Open RAN
POLICY COALITION

Open RAN Security in 5G

April 2021

A common issue raised about Open RAN is the security challenge created by shifting to a disaggregated or "open" environment. While there are certainly generic security risks such as malware, botnets, and other forms of attacks that are potential risks regardless of the underlying architecture, security controls exist in enterprise-grade security to meet the common challenges, and there are new capabilities enabled by 5G that will improve security both for traditional and Open RAN. At the same time, the benefits of innovation and supplier diversity in an open ecosystem will bring forward additional diverse security solutions to address potential threats and mitigate risk because of the ability to monitor, detect, prevent and respond more quickly.

1. 5G Security Benefits

5G networks will have improved security and subscriber privacy in comparison to previous generation networks. Several innovations in a secure network design framework and wireless technology will intersect to create a highly secure and resilient 5G network. We will have more agile and layered security as we transition from centralized core and radio access networks to distributed, virtual networks. As we shift the compute functionality closer to the edge, network operators are implementing new and embedded security functionalities to ensure a highly secure mobile network. These include Distributed Denial of Service (DDoS) detection and mitigation at the edge of the network to enhance the ability to respond to attacks and reduce potential broader network impact; stronger encryption for over-the-air interface and encryption of SUPI to further secure the communication as well protect consumer privacy information; and Security Edge Protection Proxies that will mitigate vulnerabilities in prior technologies (e.g., SS7 and Diameter) when subscribers are roaming between different carriers' networks.

All implementations of 5G will benefit from these enhancements. Likewise, the 5G Core adopts Service Based Architectures, a foundational change in mobile architectures that brings flexibility in communication between elements in IT or cloud architectures. This shift enables a range of security controls to be applied in 5G networks that were previously unavailable. A common principle that can be applied to 5G networks is the concept of "zero trust" networking. This is the principle that anything that connects to a network should inherently not be trusted unless it can be verified. This differs from traditional network architectures that relied on security at the perimeter and once a user or device was permitted access it could move freely within a network.

Zero trust networking can enhance security in a variety of ways: (1) by securing the technology and application stack including all interfaces and application programming interfaces (APIs); (2) by leveraging the cloud-based nature of 5G and deploying cloud security functionality and telemetry; (3) by enabling

tailored and customized control of security via network slicing; and (4) by deploying multiple layers of authentication. The development of these advanced security features and capabilities are underpinned by a robust standards development ecosystem that is facilitating greater security in 5G generally and in areas essential to enabling more open network architectures.

a. Securing the Technology and Application Stack

To secure the technology and application stack, it is necessary to secure all layers, interfaces and APIs, and all attack surfaces, in an automated manner. "All layers" refers to the signaling, applications, management, and data layers in network implementation, whether based upon a closed or open architecture. In both implementations, a variety of security detection and control mechanisms can be applied across the various layers: signalling, applications, management, and data.

The same applies to interfaces and APIs. An API is a type of computing interface that defines interactions between multiple software intermediaries, such as the kinds of calls or requests that can be made, how to make them, the data formats that should be used, and the conventions to follow. APIs have specific forms and characteristics (e.g., input types, value ranges) that dictate their behavior. There are numerous ways operators can secure APIs; for example, authentication, access control, monitoring for suspicious activity, and encryption and integrity protection mechanisms can be applied where appropriate in either an open or closed system.

The security controls placed around layers, APIs, and monitoring the attack surface can all be deployed in an automated fashion. This is critical as cyber-attacks are constantly evolving in both pervasiveness and sophistication. The current reality is that yesterday's reactive security is incapable of addressing the evolution of technology and the new threats brought with it. Fortunately, operators can use closed loop automation and machine learning (ML) to analyze vast amounts of telemetry data, recommend security policies, and proactively assist in intelligently stopping attacks and threats.

b. Cloud Security

In addition to securing the technology and application stack, a major component of 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. These concepts enable a more scalable and dynamic approach than the long cycles needed to develop, test, deploy, and configure for fixed-function network appliances. Because 5G is building upon similar concepts to the cloud, operators take advantage of cloud-specific security controls.

Technologies can be deployed to secure the cloud architecture, across the entire development lifecycle leveraging secure development lifecycle practices in particular during the "build" stage, when developers are pushing code into the cloud, as well as the operations and maintenance stage. Cloud security in particular uses practices that support security assurance and compliance requirements across the entire lifecycle of these services. This helps operators and enterprises alike build highly secure software, address security compliance requirements, and reduce development costs. This includes software signing, signature verification, and incorporating vulnerability management processes to periodically scan and validate services. Leveraging cloud-native services also unlocks automated security compliance capabilities across the product lifecycle from procurement to sunsetting.

Complementary to the above cloud-native capabilities, there already exist standards which further promote and elevate a secure 5G deployment centered around platform and firmware integrity. Specially, NIST 800-193 serves as a baseline for vendors and suppliers alike to integrate leading security practices and enhanced resiliency capabilities for 5G.

c. Network Slicing

5G also facilitates "network slicing" or greater network segmentation, allowing grouping and separation of security-sensitive network functions. A network slice is effectively a complete end-to-end network. End-to-end slicing is a fundamental 5G differentiator from all previous generations. 5G can allow service providers to simultaneously offer distinct, dedicated end-to-end network slices with different end-to-end resources to different enterprises on the same 5G network. Both open and closed architectures will allow for slicing and can apply different security policies per slice. This can be of particular benefit in addressing security concerns because each slice can include security appropriate to its requirements-security can be developed and deployed per slice. Different network slices can also run side by side for different purposes and have their security requirements applied to meet their respective needs. Slices can also vary in terms of their degree of mutual isolation from each other.

d. Standards Drive Interoperability and Innovation

Standards play an important role in 5G security and open RAN, including in the security concepts and activities described above. The opportunity to build open, interoperable and standards-based 5G networks has already begun to spur innovation and competition among diverse companies worldwide and more auditable. 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 choose from a variety of suppliers and providers to offer standardized interoperable solutions instead of developing a "one-size-fits-most" solution. Operators and suppliers can coordinate new information about threats, vulnerabilities, and exploits, allowing greatly accelerated development and deployment of mitigations.

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. Members of the Open RAN Policy Coalition are contributing to the development of standards for the technologies that comprise several unique differentiated security concepts as described in this document.

2. Security Benefits of Open RAN

As a complement to these security capabilities, Open RAN has the potential to build upon the security enhancements already enabled by 5G and allow the operator to fully control the security of the network, ultimately enhancing the operational security of their network. One benefit is greater visibility to security events: A network operator will have direct access to more data about network performance because the components are disaggregated and connected through open interfaces. This will allow them to gain visibility of potential security problems earlier. Data also can be finer-grained and represent activities between/within network functions that were previously hidden by internal vendor interfaces. Further, data about the running state of network functions will be more easily available through open management interfaces. This data can be combined with security log data to drive root cause analysis.

Open RAN also allows operators to build upon the capabilities enabled by 5G to shift the security capabilities closer to the edge of the network and stop attacks closer to the source. The introduction of open interfaces in the RAN allows the operator to distribute security analytics throughout the network and move RAN monitoring to the edge. This creates opportunities to create edge-focused analytics that speed the detection and prevention of network attacks, threats, and vulnerabilities and drive closed-loop actions at the RAN which blocks malicious traffic from reaching the core network. Rapid detection and response can enable efficient and more secure support of mobility services, especially IoT services by more effectively preventing DDoS attacks on the RAN by rogue mobile devices. Distributed security analytics allows an operator to share insights between the RAN and core, as well as between different RAN locations. Such insights can be used to take measures to protect radio units adjacent to a unit under attack or to use insights about the core to protect potentially vulnerable RAN units.

Open RAN will also allow operators to integrate best-in-class security platforms with open interfaces defined to be secured using modern, industry-standard security protocols. Since security platform vendors typically provide native support for standard protocols and interfaces, the operator can integrate new security platforms without implementing custom adaptors for vendor-proprietary protocols and interfaces. Furthermore, network function vendors will deliver regular protocol updates to stay current with the protocol releases, allowing operators to stay current with industry best practices at no extra cost.

Finally, Open RAN can speed the complete automation of network management. Automation enables zero-touch management which eliminates the security risks inherent in human access to network functions (NF). Such risks include the threat of humans accidentally altering the security posture of a network function or maliciously harvesting credentials, changing configurations, or implanting malware within the network. Automation also increases closed-loop response to changes in the network. For example, by using an open management interface for checking the security posture of a network function, the operator can quickly detect and fix degraded configurations – or anomalous network activity within the perimeter of a network – through closed-loop management.

Open RAN supported by cloud-based services will also increase the speed with which operators can install software and operating system security patches, thus enabling the operator to minimize the amount of time a vulnerability is in the network. This advantage will be particularly important to small rural carriers, who may have more limited resources to dedicate to upgrading and patching network software. The recent “Hafnium” attack on Microsoft Exchange servers demonstrates that even well after patches have been developed, tested, and deployed by vendors the actual processing of patching vulnerable servers may take months or years. By contrast, cloud-based services can be centrally managed from a vulnerability patching standpoint—dramatically reducing the time to secure those servers once patches have been deployed.

3. Conclusion

The Open RAN evolution has attracted a dynamic ecosystem of carriers, vendors, and suppliers that will enhance innovation, open new markets and enable digital transformation for the enterprises and industries that leverage 5G. While cyber threats continue to pose tremendous risks to carriers, enterprises, and industries, these stakeholders need the confidence that 5G networks and services – including those leveraging Open RAN--have carrier or enterprise-grade security. The Open RAN Policy Coalition is working with all collaborators to enable a secure digital transformation to 5G and unlock its potential to transform industries and give enterprises, industries, and carriers the confidence they need for business transformation.