Built-in Security Unlocks 5G

Radio access networks (RANs) are the nervous system of today's wireless communications and have been since the inception of cellular service. Throughout their history, a select few network equipment providers (NEPs) like Ericsson, Nokia, and Cisco have built the entire solution stack for these network onramps, from routing equipment to security appliances.

Security technologies in particular have been tightly integrated with the RAN architecture, consisting of solutions like proprietary countermeasures built into networking equipment, security gateways, and firewalls. This security has proven more or less sufficient in RAN deployments to date, but as networks demand more performance and flexibility through multi-vendor ecosystems like OpenRAN, these practices will have to change.

From a pure business perspective, a primary driver of this change is the proprietary nature of RAN equipment. Unfortunately, the limited vendor ecosystem has resulted in higher costs than a more open marketplace, and little interoperability among RAN vendors, whose single-source solutions keep margins high.

5G and OpenRAN

One of the goals of future RAN development is to tackle these challenges by maximizing the use of common, off-the-shelf hardware. As edge networks transition to the increased throughput and latency of 5G, initiatives like OpenRAN offer a new, software-driven approach to RAN deployment that can improve network flexibility, interoperability, and lower cost.

There are multiple versions of OpenRAN—including one specifically for the 5G New Radio (5G NR) project—but the one most relevant to this discussion is a broad initiative managed by the Telecom Infra Project **(Figure 1)**. This flavor of OpenRAN seeks to "define and build 2G, 3G, 4G, and 5G RAN solutions based on general-purpose vendor-neutral hardware, open interfaces and software," which applies to all sorts of networking equipment.

It would appear that OpenRAN is poised to deliver for the edge what SDN and NFV did for the cloud/data center, so long as the networks based on it can be sufficiently secured across solutions from multiple vendors.

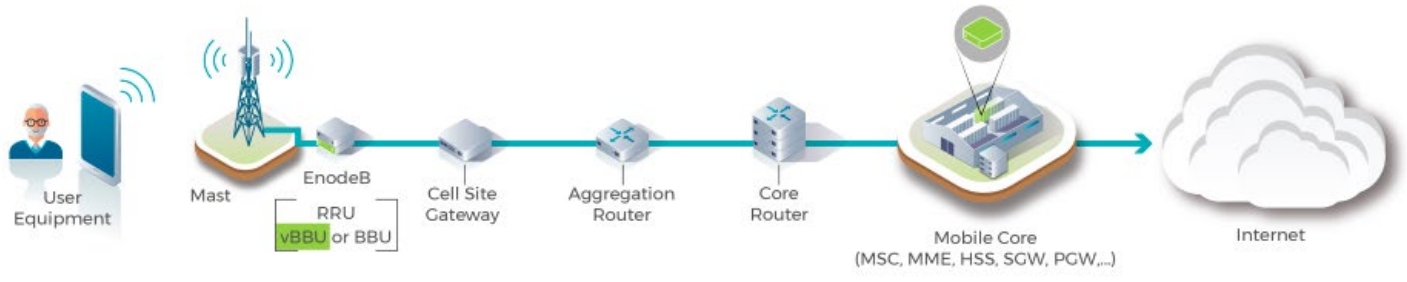

Figure 1. The OpenRAN initiative distributes open, general-purpose networking hardware across radio access networks. (Source: Telecom Infra Project)

Open, Yet Secure

Disaggregating network infrastructure and opening the traditional RAN model does raise concerns about how these deployments will be protected. Compared to the past, security on OpenRAN networks will have to consist of a chain of trust that extends across equipment supplied by multiple vendors. In many cases, this includes hardware from different suppliers at the same cell site or base station.

Platforms like the 3rd generation Intel® Xeon® Scalable processors (previously called Ice Lake SP) integrate a battery of features that protect open networks from uncertainty. These include the ability to identify whether other network entities can be trusted, controlling where data and workloads can be safely deployed on RAN infrastructure, and guarding against advanced malware.

The processor achieves this through a multilayered security stack that reaches from the silicon out to the application layer and onto the network itself:

- **Intel® Total Memory Encryption (Intel® TME)** protects the physical memory of the device—including any data stored in the memory, such as platform firmware and software-provisioned security keys.
- **Intel® Platform Firmware Resilience (Intel® PFR)** leverages the integrated Intel® MAX 10 FPGA technology to monitor system buses for malicious traffic and verify the integrity of firmware before execution.
- **Intel® Software Guard Extensions (Intel® SGX)** use hardware-assisted confidentiality and integrity mechanisms to partition application code and data into secure memory enclaves of up to 1 TB. Once there, even higher-privilege processes or an untrusted OS cannot access or modify it.
- Novel techniques like **Multi-Buffer** and **Function Stitching** combine with other hardware and software innovations on 3rd gen Intel Xeon Scalable processors to improve cryptographic algorithm execution performance by as much as 8X over the previous-generation microarchitecture.

Revolutionizing RANs with a Secure Foundation

All of these measures are available in the NA870 Rackmount Network Appliance Platform **(Figure 2)** from Axiomtek, an IPC and embedded systems design and manufacturing company. The appliance is based on dual 3rd gen Xeon Scalable Processors with up to 40 CPU cores that incorporate all of the security mechanisms mentioned above. The systems also include a trusted platform module 2.0 security chip to further extend the integrity provided by the Intel security technologies.

Figure 2. The Axiomtek NA870 2U rackmount network appliance. (Source: Axiomtek)

The OpenRAN-ready NA870 integrates up to 66 LAN ports via 8 LAN expansion modules, including 100 GbE networking cards, as well as two PCIe gen 4.0 x16 expansion slots that provide roughly 256 GT/s of throughput each.

These interface options, combined with the performance and virtualization capabilities of the two onboard Xeon processors, allows the NA870 to accommodate many different traffic types flowing across edge RANs simultaneously and securely.

And it accomplishes this without using any proprietary or single-source technology.

Opening New Ecosystems Through Security

As we move away from monolithic networks and toward the kind of market competition that has previously been missing in this space, 3rd gen Xeon processors offer the flexibility to meet the requirements of a new ecosystem of OpenRAN vendors. And they come with built-in integrity and trust technologies that tie the ecosystem together.

Vendors like Axiomtek are now capitalizing on this foundation to support a new generation of edge access networks that are more affordable, more efficient, and more secure.