\Orchestrating a brighter world NEC

Open RAN security examined

-How open, interoperable network design facilitates security improvements -

Executive summary

Open RAN represents a fundamentally different approach to RAN deployment and operation that can introduce greater efficiencies, cost savings, and a more robust multi-vendor environment compared to previous technologies. However, a number of security concerns have been brought forward recently pointing to potential Open RAN vulnerabilities in specific software implementations or the underlying cloud infrastructure that are not specific to Open RAN.

In this whitepaper, we address those concerns head-on by examining the fundamental design principles of Open RAN and the impact they have on network security. We find that principles such as openness and interoperability not only contribute to a better security posture of the network technology itself, but also facilitate the adoption of established security best practices throughout the development, integration, and operational phases. We explore how security is embedded in the Open RAN deployment and operation lifecycle and describe the roles and responsibilities of the stakeholders involved, highlighting key improvements over alternative deployment approaches. Together, these changes foster a secure ecosystem which affords MNOs with more control and visibility, which are essential elements of an improved security posture. Lastly, we outline recommendations on how to leverage the security benefits of Open RAN and improve their security posture when transitioning away from legacy deployments.

© NEC Corporation 2022

Table of contents

1. Open RAN introduces tangible security improvements 6
1-1. Moving away from proprietary interfaces 6
1-2. Open RAN implements security by design 7
1-3. Open RAN facilitates security process transformation 8
2. Security in the Open RAN lifecycle 10
2-1. Security roles and responsibilities 10
2-2. Security controls and best practices 15
3. Raising the security posture with Open RAN 18
3-1. Security governance and compliance 18
3-2. Technical capabilities 19
3-3. Processes and culture 21
4. Conclusions 22

© NEC Corporation 2022

\Orchestrating a brighter world NEC

1. Open RAN introduces tangible security improvements

Open RAN features several design choices that set it apart from alternative deployment approaches, such as legacy RAN and Cloud RAN. Thanks to this design, modern system engineering best practices can be adopted and as a result, Open RAN can facilitate significant security improvements in the radio access network.

1-1. Moving away from proprietary interfaces

The radio access network has continuously evolved over time, with Open RAN being the latest stage in this process. Main drivers of this evolution are mobile network operators (MNOs) demanding improvements on cost, operations, elimination of vendor lock-in, and all without compromising on security. Alternative approaches to Open RAN include legacy RAN and Cloud RAN, each with their own security benefits and drawbacks.

In legacy deployments, all RAN components and interfaces are co-located at the cell site. This type of deployment usually comes as one integrated package from a single vendor and comprises of the complete technology stack. This includes physical housing, business logic, proprietary management software, and security controls. As a result, the technology vendor can ensure that RAN components and security controls are harmonized. However, this approach often leads to a vendor lock-in which, in addition to negatively impacting cost and quality, can also lead to security vulnerabilities. Because MNOs have little control over legacy RAN technology, they rely entirely on the vendor's proprietary processes and policies for software updates, security patches, and integration with external systems. In fact, such a setup is vulnerable to conflicts of interests where the vendor security monitors its own deployment. Ultimately, the vendor may not solve security issues which otherwise the MNO would have demanded to be resolved. Moreover, a single vendor implementation also creates a single point of failure -- if this one vendor is compromised, the entire network is also at risk.

With Cloud RAN, security drawbacks such as a lack of control, operational visibility, and interoperability with third-party solutions remain due the dependency on a single vendor.

Advances in cloud computing have led to its gradual adoption in the radio access network. Prior to Open RAN, this development focused primarily on two aspects: decoupling software-defined RAN functionalities from hardware and centralizing functionalities of the Base Band Unit (BBU) in a cloud environment. This approach, commonly called Cloud RAN, improves network security to some extent. Deploying the BBU in a central location allows air interface protection between the mobile handset and RAN to terminate in a secure location, rather than at the cell site of which there are generally more, and which are more prone to physical attacks.

The cloud infrastructure also facilitates an easier rollout of software updates and patches. However, even though Cloud RAN leverages some benefits of the cloud, it does not resolve the fundamental security issue associated with legacy RAN since the interfaces are still proprietary or not fully standards compliant. Security drawbacks such as a lack of control, operational visibility, and interoperability remain due to the dependency on a single vendor. The result is again a vendor lock-in, including the above-mentioned issues. It is these drawbacks that Open RAN attempts to solve.

1-2. Open RAN implements security by design

Open RAN builds on the proven security design and controls of the Third Generation Partnership Project (3GPP) System, and introduces a number of features that can raise the MNO's overall security posture while maintaining full 3GPP compliance. The most important aspects can be summarized as follows: functional disaggregation, well-defined, open interfaces, software-defined implementations, and the introduction of machine learning.

© NEC Corporation 2022

Functional disaggregation

The concept of functional disaggregation is essential to Open RAN and – contrary to criticisms from legacy vendors – should serve to enhance overall security if implemented correctly. Building on 3GPP technical specifications that describe distinct Distributed Units (DU) and Centralized Units (CU) comprising the 5G radio access network, Open RAN takes this concept further to also include the Radio Unit (RU) and associated fronthaul interfaces. This development enables more flexible, distributed deployments and centralization of RAN components relevant for security. An example is the centralized deployment of the CU, which is where the user traffic is decrypted and in an unprotected deployment attackers could eavesdrop on users' data. It is true that introducing new interfaces between the network components increases the attack surface potentially available to malicious actors; however, this is outweighed by the benefit that they actually can be secured, tested, and monitored. This is always preferable to security by obscurity.

Well-defined, open interfaces

Interface specifications are essential to ensure interoperability between network components of different vendors. This includes communication protocols as well as security controls to protect the information exchanged. To that extent, Open RAN differs significantly from the alternative legacy approaches and Cloud RAN, in which the base station is practically a black box to the MNO. By also specifying these details for the fronthaul and management interfaces of network components, Open RAN empowers the MNO, who can now demand from its vendors compliance with industry standard security controls.

Software-defined implementations

Open RAN components are primarily implemented in software, minimizing the dependency on proprietary hardware to a bare minimum (e.g., RU, antennas). This is essential to allow MNOs to utilize virtualization and cloud infrastructure to deploy their networks. This aspect is not unique to Open RAN and can also be found in Cloud RAN. However, Open RAN differs in one fundamental aspect: The interfaces are openly specified.

Utilization of machine learning

Another key tenet of Open RAN is the use of machine learning capabilities to support automation and optimization of RAN components, facilitating a reduction of the total cost of ownership and quality of experience enhancements. For this purpose, custom applications – so-called xApps and rApps– can be used to expand and enhance the functionality of the Open RAN deployment. In terms of security, this presents an opportunity to implement detective security controls, such as intrusion detection, directly in the RAN. Such tools are essential to detect and respond to any successful and unsuccessful breaches of the security, minimizing the time the attacker can be present in the network. Of course, increased complexity in the RAN requires MNOs to manage the security of xApps and rApps themselves. For this purpose, the RAN Intelligent Controller (RIC) provides a dedicated integration and control point for these capabilities.

1-3. Open RAN facilitates security process transformation

Besides technology improvements, Open RAN also facilitates modernizations in the security lifecycle processes of the stakeholders involved. In fact, the way Open RAN is designed has significant impact on how networks are integrated, operated, and secured that pave the way for a more comprehensive approach to locking down security end-to-end.

Shifting security control

Because Open RAN is designed with interoperability in mind, there is no longer a single RAN vendor that controls the entire technology stack, as is the norm with legacy and Cloud RAN deployments. Instead, control over the end-to-end system shifts further towards MNOs, who can now determine RAN architecture and deployment. This ability affords them a stronger position to enforce security requirements during procurement, integration, and deployment processes. Even more importantly, it also allows MNOs to harmonize their security strategy and controls framework. A framework that, for the first time in the RAN, is decoupled from the primary RAN technology vendor and may comprise reputable, third-party security solutions selected based on their security capabilities, rather than on the vendor's preferences.

© NEC Corporation 2022

Shortening of development iteration cycles

Thanks to the disaggregation and software-defined nature of Open RAN solutions, RAN technology vendors will be able to shorten their time to market. Instead of a single monolithic, integrated solution, Open RAN vendors can ship their products in multiple software packages that are loosely coupled. For this to work in a multi-vendor deployment, the use of well-defined, open protocols is an important prerequisite. It is this loose coupling that enables MNOs to move towards a continuous integration and deployment (CI/CD) model. Such an approach can facilitate more granular and efficient security tests earlier in the process, minimizing the potential for human errors and the time to verify software updates using automated checks. Once a security defect is detected, RAN technology vendors for their part should be able to provide security patches for an isolated deployment package more efficiently than for an integrated solution.

Rethinking operations and maintenance

Open RAN's functional disaggregation also influences day-to-day network operations tasks. With legacy and Cloud RAN deployments, it is common that the system can only be managed using proprietary tools, including administrative systems, and monitoring tools. With multi-vendor Open RAN deployments, the use of *de facto* standard IT tools becomes more viable. While this does not preclude certain management tasks still requiring specialized tools, it is a major step forward in terms of streamlining and automating operation and maintenance tasks. For example, it provides the opportunity for the widespread adoption of established security best practices, such as *Security as Code*. By codifying security requirements for automated configuration and auditing, it becomes much more efficient to ensure a common security posture of cloud platforms, operating systems, and applications. This in turn, decreases the attack surface and therefore makes it more difficult for attackers to find a way in. Lastly, less specialized network technology and tooling also means that operators can tap into a significantly larger talent pool. More so than training with a proprietary telecom solution, secure operations of Open RAN relies on cloud and IT security skills, which are more widely available and can be applied across the entire network.

© NEC Corporation 2022

2. Security in the Open RAN lifecycle

Securing the radio access network requires a continuous effort by different stakeholders involved. Open RAN shifts the distribution of stakeholders' roles and responsibilities, and in turn, affords MNOs with more control over the end-to-end deployment. To successfully manage this shift, security controls need to be embedded throughout the Open RAN lifecycle.

2-1. Security roles and responsibilities

RAN technology vendors

RAN technology vendors provide the essential functionality of individual RAN components. They design, develop and implement all these components while ensuring interoperability with industry standards, such as those specified by 3GPP and the O-RAN Alliance. To that extent, Open RAN does not differ from alternative deployment approaches.

What is different in Open RAN, is that a single deployment may be comprised of RAN components by different technology vendors, allowing MNOs to mix and match. The vendors' responsibilities are focused on design, implementation, and security of the particular component they are supplying. In contrast to legacy RAN, vendors are not necessarily expected to provide proprietary hardware or support systems or perform system integration (SI) tasks. In Open RAN, the SI function is taken over either by the MNO or by specialized third parties or even by one leading Open RAN vendor. This is made possible by the use of open protocols and well-defined interfaces in Open RAN implementations. Beyond interoperability between network components from different vendors, this also allows the Open RAN deployment to be integrated with centralized security controls such as asset management, secrets management, and identity & access management systems and those involving multiple system layers such as platform measurement and attestation and secure boot. It is these integrations that help to address some of the most common attack vectors and make Open RAN deployments more secure than legacy deployments.

Infrastructure providers

Infrastructure providers supply the underlying networking, computing, and storage capacity resources required to run the RAN software, either on bare metal servers or virtualized, on a cloud platform. This approach differs from legacy deployments in which RAN infrastructure is usually provided by the RAN technology vendor in the form of specialized hardware. Cloud RAN deployments are similar, in that the RAN technology vendor commonly also supplies the virtualization layer for optimal performance. As a result, for legacy and Cloud RAN, the infrastructure provider is usually the same as the RAN technology vendor.

With Open RAN, the RAN technology vendor is not expected to provide the virtualization layer. Instead, with a focus on interoperability, the Open RAN software should be independent of the platform it is running on by using *de facto* standard software packaging formats and interfaces. The infrastructure provider operating the underlying platform needs to ensure isolation between different cloud tenants and individual workloads. Of course, the infrastructure provider is also responsible for the security of the cloud platform itself and for ensuring the availability of certain lower-layer security technology components the RAN software depends on, e.g., Trusted Platform Modules.

Mobile network operators

The MNO is at the center of the Open RAN ecosystem. It is here that individual RAN components are combined into one harmonized deployment. As such, it can determine the level of control it wants to enforce and what it demands from its technology vendors and service providers. Just as with legacy and Cloud RAN deployments, the MNO still needs to ensure that regulations and security standards are met.

© NEC Corporation 2022

The role of Mobile Network Operators in different deployment types

Open RAN deployments may not always be associated to a public mobile network operated by a telecom service provider. Other organizations, too, may decide to operate a private network for their own purposes. For instance, a manufacturer may connect their smart factory with a private 5G deployment. If it manages the Open RAN infrastructure independently, it essentially acts as the MNO and must ensure security. Alternatively, if the Open RAN infrastructure is supplied by an external telecom service provider, that external party as the MNO is responsible for securing the Open RAN deployment.

Both in legacy and Cloud RAN deployments, the MNO performs day-to-day operational and maintenance tasks. This includes the management of IT assets, identities, and privileges, operational monitoring, configuration and change management, as well as incident response and recovery. What changes with Open RAN is that the MNO can also control network architecture and system integration. The MNO may decide to perform these tasks internally, or it may delegate some of them to specialized service providers or SIs. For some, the latter option may strike an ideal balance between cost, performance, and security. During operations of the Open RAN deployment, the MNO still needs to ensure the same day-to-day tasks are being fulfilled, but it can do so leveraging standard IT tools, reducing the dependency on the RAN technology supplier.

System integrators

System integrators are becoming significantly more important as Open RAN introduces new technology vendors and more flexibility. In Open RAN, integration tasks do not comprise the integration of different network elements alone – individual software packages need to be integrated with each other, with the underlying cloud platform, and with the appropriate management tools. In addition to ensuring the interoperability of various components, system integrators can play a critical role in maintaining security by integrating Open RAN components with centralized security tooling and validation, and ensuring the performance of functions and operations throughout the Open RAN lifecycle. To support these tasks, system integrators can provide MNOs with an optimized integration pipeline. By leveraging modern CI/CD tooling that can automate security tasks throughout each process step, it is possible to provide these services efficiently and at scale. This could include building, testing, and hardening of software components. Some SIs may even go further and provide support for day-to-day operational tasks, such as operations and maintenance of the cloud platform. For instance, SIs can perform root cause analysis when defects are detected and coordinate responses and actions across the RAN. Delegating these tasks to an SI can make the transition to Open RAN significantly easier and more secure.

© NEC Corporation 2022

Industry efforts towards secure Open RAN

While each individual stakeholder needs to do their part to secure Open RAN, they depend on the industry for the development of interoperable specifications and technology implementations. Initiatives of the Open RAN community that can simplify security testing and integration efforts include, for instance, PlugFests where ecosystem players demonstrate interoperability based on O-RAN specifications. Such events have been hosted by different industry bodies, academic institutions, and telecom service providers. In addition to one-time events, there are also Open Test and Integration Centres (OTIC) that aim to provide an environment for validating Open RAN solutions. To date, several OTICs have been established in different geographies, helping to reduce the testing burden of individual MNOs.

In addition to industry representatives, policy makers and regulators also play a pivotal role in facilitating the adoption of open, interoperable technology. There are several places where these stakeholders can participate.

Promoting research, development, and standardization of Open RAN technology is important to drive innovation. This can be achieved through direct funding or incentive programs, and by sponsoring public demonstrations and testbeds that can provide the necessary infrastructure for conformance and interoperability testing.

Policymakers should promote a diverse and competitive ecosystem that affords MNOs with more choice on how to deploy their infrastructure. A global market with fair competition is essential for achieving long-term quality and security improvements. Additionally, it also facilitates lower prices, thus benefitting the consumer.

Policymakers and regulators should actively engage with industry bodies and representatives to foster the continuous exchange of information and cooperation between stakeholders. This may include initiatives aimed at capability building, education and awareness, or the development of standards and best practices to further advance the industry

Notable examples of government initiatives to facilitate Open RAN

Governments around the world actively support the expansion of the Open RAN ecosystem. For instance, in November 2020, the U.S. House of Representatives approved a bill that targets $750 million in funding over the ten years to accelerate the development of domestic Open RAN solutions and enhance competitiveness in supply chain. Meanwhile, in Japan, the New Energy and Industrial Technology Development Organization (NEDO) established a fund in 2019 for a project that aims to pioneer research and development regarding technological challenges that relate to interoperability solutions following the development of post 5G information and communication technology. Governments in other countries are also pursuing similar initiatives.

3rd Generation Partnership Project (3GPP):
Joint effort of several standards development organizations developing technical specification for cellular mobile networks to ensure interoperability.

Base Band Unit (BBU):
Legacy RAN component processing of uplink/ downlink traffic and controlling the Radio Remote Unit. In Open RAN, BBU functionality is split between DU and CU.

Centralized Unit (CU):
RAN component responsible for higher-layer, non-real-time data processing and controlling one or more DUs. Termination point of air interface protection between the UE and the RAN.

Continuous integration & deployment (CI/CD):
Software development principle that focuses on integrating new source code changes frequently, automating test and build tasks, and deploying code in production as soon as it passed validation.

Distributed Unit (DU):
RAN component responsible for lower-layer, near real-time data processing and controlling one or more RUs.

Machine learning (ML):
Subset of artificial intelligence (AI) that enables software to 'learn' from training data and make predictions or decisions.

Radio Unit (RU):
RAN component responsible for lower-layer, real-time data processing, incl. transmitting and receiving of radio signals.

RAN Intelligent Controllers (RIC):
Open RAN component optimizing performance of the control functionality of the RAN. Depending on the functionality, may be a Near-Real Time RIC or a Non-Real-time RIC.

Security as Code:
Method of codifying security requirements and policies to enable automated validation and rectification of policy violations.

Shift Left:
Security principle that emphasizes security testing and enforcement tasks starting from the early stages of the software development process.

2-2. Security controls and best practices

Design and implementation

During the design and development phases, the foundation for the security posture of the final Open RAN product is established. Due care at this initial stage is essential for enabling MNOs to secure their deployments effectively. Not only is there a need for the solution to protect itself, but it must also ensure protection of the data processed and be able to integrate with centralized security controls to be operated securely.

Due care at the initial design and development stages is essential for enabling MNOs to secure their deployments effectively.

The O-RAN specifications form the basis for the security design of both Open RAN components and the overall network. Guided by the security principle of Zero Trust, they aim to ensure security even in the presence of an attacker by realizing an approach that can be summarized as "Never trust, always verify". The development of the O-RAN security framework follows a structured risk analysis methodology as defined in ISO 27005. This ensures the identification and analysis of relevant threats which, in turn, inform the definition of security requirements. To address these requirements and to validate they are met, protocol and test specifications complete the O-RAN security framework. This holistic approach is described in further detail in the "Open RAN Security Whitepaper", published in March 2022 by a number of MNOs involved in the Telecom Infra Project[1] and demonstrates that security is an integral part of the Open RAN design.

Secure software development has undergone a so-called *Shift Left* in recent years, and the telecom industry is no exception. Implementing Shift Left security means enforcing security requirements and quality assurance continuously, and as early as possible. The earlier a defect is detected, the easier it is to fix. It is therefore essential that basic security principles are observed from day 1. Besides security by design, this includes applying secure coding practices, stringent source code governance (incl. version control, change control), the protection of software artifacts and the final products. All throughout, rigorous security testing should be embedded in the development workflow. At this stage, many security checks can be automated, including static code analysis and vulnerability checks. Many security tools will not only raise an alert, but also point out the root cause of the detected flaw, so developers know not to repeat the same mistake. Amongst others, these tools capture vulnerabilities such as remote code execution vulnerabilities, injection vulnerabilities, and hard-coded secrets. Such vulnerabilities can be abused by exploits readily available for download, and therefore detecting these vulnerabilities and mitigating them proactively is essential.

It should be noted that these security best practices for design and development are not specific or limited to Open RAN implementations. Ideally, they should be employed in the development of any RAN solution. However, Open RAN allows the MNO to validate the effectiveness of these measures more effectively. Thanks to the aforementioned shift in responsibilities and the MNO taking an active role in the solution integration process, the security testing it can perform may be more detailed.

Deployment and integration

The deployment and integration phases are likely to see the most changes due to the introduction of Open RAN. It is during these phases that security best practices are applied efficiently and consistently providing the security that is required for Open RAN.

The secure integration of virtualized Open RAN components starts with hardening the underlying cloud infrastructure. This includes locking down user access and privileges, setting up centralized security controls (e.g.,

software inventory, backup servers), and ensuring the platform provides information to the

[1] Telecom Infra Project, Open RAN MoU Group, "Open RAN Security White Paper", March 2022, https://telecominfraproject.com/openran-mou-group/#securitypaper

relevant operational security systems (e.g., log servers, Security information and event management). Using a common cloud platform ensures that many of these bootstrapping and configuration tasks can be automated, and at scale.

Next, the Open RAN solution components need to be deployed and integrated. Firstly, this includes integration of the RAN software with platform services and centralized security controls. Secondly, this step comprises the integration of various RAN components with each other, ensuring basic connectivity and confirming that each of them can be managed via the designated support systems. Third, integration tests should be performed on the end-to-end system, making sure it provides the expected functionality and meets security and performance requirements. Security is an important validation criterion, as misconfigurations that go unnoticed may cause vulnerabilities later on. Points that should be validated include:

- RAN software can make use of platform components essential for its security, e.g., Trusted Platform Module integration enabling secure boot procedure
- RAN software is reachable and manageable by centralized security controls
- RAN software reports expected information to security monitoring systems
- Attack surface of RAN software is minimized, e.g., by deactivating unneeded functionality, interfaces, and system access
- Security protocols are set up and profiled properly; insecure alternatives are disabled

As technical specifications evolve further and the Open RAN ecosystem expands, system integrators will be able to largely automate deployment and integration steps, so they can be performed repeatedly with minimal effort. Not only does this raise the efficiency of Open RAN rollouts significantly, but it also minimizes the potential for manual errors. The result is an Open RAN deployment that is trusted, integrated with centralized security controls, fully monitored, and hardened against attacks.

Operations and maintenance

Security does not end when a solution has been deployed, it is a continuous effort that requires the MNO to maintain a strong security posture of network elements, proactively monitor security events, and respond to incidents accordingly.

Certain preventive tasks need to be performed on a regular basis, such as network vulnerability scanning. If a known weakness is identified, the MNO's vulnerability management processes will ensure that it is swiftly confirmed, analyzed, and mitigated. This represents an inherent benefit of the Open RAN deployment approach: If the vulnerability is detected on a technology component that is managed by the MNO itself (e.g., in the operating system), it may be possible to test and rollout the required security patch independently. This ability to selectively deploy, test, and then roll out software packages at scale is only possible with an open solution architecture, running on a common cloud platform. Conversely, if the finding concerns software components supplied by a RAN technology vendor, the MNO will have to wait for a security patch to be provided. However, as we have explored before, there is an argument to be made that such a patch could be delivered quicker due to the shortened development cycles at the vendor's side. Should a vendor fail to address security deficiencies appropriately, the MNO may choose to replace the RAN software component affected. This process is also made simpler in Open RAN, because MNOs can run multiple software stacks in parallel –for example, split by geography– and switch between them more easily in case security issues are identified in one of them.

Operational security monitoring is also enhanced in Open RAN deployments. To detect and respond to security incidents, the ability to collect information from various sources is essential. This includes information about the cloud platform, virtualized workloads, and other network elements. Whereas legacy and Cloud RAN are closed systems that commonly rely on proprietary solutions supplied by the vendor, with Open RAN MNOs have the chance to streamline their operational monitoring by leveraging standard protocols for log collection. In turn, this makes it significantly easier to integrate the Open RAN into Security Incident and Event Management (SIEM) tools, allowing for efficient correlation and analysis of the collected data.

Overall, operations and maintenance stand to benefit from Open RAN primarily because of an increase in visibility and efficiency. Due to the reduced dependency on proprietary solutions,

© NEC Corporation 2022

MNOs have the opportunity to leverage established best practices and security tools to manage and protect their RAN deployments, and in that way deploy Open RAN more securely than legacy RANs have ever been.

	Open RAN	Cloud RAN	Legacy RAN
Interfaces and protocols	Openly specified communication between Core Network and RAN, between Distributed Unit (DU) and Centralized Unit (CU), and between Radio Unit (RU) and Distributed Unit, based on 3GPP and O-RAN Alliance specifications	Openly specified communication between Core Network and RAN, and between Distributed Unit (DU) and Centralized Unit (CU) based on 3GPP specifications	Openly specified communication between Core Network and RAN based on 3GPP specifications
Security controls	Use of open protocols and tooling allows integration with centralized, third-party security controls, e.g., for identity management, logging, etc.; Open technology and cloud platform also enables adoption of established IT security best practices	Largely proprietary, except 3GPP-defined network security protocols; centralized solutions usually dependent on components supplied by the RAN technology vendor; cloud platform may provide certain centralized security controls	Largely proprietary, except 3GPP-defined network security protocols; centralized solutions usually dependent on components supplied by the RAN technology vendor
Compute platform	Cloud platform may be managed and configured by the MNO based on established best practices; virtualization layer may need to be optimized for software supplied by the RAN technology vendor.	Cloud platform may be managed and configured by the MNO based on established best practices; virtualization layer may need to be optimized for software supplied by the RAN technology vendor.	Closed hardware platform provided by the RAN technology vendor
Secure development and integration	Development is up to the RAN technology vendor, solution integration performed by MNO or specialized third party; MNO can test and validate compliance of individual solution components	Development and integration are up to the RAN technology vendor; MNO may support cloud deployment, but has limited ability to test individual solution components	Development and integration are up to the RAN technology vendor; MNO has limited ability to test security of individual solution components
Security operations	Use of *de facto* standard IT tools allows for increased visibility, enables intelligent RAN optimization using xApps/rApps, and makes it easier to adopt established security best practices	RAN software relies on proprietary tools provided by the RAN technology vendor; platform may be managed by MNO	Entire RAN deployment relies proprietary tools provided by the RAN technology vendor
Updates and security patches	May be tested and rolled-out by the MNO independently; unless directly related to RAN software, no RAN vendor dependency	Dependency on the RAN vendor who is required to test and release patches to RAN software and platform	Dependency on the RAN vendor who is required to test and release patches to RAN software and platform

© NEC Corporation 2022

3. Raising the security posture with Open RAN

Open RAN empowers MNOs with greater control and flexibility over their network deployments. When utilized properly, these capabilities can facilitate an improved security posture.

3-1. Security governance and compliance

Control shift

Security governance is an integral part of any security program, providing structure and oversight to the management of security risks and the enforcement of associated controls. For MNOs looking to utilize Open RAN, effective security governance is indispensable, both internally and externally. This starts with recognizing the changing risk landscape when moving from an integrated RAN solution to Open RAN and managing it in alignment with business objectives. Depending on the strategy for adopting Open RAN, different approaches are possible. Is the primary objective to reduce operational expenses? Then close collaboration with external infrastructure providers and system integrators may be viable. Is it about reducing dependencies on external suppliers and service providers? In this case, more control should be centralized within the organization. Determining this split of roles and responsibilities between all stakeholders involved is essential. The more concrete these aspects can be defined early on, the easier it is to ensure a harmonized security lifecycle that addresses the relevant security controls.

Furthermore, security governance is concerned with ensuring compliance. This includes compliance with regulations, industry standards and specifications, and established best practices. As regulations differ by jurisdiction and are seldom specific to a certain technology, we will not discuss them here further. As for industry specifications, publications by both 3GPP and the O-RAN Alliance are relevant to Open RAN. These specifications aim to ensure basic interoperability between RAN components. The RAN security requirements contained in 3GPP specifications primarily focus on securing RAN interfaces for Control Plane and User Plane. The O-RAN Alliance goes beyond that by also specifying requirements covering Synchronization and Management Planes, open front haul interfaces, and the underlying O-Cloud. As such, they provide a solid foundation for building secure, reliable radio access networks.

To complement the standards and establish a comprehensive security framework, MNOs need to go further by specifying security requirements for the entire network deployment, just as with any RAN deployment. Such requirements may include details regarding expected security capabilities, protocols, and integration points. This process does not need to start from zero. For many parts of the technology stack, such as the operating system and the virtualization platform, there exist security guidelines which may be tailored and extended to match specific protection needs. To support this task of requirements definition and harmonization MNOs may also leverage specialized third parties, such as system integrators.

3-2. Technical capabilities

As RAN deployments change, technical security capabilities need to evolve to keep them secure. From an MNO perspective, security capabilities likely to be in high demand can be summarized in three categories: cloud-native security, secure software build processes, and security operations.

Cloud-native security

The move to the cloud has potential to improve the security posture of the RAN. But in order to leverage it, the use of cloud-native technology is a key enabler. Said differently, simply virtualizing existing deployments and shifting them to the cloud is unlikely to carry the expected benefits. A common cloud platform hosting the Open RAN components is well-suited to providing several fundamental security controls that would be much more difficult to enforce in legacy or Cloud RAN deployments. For example, maintaining a comprehensive and up-to-date asset inventory – the first step towards securing same assets – can be done more efficiently on a cloud platform. After all, the cloud orchestrator is aware of all virtual workloads anyway. Such an asset inventory may even extend to system configurations and patch levels and thus, help to ensure

© NEC Corporation 2022

a common security posture.

When it comes to the security of hosted RAN components, another important factor is that virtualized workloads can be profiled and controlled much more granularly than monolithic solutions. For example, containerization of applications allows them to be restricted to only those system privileges required to fulfill their purpose. Thus, individual applications are prevented from accessing any other resources by default which is how the principle of least privilege is enforced. Doing so is vital as the complexity of RAN deployments increases and is an essential prerequisite for realizing a true Zero Trust architecture.

Beyond that, identity and access management (IAM) also stand to benefit from deploying a cloud-native Open RAN. Whereas legacy deployments regularly make use of proprietary IAM solutions, an open, interoperable technology stack may be integrated with common centralized solutions. One possible implementation is a Cloud Access Security Broker, which serves as an identity verification and privilege enforcement point for anybody accessing cloud resources. It affords the MNO with the ability to manage privileges centrally in a granular fashion and control all communication between user and the cloud. As such, it not only serves internal personnel, but also external contractors and service staff. The security importance of this aspect is that many attacks start with a leaked credential. Centralized management of credentials makes it faster, easier, and more effective to prevent, detect, and mitigate attacks resulting from leaked credentials.

Secure build processes

From a security perspective, the software build and integration processes are crucial as many common security flaws can be detected and mitigated before the software is deployed. Therefore, establishing a streamlined set of tools for build, test, and integration tasks is indispensable for making the most out of the Open RAN potential. The concept itself is not new – many software companies already leverage it in their CI/CD pipelines. Security capabilities that should be part of such a pipeline include, among others:

- Static and dynamic application security testing (SAST/DAST).
- Dependency analysis of external libraries, images, manifests, etc.; and
- Security as Code, i.e., codified execution of security configuration and enforcement.

Depending on existing capabilities, MNOs can decide whether to perform these tasks internally or delegate such generic process steps to a specialized third party or SI.

Security operations

A multi-vendor Open RAN ecosystem carries changes to the way it is operated, as compared to a closed system such as a legacy or Cloud RAN deployment. Key improvements in terms of security primarily relate to three aspects: identity, visibility, and orchestration. Combined, they can facilitate more effective prevention, detection, and response to security incidents.

As discussed before, an Open RAN deployment can more easily be integrated with a centralized identity and access management solution. In terms of operations, that means that identities of third parties that manage part of the Open RAN components are easier to manage by the MNO. This provides control over identities, the lack of which is a prime reason for major security incidents.

The ability to flexibly orchestrate software-defined RAN components is beneficial for network security in multiple ways. Firstly, it can facilitate preventive controls. The aforementioned Security as Code capabilities should be used to configure and regularly validate the expected security posture of the cloud and hosted applications. This is especially critical in deployments where RAN components share a common platform with untrusted third-party applications, for example in an edge cloud. Secondly, orchestration can help MNOs respond to security-relevant events more efficiently. This may be as simple as dynamically scaling security controls based on current load or temporarily isolating misbehaving components in response to a policy violation.

Operational visibility is enabled by the security capabilities built into the cloud platform and Open RAN software. As a MNO, it is crucial to know about the security posture of the deployment and

© NEC Corporation 2022

any events that may change it. In a previous section, we already touched on log collection as one of the detective controls that stands to benefit from the use of standard protocols and tools. But log files are not the only source of security-relevant information. In a cloud-native deployment, lots of data can be gathered from the platform itself. Different options exist for the correlation of these information and the identification of relevant events. At a low-level, anomaly detection may be performed, for example, by Open RAN xApps that report and potentially even resolve the issue locally. At a larger scale, a SIEM can help to combine multiple streams of information from network components supplied by different vendors and identify security-relevant events. This supports effective detection of attacks, reducing the time the attacker is in the network.

3-3. Processes and culture

"Shift Left" security

Although the concept of Shift Left security originates from software development, the guiding principle still applies to MNOs, particularly those looking to utilize Open RAN. Given the increased control over the end-to-end security framework, MNOs can enforce security at each step of the RAN lifecycle. This starts as early as contracting and procurement. Effective supply chain security requires identifying various risks associated to direct and indirect vendors and actively managing them. Security certifications and independent security audits can help with this challenge of third-party governance.

However, to leverage these tools effectively, the security requirements expected to be fulfilled must be determined early on. For telecom equipment, MNOs can turn to the Network Equipment Security Assurance Scheme (NESAS), developed by the industry association GSMA. Compliance with this scheme ensures that vendors have processes in place required to develop secure products and that their products conform with security best practices defined by 3GPP. For generic security requirements, MNOs can leverage published best practices by organizations, such as NIST, ENISA, and COBIT.

Continuous integration and deployment

In legacy deployments, it is not unusual to update the RAN once every quarter, or even less frequently. With Open RAN, MNOs can adopt something closer to a CI/CD model of technology deployment. The ability to independently test software updates and configuration changes allows MNOs to evolve and innovate at a greater velocity than before. However, for that to happen, MNO's security teams also need to reconsider their approach. Not every change can be manually reviewed. Instead, CI/CD requires them to work more closely with the platform and the software, codifying security requirements into quality gates. Doing so allows the MNO to automate many of the proactive tasks that may still require someone to "tick a box" today.

The ability to independently test software updates and configuration changes allows MNOs to evolve and innovate at a greater velocity than before

Security automation

The potential for automating recurring security tasks goes beyond just preventive controls. Incident detection, triage, recovery – all these tasks may be supported by either hard-coded routines or more involved machine learning models. Automating these tasks is going to be a gradual process. For example, an automated response may initially require a security analyst to verify the events and resolve the issue accordingly. The goal should be to automate as many repetitive tasks as possible. Here too, an SI can be of help by providing automation capabilities and freeing the hands of MNO security teams for tasks that require more complex decision making or manual interaction, such as requirements engineering, network security design, and penetration testing.

© NEC Corporation 2022

4. Conclusions

Openness is a requirement for effective security

The evolution of mobile networks over time has led to significant advancements in both service and security. Today, large parts of modern cellular networks already utilize well-defined, interoperable interfaces. Until recently, radio access networks have not caught up with this trend.

Open RAN is the latest stage in the RAN evolution introducing fundamental changes to how RAN components are built, integrated, and operated. Overall, these changes facilitate security improvements across the solution lifecycle, which can be summarized as follows:

- **Use of standard, non-proprietary protocols and well-defined interfaces**
- **Providing MNOs with more control over the security of their networks** by shifting solution design and integration tasks away from the RAN technology vendor
- **Enabling the adoption of established security best practices** by disaggregating software components, allowing them to be built, tested, deployed, and operated like other IT systems

Open RAN specifications are developed with security in mind

Security is not just an afterthought in the O-RAN specifications, but a key consideration at every stage. By building on the proven security framework of 3GPP and extending the specification of open interfaces and associated security controls all the way to the fronthaul, Open RAN makes RAN security transparent and verifiable. Due to this fact, the Open RAN approach serves as a solid foundation for secure radio access networks, built on open, standard technology. As such, Open RAN deployments can be even more secure than the alternatives.

The Open RAN approach serves as a solid foundation for building secure radio access networks, thanks to its reliance on open, standard technology

Building secure radio access networks is an industry effort

More so than alternative deployment approaches, Open RAN exposes the different roles involved in securing radio access networks. What remains the same, however, is that all stakeholders must ensure that security best practices are incorporated and followed from day 1. System integrators can support MNOs in validating the security of individual RAN components and combine them in a harmonized deployment, helping them to fully leverage the Open RAN security benefits. Open RAN security is a joint effort of technology vendors, infrastructure providers, system integrators, and MNOs that requires all stakeholders to do their part. By doing so, they help to secure the network deployment, allow the industry to advance further and, above all, protect the subscriber.

Disclaimer:
This whitepaper is issued for information only. It does not constitute an official or agreed position of NEC. The views expressed are entirely those of the author(s). We decline all responsibility for any errors and any loss or damage resulting from use of the contents of this White Paper. Furthermore, Information on this documentation contains forward-looking statements regarding estimations, forecasts, targets and plans. The White Paper is made based on information currently available and certain assumptions considered reasonable as of the date of this material. These determinations and assumptions are inherently subjective and uncertain and are not guarantees of future performance, and actual operating results may differ substantially due to a number of factors.