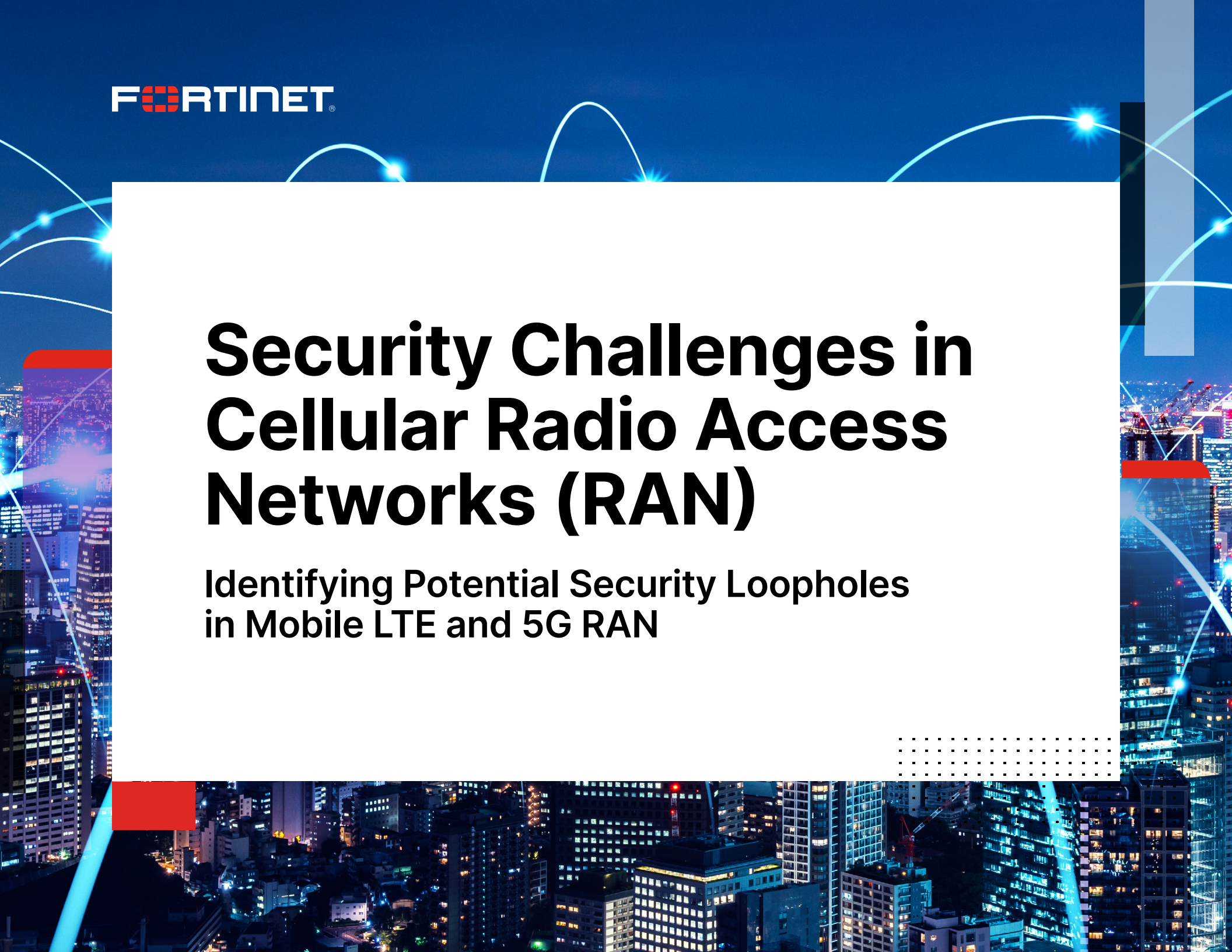


Security Challenges in Cellular Radio Access Networks (RAN)

Identifying Potential Security Loopholes in Mobile LTE and 5G RAN

Table of Contents

Executive Overview

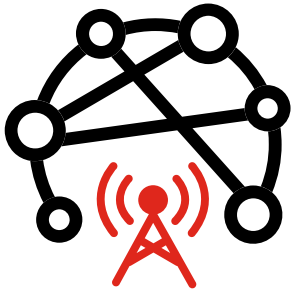
Long-Term Evolution (LTE) and 5G new radio (NR) are fundamental components in a mobile network operators' (MNOs) ability to deliver upon the promise of 5G and growth. It is fundamental for realizing 5G's cornerstone capabilities: high bandwidth, massive scale, native machine communications, high reliability, and low latency.

As enterprises contribute to an increasing part of mobile providers' revenue and margins, their demand for a secure set of public and private mobile services cannot be ignored. And as existing and new mobile radio networks are constantly evolving, so are their complexity, attack surface, and associated risks. Therefore, securing the radio access network as part of the overall mobile user and control planes is not only recommended, it's mandatory.

The 3rd Generation Partnership Project (3GPP) recommends using Security Gateways (SecGW or SEG) to secure the RAN and RAN to core communications to ensure service continuity and confidentiality. The 3GPP Security Gateway relies on Internet Protocol security (IPsec) and certificate management capabilities to provide access control through authentication and traffic confidentiality and integrity through encryption.

In the following pages, we will briefly discuss some of the mobile RAN evolution and its impact on complexity, security, and risk.

Mobile providers should consider resolving these main areas of RAN security priorities as part of their overall LTE and 5G deployment and service strategy.



"...[mobile networks'] importance is likely to grow significantly in the coming years, with critical services or critical infrastructures... As a result, the security, trustworthiness, and reliability of 5G networks are of great social relevance."[1]

Scalability Is Essential

To enable the growing scalability delivered by LTE-A and especially 5G, the deployment of an increasing network of small cells is required. Many of these femtocells', picocells', and microcells' eNodeBs (eNB) and gNodeBs (gNB) will be in the public domain and in other non-secure locations. These will also be, in many cases, connected to the MNO network via untrusted backhaul. These combined factors represent a growing risk that contributes to the increase in overall attack surface and risk for traffic tampering, misuse, and manipulation.

A growing number of eNBs and gNBs provide connectivity to an ever-growing number of devices, with various bandwidth and latency requirements, serving consumers or providing capabilities and services in utilities and other critical infrastructure. The exponential rise in connected devices runs the risk of distributed denial-of-service (DDoS) attacks, such as signaling storms, that can downgrade the services the mobile network provides or even take it down.

User Plane Traffic: Where Value Lies

The ongoing evolution of 4G and the introduction of 5G is gradually enabling the implementation of use cases that provide value beyond plain wireless connectivity. Mobile providers can now build use cases in which whole ecosystems combine to create and facilitate innovation in manufacturing, healthcare, transportation, energy, and other sectors.

Providing “beyond connectivity” services puts growing importance on the integrity and continuity of user plane traffic in the RAN and onto the multi-access edge computing (MEC) sites, enterprise networks, and any external networks. User plane traffic will become one of the most essential pieces of the operator ability to provide value-added services, such as infotainment, Internet-of-Things (IoT) services, and augmented reality (AR), just to name a few, as users’ data-target applications/services reside within the Telco Cloud or the overall use-case ecosystem.

This drives the need for greater security, integrity, and continuity of the user plane data, which will experience significant growth in some use cases in the RAN, alongside control plane and operations and management (O&M) traffic.

Diversified RAN Architectures

The need for better RAN performance, agility, scalability, flexibility, and cost-effectiveness has led to its gradual evolution in LTE and 5G. As a result, MNOs will be operating a hybrid RAN environment composed of different centralized, distributed, and virtualized/cloud architectures.

RAN architectures will also depend on specific use-case requirements per market segment or network slice. For example, the location of the eNBs and gNBs distributed and centralized units (DU and CU) will depend on requirements such as latency and bandwidth/performance requirements.

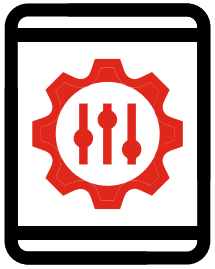
Maintaining security, integrity, and visibility for control in such a hybrid environment is mandatory. And O&M will be required via a common set of security tools flexible enough to adapt to the RAN's different architectures.

RAN Sharing

Deploying RAN infrastructure in sparsely populated areas is expensive, with a lower return on investment (ROI) than in densely populated areas. This is true for LTE and even more so for 5G NR, where a more significant number of base stations and small cells may be required.

Competing operators in many countries are reducing RAN costs and overall total cost of ownership (TCO) via actively sharing their RAN network, also known as RAN sharing. This allows competing operators to use the same RAN while keeping the mobile core separated.

RAN-sharing operators must therefore ensure their users' traffic is completely isolated from their competitors' users' traffic sharing the same RAN to ensure integrity, privacy, and protection against user equipment (UE)/RAN-originating attacks.



According to GSMA Intelligence survey, mobile operators consider security investment as the highest operational priority in enabling them to achieve their long-term enterprise revenue goals.[2]

The Open RAN/Cloud RAN Security Challenge

The aim of open RAN/cloud RAN is to make the RAN more independent of proprietary technology by defining specifications for open interfaces and abstracting network elements and functions from the hardware. Open RAN creates an open environment, allowing an ecosystem of vendors to provide RAN building blocks, thus encouraging RAN programmability, service innovation, and greater choice for the mobile operator.

This is achieved by disaggregating the RAN into several building blocks where open and standard interfaces and protocols are defined to interconnect and interwork among the different RAN elements. Important elements of RAN automation and programmability are delivered via the introduction of cloud-native controllers and applications.

Such an environment (with disaggregated function and an ecosystem of vendors, interfaces, protocols, controllers, and applications) represents a significantly larger attack surface where several key elements can be a target of cyberattacks and therefore must be protected to ensure RAN availability and continuity.

Critical Infrastructure

Both public and private LTE and 5G are today providing—and will continue to enhance and provide—an even greater set of critical capabilities, use cases, and innovation in many sectors and industries, such as healthcare, manufacturing, energy, and transportation.

Mobile infrastructure's technology "standardization" and the growing reliance on its services for critical organizations, industries, and use cases will make mobile networks easier targets for attacks and create attack vectors for their enterprise customers. This further drives the growing need for RAN security as part of the overall security visibility and controls for the mobile network and ecosystem.

[1] Germany Federal Office for Information Security: Open RAN Risk Analysis 2022

[2] GSMA Intelligence Operators in Focus: Enterprise Opportunities 2021

FORTINET®

www.fortinet.com

July 15, 2022 8:23 AM

1662637-0-0-EN