RADBOUD UNIVERSITY

Faculty of Science

SECURITY OF O-RAN
THE ROAD TO A PRACTICAL RISK ANALYSIS

June 9, 2023

Master Thesis Report

Sotiris Michaelides (s1071807)

Supervised by:
Dr. David Rupprecht, Radboud University

Examined by:
Dr. Katharina Kohls, Radboud University
Dr. Erik Poll, Radboud University

Abstract

Traditionally, the Radio Access Networks (RAN) components are only compatible with other components made by the same manufacturer, resulting in a closed marker that four major companies control. Open Radio Access Network (ORAN), a new architectural expansion of the Next Generation Radio Access Networks (NG-RAN), aims to break the closed RAN market by "opening" the interfaces between the different RAN components. Furthermore, it modernizes the RAN by introducing/adopting new technologies to the RAN, like machine learning, virtualization, and disaggregation. However, the security of O-RAN's architectural design has recently raised concerns and sparked debates following a theoretical risk analysis conducted by the German Federal Office Of Information Security (BSI). The analysis concluded that the architecture was unsecured, warranting further attention. In addition, subsequent theoretical risk analyses that have been conducted only increased concerns regarding the security of the architecture. To the best of our knowledge, no practical one has been performed yet, which is essential for an accurate evaluation of the security of the architecture. Practical risk analyses are important, as they enable the evaluation of the feasibility of every attack, and their consequences in a real world scenario. This thesis, aims to perform the first practical risk analysis on a specific component of the architecture, namely the Open Fronthaul. As a practical risk analysis requires a physical setup, we discuss, and partially deploy a minimal, future-proof O-RAN Alliance's ORAN (O-RAN) 5G network, able to accommodate various practical risk analyses on the different elements and interfaces, as well as the evaluation of suggested countermeasures. Furthermore, as the first O-RAN compliant components entering the market, we conduct an updated risk analysis that builds upon the findings of the previous analysis conducted by the BSI, taking into account the latest specifications of O-RAN, to evaluate the current state of security of the architecture and identify unacknowledged threats. Since O-RAN is a significant contender for the upcoming 6G RAN architecture, apart from the analysis, we present several recommendations that aim to improve the overall security of O-RAN.

Acknowledgements

I would like to formally acknowledge and express my gratitude to my supervisor, Dr. David Rupprecht, for his unwavering support and guidance throughout the entire process. Dr. Rupprecht demonstrated a deep understanding of my interests and proposed a change to my initial master thesis topic, which I enthusiastically embraced. He was open to suggestions and provided me with the freedom to pursue my ideas, instilling confidence in my abilities. I am truly grateful for his invaluable feedback and for the significant amount of time he dedicated to liaising with hardware and software vendors on my behalf. Furthermore, I extend my heartfelt appreciation to Dr. Rupprecht for encouraging my participation in my first academic conference, where I had the opportunity to present the poster that we, along with my first examiner, Dr. Katarina, worked on. Additionally, I am immensely grateful to both Dr. Rupprecht and Dr. Katarina for generously funding my trip to the conference, which took place in the UK.

Furthermore, I would also like to express my heartfelt gratitude to my family for their unwavering support throughout this journey, both financially and emotionally. Their constant encouragement and belief in my abilities have been instrumental in my success. I am also grateful to all of my friends for their support and encouragement along the way. Their presence and words of encouragement have been invaluable to me.

Contents

List of Figures

List of Tables

1 Introduction

5G is the latest cutting-edge generation of mobile networks, providing the communication infrastructure for billions of people worldwide. 5G technology is crucial for our modern society as it connects billions of IoT(Internet Of Things) devices, like smartphones, sensors, cars...; and supports essential services like networks for self-driving cars, energy management, and real-time connections to healthcare institutions. With its high-speed and low-latency capabilities, 5G revolutionizes various sectors, improving efficiency, safety, and quality of life. Therefore, ensuring the security of 5G technology is of paramount importance. Attacks on 5G networks have the potential to disrupt the functioning of our society and even pose threats to human lives.

The architectural design of 5G is no different from the previous generation of mobile networks, comprised of the User Equipment (UE), the RAN, and the Core Network (CN). UE is usually a 5G-capable smartphone paired with a SIM(Subscriber Identity Module) card that may access the network's functions that reside in the CN. RAN serves as the intermediary between the UE and the CN, being physically linked to the core while providing wireless connectivity to the UE.

This master thesis centers its attention on the RAN. RANs are traditionally composed of a Baseband Unit (BBU) and a Radio Unit (RU)[1]. BBU implements the whole network layer protocol stack while the Radio Frequencies (RF) are being handled by the RU. The communication between the two components uses a semi-proprietary, Point-to-Point protocol called Common Public Radio Interface (CPRI). The proprietary state of the interface enabled hardware manufacturers to implement the interface according to their preferences, resulting in optimized black-box-like implementations. Despite the optimized implementations, the flexibility and the scalability of the RAN are limited, as components from different vendors are not compatible between them, and implementing new functions to the network often requires upgrading the whole infrastructure. Consequently, Network Operators frequently encounter significant expenses when upgrading their Radio Access Networks (RANs) while relying entirely on manufacturers to implement new features into the hardware. More importantly, this approach has led to a monopolized market dominated by only four major competitors, in which innovation solely depends on them. Any new "player" interested in entering the market, must develop the entire RAN architecture which poses significant challenges and costs.

Over time, various flexible architectures for RAN have been proposed to reduce costs and enhance system flexibility and scalability. Despite their potential benefits, these architectures were not standardized, as they struggled to overcome the challenge of vendor-locked solutions. Centralized-RAN(cRAN) and Virtual-RAN(vRAN) are two examples of these critical approaches. cRAN proposes a centralized architecture in which the BBUs are located in a central location and connected to Remote Radio Units (RRUs) that remain deployed at the cell sites. vRAN supports the separation of network functions from the underlying Hardware (HW), a method known as virtualization, allowing for specialized Software (SW) that can be executed on generic hardware platforms.

During the 4G era, the 3rd Generation Partnership Project (3GPP) introduced a concept called disaggregation, which involved splitting the BBU into two modular, open, and interoperable components known as the Central Unit (CU) and Distributed Unit (DU). Building upon this disaggregated approach, ORAN[2] represents a novel architectural approach promoted by the O-RAN Alliance. O-RAN[3] inherits concepts from both cRAN and vRAN, like virtualization, while expanding on the current NG-RAN architecture. O-RAN introduces the concepts of Machine Learning (ML) to the architecture to enhance the RAN functionalities. Furthermore, O-RAN aims to break the existing monopolized market by implementing open interfaces between various

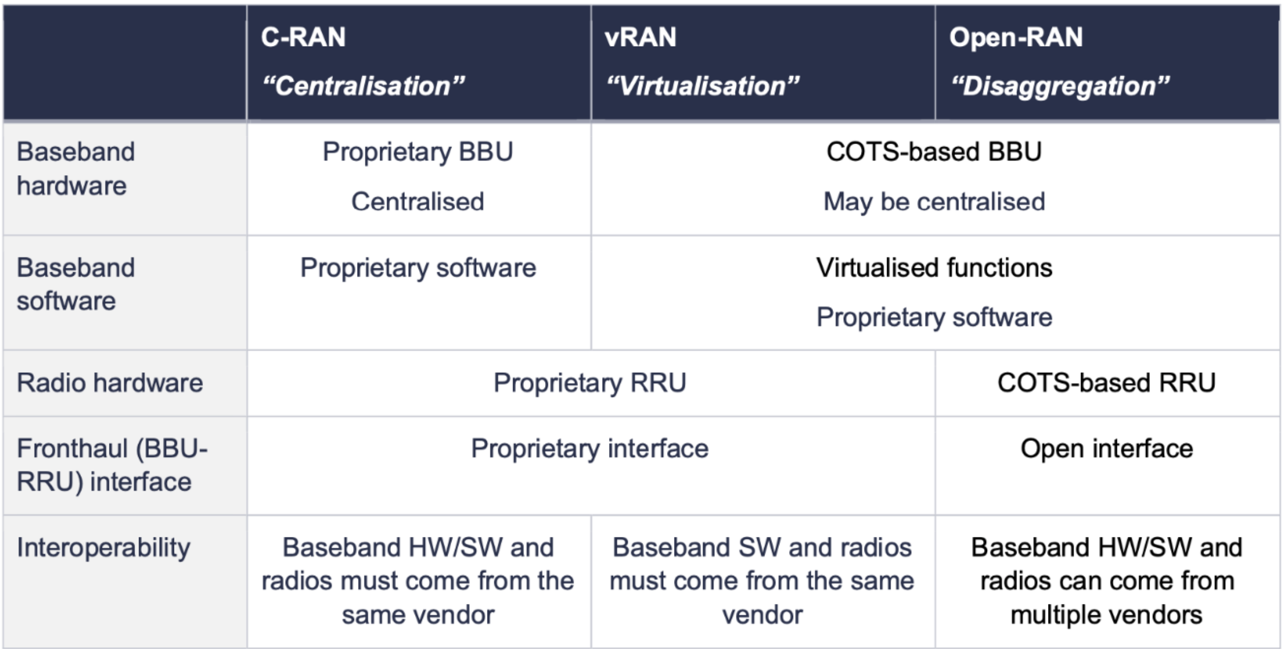
[1] Also known as Remote Radio Unit (RRH)

[2] ORAN: The idea of an open RAN architecture with open interfaces between its components

[3] O-RAN: The realization of ORAN, according to the O-RAN Alliance Specifications

components of the RAN. Doing so enables new interested parties to enter the market without the obligation of providing the entire RAN architecture. This approach fosters competition and encourages innovation while promoting a more diverse, dynamic, and flexible RAN.

Fig.1 provides a brief overview of the distinctions and similarities between cRAN, vRAN, and O-RAN while Fig.2 visually represents these differences/similarities, aiding in better understanding the different architectures.



	C-RAN *"Centralisation"*	vRAN *"Virtualisation"*	Open-RAN *"Disaggregation"*
Baseband hardware	Proprietary BBU Centralised	COTS-based BBU May be centralised	
Baseband software	Proprietary software	Virtualised functions Proprietary software	
Radio hardware	Proprietary RRU		COTS-based RRU
Fronthaul (BBU-RRU) interface	Proprietary interface		Open interface
Interoperability	Baseband HW/SW and radios must come from the same vendor	Baseband SW and radios must come from the same vendor	Baseband HW/SW and radios can come from multiple vendors

Figure 1: Differences between cRAN,vRAN and ORAN[64]

However, as the RAN architecture expands, so does the attack surface. The introduction of new concepts, such as ML, open interfaces, and virtualization, exposes the architecture to new attacks, previously unseen under the RAN concept. These new threats usually fall under three different areas: Virtualization, Openness, and ML, and expand the now-existing set of identified threats related to the NG-RAN. A BSI study concluded that O-RAN is vulnerable and exposed to attacks, as it lacks basic-mandatory security controls [35]. Other theoretical analyses have shown similar results [3][40][42].

While a theoretical risk analysis identifies potential vulnerabilities and risks in a system before attackers can exploit them, a practical analysis allows one to evaluate each attack's feasibility and consequences in a real-world environment. Attacks proven feasible in can be acceptable to live with if the required effort is high and their impact is low. In addition some attacks may require advanced setups and prior knowledge, making them difficult for an average attacker to execute. For instance, one such vulnerability in 4G networks is the lack of integrity protection for User Plane (UP) data, as many argue that higher-level protocols like Transport Layer Security Protocol (TLS) often cover this absence. Hence, it is crucial to gather results from both types of analysis before assessing whether the architecture is secure.

To the best of our knowledge, no practical security analysis of the ORAN architecture exists. The lack of easy-to-deploy O-RAN networks might be the reason behind this gap. Our original objective was to establish an O-RAN test lab and perform a practical risk assessment on a vulnerable interface within the architecture. To achieve this, we required a real setup, so we decided to deploy an O-RAN 5G network. However, our setup remained incomplete due to the lack of support for the chosen interface in the software components we used. Despite this setback, the mere exploration of ways to deploy an O-RAN test lab is itself an innovative step that can facilitate the execution of other practical risk analyses. Therefore, we choose an alternative approach to fulfill the research goals and contribute to the field.

The new approach involves a guide on deploying a basic ORAN network that can accommodate various practical risk analyses at a minimal cost, focusing on different components and interfaces of the O-RAN architecture. Furthermore, with the introduction of the first ORAN devices into the market this year, there is a pressing need for an updated theoretical risk analysis to assess the security of these devices. Deploying unsecured components in real-world scenarios poses a significant threat to Network Operators, making it essential to identify and evaluate potential vulnerabilities. For this reason, we also present a theoretical risk analysis that follows the same approach as the BSI analysis, but it is based on the latest version of security requirements($v5$). Our analysis can be described as an update to the existing analysis conducted by the BSI on the first version($v1$) of the security requirements. Additionally, we identify a new threat, currently not acknowledged by O-RAN alliance and in the end, we also provide recommendations and ideas on enhancing the security of ORAN. These suggestions are based on existing studies and our knowledge and judgment.

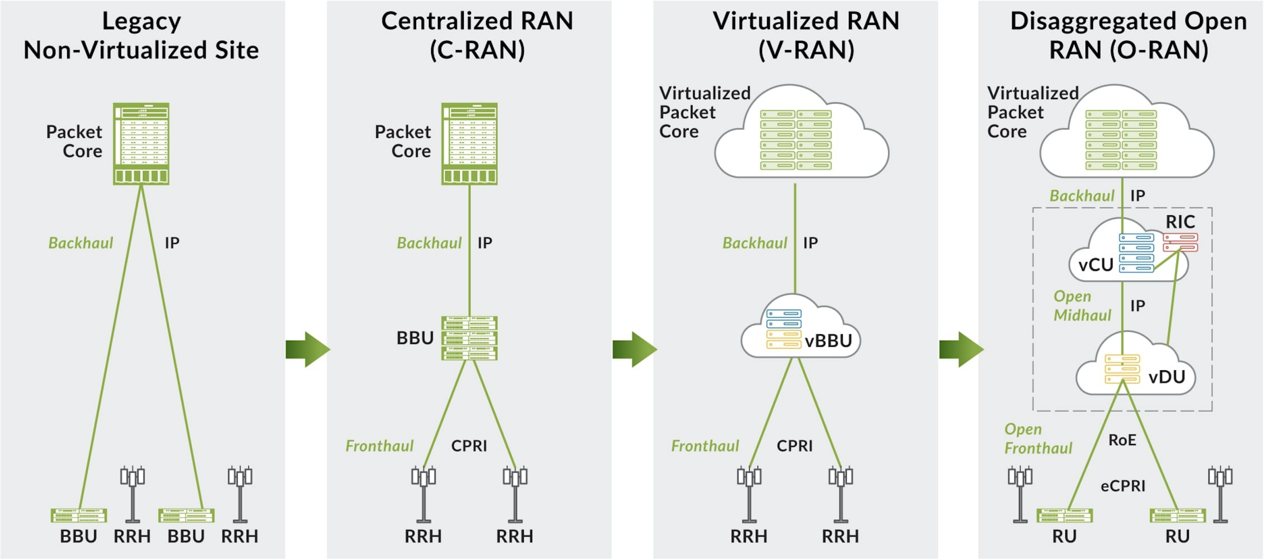


Figure 2: Visual Representation of cRAN,vRAN and ORAN[56]

It is crucial to mention that our setup is expected to be deployed by the end of June 2023, as indicated by the information provided by the software vendors. Once we have the opportunity, we will complete our setup and fulfill our initial goal of conducting the practical risk assessment on the vulnerable interface within the O-RAN architecture. We remain committed to achieving our original objective as soon as possible.

2 Technical Background

In this section, we provide information and explain basic terms and essential concepts, before describing the work conducted in the central parts of this thesis. This information includes a description of a 5G Network and its components, mainly focusing on the NG-RAN architecture. Additionally, we present the O-RAN, including its various components and interfaces. Lastly, we provide a concise overview of several security protocols to contextualize the upcoming analysis.

2.1 5G Network Overview

5G is the latest generation of Mobile Networks, designed to meet the increasing needs for high speed[4], low latency and reliable communication[5], while being able to handle the large number of devices[6] (e.g., cars, grids, sensors...) that are expected to be joining the network as the Internet of Things(IoT) era unfolds. Fig.3 shows the different use cases and applications of the 5G network in relation to the needs of each scenario. In this thesis, we are only concerned with the eMBB, which utilizes the New Radio technology capable of supporting frequencies up to 100GHz for faster speeds. The importance of this is clarified later on.

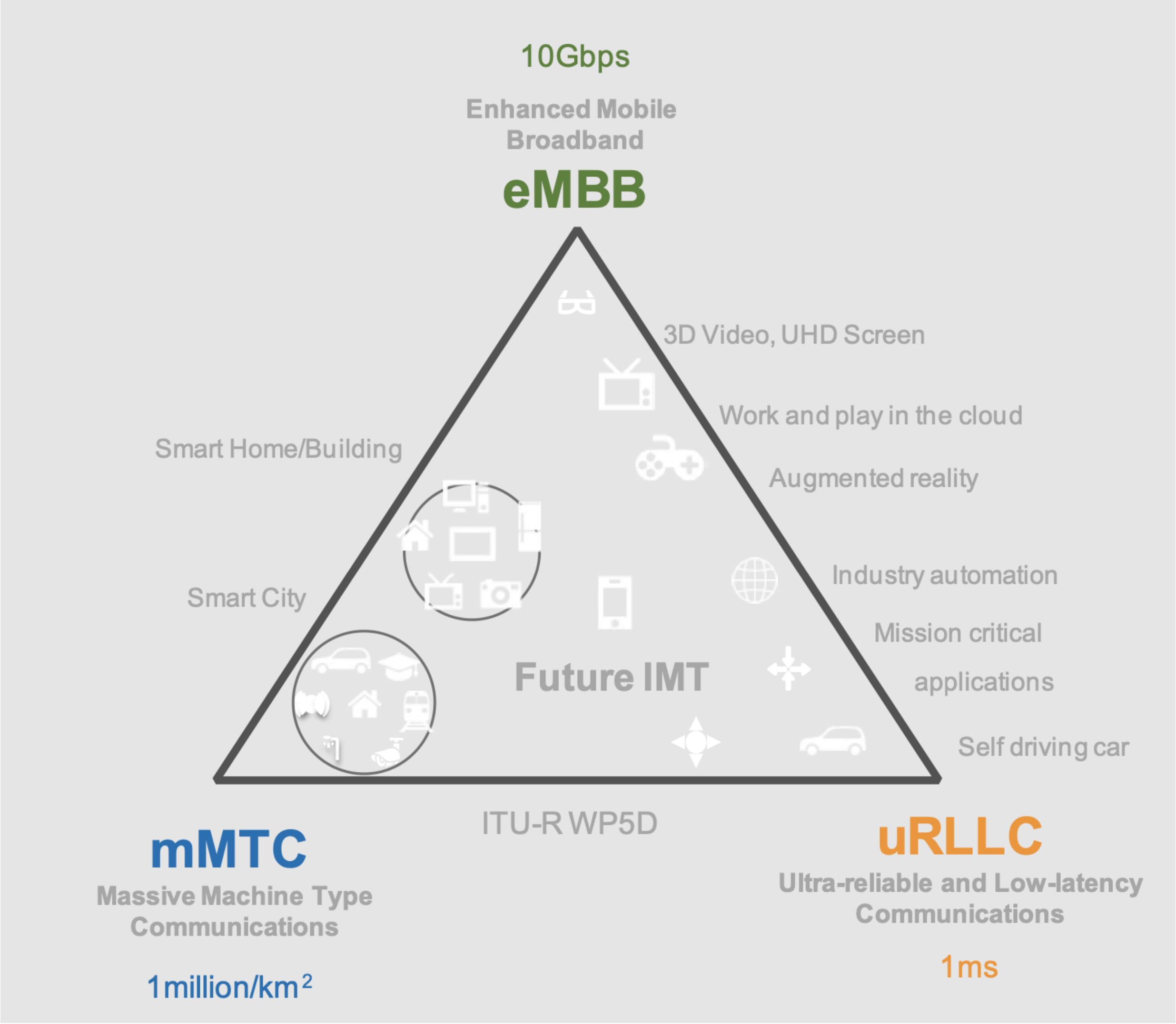
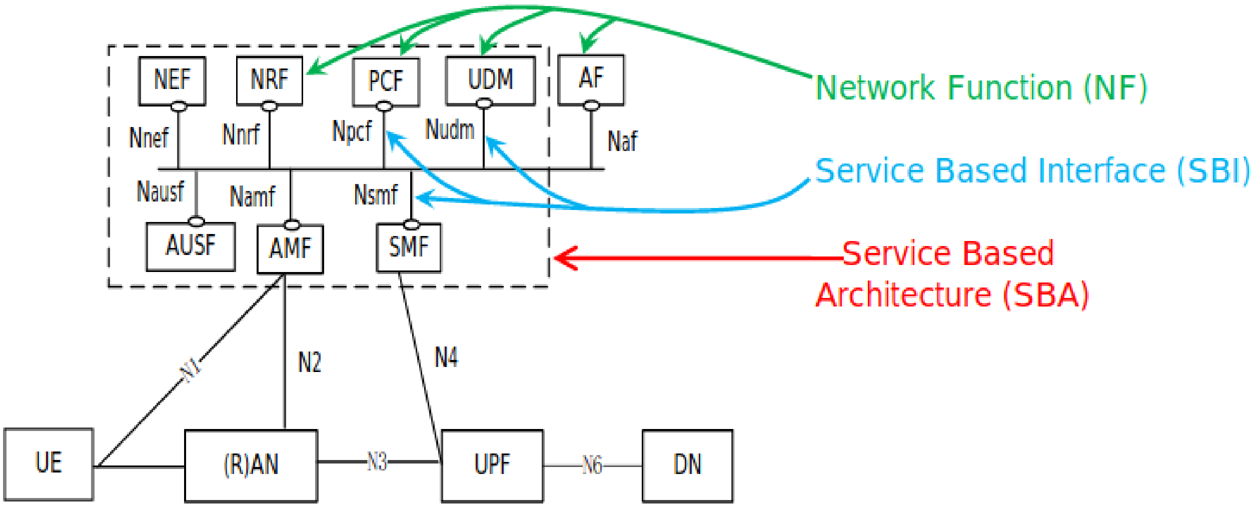

10Gbps
Enhanced Mobile Broadband
eMBB
3D Video, UHD Screen
Work and play in the cloud
Augmented reality
Industry automation
Mission critical applications
Self driving car
Smart Home/Building
Smart City
Future IMT
ITU-R WP5D
mMTC
Massive Machine Type Communications
1million/km²
uRLLC
Ultra-reliable and Low-latency Communications
1ms

Figure 3: 5G Uses Cases Depending on the Requirements[55]

[4] Also known as Enhance Mobile Broadband(eMBB)
[5] Also known as Ultra-Reliable and Low-Latency Communications(uRLLC)
[6] Also known as Massive Machine Type Communications(mMTC)

A 5G network consists of the same components as the previous generations of networks, namely the UE, the RAN, and the CN. The UE comprises a Mobile Station and a SIM card. Within the SIM, the Subscriber's Permanent Identifier(SUPI) is stored, along with a cryptographic key, which are used to authenticate the UE towards the CN. The UE establishes connections with the RAN and applies encryption and Integrity protection to the packets before transmitting them over the wireless interface. The RAN provides connectivity between the UE and the CN, and it is also responsible for managing the radio resources and applying Integrity protection/encryption to the UP data before sending them to the UE over the wireless interface. Finally, the CN hosts critical services such as the Access and Mobility Management Function (AMF) and the User Plane Function (UPF), among others. These functions can access each other's services through Application Programming Interface (API)s, a concept known as service-based architecture defined by the 3GPP. The AMF in the CN is responsible for enforcing security controls for the Control Plane (CP) data. Some examples of services provided by the CN function are Authentication, Mobility Management, Session management, and transmission of the UP data. The 5G architecture is depicted in Fig.4



NEF	Network Exposure Function	AMF	Access &Mobility Management Function
NRF	Network Repository Function	SMF	Session Management Function
PCF	Policy Control Function	UE	User Equipment
UDM	Unified Data Management	(R)AN	(Radio) Access Network
AF	Application Function	UPF	User Plane Function
AUSF	Authentication Server Function	DN	Data Network

Figure 4: 5G Network Architecture[36]

The CP and UP data mentioned earlier are associated with a feature introduced during the 4G era known as Control and User Plane Separation (CUPS). With CUPS, Operators have the flexibility to optimize the placement of network functions to enhance performance and efficiency. UP data refers to the actual data generated by Users, such as web browsing, email communications, video streaming, and other content sent over the IP network. This data is processed and transmitted by UPF, usually placed closer to the End-Users to achieve faster transmission rates and reduced latency. On the other hand, CP data refers to the data exchanged between the network elements for establishing and handling communication sessions. This data includes signaling, authentication, and mobility management messages. The AMF is responsible for handling CP data and is often positioned in a centralized location to enable better management and control. The unique placement of UPF, outside of the CN, can be seen in Fig.4.
Since this thesis primarily focuses on the RAN, we are not discussing other details related to the CN(and its functions) or the UE. The provided information should be enough to understand the content of this study.

2.2 NG-RAN Protocol Stack and Architecture

The NG-RAN can be deployed in two different methods. The first method is the monolithic deployment, where the Central Unit and the Distributed Unit are coupled together. This approach is similar to the previous generation's BBU approach. In the case of the dissagregated deployment, the CU and the DU are separated and linked with the F1 interface. The central unit is further split into two parts: CU-UP and CU-CP, which handle the UP data and CP data respectively. This split allows for independent enhancements and optimizations for each plane. Similarly, the F1 follows the same split. This deployment is depicted in Fig.5. The E1 interface, which connects the the two CU components, is not visible in this figure, but can be seen in Fig.8.

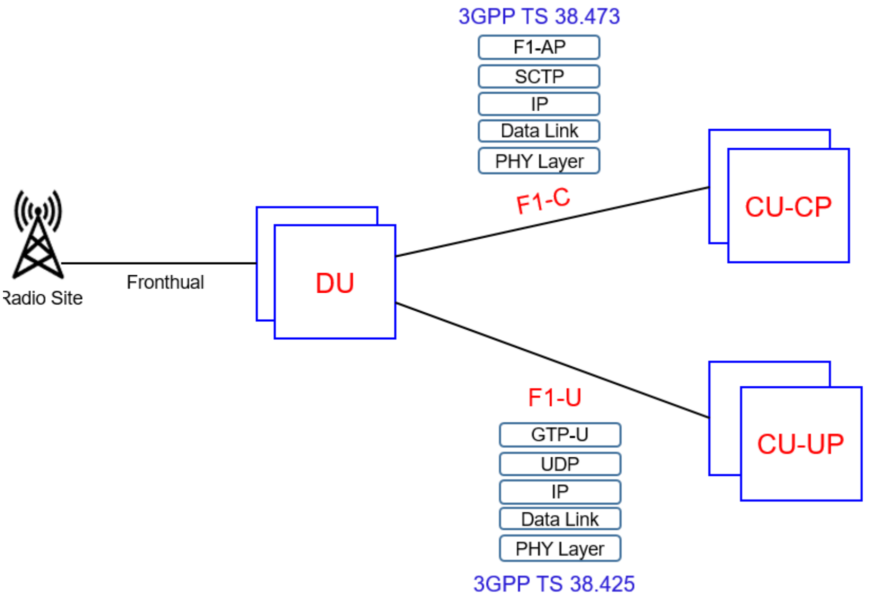


Figure 5: NGRAN Dissagregated Architecture[68]

The NG-RAN protocol stack is the set of protocols that define the communication between UE and the Next Generation NodeB (gNB), with the exception of the NAS protocol that defines communication between the UE and the AMF. The stack of protocols is shown in Fig.6. As the O-RAN architecture is building upon the disaggregated version of NG-RAN, we examine the protocols implemented by RAN component in the architecture.

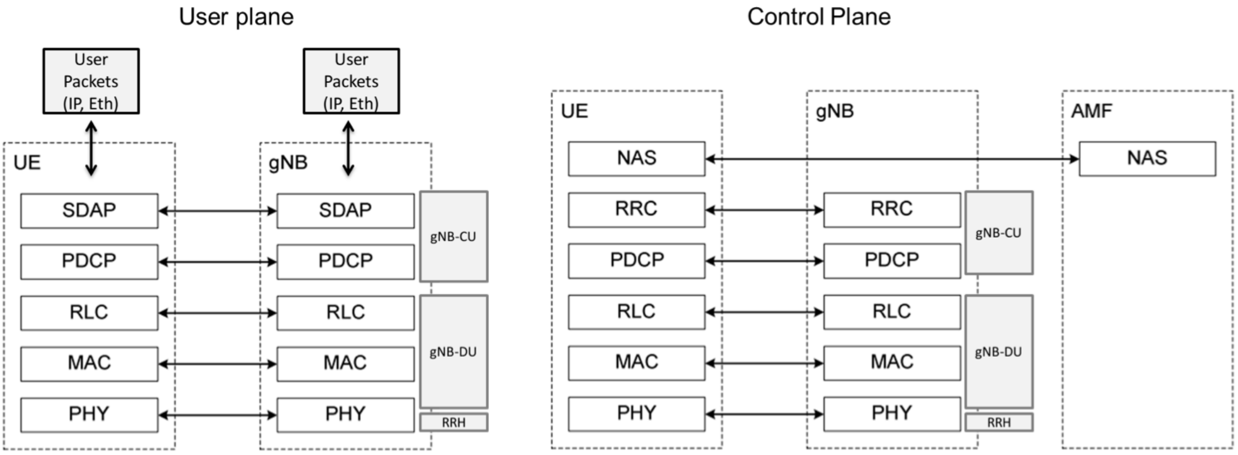


Figure 6: NGRAN Protocol Stack[19]

2.2.1 RU

As explained before, manufacturers design the Fronthaul interface according to their preferences. Therefore the exact implemented protocols/functions remain RU are unknown, as they depend on the functional split(of the protocol stack) that the manufacturer will choose. However, ORAN standards suggest that the RU implements the lower part of the Physical layer(PHY), apart from the RF processing. The PHY is the bottommost layer in the communication stack and primarily transmits and receives information over the air using signal processing techniques. It interacts with the Medium Access Control(MAC) layer. It performs various operations such as channel coding, rate matching, interleaving, scrambling, baseband modulation, multi-antenna transmission, digital precoding, resource element mapping, beam forming, modulation, and antenna mapping. The Low-PHY usually includes the functions of beamforming, precoding, and Fast Furrier Transformation for signal processing. It is important to note that many RU do not implement any part of the Low-PHY.

2.2.2 DU

The DU implements the High-PHY layer which includes the functions that are not implemented by the RU. Furthermore, it implements parts of the Data link Layer, namely the MAC and RLC:

- MAC: It is responsible for managing the communication between the gNB and the UEs at a low-level. It handles tasks such as scheduling the transmissions, error correction, and retransmissions.
- Radio Link Control(RLC): Provides three transportation modes for the data: Transparent Mode (TM), Unacknowledged Mode (UM), and Acknowledged Mode (AM). Each mode allows for data transmission and reception, but in TM and UM, two separate entities handle transmission and reception, while in AM mode, a single entity handles both functions.

2.2.3 CU

The CU implements the other protocols of the Data link layer, specifically the PDCP and SDAP, along with the RCC from the Network layer.

- Packet Data Convergence Protocol(PDCP): Performs various functions, such as robust header compression(RHCO), encryption, and Integrity protection. Additionally, the PDCP is responsible for separating Control and User data.
- Service Data Adaptation Protocol(SDAP): Handles the Quality Of Service (QoS) Flows across 5G wireless interface.
- The Radio Resource Control(RCC): It is responsible for managing the connections between the UE and the gNB. Its tasks include the establishment/release of connections, reconfiguration of radio bearers and paging notifications, among others.

2.2.4 NAS

The other protocol of the 5G stack is the Non Access Stratum Protocol(NAS) which is implemented only by the UE and the AMF. NAS is the signaling protocol and can be further divided into to two sub-layers:

- NAS Mobility Management(NAS-MM): It is responsible for paging, mobility management, authentication, and identity management.

- The NAS Session Management(NAS-SM): It is responsible for communication links establishment and management, IP address assignment, and performing functions related to the QoS.

2.3 Security Of CP/UP Data

3GPP specifications define different controls to secure CP and UP plane data[1]. Here, we briefly explain how each plane is protected, which is crucial for our upcoming analysis. For both planes, encryption and Integrity protection are the two security controls provided to ensure a secure communication channel. In the case of CP data, the encryption/Integrity protection of the data is enforced between the UE and the AMF(in the CN). This protects the the data from malicious RAN Operators. However, encryption is optional, depending on the Network Operator's decision, while Integrity protection is mandatory. For UP data, neither encryption nor Integrity protection is mandatory. Furthermore, even if the Network Operator chooses to secure the User plane data by implementing the previously mentioned optional controls, it is only protected between the UE and the gNB(CU). The security controls are visualized in Fig.7, in which *(M)* indicates a mandatory control.

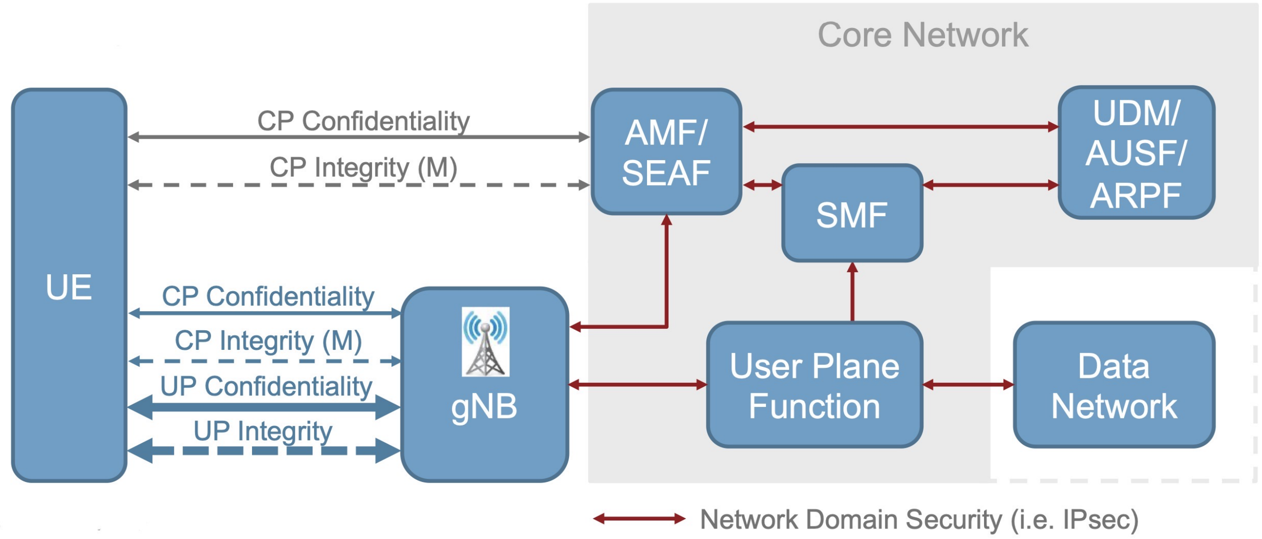


Figure 7: Security of UP/CP Data[30]

2.4 Open-RAN Architecture

In this section, we examine each component of the O-RAN architecture. O-RAN is a relatively new architecture proposed only a couple of years ago, in 2020, by O-RAN alliance to realize the idea of ORAN. O-RAN adopts the disaggregated deployment of the gNB of the NG-RAN and introduces new components, techniques, and open interfaces for improved functionality. An overall depiction of the architecture, with every component and interface, is presented in Fig.8. The O-RAN architecture promotes interoperability among various RAN components, facilitating the deployment of diverse RAN solutions, compared to the NG-RAN architecture. Additionally, O-RAN supports the implementation of third-party applications and incorporates modern techniques, like ML and Artificial Intelligence (AI), to enhance the various RAN functionalities, including End-to-End resource allocation, monitoring, and real-time enforcement of QoS. Therefore, O-RAN deployments are considered more flexible, intelligent, and vendor interdependent than traditional RANs. For these reasons, it is likely that O-RAN will be the next standard for the RAN architecture. If successful, O-RAN has the potential to revolutionize the RAN market, currently dominated by a small number of vendors, by fostering innovation and promoting fair competition.

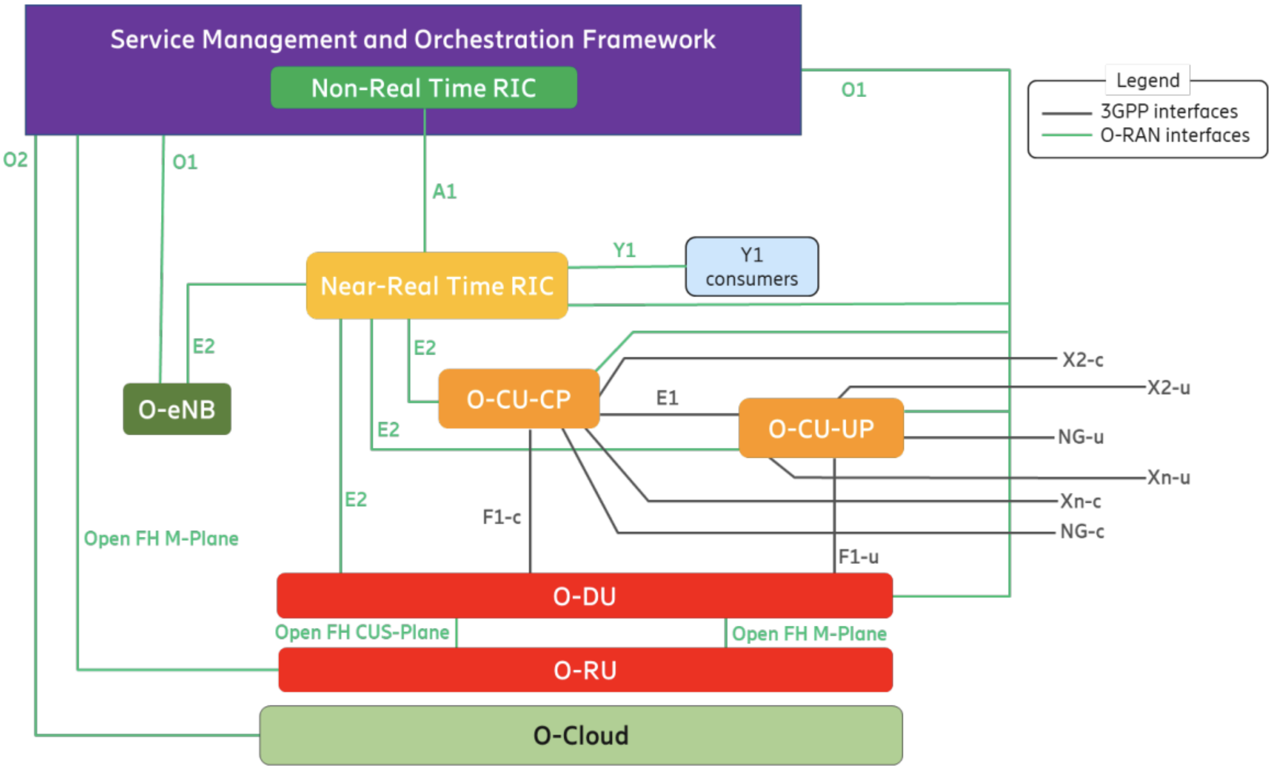


Figure 8: O-RAN Architecture[8]

Important notes: The O-eNB(4G RAN) is left out of this analysis since, in this thesis, we are concerned only with 5G Networks. Furthermore, we treat the O-CU-UP and O-CU-CP as a single unit known as O-CU. This consolidation does not impact the upcoming risk analysis, as these individual units have no distinct security requirements. In addition, non-main interfaces, like the *Y1 and CTI,* are left out of this section. However, the risk analysis section includes a brief explanation regarding their functionality (Sec.3). Components and interfaces maintained by 3GPP are not included in this section or the upcoming analysis.

The description provided here will be concise, and any additional information required for upcoming analysis is explained within those sections.

2.4.1 O-RAN Network Functions

2.4.1.1 O-CU

O-CU complies with 3GPP standards, which implements all the CU required protocols outlined in Sec.2.2. In addition to the standard protocols, an O-CU supports the O1 and E2 interfaces specified by O-RAN.

2.4.1.2 O-DU and O-RU

O-RU and O-DU also adhere to 3GPP standards regarding the RU and DU. In Sec.2.2, we discussed the protocols implemented by each function, noting that the vendors determine the specific functional split. In the case of O-RAN, the interfaces are "open", i.e., clearly defined for everyone to implement. For this purpose, O-RAN adopts the 7.2x which assigns the Low-PHY and High-PHY functions to O-RU and O-DU respectively. The Open Fronthaul interface connects these components, which both O-RU and O-DU support. Fig.9 shows the 7.2x split. The orange line separates the PHY layer, with the bottom-most functions (between the line and the DAC) implemented in the ORAN Distributed Unit (O-RU) while the rest, are implemented by the O-DU. Similar to O-CU, O-DU also supports the E2 and O1 interfaces.

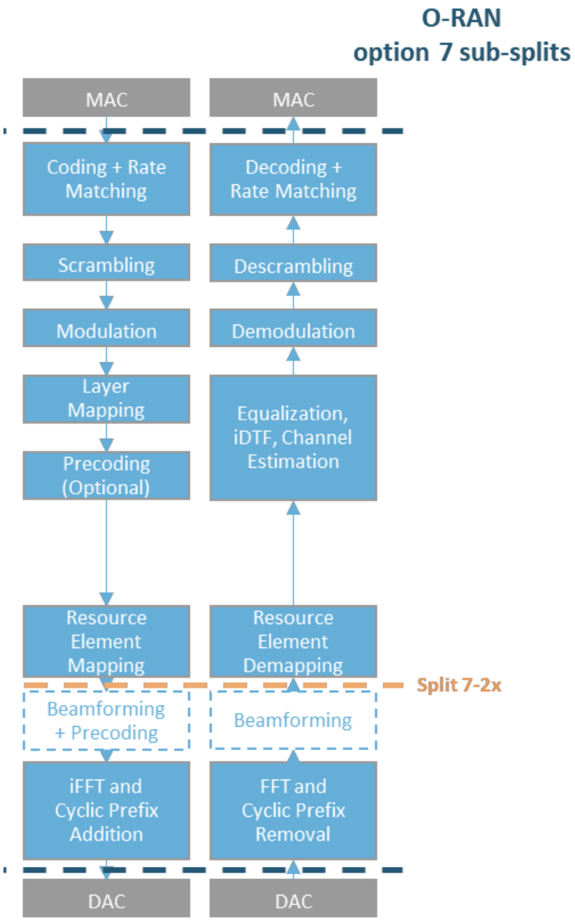


Figure 9: Split 7.2x[69]

2.4.1.3 O-Cloud

O-Cloud is the collection of physical infrastructure that hosts the execution of various RAN network functions. It consists of (decoupled) hardware and software components that allow the deployment of RAN functions such as O-DU, O-CU, Near-Real-Time RAN Intelligent Controller (nRT RIC), and non-Near-Real-Time RAN Intelligent Controller (non-RT RIC) on generic hardware. As each RAN function has unique requirements, with real-time functions needing features like real-time operating systems to manage delays, O-Cloud supports various methods of deploying a function, including containers, virtual machines, and operating systems. Furthermore, it supports means for managing, configuring, and orchestrating the hosted components.

2.4.1.4 SMO

SMO is a framework composed of several functions responsible for managing and orchestrating the O-RAN architecture, including the O-Cloud. non-RT RIC, also reside within this framework. Some critical functions of the SMO include:

- Supporting Fault, Configuration, Accounting, Performance and Security (FCAPS) management via the O1/Open Fronthaul M-Plane interface
- O-Cloud management and configuration via the O2 interface
- Collection Of data via the O1 interface
- Ran Optimisation via leveraging the non-RT RIC

- Maintain a Database (DB) with collected data, ML models and logs

The SMO is the most powerful component of the architecture.

2.4.1.5 RAN Intelligent Controllers

The intelligence and automation in the O-RAN architecture are located in the two controllers, which are leveraging ML and AI techniques to enhance RAN functionalities.

The Near-Real-Time RAN Intelligent Controller is directly connected to the O-CU and O-DU components through the E2 interface, enabling real-time data collection/analysis and modification. More specifically, the E2 Network interface function[7], allows the controller to request copy of any packet/inject new ones(including the 3GPP CP and UP data that are being processed from the O-DU and O-CU) and, enforce policies over the E2 nodes. This connection facilitates the optimization of near-real-time functionalities such as network slicing, QoS management, and monitoring, among others. These functionalities are being handled by software components known as "xApps." xApps are hosted within the nRT RIC platform and utilize the trained models available in the nRT RIC to fulfill their tasks. They have access to the nRT RIC database, which stores the information gathered from the E2 nodes(ORAN Central Unit (O-CU)/O-DU). The nRT RIC also provides a communication framework that enables RAN elements to subscribe to the xApps, and their direct configuration by them. If multiple xApps control the same component, the nRT RIC provides controls to avoid conflicts and to ensure an orchestrated management.

On the other hand, the non-Near-Real-Time RAN Intelligent Controller is responsible for improving non-real-time functionalities within the O-RAN architecture. It has access to the data SMO DB, which it may use for ML model training, policy management, configuration management, and other functionalities. The non-RT RIC communicates with the nRT RIC through the A1 interface, providing any necessary updates or decisions related to policy implementation and management or requesting feedback. Similarly to the nRT RIC, the non-RT RIC hosts the "rApps" that are responsible for performing the non-real-time functions.

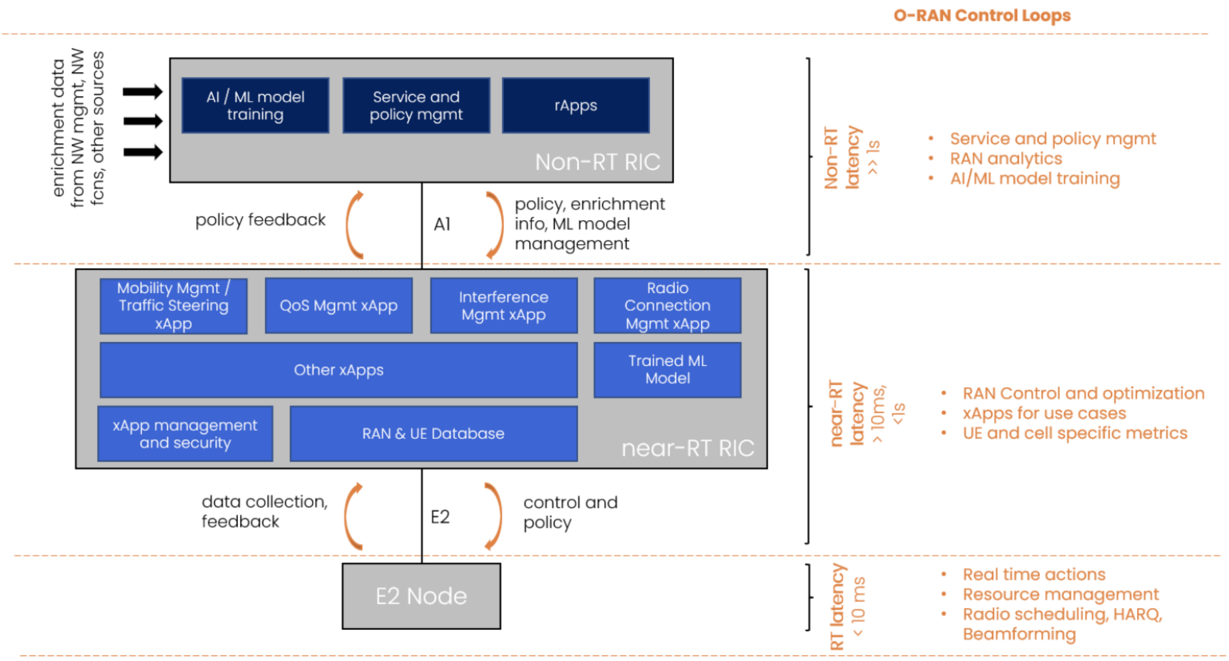

O-RAN Control Loops
enrichment data from NW mgmt, NW fcns, other sources
AI / ML model training
Service and policy mgmt
rApps
Non-RT RIC
policy feedback
A1
policy, enrichment info, ML model management
Non-RT latency >> 1s
• Service and policy mgmt
• RAN analytics
• AI/ML model training
Mobility Mgmt / Traffic Steering xApp
QoS Mgmt xApp
Interference Mgmt xApp
Radio Connection Mgmt xApp
Other xApps
Trained ML Model
xApp management and security
RAN & UE Database
near-RT RIC
near-RT latency > 10ms, < 1s
• RAN Control and optimization
• xApps for use cases
• UE and cell specific metrics
data collection, feedback
E2
control and policy
E2 Node
RT latency < 10 ms
• Real time actions
• Resource management
• Radio scheduling, HARQ, Beamforming

Figure 10: Intelligence in O-RAN[21]

Fig.10 illustrates an example of the two controllers hosting multiple Apps for various functionalities alongside the communication between the two controllers.

2.4.2 O-RAN Main Interfaces

2.4.2.1 O1

The O1 interface enables the management and orchestration of nRT RIC and the E2 nodes by the SMO. It provides support for Management Services(FCAPS) throughout the whole life-cycle of O-RAN components. O1 ensures optimal RAN performance by configuring the nodes based on Key Performance Indicators (KPIs) reports and facilitates software and file management on these nodes. O1 also allows feedback exchange, error reporting, and event notifications between the managed components and the SMO. The configuration management uses REST[7]/HTTPS[8] APIs and the Network Configuration Protocol (NETCONF) protocol. The Fault management is responsible for reporting errors and alarms that can be accessed and managed. Additionally, it monitors the RAN components by receiving Heartbeat signals, ensuring their Availability, or detecting potential failures.

2.4.2.2 O2

The O2 interface, similarly to O1, facilitates the management of the O-Cloud by the SMO. O2, apart from its ability to directly manage the O-Cloud itself, can also configure and manage the virtual components hosted within it, including OS, the RAN components themselves, among others. It can also be used to deploy new elements in the O-Cloud. Some services exposed to the SMO via the O2 include, among others:

- Software management
- O-Cloud Configuration
- Support for FCAPS functionalities
- Resources provisioning
- Integration of software instances or hardware components

Through the O2 interface, the SMO can efficiently administer, orchestrate and control the O-Cloud, and to an extent, the whole RAN architecture.

2.4.2.3 A1

The A1 interface serves as a connection between the two intelligent units within the O-RAN architecture. It facilitates the control of the nRT RIC by the non-RT RIC. Through the A1 interface, the non-RT RIC can manage policies of the nRT RIC by adding, deleting, or manipulating them. However, enforcing the policies is a nRT RIC's responsibility. Additionally, the non-RT RIC can provide enrichment data to the nRT RIC, giving it a broader perspective of the network's State. Moreover, since ML model training takes place within the non-RT RIC unit, the A1 interface also performs the management of ML models within the nRT RIC unit. The A1 interface implements the A1AP(A1 Application Protocol), enabling policy deployment and management using REST APIs/HTTP.

2.4.2.4 E2

E2 serves as the link between the nRT RIC and the E2 nodes. Through this interface, the nRT RIC can manage and configure the E2 nodes in near-real-time to enhance RAN functionalities. Additionally, the E2 interface facilitates the collection of data and feedback from the E2 nodes. This interface comprises E2 Application Protocol(E2AP) and E2 Service Model(E2SM). E2AP handles communication between the E2 nodes and the

[7] Representational State Transfer

[8] Hypertext Transfer Protocol Secure

nRT RIC, allowing for service updates. On the other hand, E2SM provides the necessary mechanisms for the nRT RIC to configure the nodes, manage policies, and collect data and metrics from the E2 nodes.

2.4.2.5 R1

The R1 interface serves as an internal interface of the non-RT RIC and connects it to the different rApps hosted within the framework. It enables the controller to manage the rApps through this interface effectively. Conversely, the reps can access the services exposed by the R1 interface, which includes A1 services and access to the SMO DB. The access to the different services is once more achieved through different open APIs. The interface can be seen in Fig.11, connecting the directly the 2 RICs.

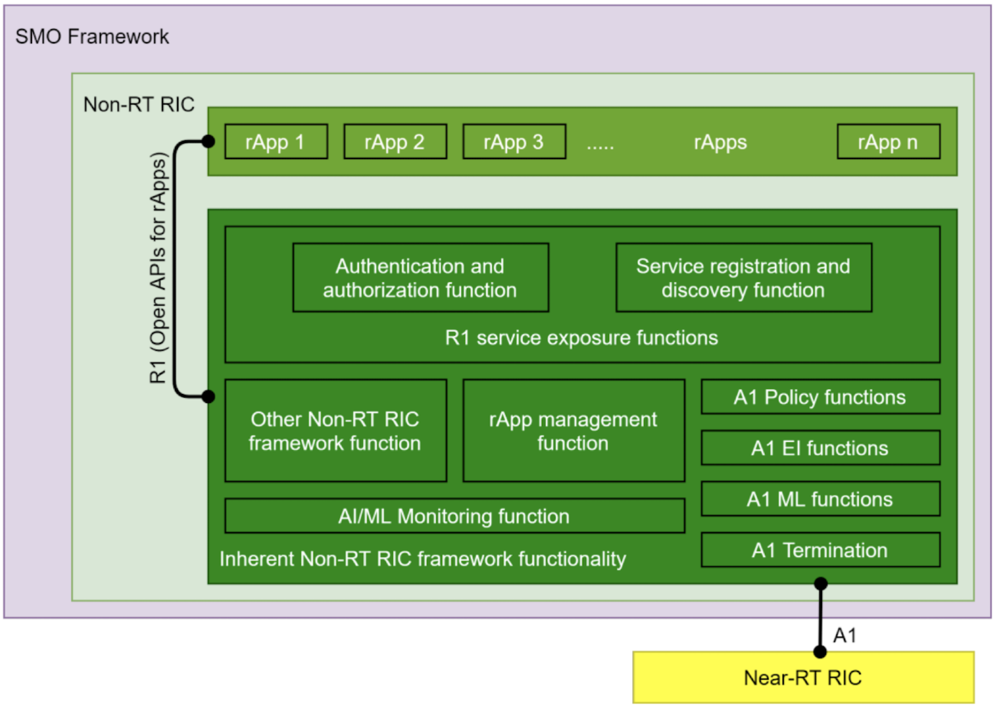

SMO Framework
Non-RT RIC
rApp 1
rApp 2
rApp 3
.....
rApps
rApp n
R1 (Open APIs for rApps)
Authentication and authorization function
Service registration and discovery function
R1 service exposure functions
Other Non-RT RIC framework function
rApp management function
A1 Policy functions
A1 EI functions
A1 ML functions
AI/ML Monitoring function
A1 Termination
Inherent Non-RT RIC framework functionality
A1
Near-RT RIC

Figure 11: R1 Interface[35]

2.4.2.6 Open Fronthaul

Open Fronthaul is the interface that connects the O-CU and the O-DU. The 7.2x split, implemented by O-RAN Alliance and was briefly explained earlier(Fig.9), achieves a balance between openness, simplicity, and performance for the O-RU. This interface is split into four different Planes:

1. U-Plane: It is responsible for transmitting UP and CP data, data compression and precoding.
2. C-Plane: It is responsible for transmitting control data related to beamforming, spectrum sharing, and UL[9]/DL[10] related information such as slots and frequencies.
3. S-Plane: It is responsible for synchronising the O-RU with the O-DU.
4. M-Plane: It enables the SMO to provide FCAPS support to the O-RU. It also supports file and software management.

Additional information about the Fronthaul will be provided in subsequent sections of this thesis.

[9] Up-Link

[10] Down-Link

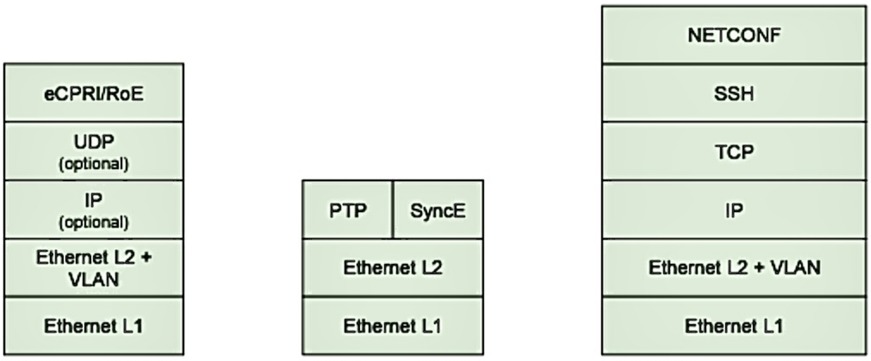


Figure 12: Open Fronthaul Protocols[65]

Each Plane requires different protocols apart from the CU-Plane, which uses the same stack. These protocols are depicted in Fig.12.

2.5 Security Protocols

This section provides an overview of the essential security protocols discussed in the risk analysis. While the technical details of these protocols are important, it is worth noting that the recommended versions specified in the protocols, such as TLS 1.2, SSHv2 and Oauth 2.0, are considered secure. For the purpose of this thesis, the focus is on understanding the role and significance of these protocols in ensuring the security of the network, rather than diving into their specific technical details. Therefore We examine these protocols in accordance with the security values they offer:

- Integrity: Ensures that the data have not been modified during the transmission. This can be achieved with the use of Digital Signatures or Message Authentication Codes(MACs).
- Confidentiality: Ensures that authorized parties cannot read the data under transmission. Strong encryption is enough to provide Confidentiality.
- Authentication: Ensures that the parties involved in the communication are who they claim to be. Asymmetric cryptography with Certificates is used to ensure authenticity. The distribution of Symmetric Keys is also an option but rarely used.
- Authorisation: Ensures that only authorized parties are granted access to specific data and services intended for their use. Credentials and Certificates can be used to match authorization access and privileges to the Users.
- Replay Protection(RP): Ensures That intercepted packets cannot be re-sent to their destination in the future and get accepted. This is achieved by adding sequence numbers in the packets before the encryption/Integrity protection.

2.5.1 TLS

TLS is a cryptographic protocol that ensures End-to-End secure communication between clients and servers over a network. It ensures data Confidentiality, Integrity, RP, and one-side authentication. It operates between the application and the transport layer. The TLS handshake establishes a secure connection by exchanging messages between the client and server, negotiating parameters, and generating session keys. During the handshake, the server authenticates himself to the client. Once the handshake is complete, the two parties establish a shared key to encrypt and provide Integrity protection through the use of MACs, to the data. The most widely used version of TLS is v1.2, as it is considered to be secure. However, the newest version, v1.3, provides improvements such as support for more robust encryption algorithms and reduced handshake time. TLS is the primary protocol used to secure communication between clients and web servers.

2.5.1.1 mTLS

Mutual Transport Layer Security Protocol (mTLS) is an enhanced version of TLS that enforces the authentication of both the server and the client, ensuring that the parties verify each other's identities using public-key cryptography and certificates.

2.5.2 IPSec

Internet Protocol Security (IPsec) is a network layer protocol that provides Confidentiality, Integrity, RP and authentication of the two ends in IP communications. IPsec utilizes the Internet Key Exchange (IKE) protocol. During the IKE phases, the endpoints authenticate each other, establish a secure channel, and exchange encryption keys or credentials. On a high level, IPSec and TLS offer the same protection, but they operate in different layers. The IKE protocol establishes the communication slightly faster than the TLS handshake but TLS offers more benefits when it comes to HTTP security as it is explained in[43].

IPsec supports two modes of operation: transport mode(encrypting only the payload) or tunnel mode (encapsulating the entire IP packet). IPsec is the main protocol used in VPNs.

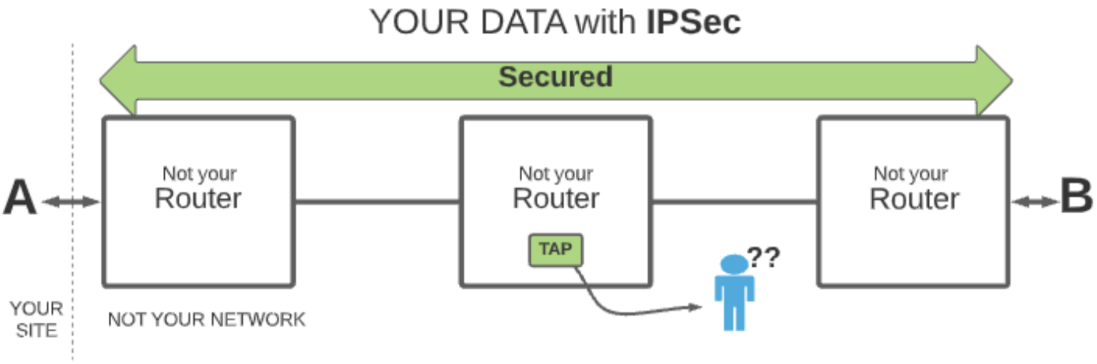


Figure 13: IPSec Point-to-Point Protection[29]

2.5.3 IEEE 802.1x

The 802.1X protocol is a widely adopted port-based authentication standard that ensures only authenticated access to Networks. It operates at the Link Layer and it employs the Extensible Authentication Protocol (EAP) for the authentication process. The protocol involves three key entities: the supplicant (device seeking network access), the switch or access point, and the authentication server. When a device connects, it undergoes an authentication procedure where its identity is validated by the authentication server. Based on the authentication result, network access is either granted or denied.

2.5.4 MACsec

Media Access Control Security (MACsec) is a security protocol that ensures data Confidentiality, RP, and Integrity and provides authentication at the data link layer. In other words, in contrast with IPSec and TLS, MACsec is a Point-to-Point protocol used to secure LAN(Local Area Networks) segments. Its hardware implementation enables faster encryption speeds than TLS and IPSec as can seen in Fig.15, which shows that IPsec supports encryption speeds up to 40Gbps while IPSec supports speeds over 100Gbps. The authentication offered by this MACsec is a byproduct of the usage of the protocol 802.1x that prevents unauthorized access to the interface. The Point-to-Point protection offered by MACsec, is shown in Fig.14, while the End-to-End of IPSec[11] in Fig.13. As can be seen, an End-to-End protection, protects the data from any malicious intermediary node, while Point-to-Point does not, as the data needs to get decrypted before they can be forwarded to the next router.

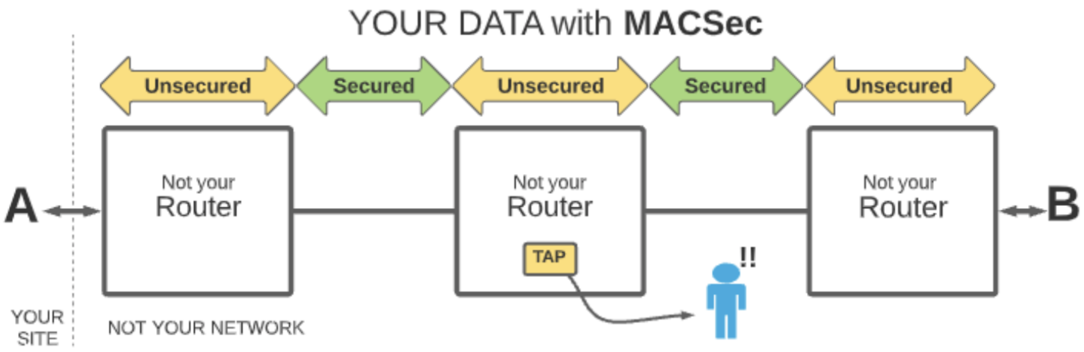


Figure 14: MACsec Point-to-Point Protection[29]

2.5.5 OAuth 2.0

Open Authorisation (Oauth) 2.0 is an authorization protocol that enables Users to grant secure access to their resources without sharing their credentials. It involves a User authorizing a client application that obtains an access token from an authorization server. This token allows the client application to access protected resources or services on behalf of the User. OAuth 2.0 focuses on authorization and access delegation, ensuring Users maintain control over their data/offered services while granting permissions to third-party applications.

2.5.6 NACM

The NACM is a component of the NETCONF protocol used to configure network elements. NACM operates by defining roles and access control rules. Roles determine the level of access for Users or groups, while access control rules specify permitted or denied operations based on those roles. When a User attempts an operation, NACM evaluates the rules and permits or denies the action accordingly, ensuring authorization.

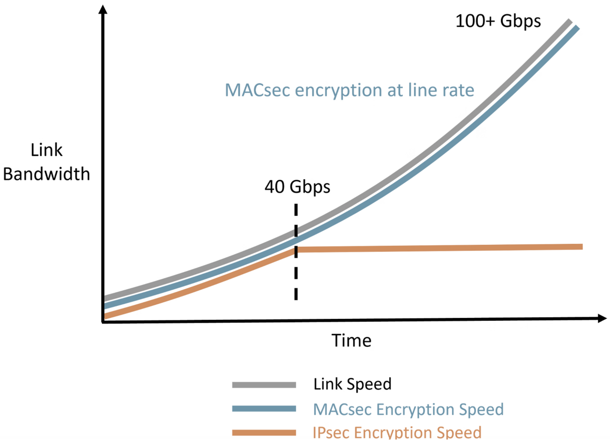


Figure 15: MACsec vs IPsec Encryption Speed[65]

[11] TLS is similar to IPSec, providing End-to-End protection but between two Application Layers

3 Security Of O-RAN

This chapter aims to analyze the security of the O-RAN architecture, which has been under heavy criticism for its security since its conception. In February 2022, the BSI published a comprehensive analysis([53]) of the architecture's security, mainly based on the first release of security specifications and threat modeling report released by O-RAN in June 2021. This analysis covered almost every component and aspect of the architecture. The analysis concluded that the architecture contained multiple risks and was not being developed according to the *"Security by default"* principle at the time. This principle maintains that *"Systems should be as secured as possible, by their default configurations"* or, in other words, *"Security out of the box"*.

Other analyses conducted by different organizations, including the European Union Agency for Cybersecurity (ENISA)[22], also identified flaws and vulnerabilities in different elements of O-RAN, further highlighting the need for security-related enhancements[3][40]. Despite several revisions to the architecture's specifications and requirements by O-RAN Alliance and its members, the security of O-RAN is still considered a major drawback, and its standardization may be threatened in the future. Therefore, keeping track of O-RAN's security is crucial to ensure its endurance, survival, and standardization. The last exhaustive analysis was conducted over a year ago based on the first O-RAN specifications. Hence, a new risk analysis is needed to evaluate the progress made to secure O-RAN as the first O-RAN-compliant solutions hitting the market.

This chapter exposes the findings of the BSI security analysis on O-RAN and its methodology. Furthermore, we presents a new updated version based on the fifth revision of the specifications. We aim to record changes, identify new threats, and re-evaluate the overall O-RAN security state.

3.1 Risk Analysis by The German Federal Office Of Information Security

This section presents the findings of BSI security analysis on ORAN, including the authors' methodology. As mentioned before, this analysis was conducted in 2022 and was based on the first security specifications of O-RAN released in 2021. We strongly believe this is the most complete/inclusive analysis conducted under the ORAN concept. The fact that every other similar analysis referencing this one further strengthens our position.

3.1.1 Methodology and Scope

This subsection defines the extent of the analysis(scope) and expounds upon the selected approach concerning identifying potential risks and the attacker models.

3.1.1.1 Scope

The study focuses exclusively on the security risks associated with the O-RAN Alliance implementation of the ORAN. The analysis only considers only the RAN component, and assumes it is connected to a CN and (at least) one UE. Following the same principle, the study only picks out and examines threats\vulnerabilities specific to 3GPP or O-RAN and mentions generic IT risks only in a few instances. The analysis does not factor in additional security measures that network providers or RAN Operators may implement to reduce risk.

3.1.1.2 Assessment's Steps

The methodology used by the authors is based on a plethora of standards related to risk identification and evaluation, namely ISO 27005[31], ISO 31000[32], IEC 31010[33] and BSI-Standard 200-3[17], and involves the following steps:

1. *Determination of the attacker to be considered*

2. *Determination of sensitive assets*
3. *Determination of the criticality of failures to meet protection goals concerning the assets (i.e., the damage that could occur)*
4. *Determination of threats to protection goals and assets*
5. *Identification and assessment of vulnerabilities in relation to the threats determined*
6. *Determination of risk on the basis of the vulnerabilities and the potential damage*

The procedure is presented as in [35],page 35.
The study defines *risk* as the *"effect of uncertainty on objectives"*[32], where the effect can be interpreted only as harm. Uncertainty refers to the probability of events occurring that would lead to that harm. The standard formula of likelihood multiplied by the impact is used to quantify the level of risk. Here, it is essential to mention that the definition of risk differentiates this detailed analysis from the corresponding one conducted by O-RAN[9], as that document evaluates a risk only based on its impact.

3.1.1.3 Protection Goals

The protection objectives established by the authors can be described as an extended rendition of the Confidentiality-Integrity-Availability (CIA) model, which serves as a guiding principle in information security. This augmented model includes Accountability and Privacy as additional attributes. A concise explanation of each attribute is provided below:

- ***Confidentiality:*** Ensures that the data/information in the system can be accessed only by authorized parties.
- ***Integrity:*** Ensures that the data/information in the system is protected from any improper/unauthorized modification or destruction.
- ***Availability:*** Ensures the data/information/services are available whenever needed.
- ***Accountability:*** Ensures that every action performed by a component in the system can be linked back to that component.
- ***Privacy**:* Ensures that metadata in the system cannot be used to violate the User's right to anonymity, unlinkability, and unobservability.

Disclaimer: *The authors declare that no measures implemented at the application level to ensure Integrity, Accountability, and Confidentiality have been considered. Moreover, the authors' focus is on the quality of the services offered with regard to Availability. Therefore, an attack that compromises the quality of a system's service is deemed to be an attack on the system's Availability..*

3.1.1.4 Attacker Models

It is crucial to consider potential attackers and their abilities before conducting a risk analysis. The BSI study identifies and examines five different attacker models. These models are explained in the following list:

- **Outsider:** The attacker, who has no inside access to the system or its services, can attack the system using the defined interfaces of O-RAN or 3GPP. The interface, which is under risk analysis, is assumed to be entirely controlled by the attacker, meaning that they can monitor, intercept, or modify any data that is transmitted over the interface.

- **User:** An attacker who is also a User of the 5G network. He uses the services of the 5G system by utilizing at least one UE with valid credentials. This attacker possesses all of the capabilities of the *Outsider*.
- **Cloud Operator:** The attacker who has control over the cloud infrastructure that hosts the different ORAN components. This attacker performs his attacks either by exploiting the SW part or HW part of the component under the risk assessment. He also has all of *User's* capabilities.
- **Insider:** This attacker controls one component defined by O-RAN or 3GPP. The authors assume that the component under investigation is connected to the interfaces it terminates, according to the O-RAN architecture. This attacker is also an extension of the *User*.
- **RAN Operator**: This attacker controls the entirety of RAN. By definition, he is the most powerful attacker.

All potential attackers share certain assumptions, including possessing significant but limited resources (such as computing power and financial support), which may include State-sponsored or resourceful criminals. Additionally, attackers are assumed to be active and willing to manipulate data beyond their controlled system parts. It is also assumed that the currently implemented cryptographic algorithms and protocols are secure and that attackers have no prior knowledge of cryptographic secrets, such as cryptographic keys. The hierarchy of the attacker models is depicted in Fig.16.

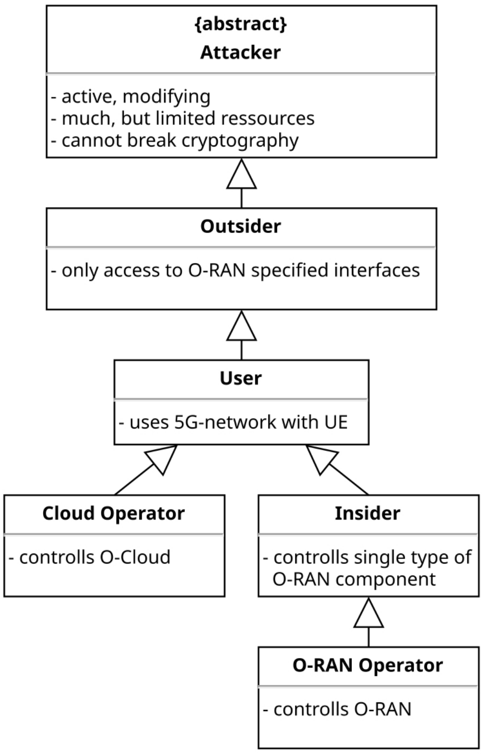

{abstract}
Attacker
- active, modifying
- much, but limited ressources
- cannot break cryptography
Outsider
- only access to O-RAN specified interfaces
User
- uses 5G-network with UE
Cloud Operator
- controlls O-Cloud
Insider
- controlls single type of O-RAN component
O-RAN Operator
- controlls O-RAN

Figure 16: Hierarchical Representation Of The Attacker Models[35]

3.1.1.5 Security Perspectives

Incorporating different viewpoints on security by various stakeholders constitutes an additional aspect of the author's security analysis. This inclusion facilitates a nuanced examination of the risks associated with RAN, given that distinct security requirements and interests are inherent to each stakeholder. The analysis points out three interested parties and their respective standpoints. These parties are The End-User, the

Government/State, and the Network Operator. The End-User, who typically uses at least one UE to access the 5G network and services, is primarily interested in protecting the UP data. Any potential failure to meet the requirements mentioned in Sec.3.1.1.3 compromises mainly the End-User's Privacy and may have severe consequences. From the Network Operator's viewpoint, the most valuable asset is the CP data, as this data is responsible for the smooth and uninterrupted functionality of the Operator's network. Compromised CP data has the potential to interfere with the CN functionalities or disrupt the Availability of the offered services. The Government's view is more complex as its concerns are split equally between the two planes. 5G serves as the communication infrastructure for billions of people worldwide, and its significance is expected to skyrocket in the following years as smart cities and smart grids become a reality. These concepts depend on data transmitted on both planes, and their smooth operation is vital. Availability is the most significant security aspect.

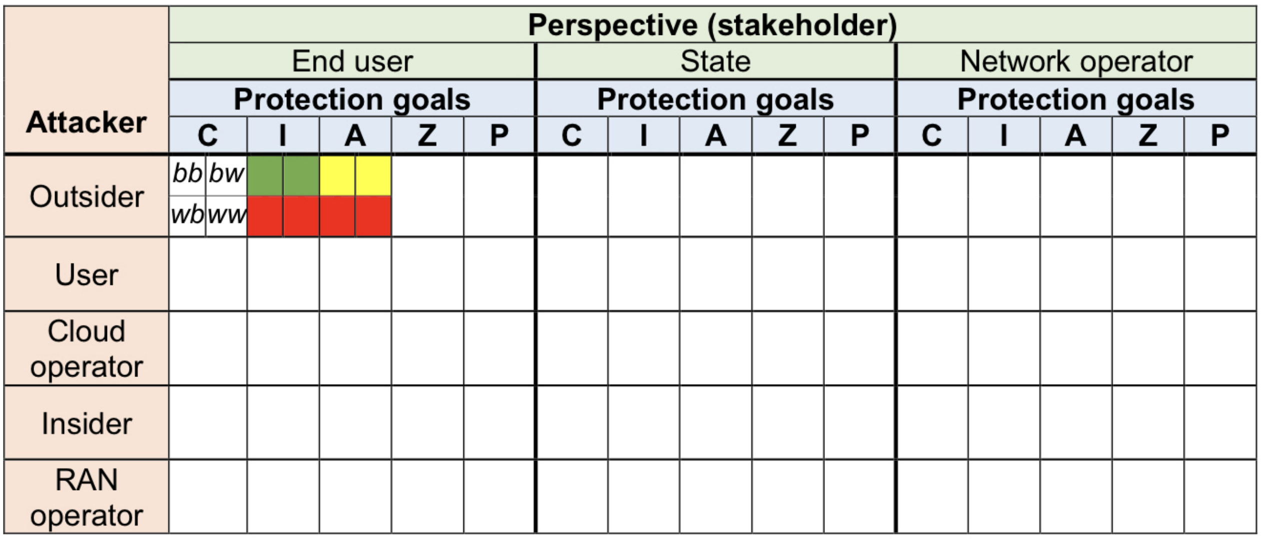
3.1.1.6 Risk Analysis Methodology

The analysis is based on the security specifications of the first release of O-RAN, as explained in Sec.3. Since O-RAN is an extension of NG-RAN, the security measures outlined by the 3GPP specifications[1] are also taken into account. Both specifications consist of mandatory and optional security mechanisms. To address this, the authors establish two typical scenarios for each specification: the Worst Case scenario, in which only the mandatory requirements are implemented, and the Best Case scenario, in which both mandatory and optional requirements are implemented. This approach allows for the investigation of the most extreme possible cases. Risk can be calculated using the formula given in Sec.3.1.1.4, namely $Risk = Impact * Likelihood$. However, in the risk analysis, the impact is not included in the equation, as it is believed to be equally significant for at least one of the stakeholders in every case. To account for this, three possible levels are defined for the likelihood: *High, Medium, and Low.* If an adversary can exploit a vulnerability with little effort, the associated risk is classified as a "High level" risk. In the case that the exploitation requires a significant amount of effort, then the risk is categorized as "Medium level". In both cases, the attacker has the necessary skills and resources to deploy the attack successfully. On the other hand, "Low level" risk is related to excessive effort and necessitates capabilities that the attacker does not possess to exploit. The authors support that the likelihood cannot be mathematically proven, and is often based on a subjective-empirical evaluation.

The presented risk analysis aims to evaluate the probability of a breach for different attackers, perspectives, and protection goals, as discussed in the previous sections. To achieve that, the authors examine four possible scenarios for each interface in the architecture. These scenarios are defined as:

1. Absolute Best Case Scenario (***bb***): Both O-RAN and 3GPP Optional security requirements are implemented
2. Absolute Worst Base Scenario (***ww***): None of the optional security requirements are implemented
3. O-RAN Best Case Scenario (***bw***): Only the O-RAN optional requirements are implemented
4. 3GPP Best Case Scenario (***wb***): Only the 3GPP optional requirements are implemented

Mandatory security controls are assumed to be in place in every scenario. After the risk analysis of each element, an overall security-review of ORAN is evaluated. The Fig.17 presents the *"Scheme for the overview of the risk assessment. The cells in the table reflect the likelihood of occurrence of a breach of the protection goal with regard to a given attacker and a given perspective (stakeholder) in the best case (b) or worst case (w). Green means low; yellow medium; and red a high likelihood of occurrence, while a white field means that* *no statement is possible at present. The abbreviations for the protection goals represent Confidentiality (C), Integrity (I), Availability (A), Accountability (Z) and Privacy (P)"*[35].



Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Outsider	bb bw	🟩🟩	🟨🟨												
	wb ww	🟥🟥	🟥🟥												
User															
Cloud operator															
Insider															
RAN operator															

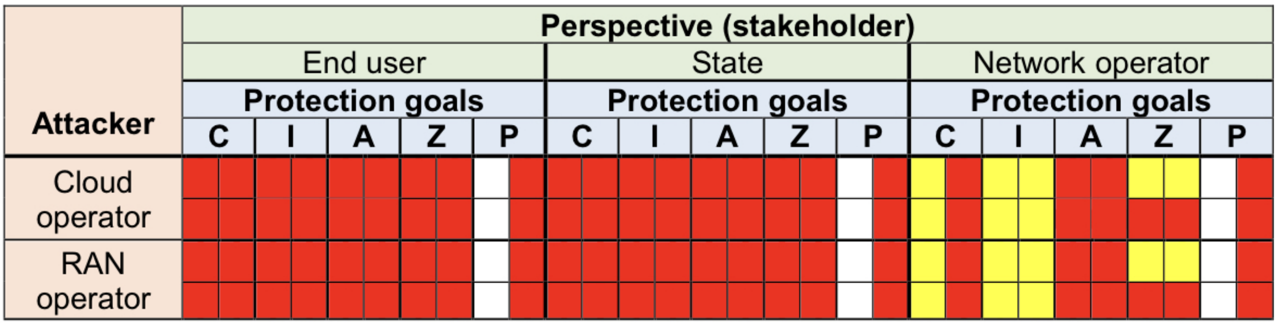
Figure 17: Scheme for the Overview of the Risk Assessment[35]

3.1.2 The BSI Risk Analysis

This section presents the risk analysis findings based on previously explained methodology. For each attacker, an atomic analysis of each element (interface or entity) is carried out before an all-inclusive evaluation of the architecture's security is calculated by combining the individual results.

3.1.2.1 The Special Case of Cloud/RAN Operators

The authors explain that risks associated with the Cloud/RAN Operators are equivalent to the architecture as a whole, before analyzing the individual components. This is because O-RAN Alliance does not define any protection measures against potential malicious Cloud Operators as they are assumed to be trusted, among administrators and integrators. Therefore, implementing O-RAN security requirements do not affect Cloud Operators. Similarly, RAN Operators have control over the O-RAN security safeguards and thus they are not affected by them.



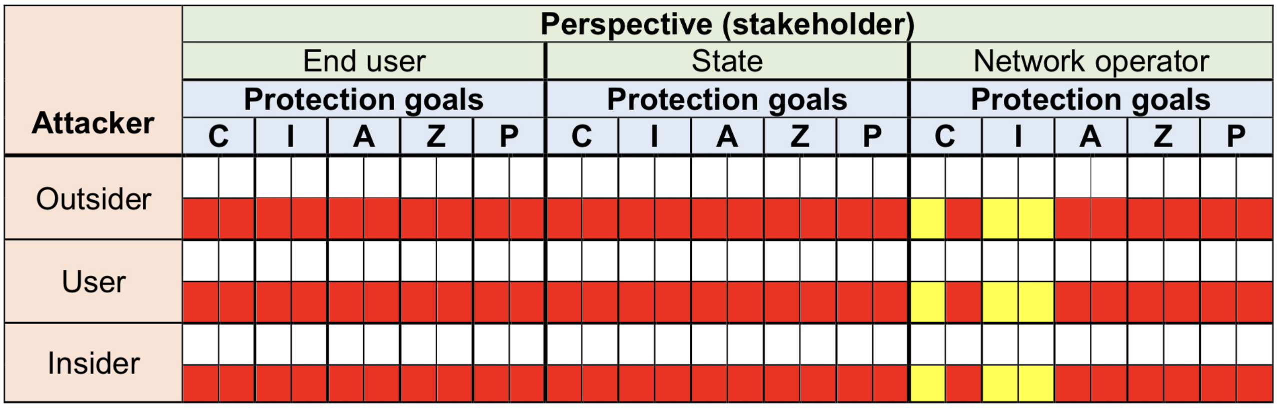
Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Cloud operator	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟨🟨	⬜🟥
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥
RAN operator	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟨🟨	⬜🟥
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥

Figure 18: Risk Assessment for RAN and Cloud Operators for the whole architecture[35]

Consequently, only the ***bb*** and ***ww*** scenarios can be evaluated. In the ***ww*** scenario, none of the security measures defined by 3GPP or O-RAN are utilized, leaving all protection goals vulnerable to security breaches due to unrestricted access to all processed data by attackers. The Integrity of the CP is the only area where protection remains intact, as is the only mandatory control in place (Fig.7). However, control O-RAN data exchanged between system components for synchronization, configuration, etc., remain unprotected, resulting in an overall medium level of risk from the Operator's view. In the ***bb*** scenario, encryption/Integrity protection is applied to UP data exchanged between the UE and the CU in the ***bb***. However, UP is protected between the UE and the RAN, and thus, the encryption keys are accessible by these attackers, posing a high level of risk to all protection goals, a critical concern for both the End-User and the State, as outlined in Sec.3.1.1.5. In contrast, CP is End-to-End protected between the UE and the CN, making it secure. Nevertheless, O-RAN control data are still exposed, leading to an overall medium risk level.

3.1.2.2 O-Cloud

The authors begin their assessment by scrutinizing the O-Cloud, the backbone infrastructure hosting the ORAN functions. If an attacker manages to exploit the O-Cloud, he will gain complete control over the RAN. The O-Cloud's lack of mandatory security requirements, except for isolation mechanisms, which are rendered ineffective without authentication and authorization, makes it highly vulnerable to attacks. Hence, the analysis focuses primarily on the ***ww*** scenario. Without mandatory security controls, the O-Cloud is highly vulnerable to all potential attackers in the ***ww*** scenario, who could exploit it to take control of the entire RAN. In the ***wb*** scenario, the risk is assessed as medium due to the absence of mandatory security measures for O-RAN control data, although control data between the UE and the AMF are protected for Integrity and Confidentiality.

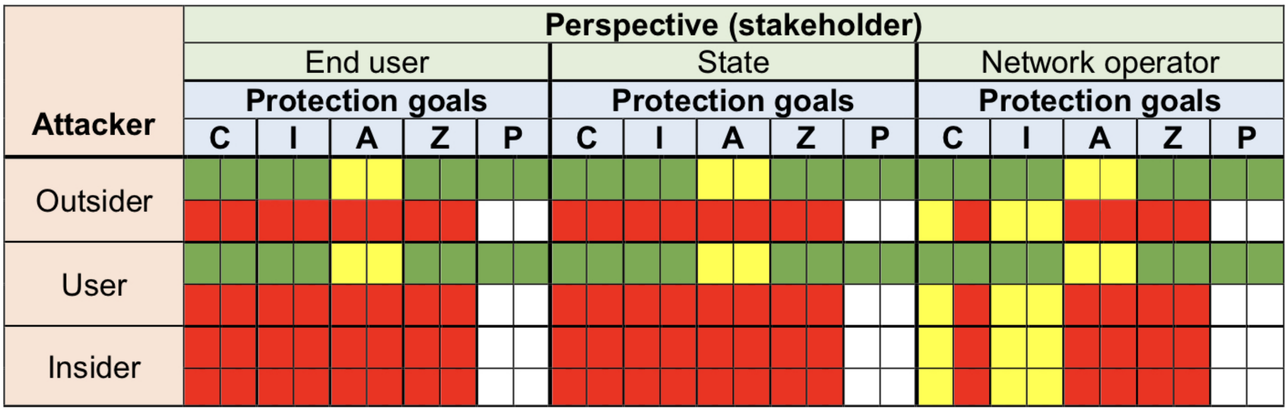


Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider																														
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟥
User																														
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟥
Insider																														
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	🟥	🟥

Figure 19: Risk Assessment of O-Cloud[35]

3.1.2.3 O2 Interface

According to the analysis, O2 is one of the most powerful interfaces, as it is used for the configuration of the O-Cloud by the SMO, enabling the management of the execution environment and facilitating the deployment of various components within the architecture. Therefore, if exploited, the O2 interface can grant an attacker complete control over the O-Cloud, which extends to the control of the whole architecture. At that time, conducting a comprehensive risk assessment was challenging because the requirements were only expressed in relation to the services provided over the O2 interface. The only mandatory security control for O2 is the support of TLS version ≥ v1.2. Although O-RAN states that the communication over the O2 interface is secured with TLS, the authors argue that its usage is not mandatory, only its support. The authors recommend implementing privileges and access control. For the ***ww*** scenario, the risk is high for every attacker and protection goal, as anyone can access the unprotected interface. The Integrity protection provided by the mandatory 3GPP controls offers the only security protection. Therefore, the risk is assessed medium regarding the Integrity from the Operator's view, as O-RAN controls remain unprotected. The ***wb*** is similar to the ***ww*** scenario. However, the control data between the AMF and UE are also encrypted, resulting in a medium risk from the Network Operator's perspective regarding Integrity. For the ***bb*** and ***bw*** scenarios, both planes are partially protected by implementing the optional security controls provided by O-RAN. Only the Insider attacker is linked to high risk as TLS only protects the interface from external threats. Availability attacks are still possible from Outsiders, and the risk is assessed as medium. The only difference between the two scenarios is the lack of encryption for the CP data between the UE and AMF, resulting in a high risk, in terms of Confidentiality.



Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Outsider	🟩🟩	🟩🟩	🟨🟨	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟨🟨	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟨🟨	🟩🟩	🟩🟩
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜⬜
User	🟩🟩	🟩🟩	🟨🟨	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟨🟨	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟨🟨	🟩🟩	🟩🟩
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜⬜
Insider	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜⬜
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜⬜

Figure 20: Risk Assessment of O2[35]

3.1.2.4 O1 Interface

The O1 interface plays a vital role in connecting the SMO with the nRT RIC, O-DU, and O-CU, allowing for the configuration of every component except from the SMO itself. The authors note that the O1 interface is powerful and requires robust security measures. Two different security specifications were provided for the O2 interface, one covering O1 in general, and the other providing a detailed analysis of the connection between the O-DU and SMO using the O1 interface, including security requirements and safeguards. Therefore, the authors present two distinct security analyses for the O1 interface.

A. General O1 Interface

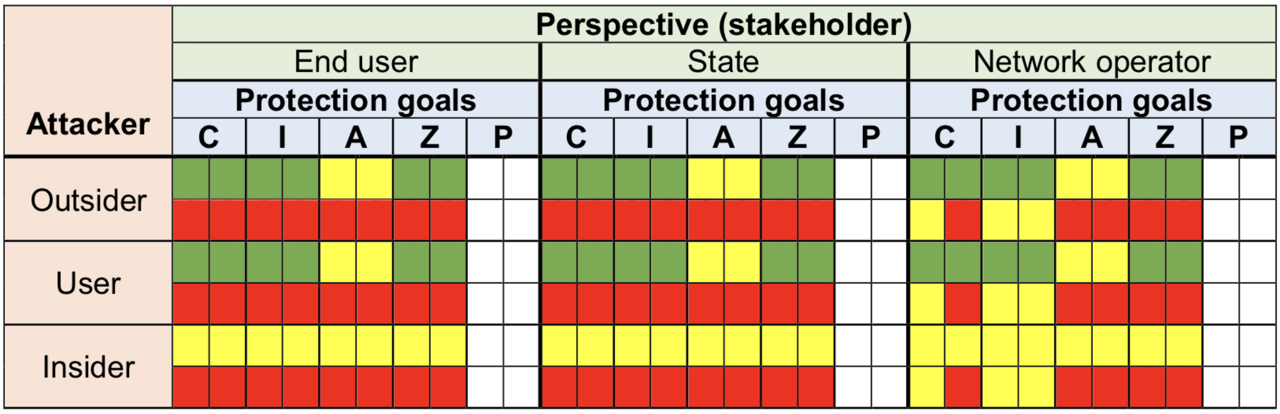
The general requirements specification includes optional security controls, such as using Secure Shell (SSH), TLS, and enforcing the least privilege principle for authorization control. However, there is a contradiction between the security requirements document and the general requirements specification, as the former document mandates using TLS 1.2 to secure the interface. The authors choose to consider the worst-case scenario, in which no mandatory security controls exist. At this point, the authors explain that SSH is fundamentally more dangerous than TLS, as the former protocol allows the execution of any program, while the latter does not. As the NETCONF protocol runs over SSH/TLS, additional security controls are necessary to ensure that only authorized NETCONF programs are executed. To ensure the least-privilege access control, O-RAN recommends using the Network Access Control Model (NACM). NACM shall include support for five predefined groups to restrict the NETCONF protocol powers based on the group(Tab.1).

Table 1: NACM Groups

Group	Rights
NACM management	Management of the NACM objects and groups (rights management)
User Management	Management Of Users and Roles on the O1 components
Network Management	Read/Write/ operations on the NETCONF Database but not on the NACM objects
Network Monitoring	Read configuration data but not the NACM objects
Software Management	Install/Update software

In the ***ww*** scenario, all risks are evaluated as high, except for the Integrity of the CP data between the UE and

AMF, which is protected from the Operator's perspective. However, the O-RAN control data is not protected, resulting in a medium risk. The ***wb*** scenario offers Integrity and Confidentiality protection for the CP data. The O-RAN control data remains unprotected, resulting in a medium risk from the Network Operator's perspective. In both ***ww*** and ***wb*** scenarios, an attacker may access the encryption keys from O1, allowing them to access the UP data potentially. In the ***bb*** scenario, TLS provides protection against Outsiders, TLS and NACM provides access control. However, Availability attacks are still possible, such as desynchronizing the system components resulting in a medium risk. In the case of an Insider attacker, he may have access to cryptographic keys, leading to a medium risk for the Integrity/Accountability and Confidentiality from the User/State perspective. The same holds for the Operator, as a breach of O1 may have catastrophic consequences. The ***bw*** scenario is identical to the ***bb*** scenario regarding O1 protection. The risk assessment for an Insider attacker remains the same in both scenarios.



Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Outsider	🟩🟩	🟩🟩	🟨🟨	🟩🟩		🟩🟩	🟩🟩	🟨🟨	🟩🟩		🟩🟩	🟩🟩	🟨🟨	🟩🟩	
	🟥🟥	🟥🟥	🟥🟥	🟥🟥		🟥🟥	🟥🟥	🟥🟥	🟥🟥		🟨🟥	🟨🟨	🟥🟥	🟥🟥	
User	🟩🟩	🟩🟩	🟨🟨	🟩🟩		🟩🟩	🟩🟩	🟨🟨	🟩🟩		🟩🟩	🟩🟩	🟨🟨	🟩🟩	
	🟥🟥	🟥🟥	🟥🟥	🟥🟥		🟥🟥	🟥🟥	🟥🟥	🟥🟥		🟨🟥	🟨🟨	🟥🟥	🟥🟥	
Insider	🟨🟨	🟨🟨	🟨🟨	🟨🟨		🟨🟨	🟨🟨	🟨🟨	🟨🟨		🟨🟨	🟨🟨	🟨🟨	🟨🟨	
	🟥🟥	🟥🟥	🟥🟥	🟥🟥		🟥🟥	🟥🟥	🟥🟥	🟥🟥		🟨🟥	🟨🟨	🟥🟥	🟥🟥	

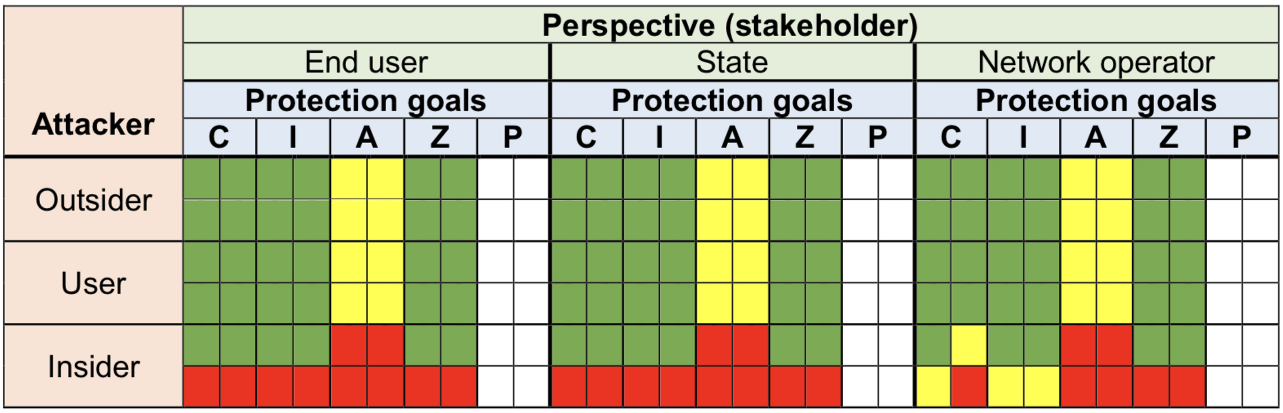
Figure 21: Risk Assessment of O1 (General) [35]

B. O1 Interface: SMO to O-DU Requirements

Communication between SMO and O-DU requires special consideration as TLS is mandatory for authentication of O-DUs, along with the implementation of least privilege access control using NACM. Although the interface is secured even in the ***ww*** scenario, Availability attacks are still possible, as explained in the ***bb*** case of the general O1 analysis. There is a correlation between the current analysis and the general O1 analysis, since all optional O-RAN security controls are now mandatory,:

- ***ww***(SMO-(O-DU_O1)) = ***bw***(SMO-(O-DU_O1)) = ***bw***(General_O1)
- ***wb***(SMO-(O-DU_O1)) = ***bb***(SMO-(O-DU_O1)) = ***bb***(General_O1)

The equations above apply to all protection goals but only when an Outsider or User attacks. In the case of an Insider attacker who controls the O-DU, the ***ww*** scenario presents a significant risk. An Insider attacker can compromise all protection goals for State and User stakeholders since the UP data are left unprotected, and Availability attacks can be launched by installing malicious software in the O-DU or by shutting down/turning off the entire O-DU. The installation of software depends on the attacker's privileges, but this analysis assumes the worst-case scenario. The risk is evaluated as high for all protection goals except for Integrity from the Network Operator's perspective since CP data is Integrity-protected between the UE and the AMF. In the ***wb*** scenario, the Network Operator's perspective sees an improvement in Confidentiality since CP data is now encrypted between the UE and CN, reducing the risk level from high to medium. However, in the ***bb*** scenario, the optional 3GPP controls protect Integrity, Confidentiality, and Accountability, but they fail to prevent Availability attacks on the O-DU. On the other hand, in the ***bw*** scenario, the mandatory O-RAN security controls do not require encryption of CP data, leading to a reduction in Confidentiality to medium from the Operator's perspective.



Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜
	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜
User	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜
	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	⬜	⬜
Insider	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜	🟩	🟨	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	⬜

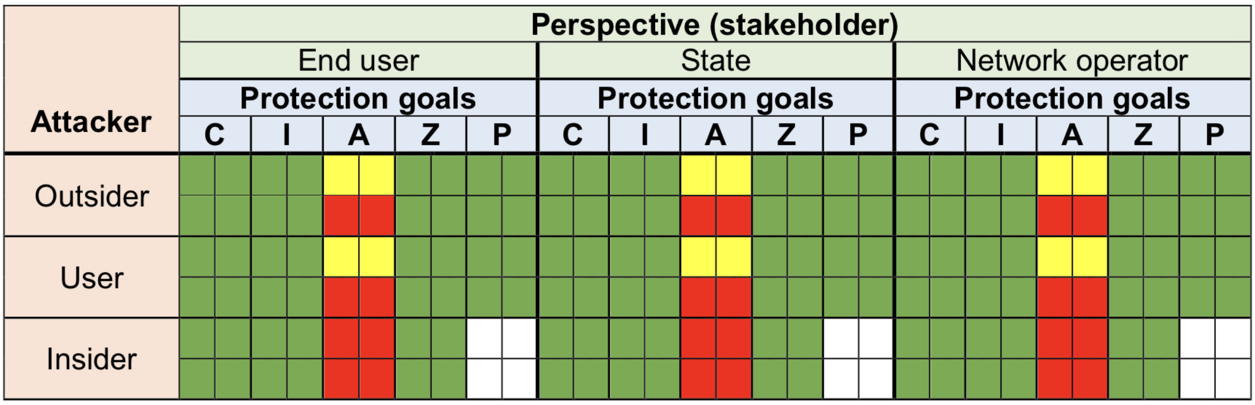
Figure 22: Risk Assessment of O1 (SMO and O-DU)[35]

3.1.2.5 Machine Learning

Machine learning is a new addition to the RAN architecture. Both controllers utilize collected data to train ML models to enhance the RAN functionalities. Ill-trained models may impact the QoS, as based on the ML models, decisions regarding policies and ran operations are generated. For this reason, the authors claim a medium risk regarding the system's Availability. Additionally, the Confidentiality of trained models is a concern, as they represent sensitive assets that should remain undisclosed. "Model stealing" attacks enable attackers to extract or restrict model parameters through clever queries or system manipulation. Furthermore, if UP or CP data is employed in model training, there is also a potential risk of breaking the Confidentiality of that data. Based on available specifications, the precise implications and security risks associated with this in O-RAN are not currently clear. According to the authors, security risks cannot be appropriately evaluated due to the lack/incompleteness of the specification. Consequently, they do not present a concrete analysis regarding the ML.

3.1.2.6 CTI Interface

To meet its requirements, the Cooperative Transport Interface (CTI) is a vital support interface for the Open Fronthaul CUS-Plane, ensuring that the interface always has the necessary available resources. Any attack on the interface can severely impact the RAN's quality of service and, in the worst-case scenario, completely disrupt the network's functionality. A digital signature is the only recommended requirement to ensure the interface's Integrity and origin authentication. However, the CTI interface does not transfer UP or CP data, so attacks on it can only affect the system's Availability. The risk is high for all attackers, except those in scenarios that implement the optional security controls of O-RAN. The signature improves the risk for Outsider and User attackers from high to medium. However, Insiders are unaffected as they can access the cryptographic keys.

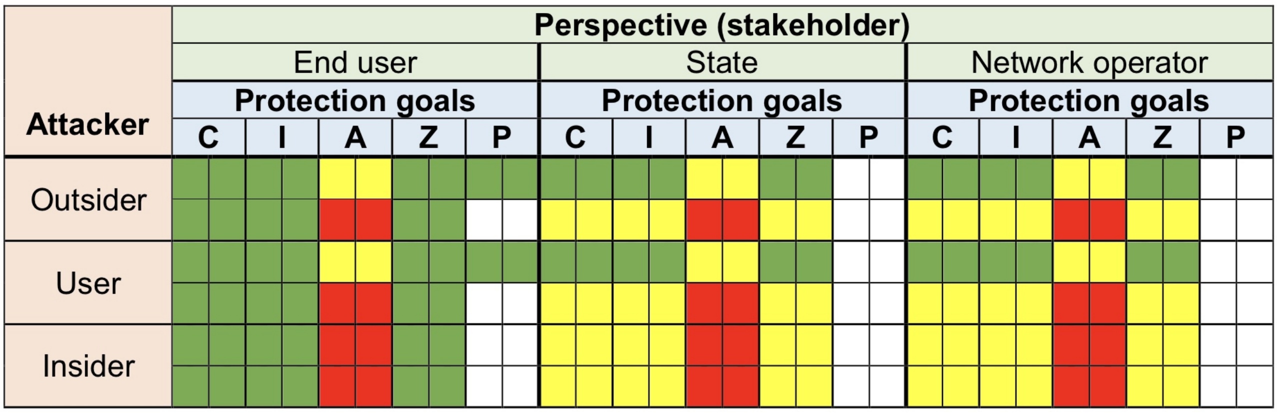


Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩
User	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	🟩	🟩
Insider	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜
	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩	⬜	⬜

Figure 23: Risk Assessment of CTI[35]

3.1.2.7 A1 Interface

The A1 interface is responsible for connecting nRT RIC and non-RT RIC to transfer data for Policy Management purposes and for use in ML models to improve RAN functionality. At the time, there were no mandatory security controls for A1, and only TLS was recommended for Confidentiality, Integrity, and authenticity. The security of A1 is claimed to be independent of 3GPP standards, so the authors considered only two scenarios: a worst-case scenario where the interface is unprotected and a best-case scenario where TLS is used. In the worst-case scenario, the risk of Availability is high for any attacker as external access can be gained and this could affect the Availability of the RAN. There is low risk for Confidentiality, Integrity, and Accountability breach from an end User perspective, since UP data is not transmitted over the interface. However, operational data of the RAN is sent over the interface, and hence the risk is medium for other stakeholders. In the best-case scenario, the use of TLS reduces the risk of Outsider and User attackers, but Availability attacks are still feasible, and the risk is evaluated as medium. The evaluation for Insider attackers remains unchanged.



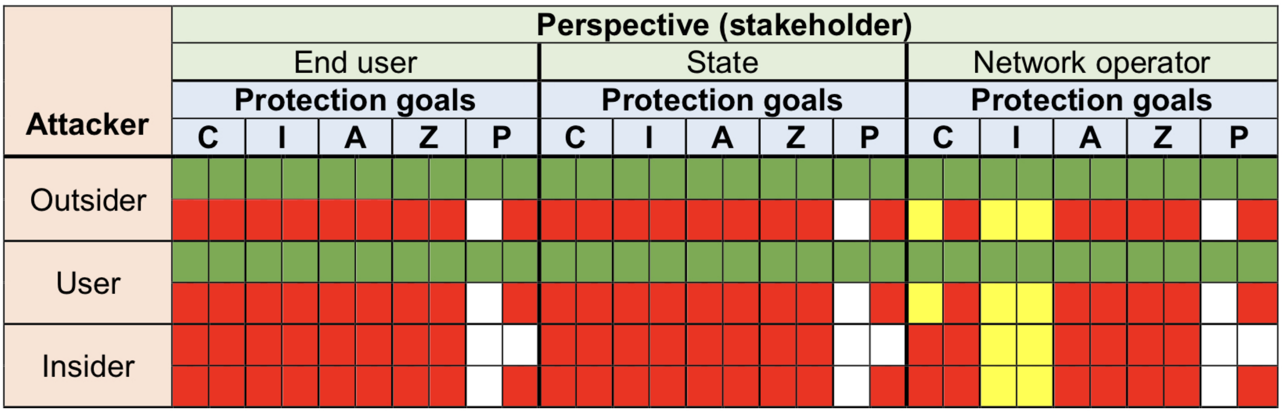
Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩			🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩		
	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩			🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨			🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨		
User	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩			🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩		
	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩			🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨			🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨		
Insider	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩			🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨			🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨		
	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩			🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨			🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨		

Figure 24: Risk Assessment of A1 [35]

3.1.2.8 R1 Interface

The R1 interface enables rApps to access non-RT RIC functions and other services required to fulfill their tasks. However, the interface was at the time largely unspecified and there was no concrete design for it. This lack of specification made it difficult to determine how the R1 interface is implemented and even more difficult to perform a risk assessment. For this reason, the authors use the results of the risk assessment conducted for the O1, O2, and A1 interfaces. They consider the highest risk among these interfaces as the minimum level of risk for the R1 interface. Therefore, the authors rely on the available information and assumptions to conduct the risk assessment. This approach is based on two main facts: first, that the O1/O2 interfaces have the capability to configure every component in the architecture, allowing an attacker to take control of the interface. Second, the A1 interface serves as a link between controllers and is used to transfer every policy/RAN configuration set by the rApps-non-RT RIC, and thus can be consider as an upped bound for the security of R1.

Furthermore, the analysis explains that the level of security risk for the R1 interface depends (almost entirely) on the O-RAN specifications, as no UP or CP data are being transmitted over. The O-RAN specifications have a significant impact on ***bb***/***ww***-scenario considerations for security. In the ***ww*** scenario the O1/O2 interface can be used to take control of the R1 interface, rendering any 3GPP security measures ineffective. On the other hand, in the ***bb*** case, the safety of R1 is ensured via the safety of the other interfaces, which reduces the need for 3GPP protective measures. However, 3GPP controls are not completely ineffective as they ensure Integrity protection for the CP data even in the ***ww*** scenario and End-to-End protection (Confidentiality and Integrity protection) in the ***bw*** scenario.



Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Outsider	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥
User	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥
Insider	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜⬜	🟥🟥	🟨🟨	🟥🟥	🟥🟥	⬜⬜
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥

Figure 25: Risk Assessment of R1 [35]

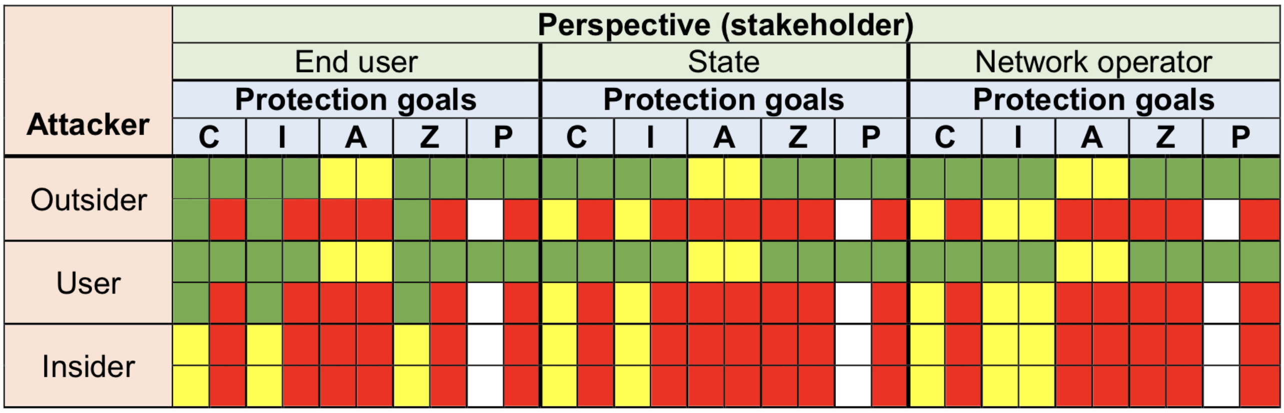
3.1.2.9 E2 Interface

The E2 interface is employed for the administration of the E2 nodes, comprising the O-DU and O-CU, by the nRT RIC. It allows observing and modifying any data traffic flowing through the E2 nodes. As per the analysis, this constitutes a significant security hazard since the CP and UP can be directly tampered, if the interface is not properly secured. As before, mandatory controls are non-existent, except for a prerequisite that mandates Confidentiality, Integrity, and replay protection support. The recommended approach to achieving this is using IPsec. The absence of mandatory security controls renders the interface entirely vulnerable to attacks, including from external attackers. Consequently, there is a high risk regarding Availability, Confidentiality/Privacy, and Accountability for all stakeholders since data from both planes are exposed to every potential attacker in the ***ww*** scenario. The only exception is the Integrity-protected CP data between the UE and the AMF, which mitigates the risk from high to medium (as the O-RAN control data remains unprotected) from the Operator's point of view. In the ***wb*** scenario, 3GPP optional security controls require the protection of UP data between the UE and the O-CU, which protects the data from Outsiders and (most of them) Insider attackers. If the Insider controls the O-CU or a powerful configuration interface, he might be able to extract the encryption keys and compromise Confidentiality, Integrity/Privacy, and Accountability. As a result, the risk is deemed medium for these protection goals but high for Availability. In the ***bb*** scenario, the authors explain that only Availability attacks are possible as E2 is protected by the IPsec and the data at the E2 nodes are secured under the 3GPP optional controls. The potential threats are identified for each attacker while the respective risk is calculated. The threats are depicted in Tab.2.

Table 2: Threats associated with the E2

Attacker	Threat	Consequences
Outsider	Stupid Denial Of Service (DoS) attacks	Limited effect on the QoS, as RAN can function without the E2
	Intelligent Manipulation of E2 traffic	Potential overloading of the E2 nodes
	Interception of O-RAN Control Data	May prevent the detection of failures related to the E2
User	Generation of Legitimate Malicious Traffic	Legitimate traffic is used by ML models for RAN optimisation. This might result to ill-trained models. Buffer overflow and SQL Injection attacks are also possible
Insider	Control Of The Interface	Availability attacks are effortless. Compromised UP data iff the attacker has access to the cryptographic keys. Exposed Configurations on the E2 node

The overall risk for Availability in the ***bw*** scenario is evaluated as medium for Outsider/User attackers and high for Insider attackers. Insider attackers pose a high risk to the Confidentiality, Integrity, and Accountability of UP and O-RAN control data. The usage of IPsec provides protection against external threats, but risks are still considered severe, similar to the ***bb*** scenario. The difference is that Insider attackers can compromise all protection goals, except for Integrity-protected CP data, since the data is not secured by the 3GPP optional security controls. Therefore, the overall risk for Confidentiality, Integrity is evaluated as medium and high for all other protection goals.



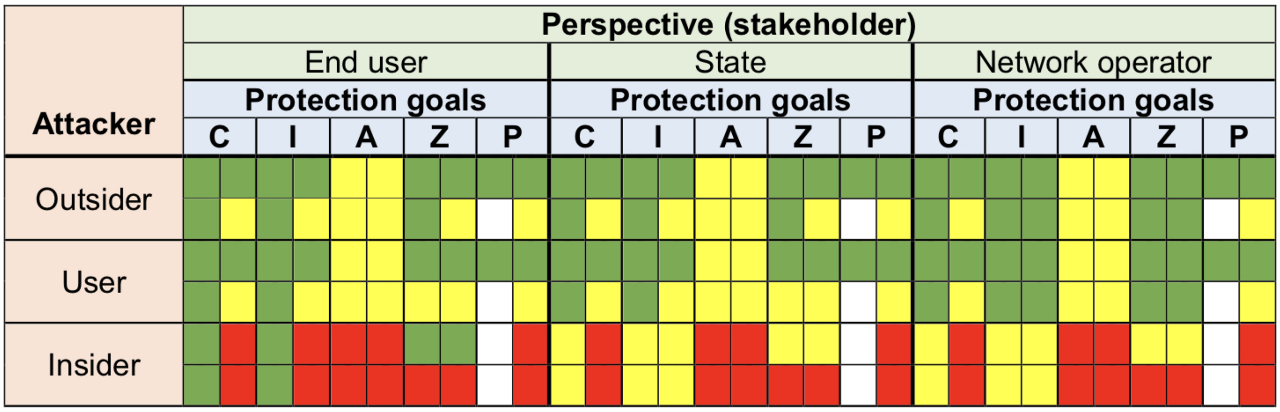
Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
	🟩	🟥	🟩	🟥	🟥	🟥	🟩	🟥	⬜	🟥	🟨	🟥	🟨	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
User	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
	🟩	🟥	🟩	🟥	🟥	🟥	🟩	🟥	⬜	🟥	🟨	🟥	🟨	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
Insider	🟨	🟥	🟨	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟨	🟥	🟨	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
	🟨	🟥	🟨	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟨	🟥	🟨	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥

Figure 26: Risk Assessment of E2[35]

3.1.2.10 Open Fronthaul M-plane

The Open Fronthaul M-Plane interface allows for managing O-RU components, including the ability to perform software updates. Only the optional use of SSH is specified in the specifications (but mandatory support), along with a recommendation to support also TLS. Statements that mandate the authentication of O-DU are also present but without any recommended or mandatory control. The authors explain that the ability to change configuration (of the O-RU) data through the Open Fronthaul M-Plane interface can result in Availability attacks that may cause the complete functional failure of the RAN. Despite extensive security considerations in the specification documents, the mandatory security mechanisms were unclear. In addition, the provision of a rights/roles concept and various functional groups in the interface, including a default User with "sudo" rights and a default password, only raises concerns about the security of the interface. In the ***ww*** scenario, the optional security controls are assumed to be mandatory due to strong statements provided in the specifications. According to the assessment, the O-RAN security measures provide a low level of risk against attacks by User/Outsider attackers on Confidentiality, Integrity, and Accountability for all stakeholders. However, because the mandatory implementation of these security measures is unclear, the risk is elevated to a medium level. A similar risk level is given to Availability. Insider attackers with access to the interface can manipulate control and UP data, leading to a high risk to all protection goals for all stakeholders (this is possible through software-update manipulation) except from the Integrity goal, as CP are protected between UE and the AMF, from the Operator's/State's point of view. The presence of sensitive control data in the O-RU results in an overall medium Integrity-related risk. The assessment of ***wb*** scenario is similar to the previous assessment. However, the 3GPP safeguards protect the CP data, even from an Insider (with control of the O-RU), but due to the existence of control data in the O-RU, the risk is evaluated to be medium. In the ***bb*** scenario, Outsider/User and Insider attackers are at low risk of violating Confidentiality, Integrity, Accountability, and Privacy of User and Control Plane data as the O-RAN security measures prevent successful attacks. In the ***bw*** scenario, the use of SSH/TLS prevents Outsiders from accessing the interface resulting in a low risk of breaching Confidentiality, Integrity, Accountability, and Privacy of User and Control Plane data. However, Insider attackers with access to the O-RU pose a high risk due to the lack of protection for UP data. For the Network Operator, Confidentiality risk is the same, but Integrity is secured by mandatory

Integrity protection of CP data between UE and AMF. However, as said before, the control data in the O-RU/O-DU is not protected.

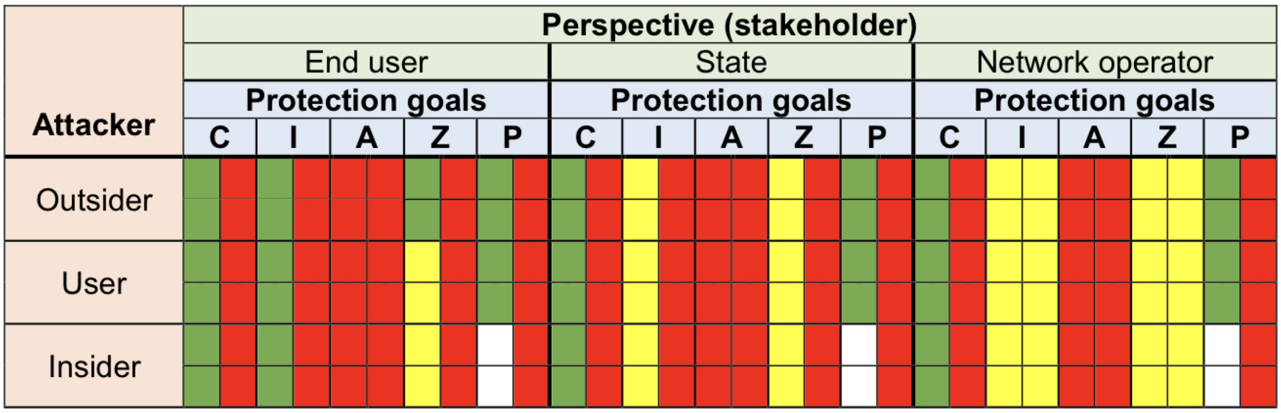


Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	⬜	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	⬜	🟨	🟩	🟨	🟩	🟩	🟨	🟨	🟩	🟩	⬜	🟨
User	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
	🟩	🟨	🟩	🟨	🟨	🟨	🟨	🟨	⬜	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟨	🟨	⬜	🟨	🟩	🟨	🟩	🟩	🟨	🟨	🟩	🟩	⬜	🟨
Insider	🟩	🟥	🟩	🟥	🟥	🟥	🟩	🟩	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟨	🟨	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟨	🟨	⬜	🟥
	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥

Figure 27: Risk Assessment of Open Fronthaul M-Plane[35]

3.1.2.11 Open Fronthaul CUS-Plane

The CUS-Plane is responsible for transmitting 3GPP data of both planes and synchronization messages between the O-RU and O-DU in the open Fronthaul network. At the time of analysis, this interface had no security measures due to high requirements for delay time and bandwidth and the assumption that 3GPP standards already secure the transmitted data. The authors consider only two scenarios, depending on the implementation of optional 3GPP standards. In the ***ww*** scenario, the risk of breaching every protection goal is high for all stakeholders, as an Outsider can access the unprotected interface. A medium risk is associated with the Operator's view regarding Integrity, as CP data are secured by 3GPP standards, but synchronization data is exposed. In the ***bb*** scenario, UP data is protected by 3GPP safeguards, which lowers the risk for "User" and "Insider " attackers in terms of Confidentiality, Integrity, and Accountability. However, a medium risk is still present for "User" attackers in terms of Accountability due to the lack of protective measures by 3GPP. The Availability risk is still regarded as high, as attacks on the Open Fronthaul Plane can threaten the functionality of RAN. Although the CP data exchanged between UE and AMF is secured by 3GPP safeguards, in the best-case scenario, the time synchronization data remain unprotected, resulting in a medium risk.

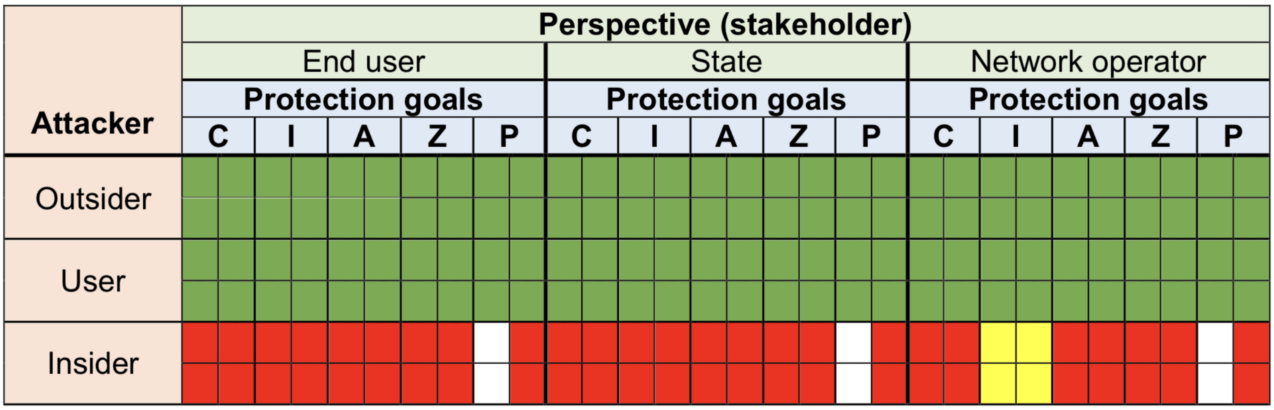


Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟥	🟩	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	🟩	🟥
	🟩	🟥	🟩	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	🟩	🟥
User	🟩	🟥	🟩	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	🟩	🟥
	🟩	🟥	🟩	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	🟩	🟥
Insider	🟩	🟥	🟩	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	⬜	🟥
	🟩	🟥	🟩	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	⬜	🟥

Figure 28: Risk Assessment of Open Fronthaul CUS-Plane[35]

3.1.2.12 xApps/rApps

The study indicates that the analysis for the rApps/xApps is similar, with the leading security issue being the co-existence of these applications with other apps and functions on the same hardware. The rApps are located in the SMO framework, and the xApps in the nRT RIC. Weak isolation between these apps is a potential vulnerability that could be catastrophic when combined with the absence of security controls for accessing the various interfaces associated with the apps. Additionally, parser attacks and insecure programming may compromise the apps' security. However, the analysis presented in the report only considers the apps' security and not attacks on the apps or the RAN. Therefore, the risk related to Outsider and User attacks is considered low. However, an Insider can compromise every security objective, in every scenario, except for the Integrity protection of the CP data.



Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
User	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Insider	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥

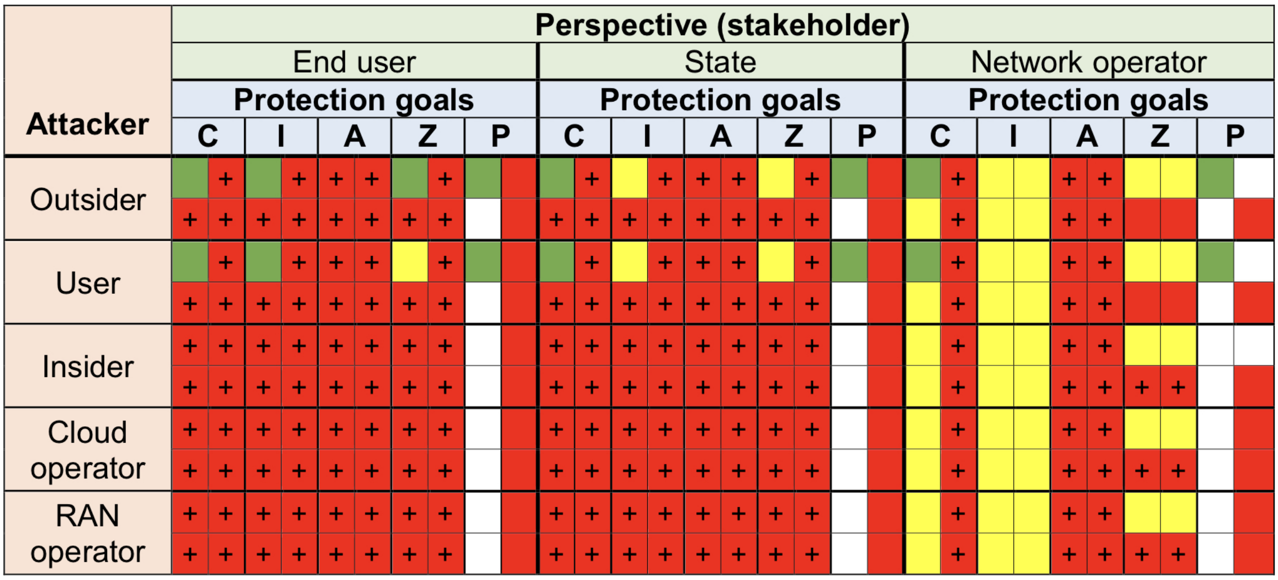
Figure 29: Risk Assessment of xApps/rApps[35]

3.1.2.13 Other Analyses

The BSI analysis covers additional interfaces and aspects of the architecture, such as the AI/ML Interface and the Human Machine interface. These interfaces are mainly used to access enrichment information and are almost unspecified. Herefore, only some possible threats are discussed, and this report does not provide a comprehensive analysis. More information on the analysis can be found in [35].

3.1.3 Overall Analysis and Evalaution

3.1.3.1 Summarised Results



Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟥+	🟩	🟥+	🟥+	🟥+	🟩	🟥+	🟩	🟥	🟩	🟥+	🟨	🟥+	🟥+	🟥+	🟨	🟥+	🟩	🟥	🟩	🟥+	🟨	🟨	🟥+	🟥+	🟨	🟨	🟩	⬜
	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟨	🟥+	🟨	🟨	🟥+	🟥+	🟥	🟥	⬜	🟥
User	🟩	🟥+	🟩	🟥+	🟥+	🟥+	🟨	🟥+	🟩	🟥	🟩	🟥+	🟨	🟥+	🟥+	🟥+	🟨	🟥+	🟩	🟥	🟩	🟥+	🟨	🟨	🟥+	🟥+	🟨	🟨	🟩	⬜
	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟨	🟥+	🟨	🟨	🟥+	🟥+	🟥	🟥	⬜	🟥
Insider	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟨	🟥+	🟨	🟨	🟥+	🟥+	🟨	🟨	⬜	⬜
	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟨	🟥+	🟨	🟨	🟥+	🟥+	🟥+	🟥+	⬜	🟥
Cloud operator	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟨	🟥+	🟨	🟨	🟥+	🟥+	🟨	🟨	⬜	🟥
	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟨	🟥+	🟨	🟨	🟥+	🟥+	🟥+	🟥+	⬜	🟥
RAN operator	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟨	🟥+	🟨	🟨	🟥+	🟥+	🟨	🟨	⬜	🟥
	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	🟥+	⬜	🟥	🟨	🟥+	🟨	🟨	🟥+	🟥+	🟥+	🟥+	⬜	🟥

Figure 30: Summary Analysis [35]

The summarised analysis presented in Fig.30 is based on the worst-case scenario for each individual analysis, with the results summarized in the table below. Entries marked with a "+" indicate high confidence in the assessment results. The analysis shows that the ***bb*** scenario with all optional security controls implemented is the only scenario that can ensure the protection of all security goals except for Availability, but only from external attackers. From the Network Operator's perspective, the mandatory Integrity protection of CP provides some security even in the ***ww*** scenarios. However, ensuring Availability remains challenging, and the architecture lacks protection controls against Insiders and Cloud-Operators who can violate every protection goal except for the Integrity of the CP data. Overall, the analysis concludes that the architecture is unsecured even if all O-RAN optional controls are made mandatory, as Cloud/Ran Operators and Insiders can still violate almost every security goal.

3.1.3.2 Evaluation Of the Analysis

The presented analysis is the most extensive one conducted over the years. Its focus is mainly the architectural security of O-RAN as essential aspects such as ML and Virtualisation are not covered extensively. This absence is justified as the specifications did not allow for a deeper analysis of these sections. In addition, these sectors are under comprehensive studies outside of the concept of networks. As mentioned, the analysis is based on the initial security specifications provided by O-RAN and therefore requires updating. Adding new components to the architecture, such as the Y1 interface, further justifies our earlier statement. Moreover, the logical functions of the architecture, such as O-DU/nRT RIC.../O-CU, were not included in the analysis. The introduction of the Insider attacker compensates for the absence of a separate analysis for the logical functions. For instance, the analysis implies that an exposed O-CU could compromise the UP data as cryptographic keys are stored there, even though an individual analysis of the O-CU has never been performed. Although the analysis was mostly accurate, some inconsistencies exist between the explanation and the graphical representation of the results. Furthermore, our understanding of the specifications differs from the author's view in some cases. Consequently, we firmly believe an updated analysis version is needed.

3.1.3.3 The Issue of Privacy

The analysis results reveal that the Privacy risk is not assessed in numerous instances. Within the O-RAN framework, there are two ways in which User Privacy can be compromised: through unprotected UP data or reports related to UP data(metadata). These reports might be used for ML model training to improve RAN functionality or to provide RAN analytics. Given that O-RAN is still in its early stages of development, the data required for Privacy-Preserving ML model training is still under investigation. This provides some justification for the lack of Privacy-risk assessment. In our opinion, conducting an accurate Privacy evaluation is not currently feasible.

3.2 Risk Analysis on The Latest Specifications *(v05)*

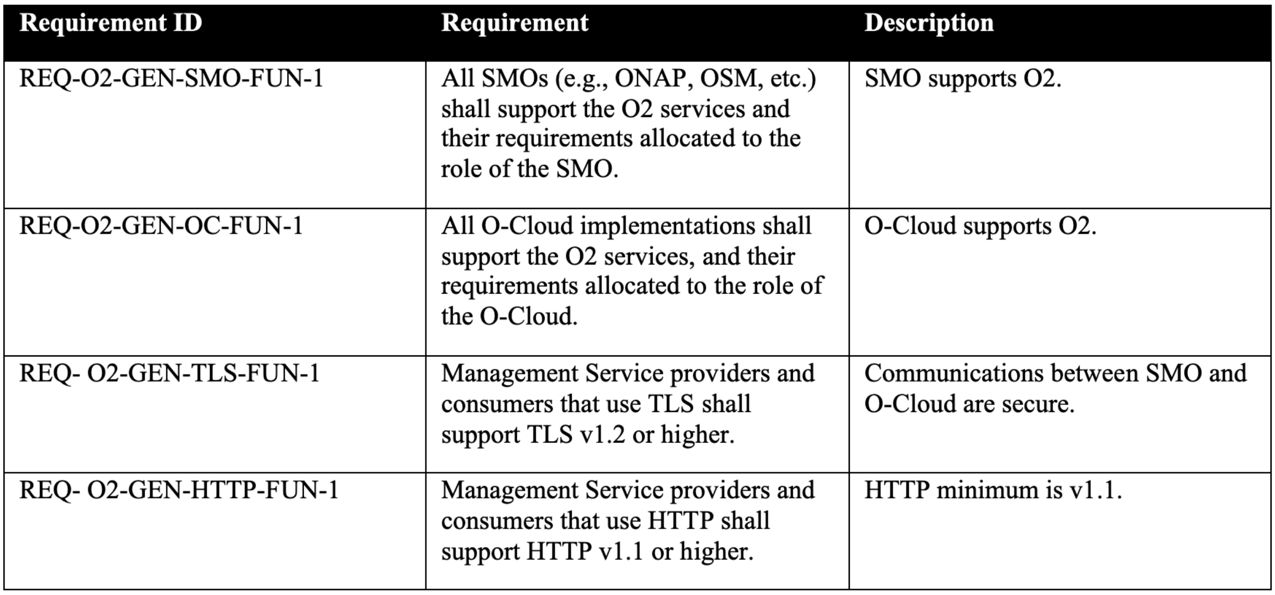
3.2.1 Approach

Our Approach will be similar to the approach followed by the BSI team (Sec.3.1.1.6). This will enable a fair comparison between the 2 analyses. However, our analysis apart from all of the interfaces, will include also all the logical functions of the O-RAN architecture. The approach of the evaluating the logical function, is identical with the approach the authors of BSI report performed for the xApps/rApps evaluation, in other words, we will consider only an exploited function by an Insider attacker, as external attackers are required to exploit an interface first, before they gain access, and these threats are covered in the analysis of the individual interfaces. Furthermore, in the case of the Open Fronthaul, we will consider also the possibility of an external that posses the ability to physically connect malicious devices in the network. For interfaces without any specifications like the Y1, we will perform a risk analysis based on common knowledge related to the services offered by the interface. In addition, weak security statements are not taken under consideration. Furthermore, we adopt the BSI analysis related to Cloud/RAN Operator, as the only protection from these attackers, is still offered by the 3GPP security optional and mandatory security controls. Lastly, as the BSI analysis, our analysis is mainly focused on the architectural security of O-RAN, as the lack of specification makes the evaluation of ML and Virtualisation extremely difficult and almost completely based on assumptions. However, in some cases, we are considering these aspects and in the Chapter.5 we are recommending some controls related to the security of these aspects.

3.2.2 Risk Analysis of the Interfaces

3.2.2.1 O2 Interface

During the BSI analysis, it was challenging to perform a precise analysis of O2 due to the interdependence of the interface requirements with the services provided by the interface. Detailed design elements such as protocols and privileges were expected to be outlined in the upcoming O2 specifications, as stated by O-RAN. The O2 specifications were released as a separate paper by O-RAN[13], defining the services provided by O2 but leaving the practical implementation undefined. According to the specifications, the implementation of O2 adheres to current standards and specifications set by 3GPP, European Telecommunications Standards Institute (ETSI) NFV, Kubernetes, OpenStack, Internet Engineering Task Force (IEFT), and Open Network Automation Platform (ONAP)/Open Source Mano (OSM). However, only some adopted standards from ETSI NFV and 3GPP are shown in the paper, while standards from other organizations are labeled as "Future study". On the positive side, some configuration standards adopted by ETSI NFV may prevent potential misconfigurations of the system. Regarding security, O-RAN supports that "The O2 interfaces will generally follow ETSI GS NFV-SOL 013 (section 8) for interface security" [13]. The existing standard utilizes both TLS and Oauth 2.0 to secure the interface, but the O2 specifications (Fig.31) only recommend the use of TLS.



Requirement ID	Requirement	Description
REQ-O2-GEN-SMO-FUN-1	All SMOs (e.g., ONAP, OSM, etc.) shall support the O2 services and their requirements allocated to the role of the SMO.	SMO supports O2.
REQ-O2-GEN-OC-FUN-1	All O-Cloud implementations shall support the O2 services, and their requirements allocated to the role of the O-Cloud.	O-Cloud supports O2.
REQ- O2-GEN-TLS-FUN-1	Management Service providers and consumers that use TLS shall support TLS v1.2 or higher.	Communications between SMO and O-Cloud are secure.
REQ- O2-GEN-HTTP-FUN-1	Management Service providers and consumers that use HTTP shall support HTTP v1.1 or higher.	HTTP minimum is v1.1.

Figure 31: O2 Requirements[13]

The security analysis conducted by BSI remains valid as the security requirements have remained largely unchanged, with only the support of TLS v1.2 or v1.3 being mandatory. Furthermore, no effective mechanisms have been implemented to prevent privileges escalation or ensure privileges delegation. The adoption of standards from ETSI NFV[24], is not sufficient to mitigate any risk, presented in the BSI analysis.

3.2.2.2 O1 Interface

The security of the O1 interface remains largely unchanged since the BSI analysis. However, the methodology employed in this section differs from the original analysis for two primary reasons. Firstly, there are no longer separate specifications for the interface. Secondly, a dedicated analysis for the O-DU is provided in subsequent chapters. Therefore, we are providing only an analysis equivalent to the previous general analysis of the interface.

The specification document still does not mandate any security controls other than the general abstract requirements of enforcing Confidentiality, Integrity, Authenticity, and least privilege access control through encrypted transport. The recommended measures are still limited to using TLS and NACM, and there is no explicit ban on the use of SSH, even if its usage is no longer under the recommended options. However, the document has introduced some new security controls that relate to the configuration of NACM. Of these, REQ-NAC-FUN-9 is the most significant, as it requires external User mapping using protocols such as Oauth 2.0 to ensure privilege delegation. Additionally, the O1 interface specifications for communication between the SMO-O-CU have been defined[11], but like the specifications for SMO-O-DU[12] communication, the use of TLS and NACM is no longer mandatory. Having said tat, we conclude that the security of O1 has degraded, as the the BSI general analysis of the interface is now valid for the SMO-O-DU part of the interface.

3.2.2.3 A1 Interface

The optional security controls of A1 were found to have a significant issue regarding inadequate protection against internal attacks. However, implementing TLS can effectively safeguard the Integrity and Confidentiality of interfaces against external attacks. To address the issue above, the latest security specifications of O-RAN have introduced two key requirements that provide adequate protection against internal attacks. The first control requires mandatory support for mTLS to enable mutual authentication and Oauth for authorization. In the absence of the mandatory usage of the security controls, we consider the BSI analysis to be valid for the ***ww*** but not for the ***bb*** case (since A1 is evaluated only under two scenarios due to its independence from 3GPP standards). In the ***bb*** scenario, using mTLS prevents unauthorized parties from accessing the interface. Therefore the unauthorized ends (such as controllers or Apps) are prevented from accessing any interface service. Furthermore, using Oauth ensures delegated access with privilege-corresponding access tokens. In other words, it may limit the power of the Insider attacker by restricting his access to the services offered by A1. As a result, the capability of an Insider attacker to manipulate policies(O-RAN control data) can be restricted. For example, the policy management function of the A1 interface can only be used by the non-RT RIC to guide policies in the nRT RIC. The function allows for the creation/deletion/modification of policies. However, despite not having access to this function, a malicious nRT RIC may 'trick' the non-RT RIC to generate unwanted policies by providing carefully crafted feedback. Even though the implemented optional security measurements provide some protection in the case of an nRT RIC, there are ways to bypass them, and the non-RT RIC can still manipulate policies. The BSI analysis remains valid.

3.2.2.4 R1 Interface

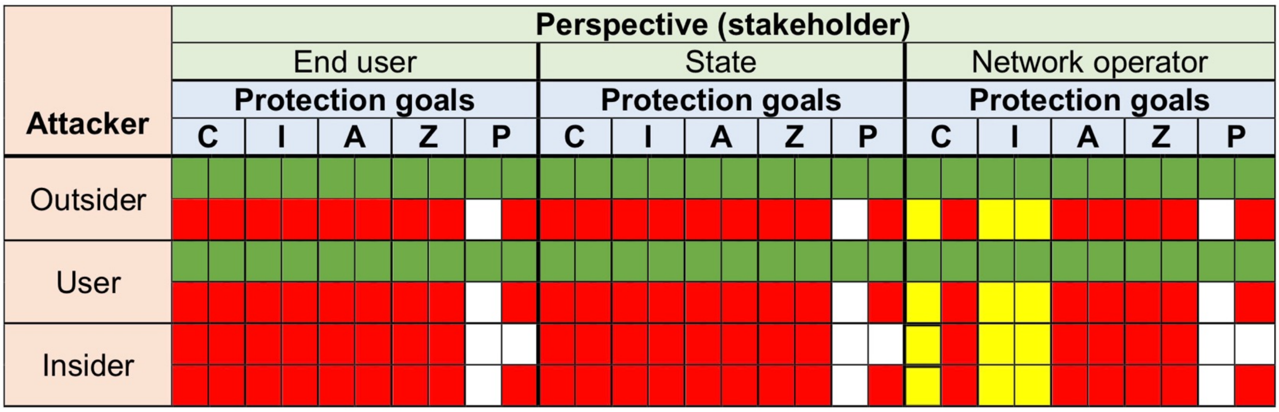
The R1 interface now has a concrete design and specifications, revealing the extensive and powerful services it exposes to rApps, including data access, configuration management, and policy management. In the past, the lack of specifications forced the authors to rely on the analysis of other interfaces to infer security results for R1. However, a more comprehensive analysis can be performed now that the specifications and aspects paper has been released by O-RAN[10]. The BSI report identified a major issue with R1: the potential for an attacker to take control of every architecture component via the O1/O2 interface. While the O1 services are no longer exposed to the R1, O2 services still are, including the service to provision changes to the configuration

of the O-Cloud, which could give an attacker control over the entire architecture. Even if this capability is somehow limited, the recommended security mechanisms for R1 are still insufficient to secure the interface adequately.
The specifications describe three optional security measures:

- TLS for security protection at the transport layer
- mTLS for mutual authentication
- Oauth 2.0 for authorization

If implemented, the security requirements provide protection against external threats and some protection against internal threats, as explained in the A1 analysis. While the BSI analysis remains valid for the Outsider and User attacker, the implementation of optional security mechanisms affects the Insider attacker in the ***bb*** and ***bw*** scenarios. A firm access policy can limit data access to a small number of rApps, and a service can prevent certain data types from being discovered. Currently, Privacy-Preserving ML concepts are being investigated to protect User Privacy when sharing data with rApps. However, the non-RT RIC can still access data collected by the SMO to perform Model Training. In the ***bb***/***bw*** scenarios, data are somewhat protected by authorized access, except when Insider have full access rights. Despite the restricted access, the fact that Insiders with full access rights, such as the non-RT RIC, can access data, and the lack of Privacy-Preserving ML techniques, means that the BSI analysis still holds from the User's perspective. About other stakeholders, the BSI report also holds, as the interface transmits ML workflows that an Insider can eavesdrop on or manipulate and other O-RAN control data.

However, even though its explicitly mentioned in the BSI analysis that the CP data are End-to-End protected (Confidentiality and Integrity), if the optional 3GPP controls are implemented, their analysis R1 analysis asses the risk for the Integrity as high, from the Network Operators perspective. In our opinion, the risk should be medium and not high, as CP data are protected between the UE and the AMF, but O-RAN control data remain unprotected.



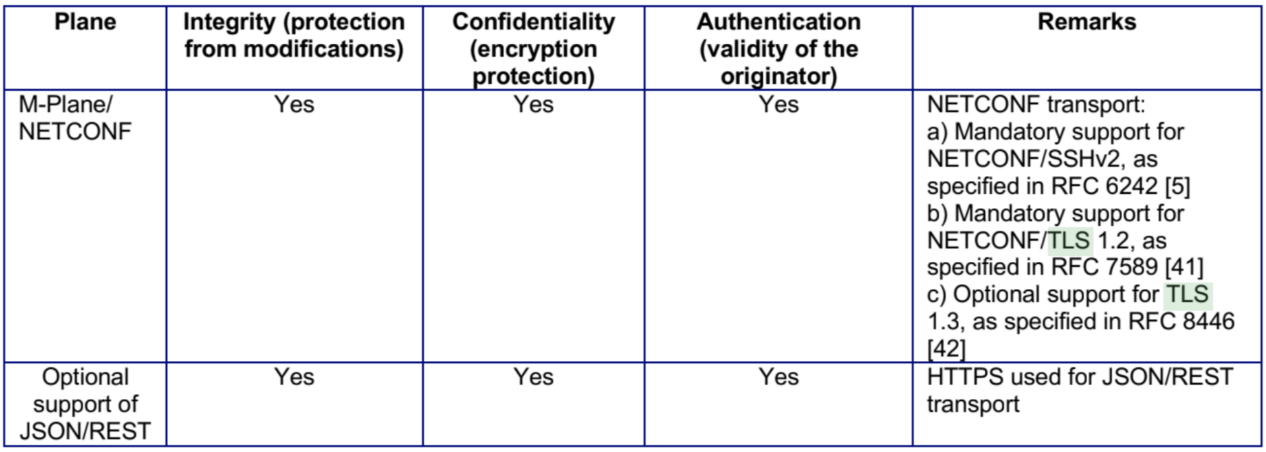
Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
User	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
Insider	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	⬜	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	⬜
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥

Figure 32: Updated Risk analysis of R1

3.2.2.5 Open Fronthaul M-Plane

The mandatory security controls for M-Plane remain unchanged. However, new optional security control is introduced to restrict access to the physical network infrastructure to only authorized devices[15]. The IEEE 802.1X protocol is a port-based access protocol that enforces authenticated and authorized access to the network, preventing malicious components such as an O-RU from accessing the network. This protocol also includes mechanisms to block all incoming traffic to unauthorized ports, reducing the impact of potential

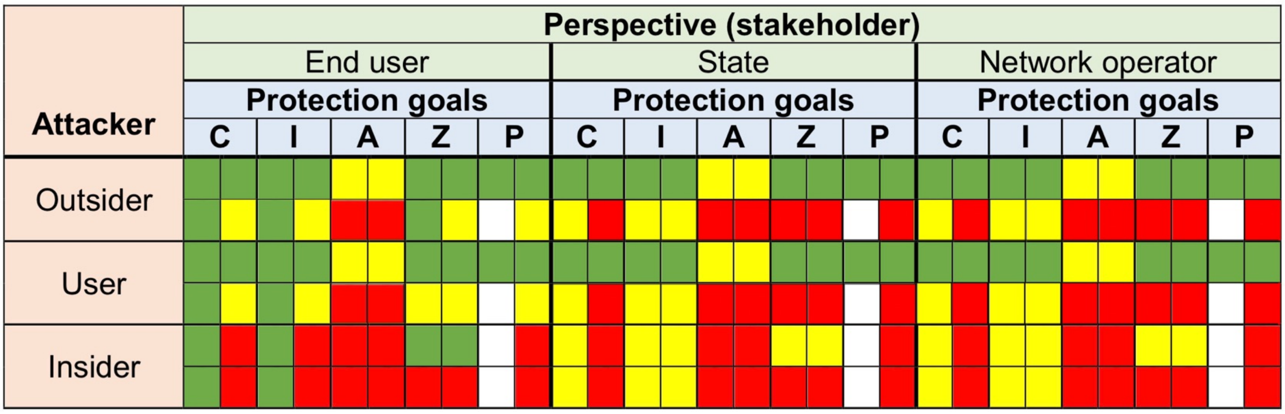
DoS attacks. This implementation does not affect the analysis, as it does not consider attackers attempting to access the network by connecting a malicious element. However, we disagree with the BSI analysis regarding Outsider and User attackers. The analysis assumes that the use of TLS/SSH is mandatory even in the ***ww*** scenario, while Fig.33 indicates that both protocols are only mandatory to support.



Plane	Integrity (protection from modifications)	Confidentiality (encryption protection)	Authentication (validity of the originator)	Remarks
M-Plane/ NETCONF	Yes	Yes	Yes	NETCONF transport: a) Mandatory support for NETCONF/SSHv2, as specified in RFC 6242 [5] b) Mandatory support for NETCONF/TLS 1.2, as specified in RFC 7589 [41] c) Optional support for TLS 1.3, as specified in RFC 8446 [42]
Optional support of JSON/REST	Yes	Yes	Yes	HTTPS used for JSON/REST transport

Figure 33: Optional/Mandatory Security Requirements of Open Fronthaul M-Plane[6]

Due to the lack of mandatory protection from Outsider/User attackers in both the ***ww*** and ***bw*** scenarios, a re-evaluation of the risk assessment is necessary. The unprotected interface in these scenarios allows for management of the O-RU even from an Outsider, and a miss-configured O-RU could result in a non-functional RAN, leading to high risk for all stakeholders in both scenarios, concerning Availability. As for UP data and the End-User's protection goals, the risk remains at a medium-high level for Confidentiality, Integrity, Accountability, and Privacy, as no UP data is transmitted over the interface in the ***ww*** scenario. However, further investigation is needed to determine how much an Outsider can manipulate an update over transmission to gain access to UP data. From the State's/Operator's perspective, the risk assessment differs from the End-User's. Apart from the CP that may be accessed and modified via manipulation of an update even by an Outsider, O-RAN control/configuration data transmitted can be manipulated with less effort than CP data. This results in a high risk for all protection goals (except for Integrity). In the ***ww*** and ***wb*** scenarios, the Integrity protection of CP data improves the Integrity-risk level from high to medium.



Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
	🟩	🟨	🟩	🟨	🟥	🟥	🟩	🟨	⬜	🟨	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
User	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩
	🟩	🟨	🟩	🟨	🟥	🟥	🟨	🟨	⬜	🟨	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
Insider	🟩	🟥	🟩	🟥	🟥	🟥	🟩	🟩	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟨	🟨	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟨	🟨	⬜	🟥
	🟩	🟥	🟩	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥

Figure 34: Updated Risk analysis of Open Fronthaul M-Plane

3.2.2.6 E2 Interface

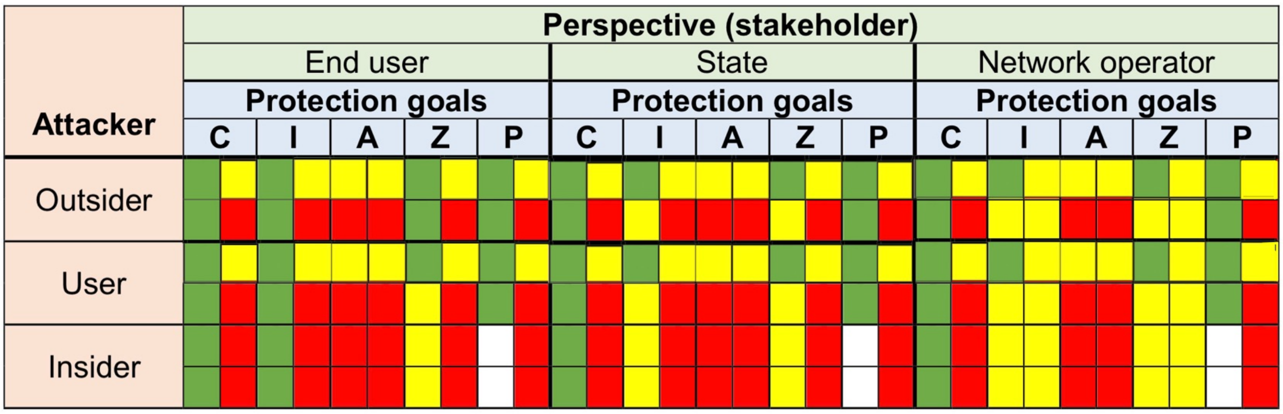
The specifications for the E2 interface [15][5] have remained essentially unchanged since their initial release, with the only optional security control being the use of IPsec to secure the interface. The critical change is that support for IPsec is now mandatory. However, mandatory support does not necessarily mean mandatory usage; therefore, the risk analysis conducted by BSI still holds.

3.2.2.7 CTI Interface

The CTI interface has not had any new security controls added; the only recommended safeguard is digital signatures, which only provide protection for Integrity and Accountability[4]. Therefore, a new analysis is unnecessary, as the analysis conducted by BSI remains valid.

3.2.2.8 Open Fronthaul CUS-Plane

The interface under consideration lacked security controls during the analysis. However, in the current specifications, O-RAN introduces some optional controls for the *C and S* planes to secure the interface[15]. The C-Plane is crucial as its messages control the processing of 3GPP data transmitted over the Uu interface. According to the specifications, a disruption in the operation of this plane will force the O-RU to drop every packet received over the Uu interface. Thus, O-RAN recommends using the IEEE 802.1x protocol for authentication and authorization to protect the network from unauthorized access. However, the protocol does not offer any protection if the attacker has physical access to the infrastructure, as there is no encryption or Integrity protection for the communication. Moreover, an Insider attacker may still interrupt the operation of this interface by intentionally delaying the transmission of DL/UL packets. The S-Plane is also recommended to use this protocol for security, as it synchronizes the clocks of the O-RU and O-DU. Attacks on degrading synchronization are prevented except when the attacker is an Insider or has physical access to the interface. On the other hand, the U-Plane is used to transport User data, and as per the first specification, its security is provided by the 3GPP security controls, according to O-RAN Alliance. However, implementing these security controls is optional, and it is up to the Operator to decide. Thus, the security of the data cannot be assumed. The implementation of the new security controls has resulted in improved outcomes of the BSI analysis in both the ***bw*** and ***bb*** scenarios. These controls have effectively reduced every high-risk level assigned to Users and Outsiders to a medium level for all protection goals. However, it should be noted that the risk level is still assessed as medium and not low due to the possibility of attacks with physical access to the interface.

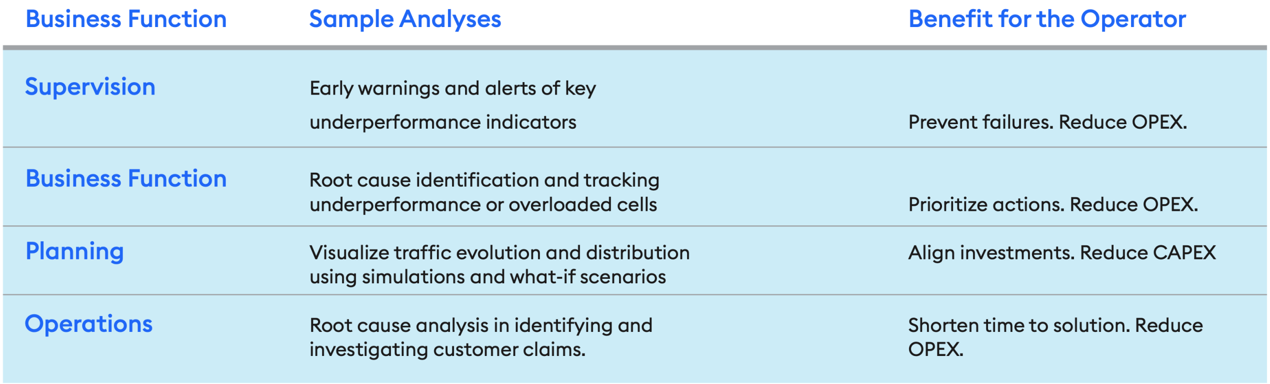


Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟨
	🟩	🟥	🟩	🟥	🟥	🟥	🟩	🟥	🟩	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	🟩	🟥
User	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟩	🟨	🟨	🟨	🟩	🟨	🟩	🟨
	🟩	🟥	🟩	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	🟩	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	🟩	🟥
Insider	🟩	🟥	🟩	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	⬜	🟥
	🟩	🟥	🟩	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟩	🟥	🟨	🟥	🟥	🟥	🟨	🟥	⬜	🟥	🟩	🟥	🟨	🟨	🟥	🟥	🟨	🟨	⬜	🟥

Figure 35: Updated Risk analysis of Open Fronthaul CUS-Plane

3.2.2.9 Y1 Interface

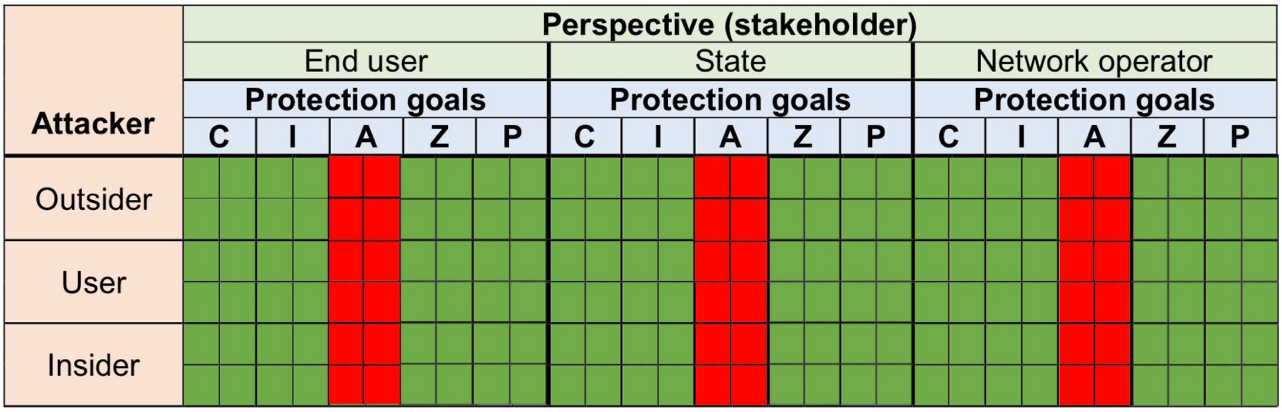
The Y1 interface is a recent addition to the O-RAN architecture, having been introduced in the latest specifications version. It aims to provide RAN analytics generated by the nRT RIC to Y1 consumers. However, the interface is undocumented, with no design or security specifications. The most detailed description of the interface is as follows: *"The Near-RT RIC provides RAN analytics information services via Y1 interface. Y1 consumers can consume the RAN analytics information services by subscribing to or requesting the RAN* *analytics information via the Y1 interface. Y1 consumers could be Application Functions (AFs) when they are in an O-RAN trusted domain. Alternatively, the RAN analytics information could be securely provided to AFs via an exposure function, e.g., as in 3GPP TS"[8]*. Typically, RAN analytics are used for control and management purposes [34][58]. Fig.36 shows examples of RAN analytics.



Business Function	Sample Analyses	Benefit for the Operator
Supervision	Early warnings and alerts of key underperformance indicators	Prevent failures. Reduce OPEX.
Business Function	Root cause identification and tracking underperformance or overloaded cells	Prioritize actions. Reduce OPEX.
Planning	Visualize traffic evolution and distribution using simulations and what-if scenarios	Align investments. Reduce CAPEX
Operations	Root cause analysis in identifying and investigating customer claims.	Shorten time to solution. Reduce OPEX.

Figure 36: Examples of RAN Analytics[58]

Based on the illustration provided, it is evident that leveraging RAN analytics can help prevent malfunctions and optimize the system's performance. However, since the reports generated do not include User data, any interface compromise would only affect the system's Availability. Since the interface lacks any form of protection, an adversary can gain access to it and disrupt the RAN functionality by injecting malicious reports or preventing legitimate ones from reaching their destination. Failure to identify a critical issue could lead to a non-operational RAN. Consequently, the risk associated with such an attack is considered high for any attacker.



Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Outsider	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟥	🟩	🟩
User	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟥	🟩	🟩
Insider	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟥	🟩	🟩	🟩	🟩	🟥	🟩	🟩

Figure 37: Risk Analysis of Y1

3.2.3 Risk Analysis on the ORAN Functions and O-RU

3.2.3.1 O-Cloud

As a critical component of ORAN, O-Cloud must be protected at all costs, as it may compromise the whole RAN. The mandatory isolation mechanisms and the optional authentication/authorization are still the main security requirements. However, a considerable effort was made by O-RAN Alliance to offer *1)Software protection to the Network functions and the Application layer, 2)Secure Update, 3)Secure Storage, 3)Chain Of Trust.* Many security controls have been adopted related to these areas:

1. Software Protection to the Network:

- All packages, including apps, VNFs, CNFs, and any external artifacts, must be certified and signed by their respective providers.
- Critical artifacts must be encrypted with either symmetric or asymmetric cryptography
- Every package must be in line with ETSI NFV specifications
- All of the cryptography keys must be secured via the use of cryptography

2. Secure Update:
    - Signature generation/verification must be in line with O-RAN Security Protocol Specification
3. Secure Storage:
    - Data and cryptographic keys must be stored encrypted with authentication and access control
    - Secure deletion of data by overwriting the allocated memory
    - Sanitisation of sensitive media
4. Chain of Trust:
    - The Chain of Trust must begin from the hardware
    - Support for a remote attestation service that collects configurations and Integrity measurements from O-Cloud

Although implementing the requirements undoubtedly improves the architecture's security, we maintain that the security standards set by BSI remain valid. These measures do not provide adequate security without mandatory authentication and authorization controls. Furthermore, even though isolation is mandatory, there is no mandatory recommended security controls[15].

3.2.3.2 SMO and O-CU

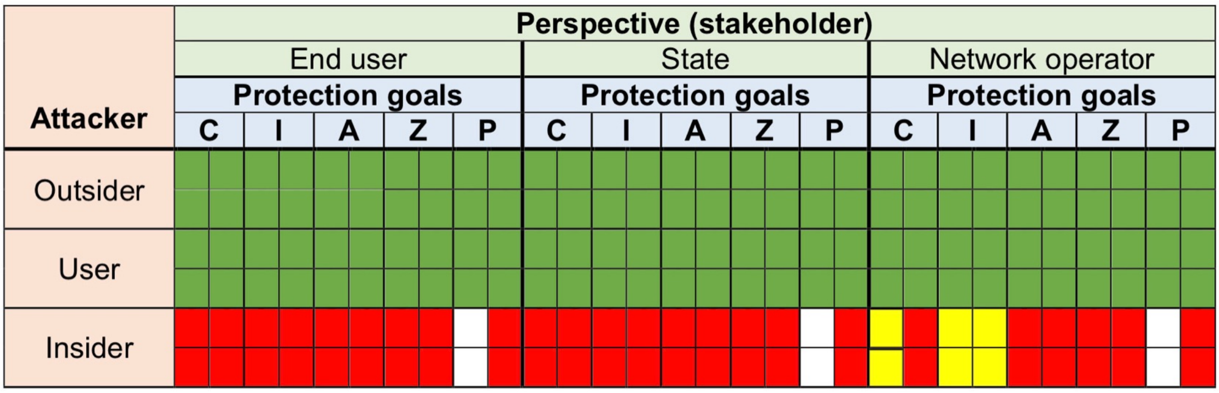
SMO is the most powerful component of the architecture as its responsible for the management and the orchestration of the underline infrastructure (the O-Cloud), among other crucial tasks. The security requirements assigned to the SMO are meant to protect data, logs, and services from being accessed by unauthorized parties. By itself, the SMO poses a significant threat to all protection goals in the system. According to the SMO security analysis[16], sensitive assets in the SMO include:

- *O1 Data: Critical O-RAN management data,...*
- *O2 Data: Telemetry data, Cloud provisioning data,...*
- *Passwords, Certificates, and Private Keys*
- *ML Models and ML data collected by the E2 nodes/nRT RIC (3GPP data)*

The data presented above demonstrate that a malicious SMO can compromise all protection goals (except Availability) for all stakeholders. While the Integrity of CP data provides some protection, the amount of O-RAN control data stored in the SMO results in a medium risk to the Integrity of the data in every scenario. It should be noted that certain logs and data require Integrity and Confidentiality protection. However, in this case, the attacker knows the malicious keys as it controls the entire SMO. Moreover, the SMO controls and configures every O-RAN component via the O2 and O1 interface and may configure the entire O-Cloud and effectively take control over any device. This provides access to 3GPP data and encryption keys from O-CU, allowing the attacker to compromise every security goal except the Integrity protection of CP data.

However, in ***wb*** and ***bb*** scenarios, CP data is also encrypted, making Confidentiality, like Integrity, subject to medium risk of exposure by the attacker. This analysis combines the O2, and A1 analyses while considering the data stored in the SMO.

The analysis for the O-CU case is identical to that of the SMO. As 3GPP data are transmitted over the O-CU before being forwarded to the CN, all data are exposed to an Insider who controls the unit. Even with all optional 3GPP controls in place, the O-CU has access to the UP data, as the decryption of this data occurs within the O-CU itself, and the cryptographic keys are stored locally. As explained previously, only the Integrity of CP cannot be threatened. Both of the attackers can manipulate packets during their transmission and possess the ability to perform attacks resulting in a complete loss of the Availability of the RAN. The SMO may configure every component to drop any incoming traffic, and the CU attacker can perform the same attack on the O-CU itself. For this reason, Availability risk is also high concerning every stakeholder.



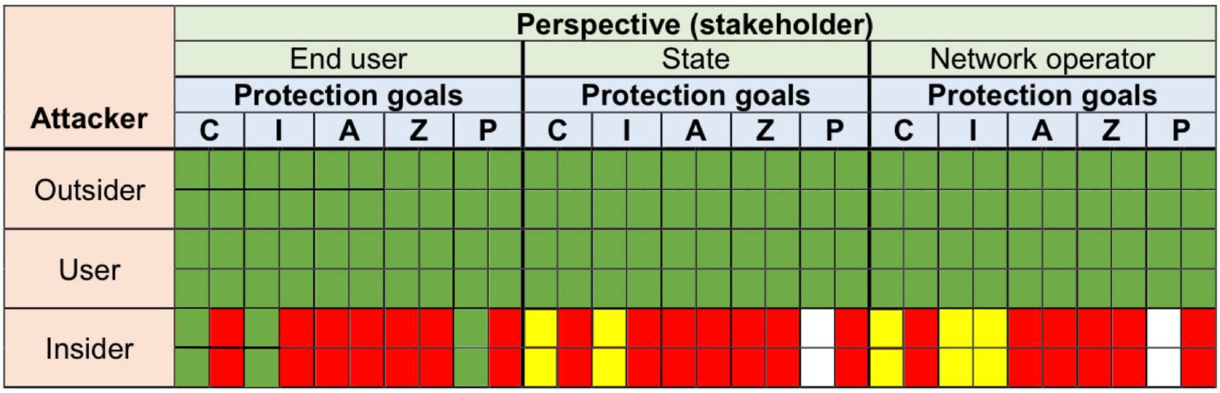
Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Outsider	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
User	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Insider	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥

Figure 38: Risk Analysis of SMO and OCU

3.2.3.3 O-DU and O-RU

The devices under consideration facilitate the transmission of 3GPP data between the UE and the CN. From the Operators' perspective, evaluating these devices is similar to the SMO and O-CU analyses discussed earlier. In the ***bb*** and ***wb*** scenarios, End-to-End UP and CP data are protected between the UE-(O-CU) and UE-AMF, respectively, through optional 3GPP security controls. These control lower(to low risk) the Confidentiality/Integrity/Privacy risks for the End-User, as neither component has access to the decryption keys for UP data. However, despite End-to-End protection for CP data, O-RAN control data and configurations remain unprotected from Insiders, as previously explained in several interface analyses. As a result, the two risks (except for Privacy risk) are elevated to medium for the State stakeholders as it is concerned with the safety of both controls (O-RAN and CP) and UP data.

It shall be noted here that non of the interfaces connecting the O-RU or the O-DU with the SMO allows for accessing the sensitive data located in the SMO's DB [12][6].



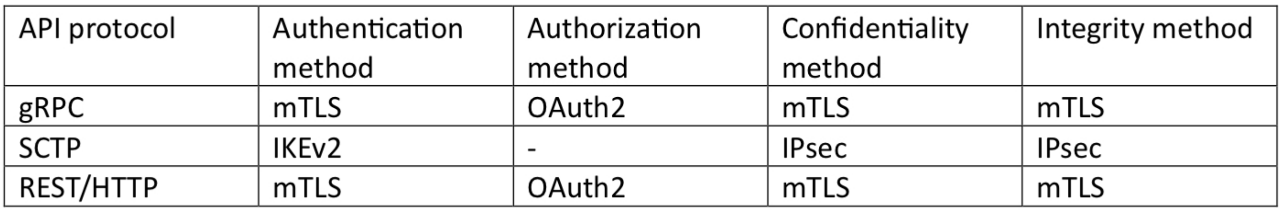
Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Outsider	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
User	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Insider	🟩🟥	🟩🟥	🟥🟥	🟥🟥	🟩🟥	🟨🟥	🟨🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥
	🟩🟥	🟩🟥	🟥🟥	🟥🟥	🟩🟥	🟨🟥	🟨🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥

Figure 39: O-DU and O-RU analysis

3.2.3.4 xApps/rApps

To analyze both types of Apps, it is necessary to consider the security controls implemented by the controllers. Both nRT RIC and non-RT RIC now require support for authorization using OAuth 2.0 to secure the exposed APIs and Services.

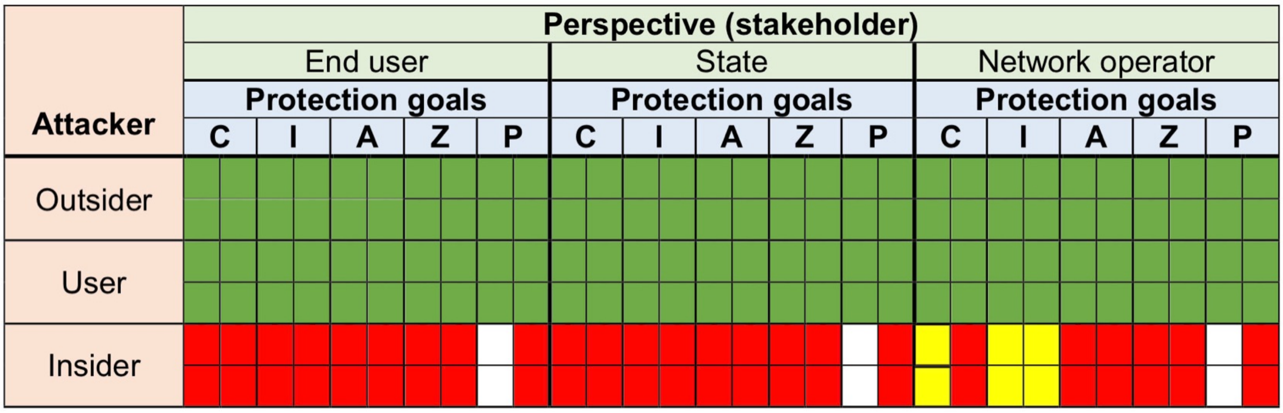
In the case of nRT RIC, additional optional security controls have been implemented to enhance the security of nRT RIC APIs. These controls involve protocols for authorization, authentication, and End-to-End data protection, depending on the type of API (see Fig.40). However, for this analysis, only the optional authorization control provides security improvements, as we assume that the attacker has already gained access to an xApp or rApp. As explained before, authentication and End-to-End protection only provide security from external attackers.



API protocol	Authentication method	Authorization method	Confidentiality method	Integrity method
gRPC	mTLS	OAuth2	mTLS	mTLS
SCTP	IKEv2	-	IPsec	IPsec
REST/HTTP	mTLS	OAuth2	mTLS	mTLS

Figure 40: Security Controls for Near-RT RIC APIs

Although OAuth 2.0 authorization has been adopted for the A1, R1, and thenRT RIC, malicious apps may have already acquired the necessary privileges to access sensitive data. The apps require data to optimize RAN functionality using ML. The rApps may access data in the SMO via the R1 interface, while the xApps may access data in the nRT RIC DB. The data stored in the SMO has been previously discussed. Similarly, the nRT RIC's database contains information collected through E2 nodes, i.e., 3GPP data. Even with optional 3GPP controls in place, UP data is assumed to be decrypted as the nRT RIC may receive the data from the O-CU after decryption. Even if an app is prevented from accessing specific data or services due to authorization control, there is a high risk of an app breaking isolation or elevating its privileges to gain access, as there are no specific security controls to protect against such threats. Furthermore, many apps may be written in unsecured languages, increasing the risk of these attacks. The only effective security control is the Integrity protection provided by 3GPP security controls CP data Integrity. Therefore, we believe the implemented controls are insufficient to improve security, and thus BSI's analysis remains valid. However, the BSI analysis claims that xApps are inside the O-CU instead of the nRT RIC. Thus, if they brake isolation, they might be able to modify 3GPP traffic packets even though this is not true, as xApps may still use the E2 interface to modify traffic on the E2 nodes.



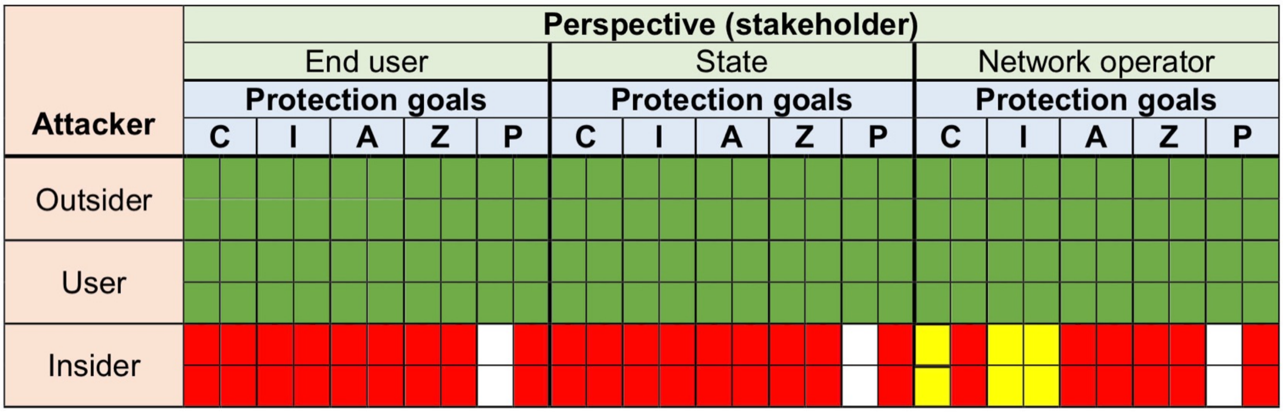
Attacker	Perspective (stakeholder)														
	End user					State					Network operator				
	Protection goals					Protection goals					Protection goals				
	C	I	A	Z	P	C	I	A	Z	P	C	I	A	Z	P
Outsider	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
User	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩	🟩🟩
Insider	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥
	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟥🟥	🟥🟥	🟥🟥	🟥🟥	⬜🟥	🟨🟥	🟨🟨	🟥🟥	🟥🟥	⬜🟥

Figure 41: Updated Risk analysis of rApps/xApps

It is also important to note that the same mistake regarding the Confidentiality of CP data as in the R1 analysis occurred in the (BSI) analysis of the xApps and rApps. As explained in the SMO and O-CU analysis, in ***bb*** and ***wb*** scenarios, optional 3GPP security controls require the encryption of CP data between the UE and the AMF. Nevertheless, this only improves the situation for the Network Operator to a moderate degree since O-RAN control data remains unprotected from Insider attacks. Both analyses presented here fix this mistake.

3.2.3.5 non-RT RIC/nRT RIC

The nRT RIC and non-RT RIC play a crucial role as they host xApps and rApps, respectively, and offer various services to these Apps depending on their specific nature, including data access and configuration management. Given this, it is important to note that the security analysis of the two controllers cannot be better than that of the rApps/xApps themselves. Therefore, we evaluate the security risks of the two controllers to be identical to the xApps/rApps' analysis, as controllers have unlimited access to the interfaces and data stored data. The xApps/rApps analysis already describes a worst-case scenario where the only protection available comes from mandatory 3GPP controls.



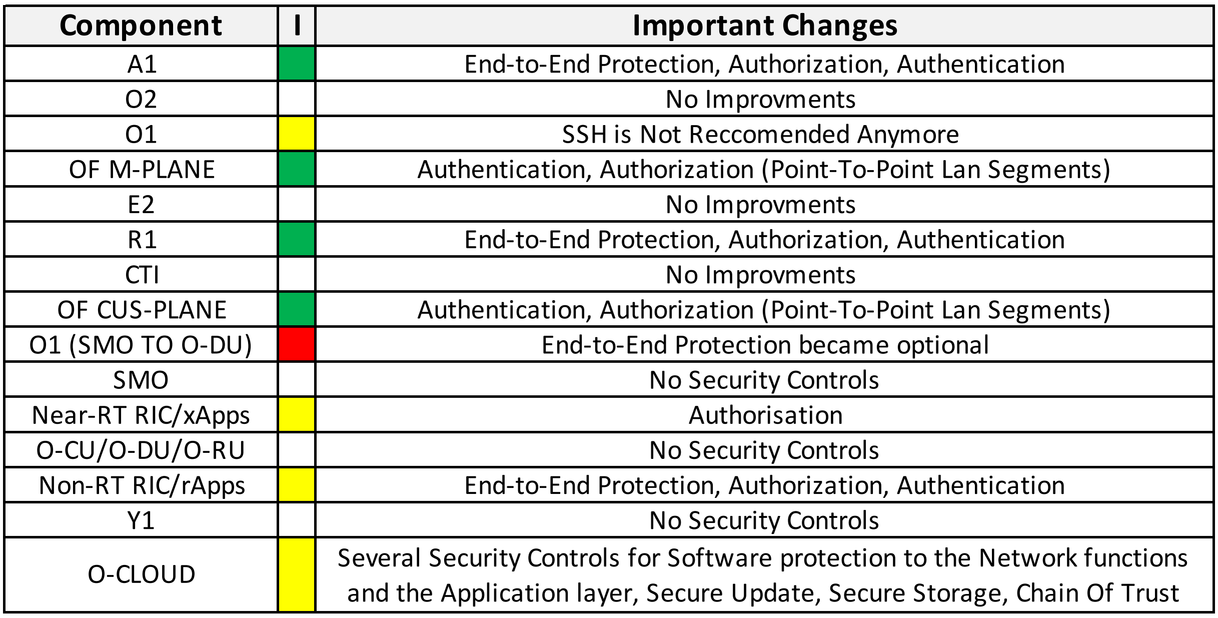
Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
User	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩
Insider	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥
	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	⬜	🟥	🟨	🟥	🟨	🟨	🟥	🟥	🟥	🟥	⬜	🟥

Figure 42: Risk analysis of non-RT RIC and nRT RIC

3.3 Overall Security Assessment of ORAN

The overall security analysis of O-RAN remains unchanged from the previous analysis due to significant deficiencies in the security controls of critical components, namely the SMO and (mainly) the O-Cloud, along with inadequate protection against Insider attackers. It is important to note that even if all interfaces are strongly secured, a malicious SMO or an unprotected O-Cloud compromises the protection goals for every stakeholder, as previously discussed in the analyses. Consequently, presenting a new summarised analysis is unnecessary since the findings and conclusions presented in Section 3.1.3.1 remain valid. The overall assessment underscores that the specifications of O-RAN continue to fall short in following the fundamental principles of "Security by default" and "Zero-Trust".

However, since a new overall analysis is not required, we present a table (Fig.43) to highlight the significant changes concerning the security of each component. In Fig.43, the "Impact"(I) column denotes the level of impact observed. A red entry signifies a negative impact, indicating a decrease in the security level of that component compared to the initial analysis. On the other hand, a green color indicates that the additional security controls or changes implemented have resulted in improved component analysis in at least one scenario. A yellow color is used to signify that although new security controls or improvements have been introduced, their impact on the BSI analysis was deemed insufficient. Lastly, components that were not part of the BSI analysis or whose security specifications remained unchanged over the past two years are represented by white entries. This table is a valuable resource for understanding the key security-related modifications made for each component.



Component	I	Important Changes
A1	🟩	End-to-End Protection, Authorization, Authentication
O2		No Improvments
O1	🟨	SSH is Not Reccomended Anymore
OF M-PLANE	🟩	Authentication, Authorization (Point-To-Point Lan Segments)
E2		No Improvments
R1	🟩	End-to-End Protection, Authorization, Authentication
CTI		No Improvments
OF CUS-PLANE	🟩	Authentication, Authorization (Point-To-Point Lan Segments)
O1 (SMO TO O-DU)	🟥	End-to-End Protection became optional
SMO		No Security Controls
Near-RT RIC/xApps	🟨	Authorisation
O-CU/O-DU/O-RU		No Security Controls
Non-RT RIC/rApps	🟨	End-to-End Protection, Authorization, Authentication
Y1		No Security Controls
O-CLOUD	🟨	Several Security Controls for Software protection to the Network functions and the Application layer, Secure Update, Secure Storage, Chain Of Trust

Figure 43: Significant Changes on The Security of O-RAN Components

3.4 Challenges

Although the assessment method was simple, understanding the O-RAN specification posed challenges. The specification was spread across multiple documents, making it harder to navigate. The main issue, however, was the inconsistencies found within the documents. An example would be the statement that an interface will use End-to-End protection for its traffic while every encryption algorithm is stated as optional (M-Plane is such an example, Fig.33). Another problem arises when components are supposed to follow existing standards for protection, but only a subset of those standards are implemented. The lack of architectural specifications, like a Y1 interface specification, also required us to make assumptions during analysis. Furthermore, the specification does not clearly specify which data will be used/stored for machine learning training. For instance, the SMO document states for the stored data: *"asset-d-25: Training or test data: data sets collected externally or internally from the Near-RT RIC, O-CU and O-DU and passed to the ML training hosts in a ML system"[16].* A clear and explicit clarification is necessary to determine whether CP and UP data is directly utilized by intelligent units to enhance functionality. This clarification is crucial for conducting an accurate security assessment. Lastly, an analysis on the virtualisation is very hard to be performed, as O-Cloud supports many virtualization tools, including VMs, OSs and Containers. Certain tools must be chosen for this purpose, e.g VirutalBox, Linux OS, Kubernetes, so their security can be properly assessed under the O-RAN concept.

3.5 NTIA Analysis

Another important analysis worth mentioning is the risk analysis conducted by the National Telecommunications and Information Administration (NTIA) in May 2023[44]. Our assessment and the NTIA assessment are based on the latest specifications, so it is helpful to compare them. However, that analysis can be characterized as a threat-based analysis, as it examines each currently known threat associated with O-RAN.

To begin with the comparison, both analyses agree that the O-Cloud component of the architecture presents the highest security risk. However, the NTIA assessment overlooks the potential risks associated with the Open Fronthaul interface, a significant concern that should be addressed.

Additionally, the NTIA analysis considers protocols like TLS and IPSec as mandatory, whereas we believe that only the support of these protocols is mandatory. This difference in perspective might be due to the incomplete and unclear nature of the specification, which both analyses recognize.
Furthermore, the NTIA analysis concludes that O-RAN expands the attack threat surface, but not significantly, as only a few threats are exclusively related to O-RAN. They also state that attacks related to virtualization and ML cannot be considered attacks on O-RAN. While we agree with this reasoning, we strongly recommend further research to explore the real-world consequences of ML and virtualization attacks in the context of RAN. The attacks may be known, but their specific impact within the RAN concept cannot be assessed yet.

4 Towards a Practical Risk Analysis

The analysis in the previous section has provided evidence that proved that despite being in development for three years, O-RAN can still be characterized as an architecture with significant security vulnerabilities. Despite undergoing multiple risk analyses and revisions of the security specification, the newly implemented security controls have been proven insufficient over the last years as they failed to enhance the architecture's security. However, this chapter emphasizes the significance of conducting a practical risk analysis before definitively labeling an architecture as unsecured. It describes our initial plan for conducting the first practical risk analysis of O-RAN. Our plan involved the deployment of an O-RAN test lab and introducing a new attack on the Open Fronthaul, which are also presented in this section.

4.1 The Need For A Practical Risk Analysis

Over the years, multiple practical risk analyses have been conducted to assess the security of various components within the mobile network architecture. However, as a relatively new architecture, O-RAN has not yet undergone a practical risk analysis. While a theoretical risk analysis identifies potential vulnerabilities and risks before attackers exploit them, a practical risk analysis evaluates the feasibility and consequences of attacks in real-world scenarios. In contrast to the absence of practical risk analyses, several theoretical risk analyses have been conducted in recent years[35][3][40][42][22].
Several possible explanations for the lack of practical risk analysis have been identified, all stemming from the challenges associated with implementing a real-world setup. One key factor is the frequent updates to the O-RAN architecture specifications, which occur multiple times yearly. This rapid evolution makes vendors hesitant to invest in designing and manufacturing products that may quickly become outdated. Additionally, the cost of deploying an O-RAN network is prohibitively high, mainly due to the absence or inadequate implementation of open solutions.

4.2 Initial Planning

The initial goal of this master's thesis was not a theoretical risk analysis. We aimed to deploy an O-RAN test-lab and assess the promising component's risk. For this reason, the master thesis was split into two major phases:

- **Phase 1** (January-March/2023): Study of the architecture and identification of promising components for a practical risk assessment. A *promising component* is defined as a specific element, interface, or function within the system that exhibits notable vulnerabilities and threats which have not been adequately addressed or considered within the context of O-RAN. Furthermore, during this phase, various options for the different RAN components were explored. Both open-source and commercial solutions were taken into consideration. Additionally, at this step, several attacks were identified and structured (at an abstract level) to be utilized in the subsequent phase.

- **Phase 2** (April-June/2023): Deployment of the O-RAN network and the conduction of the selected attacks. Unfortunately remained incomplete due to reasons elaborated in Sec.4.3. Due to the unexpectedly challenging nature of deploying an O-RAN network, we decide to shift our focus and conduct the theoretical risk analysis of the previous chapter.

A comprehensive examination of each phase is provided in the subsequent chapters. Specifically, regarding the first phase, we explain the rationale behind selecting Open Fronthaul for our practical analysis and present our planned attacks. Particular emphasis is placed on a specific attack that undermines the assertion made by O-RAN specifications regarding the security of 3GPP data during transmission over the Open Fronthaul. Regarding phase two, we provide a detailed discussion on the current state of our setup, including an overview of the components we ultimately select for our configuration.

4.2.1 The Special Case Of Open FrontHaul(CUS-Plane)

In traditional mobile networks, the Fronthaul Interface connects the BBU and Remote Radio Unit (RRU) in a monolithic architecture. The industry introduced and standardized the CPRI protocol to facilitate this connection in 2003. CPRI defined standardized specifications for the transport, connectivity, and control between the BBU physical layer and RRU(a method known as *split 8* (Fig.44)). However, the implementation of CPRI was left almost entirely to the vendors, leading to black-box implementations of the RAN. This semi-proprietary approach allowed for the development of highly optimized solutions but also limited the interoperability of RAN components sourced from different manufacturers.

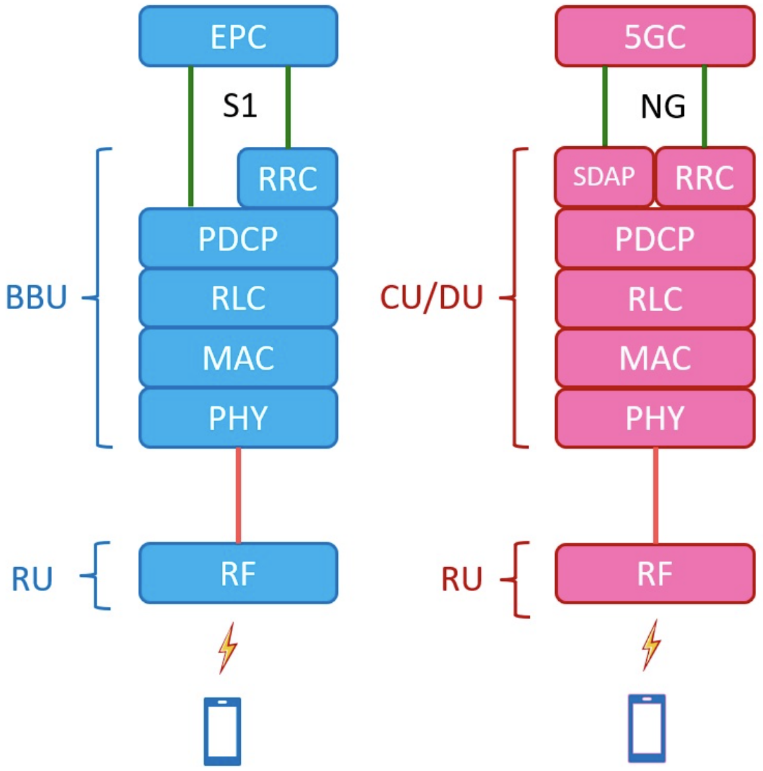


Figure 44: Split 8 (CPRI) [26]

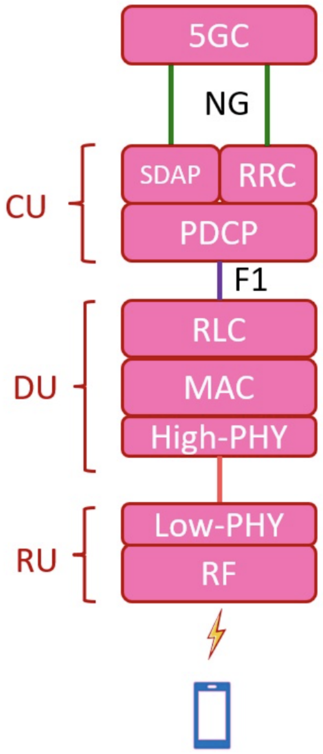


Figure 45: Split 7.2 (eCPRI) [26]

As the O-RAN tries to establish an open architecture for NG-RAN, it incorporates the utilization of a new protocol called evolved Common Public Radio Interface (eCPRI) (eCPRI). eCPRI introduces the capability to divide the physical layer of the BBU or (DU in 5G) into two distinct components known as "High-PHY" and "Low-PHY". This division, formally referred to as the *split 7.2x*(Fig.45), is adopted by O-RAN for its Fronthaul interface. Numerous advancements have been made compared to the previous generation protocol CPRI, yet in our particular scenario, the primary significance lies in the openness of the protocol. More information about the benefits and the design of eCPRI can be found in [66] [25].

Despite the drawbacks associated with the proprietary implementation of the Fronthaul interface, it does offer an additional layer of security to the interfaces. Attacks targeting the Fronthaul interface cannot be classified as "universal" since they are more prone to failure when attempting to compromise the security of a Fronthaul interface implemented by a different manufacturer. Therefore, successful attacks compromise only the RANs developed by the same manufacturer.

In the architecture of O-RAN, the conversion from Fronthaul to an Open Fronthaul interface enables the interoperability between O-DUs and O-RUs produced by different manufacturers. Nonetheless, the open nature of the Open Fronthaul interface exposes it to "Universal" attacks. In other words, if a successful attack is executed, it can be replicated across any O-RAN Fronthaul interface.

Despite the significance of the Open Fronthaul interface, the O-RAN specifications do not enforce any mandatory security controls for this interface. Moreover, the available optional security controls only pertain to the "C and S-Planes," leaving the U plane entirely unprotected. The security of the U plane is claimed to be guaranteed by the security controls defined by the 3GPP. However, the mandatory security controls of 3GPP only ensure Integrity protection for the CP data. The optional security controls offer encryption and Integrity protection for both UP and encryption for CP data transmitted over the Fronthaul interface. The responsibility for implementing these controls lies with the Network Operators. A recent publication by LaSierra et al. (2023) [37] reveals that none of the Network Operators surveyed in European and Asian countries have implemented integrity protection for UP (User Plane) data. Furthermore, the study also found that some of these operators do not even implement encryption for UP data.

Additionally, 5G campus networks can be used to control machines in industrial facilities, including manufacturing robots. In such environments, real-time communication is crucial, and any added latency can lead to issues in the production cycle. In such cases, the optional security controls are usually not implemented. The compromised security of the Open Fronthaul interface and dependence on optional security protocols provided by the 3GPP specifications are the primary factors we considered in selecting the Open Fronthaul for our practical risk analysis. The indivisible nature of Open Fronthaul within the architecture and the assurance that it would be one of the first O-RAN interfaces to be implemented by vendors further reinforce our decision.

4.2.2 Attacking the Open Fronthaul (CUS-Plane)

This section presents our concepts for attacking the O-RAN Fronthaul interface, providing a brief overview of generic attacks. However, a specific attack exploiting the absence of 3GPP security controls will be explained in detail. This detailed explanation is crucial as it challenges the claims made by O-RAN regarding the security of Fronthaul's U-Plane data under the protection of 3GPP security controls.

4.2.2.1 Attacking The U-Plane

An abstract version of an identified attack on the U-Plane of the Open Fronthaul interface is presented here. The technical details of this attack are explained in the Sec.6. This attack aims to demonstrate to the O-RAN community that relying solely on optional security controls provided by 3GPP cannot guarantee adequate protection. By highlighting the vulnerabilities in the U-Plane, we aim to emphasize the need for stronger security measures and mandatory controls in the O-RAN architecture.

A.The Alter Attack

Academic research published in 2019 identified three attack vectors, two passive and one active, for the Long Term Evolution (LTE) data link layer [49]. The active attack was named aLTEr attack and exploited the fact that in 4G-LTE, there is no Integrity protection for the UP data. The attack requires the construction of a relay in order to intercept packets as they are being transmitted over the wireless Uu interface. This attack can be described as Man In The Middle (MITM) attack, as the relay impersonates the UE towards the gNB and vice versa. The attack involved the modification of Domain Name Server (DNS) traffic in order to redirect the User to a malicious website.

The attack is visually illustrated in Fig.46, which depicts the attack process divided into five distinct stages. In the first stage, the malicious relay acts as a pass-through device, simply forwarding packets in both directions until the Authentication and Key Agreement (AKA) process is completed. AKA is a mechanism utilized in mobile networks to authenticate the UE towards the CN and vice versa. Once the UE attempts to establish a connection with a web server, a DNS request is transmitted over the network to a DNS server. The DNS server is responsible for matching the domain name of the website with its corresponding Internet Protocol (IP) address and returning it to the UE. In this attack scenario, it is assumed that the User Equipment (UE) encrypts the DNS traffic using stream generation algorithms, specifically AES-CTR [38]. When the malicious gNB detects a DNS request packet, it alters the destination IP address(the IP of the legitimate DNS server), replacing it with the IP address of a malicious DNS server that the attackers have established. To manipulate the encrypted data, the authors employ a technique called a "known plaintext attack." Since the structure of DNS packets is known, and the IP address of the default DNS server of the Operator can be obtained, the authors create a mask represented as $'mask = m \; xor \; m'$, where m represents the expected decrypted DNS request, and m' represents the intended manipulated malicious decrypted DNS request. By XORing this mask with the ciphertext, a new ciphertext is generated. Based on the design of steam ciphers, when this new ciphertext is decrypted, it will yield the intended manipulated malicious decrypted DNS request. Subsequently, the malicious DNS server redirects the phone to a website under the control of the attackers rather than the intended legitimate website. Upon receiving the response from the malicious server, the malicious relay modifies the source IP address to match the IP address of the legitimate DNS server. Additionally, it manipulates several bits in the IP/UDP fields, ensuring that checksum controls cannot detect the manipulation. These bit alterations are performed in non-significant fields of the IP/UDP headers.

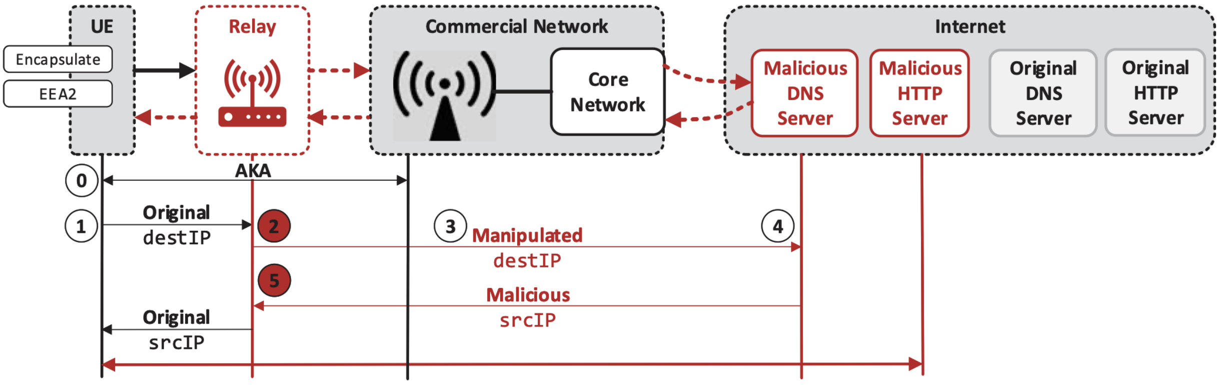


Figure 46: The aLTEr Attack[49]

Significant challenges in conducting the attack, mentioned in the paper include:

- Force the UE to connect to the malicious gNB
- Maintain a stable Radio Connection
- Detect the DNS traffic
- Modify the DNS destination/source IP address, while ensuring that the checksum values remain valid

A potential method to compel the UE to connect to the malicious gNB involves overshadowing the signal emitted by the commercial gNB. However, this approach carries the risk of the malicious relay inadvertently connecting to itself. Additionally, maintaining a stable connection in this scenario necessitates prior knowledge of the configurations of the commercial gNB. In our assessment, these factors make the execution of the attack challenging in a real-world scenario but not infeasible as similar attacks have been performed.

While the aLTEr attack can be performed over the air, conducting such attacks within the O-RAN infrastructure offers scalability to a larger number of end devices. Consequently, it is essential to undertake a practical evaluation to estimate the associated efforts involved in executing this attack. In contrast, a similar attack conducted over a physical interface like the Open Fronthaul eliminates challenges related to setting up a relay, "tricking" the UE to connect to the relay, and intercepting packets during their transmission over the air.

B.Spoofing Attack on the Open Fronthaul

The absence or weak protection controls, particularly in the U-Plane and the O-RU of the Open Fronthaul, create multiple avenues through which an attacker can gain access to the interface. The O-RU, as explained briefly in Sec.4.2, is now implementing some functionalities of the physical layer. This implementation makes the O-RU future-proof, as the software component of O-RU allows for updates and the implementation of new capabilities. Research is currently being conducted on fully virtualized O-RU implementations. This introduces a potential vulnerability wherein an attacker could inject malicious code into the O-RU unit. A similar situation arises for the O-DU unit, where the virtualized nature opens up possibilities for code injection attacks. The most realistic scenario for an attack on the Open Fronthaul is a genuine man-in-the-middle attack. A similar approach to the aLTEr attack can be employed, wherein the attacker impersonates the O-RU towards the O-DU and vice versa. In contrast with CPRI, eCPRI as a packet-based protocol enables an Ethernet connection between the O-RU and O-DU. Therefore a straightforward setup involving a Linux machine (e.g., a Raspberry Pi) equipped with two Ethernet connections can be positioned between the two devices. These options for a MITM are depicted in Fig.47.

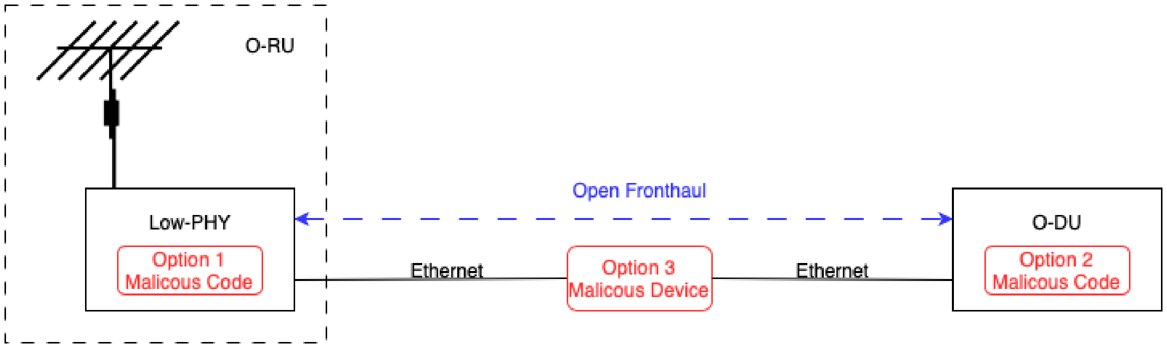


Figure 47: MITM Options For Attacking the Interface

Another important consideration regarding the Open Fronthaul is that it is the only interface physically exposed to potential attackers. Gaining physical access to this interface is possible because the O-RUs are often located in exposed areas. Therefore, additional security controls should be implemented to safeguard the interface, such as secure and authorized access to the location of the O-RU. The lack of specifications regarding the physical security of this component increases the risk of a potential attack. Furthermore, one of the key characteristics of 5G is the introduction of small cells(for higher speeds), which may operate at frequencies up to 100 GHz [46]. These cells are considerably smaller than those used in previous generations of networks. As a result, a larger number of radio units must be deployed to cover the same corresponding area, leading to an increased number of possible access points for an attacker. Fig.48 depicts this scenario. Lastly, it is worth noting that the M-Plane, responsible for the software updates of the O-RU, may be unsecured due to the lack of mandatory controls. This only increases the risk as it may be another access point for attackers. An update manipulation may allow the installation of malicious code inside the O-RU. A successful establishment of a MITM in the Open Fronthaul can be catastrophic in scenarios where real-time communication is crucial. The optional 3GPP security controls are not implemented, as U-Plane, which is responsible for the transportation of both UP and CP data, remains entirely unprotected. The benefits of a

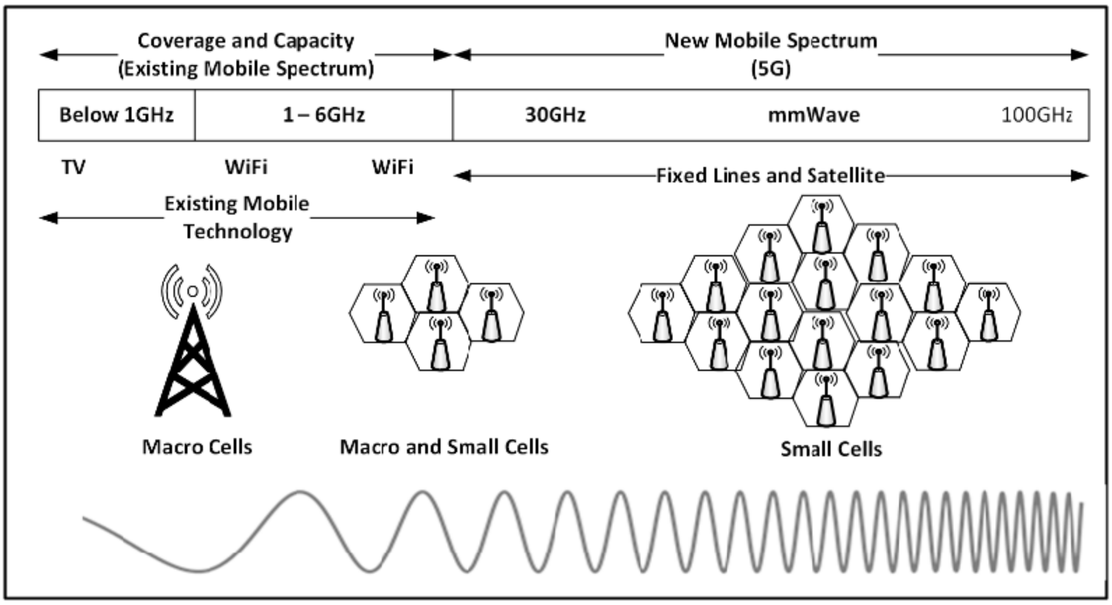


Figure 48: 5G Spectrum and Cells[46]

spoofing attack over the Open Fronthaul are summarised in Tab.3.

Table 3: Benefits of A Spoofing Attack on the Open Fronthaul over Fonthaul and aLTEr Attacks

Fronthaul Interface	Over The Air Spoofing(aLTEr)	General Benefits
Attacks can be Replicated in any Open Fronthaul	OTA Interception is Challenging	Unsecured U-Plane (No Security Controls)
No Prior Knowledge Required	No Prior Knowledge Required	Multiple Points of Access
Better Scalability	No Advanced Setup Required	Exposed Physical Interface
-	Better Scalability	Potentially Unsecured S and C Planes (Only Optional Security Controls)

C.Consequences

Since we could not successfully deploy our o-RAN test lab, we rely on the results of our Internship project to demonstrate the potential consequences of an attack on the Open Fronthaul U-Plane. Our Internship project aimed to conduct a spoofing attack on commands transmitted to a robotic arm over a 5G network. This simulated a factory environment where robotic arms are utilized for time-critical tasks, and as a result, the optional security controls specified by 3GPP were not implemented. It should be noted that this attack is considered "cheated" since the modification of packets occurred after they exited the core network. For more detailed information about the internship project, please refer to the document provided here. During the internship, we successfully executed a spoofing attack on the U-Plane data, and a video showcasing the attack can be accessed through this link. The video demonstrates that access to unprotected UP data can result in payload modification, as mandatory encryption or Integrity protection controls are not provided by 3GPP. Even if the data is encrypted, the attacker can bypass the encryption using the method employed in the aLTEr attack. We utilized the internship report as clear evidence to highlight the severe consequences, as we were able to alter the commands sent to the robotic arm during that project. An attack on the Open Fronthaul is almost identical to the attack presented in the internship report, with the only difference being that the modification of the packets is taking place over the Fronthaul interface, and thus an eCPRI decoder will be required.

4.2.2.2 Generic Attacks on the S and C Plane

Although the CS-Planes and M-Plane offer some authorization mechanisms, a MITM attacker can still carry out attacks due to the absence of mandatory Integrity protection for the data transmitted through these interfaces. Only in the case of the S-Plane, the Integrity protection is optional. Our plan for these interfaces mainly revolves around attacking the Availability of the RAN. The planned attacks include:

1. Flooding the S-Plane with random data to achieve desynchronization between the O-RU and the O-DU, as desynchronized components degrade the QoS.
2. Intercepting CL/DL traffic to cause a complete loss of Availability, as any delay or blockage of this packet will force the O-RU to drop the traffic.

These attacks aim to disrupt the proper functioning of the RAN, potentially leading to service unavailability and operational issues. The physical access to the interface bypasses any authentication ad authorization controls, and the data are not End-to-End Integrity protected encrypted.

4.2.3 Deploying an OPEN-RAN Test Lab

After conceiving an abstract version of our attacks, we focus on deploying an O-RAN compliant RAN. This section describes the process we follow to deploy an O-RAN compliant RAN.

4.2.3.1 Requirements

For our purposes, only the basic components are required, namely an O-RU, an O-CU, and an O-DU apart from the 5G components:UE and CN. Other functions and components, such as an nRT RIC or the SMO, are optional, only meant to enhance the quality of service offered by the RAN while providing other necessary functionalities like orchestration and management. Despite this fact, as open-source nRT RICs are already available, we decide to include a controller in our setup for a future security analysis of the ML aspect of O-RAN. This selection would not only facilitate the analysis of the Open Fronthaul but also enable future investigations into the ML aspects of O-RAN. Attacks targeting the ML component involve the injection of poorly trained models into the nRT RIC and xApps. Given that the controller plays a crucial role in critical functions such as Network Slicing, evaluating the consequences of such attacks in a real world-Environment is important.

4.2.3.2 Selecting The Components

One of the critical tasks in deploying any setup is the selection of components. Several factors and restrictions come into play, including cost considerations and the future-proofness of the chosen components. We evaluate open-source and commercial implementations for the O-DU and O-CU components during the selection process. However, due to the current lack of virtualized O-RUs and the limited support for the Open Fronthaul interface in software-defined radios, we determined that a commercial solution was the only viable option for our deployment. For reasons analyzed in the Sec.4.3, we decide to use open source implementations for the O-CU and O-DU.

Table 4: Components

Comp	Out Choice	Alternatives
CN	Free5GC[54]	Open5GS[61], OAI CN[60]
O-CU	OAI CU[27]	AirSpan vCU[51], SRS CU[63]
O-DU	OAI DU[27]	AirSpan vDU[51], SRS DU[63]
O-RU	Benetel RAN550[52]	Mavenir Openbeam RRUs[59]
nr-RIC	FLEX RIC [28]	AirSpan RIC[51], SD-RAN RIC[62]
UE	COTS UE	Any 5G UE

The Open Air Interface (OAI) offers open-source CU and DU components, which are regularly updated to incorporate various O-RAN interfaces. Considering OAI's recent demonstration of Open Fronthaul implementation, we choose to utilize these units in the Mobile World Congress and the plan of OAI to support the Open Fronthaul by March/2023. Another relevant project is FlexRIC, developed by the MOSAIC5G Group Project, which serves as a nRT RIC and implements the O-RAN E2 interface. To handle the Core Network functions, we employ the distributed version of Free5GC, deployed on a Kubernetes cluster. Free5GC is an open-source CN that adheres to the 3GPP specifications, and its distributed deployment, which we use in our setup, closely resembles real-world scenarios, providing a more realistic testing environment. Commercial products utilized in our setup include a Benetel-manufactured O-RU, supporting the 7.2x O-RAN split, and a Commercial Of The Shelf (COTS) UE comprising an Android smartphone and a programmable SIM card.

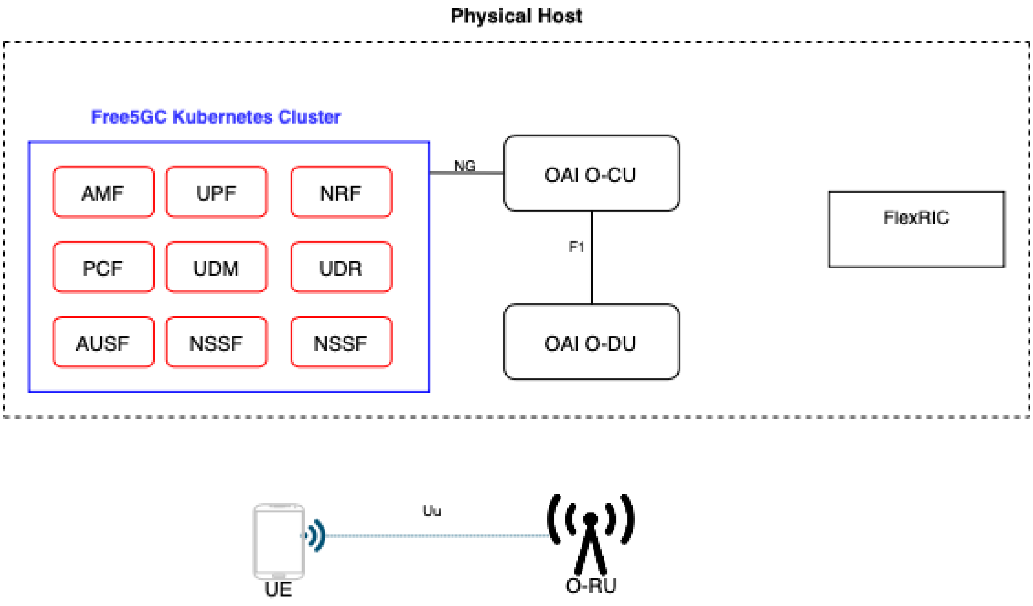
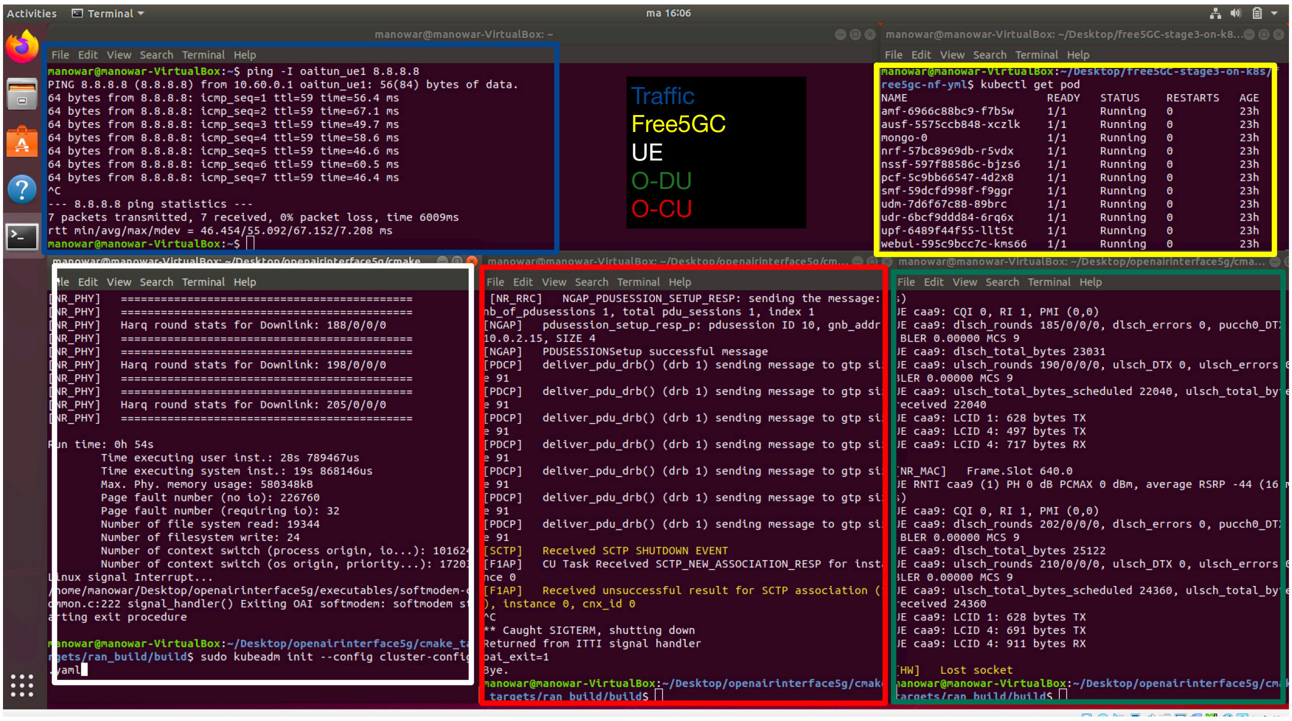


Figure 49: Deployment

4.2.3.3 Deployment of the Components

To deploy our setup, we utilize a physical host, where all of the network functions are running as processes within it. Each network function is assigned to a unique Kubernetes Pod, allowing for individual IP addresses to be assigned to each. The AMF and UPF are configured to connect with the O-CU in order to handle the control plane and User plane transfers between the UE and the CN, respectively. The O-CU and O-DU are connected via the F1 interface.

A visual representation of our deployment is illustrated in Fig.49. However, it is important to note that currently, the O-RU is not connected to the O-DU, and the controller is not connected to either the O-CU or the O-DU (Open Distributed Unit). The reasons behind this are explained later in the challenges section (4.3). However, to ensure connectivity between the components, we can use a virtual UE and the RF simulator offered by OAI. A video demonstrating the connectivity between the UE and the CN can be found in this Link. Moreover, we recommend referring to Fig.50, which identifies the various components, before watching the video.


Activities
Terminal
ma 16:06
Traffic
Free5GC
UE
O-DU
O-CU
manowar@manowar-VirtualBox: ~
manowar@manowar-VirtualBox: ~/Desktop/free5GC-stage3-on-k8...
manowar@manowar-VirtualBox: ~/Desktop/openairinterface5g/cmake...
manowar@manowar-VirtualBox: ~/Desktop/openairinterface5g/cm...
manowar@manowar-VirtualBox: ~/Desktop/openairinterface5g/cma...
File Edit View Search Terminal Help

```
manowar@manowar-VirtualBox:~$ ping -I oaitun_ue1 8.8.8.8
PING 8.8.8.8 (8.8.8.8) from 10.60.0.1 oaitun_ue1: 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=56.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=59 time=67.1 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=59 time=49.7 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=59 time=58.6 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=59 time=46.6 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=59 time=60.5 ms
64 bytes from 8.8.8.8: icmp_seq=7 ttl=59 time=46.4 ms
^C
--- 8.8.8.8 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6009ms
rtt min/avg/max/mdev = 46.454/55.092/67.152/7.208 ms
manowar@manowar-VirtualBox:~$
```

```
manowar@manowar-VirtualBox:~/Desktop/free5GC-stage3-on-k8s/f
ree5gc-nf-yml$ kubectl get pod
NAME                        READY   STATUS    RESTARTS   AGE
amf-6966c88bc9-f7b5w        1/1     Running   0          23h
ausf-5575ccb848-xczlk       1/1     Running   0          23h
mongo-0                     1/1     Running   0          23h
nrf-57bc8969db-r5vdx        1/1     Running   0          23h
nssf-597f88586c-bjzs6       1/1     Running   0          23h
pcf-5c9bb66547-4d2x8        1/1     Running   0          23h
smf-59dcfd998f-f9ggr        1/1     Running   0          23h
udm-7d6f67c88-89brc         1/1     Running   0          23h
udr-6bcf9ddd84-6rq6x        1/1     Running   0          23h
upf-6489f44f55-llt5t        1/1     Running   0          23h
webui-595c9bcc7c-kms66      1/1     Running   0          23h
```

```
[NR_PHY]   ==========================================
[NR_PHY]   ==========================================
[NR_PHY]   Harq round stats for Downlink: 188/0/0/0
[NR_PHY]   ==========================================
[NR_PHY]   ==========================================
[NR_PHY]   Harq round stats for Downlink: 198/0/0/0
[NR_PHY]   ==========================================
[NR_PHY]   ==========================================
[NR_PHY]   Harq round stats for Downlink: 205/0/0/0
[NR_PHY]   ==========================================

Run time: 0h 54s
        Time executing user inst.: 28s 789467us
        Time executing system inst.: 19s 868146us
        Max. Phy. memory usage: 580348kB
        Page fault number (no io): 226760
        Page fault number (requiring io): 32
        Number of file system read: 19344
        Number of filesystem write: 24
        Number of context switch (process origin, io...): 101624
        Number of context switch (os origin, priority...): 17203
Linux signal Interrupt...
/home/manowar/Desktop/openairinterface5g/executables/softmodem-c
ommon.c:222 signal_handler() Exiting OAI softmodem: softmodem st
arting exit procedure

manowar@manowar-VirtualBox:~/Desktop/openairinterface5g/cmake_ta
rgets/ran_build/build$ sudo kubeadm init --config cluster-config
.yaml
```

```
 [NR_RRC]   NGAP_PDUSESSION_SETUP_RESP: sending the message:
nb_of_pdusessions 1, total pdu_sessions 1, index 1
[NGAP]   pdusession_setup_resp_p: pdusession ID 10, gnb_addr
10.0.2.15, SIZE 4
[NGAP]   PDUSESSIONSetup successful message
[PDCP]   deliver_pdu_drb() (drb 1) sending message to gtp si
e 91
[PDCP]   deliver_pdu_drb() (drb 1) sending message to gtp si
e 91
[PDCP]   deliver_pdu_drb() (drb 1) sending message to gtp si
e 91
[PDCP]   deliver_pdu_drb() (drb 1) sending message to gtp si
e 91
[PDCP]   deliver_pdu_drb() (drb 1) sending message to gtp si
e 91
[PDCP]   deliver_pdu_drb() (drb 1) sending message to gtp si
e 91
[PDCP]   deliver_pdu_drb() (drb 1) sending message to gtp si
e 91
[SCTP]   Received SCTP SHUTDOWN EVENT
[F1AP]   CU Task Received SCTP_NEW_ASSOCIATION_RESP for insta
nce 0
[F1AP]   Received unsuccessful result for SCTP association (
), instance 0, cnx_id 0
^C
** Caught SIGTERM, shutting down
Returned from ITTI signal handler
oai_exit=1
Bye.
manowar@manowar-VirtualBox:~/Desktop/openairinterface5g/cmake
 targets/ran build/build$
```

```
s)
JE caa9: CQI 0, RI 1, PMI (0,0)
JE caa9: dlsch_rounds 185/0/0/0, dlsch_errors 0, pucch0_DTX
 BLER 0.00000 MCS 9
JE caa9: dlsch_total_bytes 23031
JE caa9: ulsch_rounds 190/0/0/0, ulsch_DTX 0, ulsch_errors 0
BLER 0.00000 MCS 9
JE caa9: ulsch_total_bytes_scheduled 22040, ulsch_total_byte
received 22040
JE caa9: LCID 1: 628 bytes TX
JE caa9: LCID 4: 497 bytes TX
JE caa9: LCID 4: 717 bytes RX

[NR_MAC]   Frame.Slot 640.0
JE RNTI caa9 (1) PH 0 dB PCMAX 0 dBm, average RSRP -44 (16 m
s)
JE caa9: CQI 0, RI 1, PMI (0,0)
JE caa9: dlsch_rounds 202/0/0/0, dlsch_errors 0, pucch0_DTX
 BLER 0.00000 MCS 9
JE caa9: dlsch_total_bytes 25122
JE caa9: ulsch_rounds 210/0/0/0, ulsch_DTX 0, ulsch_errors 0
BLER 0.00000 MCS 9
JE caa9: ulsch_total_bytes_scheduled 24360, ulsch_total_byte
received 24360
JE caa9: LCID 1: 628 bytes TX
JE caa9: LCID 4: 691 bytes TX
JE caa9: LCID 4: 911 bytes RX

[HW]   Lost socket
manowar@manowar-VirtualBox:~/Desktop/openairinterface5g/cmak
targets/ran build/build$
```

Figure 50: Identification of Components in the Physical Host

4.3 Challenges

This section analyzes the challenges encountered during this thesis. The challenges were solely related to the deployment of the O-RAN test lab, which ultimately forced us to change the topic of our project and postpone our planned risk analysis for the future. However, these challenges also motivated us to submit a poster to the ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2023). More information about the poster is presented later in Sec.4.4.

4.3.1 Cost and not Interoperable Hardware

The initial challenge we faced was the high cost of O-RAN components. A fully equipped O-RAN-compliant gNB was priced at approximately 30,000 euros. Moreover, the lack of concrete designs and clear specifications for several O-RAN interfaces resulted in different vendors implementing these interfaces with their own interpretations and variations of O-RAN standards. This situation created contradictions and discrepancies among hardware vendors, where one vendor claimed compatibility between their O-CU product and another vendor's O-DU, while the other vendor claimed non-compatibility between the two products. In our opinion, it is not justifiable for two products to claim O-RAN compliance if they are not interoperable, as interoperability is one of the fundamental objectives of the O-RAN architecture. The whole purpose of O-RAN is to enable seamless integration and compatibility among different components and vendors within the RAN ecosystem. If two products cannot work together as intended within the O-RAN framework, claiming compliance would be misleading and counterproductive to the goals of the architecture. It is crucial for vendors to ensure true interoperability and adherence to O-RAN standards to provide customers with reliable and efficient O-RAN solutions. These contradictions raised concerns about investing a significant amount of money in a system that might not be properly implemented or standardized.

To address this challenge, we opted to utilize open-source implementations for the O-CU and O-DU components. This decision allowed us to reduce costs significantly as we only needed to acquire an O-RU, which typically costs around 10,000 euros. By leveraging open-source implementations, we aimed to ensure compatibility and adherence to O-RAN standards while mitigating the risks associated with vendor-specific interpretations. Furthermore, using open source implementations is considered future-proof, as it offers advantages such as easier and faster implementation of new standards. By relying on software-based solutions, open-source implementations have the flexibility to adapt and incorporate updates and enhancements as new standards and specifications emerge.

4.3.2 Software Related Challenges

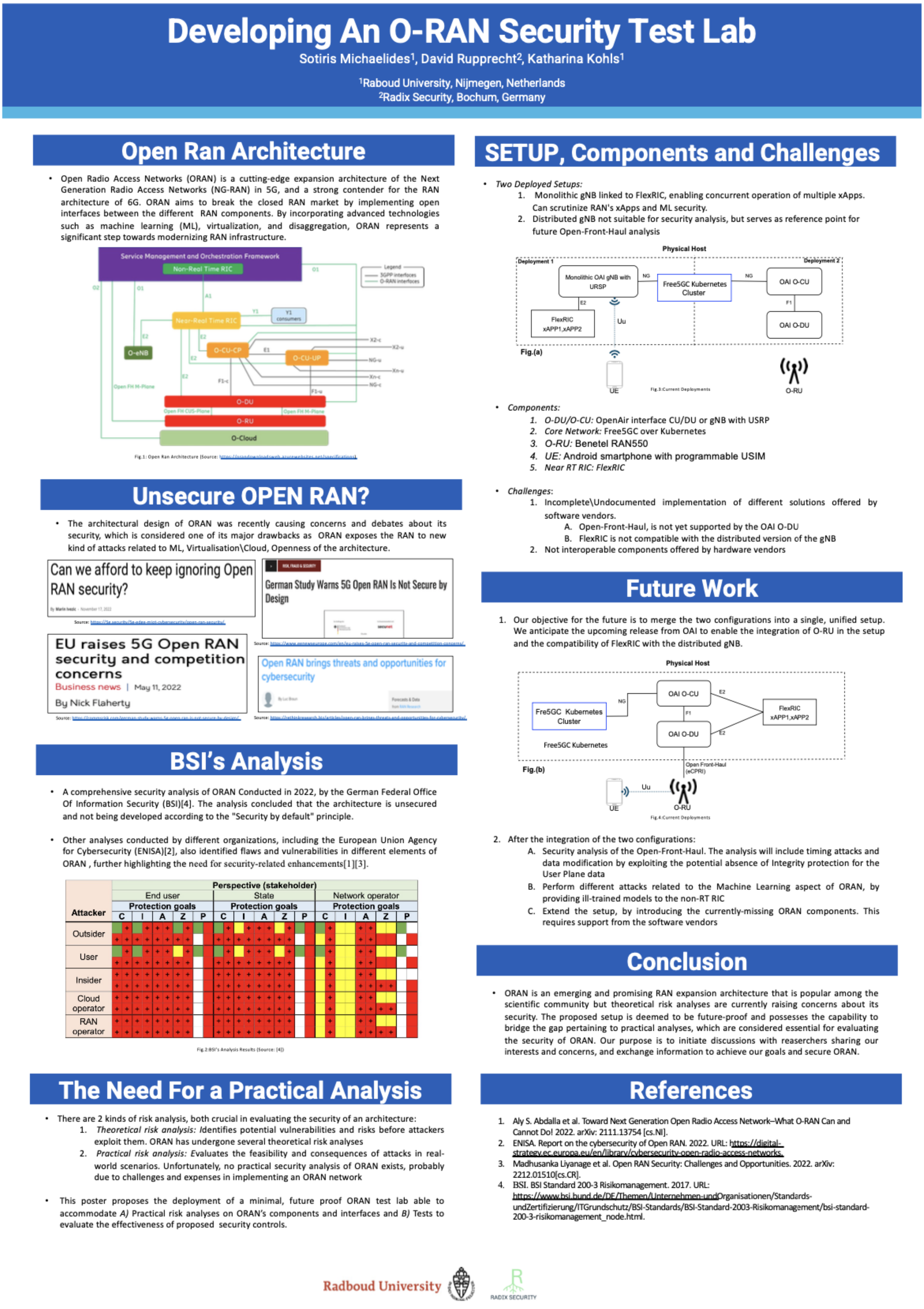
As previously explained, we decided to utilize open-source O-CU and O-DU vendors. Our research identified three main open-source O-RAN software developers: SRS (Software Defined Radios), OAI (Open Air Interface), and the O-RAN Alliance software community. Initially, we considered the O-RAN community a potential option, but we excluded it due to incomplete implementation for the O-DU. Considering the available options, we had to choose between SRS and OAI. During our evaluation in late January, it was anticipated that SRS would release an O-RAN-compliant distributed gNB in March. However, OAI was already offering the distributed version of the gNB and had plans to support the Open Fronthaul interface by the end of March, as indicated on their website.

Based on the evaluation, we proceeded with the implementation of OAI, considering it the most promising option at that time. However, the anticipated update for Open Fronthaul support from OAI did not materialize, despite their website indicating plans to support it by the end of March. Consequently, we have been unable to establish a connection between the O-RU and the O-DU in our setup. Additionally, the E2 interface is only supported in the case of a monolithic gNB and not in the ORAN distributed version, which prevents the O-CU and O-DU from connecting to the nRT RIC.

Regarding SRS, they released their proclaimed O-RAN-compliant O-CU and O-DU as planned. However, upon examining the code and discussing it with the developers, it was discovered that none of the O-RAN interfaces were implemented. Their solution only supports the O1 interface, with plans to implement the others in the future.

Furthermore, Inspecting every developer's code was very often necessary to understand the different implemented protocols or the deployment configurations. The bad documentation and the invalid branches on GitHub only worsened the situation. Despite the promises made by developers, support for the Open Fronthaul interface is still unavailable. As a result, we were unable to deploy our O-RAN test lab as planned initially. In light of this limitation, we made the decision to shift our focus toward conducting an updated theoretical risk analysis of the architecture.

4.4 WiSec Poster



Developing An O-RAN Security Test Lab

Sotiris Michaelides[1], David Rupprecht[2], Katharina Kohls[1]

[1]Raboud University, Nijmegen, Netherlands
[2]Radix Security, Bochum, Germany

Open Ran Architecture

- Open Radio Access Networks (ORAN) is a cutting-edge expansion architecture of the Next Generation Radio Access Networks (NG-RAN) in 5G, and a strong contender for the RAN architecture of 6G. ORAN aims to break the closed RAN market by implementing open interfaces between the different RAN components. By incorporating advanced technologies such as machine learning (ML), virtualization, and disaggregation, ORAN represents a significant step towards modernizing RAN infrastructure.

Fig.1: Open Ran Architecture (Source: https://orandownloadsweb.azurewebsites.net/specifications)

Unsecure OPEN RAN?

- The architectural design of ORAN was recently causing concerns and debates about its security, which is considered one of its major drawbacks as ORAN exposes the RAN to new kind of attacks related to ML, Virtualisation\Cloud, Openness of the architecture.

Can we afford to keep ignoring Open RAN security?

By Marin Ivezic - November 17, 2022

Source: https://5g.security/5g-edge-miot-cybersecurity/open-ran-security/

RISK, FRAUD & SECURITY

German Study Warns 5G Open RAN Is Not Secure by Design

Source: https://www.eenewseurope.com/en/eu-raises-5g-open-ran-security-and-competition-concerns/

EU raises 5G Open RAN security and competition concerns

Business news | May 11, 2022

By Nick Flaherty

Source: https://commsrisk.com/german-study-warns-5g-open-ran-is-not-secure-by-design/

Open RAN brings threats and opportunities for cybersecurity

By Luc Braun

Forecasts & Data from RAN Research

Source: https://rethinkresearch.biz/articles/open-ran-brings-threats-and-opportunities-for-cybersecurity/

BSI's Analysis

- A comprehensive security analysis of ORAN Conducted in 2022, by the German Federal Office Of Information Security (BSI)[4]. The analysis concluded that the architecture is unsecured and not being developed according to the "Security by default" principle.

- Other analyses conducted by different organizations, including the European Union Agency for Cybersecurity (ENISA)[2], also identified flaws and vulnerabilities in different elements of ORAN , further highlighting the need for security-related enhancements[1][3].

Attacker	Perspective (stakeholder)																													
	End user										State										Network operator									
	Protection goals										Protection goals										Protection goals									
	C		I		A		Z		P		C		I		A		Z		P		C		I		A		Z		P	
Outsider	🟩	+	🟩	+	+	+	🟩	+	🟩	🟥	🟩	+	🟨	+	+	+	🟨	+	🟩	🟥	🟩	+	🟨	🟨	+	+	🟨	🟨	🟩	⬜
	+	+	+	+	+	+	+	+	⬜	🟥	+	+	+	+	+	+	+	+	⬜	🟥	🟨	+	🟨	🟨	+	+	🟥	🟥	⬜	🟥
User	🟩	+	🟩	+	+	+	🟨	+	🟩	🟥	🟩	+	🟨	+	+	+	🟨	+	🟩	🟥	🟩	+	🟨	🟨	+	+	🟨	🟨	🟩	⬜
	+	+	+	+	+	+	+	+	⬜	🟥	+	+	+	+	+	+	+	+	⬜	🟥	🟨	+	🟨	🟨	+	+	🟥	🟥	⬜	🟥
Insider	+	+	+	+	+	+	+	+	⬜	🟥	+	+	+	+	+	+	+	+	⬜	🟥	🟨	+	🟨	🟨	+	+	🟨	🟨	⬜	⬜
	+	+	+	+	+	+	+	+	⬜	🟥	+	+	+	+	+	+	+	+	⬜	🟥	🟨	+	🟨	🟨	+	+	+	+	⬜	🟥
Cloud operator	+	+	+	+	+	+	+	+	⬜	🟥	+	+	+	+	+	+	+	+	⬜	🟥	🟨	+	🟨	🟨	+	+	🟨	🟨	⬜	🟥
	+	+	+	+	+	+	+	+	⬜	🟥	+	+	+	+	+	+	+	+	⬜	🟥	🟨	+	🟨	🟨	+	+	+	+	⬜	🟥
RAN operator	+	+	+	+	+	+	+	+	⬜	🟥	+	+	+	+	+	+	+	+	⬜	🟥	🟨	+	🟨	🟨	+	+	🟨	🟨	⬜	🟥
	+	+	+	+	+	+	+	+	⬜	🟥	+	+	+	+	+	+	+	+	⬜	🟥	🟨	+	🟨	🟨	+	+	+	+	⬜	🟥

Fig.2:BSI's Analysis Results (Source: [4])

The Need For a Practical Analysis

- There are 2 kinds of risk analysis, both crucial in evaluating the security of an architecture:
  1. *Theoretical risk analysis: I*dentifies potential vulnerabilities and risks before attackers exploit them. ORAN has undergone several theoretical risk analyses
  2. *Practical risk analysis: E*valuates the feasibility and consequences of attacks in real-world scenarios. Unfortunately, no practical security analysis of ORAN exists, probably due to challenges and expenses in implementing an ORAN network

- This poster proposes the deployment of a minimal, future proof ORAN test lab able to accommodate *A)* Practical risk analyses on ORAN's components and interfaces and *B)* Tests to evaluate the effectiveness of proposed security controls.

SETUP, Components and Challenges

- *Two Deployed Setups:*
  1. Monolithic gNB linked to FlexRIC, enabling concurrent operation of multiple xApps. Can scrutinize RAN's xApps and ML security.
  2. Distributed gNB not suitable for security analysis, but serves as reference point for future Open-Front-Haul analysis

Fig.3:Current Deployments

- *Components:*
  1. *O-DU/O-CU:* OpenAir interface CU/DU or gNB with USRP
  2. *Core Network:* Free5GC over Kubernetes
  3. *O-RU:* Benetel RAN550
  4. *UE:* Android smartphone with programmable USIM
  5. *Near RT RIC: FlexRIC*

- *Challenges*:
  1. Incomplete\Undocumented implementation of different solutions offered by software vendors.
     A. Open-Front-Haul, is not yet supported by the OAI O-DU
     B. FlexRIC is not compatible with the distributed version of the gNB
  2. Not interoperable components offered by hardware vendors

Future Work

1. Our objective for the future is to merge the two configurations into a single, unified setup. We anticipate the upcoming release from OAI to enable the integration of O-RU in the setup and the compatibility of FlexRIC with the distributed gNB.

Fig.4:Current Deployments

2. After the integration of the two configurations:
   A. Security analysis of the Open-Front-Haul. The analysis will include timing attacks and data modification by exploiting the potential absence of Integrity protection for the User Plane data
   B. Perform different attacks related to the Machine Learning aspect of ORAN, by providing ill-trained models to the non-RT RIC
   C. Extend the setup, by introducing the currently-missing ORAN components. This requires support from the software vendors

Conclusion

- ORAN is an emerging and promising RAN expansion architecture that is popular among the scientific community but theoretical risk analyses are currently raising concerns about its security. The proposed setup is deemed to be future-proof and possesses the capability to bridge the gap pertaining to practical analyses, which are considered essential for evaluating the security of ORAN. Our purpose is to initiate discussions with reaserchers sharing our interests and concerns, and exchange information to achieve our goals and secure ORAN.

References

1. Aly S. Abdalla et al. Toward Next Generation Open Radio Access Network–What O-RAN Can and Cannot Do! 2022. arXiv: 2111.13754 [cs.NI].
2. ENISA. Report on the cybersecurity of Open RAN. 2022. URL: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks.
3. Madhusanka Liyanage et al. Open RAN Security: Challenges and Opportunities. 2022. arXiv: 2212.01510[cs.CR].
4. BSI. BSI Standard 200-3 Risikomanagement. 2017. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-undOrganisationen/Standards-undZertifizierung/ITGrundschutz/BSI-Standards/BSI-Standard-2003-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html.

Radboud University

RADIX SECURITY

Figure 51: Wisec Poster

O-RAN is an emerging architecture expected to become the standard in 6G networks. Due to its significance and the attention it receives from the academic community, we decided to submit a poster to the WiSec conference.

Our poster proposal aims to address the lack of practical risk analyses by presenting a minimal and future-proof deployment of an O-RAN 5G network. This deployment, although not currently feasible, enables various hands-on security analyses for different network elements, aligning with the objectives of our master's thesis. In our poster, we also discuss the challenges associated with commercial and open-source products and present a setup that utilizes a monolithic gNB and Flexric for testing the security of ML in O-RAN. Our proposed setup is expected to be deployable shortly, contingent upon the Availability of support for the Open Fronthaul ad E2 interface. We can effectively execute our deployment plan once the necessary updates and implementations are released. As there are currently no O-RAN test labs in universities and research facilities, our objective is to contribute to developing a practical framework for conducting security analyses in O-RAN networks.

Our poster, titled *Deploying an ORAN Test Lab*, was accepted at the conference, in which we had the opportunity to present our findings and plans to fellow scientists, engaging in meaningful conversations with those who share our concerns and interests in O-RAN. Our proposed setup can help fill the gap in practical risk analyses and contribute to advancing O-RAN security. For more details, please refer to our poster in Fig.51 and the poster's paper [41].

5 Securing O-RAN

In this section, we present our recommendations for securing O-RAN based on the findings of the two preceding chapters. These recommendations encompass a combination of existing studies that we believe are applicable to the architecture and our own suggested measures. Before delving into these recommendations, we first provide a summary of the security controls and general requirements, currently presented in the architecture's specifications. This summary serves as an important foundation for identifying areas of improvement. Our suggestions include security requirements and, in some cases, security controls. Security requirements identify abstract security protections without specifying any control, while security controls focus on how to enforce a requirement. The recommendations and controls will vary based on the findings and context discussed in the preceding chapters.

5.1 Summary of Controls and Requirements

The mandatory, general security requirements are outlined in Tab.5 and have been extracted form Section 5 of [15]. Despite their mandatory nature, no specific security controls are in place to address these requirements. This presents an opportunity for proposed security controls to improve and enhance the overall security posture of the system. An exception is the use of digital signatures, which according to the Protocol Specification Document[14], vendors are forced to choose from National Institute of Standards and Technology (NIST)-approved algorithms. Furthermore, we will not address the documentation-related requirements, as they fall outside the scope of this thesis. Our primary focus is to provide recommendations and controls for the technical aspects of O-RAN security, with some exceptions regarding physical security.

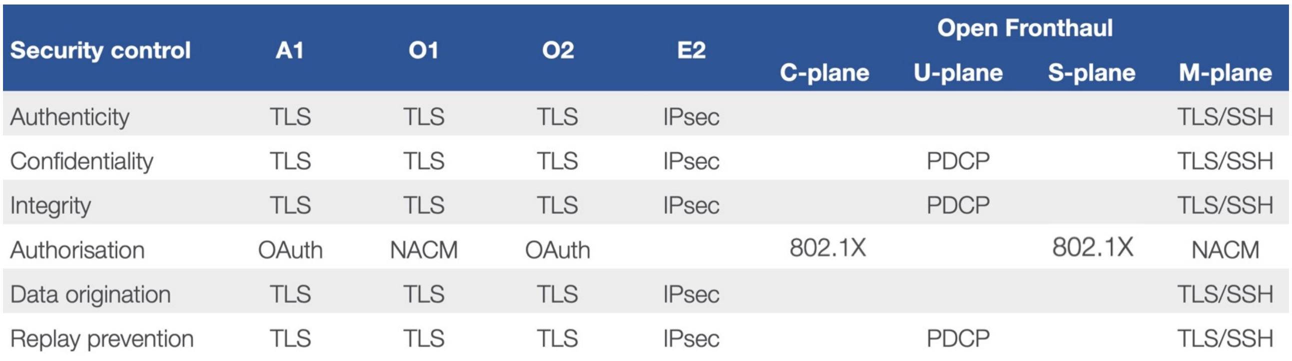
Table 5: Mandatory Requirements

Scope	Requirements
Application Packages	Must be Signed by the Vendor and Verified by the SMO
All Components	Vendor must provide a list of supported Protocols and Services
Transport Protocols[1]	Strong Input Validation
Components with External interfaces	Must be resistant against DoS Attacks
OS and Applications	Vendor must provide documentation with known vulnerabilities
Passwords Protected Devices [2]	Must provide protection against password-based attacks, if password authentication is used.

[1] Transport Protocols: IP, UDP, TCP, SCTP, SSH, HTTP and HTTP 1.2

[2] Password Protected Devices: Virtualised RAN Functions, O-RU and O-Cloud

Fig.52 summarizes the optional security controls for each interface. This provides an abstract view of the areas that are currently protected, assuming the optional security requirements are implemented.



Security control	A1	O1	O2	E2	Open Fronthaul			
					C-plane	U-plane	S-plane	M-plane
Authenticity	TLS	TLS	TLS	IPsec				TLS/SSH
Confidentiality	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH
Integrity	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH
Authorisation	OAuth	NACM	OAuth		802.1X		802.1X	NACM
Data origination	TLS	TLS	TLS	IPsec				TLS/SSH
Replay prevention	TLS	TLS	TLS	IPsec		PDCP		TLS/SSH

Figure 52: Optional Security Controls For Each Interface[50]

5.2 Security Recommendations

The security recommendations section is divided into two parts. The first part focuses on controls that can be enforced by the 3GPP, while the second part pertains to requirements that the O-RAN Alliance can enforce. It is important to note that the first section is relatively brief, as the security requirements set by the 3GPP are beyond the scope of this thesis.

5.2.1 3GPP Security Reccomedations

Security controls offered by 3GPP can protect the data from Insiders, Cloud, and Ran Operators. In both analyses, even in the ***ww*** scenarios, the mandatory Integrity protection between the UE and the AMF often was the only security control that could protect the data to some degree. By implementing more mandatory controls at this level, the security of the data can be ensured without relying completely on security control provided by O-RAN. Therefore we propose three main controls:

1. Mandatory encryption between UE and O-CU for CP data
2. Mandatory encryption between the UE and the O-CU for the UP data
3. Mandatory Integrity protection data between the UE and the UPF for the UP data

The third recommendation aims to mitigate the risk of compromising the Integrity of UP data, even from Insiders and Operators, similar to the mandatory Integrity protection for CP data. The obvious option would be to recommend mandatory encryption between the UE and the CN for both planes. However, this option is currently not feasible due to the collection of 3GPP data by the two controllers to enhance RAN functionalities. However, we suggest conducting further studies to explore potential controls to address this issue. One possible approach to enable encryption between the UE and the CN while still allowing the collection of 3GPP data for RAN enhancement is to implement sample-based encryption. For example, for every ten encrypted packets, one packet could remain decrypted for the controllers to collect and utilize. The feasibility and effectiveness of this approach are currently unknown, so we propose additional research to investigate this matter thoroughly. Even in the current state, implementing these protection controls will safeguard the Confidentiality of data from Insiders who may have control over the ODU and ORU and, most importantly, will offer protection of 3GPP data transmitted over the Open Fronthaul interface, which, as previously explained, is the most vulnerable interface and can be targeted by external attackers.

The security controls offered by 3GPP are the only mechanisms proved to be effective in securing the data from malicious Operators and Insiders. After the identification of methods that enable RAN optimization techniques without access to the 3GPP data, we recommend the encryption between the UE and the CN to become mandatory for both planes.

5.2.2 O-RAN Security Recommendations

5.2.2.1 General Enhancements

Here we analyze some general security enhancements to improve existing requirements and controls presented in the O-RAN's specification. Furthermore, we also provide some suggestions for the adoption of new requirements and controls that will further increase O-RAN's security:

1. Replace SSH with TLS wherever both protocols are recommended. Explicitly prohibit the use of SSH. The BSI analysis summary highlights the benefits of TLS over SSH and recommends this control.

2. Upgrade the minimum supported version of TLS to TLS 1.3. While TLS 1.2 is considered secure, TLS 1.3 offers several enhancements, including stronger encryption algorithms and improved performance. It reduces handshake time, resulting in faster and more efficient communication.

3. Enforce the use of secure programming languages for developing xApps and rApps. Utilizing safe programming languages helps mitigate threats associated with these applications, such as buffer overflow attacks and isolation breaches. This control is also suggested by [35].

4. Provide clear definitions of security specifications for each interface. Ambiguous or conflicting specifications can lead to insecure configurations. Establishing unambiguous security specifications ensures consistency and promotes secure implementations of the interfaces.

5. Define roles and privileges related to the services provided by each interface. Proper access controls and restricted privileges based on user roles are important. Users with "sudo" rights should not rely on default passwords, as this poses a significant security risk.

6. Secure O-RU updates by employing digital signatures to ensure update integrity. Store both the updated function and encryption keys in a hardware security module (HSM) for enhanced protection. Restrict access to the HSM to authorized parties, preferably only the Network Operator, to minimize the risk of unauthorized access or tampering.

7. Replace password authentication with multi-factor authentication (MFA) to mitigate vulnerabilities associated with weak authentication. By implementing MFA, the system requires Users to provide multiple forms of authentication, such as a combination of passwords, biometrics, tokens, or other factors. This adds an extra layer of security and reduces the likelihood of unauthorized access. To ensure the effective implementation of MFA, we suggest following guidelines provided by reputable sources such as Cybersecurity & Infrastructure Security Agency (CISA). CISA offers comprehensive guidelines for implementing strong authentication measures, including best practices, considerations, and recommendations to enhance security[18]. This will provide efficient, secure access to critical components like the O-Cloud. Additionally, it is crucial that the specification of every involved component explicitly includes mandatory controls for enforcing MFA authentication.

8. Provide guidelines for implementing strong input validation measures to mitigate the risks associated with potentially dangerous inputs. It is important to define which types of inputs should be considered dangerous and establish countermeasures to handle them effectively. While the Open Web Application Security Project(OWASP) provides basic guidelines for input validation[47], further tailoring is necessary to address the specific context of O-RAN.

9. All of the data stored in SMO and the nRT RIC database should be encrypted and Integrity protected. Encryption ensures that the data remains confidential, while Integrity protection ensures that the data remains unchanged and uncorrupted. The responsibility of decrypting the data stored in the SMO and nRT RIC DB lies with the two Controllers, who should perform decryption only upon receiving a valid request from authorized parties.

10. DDoS protection mechanisms shall be implemented to reduce the risk of attacks on the system's Availability. At the moment, ML-based mechanisms and Firewalls are the most prominent candidates with the different theoretical analyses supporting either the first[40], other the second[35].
    ML-based mechanisms utilize machine learning algorithms to detect and mitigate DDoS attacks by analyzing network traffic patterns, sometimes by performing deep analysis on the packet and identifying anomalies. ML models can adapt and learn from new attack patterns, improving their effectiveness in identifying attacks over time. Their main advantage is their capability to detect previously unknown attacks. On the other hand, firewalls provide a "wall" between the internal network and external sources as they filter incoming traffic based on predefined rules. They can be configured to block or allow specific types of traffic, providing a line of defense against DDoS attacks. Firewalls have the advantage of being able to block known attack vectors effectively.

11. Security controls must be implemented to protect against threats arising from the virtualization aspect of Open RAN. Kubernetes, the most widely used tool for container orchestration, plays a crucial role in ensuring the system's security. Important areas that require attention include:

    (a) Implementing Isolation Mechanisms for Pods: Isolation is important under the O-RAN concept, as it ensures that the logical functions, xApps and rApps, cannot break isolation and gain control over other processes and their resources. Kubernetes offers some native features that can be used to enforce isolation between Pods, including namespaces and resource quotas.

    (b) Implementing Controls to prevent Privileges escalation: Privilege escalation is one of the most important security concerns in the whole architecture. A process must be limited to only accessing the resources, data, and services intended for its use. To mitigate the risk of privilege escalation in Kubernetes, the following measures should be considered:

        i. Least Privilege Principle (The same as in Oauth 2.0, discussed in the previous analysis).

        ii. RBAC Configuration: RBAC (Role-Based Access Control) allows "sudo"-Users to specify fine-grained permissions for individual Users and groups to ensure that only authorized entities can access critical resources and services.

        iii. Regular Monitoring: Monitoring mechanisms must be established to detect and investigate suspicious activities within a Kubernetes cluster.

    It is important to note that these recommendations are not exhaustive as the security of Kubernetes is a complex topic that requires further study to establish sufficient security controls. More detailed information on Kubernetes security can be found in [57].

12. Specify the types of data that will be collected by the controllers for training the ML models. In the case of UP data, we propose further research on Privacy-Preserving machine learning techniques, which can potentially guarantee User's Privacy. Some promising techniques are Homomorphic Encryption and Differential Privacy. However, to the best of our knowledge, no published research currently examines Privacy-Preserving machine learning techniques for RAN optimization. This may be attributed to the early stages of development of O-RAN and the lack of real-world deployments.

13. Identify and implement controls to protect the architectures from the Cloud/Ran Operators. existing literature, such as the analysis presented in [35], primarily focuses on suggestions regarding utilizing Trusted Execution Environments(TEEs). We propose that Operators shall only select trusted and well-established Cloud providers until proper controls are implemented to mitigate the risks associated with these actors effectively.

14. Introduce security requirements for physical security controls. Physical access to components must be possible only after identification and authorization. Such controls will reduce the number of threats in critical components like the Open Fronthaul, as explained before.

5.2.2.2 Crucial Recommendations

This section deals with two recommendations that will ensure the protection of O-RAN against external attackers. At the current moment, only the 3GPP controls are capable of providing adequate protection against Insiders-attackers.

First Recommendation: From Optional to Mandatory

By analyzing Fig.52, it is evident that the optional security controls offer sufficient protection for almost every interface with the exception of the Open Fronthaul's CUS plane. The absence of authorization control in the E2 interface can be justified due to the nature of its services, which are exclusively accessible and managed by the controller, and IPSec ensures the authentication of the two ends. Hence, our first recommendation is to make every optional security control mandatory. The use of TLS and IPSec ensures protection from Outsiders and User attackers, as explained in our analysis. This approach will greatly reduce the risk of breaching the previously-defined protection goals, except for Availability. This reccomendtation was previously proposed in [35] but has not yet been adopted.

Second Recommendation: Securing the CUS-Plane

In the first control, we specifically excluded Open Fronthaul's CUS-Plane. While the 802.1x protocol provides a level of authorization and authentication, there is a lack of additional controls to ensure Integrity, Privacy, and Accountability within this interface. The Open Fronthaul's CUS-Plane operates under strict performance restrictions, making implementing protocols like TLS and IPSec impractical. Therefore we recommend the use of MACsec as [20]. As described in the Protocols Sec.2.5, MACsec plays a crucial role in protecting Ethernet links by providing Authentication, Confidentiality, and Integrity for transmitted data. As MACsec operates at a hardware level, it's more efficient in terms of performance over protocols such as TLS and IPsec. However, the hardware implementation mandates a redesign of O-RUs to ensure support for MACsec, the use of specialized hardware to host the O-DU. However, as the data are not protected in the endpoints, a strong physical access policy must be implemented to protect the O-RUs from unauthorized access.

The combination of these two security controls, along with the implementation controls aimed at preventing DoS attacks, will establish a comprehensive safeguard against external attackers, as every interface will be protected by either TLS or IPSec, or MACsec. However, additional research is necessary to develop strategies for establishing protection from malicious Insiders and Cloud-Operators, which currently relies on implementing the 3GPP optional security controls.

6 Future Work

As mentioned previously, our current setup is not yet complete. Our primary objective is to integrate the O-RU. Once the software update from OAI is released to support Open Fronthaul, we will proceed with the practical risk analysis of the Open Fronthaul. We plan to deploy a Raspberry Pi as a man-in-the-middle device during this analysis. The Raspberry Pi will utilize the NetFilterQueues (NFQueues)[12] feature of the Ubuntu OS to block packets in the UP-Link direction. To achieve this, we will monitor the communication over the interface to identify the MAC address of the ORU, allowing us to block any packets originating from the ORU. The intercepted packets will be forwarded to the User space where a Python program with the use of Scapy[13] will separate the three planes (C-Plane, U-Plane, and CS-Plane). Ensuring that CS-Plane data can pass without significant delay is crucial to maintain uninterrupted communication between the endpoints. S-Plane packets can be identified as the plane is using the Precision Time Protocol(PTP) instead of the eCPRI. Regarding the identification of U/C-Plane packets, the eCPRI Message-Type field will be used, as packets transmitting UP are marked with the value "3" in the previously mentioned field[2]. Afterward, U-Plane data will be modified and then sent back into the network. In scenarios where TCP/IP is utilized, checksum recalculation will be performed to avoid detection. We will examine unprotected and encrypted packet scenarios as part of our analysis to evaluate the feasibility. In the case of enabled encryption, the method presented in [49] will be utilized. Some other attacks on the CS planes will also take place to disrupt the system's Availability. **Even though the attack may appear straightforward on paper, the required inspection of packets for Plane separation can introduce delays for the CS-Plane packets, leading to the O-DU dropping the modified U-Plane packets. This is a compelling reason why we emphasize the need for a practical risk analysis of each component to assess its security**.

Additionally, once OAI provides support for E2 by the CU and DU components, we will analyze the ML aspect of the architecture. We plan to develop an xApp to enforce QoS among different UE devices. Subsequently, we will intentionally generate carefully crafted legitimate traffic from a genuine UE to disrupt the QoS. This crafted traffic aims to impact the ML model, tricking it into enforcing incorrect policies. This is feasible as legitimate traffic is used by the nRT RIC and the xApps to enhance their operations.

Lastly, we will try to expand our deployment by adding the missing O-RAN components. This will enable the conduction of more practical risk analysis on other interfaces. This will only be possible after the required updates from the software vendors to enable support for the different O-RAN interfaces.

[12] Nfqueues are specialized queues managed by the kernel packet filter. They can be accessed by a User-space Python program to inspect, modify, accept, or drop packets

[13] Scapy, a powerful Python module, will be used for packet manipulation, allowing us to decode and edit captured packets

7 Conclusion

The RAN architecture has undergone significant changes in recent years, including:

1. Separation of BBU and the RU which enabled greater flexibility and scalability
2. The virtualization of the RAN components which reduced the cost and allowed for easier management and resource allocation
3. The split of the BBU to the CU and the RU enabled a distributed with improved performance

Despite the advancements in RAN architecture, the market is still dominated by a few vendors. The semi-proprietary implementation of protocols has hindered interoperability between components, creating a closed market that limits innovation and prevents new "players" from entering. As a result, Network Operators remain dependent on a single vendor for implementing new functionalities in the RAN, often requiring costly infrastructure upgrades. This lack of vendor diversity and interoperability poses challenges for Operators in terms of flexibility, cost-effectiveness, and the ability to introduce advancements in a timely manner.

The O-RAN is an emerging architecture that promises to break the monopoly in the RAN market. O-RAN addresses this by "opening" the interfaces between the RAN components, enabling the deployment of diverse RAN products. This allows new contenders to enter the O-RAN market with their own unique offerings without the requirement to develop the entire RAN architecture. This approach promotes innovation and competition within the industry, leading to advancements and improvements in RAN technology. Furthermore, ORAN supports the introduction of ML to architecture, which will further enhance the RAN's functionalities.

Nevertheless, ORAN has been criticized for its security. Several theoretical risk analyses indicated an exposed, vulnerable architecture. New attacks are now possible because of the new technologies introduced to the RAN, i.e., the open interfaces, ML, and virtualization. However, to the best of our knowledge, not even a single practical risk analysis has been performed to evaluate the feasibility of possible attacks and test proposed countermeasures. We believe that conducting both practical and theoretical risk analyses is essential for assessing the security of an architecture. The absence of practical risk analysis can be attributed to the non-existent deployments of O-RAN 5G networks in universities and research facilities.

The original objective of this master's thesis was to establish an O-RAN test lab and conduct the first practical risk analysis on the Open Fronthaul. The Open Fronthaul was chosen due to its reliance on security controls specified by 3GPP. However, due to limitations, such as software vendors' inability to deliver the required updates within the given timeframe, the test lab deployment proved unfeasible. Nevertheless, we anticipate that support for the Open Fronthaul will become available in the near future. In the meantime, we have utilized this opportunity to share our setup with the academic community by presenting a poster at the ACM WiSec conference held in the UK, hoping to fill this gap and enable other researchers to make use of it in the future for practical risk analyses.

The BSI released a theoretical risk analysis last year, which we consider to be the most accurate and extensive assessment conducted thus far. This analysis demonstrated that O-RAN is highly vulnerable, even to external attackers with minimal capabilities. In this master's thesis, we present an updated version of this analysis, taking into account the technical updates and security improvements introduced in the four subsequent releases of the security specifications. Despite these enhancements, our risk analysis concludes that the architecture remains exposed, and we provide recommendations to enhance its security. Additionally, we abstractly present an attack on the Open Fronthaul, which is currently not recognized as a potential threat by the O-RAN Alliance. We also propose countermeasures to mitigate this attack, as its consequences could be severe.

We have strong confidence in the potential of the O-RAN architecture to revolutionize the RAN landscape. With the introduction of new elements and techniques, it has the capability to enable flexible, scalable, and intelligent RAN deployments. However, ensuring its security is of utmost importance. Currently, the security of O-RAN relies heavily on the security controls provided by 3GPP. We strongly urge the O-RAN Alliance to implement mandatory security controls to establish the security of O-RAN independently of 3GPP controls. Furthermore, we emphasize the need for further research on critical matters such as protecting the architecture from malicious Cloud Operators and developing Privacy-Preserving xApps/rApps to safeguard User Privacy. Additionally, we call upon the scientific community to conduct practical security analyses to evaluate potential attacks and promote the development of robust security controls. As O-RAN holds the potential to become the next standard in 6G networks, its security must be taken seriously and addressed in advance.

References

[1] 3GPP. *Security architecture and procedures for 5G System.* 2020. URL: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf.

[2] Ericsson AB et al. *eCPRI Spesification.* 2022. URL: http://www.cpri.info/downloads/eCPRI_v_2.0_2019_05_10c.pdf.

[3] Aly S. Abdalla et al. *Toward Next Generation Open Radio Access Network–What O-RAN Can and Cannot Do!* 2022. arXiv: 2111.13754 [cs.NI].

[4] O-Ran Alliance. *Cooperative Transport Interface Transport Control Plane Specification.* 2023. URL: https://drive.google.com/file/d/1b9NXXRWZfrts6Zarl_omD5HCoL33epb4/view?usp=share_link.

[5] O-Ran Alliance. *E2 General Aspects and Principles.* 2023. URL: https://docs.google.com/document/d/1ZF2AI96nQ5nPej9vvXbR-hLnMNeqohg8/edit?usp=share_link&ouid=101626630738807925632&rtpof=true&sd=true.

[6] O-Ran Alliance. *Management Plane Specification.* 2023. URL: https://drive.google.com/file/d/1hmEktfQvaVgf0T8d8F-8FCVdTWBgowCZ/view?usp=share_link.

[7] O-Ran Alliance. *Near-Real-time RAN Intelligent Controller E2 Service Model (E2SM), RAN Function Network Interface (NI).* 2020. URL: https://drive.google.com/file/d/1uB91j06I4qm7N_tnNh539AHT88TAZ2cF/view?usp=share_link.

[8] O-Ran Alliance. *O-RAN Architecture Description.* 2023. URL: https://drive.google.com/file/d/1cQ3qP-CtuQ67TTOUkThqH_T6W4FXUC64/view?usp=share_link.

[9] O-Ran Alliance. *O-RAN Security Threat Modeling and Remediation Analysis.* 2023. URL: https://docs.google.com/document/d/119u8PNhYYsrqXgjIdy2Z-GIKiFDXWwzN/edit?usp=share_link&ouid=101626630738807925632&rtpof=true&sd=true.

[10] O-Ran Alliance. *O1 Interface specification for O-CU-UP and O-CU-CP.* 2023. URL: https://drive.google.com/file/d/1gKqUgi8VOiEXtAsdX58ZTTZwCUx4XM7L/view?usp=share_link.

[11] O-Ran Alliance. *O1 Interface specification for O-CU-UP and O-CU-CP.* 2023. URL: https://drive.google.com/file/d/1ccLztXnBSBtpEEOTb0XEwoCwfWJwc3zS/view?usp=share_link.

[12] O-Ran Alliance. *O1 Interface specification for O-DU.* 2023. URL: https://drive.google.com/file/d/1sHpFUQtzT8QiUo1uiWBMEWQlCzmDOjcr/view?usp=share_link.

[13] O-Ran Alliance. *O2 Interface General Aspects and Principles.* 2023. URL: https://drive.google.com/file/d/16G5W4ngxn49nWrg4CescpFK_-MY2zhlz/view?usp=share_link.

[14] O-Ran Alliance. *Security Protocols Specification.* 2023. URL: https://drive.google.com/file/d/11QYn7XgpSCqP-UOm4srpYzpzwKNPQKQs/view?usp=share_link.

[15] O-Ran Alliance. *Security Requirements Specifications.* 2023. URL: https://drive.google.com/file/d/15E9RXdm5df6tomJu59BsT_ZtTN55LJcZ/view?usp=share_link.

[16] O-Ran Alliance. *Study on Security for Service Management and Orchestration.* 2023. URL: https://docs.google.com/document/d/1id4SFWX_0If1vPaoPb0u2dTyMbbQq8Vw/edit?usp=share_link&ouid=101626630738807925632&rtpof=true&sd=true.

[17] BSI. *BSI Standard 200-3 Risikomanagement.* 2017. URL: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html.

[18] CISA. *CAPACITY ENHANCEMENT GUIDE: Implementing Strong Authentication.* 2023. URL: https://www.cisa.gov/sites/default/files/publications/CISA_CEG_Implementing_Strong_Authentication_508.pdf.

[19] Andrea Detti. *Functional Architecture.* URL: https://www.5gitaly.eu/2018/wp-content/uploads/2019/01/5G-Italy-White-eBook-Functional-architecture.pdf.

[20] Daniel Dik and Michael Stübert Berger. "Transport Security Considerations for the Open-RAN Fronthaul". In: *2021 IEEE 4th 5G World Forum (5GWF).* 2021, pp. 253–258. DOI: 10.1109/5GWF52925.2021.00051.

[21] Marcin Dryjański. *RAN Intelligent Controller (RIC): Overview, xApps, and rApps.* URL: https://rimedolabs.com/blog/ran-intelligent-controller-ric-overview-xapps-and-rapps/.

[22] ENISA. *Report on the cybersecurity of Open RAN.* 2022. URL: https://digital-strategy.ec.europa.eu/en/library/cybersecurity-open-radio-access-networks.

[23] Morten Kofoed Esbjørn. *What is MACsec?* 2022. URL: https://www.comcores.com/what-is-macsec/.

[24] ETSI. *Specification of common aspects for RESTful NFV MANO APIs.* 2023. URL: https://www.etsi.org/deliver/etsi_gs/NFV-SOL/001_099/013/03.05.01_60/gs_NFV-SOL013v030501p.pdf.

[25] Faysalji. *Introduction to CPRI & eCPRI Technologies.* URL: https://forum.huawei.com/enterprise/en/introduction-to-cpri-ecpri-technologies/thread/903283-100305.

[26] Zahid Ghadialy. *RAN Functional splits.* Dec. 2021. URL: https://blog.3g4g.co.uk/2021/03/5g-ran-functional-splits.html.

[27] OAI 5G RAN PROJECT GROUP. *OAI 5G RAN PROJECT GROUP.* 2023. URL: https://openairinterface.org/oai-5g-ran-project/.

[28] OAI MOSAIC5G PROJECT GROUP. *OAI MOSAIC5G PROJECT GROUP.* 2023. URL: https://openairinterface.org/mosaic5g/.

[29] Brad Hedlund. *Securing Your Network Connection Cloud MACsec vs IPSec.* 2022. URL: https://www.linkedin.com/pulse/securing-your-network-connection-cloud-macsec-vs-ipsec-brad-hedlund.

[30] Ir.F.Fransen. *5G SECURITY: Can 5G secure IoT?* 2019. URL: https://www.surf.nl/files/2019-03/5G%5C%20Groningen%5C%205%5C%20-%5C%20Can%5C%205G%5C%20secure%5C%20IOT.pdf.

[31] ISO. *Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* 2022. URL: https://www.iso.org/standard/80585.html.

[32] ISO. *Risk Management.* 2018. URL: https://www.iso.org/iso-31000-risk-management.html.

[33] ISO. *Risk management — Risk assessment techniques.* 2019. URL: https://www.iso.org/standard/72140.html.

[34] Yousef Khalidi. *Microsoft Innovation in RAN Analytics and Control.* 2022. URL: https://azure.microsoft.com/en-us/blog/microsoft-innovation-in-ran-analytics-and-control/.

[35] Stefan Köpsell et al. *OPEN RAN RISK ANALYSIS*. 2022. URL: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Studies/5G/5GRAN-Risk-Analysis.pdf?__blob=publicationFile&v=7.

[36] Devendra Kumar. *5G network architecture*. June 2020. URL: https://www.5gfundamental.com/2020/06/5g-network-architecture.html.

[37] Oscar Lasierra et al. *European 5G Security in the Wild: Reality versus Expectations*. 2023. arXiv: 2305.08635 [cs.CR].

[38] Helger Lipmaa, Phillip Rogaway, and David Wagner. *Comments to NIST concerning AES Modes of Operations: CTR-Mode Encryption*. 2020. URL: https://www.cs.ucdavis.edu/~rogaway/papers/ctr.pdf.

[39] Madhusanka Liyanage. *Open RAN Security and Privacy: Opportunities and Challenges*. Dec. 2022.

[40] Madhusanka Liyanage et al. *Open RAN Security: Challenges and Opportunities*. 2022. arXiv: 2212.01510 [cs.CR].

[41] Sotiris Michaeldes, David Rupprecht, and Katharina Kohls. *Developing an ORAN Security Test Lab*. May 2023. URL: https://drive.google.com/file/d/1OScD5OMfWM2dC03FlaV1IFwbefDh9TVL/view?usp=share_link.

[42] Dudu Mimran et al. "Security of Open Radio Access Networks". In: *Computers & Security* 122 (2022), p. 102890. ISSN: 0167-4048. DOI: https://doi.org/10.1016/j.cose.2022.102890. URL: https://www.sciencedirect.com/science/article/pii/S016740482200284X.

[43] Nokia. *TLS versus IPsec for HTTP security*. 2002. URL: https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_26_Oxford/Docs/PDF/S3-020666.pdf.

[44] NTIA. *Open RAN Security Report*. 2023. URL: https://ntia.gov/sites/default/files/publications/open_ran_security_report_full_report_0.pdf.

[45] OAI. *Open Air Intrface*. 2023. URL: https://openairinterface.org.

[46] Innocent Onwuegbuzie. "5G: Next Generation Mobile Wireless Technology for A Fast Pacing World". In: *Journal for Pure and Applied Sciences (JPAS)* 1 (June 2022), pp. 1–9. DOI: 10.56180/jpas.vol1.iss1.57.

[47] OWASP. *Input Validation Cheat Sheet*. 2023. URL: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html.

[48] Krupa Patil. *Why Is TLS 1.3 Better And Safer Than TLS 1.2?* URL: https://www.appviewx.com/blogs/why-is-tls-1-3-better-and-safer-than-tls-1-2/.

[49] David Rupprecht et al. "Breaking LTE on Layer Two". In: *2019 IEEE Symposium on Security and Privacy (SP)*. 2019, pp. 1121–1136. DOI: 10.1109/SP.2019.00006.

[50] T-Mobile et al. *Open RAN MoU progress update on maturity, security and energy efficiency*. 2019. URL: https://telecominfraproject.com/wp-content/uploads/joint-mou-white-paper-mwc-2023.pdf.

[51] AIRSPAN TEAM. *Open Architecture*. 2023. URL: https://www.airspan.com/open-architecture/.

[52] BENETEL TEAM. *RAN550*. 2023. URL: https://benetel.com/ran550/.

[53] BSI TEAM. *BSI*. 2023. URL: https://www.bsi.bund.de/EN/Home/home_node.html.

[54] FREE5GC TEAM. *FREE5GC*. 2023. URL: https://www.free5gc.org.

[55] HUAWEI TEAM. *5G Network Architecture.* 2021. URL: https://carrier.huawei.com/~/media/CNBG/Downloads/Program/5g_nework_architecture_whitepaper_en.pdf.

[56] JUNIPER TEAM. *What Is Open Ran.* 2021. URL: https://www.juniper.net/nl/nl/research-topics/what-is-open-ran.html.

[57] KUBERNETES TEAM. *Security.* 2023. URL: https://kubernetes.io/docs/concepts/security/.

[58] KX Sales Team. *Radio Access Network (RAN) Analytics.* 2022. URL: https://kx.com/wp-content/uploads/2020/09/Kx-for-Telco-Use-Case-RAN-Analytics.pdf.

[59] MAVERIN TEAM. *Open vRAN.* 2023. URL: https://www.mavenir.com/portfolio/mavair/radio-access/vran/.

[60] OAI 5G CN TEAM. *OAI 5G CN PROJECT GROUP.* 2023. URL: https://openairinterface.org/oai-5g-core-network-project/.

[61] OPEN5GS TEAM. *Open5GS.* 2023. URL: https://open5gs.org.

[62] SD-RAN TEAM. *SD-RAN RIC.* 2023. URL: https://docs.sd-ran.org/sdran-1.1/sdran-in-a-box/docs/HW_Installation_ric_only.html.

[63] SRS TEAM. *SRS RAN.* 2023. URL: https://www.srslte.com.

[64] STLPARNERS TEAM. *What Is Open Ran.* 2021. URL: https://stlpartners.com/articles/telco-cloud/what-is-open-ran-2021/.

[65] Moniem Tech. *What are C/U/M/S Fronthaul (FH) Planes in ORAN ?* URL: https://moniem-tech.com/2022/05/05/what-are-c-u-m-s-fronthaul-fh-planes-in-oran/.

[66] Moniem tech. *The Evolution from 4G to 5G by CPRI to eCPRI Transformation.* URL: https://moniem-tech.com/2022/10/19/the-evolution-from-4g-to-5g-by-cpri-to-ecpri-transformation/.

[67] Prabhu Kaliyammal Thiruvasagam et al. *Open RAN: Evolution of Architecture, Deployment Aspects, and Future Directions.* 2023. arXiv: 2301.06713 [cs.NI].

[68] Uknown. *Open Midhaul F1 Interface F1-C and F1-U.* URL: https://www.techplayon.com/open-midhaul-f1-interface-f1-u-and-f1-c/.

[69] Uknown. *Opening the 5G Radio Interface.* URL: https://www.comcores.com/wp-content/uploads/2020/11/Opening-the-5G-virtual-Radio-Interface-Whitepaper-part-2.pdf.