing vulnerabilities within the outdated software stacks and non-easy patchable issues on the air interface front. This complex environment and the increased threat surface offer a potential pathway for adversaries to launch numerous malicious activities aimed at - data interception, accessing sensitive information and violating network operations.

- By exploiting vulnerabilities within the encryption algorithms, an attacker can easily decrypt the transmitted data. Additionally, the persistent age-old challenge of inadequate protection from the IMSI-Catcher or FakeBTS to which telecom subscribers are connected presents another threat vector for data interception. Leveraging the vulnerabilities, an intruder can listen to subscribers' conversations, steal sensitive information, modify the transmitted data, and use the information for criminal purposes-conducting fraudulent transactions, launching social engineering attacks against subscribers along with a host of MiTM attacks.


External attacker
1. Obtaining IMSI, TMSI, session encryption key, service messages, and subscriber traffic (calls, text messages, etc.
RAN
Subscriber
BTS
2. Using received information to conduct attacks
Fraud
Subscriber traffic interception
Subscriber location tracking

- Additionally, exploiting the lack of protection against cloning mobile subscribers, IMEI duplication, and with the use of mobile devices crafting TMSI value, a hacker can bypass the billing system and use resources without charge. Using a similar technique, the malicious actors can compromise the network by organizing DoS attacks or using jammers to degrade or deny authorized and legal communications.

The evolution of the 5G era characterised by a rapid rise in intelligent connectivity has resulted in mobile communications connecting many critical infrastructures, including industrial control systems and ATMs. The high bandwidth and reliability, low latency premise of 5G will propel the mobile ecosystem into new paradigm – of massive IoT connectivity. But to realise this potential, the Telecom industry needs to transform and equip their ecosystems to scale and drive new services and enhanced efficiencies.

O-RAN: The new age architecture to drive scalability and efficiency

With changing times, reducing costs, and generating revenue from new service opportunities has become crucial for the MNOs. There have been numerous advances on the RAN (radio access network) to enable this by creating flexible, scalable, and cost-efficient network models. With O-RAN being the most recent and the most -talked-about development. And more so in the 5G context.

RAN infrastructure accounts for nearly 60-70% of the MNO's CAPEX and OPEX. Additionally, the traditional RAN architectures built on proprietary software and purpose-built hardware are complex by nature and limit flexibility. 'Open' RAN – is the technology intended to disaggregate hardware and software and create open interfaces, which will help reduce costs and promote a new ecosystem for service innovation.

The main objective of this architecture is to impart flexibility to MNOs by breaking the vendor-lock-in, thus resulting in a significant reduction in CAPEX and OPEX for their radio access networks (RANs). As operators look to manage cost and enable intelligent connectivity through 5G, O-RAN provides the platform for flexibility, interoperability (between devices, networks, and vendors), and agility.

The different types of architectures:

- **Open-RAN** (note the confusing hyphenation): Replacing the legacy, proprietary interfaces between the baseband unit (BBU) and the remote radio unit (RU) with open standards enables units from one vendor to interoperate with units from the other vendors

- **Virtual RAN (vRAN)**: By virtualising (and containerisation), the baseband unit can now run as software on generic hardware platforms. With this, the baseband, radio software and hardware, and even different software and hardware components can be supplied by other vendors.

- **Centralised/Cloud RAN (C-RAN)**: Concentrating and consolidating the baseband functionality across a smaller number of sites spread across the telco's network and cloud setup.

Leading O-RAN industry bodies: Driving the change

- Telecom Infra Project (the OpenVPN project group) is an initiative to define and build 2G, 3G, and 4G RAN solutions based on general-purpose, vendor-neutral hardware and software-defined technology, or the OpenVPN 5G NR project group, which focuses on 5G NR).

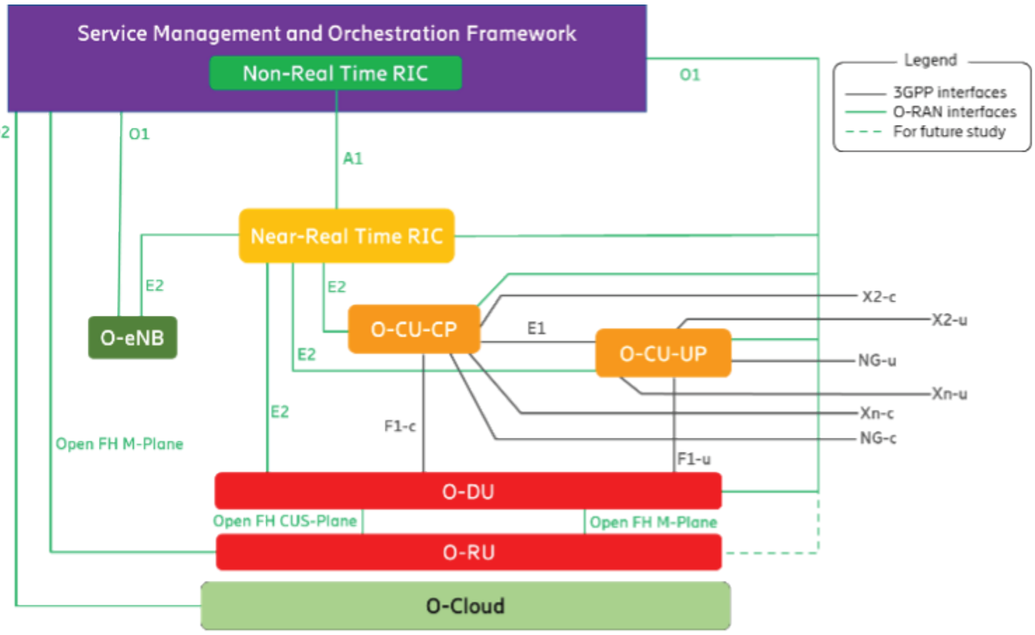
- "O-RAN" and "ORAN." O-RAN with the hyphen refers to the O-RAN Alliance, which publishes new RAN specifications, releases open software for the RAN, and supports its members with integration and testing services. "ORAN" can also be used to refer to the Open RAN movement; however, O-RAN with the hyphen largely refers to the O-RAN Alliance. #oRAN or #ORAN are also used as hashtags on social networks and often referred to as either the O-RAN Alliance or the Open RAN architecture.

O-RAN: components, interfaces, and platforms

- **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, OeNB

- **Cloud computing platform**: O-Cloud comprising the ensemble of physical infrastructure nodes that meet O-RAN requirements to host the O-RAN functions (Near-RT RIC, O-CU-CP, O-CU-UP, O-DU), the supporting software components (OS's, Virtual Machine Monitor, Container Runtime), and the appropriate management and orchestration functions.

- **Relevant interfaces in O-RAN:**



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 - O2 Interface between the SMO and the O-Cloud - E2 Interface connecting the Near-RT RIC or more O-CU-CPs/UPs/DUs/O-eNBs - Open Fronthaul CUS-Plane Interface between O-RU and O-DU - Open Fronthaul M-Plane Interface between O-RU and O-DU and between O-RU and SMO.

O-RAN: Multiple interfaces and heightened security challenges

In general, this "Open" RAN architecture differs from the architecture of 3GPP RAN, with third-party software, which on one side presents a more flexible and cost-effective solution. But on the other side, new components, complex interfaces, multiple software stacks, and technologies mean an expanded threat surface area and potential new attack vectors.

These O-RAN scenarios will raise numerous security challenges and resulting risks due to the new specific interface and components to check, the virtualization / containerization security to check, the support of open-source code, and the capability to support an AI/ML model, etc with various interfaces. All of this will create enhanced complexity and new expected vulnerabilities & threats. Thus, it is critical to assess the model and implement a comprehensive zero-trust-based security-by-design approach to ensure security, resilience, and unmatched performance of the complex 5G environment

O-RAN: Enhanced security protocol

- TLS: This will help protect the traffic between the O-RAN system and other network elements. Establishing a secure channel will ensure CIA (Confidentiality, Integrity, Authenticity) features. Should be used in O1 Interface for NETCONF over TLS and JSON/REST over TLS. It should be used in the A1 Interface.

- SSH, IPSEC, FTP, and FTPS: SSH should be used in the O1 Interface, and Fronthaul M-Plane for NETCONF, IPsec, FTP and FTPS should be used to protect E2 traffic & file transfers over O1.

- PTP (Precision Timing Protocol, IEEE 1588-2019

References

[1] 3GPP TS 33.511 V16.4.0 (2020-07): Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class

[2] O-RAN Alliance architecture & design O-RAN ALLIANCE

[3] ENISA threat landscape for 5g networks

About SecurityGen

Founded in 2022, SecurityGen is a global start-up focused on telecom security. We deliver a solid security foundation to drive secure telecom digital transformations and ensure next-gen enterprise intelligent connectivity.

Connect With Us

✉ Email: **contact@secgen.com**

🌐 Website: **www.secgen.com**

UK | Italy | Czech Republic | Brazil | Mexico
India | South Korea | Japan | Malaysia