Open Radio Access Network Security Considerations

DISCLAIMER

This document was written for general informational purposes only. It is intended to apply to a variety of factual circumstances and industry stakeholders. The guidance in this document is provided "as is" based on knowledge and recommended practices in existence at the time of publication. Readers should confer with their respective network administrators and information security personnel to obtain advice applicable to their individual circumstances. In no event shall the United States Government be liable for any damages arising in any way out of the use of or reliance on this guidance.

Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes. All trademarks are the property of their respective owners.

PURPOSE

NSA and CISA developed this document in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact

Client Requirements / Inquiries: Enduring Security Framework nsaesf@cyber.nsa.gov

Media Inquiries / Press Desk:

- NSA Media Relations, 443-634-0721, MediaRelations@nsa.gov
- CISA Media Relations, 703-235-2010, CISAMedia@cisa.dhs.gov

Table of Contents

EXECUTIVE SUMMARY

Mobile network operators provide cell services with a vast deployment of antennas and radios on cell towers connected to base station equipment. The base station equipment converts the wireless signals to data consisting of text messages, phone calls, streaming videos, and all the other pervasive apps offered today. The mobile network industry calls the radios, cell towers, and base station equipment converting wireless signals to data the Radio Access Network (RAN).

This assessment considers the security of a mobile industry initiative toward an Open RAN.

The DoD characterizes Open RAN in a new line-of-effort for the 5G Strategy Implementation Plan: "*RANs are traditionally vendor-locked, vertically integrated telecommunications architectures that enable wireless communications, such as 4G, 5G, and subsequent generations of communications technologies. By disaggregating RAN architectures – thus making them 'Open' - more companies can pursue innovation on advanced 5G network architectures and related security*."[1]

The Enduring Security Framework (ESF)[2] Open RAN Working Panel assessed the security considerations associated with implementing an Open RAN as architected and specified by the O-RAN Alliance.[3] The working panel focused on current designs and specifications for Open RAN architectures, and considered how these security considerations compared to, or are distinct from, traditional, proprietary RANs. The ESF Working Panel also addressed the additional resources required to fulfill the vision of interoperable, multi-vendor RAN powered by cloud services and software.

The working panel focused on security considerations for several key technical aspects of the Open RAN: multi-vendor management, the Open Fronthaul connecting radios to base station equipment, a new RAN application framework comprising rApps and xApps, Artificial Intelligence/Machine Learning (AI/ML) in the RAN, and other general network considerations including open source software, virtualization/cloudification, and distributed denial-of-service.

The working panel found security concerns and potential for their mitigations across these key technical aspects from Open RAN architecture. The working panel identified Open RAN

[1] https://www.defense.gov/News/Releases/Release/Article/3052013/dod-and-national-spectrum-consortium-team-for-open-ran-acceleration/

[2] The ESF is a cross-sector working group that operates under the auspices of Critical Infrastructure Partnership Advisory Council (CIPAC) to address threats and risks to the security and stability of U.S. national security systems. It is comprised of experts from the U.S. government as well as representatives from the Information Technology, Communications, and the Defense Industrial Base sectors. The ESF is charged with bringing together representatives from private and public sectors to work on intelligence-driven, shared cybersecurity challenges.

[3] The O-RAN ALLIANCE (O-RAN) was formed in 2018 by uniting two earlier organizations covering different parts of the world – US based xRAN Foundation and China based C-RAN.

security considerations with applications, open source software, supply chain, and zero trust to be consistent with the same concerns found in the Information and Communications Technology (ICT) industrial sector, and Open RAN needs to adopt ICT best practices to mitigate these concerns. Since Open RAN is adopting technologies found in 5G core networks such as multi-vendor core network functions and 5G cloud infrastructures, any Open RAN would benefit from following the best security practices applied today in 5G specifications, deployments, and operations. Open RAN brings new capabilities with an xApps/rApps application frameworks and AI/ML technology. The ICT industrial sector is also confronting security considerations with software application frameworks and AI/ML technology, and Open RAN must do so as well.

The O-RAN Alliance defined Open Fronthaul network connecting radios to base station equipment is built with an IT infrastructure but must perform like a real-time system. Many proprietary RANs operate today on a similar IT infrastructure, so Open RAN shares these IT security concerns. Like all commercial high-speed radio networks, real-time system requirements of both proprietary fronthaul and Open Fronthaul networks push the boundaries of high-speed performance and the ability of cryptographic security mechanisms to keep up, all while keeping unit deployment and operations costs down. Differing Open Fronthaul deployment scenarios for consumer, enterprise, and military applications will drive the required mitigations to meet the security objectives and Open RAN cost goals within the Open Fronthaul.

Security considerations always emerge in new open systems aiming for improved cost, performance, and supply chain benefits. Open RAN shares these security considerations too, and, with continuing efforts by the Open RAN ecosystem, they can be overcome.

SCOPE

The 5th generation (5G) of cellular communications promises faster and more reliable communications, with high-bandwidth and real-time capabilities that will offer enormous potential by enabling new use cases. The future of 5G is more than just the next high-speed mobile network. The use of cloud computing, AI/ML, augmented reality, virtual reality, and billions of connected devices will push the boundaries of wireless communications. To implement the capabilities of 5G, Mobile Network Operators (MNO) are looking at ways to adopt open, virtualized, and cloud-based Radio Access Networks (RAN) that will allow them to achieve greater network flexibility, reliability, and the ability to quickly implement new service types as 5G use cases are discovered. To realize these 5G benefits, MNOs are moving away from traditional, proprietary RANs that use purpose-built hardware and software to an open hardware and software-based ecosystem called Open RAN.

The ESF Open RAN Working Panel assessed the security considerations associated with implementing an Open RAN as architected and specified by the O-RAN Alliance. The working panel focused on current designs and specifications for Open RAN architectures, and investigated how these security considerations compared to, or are distinct from, traditional, proprietary RANs. The ESF Working Panel also addressed the additional resources required to fulfill the vision of interoperable, multi-vendor RAN powered by cloud services and software. This white paper comprises these technical aspects and security considerations faced by the Open RAN ecosystem.

Open RAN

Open RAN is the industry term for the evolution of traditional RAN architecture to open interoperable interfaces, virtualization, and big data and AI-enabled intelligence. Open RAN includes O-RAN Alliance, cloud RAN, and other technologies. O-RAN Alliance specifications aim to make RAN disaggregated, open, intelligent, virtualized, and fully interoperable.

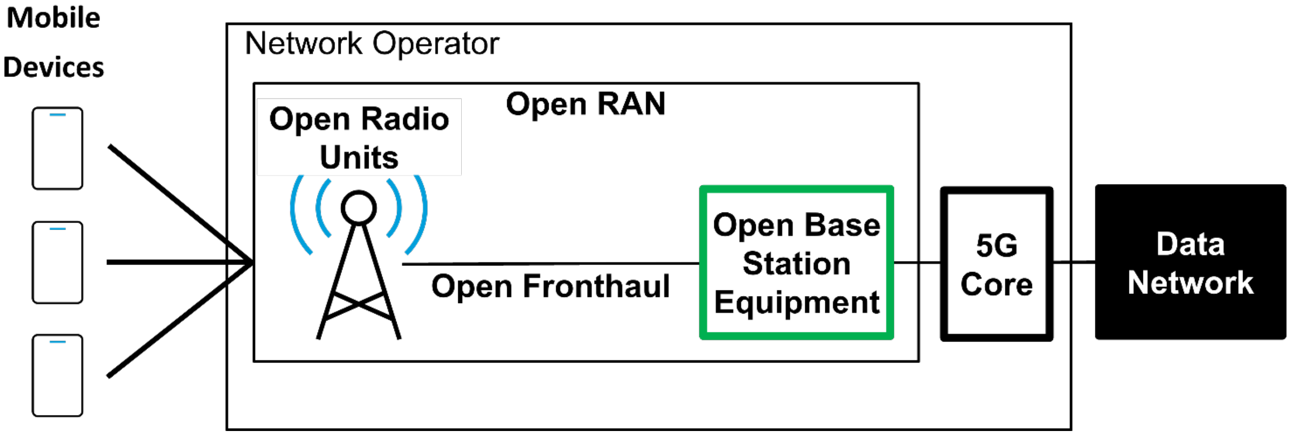


Figure 1 Open architecture

The O-RAN Alliance defined architecture, shown in Figure 2, disaggregates the radio unit (O-RU) and the distributed unit (O-DU) interfaces and RAN Intelligent Controllers (RICs) leveraging AI/ML to make dynamic policy decisions and parameter settings for the RAN[4].

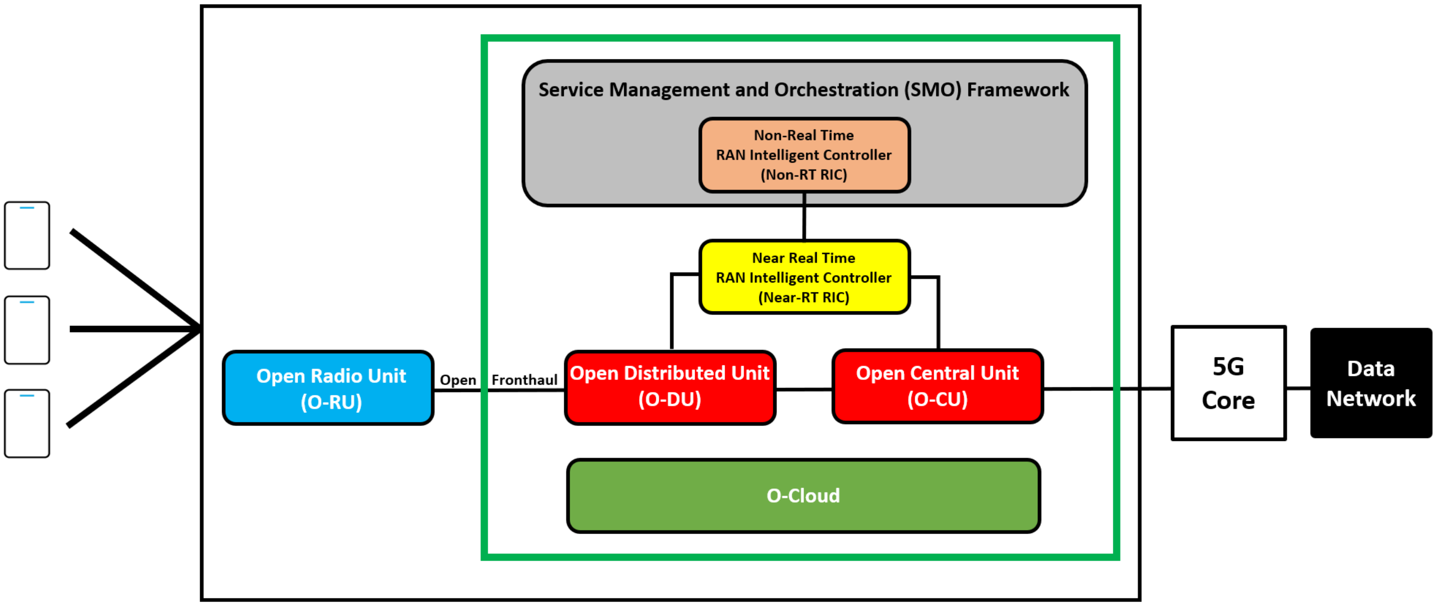

Service Management and Orchestration (SMO) Framework
Non-Real Time RAN Intelligent Controller (Non-RT RIC)
Near Real Time RAN Intelligent Controller (Near-RT RIC)
Open Radio Unit (O-RU)
Open
Fronthaul
Open Distributed Unit (O-DU)
Open Central Unit (O-CU)
O-Cloud
5G Core
Data Network

Figure 2 O-RAN Alliance defined network architecture

[4] A complete overview of the open architecture depicted in Figure 2 can be found at https://docs.o-ran-sc.org/en/latest/architecture/architecture.html

BENEFITS

Open RAN architectures encompass two distinct dimensions "decomposition" that enables "modularity" and disaggregation that enables cloudification and virtualization. The goal of this architecture design is to lower barriers to entry, and, therefore, promote increased competition, vendor diversity, and innovation.

One of the key goals driving the deployment of Open RAN is the creation of a robust multi-vendor ecosystem that drives competition and innovation. The establishment of a multi-vendor Open RAN ecosystem not only creates opportunities for new businesses, both small and large, to enter the previously closed market, but it also limits vendor "lock-in" that can occur under the traditional RAN environment in which the proprietary hardware and software are provided by a single vendor.

Open RAN has the potential to offer increased agility, resiliency, and flexibility in telecommunications networks by allowing service providers to select "best-of-breed" solutions from multiple vendors. Open RAN also builds on the security enhancements of 5G, extending the security benefits offered by virtualization from the core to the edge of the network. Open RAN also provides increased transparency into the RAN, allowing operators to see all aspects of the network and diagnose, remedy, and prevent problems in real time.

SECURITY CONSIDERATIONS

The deployment of Open RAN introduces new security considerations for mobile network operators (MNO). By nature, an open ecosystem that involves a disaggregated multi-vendor environment requires specific focus on changes to the threat surface area at the interfaces between technologies integrated via the architecture. In addition to addressing security considerations related to integrating components from multiple vendors, service providers will continue to deal with other considerations related to use of open source applications and new 5G network functions and interfaces whose standards are still under development. Additionally, MNOs will need to address security considerations related, but not unique to Open RAN, such as cloud infrastructure, virtualization, containerization, and Distributed Denial of Service attacks.

MULTI-VENDOR MANAGEMENT

Open RANs will introduce flexible and disaggregated architectures that support increasing data and service requirements of users. While traditional RANs are inherently single-vendor, Open RAN architecture will introduce more complexity due to the increased number of vendors and disaggregation of traditional network functions. These Open RANs are comprised of components that vary based on their specific function or use case they support. For example, a RAN could utilize small cells, Massive Input Massive Output devices, and macro towers to facilitate the communication needs of their users. These heterogenous components, and the back-end networking components they connect to, may use open interfaces to enable integration with a variety of different components and vendors. While this openness enables vendors to maintain interoperability and functionality for the many components of a RAN, it can also exacerbate existing integration and security considerations for operators of the network.

SOFTWARE AND HARDWARE COMPONENTS

Integration and compatibility between Open RAN components and functions from different vendors is critical to network security. Since it is crucial to update devices as quickly as possible, additional delays may introduce risks for network operators. For example, if a zero-day vulnerability is identified, vendors could release patches at different times. If one vendor's device is patched in response to a critical vulnerability, and others are not, it could lead to incompatibility of network devices and loss of network service availability. Until all the vendors within a network release a patch for the exploit, the operator's network may be vulnerable.

Component Lifecycle

When a network operator implements a change, such as an update, service implementation, or addition of a new component, they must ensure that there are no negative impacts to the network. While traditional networks require testing, Open RAN will introduce more complexity, which may present challenges for operators since that interoperability will need to be tested before each network change throughout the device's lifecycle.

OPERATOR AND VENDOR COOPERATION

When a vulnerability arises within an Open RAN network, identifying which vendor is responsible for addressing it may require more extensive coordination between vendors. In a traditional network with limited vendors, responsibility would fall on the vendor to identify and repair the issue. With an Open RAN network, it may be difficult to identity which vendor is responsible when there is component incompatibility that will require the operator to bring multiple vendors together to remediate the issue. Operators may be less likely to implement security changes if vendor coordination is too difficult or time consuming.

UTILIZING OPEN RAN SPECIFICATIONS

Devices must utilize defined Open RAN standards and specifications that support the development of open interfaces, network flexibility, and multi-vendor network support. If a device is not configured to established Open RAN specifications and attempts to communicate with another device that is also not properly configured, it may cause communication failures and transmission delays within the network.

OPEN FRONTHAUL SECURITY

A fronthaul network is a system comprising the radios on top of cell towers connected to base station equipment. The O-RAN Alliance specifies than an Open Fronthaul network is built with an IT infrastructure but must perform like a real-time system. Many traditional proprietary RANs operate on a similar IT infrastructure, but Open RAN goes further with interoperable connections between the radios and base station equipment.

OPEN FRONTHAUL SECURITY OBJECTIVES

The Open Fronthaul is a key O-RAN Alliance architectural element for operating 5G base stations. The Open Fronthaul relies on real-time communication interfaces to move 5G air interface messages between the O-RU radios and O-DU in base station equipment. Two Open Fronthaul interfaces coordinate for real-time transport of 5G air interface messages and a third interface provides timing signals to maintain real-time coordination. These three Open Fronthaul interfaces form the real-time communication system. A fourth interface manages O-RU radio configuration and security policies and is not a real-time interface.

The key security objectives for the Open Fronthaul provide for

- Confidentiality and integrity of mobile subscriber data
- Availability to transport 5G air interfaces
- Authenticity for the Open Fronthaul

CONFIDENTIALITY AND INTEGRITY OF MOBILE SUBSCRIBER DATA

Mobile operators can implement 3rd Generation Partnership Project (3GPP) 5G air interface security control mechanisms to protect the confidentiality and integrity of mobile subscriber data when transported over the Open Fronthaul. Air interface encryption prevents subscriber data from eavesdropping and user plane integrity protection counters unauthorized subscriber data modification. The 5G Subscription Concealed Identifier keeps the mobile subscriber identity private.

AVAILABILITY OF OPEN FRONTHAUL TO TRANSPORT 5G AIR INTERFACE MESSAGES

The availability of a mobile network to provide service to a subscriber is an imperative for mobile operators. The ability to provide a mobile service is dependent on the availability of the Open Fronthaul. The Open Fronthaul attack surface comprises the real-time communication interfaces, management interfaces, and the Open Fronthaul network. From a security perspective, the Open Fronthaul must implement security controls to counter potential denial of service attacks against the ability of a mobile network to provide services.

One security concern is unauthorized device access to the Open Fronthaul network. Only O-RU radios, O-DU in the base station equipment, and other authorized network devices should operate on the Open Fronthaul. An unauthorized device on the Open Fronthaul could launch denial of service attacks on the RAN. Mitigations for unauthorized access include network access control mechanisms, hardening and other O-RU physical security measures, and access control on O-RU management functions.

For defense in depth of a RAN, network access control is the first line of defense to mitigate attacks on the Open Fronthaul real-time communication interfaces. Without appropriate cryptographic security mechanisms for these real-time interfaces other availability attacks might still exploit vulnerabilities in the Open Fronthaul.

Like all commercial high-speed radio networks, real-time system requirements of both proprietary fronthaul and O-RAN Alliance defined Open Fronthaul networks push the boundaries of high-speed performance and the ability of cryptographic security mechanisms to keep up, all while keeping unit deployment and operational costs down. These cryptographic security mechanisms require further industry study and consideration. Differing Open Fronthaul deployment scenarios for consumer, enterprise, and military applications will drive the required mitigations to meet the security objectives and open RAN cost goals within the Open Fronthaul.

AUTHENTICITY FOR OPEN FRONTHAUL

The O-RAN Alliance defined management interface for the O-RU allows the operator to optionally use certificate-based authentication with mutual TLS[5] or password-based authentication with SSH. Password-based authentication is considered weak and vulnerable to brute force attacks. Weak authentication can be exploited by a malicious actor to gain access to the local system and move laterally across the network to gain access to northbound systems for greater visibility and control across the RAN. Authentication on the O-RAN Alliance defined management interface with mutual TLS (1.2 or 1.3) comprising Public Key Infrastructure (PKI) based X.509 certificates will move the O-RAN alliance defined management interface toward adopting an accepted industry best security practice.

rAPPS / xAPPS

rApps and xApps are novel O-RAN Alliance defined network automation applications that interface with the RAN through application programming interfaces exposed by the RAN to perform value added automation functions. Initially, these apps are focused on RAN optimization functions that will leverage AI and ML but may potentially extend to other RAN functions such as capacity planning, sustainability, and security as deployments mature.

rApps focus on higher layer automation policies with a control loop greater than 1 second and are designed to interact with the O-RAN Alliance defined Non-Real Time RAN Intelligent Controller (Non-RT RIC). rApps can also interact with other rApps through the O-RAN Alliance defined R1 interface enabling them to be used as building blocks to implement complex use cases. xApps operate with control loops as low as 10 mSec and run on the O-RAN Alliance defined Near-Real Time RIC (Near-RT RIC).

[5] Certificates provide digital signature and encryption capabilities which can be used to implement security services such as identification and authentication, data integrity, and confidentiality. Mutual TLS refers to two parties authenticating each other at the same time with the TLS protocol.

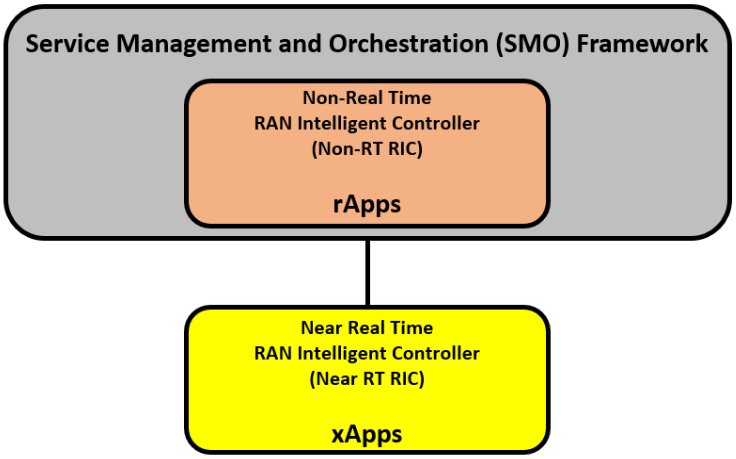

Service Management and Orchestration (SMO) Framework
Non-Real Time
RAN Intelligent Controller
(Non-RT RIC)
rApps
Near Real Time
RAN Intelligent Controller
(Near RT RIC)
xApps

Figure 3 O-RAN Alliance defined rApps and xApps

SECURITY CONSIDERATIONS

A motivation for rApps and xApps is to provide greater vendor diversity in which multiple vendors can contribute applications to the Open RAN ecosystem. As the development of rApps[6] and xApps[7] progresses, it is critical to incorporate industry best practices that enable RAN security, with a focus on the protection of confidentiality, integrity, availability, and authenticity of RAN functions, interfaces, and data.

The challenge of ensuring security in applications is universal. The following practices could be used to mitigate threats associated with the development of rApps and xApps.[8]

- Use secure AI and ML data sets and models. For further discussion about AI and ML security, see the *AI/ML* section of this assessment.
- Secure peering between rApps should be provided with mutual authentication across the O-RAN Alliance defined R1 interface. Confidentiality and integrity protection should also be provided on the R1 interface to protect against malicious snooping, modifying, or injecting messages on the interface.
- Secure peering between xApps should be provided with mutual authentication for xApp to xApp communications and xApp to Near-RT RIC communications. Confidentiality and integrity protection should also be provided to protect against malicious snooping, modifying, or injecting messages for these communications.

[6] Non-RT RIC Security Analysis Technical Report, v1.00, O-RAN Alliance, June 2022
[7] Near-RT RIC Security Analysis Technical Report, v01.00, O-RAN Alliance, June 2022
[8] O-RAN Security Threat Modeling and Remediation Analysis, v3.00, O-RAN Alliance, June 2022

- To prevent RAN performance degradation and outages in a multi-vendor environment, policy and parameter conflict mitigation should be implemented.
- Data in use and at rest should be protected against snooping attacks to protect any sensitive information.
- All access to data sources integrated with rApps and xApps should be protected with multi-factor authentication, and confidentiality, integrity, and availability.
- As the O-RAN Alliance defined A1 interface enables the Non-RT RIC to provide policy-based guidance, ML model management, and enrichment information to the Near-RT RIC, secure peering on the A1 interface should be provided with mutual authentication. Confidentiality and integrity protection should also be provided on the A1 interface to protect against a malicious actor snooping, modifying, or injecting messages on the interface.

While the introduction of xApps and rApps increases vendor diversity and makes greater innovation possible, the increased vendor diversity also introduces supply chain challenges which must be addressed to enable a trustworthy ecosystem of rApps and xApps vendors.

The Open RAN ecosystem should follow industry best practices for the development of a trusted supply chain of rApps and xApps, to include the development of secure application development guidelines, processes for independent evaluation, processes for vulnerability assessments, recommendations on the development of applicable software bill of materials (SBOM), software integrity mechanisms, and a common approach for secure onboarding of rApps and xApps.

As the maturity of the Open RAN ecosystem and deployments evolve, additional considerations may be necessary to ensure the implementation of a secure RAN application market. The goal is to balance innovation and security to give network operators a trusted market from which to choose curated applications that meet the industry recognized best practices for security and privacy.

AI / ML

Open RAN specifications are designed to replace as much custom or proprietary RAN hardware as possible with Commercial Off the Shelf (COTS) hardware. AI and ML algorithms are proposed to efficiently and automatically manage network resources such as traffic steering, quality of experience prediction, and anomaly detection/correction without resorting to customized hardware.

AI and ML algorithms in Open RAN components can behave unpredictably or maliciously when subject to “data poisoning attacks”, subtle changes to input data that could be indistinguishable from random noise. Therefore, AI and ML algorithms deployed in Open RAN components should be chosen, trained, deployed, and updated using approaches that harden them against data poisoning attacks. Open RAN also proposes AI and ML algorithms be implemented in a modular way to allow for independence and re-use across software components. For supervised algorithms, like Deep Neural Networks (DNNs), it is recommended that offline training with known data precedes deployment.

When AI and ML algorithms are introduced into a software system, they can present additional and novel vulnerabilities that need to be understood and mitigated. By "poisoning" the data input to an AI and ML algorithms, an attacker can induce effects ranging from denial of service by one or more Open RAN components to unexpected output from an AI or ML module that alters Open RAN behavior to the attacker's benefit.

Protecting AI/ML against data poisoning attacks is still a growing field of investigation. Appendix A list four widely referenced papers that will enable an experienced practitioner to develop, test, and deploy AI/ML algorithms that are robust against a variety of attacks. Appendix B lists published attacks on AI and ML used in RANs.

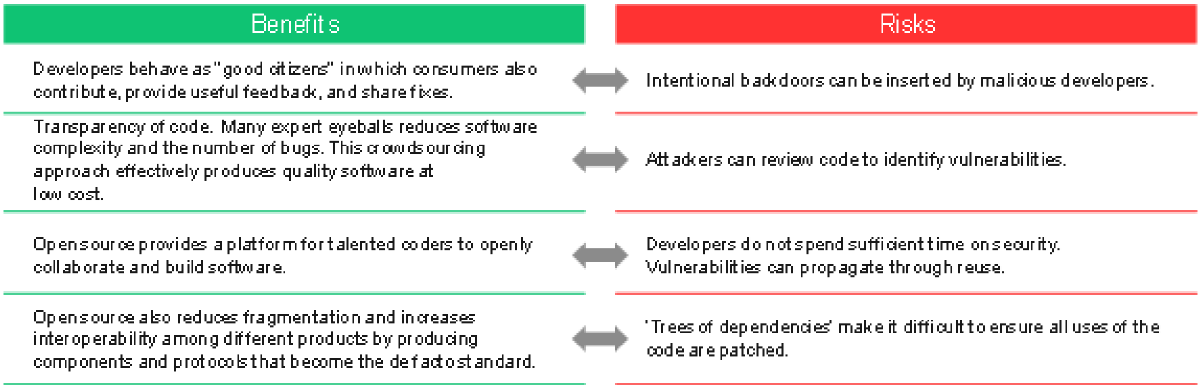
ASSOCIATED SECURITY CONSIDERATIONS

While there are security considerations due to the expanded threat surface of a multi-vendor Open RAN, other security considerations that apply to the ICT industry at large are also applicable to Open RAN. These include the use of open source software, virtualization and cloudification, Denial of Service (DoS) attacks, and the data sources used to train AI and ML.

OPEN SOURCE SOFTWARE (OSS)

OSS is a powerful tool that can be used by organizations to accelerate innovation while reducing the development, time to market, and overall cost of a product. OSS can help to reduce fragmentation and increase interoperability among different products by producing components and protocols that become the de facto standard. OSS also provides a platform for talented coders to openly collaborate and build software. OSS works optimally when developers behave as "good citizens" in which consumers also contribute, provide useful feedback, and share fixes. Consumers of closed-source software are limited in their ability to independently verify the accuracy of a closed-source Software Bill of Material (SBOM) or any security risks with closed-source software besides published vulnerabilities The transparency of OSS code reviewed by many expert eyeballs reduces software complexity and the number of bugs and allows for independent verification of source code and vulnerabilities. This crowdsourcing approach to software development has effectively produced quality software at low cost.

As experienced with recent security incidents, there is a tradeoff as OSS's advantages can be exploited as disadvantages and its strengths can be exploited as weaknesses. While the community approach benefits OSS, it also provides an expanded attack surface. OSS has many possible attack vectors similar to proprietary software, including intentional backdoors made by malicious developers, propagation of vulnerabilities through reuse, exploitation of publicly disclosed vulnerabilities, and human error. The tradeoffs with OSS security are outlined in the figure below. Verified SBOM and Software Composition Analysis are valuable tools to determine when OSS components with reported vulnerabilities are used in Open RAN deployments.



Benefits		Risks
Developers behave as "good citizens" in which consumers also contribute, provide useful feedback, and share fixes.	↔	Intentional backdoors can be inserted by malicious developers.
Transparency of code. Many expert eyeballs reduces software complexity and the number of bugs. This crowdsourcing approach effectively produces quality software at low cost.	↔	Attackers can review code to identify vulnerabilities.
Opensource provides a platform for talented coders to openly collaborate and build software.	↔	Developers do not spend sufficient time on security. Vulnerabilities can propagate through reuse.
Opensource also reduces fragmentation and increases interoperability among different products by producing components and protocols that become the defacto standard.	↔	'Trees of dependencies' make it difficult to ensure all uses of the code are patched.

Figure 4 Open Source software benefits and software risks [9]

VIRTUALIZATION AND CLOUDIFICATION

The key stakeholders in cloud deployments are the cloud provider and the cloud consumer. The cloud consumer uses cloud provider services in one of several models, including: Software as a Service, Platform as a Service, and Infrastructure as a Service. The responsibilities of the cloud consumer, and cloud provider, to provide security at each layer of the cloud varies with the service models as shown in the "Cloud Shared Responsibility Model" shown in Appendix C. The cloud consumer, as the data owner/controller, is always accountable for the security posture of the cloud deployment. The cloud consumer must ensure the Cloud Service Agreement clearly articulates the security responsibilities for each stakeholder, which is especially challenging in a hybrid cloud deployment model. Changes to risk due to evolving threats, attack vectors, and security control technologies should be periodically reassessed by the stakeholders.

The use of cloud infrastructure introduces security considerations that must be addressed to protect against internal threats and advanced persistent threats that can move laterally through a cloud deployment. To address the potential vulnerabilities in microservices, container engines, host operating system, and third-party hardware, and secure against attack vectors such as supply chain attacks, container and host escape attacks, weak authentication, and misconfiguration that can be exploited by internal and external threat actors. Cloud security controls should include isolation, micro-segmentation, mutual authentication, data protection and privacy, security policy automation, and threat detection and response. It is recommended that Open RAN deployments in hybrid and public cloud follow industry recognized best practices for virtualization and cloud-based services. Some recommended guidelines are listed in Appendix D.

[9] Opensource software security in an ICT context – benefits, risks, and safeguards, Ericsson https://www.ericsson.com/en/blog/2021/1/open-source-security-software

Distributed Denial-of-Service (DDoS)

A security posture for the cloud must also provide protections against botnets, volumetric DDoS, and application DDoS attacks sourced from internal devices and external networks that could impact the availability of the cloud and cloud applications. These attacks may target a 5G cloud deployment. Open RAN specific attack points at risk of DDoS attacks include, but are not limited to, the Open Fronthaul interface and rApps/xApps. Security of these parts of the Open RAN architecture are discussed further in previous sections of this document. It is recommended that Open RAN deployments in hybrid and public cloud follow industry recognized best practices against DDoS. Some recommended guidelines are listed in Appendix D.

Summary

This assessment has discussed the benefits of Open RAN and the security considerations associated with implementing and operating an open and disaggregated RAN. Shifting to a mobile network comprised of standardized open interfaces that allow for interoperability between software and hardware sourced from different suppliers is in contrast to traditional network infrastructures that are built with a single equipment provider's solution.

The identified security considerations in this assessment are ones present at this point in time, as Open RAN standards are being developed by standards bodies. As standards are developed and adopted by equipment manufacturers, software developers, integrators, and mobile network operators, these security considerations may be mitigated through the adoption of standards and industry best practices. Some of the security considerations identified in this assessment are not unique to Open RAN and exist in current closed RAN deployments, both would benefit by mitigating these security considerations.

Security considerations always emerge in new open systems aiming for improved cost, performance, and supply chain benefits. Open RAN shares these security considerations too, and, with continuing efforts by the Open RAN ecosystem, they can be overcome.

Appendix A: AI and ML References

The basics of attacks and protection: An introduction for the AI/ML practitioner is the widely referenced paper "*Can machine learning be secure?*" published in 2006 by Barreno et. al.[10] The paper covers: (i) a taxonomy for the types of AI/ML attacks, (ii) defenses against those attacks, and (iii) fundamental ideas to secure AI/ML against attacks. The results are applicable to defending a wide variety of algorithms including Regression, Support Vector Machines (SVM), and Random Forests.

Understanding how and why a DNN algorithm can be fooled: The paper "*Explaining and Harnessing Adversarial Examples*" published in 2014 by Goodfellow et. al.[11] demonstrates how input data poisoning can be used to cause any DNN to misclassify input. The classic example is setting an "attack DNN" against a "target DNN" to discover how to perturb data input to the target DNN to produce a pre-determined classification decision regardless of what the input data would typically produce.

A deep review of AI/ML vulnerabilities and defenses: The 2017 paper "*Wild Patterns: Ten Years After the Rise of Adversarial Machine Learning*" by Biggio and Roli[12] provides an overview of the evolution of AI/ML attacks and mitigations from 2006 to 2017 starting with early work on the securing non-DNN algorithms before considering how to attack (and secure) more recent DNNs. The paper reviews the main threat models and attacks and limitations of defenses.

Towards robust defenses for AI/ML algorithms (especially DNNs): The 2018 paper "*Adversarial Attacks and Defences: A Survey*" by Chakraborty et. al.[13] shows there are only a handful of strong countermeasures that can be used in all types of DNN attack scenarios. The authors start with a detailed discussion of the different types of adversarial attacks and threat models followed by an evaluation of the efficiency (and challenges) of countermeasures against them.

[10] https://people.eecs.berkeley.edu/~adj/publications/paper-files/asiaccs06.pdf
[11] https://arxiv.org/abs/1412.6572
[12] https://arxiv.org/pdf/1712.03141.pdf
[13] https://arxiv.org/abs/1810.00069

APPENDIX B: PUBLISHED ATTACKS ON AI/ML IN RAN

Black-box Adversarial Machine Learning Attack on Network Traffic Classification

- https://ieeexplore.ieee.org/document/8766505
- Generate radio signals that fool RAN traffic steering AI

Deep Learning for Launching and Mitigating Wireless Jamming Attacks

- https://ieeexplore.ieee.org/document/8558114
- Jamming attacks that adapt based on responses received from RAN

Trojan Attacks on Wireless Signal Classification with Adversarial Machine Learning

- https://ieeexplore.ieee.org/document/8935782
- Slightly altered training data poisons a deep learning modulation symbol classifier so an attacker can trigger performance degradation at any time in the future

Generative Adversarial Network in the Air: Deep Adversarial Learning for Wireless Signal Spoofing

- https://ieeexplore.ieee.org/document/9144305
- Confuse a RAN by generating synthetic wireless signals that cannot be statistically distinguished from intended transmissions

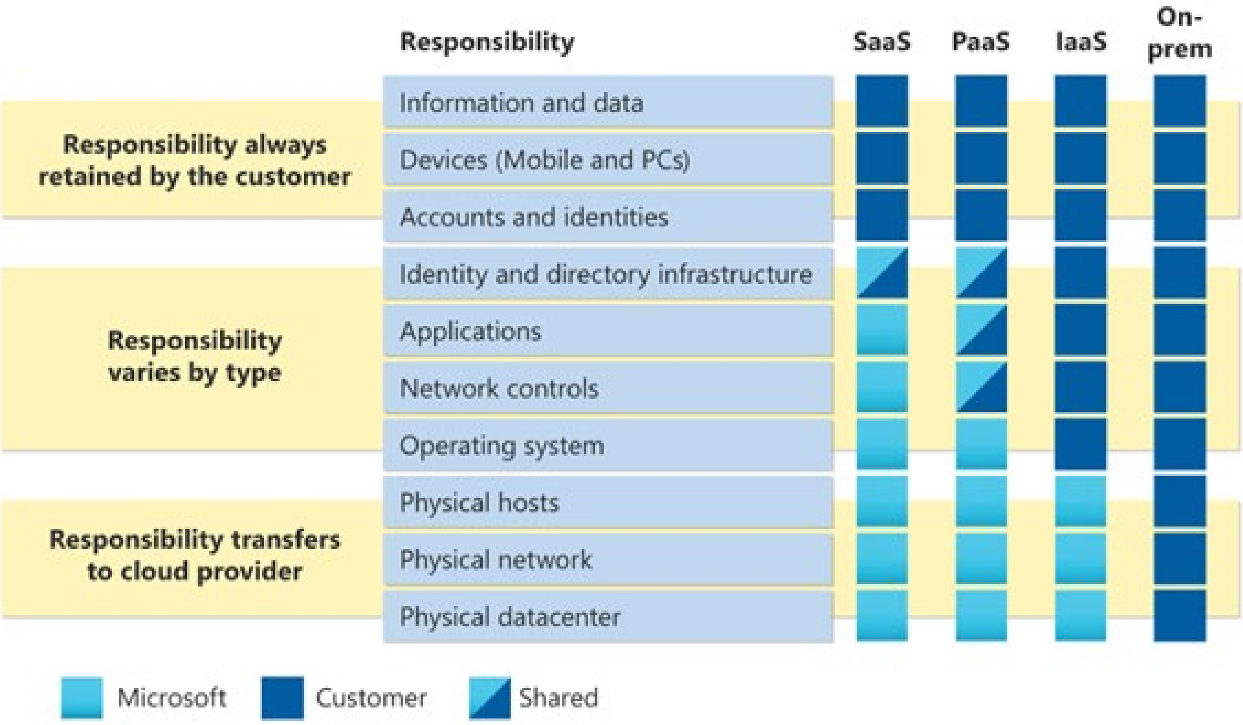
Spectrum Data Poisoning with Adversarial Deep Learning

- https://ieeexplore.ieee.org/document/8599832
- Adversary AI learns a transmitter's behavior and sends false spectrum sensing data to manipulate the transmitter decision-making ML

Adversarial Machine Learning Threat Analysis in Open Radio Access Networks

- https://arxiv.org/abs/2201.06093
- A systematic threat analysis of O-RAN adversarial machine learning attacks

Appendix C: Cloud Shared Responsibility Matrix



	Responsibility	SaaS	PaaS	IaaS	On-prem
Responsibility always retained by the customer	Information and data	■	■	■	■
	Devices (Mobile and PCs)	■	■	■	■
	Accounts and identities	■	■	■	■
Responsibility varies by type	Identity and directory infrastructure	◩	◩	■	■
	Applications	□	◩	■	■
	Network controls	□	◩	■	■
	Operating system	□	□	■	■
Responsibility transfers to cloud provider	Physical hosts	□	□	□	■
	Physical network	□	□	□	■
	Physical datacenter	□	□	□	■

□ Microsoft ■ Customer ◩ Shared

Figure 5 Cloud Shared Responsibility Matrix[14]

[14] https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

APPENDIX D: VIRTUALIZATION, CLOUD AND DDOS REFERENCES

References for Secure Virtualization and Cloudification

- CIS Benchmarks, Center for Internet Security. https://www.cisecurity.org/cis-benchmarks

- Kubernetes Hardening Guide, Cybersecurity Technical Report, U.S. National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), v1.1, March 2022.

- NIST SP 800-190, Application Container Security Guide, Souppaya, M., Morello, J., Scarfone, K., U.S. NIST, September 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf

- Security Guidance for 5G Cloud Infrastructures, U.S. National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA), October 2021. https://www.cisa.gov/news/2021/10/28/nsa-and-cisa-provide-cybersecurity-guidance-5g-cloud-infrastructures

References for DDoS Protection

- Cybersecurity and Infrastructure Security Agency
  - DoS and DDoS Attacks against Multiple Sectors. https://us-cert.cisa.gov/ncas/current-activity/2020/09/04/dos-and-ddos-attacks-against-multiple-sectors
  - Understanding Denial-of-Service Attacks. https://www.cisa.gov/tips/st04-015
  - DDoS Quick Guide. https://www.cisa.gov/uscert/sites/default/files/publications/DDoS%20Quick%20Guide.pdf

- Center for Internet Security
  - Technical White Paper – Guide to DDoS Attacks. https://www.cisecurity.org/insights/white-papers/technical-white-paper-guide-to-ddos-attacks

- National Institute of Standards and Technology
  - DDoS - Glossary | CSRC. https://csrc.nist.gov/glossary/term/ddos
  - Advanced DDoS Mitigation Techniques. https://www.nist.gov/programs-projects/advanced-ddos-mitigation-techniques

- UK National Cyber Security Centre
  - Denial of Service (DoS) guidance. https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection