Open RAN
POLICY COALITION

5G and Open RAN Security: Next Generation Trust

Open RAN: Secure Open Interfaces

One of the common misconceptions about an open RAN is that open interfaces introduce security risk. In fact, these same open interfaces, defined in technical specifications, provide a foundation and architecture for improving security. Although operators procure and integrate open RAN network functions in new ways, operators bring the same expertise, diligence and requirements for security and resilience to these environments.

5G and an open RAN also enable new capabilities and control points that allow suppliers, test equipment manufacturers, wireless carriers and network operators to assess and to manage security risks. Because an open RAN is a fundamentally open architecture, it opens the ecosystem to new suppliers, increasing the diversity of virtualized RAN solutions.

Network enhancements inherent to 5G architectures, such as Multi-Access Edge Computing (MEC), provide the opportunity for improved security by enabling capabilities presently deployed in core networks, such as network monitoring for security threats, to be pushed closer to the edge. Network slicing can also enable isolated network capacity for highly critical use cases separate from general Internet traffic. Open interfaces also support more virtualized network functions, enabling additional security controls through micro-segmentation and containerization.

5G Security

While 5G delivers many breakthough benefits, security is the first priority, not an afterthought. 5G networks introduce advanced security features, which include enhanced subscriber privacy, secure communications, and secure intra-operator and inter-operator communications. 5G networks also bring significant security enhancements in multiple areas:

- Standards driving transparent and vetted security, interoperability and trust.
- Cloud architecture ensuring resilience, scalability and segmentation and the introduction of Multi-Access Edge Computing (MEC)
- Microsegmentation, containerization and virtualization providing enhanced security and isolation from the hardware up.

Standards Drive Interoperability and Innovation

Standards play an important role in 5G security and an open RAN. The opportunity to build open, interoperable and standards-based 5G networks has already begun to spur innovation and competition among diverse companies worldwide, enabling greater security for 5G. Standards development organizations, including but not limited to 3GPP, GSMA, ETSI, the O-RAN Alliance, and the Telecom Infrastructure Project (TIP) help grow the ecosystem by enabling new and existing technology providers and wireless carriers to rapidly align on security requirements.

Open standards help users and network operators better understand, align on, and demonstrate successful implementation of security requirements. This effectively grows the market for 5G solution suppliers as network operators have the option to chose from a variety of suppliers and increasing the opportunity in the ecosystem and for solutions providers to offer standardized solutions to many operators, instead of developing unique, one-off solutions for individual carriers. Most importantly, operators and suppliers can coordinate new information about threats, vulnerabilities and exploits, allowing greatly accelerated development and deployment of mitigations.

5G and Open RAN: Built on Cloud

5G is built on cloud architecture – the same cloud architecture that is the bedrock of today's internet and the public cloud. Cloud architecture allows for rapid, standards-based deployment of infrastructure as needed. It is a far more scalable and dynamic approach than the long cycles needed to develop, test, deploy, and configure for fixed function network appliances.

For example, in response to live traffic on the 5G network, with a cloud architecture, the 5G core can immediately detect the need, and automatically provision and deploy capabilities as needed. Network operators have seen this dynamic play out as they provision their networks in response to the unprecedented demands placed on networks during COVID-19. These developments will increase network resiliency.

5G cloud architecture also facilitates improved network segmentation, allowing grouping and separation of security sensitive network functions. The same architecture allows the deployment and lifecycle management of entire use cases using "network slicing." Because a network slice is effectively a complete end-to-end network, each slice will include security appropriate to its own requirements and can be developed and deployed as a slice. Different network slices can also run side by side for different purposes and have their own security requirements applied to meet their respective needs.

The 5G architecture also introduces new security capabilties including: (1) leveraging Multi-Access Edge Computing (MEC) to collate and process sensor traffic at a factory, for example, or to shift Distributed Denial of Service (DDoS) detection and mitigation to the edge of the network to enhance the ability to respond to attacks and reduce potential broader network impact; (2) strengthening encryption to 256-bit end-to-end encryption for the over-the-air interface and encryption of each device's International Mobile Subscriber Identity (IMSI) to further secure consumer device-specific information; and (3) establishing a security edge protection proxy that will mitigate vulnerabilities in prior technology (*e.g.,* SS7 and Diameter) and attacks when subscribers are roaming between different carriers' networks.

Software-based Networking and Virtualization

An open RAN takes advantage of the migration towards software-based networks and virtualization. These are concepts that have been deployed in networks for several years in the core and backbone networks and are now being increasingly introduced in the RAN. A software-based network moves the network functions to software as opposed to the past, where network operators would deploy purpose-built physical appliances for network functions. Software-based functions and virtualization enable the replacement of costly, purpose-built hardware devices with general purpose servers found in every cloud data center.

From a security perspective, software-based networking and virtualization enables techniques such as sandboxing, microsegmentation, containerization, and network slicing. There are also important trust and security capabilities of virtualization enabled by modern hardware and processors. The end result is that through the advancements of hardware and virtualization, operators have more tools to ensure the security and resilience of the network.

Conclusion

Open RAN standards have attracted a dynamic ecosystem of carriers, vendors and suppliers that will enhance innovation, open up new markets and improve the scale and performance of 5G networks. The requirements of throughput, performance and latency that will be placed on the 5G network will require scale and dynamism that have not been present in traditional mobile networks. Open RAN standards open the door to software-based networks, virtualization and cloud computing to meet these requirements. Bringing these capabilities to 5G will deliver a next generation, secure network that will drive commerce, innovation and society into the future.