ERICSSON

Security considerations of Open RAN

Ensuring network radio systems are open, interoperable, and secure by design

August 2020

Contents

RAN evolution

5G technology will benefit society and industries with enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC), and massive Machine Type Communications (mMTC). In addition to higher bandwidth and lower latency, 5G has the promise to be the secure digitalization platform for industry and society by providing secure connectivity for everything and everyone. 3GPP has standardized many security improvements with 5G, including:

- improved signaling plane and user plane protection
- International Mobile Subscriber Identity (IMSI) encryption with Subscription Permanent Identifier (SUPI) / Subscription Concealed Identifier (SUCI)
- device and network mutual authentication with the home network
- use of TLS between 5G Core functions, with option to use DTLS to protect signaling between RAN and Core
- Security Edge Protection Proxy (SEPP) for secure roaming
- network slicing for traffic segmentation

(Additional information about 5G security can be found at: https://www.ericsson.com/en/security/a-guide-to-5g-network-security)

Architectural changes in 5G have created the opportunity for network virtualization to maximize flexibility and reduce costs to meet use-case-specific requirements. Virtualization means that security needs to be handled in a new way. As the industry evolves towards RAN virtualization, with virtual RAN (vRAN) or Open-RAN (O-RAN), it is important that a risk-based approach is taken to adequately address security risk. vRAN leverages the 5G split-RAN architecture, interfaces, and security protection mechanisms standardized by 3GPP. Building upon the foundation set forth by 3GPP, O-RAN is standardized by the O-RAN Alliance with new functions and open, interoperable interfaces. The O-RAN Alliance has recently formed a security task group, in which Ericsson will participate, within O-RAN WG1 (Use Cases and Overall Architecture) to address new security risks. With any nascent technology, including O-RAN, security cannot be an afterthought and should be built upon a security-by-design approach. Ericsson, leveraging its experience, will continue its leadership role with the O-RAN Alliance to define security best practices. The purpose of this paper is to provide guidance on security best practices to ensure that O-RAN is ready to meet the level of security expected by service providers and their customers.

RAN virtualization

The discussion of RAN virtualization has three commonly used terms: Open RAN, vRAN and O-RAN. Each of these three terms is explained below:

Open RAN is the industry's generic term for an open radio access network architecture. An Open RAN has open interoperable interfaces, RAN virtualization, and support for big data and AI-enabled RAN. Open RAN is a vehicle for innovation in an open ecosystem while providing seamless coexistence with traditional RAN in a zero-touch management framework. Providers deploying an Open RAN can choose between a between a 3GPP or O-RAN architecture. The functional components of this chosen architecture can be realized over a tightly integrated hardware/software platform or COTS-based disaggregated platform. Figure 1 below shows the comparison of the 3GPP and O-RAN architectures.

vRAN refers to the virtualization of RAN functions, particularly the higher layer and lower layer function of the baseband unit. 3GPP Release 15 CU-DU split architecture facilitated this journey to begin by separating the centralized and distributed functions of RAN. With vRAN, 5G becomes software-defined and programmable, generating additional RAN architecture flexibility, platform harmonization and operational simplification. vRAN enables baseband units, typically in centralized hub location, to be virtualized and connected to remote radio units using standard CPRI (Common Public Radio Interface) or enhanced CPRI (eCPRI) protocols.

O-RAN refers to the Open RAN standardized by the O-RAN Alliance. The O-RAN Alliance has four main objectives: Open Interfaces, Virtualization, Intelligence, and Interoperability. O-RAN enables service providers to deploy radio units (RU) and distributed units (DU) from different vendors with a new Lower Layer Split (LLS) split, called Option 7-2x, transported over eCPRI protocol.

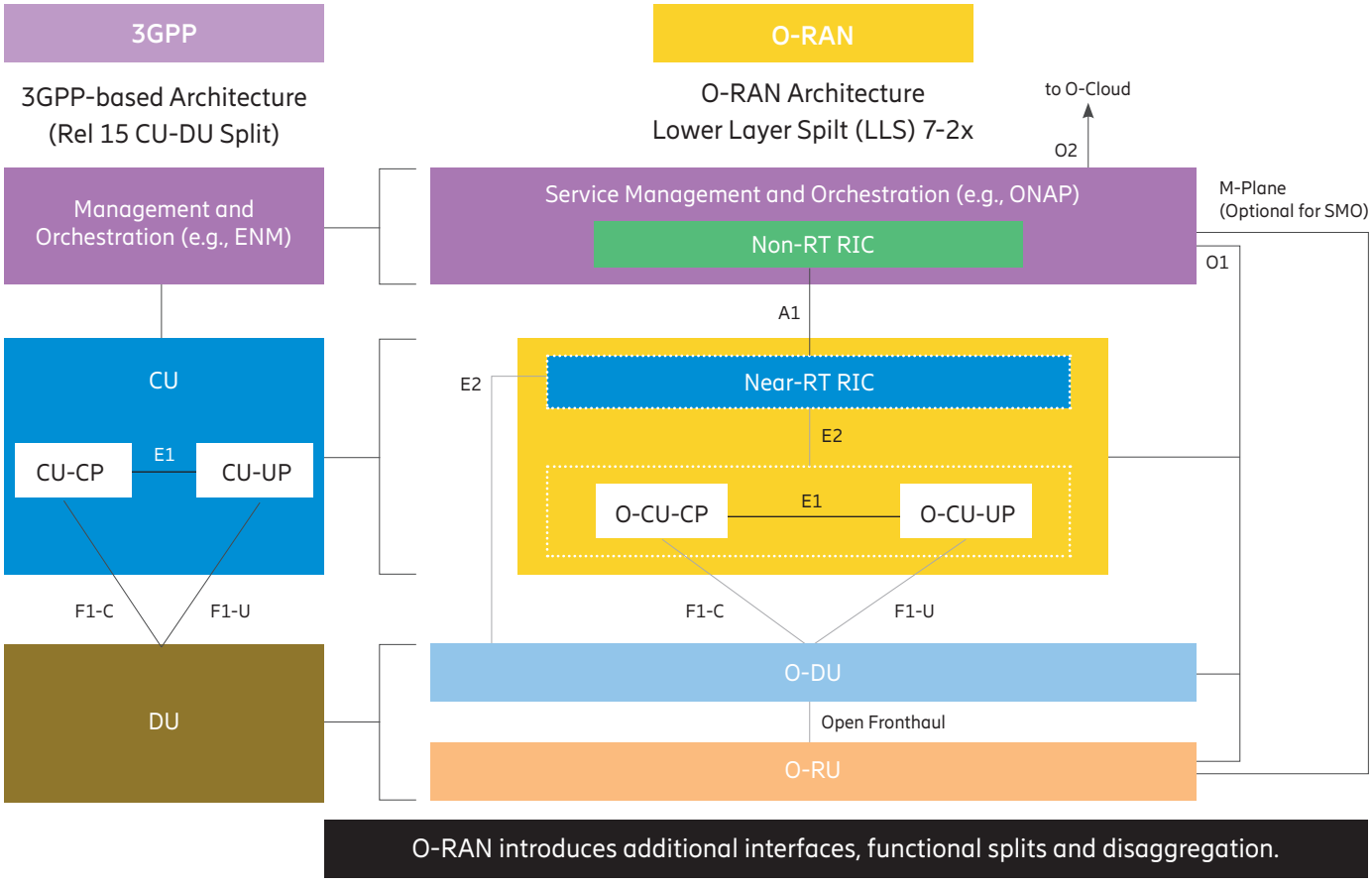


Figure 1: Open RAN Architectures: 3GPP versus O-RAN

O-RAN security risks

The O-RAN architectural diagram is shown in Figure 2 below. Security measures should be taken to address security risks specific to O-RAN deployments. These security measures include the following recommendations:

- Protect expanded threat surface.
- Close security vulnerabilities associated with Near-RT RIC .
- Address threat to trust chain introduced by decoupling of functions.
- Ensure management interfaces are secured according to industry best practices.
- Practice a higher level of due diligence for exposure to public exploits from use of Open Source code.
- Implement defenses from physical attacks.

Please note that the security threats associated with 'public exposure to Open Source code' and 'defense from physical attacks' are not exclusive to open network deployments such as O-RAN. Each of these security risks specified above are addressed in the subsections below.

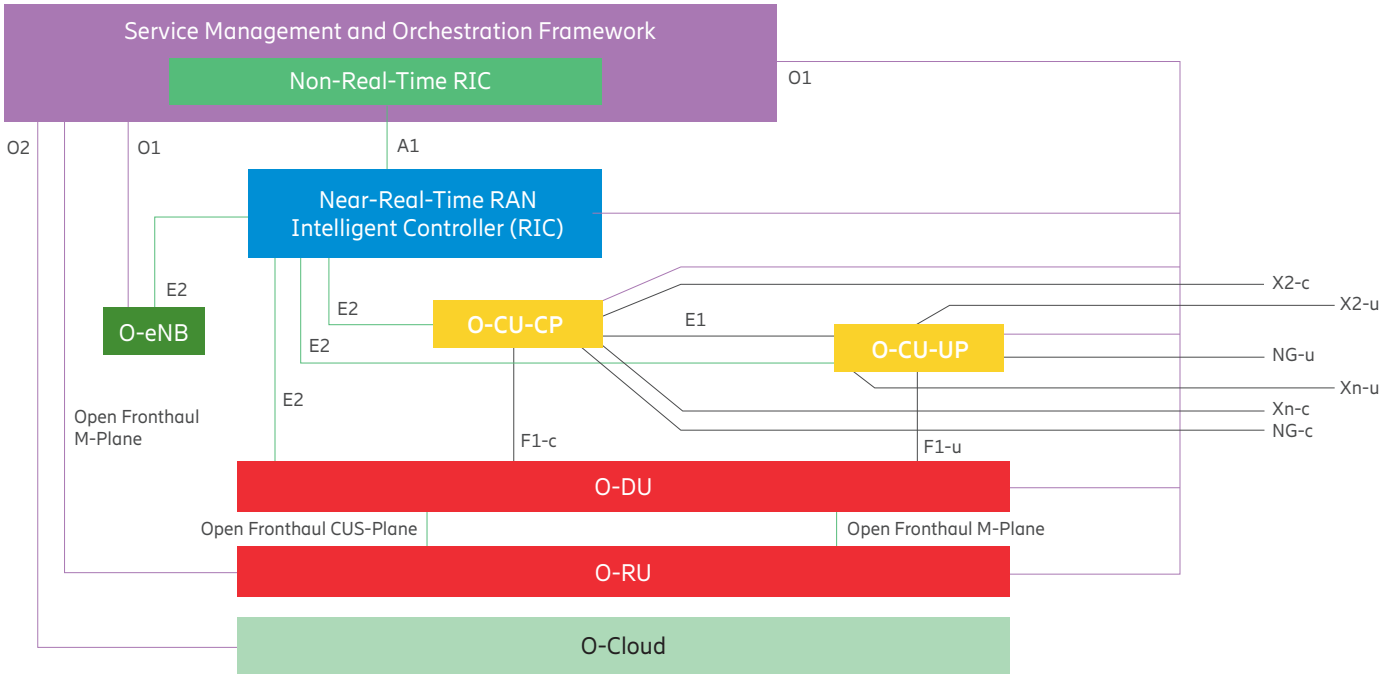


Figure 2: O-RAN Architecture (Source: O-RAN Alliance)

Expanded Threat Surface

The O-RAN architecture introduces new functions and interfaces, as shown in Figure 3 below. The introduction of additional interfaces and nodes, and the decoupling of hardware and software, expands the threat and attack surface of the network. These new security risks are explained in the following sections:

- Lower Layer Split (LLS) 7-2x
- Near-RT RIC
- disaggregation of software and hardware using cloud
- additional interfaces (O1, O2, and Open Fronthaul M-Plane)

3GPP	O-RAN
Functions • Management and Orchestration • CU-CP/CU-UP • DU	Additional Functions • SMO • Non-Real-Time RIC • Near-Real-Time RIC
Interfaces • E1 • F1-C/F1-U	Additional Interfaces • A1 • E2 • O1 • O2 • Open Fronthaul
	Modified Architecture • O-RAN LLS (7-2x)

Figure 3. O-RAN Expanded Threat Surface

O-RAN LLS 7-2x

The ORAN Alliance promotes the support for LLS, also referred to as Open Fronthaul, with the goal to increase the flexibility and competition on the telecom market. LLS refers to the split between the Radio Unit (RU) and the Distributed Unit (DU) as illustrated in Figure 4. The O-RAN fronthaul interface can be transported on eCPRI. The CPRI corporation (see http://www.cpri.info/) has worked together with industry to evolve the existing CPRI specification to create eCPRI. The eCPRI specification is designed to support 5G fronthaul requirements and offers several advantages to existing radio base station designs. One difference comparing traditional CPRI with the eCPRI interface is that eCPRI enables the efficient use of packet-based transport technologies and allows RAN payloads to be carried over Ethernet technology. The higher layers of the O-RU interface are implemented on top of eCPRI, with several different LLS options to split the functionality between the O-RU and the O-DU.

The traditional CPRI interface covers Layers 1 and 2 of the OSI stack, including all the necessary items for transport, connectivity and control. The higher layers of the interface between the RU and the DU are implemented by each RAN vendor as a vendor-specific protocol on top of the open standard Common Public Radio Interface (CPRI).

The security challenges with an LLS solution is that many of the benefits with traditional type of deployments will become a challenge unless the right security measures are in place. When having two different vendors, the O-RU and the O-DU needs to be managed as different entities. The O-DU will still control the other vendor's O-RU, but not fully. Instead, the O-DU will have to bridge the management traffic between the management system and the O-RU. Hence the possibilities to reach the northbound systems beyond the O-DU through the Open Fronthaul interface become a possible attack vector in this split architecture. In addition, access to the O-DU configuration could possibly be achieved via the Open Fronthaul interface, depending upon the design of the hardware-software system and how different functions are segregated in the node. An adversary could, in such case, either harm the node, create a performance issue by manipulation of parameters, or reconfigure the node and disable the over-the-air ciphers with the purpose of eavesdropping or other type of breaches.

The management and control traffic across the Open Fronthaul interface are not protected in the current standards for this split architecture. This opens the risk of Man-in-the-Middle (MITM) attacks over this interface. An adversary could possibly manipulate the management and control traffic that runs between the O-DU and O-RU. The user plane and control plane traffic to/from the UE may still be protected by the air interface protection. Finally, the O-RU can be subject for an attack with the purpose of reaching the network beyond the O-DU or with the purpose of gaining access to the O-DU. This depends on the vendor's implemented security controls such as access control, HW and SW design.

The following recommendations mitigate LLS security risks:

- Mutual authentication between O-RU and O-DU to assure that no unauthorized equipment can be connected to the O-DU via the Open Fronthaul interface
- Mutual authentication of management RU to management system
- Integrity protection and encryption of management plane and control plane between RU/DU
- Signed software and secure boot in O-RU and O-DU
- Network Access Controls for filtering u nauthorized/unexpected traffic in the DU over the fronthaul interface
- Segregation of O&M for O-DU with Open Fronthaul interface
- User access control in O-RU (if local management ports exists)
- Open Fronthaul interface security logging in O-RU and O-DU (for CP, UP, and Management)

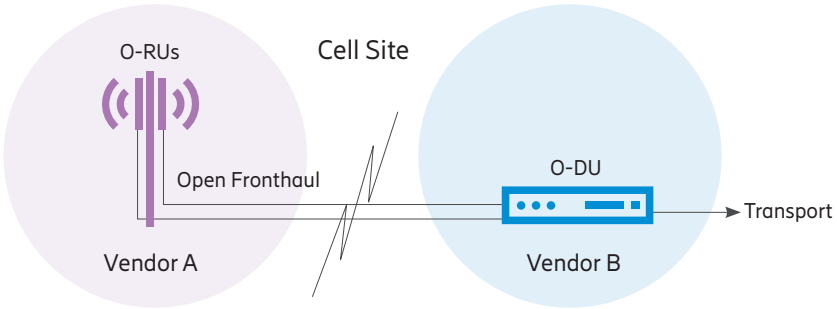


Figure 4: O-RAN Open Fronthaul

Near-RT RIC

The Near-RT-RIC also has potential security vulnerabilities, such as the following:

- Near-RT RIC signaling conflicts with gNodeB
- Near-RT RIC xApps signaling can conflict
- xApp Root of Trust
- UE identification in the RIC

Each of the potential vulnerabilities is explained further in the subsections below. Further study is required to identify the best solutions to close these security risks.

Near-RT RIC conflicts with gNodeB

The Near-RT RIC is a logical entity that enables near-real-time control and optimization of a subset of the Radio Resource Management (RRM) functions performed by the gNB (CU-CP, CU-UP and/or DU). The Near-RT RIC is composed of a software platform with applications, referred to as xApp, running on top. Each xApp can enable the Near-RT RIC to control one or multiple RRM functions. This is achieved by exchanging data between the xApps and the gNB over the E2 interface with control loops having timing in the order of 10ms to 1s. The RRM functions that can be controlled by the Near-RT RIC depend on the xApps and the capability of the RAN nodes exposed over the E2 interface. For example, the Near-RT RIC can control mobility and load balancing by exchanging information between a specific xApp and the CU-CP over E2. Another example is that the Near-RT RIC can control scheduling policies by exchanging information between another xApp and the DU. It is important to note that the RAN must be able to operate and provide services also without the Near-RT RIC or in case of Near-RT RIC failure.

The challenge with this definition of the Near-RT RIC is that there is no clear functional split between the Near-RT RIC and the gNB (CU-CP, CU-UP, DU). The functional split depends on the available xApps and the capabilities exposed by the gNB. This creates possible conflicts between the decisions taken by the Near-RT RIC and the gNB vendors that could lead to instability in the network, which introduces vulnerabilities that could be exploited by threat actors. For example, a threat actor can utilize a malicious xApp that intentionally triggers RRM decisions conflicting with the gNB internal decisions to create denial of service.

xApps conflict scenarios

The xApps in the Near-RT RIC can be provided by different vendors. For example, one vendor can provide the xApp for mobility management and another vendor provide the xApp for load balancing. This creates the risk that different xApps will take conflicting decisions, unless they are properly coordinated. For example, the xApps for mobility management and load balancing can trigger different handover decisions at the same instance in time for the same user with the risk to trigger a radio link failure. In ORAN WG3 specifications, O-RAN.WG3. RICARCH-v01.00, the following possible conflicts between xApps are identified:

- Direct conflicts: different xApps request change for the same parameter.
- Indirect conflicts: different xApps request change to different parameters that will create opposite effects, for example, antenna tilt and measurement offset.
- Implicit conflicts: different xApps request change to different parameters that are not creating any obvious opposite effect but result in an overall network performance degradation. These conflicts are most difficult to mitigate since dependencies are impossible to observe.

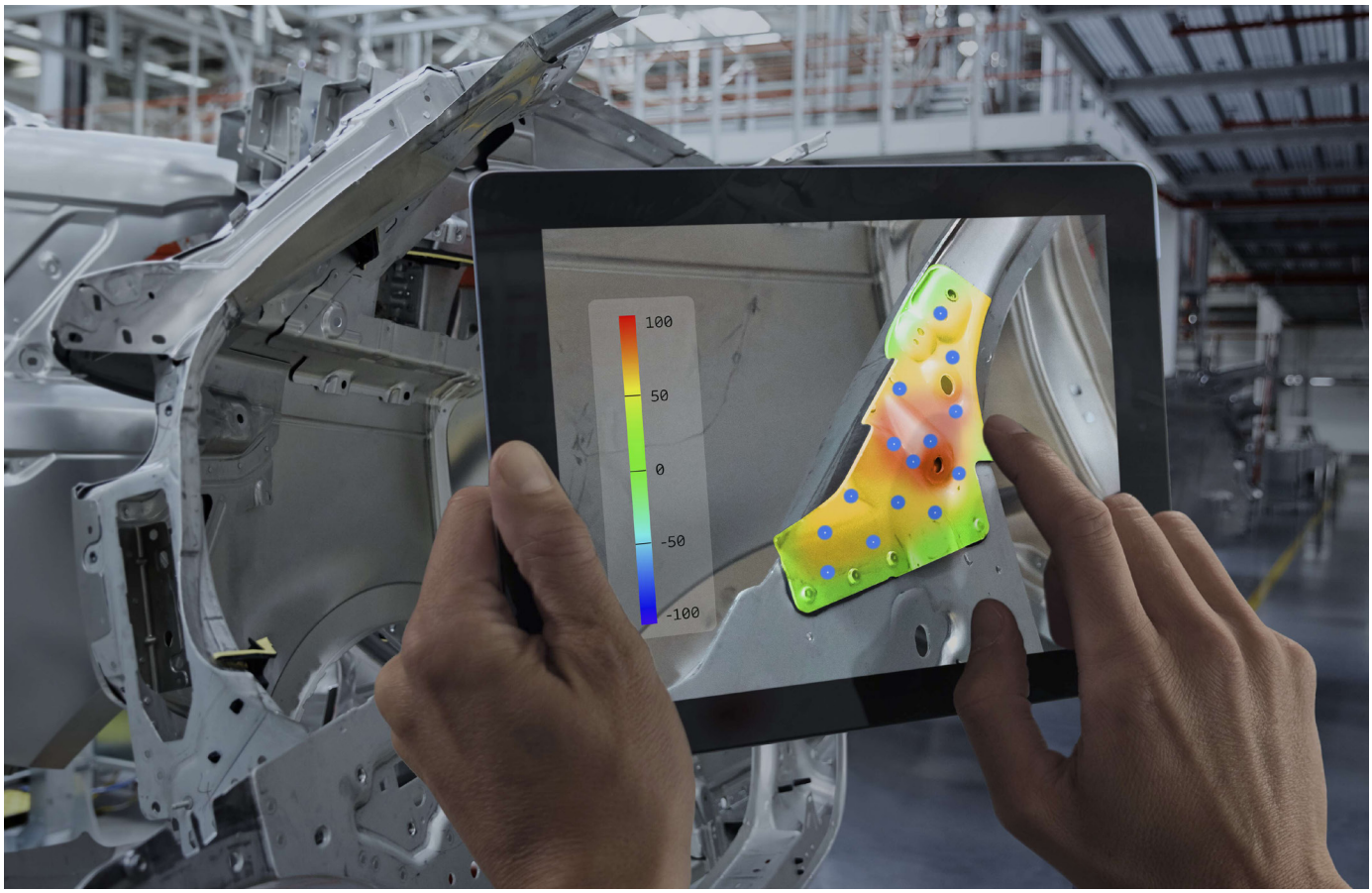
Performance degradation and instabilities that result from these xApps conflicts introduce vulnerabilities that could be exploited by threat actors. O-RAN is working on solutions to mitigate the impact of these identified xApps conflicts. However, as of today, no solution is defined in the specifications. Indirect and implicit conflicts are especially difficult to mitigate due to lack of observability.

xApp Root of Trust

xApps in the Near-RT-RIC have the capability to manipulate behavior of a certain cell, a group of UEs, and a specific UE. A malfunctioning xApp from a 3PP could potentially cause issues on the network. For example, the xApp could track a certain subscriber or impact service for a subscriber or a dedicated area. In addition, an xApp can receive order via A1 to control a certain UE and if a malfunctioning xApp receives an order to prioritize this UE, then the owner of the malfunctioning xApp knows a VIP that they want to track is in a certain area. With this command exposure, the attacker can obtain a rough location of a very important person and change the order from prioritize to deprioritize for a UE. In order to mitigate these risks, a solid trust chain, preferably from hardware up to the applications, (in this case 3PP xApp) is necessary, which makes it possible to authenticate xApps before loading and starting them.

UE Identification in the RIC

As the E2 interface (similar to A1 interface) can point out a certain UE in the network, this will create a correlation between the randomized (anonymized) UE identities between the RAN nodes. For example, a 3PP xApp can potentially be used as a "sniffer" for UE identification. The additional challenge for the Near-RT RIC / E2 compared to the Non-RT RIC / A1 is that more frequent signaling is expected over the E2 interface to enable near-real-time operation. Therefore, the UE identifier will be exchanged more frequently over the E2 than over the A1. To alleviate this, Ericsson is proposing solutions that reuse randomized UE identifiers defined in 3GPP over the E2 and A1 interfaces. These solutions are currently under discussion within the O-RAN Alliance for inclusion in future releases of the specifications.



Decoupling increases threat to Trust Chain

Virtualization and the use of cloud platforms give the possibility to utilize hardware resources better between different application, but it will also introduce security risks as isolation between applications are only "logical" in software without physical isolation across hardware resources. Recently discovered vulnerabilities like Meltdown and Spectre (https://meltdownattack.com/) reveal that there are security risks when sharing hardware resources. More vulnerabilities are likely already part of firmware and software to be discovered in the future.

A cloud-native or a virtualized environment includes many different layers, each with its own security functions. From an application perspective the use of all these security functions at the different layers involves trust at all layers. The host operating system has access to all RAM memory, disk volumes mounted on virtual machines, and containers. This means that a malicious host operating system can get access to all data processed in the workloads. There are techniques in newer CPUs/chipsets that intend to provide trusted computing like secure enclaves. In this case, a workload can use a secure enclave to protect data and processing from the host system, but the application will be hardware-instance dependent.

The virtualization layer includes the hypervisor that is executed on the host environment and is providing its own security functions and APIs to the host systems security functions. Hardware security functions also need to be accessed via the hypervisor as APIs, which means that the hypervisor (and cloud environment) can intercept all security functionality from the lower layers and hence needs to be trusted if these security functions are used. To get a fully trusted virtualized application, one needs to trust all the layers in the stack from hardware to firmware to virtualized software, as it is impossible to protect a virtual machine or containers from the host system.

In a cloud-native environment using containers there is no hypervisor. A container management system, for example, Docker plus the Linux kernel, provides isolation between the host operating system and the container environment. Containers don't have a full operating system and use name spaces to isolate from other containers. Containers on shared hardware resources are not meant to be used in multi-tenancy environment. Separate hardware and k8s clusters are needed for multi-tenant workloads.

To establish a secure and trusted communication channel between two endpoints, one needs first to authenticate each side before a secure (confidentiality- and integrity-protected) channel can be established. To authenticate each endpoint, a unique identifier and one or more credentials that shall be kept secret are needed.
To protect the credentials in computer environment, hardware security functionality such as Trusted Platform Module (TPM), Hardware Security Module (HSM), and secure enclaves, is used to get a hardware root of trust. Newer processors and chipsets also provide secure enclaves so specific software and date can processed in an isolated part of the processor.

In the case of virtualization and cloud environment, there are many layers that need to be considered to ensure the trust chain is maintained between applications and the underlying hardware. The authentication process is the base for establishing a secure communication channel based on the security association established in the authentication process. As there are different layers between the hardware and its security functions and the application, one needs standardized interfaces and APIs to use the hardware security functions. This is important as different hardware vendors may have different security functions. Together with standardized and interoperable APIs, there must also be a transparency into how the different layers use and provide the security functions in the chain. Security assurance and supply chain best practices will give a better transparency.

Management interfaces may not be secure to industry best practices

O-RAN's O1, O2, A1, and E2 are the new open interfaces that allow software programmability of RAN. These interfaces may not be secured to industry best practices. For example, the use of SSH on the O1 interface does not meet industry best practice. The O-RAN O1 interface allows optional use of TLS (reference O-RAN-WG1.O1-Interface-v02.00), but industry best practice recommends use of TLS. An implementation that does not implement TLS, since it is optional, may become the key source of vulnerability that a malicious code will exploit to compromise the RAN system. The O1 interface should meet industry best practice to establish a secure management connectivity based on strong digital identities, such as X.509 certificates, with mutual authentication, confidentiality and integrity protection using TLS. In addition, access controls for 3PP hardware should also be implemented to maintain the trust chain.

Areas of concern not exclusive to open networks

Increased exposure to public exploits due to use of Open Source code
The O-RAN Software Community is a Linux Foundation project, supported and funded by O-RAN to lead the implementation of the O-RAN specifications in Open Source; further guiding security principles and overviews of using Open Source software can be found at https://www.o-ran.org/software, https://o-ran-sc.org/, https://www.lfnetworking.org/ and https://www.linuxfoundation.org/blog/2019/04/how-o-ran-sc-completes-the-open-source-networking-telecommunications-stack/. Industry has recognized that Open Source code introduces security risks. Open Source vulnerabilities are publicly available on the National Vulnerability Database (NVD). While this is intended for developers to disclose vulnerabilities, it is also used by hackers to exploit those vulnerabilities. Vulnerabilities frequently propagate as developers re-use free open source code enabling backdoors to attacks. Vendors using Open Source code must enhance its security by applying industry coding best practices as described in the Security Best Practices section. There have been notable vulnerabilities from downloading open source libraries and dependencies, as well as supply chain risks when downloading Open Source code from untrusted repositories. It is recommended that vendors practice a higher level of due diligence for exposure to public exploits when using Open Source code. Recognized industry best practices include security-by-design principles from SAFECode (see https://safecode.org/) and OWASP SAMM (see https://owasp.org/www-project-samm/) and supply chain security from NIST SCRM (see https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management) and CISA ICT SCRM (see https://www.cisa.gov/ict-scrm-task-force).

Lack of defense from physical attacks
Use of 3PP hardware opens a new attack surface of physical attacks. Physical attacks include adversarial threats against power to disrupt availability, or hardware interfaces to gain access to information. It is expected that requirements to protect against physical attacks will persist for virtual deployments running on third-party hardware. Potential new risks from physical attacks, as well as applicable mitigation techniques, are ongoing areas of study. Some National Institute of Standards and Technology (NIST) recommendations are provided here.

NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, FAMILY: PHYSICAL AND ENVIRONMENTAL PROTECTION states that "The physical and environmental protection policy should ensure that the physical interfaces of the ICT supply chain infrastructure have adequate protection and audit for such protection."

NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security, Table C-5 Physical Vulnerabilities and Predisposing Conditions includes hardware vulnerabilities due to radio frequency, electromagnetic pulse (EMP), static discharge, brownouts and voltage spikes. NIST recommends that hardware provide proper shielding, grounding, power conditioning, and/or surge suppression.

Security best practices

It is important to implement security best practices in a multi-vendor environment using Open Source code to build open, interoperable, secure network systems. This enables vendors and network providers to minimize the number of vulnerabilities and quickly respond in case a new vulnerability is found or exploited. These best practices should be implemented by each vendor at the individual product level and by the service provider at the network level:

- Life Cycle Management (LCM) with early integration of security to implement "security by design"
- Continuous development and continuous integration (CD/CI) with continuous regression testing and software security auditing
- Supplier Relationship Management with an inbound development process and strict security controls for FOSS
- Trust stack with software anchored to reliable, trusted supply chains and trusted operations with well-defined processes to reduce risk
- Vulnerability management with intelligence to continuously track, identify and remediate vulnerable applications
- Multi-vendor system integration (SI) with continuous verification to ensure all vendors share the same interpretation and implementation of functions

Vendors should ensure that its software meets 3GPP SA3 Security Assurance Methodology (SECAM) and GSMA Network Equipment Security Assurance Scheme (NESAS) guidelines for development and testing process. A holistic approach across technology and services ensures that security is built in from the start, across supply chain, software and hardware development, testing, implementation and operation. The vendors should also consider security assurance across the product life cycle. For example, Ericsson's process takes a holistic approach across technology and services ensures that security is built in from the start, across supply chain, software and hardware development, testing, implementation and operation. The Ericsson Security Reliability Model provides risk assessment, privacy impact report, secure code review, vulnerability analysis and hardening guidelines for every release. Product Security Incident Response Team (PSIRT) keeps track of any new vulnerabilities that are found outside of that process and is ready to act on customer product security incidents and reported security issues affecting Ericsson products, solutions and services.

(Additional information about 5G security best practices can be found at https://www.ericsson.com/en/blog/2020/6/security-standards-role-in-5g)

Conclusions

Several service providers intend to leverage virtual RAN in an Open RAN architecture to build secure, open, interoperable, disaggregated, virtual networks based upon industry standards. RAN virtualization means that security needs to be handled in a new way. As the industry evolves towards RAN virtualization, with 3GPP or O-RAN, it is important that a risk-based approach is taken to adequately address security risk. Secure, Open RAN systems will require additional security measures not fully addressed in the standards, a trusted stack for software and hardware, and interoperability between vendors with common understanding and implementation of security requirements.

It is recommended by Ericsson that O-RAN implementations provide the following security measures:

- Protect expanded threat surface due to more interfaces and functions.
- Close security vulnerabilities with Near-Real-Time RIC.
- Address threat to trust chain introduced by decoupling of functions.
- Ensure management interfaces are secured according to industry best practices using TLS and digital signing.
- Practice a higher level of due diligence for exposure to public exploits from use of Open Source code.
- Implement defenses from physical attacks.

Ericsson will continue its leadership role within the O-RAN Alliance to incorporate security best practices. This will ensure that when O-RAN is ready to meet the level of security expected by service providers and their customers. Ericsson's integrated and open network solutions will allow our customers to build robust, secure and trusted 5G networks.

Author biographies

Jason S. Boswell is Ericsson North America's expert in telecommunications and network security, advising Ericsson's technicians, engineers and customers in creating and maintaining secure Ericsson solutions across the region.

Mr. Boswell brings over 20 years of experience from within the domains of telecommunications security design, engineering, consulting, sales and thought leadership for global service providers, governments and enterprises.

Scott Poretsky is an Ericsson North America leader in telecommunications and network security, advising Ericsson's technicians, engineers and customers in creating and maintaining secure Ericsson solutions across the region.

Mr. Poretsky brings over 25 years of network architecture and security design experience. He has served in numerous industry leadership roles and currently represents Ericsson in working groups, industry fora and government committees to provide thought leadership in security.

Acronyms

3GPP	3rd Generation Partnership Project
5G	5th Generation
CD/CI	Continuous Integration/Continuous Delivery
CISA	Cybersecurity and Infrastructure Security Agency
CP	Control Plane
CPRI	Common Public Radio Interface
DTLS	Datagram Transport Layer Security
EMP	Electromagnetic Pulse
FOSS	Free Open Source Software
GSMA	Global System for Mobile Communications Association
eMBB	enhanced Mobile Broadband
HSM	Hardware Security Module
ICS	Industrial Control Systems
ICT	Information and Communications Technology
IMSI	International Mobile Subscriber Identity
LCM	Life Cycle Management
LLS	Lower Layer Split
MITM	Man-in-the-Middle
mMTC	massive Machine Type Communications
NESAS	Network Equipment Security Assurance Scheme
NIST	National Institute of Standards and Technology
NVD	National Vulnerabilities Database
O-CU	O-RAN Central Unit
O-DU	O-RAN Distributed Unit
O-RAN	Open-Radio Access Network
O-RU	O-RAN Radio Unit
OWASP	Open Web Application Security Project
PSIRT	Product Security Incident Response Team
RAN	Radio Access Network
RRM	Radio Resource Management
RT-RIC	Real-Time Radio Intelligent Controller
SAMM	Software Assurance Maturity Model
SCRM	Supply Chain Risk Management
SECAM	Security Assurance Methodology
SEPP	Security Edge Protection Proxy
SI	System Integration
SSH	Secure Shell
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security
TPM	Trusted Platform Module
UP	User Plane
URLCC	Ultra-Reliable Low Latency Communications
vRAN	virtual Radio Access Network

About Ericsson

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York. www.ericsson.com

www.ericsson.com/5G
SE-126 25 Stockholm, Sweden
Telephone +46 10 719 00 00