A Brief Look at O-RAN Security

White Paper

Executive Summary

The paper presents a brief history of O-RAN alliance and outlines its goals and vision [1]. Then O-RAN security working group and its specifications are introduced, and its objectives and approach are reviewed. Architectural component of O-RAN and security solution for each component is addressed in some detail. Next a few key security features of the O-RAN architecture are highlighted. Security testing objectives, types and procedures are also described. Lastly, Fujitsu's viewpoint on security is described. The presentation showcases how the use of technology, processes and best practices result in a secure solution for 5G networks.

1 O-RAN Alliance

O-RAN was formed by the merger of the C-RAN Alliance and the XRAN Forum in 2018. The C-RAN alliance consisted of China Mobile and many other Chinese vendors, while the XRAN Forum was formed by US, European, Japanese, and South Korean vendors and operators. The founding operators of the O-RAN Alliance were AT&T, China Mobile, Deutsche Telekom, NTT Docomo and Orange. Since then, many other operators, vendors, integrators, and academic institutions have joined the alliance. Today ORAN Alliance eco system consists of over 340 companies and institutions across the world. The Alliance's vision is to enable open, virtual, intelligent and interoperable radio access networks resulting in faster innovation cycles, efficient mobile networks and competitive supplier eco system which benefits both customers and mobile operators [1].

O-RAN alliance develops access O-RAN specifications, releases open-source code in conjunction with Linux foundation and supports companies in testing and integration of their O-RAN implementations. There are currently a total of 11 technical working groups developing specifications for various aspects of O-RAN architecture. Related topics above and beyond what working groups are developing are dealt with in three focus groups and a next generation research group.

2 O-RAN Security

Over the past few years O-RAN working groups have been developing detailed specifications for security requirements, security protocols, security threats and risk assessment as well as testing and integration procedure [2],[3],[4],[5]. These are living documents and the work is still in progress. However, upon completion of parts of the tasks, every few months or so new releases are published.

Up until June 2022, Security Focus Group (SFG) was addressing the security aspects of O-RAN architecture. Placing even more emphasis on security, the alliance was converted the group into a full fledge technical working group (WG11). WG11 is responsible for security guidelines that span across the entire O-RAN architecture. The security analysis and specifications are being developed in close coordination with other O-RAN Working Groups, as well as regulators, and standards development organizations.

One can think of O-RAN architecture as an ensemble of functions, interfaces and the information that flows through the entire system. O-RAN addresses the security for every component of the system such as individual interfaces and functions. Above and beyond that, security for the entire end-to-end system as the information flows into and out of the system is investigated as well. It is noteworthy that O-RAN benefits from 5G advanced security features as it is built on 3 GPP's architecture. In the remainder of this section, security measures for various components of O-RAN are addressed.

2.1 Near-RT RIC

The Near-Real Time RAN Intelligent Controller (Near-RT RIC) is a virtual function introduced by O-RAN which adds programmability to radio access networks and is designed to enable optimization and control of radio access network elements by utilizing AI/ML schemes. The three interfaces associated with it are E2 interface as well as A1 and O1 open interfaces. xApp micro service-based applications consisting of one or more micro services run on Near-RT RIC. Association between xApp and RAN functionality is made through E2 interface. The security issues related to Near-RT RIC, xApp and its interfaces E2, A1 and O1 have examined in detail [6].

O-RAN threat model took identified risks and threats into account. That led to a list of key security issues. Each key issue was described in details and the relevant security threats were extracted. Then security requirements addressing the threats were identified. Eventually multiple solutions and mitigation strategies associated with the identified key security issues were provided [6].

2.2 Non-RT RIC

The communications and information exchange between the Near-RT RIC and Non-RT RIC is supported by A1 interface. Assets and threats that could impact Non-RT RIC or can utilize Non-RT RIC to impact other parts of O-RAN system are identified. Additionally, points that intruder can gain entry or exploit a vulnerability to compromise the system or data are identified. Risk analysis based on likelihood and the potential loss is carried out. In conclusion, management, operational and technical recommendations to protect the integrity, availability, confidentiality of Non-RT RIC and its information are made [7].

2.3 O-Cloud

Assets and threats that could impact O-Cloud are identified and documented. In this exercise, CISA/NSA, ETSI and ENSIA reports have been used. A common threat template that uses a core set of attributes for each threat is used. Threats are prioritized based on the threat likelihood vs the potential threat damage. In the end, recommendations, best practices and mitigation schemes are presented [8].

2.4 Interfaces

O-RAN introduces several new interfaces. Addition of new interfaces could result in security concerns. However, Communications on all interfaces, both 3GPP and O-RAN defined, are secure. A collection of mature, proven and secure protocols has been selected. The utilized security protocols include SSH, TLS, DTLS or IPsec. Generally, X.509 certificates are utilized for mutual authentication purposes. For added confidence and building trust, certificate authorities must be audited. To provide secure communications between O-RAN functions, in addition to using proven protocols, mutual authentication of endpoint functions and trusted certificate authorities are deployed [4].

Specifications supports SSHv2 and provides the upgrade path for future SSH changes. Similarly, the spec supports TLS 1.2 and TLS 1.3, stays current with TLS and provides the upgrade path for TLS changes. As for IPsec, a subset of capabilities is supported. Parallel utilization of IPsec with SSH and TLS are described [4].

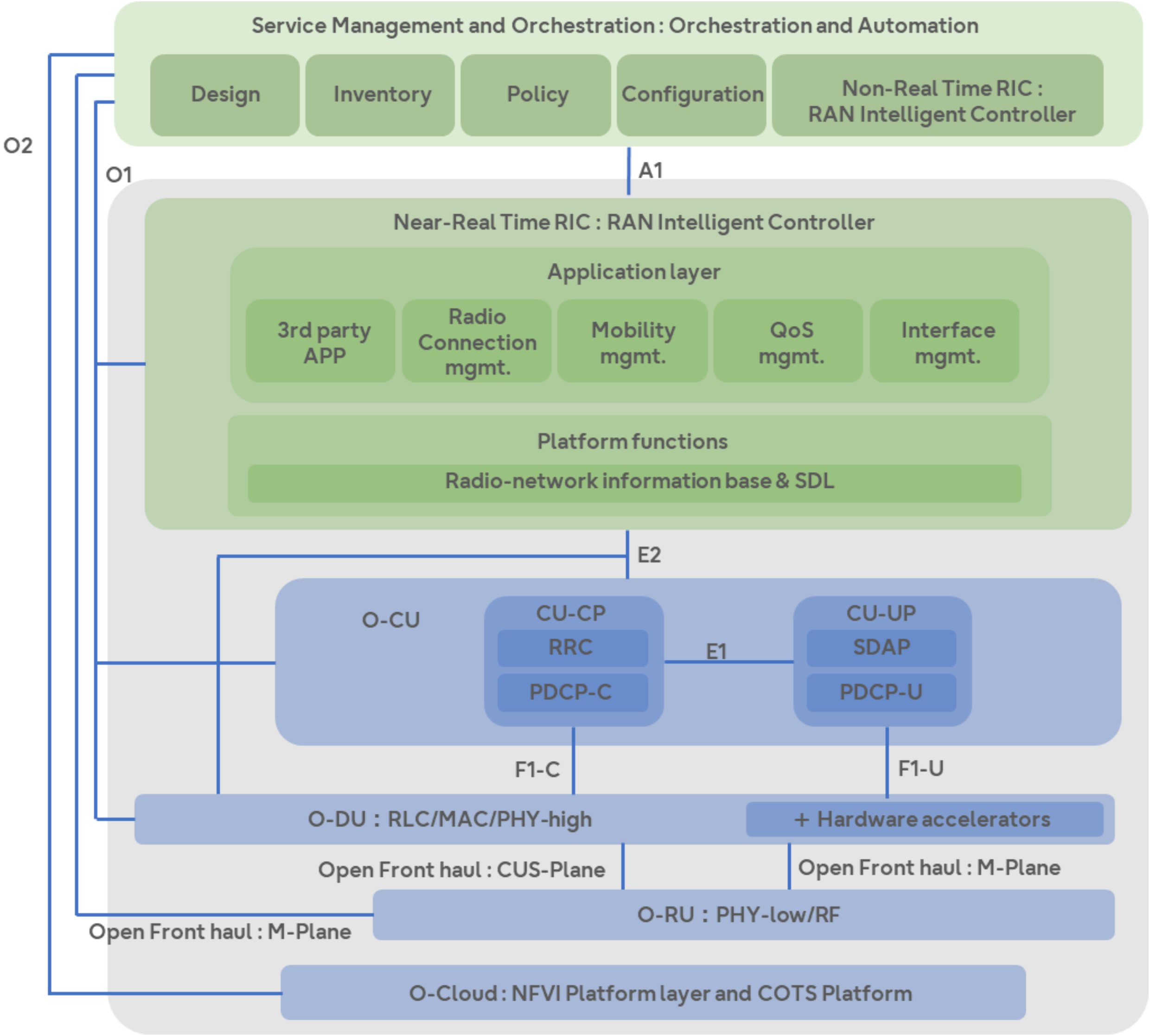
Service Management and Orchestration : Orchestration and Automation
Design
Inventory
Policy
Configuration
Non-Real Time RIC : RAN Intelligent Controller
O2
O1
A1
Near-Real Time RIC : RAN Intelligent Controller
Application layer
3rd party APP
Radio Connection mgmt.
Mobility mgmt.
QoS mgmt.
Interface mgmt.
Platform functions
Radio-network information base & SDL
E2
O-CU
CU-CP
RRC
PDCP-C
E1
CU-UP
SDAP
PDCP-U
F1-C
F1-U
O-DU : RLC/MAC/PHY-high
+ Hardware accelerators
Open Front haul : CUS-Plane
Open Front haul : M-Plane
O-RU : PHY-low/RF
Open Front haul : M-Plane
O-Cloud : NFVI Platform layer and COTS Platform

Figure 1 : O-RAN Architecture

3 A Few Key Features of O-RAN Architecture

In this section some key security features of O-RAN such as "zero trust principle", secure SDLC, SBOM and operator's role are addressed.

3.1 Zero Trust

O-RAN Alliance's architecture for RAN is built on the secure foundation of "zero trust" where network elements mutually authenticate with each other in order to communicate. Entities and users are authenticated, authorized, and continuously validated to access or keep access to services and data. Additionally, access to resources is granted only when it is needed minimizing the risk of security mishaps.

3.2 Secure SDLC

SDLC (Software Development Life Cycle) is a process that enables the generation of high-quality, low-cost software, in a short time. Traditionally, security testing is completed at the end. As such vulnerabilities are found late in the game when it is more costly and takes longer to repair. A preferred approach is to utilize "secure by design" principle by integrating security testing and other security related activities into an existing development process and is referred to as secure SDLC. Utilization of secure SDLC in O-RAN networks results in significant mitigation of security risks.

Security automation is implemented in O-RAN architecture software. In fact, at every stage of continuous integration/continuous deployment (CI/CD) security is incorporated. This way security risks are eliminated -or reduced- as vulnerabilities are discovered before actual deployment phase.

3.3 SBOM

Software Bill of Material (SBOM) is an inventory of software components and dependencies, information about those components, and their hierarchical relationships. It documents both proprietary and third-party software including commercial, free and open-source software. Lack of information contained in SBOM contributes substantially to cybersecurity risks as well as the costs of development, procurement, and maintenance. Benefits of SBOM include reducing cost, security risk, license risk, and compliance risk [3].

A set of SBOM requirements were developed based on a US DoC and NTIA [9]. For instance, vendors should deliver SBOM with not only software delivery, but patches as well. SBOM must be kept encrypted for either delivery or storage purposes. Acceptable formats include Software Package Data eXchange (SPDX) [10], CycloneDX [11], or 19 Software Identification (SWID) [12]. Risk level for any given vulnerability should be determined by vendor and operator based on the specific use case and environment. Vendors and operators should utilize SBOM for risk identification [3].

3.4 Operator's Role

Due to disaggregated nature of O-RAN, operators enjoy improved visibility into the working of the network. On one hand, they can directly enforce security measures with the cloud infrastructure and software suppliers. On the other hand, they can deploy the latest security tools to insure safe and secure operation of the network. Above and beyond that, by deploying AI based automated detection and monitoring tools, Operators can quickly detect and resolve anomalies in the network.

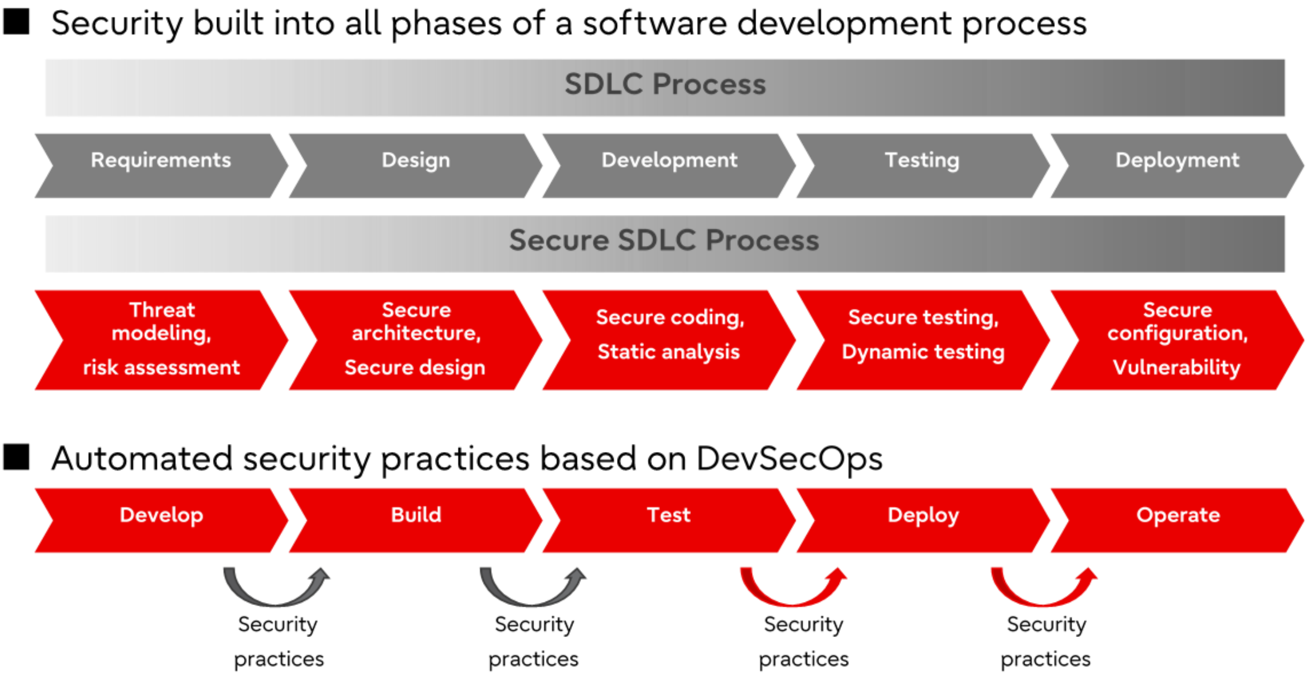
■ Security built into all phases of a software development process
SDLC Process
Requirements
Design
Development
Testing
Deployment
Secure SDLC Process
Threat modeling, risk assessment
Secure architecture, Secure design
Secure coding, Static analysis
Secure testing, Dynamic testing
Secure configuration, Vulnerability
■ Automated security practices based on DevSecOps
Develop
Build
Test
Deploy
Operate
Security practices
Security practices
Security practices
Security practices

Figure 2 : Secure SDLC

4 Security Tests

A comprehensive set of security testing methodologies and processes are put into place to ensure secure and robust operation of end-to-end O-RAN system. The goals of the security tests specifications are 1) to validate implementation of security protocols, 2) to emulate attacks against components of O-RAN system, 3) to measure system robustness and 4) to validate the effectiveness of security mitigation methods. To address the test methodology and configuration, required test tools are listed. The recommendations for producing detailed test reports are described. Lastly, a test template is provided [5].

Two types of security tests known as common test and O-RAN specific tests are described. Common security tests include service enumeration, password-based authentication, network protocol fuzzing, and DoS. In addition to the common security tests, testing of various system software, ML, components and interfaces of the O-RAN system are discussed [5].

5 Fujitsu's Thoughts

Fujitsu has been a global supplier of RAN solutions for over 25 years. Over the years, customer specific solutions have been designed and shipped to various markets across the globe. As for 5G, Fujitsu has supplied various components of RAN architecture since 2019. Fujitsu has been following O-RAN developments and specifications.

O-RAN Alliance advocates the use of open, virtual, containerized, cloud -based components in the radio access network architecture. Some of these attributes have been deployed in IT, but they are new to the RAN industry. It might appear that due to attributes such as openness, virtualization and open interfaces the RAN security is compromised.

This paper we have examined various components of O-RAN security and summarized O-RAN's proposed security solutions. It is our belief that the O-RAN's ensemble of security aware architecture, powerful security protocols, risk based-detailed upfront analysis, well-devised processes and industry best practices results in sufficiently secure RANs.

6 Concluding Remarks

The paper examined the architectural components of O-RAN such as interfaces, functions and data paths. Specific security measures for Near-RT RIC, Non-RT RIC and O-Cloud were described and their benefits were listed. Then the utilized security protocols, their implementation details as well as their benefits were outlined. Prominent security features deployed in O-RAN such as zero trust principle, utilization of secure SLDC and SBOM and operator's role were also explored.

Analysis of security issue in O-RAN demonstrates that recommended and beneficial guidelines as well as powerful protocols have been designed to enable end-to-end security. To gain enough confidence in secure operation of a network a comprehensive set of security tests and procedures have been provided to cover the most conceivable scenarios. It is believed that the thoughtful security designs, utilized principles, best practices and advanced protocols deployed in O-RAN result in secure radio networks. However, cybersecurity risks can only be mitigated with a combination of people, processes, and technology.

To further secure such a software base station is a life cycle of software centering on an SBOM. Carriers will be able to share all the software in their supply chain as a bill of materials from vendors so that they can work quickly to update the included software. Vendors need a modern IT development environment in addition to networking technology to respond quickly.

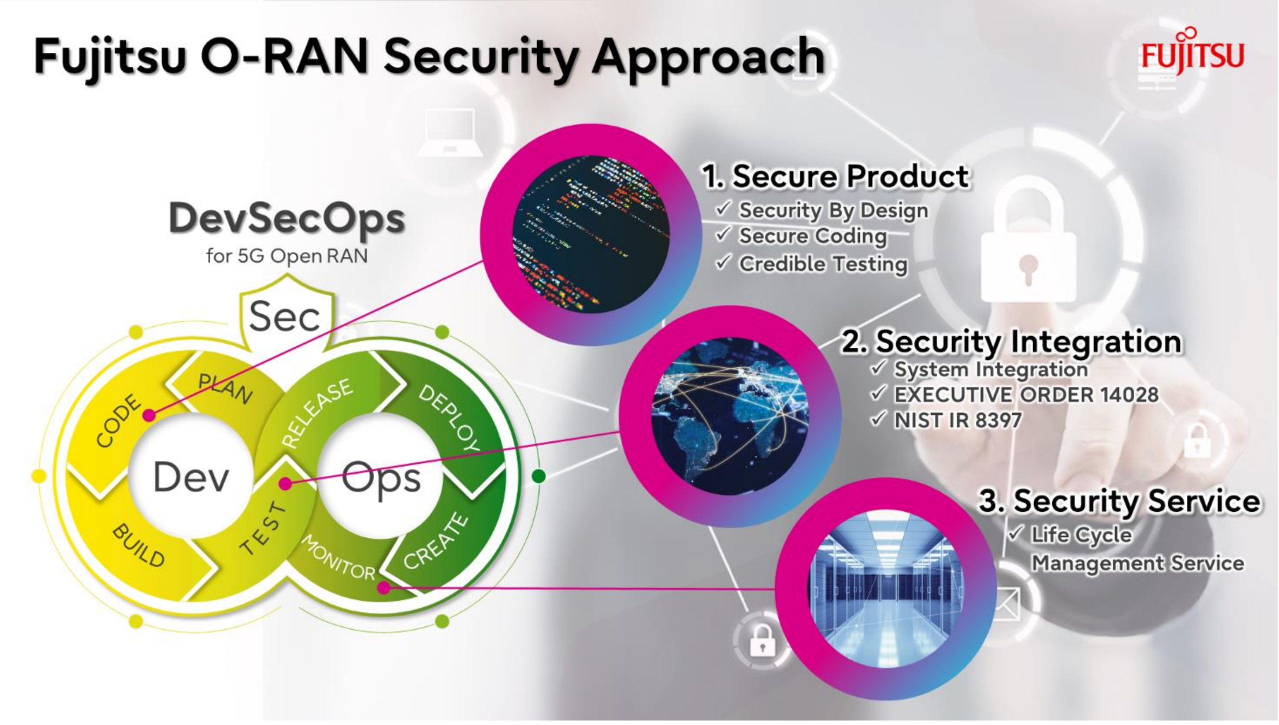

Figure 3：Fujitsu O-RAN Security Approach

7 References

[1] https://www.o-ran.org/
[2] O-RAN ALLIANCE, "O-RAN Security Threat Modeling and Remediation Analysis 3.0", July 2022
[3] O-RAN ALLIANCE, "O-RAN Security Requirements Specifications 3.0", July 2022
[4] O-RAN ALLIANCE, "O-RAN Security Protocols Specifications 3.0", March 2022
[5] O-RAN ALLIANCE, "O-RAN Security Tests Specifications 2.0", July 2022
[6] O-RAN ALLIANCE, "O-RAN Study for Near Real Time RIC and xApp 1.0", July 2022
[7] O-RAN ALLIANCE, "O-RAN Study for Non-RT-RIC 1.0", July 2022
[8] O-RAN ALLIANCE, "O-RAN Study for O-CLOUD 1.0", July 2022
[9] "The Minimum Elements for a Software Bill of Materials (SBOM), Pursuant to Executive Order 14028 on Improving the Nation's Cybersecurity", U.S. DoC and NTIA, July 2021
[10] SPDX, https://spdx.dev/
[11] CycloneDX, https://cyclonedx.org/
[12] Guidelines for the Creation of Interoperable Software Identification (SWID) Tags, https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8060.pdf

For detail access …

https://www.fujitsu.com/global/products/network/solutions/wireless.html

Fujitsu Limited

Shiodome City Center
1-5-2, Higashi Shimbashi
Minato-ku, Tokyo 105 -7123, JAPAN
https://www. fujitsu. com/global/

Fujitsu Limited registered in many jurisdictions worldwide. Other product, service and company names mentioned herein may be trademarks of Fujitsu or other companies. This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assets no liability related to its use.