†

5G OPERA

5G-OPERA Deliverable 5.4

Security specific Extensions

Document Properties	
Name of project	5G-OPERA
Document title:	WP 5.4 Security specific Extensions
Client:	Ministère de l'économie, des finances, et de la relance, Bundesministerium für Wirtschaft und Energie
Official reference:	5G-OPERA D5.4
Reviewer IABG:	Maik Holzhey
Reviewer NXP GE	Javier Velásquez
Reviewer TU Dresden	Mehmet Akif Kurt
Abstract:	WP 5.4: OPERA Security testing is needed of the developed and realised Open-RAN architecture. Following the steps of the MITRE ATT&CK and MITRE D3FEND framework for a private 5G network will enable the IT departments of private companies to ensure a decent level of information security for mobile networks in an enterprise IT landscape. Targets for testing are the availability (fall out), integrity (access to the operating infrastructure (layer 1 – 4) and application data (layer 5-7), authentication (monitoring, sniffing) and confidentiality (control and user data). Suitable monitoring of the attack in combination with a risk evaluation (ISO27005) provides a holistic picture of the security using the Open-RAN private network. Resilience measures to reduce risks are suggested. The cryptography used for the information spaces within the mobile radio is evaluated for its suitability in a post-quantum era.
Date of publication:	30/06/2024
Version:	1.0
Access:	Consortium
Keywords:	Open-RAN, 5G Private Networks, Security

Executive Summary

Within the 5G-OPERA project, German and French partners cooperate to develop a technological ecosystem for open Radio Access Networks (RAN) for private networks. This report explains the Security specific Extensions from IABG, NXP-GE and TUD. We have jointly contributed to the development of a comprehensive security framework to address the unique security challenges posed by the advanced capabilities and complexities of Open-RAN 5G technology.

This document details the security-specific extensions developed within the 5G-OPERA Project, highlighting the innovative approaches and methodologies employed to fortify the 5G infrastructure. Throughout the document we followed ISO-27005 framework and developed a "Opera Security Model" to explore various aspects of the security enhancement. The model identified all the security requirements on 5G infrastructure installed in 5G-OPERA project and it is integrated with "Security-To-Do-Tool" for Protocol requirement from 5G Core and 5G RAN.

Moreover, we performed Threat Modelling to identify the vulnerabilities in the system and carried Penetration testing on different interfaces and components of 5G-SA network and every executed attack was measured and mapped to ORR (OWASP Risk Rating) and CCR (Common Criteria Rating). For cyber security framework we used MITRE ATT&CK for splitting attacks in phases using TTP's (Techniques & Sub-Techniques), then we map these attack steps to MITRE D3FEND and countermeasures for each attack phases using TTP's (Classes & Sub-Classes). We also did a ML-based model for edge security.

The result for network administrators regarding counter measures was to harden the 5G system, so we included the Stride Model for generating a better effectiveness for running countermeasures. For each attack which was executed, a bouquet of relevant countermeasures was added and mapped to different 5G Layers. Of course, basic security features from NIST, 3GPP and Open-RAN state of the current cyber space must be already implemented.

The following sections will provide a detailed overview of the security-specific extensions, methodologies, and results achieved in the 5G-OPERA Project. This document serves as a comprehensive guide for stakeholders, including network operators, security professionals, and policymakers, offering insights into the robust security measures essential for the deployment and operation of secure 5G networks.

The Focus of the project is 5G signaling and basic network traffic. So, tests regarding speed transport, preferred transport (QoS mechanisms), normal traffic load and overload behavior of the new 5G OAI was not in the scope of work. So, Traffic dependent attacks like DNS flooding have not been tested.

Table of Contents

Abbreviations

3GPP	Third Generation Partnership Project
AE	Auto Encoder
AES	Advanced Encryption Standard
AMF	Access and Mobility Function
AN	Access Network
APN	Access Point Name
API	Application Programming Interface
ARP	Adress Resolution Protocol
AUSF	Authentication Server Function
AVC	Application Visibility and Control
BH	Backhaul
BSI	Bundesamt für Sicherheit in der Information Technik
CCR	Common Criteria Ranking
CN	Core Network
CNF	Cloud-Native Network Function
COTS	Commercial Off the Shelf
CSF	Cybersecurity Framework
CUPS	Control and User Plane Separation
DH	Diffie Hellman
DL	Deep Learning
DTLS	Datagram Transport Layer Security
E2E	End-to-End
ECDSA	Elliptic Curve Digital Signature Algorithm
ETSI	EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE
FH	Fronthaul
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
gNB	Next Generation Node B
GNU Radio	free & open-source Software Development Toolkit
GPL	General Public License
GTPU	GPRS Tunnelling Protocol User Plane
HBRT	Hardware-Based Root of Trust
HE	Home Environment
HMAC	Homomorphic Message Authentication Code
HPLMN	Home Public Land Mobile Network
HPC	High Performance Computing
HSM	Hardware Security Modul
IDPS	Intrusion Detection and Prevention System
IEEE	INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS
IETF	INTERNET ENGINEERING TASK FORCE
IKE	Internet Key Exchange
IMSI	International Mobile Subscriber Identity
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
KDE	Kernel Density Estimation
KEM	Key Encapsulation Mechanisms
KNN	K-Nearest Neighbours
LOF	Local Outlier Factor
LTS	Long Term Licenses
MAC	Media Access Control
MANO	Management and Orchestration
MBB	Mobile Broadband
MCC	Mobile Country Code
MD5	Message-Digest Algorithm 5

ME	Mobile Environment
ML	Machine Learning
MNC	Mobile Network Code
MNO	Mobile Network Operator
MTC	Machine Type Communication
mTLS	Mutual TLS
NAS	Non-Access Stratum
NACM	Network Configuration Access Control Model
NEFS	Network Exposure Function Security
NFVO	Network Function Virtualization Orchestration
NGAP	Next-Generation Application Protocol
NIC	Network Interface Controller
NMA	Network Management and Automation
Nmap	Network Mapper
NIST	National Institute of Standards and Technology
NR	New Radio
NRF	Network Repository Function
NSMF	Network Slice Management Function
NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
OAI	OpenAirInterface
OAM	Operations, Administration, and Maintenance
OCSVM	One-Class Support Vector Machines
O-CU-CP	Centralized Unit Control Plane
O-CU-UP	Open Centralized Unit User Plane
O-DU	Open Distributed Unit
ONAP	Open Network Automation Platform
O-RAN	Open Radio Access Network
ORR	Over All Response Rate
O-RU	Open Radio Unit
OSM	Open-Source Model
OTA	Over The Air
PCA	Principal Component Analysis
PCF	Policy Control Function
PCFP	Packet Forwarding Control Protocol
PDU	Protocol Data Unit
PLMN	Public Land Mobile Network
PNF	Physical Network Functions
PQS	Post-Quantum Cryptography
PRACH	Physical Random-Access Channel
PSS	Probabilistic Signature Scheme
RAN	Radio Access Networks
RAR	Random Access Response
RBAC	Rolled Based Access Controller
RF	Radio Frequency
RFP	Reverse Path Filter
RIC	Radio Intelligent Controller
RRC	Radio Resource Control
RSA	Rivest–Shamir–Adleman
RT	Real Time
SA	Stand Alone
SBA	Service Based Access
SDA	Software Defined Access
SDLC	Software Development Life Cycle
SDN	Software Defined Networks
SDR	Software Defined Radio
SHA	Secure Hash Algorithm
SIB	System Information Block
SMF	Session Management Function

SMO	Service Management and Orchestration
SN	Secondary Node
SNR	Signal to Noise Ratio
SSH	Secure Shell (Network Protocol)
SPGWU	Serving and Packet Data Network Gateway User
SUCI	Subscriber Concealed Identifier
SW	Software
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TS	Technical Specification
t-SNE	t-distributed Stochastic Neighbour Embedding
TTPs	Tactics, Techniques, and Procedures
UDM	Unified Data Management
UDP	User Datagram Protocol
UDR	Unified Data Repository
UE	User Equipment
UPF	User Plane Function
URLLC	Ultra Reliable Low Latency Communication
USRP	Universal Software Radio Peripheral
VAE	Variational Auto Encoders
VIM	Virtualized Infrastructure Manager
VM	Virtual Machine
VNFD	Virtual Network Function Description
VNFM	Virtual Network Function Manager
VPLMN	Visited Public Land Mobile Network
VSFTPD	Very Secure FTP Daemon

List of Figures

List of Tables

List of ANNEXES

1 Introduction

The **5G-OPERA** project aims to build a Franco-German ecosystem for private 5G networks under the joint leadership of TU Dresden (TUD) and EURECOM (Sophia Antipolis). The focus of the project is the idea of open hardware and software with open interfaces in mobile communication networks to allow multi-vendor options for technical equipment. The goal of the project is to ensure that the hardware and software of all project partners can work together. In addition to setting up reference test environments and demonstrators in Industry 4.0 environments, **5G-OPERA** is supporting the trials in the three demonstration projects and will advise all additional projects joining the program.

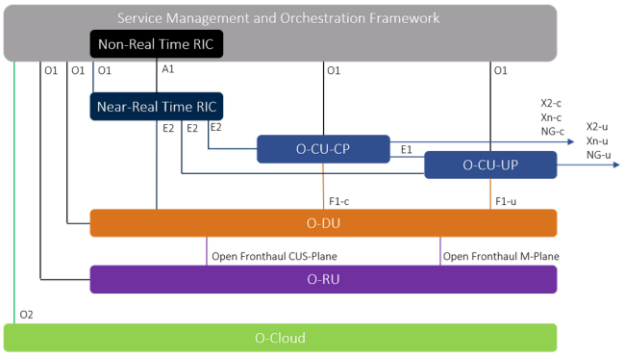

Figure 1 Architecture and Interface and Network functions [1]

2 Security specific Extensions

WP 5.4: Opera Security testing is needed of the developed and realised Open RAN architecture by the established cyber kill chain in a red teaming approach. Following the steps of the cyber kill chain for a private 5G network will enable the IT departments of private companies to ensure a decent level of information security for mobile networks in an enterprise IT landscape. Targets for testing are the availability (fall out), integrity (access to the operating infrastructure (layer 1 – 4) and application data (layer 5-7), authentication (monitoring, sniffing) and confidentiality (control and user data). Suitable monitoring of the attack in combination with a risk evaluation (ISO27005) provides a holistic picture of the security using the Open RAN private network. Resilience measures to reduce risks shall be suggested. The cryptography used for the information spaces within the mobile radio network shall be evaluated for its suitability in a post-quantum era.

Also work on the definition of procedures and mechanisms that guarantee hardware- and software-based end-to-end security of information and privacy of data when proprietary algorithms or applications are delivered through 5G-based federated AI systems and executed on not totally trustworthy nodes, like end devices or edge components. The different alternatives of hardware- and software-based security, as well as AI solutions, will require an optimisation for their integration and deployment in smart networks and its access nodes.

3 Introduction to Security in the 5G-OPERA World

Cellular network technologies have evolved over several generations, including 2G, 3G, and 4G, and 3GPP (3rd Generation Partnership Project) is actively developing 5G specifications. 5G differs from prior generations primarily in that it will not only provide faster speed, higher bandwidth, and lower delays, but also support more use cases such as enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low-latency communications (uRLLC).

One critical aspect of this technological evolution is the implementation of Open Radio Access Network architectures, which aim to foster innovation, flexibility, and cost-efficiency by allowing the use of interoperable components from different vendors.

The 5G Opera project addresses these concerns, focusing on enhancing the security framework within the Open RAN environment, refer to the image below: Figure 2 4G vs 5G Security Enhancements" to safeguard against potential threats and vulnerabilities that could compromise the integrity and reliability of 5G networks. (1)

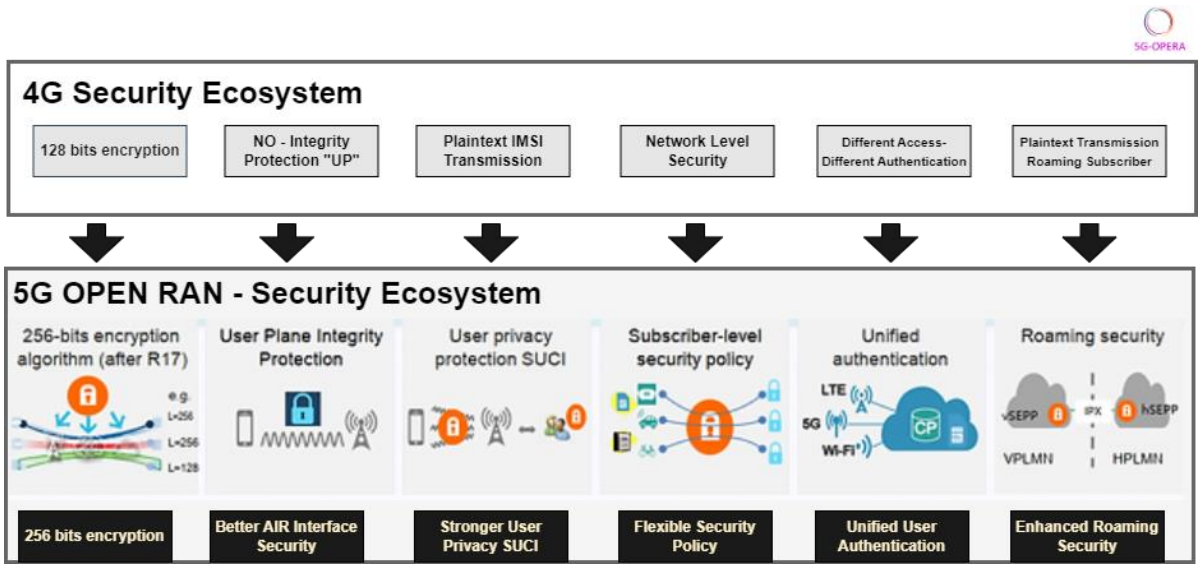

Figure 2 4G vs 5G Security Enhancements

In the context of the **5G-OPERA** project, WP 5.4 is dedicated to the development and implementation of security-specific extensions tailored for the Open RAN architecture. This work package aims to deliver a comprehensive set of security enhancements that addresses the unique challenges posed by the open and disaggregated nature of Open RAN.

Our deliverable focuses on fortifying the network against a wide array of security threats, ensuring secure communication channels, protecting data integrity, and maintaining the privacy of users. By integrating these security-specific extensions, the project strives to create a resilient 5G network infrastructure capable of supporting the diverse and demanding applications of the future while maintaining the highest standards of security.

4 Background Security Standardizations – 5G

There are five standard bodies under the European Commission's a refer to the image below: Figure 3 5G Security Standardization" and with the support of ENISA, developed a single EU Coordinated Risk Assessment on Cybersecurity. It identifies the main threats and threat actors, the most sensitive assets, the main vulnerabilities, and the main risks and on 29 January 2020, the NIS Cooperation Group published the EU toolbox of risk mitigating measures.

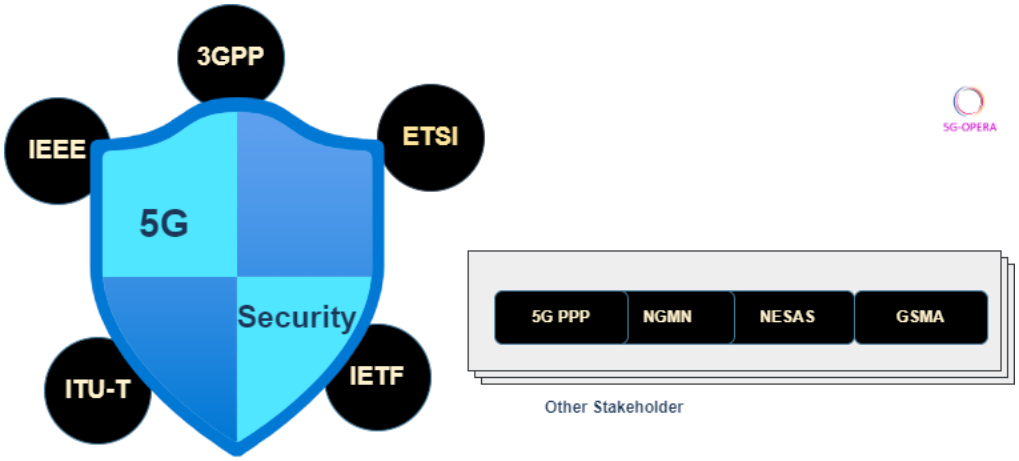

Figure 3 5G Security Standardization

4.1 3GPP - 3rd GENERATION PARTNERSHIP PROJECT - SA3

3GPP SAS3 (2) SA WG3 (3gpp.org) - started in 2016 is the main active working group addressing 5G security and privacy issues. It is developing technical specifications for 5G networks, including security specifications. However, some of these security controls are defined as optional or there is a degree of flexibility on how to implement.

3GPP SA3 also ensures refer to the image below: Figure 4 3GPP Defined Security - TS 33.501 that cryptographic algorithms which need to be part of the 5G security specifications. The 1st version 5G security Technical Specification 3GPP TS 33.501 Version was published in June 2018.

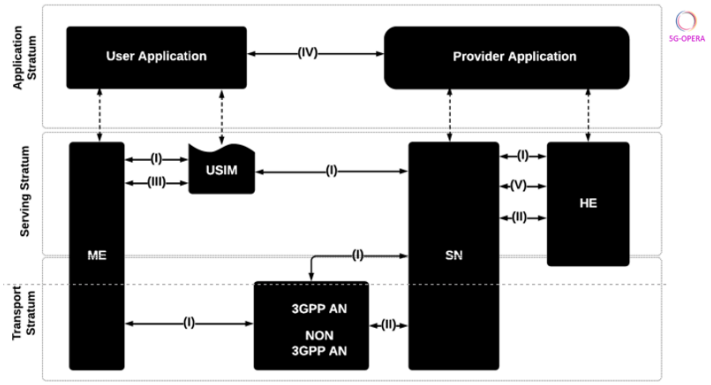

Figure 4 3GPP Defined Security - TS 33.501

I. Network access security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN to AN for the access security.

II. Network domain security (II): the set of security features that enable network nodes to securely exchange signalling data and user plane data.

III. User domain security (III): the set of security features that secure the user access to mobile equipment.

IV. Application domain security (IV): the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely.

V. SBA domain security (V): the set of security features that enables network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. Such features include network function registration, discovery, and authorization security aspects, as well as the protection for the service-based interfaces. SBA domain security is a new security feature compared to TS 33.401

4.2 ETSI - EUROPEAN TELECOMMUNICATIONS STANDARDS INSTITUTE

This has several subgroups addressing various elements related to 5G system security. (3) ETSI ETSI - Cyber Security | Cyber Security Standards | Cyber Security Technology mostly focus on:

- Network Function Virtualization Security (NFV SEC)
- Technical Committee for Cybersecurity (TC CYBER)
- Technical Committee for Lawful Interception (TC LI)
- Technical Committee for Intelligent Transport Systems (TC ITS)
- Industry Specification Group on Securing Artificial Intelligence (ISG SAI)
- Security Algorithms Group of Experts (SAGE)

4.3 ITU - INTERNATIONAL TELECOMMUNICATION (ITU-T)

This standardization work is undertaken by various technical Study Groups (SGs 17) SG17: Security (itu.int) and ITU-T (4) mostly focus on the : refer to the image below: Figure 5 ITU-T 5G Security Study Group.

- Software Defined Network (SDN)
- Network Function Virtualization (NFV)
- Internet of Things (IoT)
- Big data analytics in mobile internet services
- Cloud computing
- Cryptographic profiles

Figure 5 ITU-T 5G Security Study Group

4.4 IETF - INTERNET ENGINEERING TASK FORCE

It is an internet standard body IETF | RFCs (5) and addresses technical areas covering protocols and architectures designed to support delay-sensitive and delay-tolerant applications, IP layer, network management, routing, end-to-end data transport on the internet and security.

- OAUTH 2.0 - AUTHORIZATION Framework
- EAP- Extensible Authentication Protocol
- HTTP/2 – Hypertext Transfer Protocol Version 2
- IKEv2 – Internet Key Exchange Version 2
- TLS – Transport Layer Security Protocol

4.5 IEEE - INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS

IEEE SA - The IEEE Standards Association - Home (6) describes itself as a “leading developer of industry standards in a broad range of technologies that drive the functionality, capabilities, and interoperability of products and services. In the context of 5G networks, the most relevant standards developed by IEEE are those in the standard 802.11 series on Wireless being one of the key of non-3GPP protocol for 5G networks access.

5 Background Security Standardizations – Open RAN

The Open Radio Access Network (Open RAN) Alliance is a global organization that promotes and advances the development and deployment of Open RAN technologies. The Alliance closely collaborates with the 3rd Generation Partnership Project (3GPP). Open Radio Access Network (O-RAN) Alliance in Security has developed a comprehensive threat model for Open RAN networks. This model outlines the various threats and risks that can impact an Open RAN network and provides guidance on how to mitigate and manage these risks.

Open RAN comprehensive approach to cybersecurity involves considering all aspects of digital security in the enterprise and protecting against all potential vulnerabilities. One such comprehensive security framework is

coming from National Institute of Standards and Technology (NIST) refer to the image below: Figure 6 Open RAN Standardization based on NIST and CSF. The O-RAN Alliance combined security recommendations can be combined with the NIST framework – SDLC (Software Development Life Cycle) and CSF (Cybersecurity Framework) while aligning with required industry specific security standards, local and regional. [2]

OPENAIRINTERFACE SOFTWARE ALLIANCE (OSA) OpenAirInterface – 5G software alliance for democratizing wireless innovation , in **5G OPERA** Project follows the O-RAN Alliance security working group has done an excellent job of analyzing these threats and recommending appropriate security controls based on their risk level. To effectively address these security threats, it is necessary to follow a holistic and comprehensive security strategy that includes additional security controls based on industry best practices. (7)

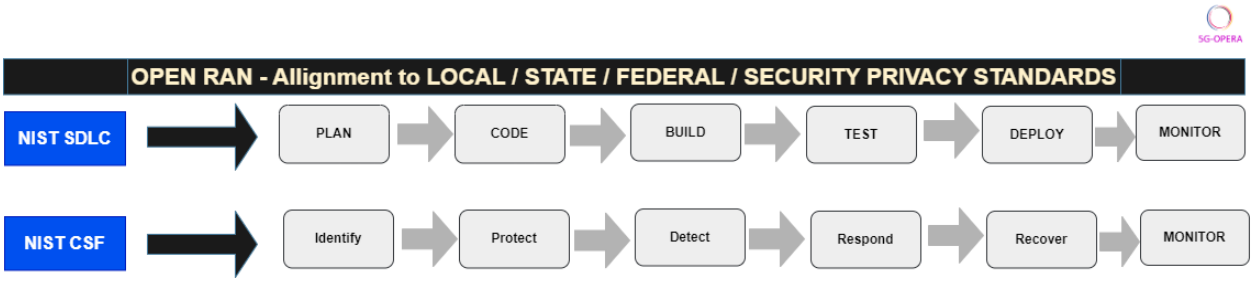

Figure 6 Open RAN Standardization based on NIST and CSF

6 Cybersecurity Framework

There are two challenges we in cybersecurity face when it comes to communicating what we do the rest of the business (and the rest of the world). The first challenge is communicating the technology and basic understanding of how it works to then show how it can be misused. The second challenge is then imparting how the criminals carry out their attacks.

In **5G-OPERA** IABG examined two different frameworks that are used to communicate hacking processes.

1. The Cyber Kill Chain Framework. (8)
2. The MITRE ATT&CK framework. (9)

6.1 Cyber Kill Chain Framework.

The Cyber Kill Chain Cyber Kill Chain® | Lockheed Martin, developed by Lockheed Martin refers to the image below: Figure 7 Cyber Kill Chain Framework" , which is a conceptual framework that outlines the various stages of a cyberattack. In the context of the 5G-OPERA Project's deliverable on Security Specific Extensions, a red teaming approach using the Cyber Kill Chain refer to figure 3 can help to identify vulnerabilities and potential points of exploitation in the 5G Open RAN environment. The stages of the Cyber Kill Chain are: (10)

- Reconnaissance: Identifying targets and gathering intelligence about the 5G Open RAN components.
- Weaponization: Developing a payload to exploit identified vulnerabilities.
- Delivery: Transmitting the payload to the target, for instance, through phishing or exploiting open ports.
- Exploitation: Triggering the payload to exploit a vulnerability and gain initial access.
- Installation: Installing malware or tools to establish persistence.
- Command and Control (C2): Establishing a backdoor for remote control.

- Actions on Objectives: Executing the end goals of the attack, such as data exfiltration or disruption of services.

Applying this model helps in understanding how an attacker might infiltrate and navigate through the 5G Open RAN network, allowing security teams to anticipate and mitigate these actions.

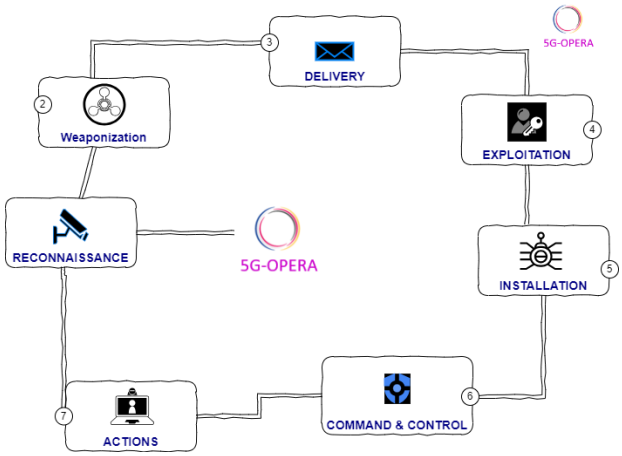

Figure 7 Cyber Kill Chain Framework

6.2 MITRE ATT&CK Framework

The MITRE ATT&CK Framework MITRE ATT&CK® refer to the image below: Figure 8 MITRE ATT&CK Framework" is a more granular and comprehensive model that outlines adversary tactics, techniques, and procedures (TTPs) across various stages of an attack lifecycle. Unlike the linear structure of the Cyber Kill Chain, MITRE ATT&CK provides a matrix that covers a wide array of potential attack vectors and methods, making it highly detailed and adaptable to different contexts. (11)

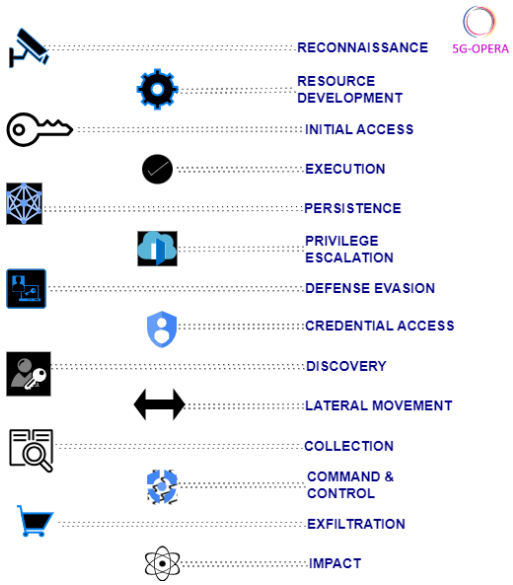

Figure 8 MITRE ATT&CK Framework

- Reconnaissance: It involves gathering and organizing information to prepare for an attack.
- Resource Development: Creating, compromising, buying, or stealing resources for an attack.
- Initial Access: It defines as acquiring access to the victim's systems.
- Execution: Executing malicious code on compromised networks or systems.
- Persistence: Appropriately sustaining access to that system.
- Privilege Escalation: Attempting to achieve higher-level concessions.
- Defense Evasion: Avoid detection by acting.
- Credential Access: Attempting to gain access to accounts.
- Discovery: Gathering information
- Lateral Movement: Moving from system to system.
- Collection: To support the high-level attack goal, gathering data.
- Command and control: Establishing control over prey's systems and communicating with compromised systems externally.
- Exfiltration: Stealing the prey's data
- Impact: Destroying, damaging, or making networks, systems, and data unavailable to the victim.

6.3 Implemented Cybersecurity Framework in 5G-OPERA – MITRE ATT&CK

There is no bulletproof framework out there and you will need all the “weapons” you have at your disposal; both the framework provides a way to counterattack and a way to stop and provide crucial insights into cyberattack behavior.

Cyber Kill Chain: It offers a straightforward, linear model for understanding the stages of a cyber attack, but it has its limitations and detailed insights into the specific procedures ‘attackers use, *which can limit its effectiveness in more complex or nuanced security scenarios as we have seen the deployment of 5G SA Open RAN Network.*

MITRE ATT&CK Framework (12)provides an extensive library of adversarial tactics, techniques, and procedures (TTPs), offering a deeper and more nuanced understanding of cyber threats when we started the OPERA Journey on 5G SA refer to image below, Figure 9 MITRE ATT&CK Framework with MITRE D3FEND Framework-5G-OPERA

- Actionable Intelligence: This framework includes a robust database of cyber threat intelligence (CTI), making it a valuable tool for identifying and mitigating threats in real-world scenarios.
- Holistic Coverage: By serving as a comprehensive knowledge base, MITRE ATT&CK acts as a checklist of attacker methodologies and goals, ensuring that security controls are through and address all aspects of cyberattacks.
- Utility for Security Professionals: The detailed and actionable nature of MITRE ATT&CK makes it particularly useful for threat hunters, red teamers, and those involved in designing and implementing security policies and controls, such as security architects and network administrators.

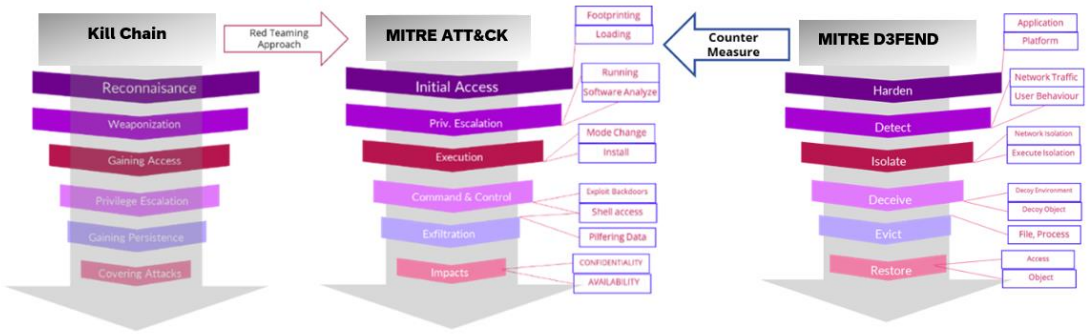

Figure 9 MITRE ATT&CK Framework with MITRE D3FEND Framework-5G-OPERA

MITRE ATT&CK is superior for providing detailed, actionable intelligence and comprehensive coverage of attacker methodologies, making it indispensable for advanced threat detection and response. In the 5G OPERA project we performed penetration testing on different interfaces, and we have used following:

- **MITRE ATT&CK** – To understand the techniques and tactics used by adversaries, including nation-state actors, cybercriminals, and hacktivists. The framework is designed to help security professionals better understand the tactics and techniques used by attackers.
- **MITRE D3FEND** – It helps against the tactics, techniques, and procedures (TTPs) outlined in the MITRE ATT&CK Framework. (13) MITRE D3FEND D3FEND Matrix | MITRE D3FEND™ is designed to provide a structured approach to defense, focusing on the implementation of controls and countermeasures to mitigate the TTPs described in MITRE ATT&CK.

7 OPERA Security Architecture

At OPERA, we put best efforts to incorporate security and privacy considerations into all relevant aspects and phases of our product according to ENISA ISO 27005 Security Framework for Trust Service Providers — ENISA (europa.eu) .

The ISO 27005, a widely adopted risk management standard, defines that risks emerge, refer to image below, Figure 10 Concept of Threat / Risk Architecture Threats abuse vulnerabilities of assets to generate harm for the organization". Following this methodology, we have identified assets, threats, and threat agents.

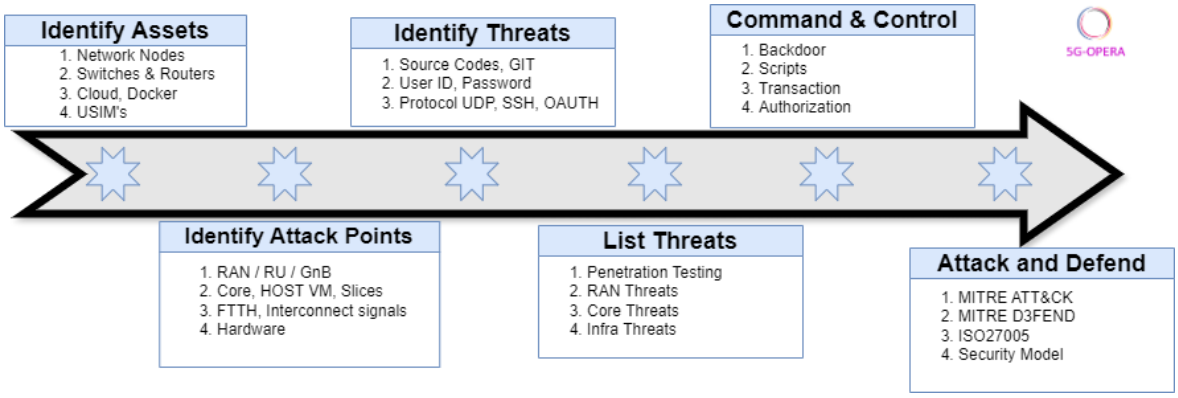

Figure 10 Concept of Threat / Risk Architecture

Our efforts in this area follow internal control framework known as **OPERA Security Model (OSM)**. The OSM is an approach to achieve product security and privacy by design and type of deployment ambitions. High-performance 5G networks are bringing limitless connectivity for connected devices and mobile applications. At 5G-OPERA defined architecture in deliverable work-package 3 refer to image below, Figure 11 OPERA High Level Security Architecture" IABG did the networks study to protect different interfaces, components, and assets of the 5G OPERA project. The 3GPP component and interfaces is already a written standard and it has not been captured in this deliverable 5.4 OPERA Security Specifications.

At 5G-OPERA, we follow the security standardization on 3GPP, and Open RAN standards as introduced earlier. 5G-OPERA summarizes of this key milestone in the development of the open Radio Access Networks (RAN) system.

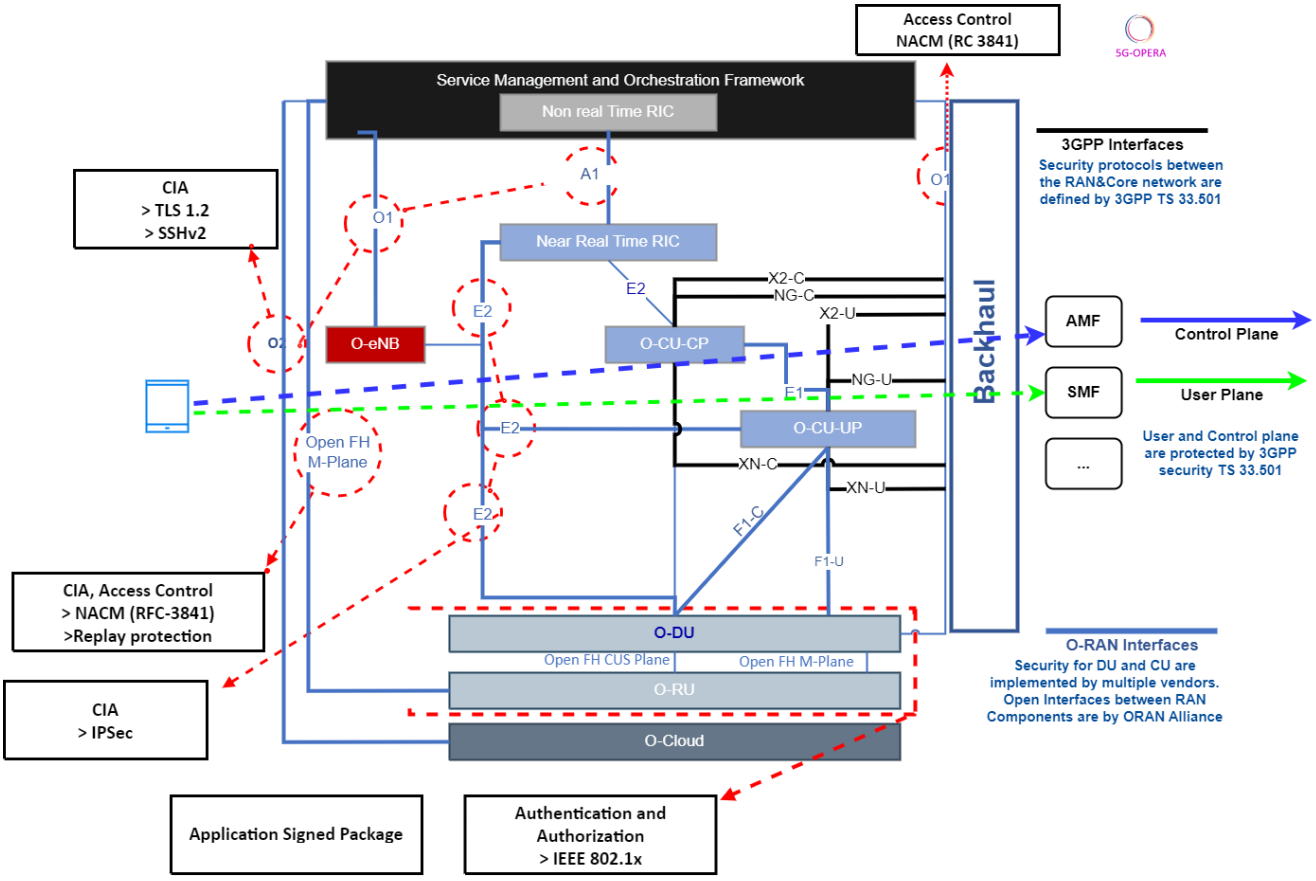

Figure 11 OPERA High Level Security Architecture

7.1 OPERA Security Assessment Methodology

The initial security requirements per Open Air Interface (OAI) and as per OPERA component refer to table below, Table 1 Security Assessment OPERA Requirements address key security pillars – **C-I-A-A**: (14)

Confidentiality **[C]**, Integrity **[I]**, Availability **[A]** & Authenticity **[A]**.

- **Requirement 1:** Confidentiality, Integrity, Replay protection and Data origin authentication mandatory requirements for A1, O1, O2, E2 interfaces.
- **Requirement 2:** Least Privilege Access Control on O1 interface enforcement with IETF RFC- 8341 Network Configuration Access Control Model (NACM).

- **Requirement 3:** Authentication and Authorization based on IEEE 802.1x Port based Network Access Control requirements to control network access points.
- **Requirement 4:** Mandatory support for TLS 1.2+ and Public Key Infrastructure X. 509 (PKIX) for mutual authentication on the Fronthaul M-Plane.
- **Requirement 5:** Networks Protocols and Services, Distributed Denial of Service (DDoS) attacks protection, password protection policies and vulnerability scanning.

Components	Between nodes	Security Mechanism	Standardization
O1 Interface	SMO and OPERA elements	mTLS	O-RAN
A1 Interface	Near-RT RIC and Non-RT RIC	mTLS	O-RAN
E1 Interface	O-CU-CP and O-CU-UP	NDS/IP (IPsec) or DTLS	3GPP
F1 Interface (Midhaul)	O-CU-CP and O-DU (F1-C)	NDS/IP (IPsec) or DTLS 3GPP	3GPP
	O-CU-UP and O-DU (F1-U)		
Open Front Haul M-Plane	O-RU and O-DU/SMO	mTLS, SSHv2	O-RAN
Open Front Haul CUS Interface	O-DU and O-RU	IEEE 802.1x with EAP-TLS O-RAN	O-RAN
Backhaul Interface	O-CU-CP and 5GC (N2)	NDS/IP (IPsec) or DTLS	3GPP
	O-CU-UP and 5GC (N3)		
E2 Interface	Near-RT RIC (xApps) and O-CU-CP	NDS/IP (IPsec) or DTLS	O-RAN
O2 Interface	SMO and O-Cloud	Under Study	O-RAN
X/R Apps Interface	Non/Near-RT RIC	Under Study	O-RAN
Xn Interface	Source gNB and Target gNB	NDS/IP (IPsec) or DTLS	3GPP
Secure Physical Assets	All	Apply Best Practices	3GPP

Table 1 Security Assessment OPERA

7.2 OPERA Risk Assessment Methodology

The criticality of the identified threats is assess based on their potential impacts mention in table 1. Indications of severity level for each threat are given whether they are considered as high, medium, or low which we will observe in OSM Architecture model.

It is the Security principles that identifies authentication and access control mechanisms, trusted communication, secure cryptographic operations, secure storage, secure boot, trusted and secure update, secure management of open-source components, robust isolation, continuous security development, testing, logging, monitoring and vulnerability handling, and security assurance. The security principles rationale is provided to trace all security principles back to threats and demonstrate that the defined security principles contribute to counter those threats. The focus of the security test specifications is on.(15)

- **Security Testing-1:** Validating the proper implementation of security protocols requirements specified by 3GPP and Open RAN in Security Protocols Specifications (SSH, TLS, DTLS, and IPSec).
- **Security Testing-2:** Emulating security attacks penetration testing refer to table below, Table 2 Risk Assessment OPERA 5G" discussed in this document and doing vulnerability testing against the OPERA components, interfaces, and the system to measure the robustness.
- **Security Testing-3:** Validating the effectiveness of the security mitigation methods to protect the OPERA system and the services it offers.

Penetration Testing	Affected Node	Framework
Metasploit Threat using Backdoor	Core	MITRE ATT&CK, -D3fend and Countermeasures
Hydra Threat without using Backdoor	Core	MITRE ATT&CK, -D3fend and Countermeasures
VSFTPD Threat using Backdoor	Core	MITRE ATT&CK, -D3fend and Countermeasures
Data Exfiltration Threat	RAN NAS-5GS	MITRE ATT&CK, -D3fend and Countermeasures
Fuzzing RAN	RAN UE Air Interface Attack	MITRE ATT&CK, -D3fend and Countermeasures

Fuzzing CORE	**Core NGAP - Control Plane**	**MITRE ATT&CK, -D3fend and Countermeasures**
Jamming Threat	**Radio UE Air Interface - User Plane**	**MITRE ATT&CK, -D3fend and Countermeasures**

Table 2 Risk Assessment OPERA 5G

7.3 OPERA Defend Assessment Methodology

Implementing MITRE D3FEND in a 5G-Open RAN system involves integrating proactive defense measures and countermeasures to enhance the resilience and security of the network. MITRE D3FEND is a knowledge base of active defense techniques that can be used to counter adversarial activities.

We tried to map MITRE D3FEND techniques and mapped to general countermeasures refer to image below, Figure 12 Mitigation Assessment using Countermeasure & MITRE D3FEND" which should be followed as standard for cybersecurity and for 5G networks we have discussed in detail in OSM. Using MITRE D3FEND techniques are applicable to the components of the Open RAN architecture, such as the Radio Access Network (RAN), the Centralized Unit (CU), the Distributed Unit (DU), and the core network.

Then we conduct a threat modeling and risk assessment to identify potential attack vectors specific to the 5G Open RAN environment using MITRE ATT&CK as a reference for potential adversary tactics, techniques, and procedures (TTPs). (16)

- **Mitigating Threat-1**: Mutual authentication SHOULD be established between communicating entities in an OPERA system, with each entity identified by a unique identifier and credentials.
- **Mitigating Threat-2:** Access control SHOULD be implemented that only allows authenticated and authorized personnel and services to access OPERA resources.
- **Mitigating Threat-3:** Measures SHOULD be taken to provide a secure and trusted runtime environment for cloud applications by implementing security controls that reduce the risk of firmware exploitation.
- **Mitigating Threat-4:** Security controls SHOULD ensure that lateral movement is detected and prevented when attackers have successfully exploited a vulnerability.
- **Mitigating Threat-5:** The system SHOULD be bootstrapped to be secured by default and it should be up to the admin to reduce the security perimeter of the end user system.
- **Mitigating Threat-6:** Industry best security such as DevSecOps practices SHOULD be followed when using open-source components, to minimize risks.
- **Mitigating Threat-7:** System should be pre-tested by offensive security testing team like MITRE D3FEND framework as developed in 5G-OPERA Project.

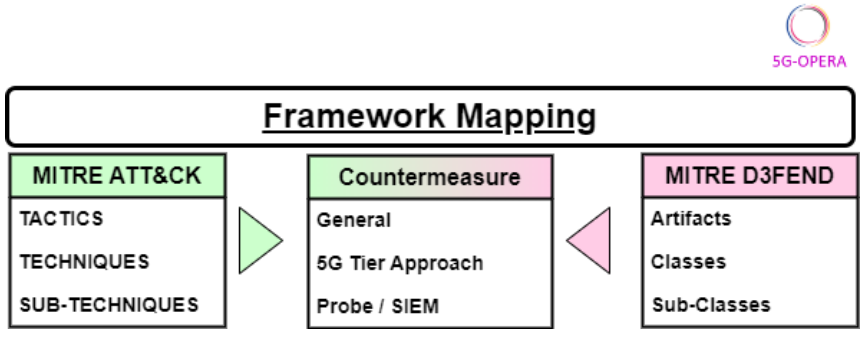

Figure 12 Mitigation Assessment using Countermeasure & MITRE D3FEND

8 Penetration Testing

Penetration testing is crucial for securing 5G-Open RAN systems, such as the OPERA project. This testing ensures comprehensive coverage of all interfaces and components by employing professional testers, often ethical hackers, to identify and address vulnerabilities in current and new systems, networks, and applications. This proactive measure protects against unauthorized access by malicious actors. (17)

Cybersecurity experts recommend conducting penetration tests when new IT threats emerge, significant changes occur (like office relocation or shift to remote work), or after a cyberattack (such as adware or ransomware). Ethical hacking replicates the strategies of malicious attackers to reveal security weaknesses, allowing organizations to fix them before exploitation. Known as "white hats," ethical hackers are authorized security professionals focused on improving an organization's security posture, distinguishing their mission from that of malicious hackers. Ethical hackers frequently identify critical cybersecurity vulnerabilities refer to image below, Figure 13 Penetration Testing Components".

Despite having authorization, ethical hackers must adhere to legal protocols, ensuring they obtain proper approval before accessing and assessing any IT asset. This careful approach in 5G OPERA project ensures that penetration testing remains a lawful and effective method for enhancing security in 5G-Open RAN environments.

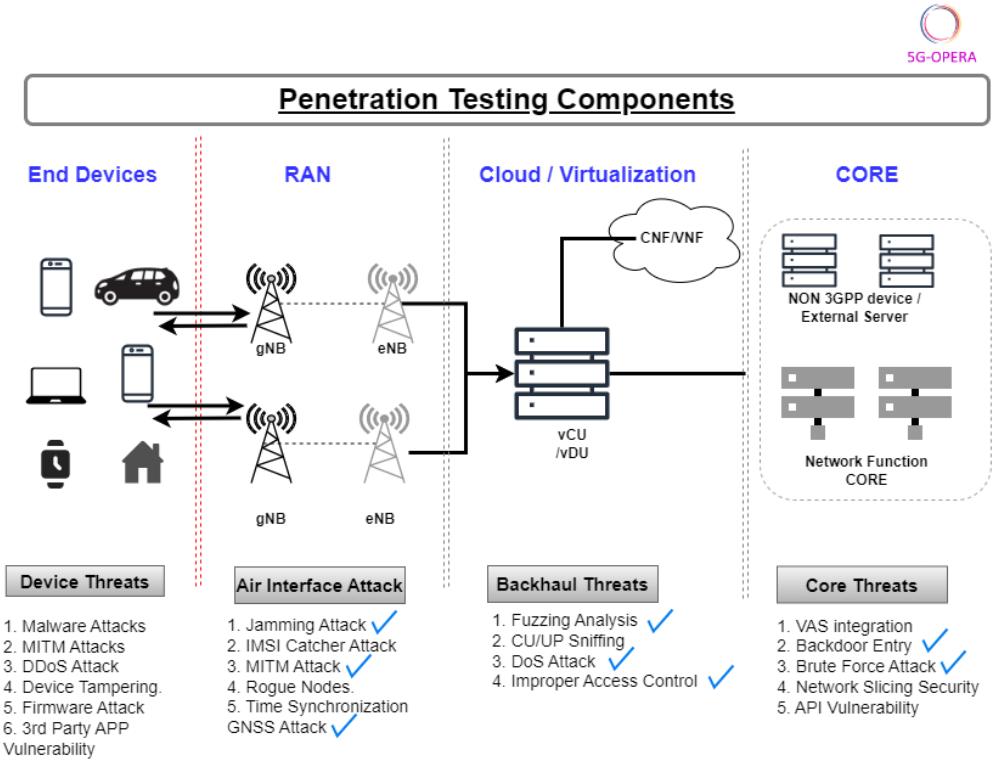

Figure 13 Penetration Testing Components

In Open RAN – 5G OPERA the threat surface expands for several main reasons, among which are:

- The physical structure of the network is changing, (future) applications and use cases need to compute and storage locations closer to the edge for reasons of localization and latency.
- The structure of the networking functions has changed from physical to virtual implementations, and the functions virtualized components can be placed across distributed edge and centralized core clouds.
- There is an emphasis on flexible software-based architecture enablers such as SDN (Software Defined Networks), SDA (Software Defined Access), SDR (Software Defined Radio). (18)

In short, we could summarize this situation in the following way, most of the threat surfaces in the 5G networks is due to the network architecture being more flexible and open towards the internet.

9 Hydra Threat

9.1 Introduction & Pre-Requisite - Hydra Threat

Hydra represents a potent tool employed for the purpose of brute-forcing username and password combinations, enabling attackers to systematically ascertain valid login credentials. This tool facilitates the execution of password spraying and dictionary attacks, two methodologies particularly adept at infiltrating enterprise or public networks of unknown vulnerability. Notably, Hydra offers a "verbose mode" feature, which permits the surveillance of failed login attempts, thereby affording insights into the efficacy of cracking endeavors. (19)

In the initial stages of network reconnaissance, it is customary to commence with an ICMP-Ping operation directed towards a presumed entity within the target network, typically a component within the white box. Should this endeavor yield no fruitful outcomes, recourse to utilizing EtherApe becomes advisable, as it enables a more nuanced examination of network traffic without eliciting conspicuous alterations. Upon closer inspection within Ether Ape's refer to image below, Figure 16 EtherApe Hydra Validation" interface, during concurrent execution of Hydra attacks, discernible patterns emerge, with SSH Protocol (port 22) and FTP (ports 21 or 3000) standing out as the primary targets for password and login credential exploitation. In instances where the port's designation is unknown, the utility of the "-s" command proves invaluable in port identification, especially in scenarios where network administrators have opted to deviate from default port configurations. (20)

$ hydra -l <username> -p <password> <ip> <service> -s <port>

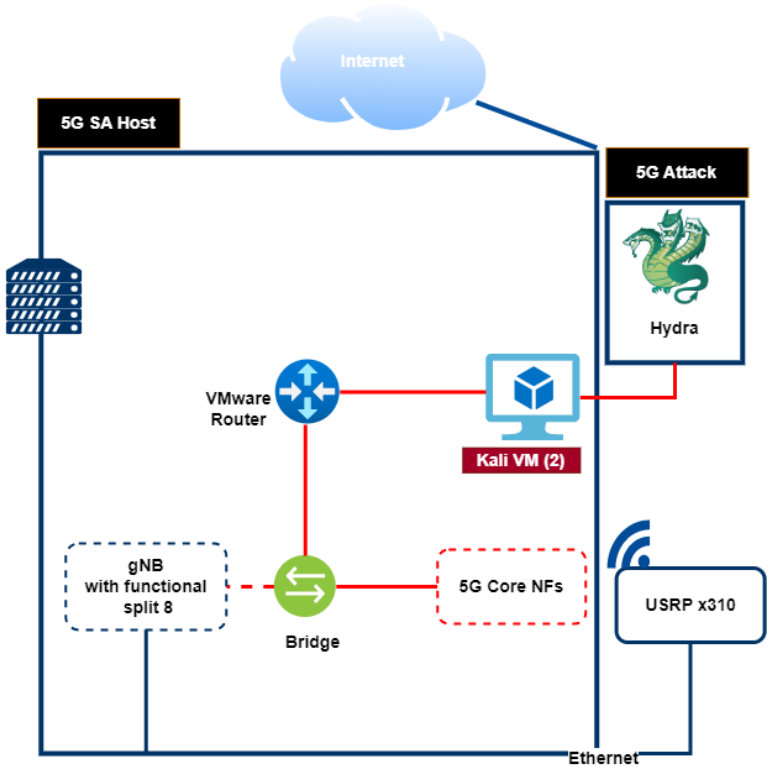

Figure 14 Architecture – Hydra Attack

In the context of the 5G Lab environment, the attack methodology, refer to image above, Figure 14 Architecture – Hydra was implemented through the virtual machine "VM3," leveraging Hydra pre-installed via the Host Server. The primary target of this assault pertained to the Central Unit of the 5G network, with the objective of illicitly acquiring credentials associated with users connected to the Radio Access Network (RAN). The Apache Tomcat Web server is hosted on 5G OAI Core, the vulnerable machine. This is the purposely deployed webserver which gains a backdoor entry to penetration tester.

The effective penetration testing requires refer to image below, Figure 15 Requisite – Hydra " obtaining permission, defining roles, selecting appropriate hardware and software tools, and ensuring the test environment's testability to accurately assess the security posture of the target systems.

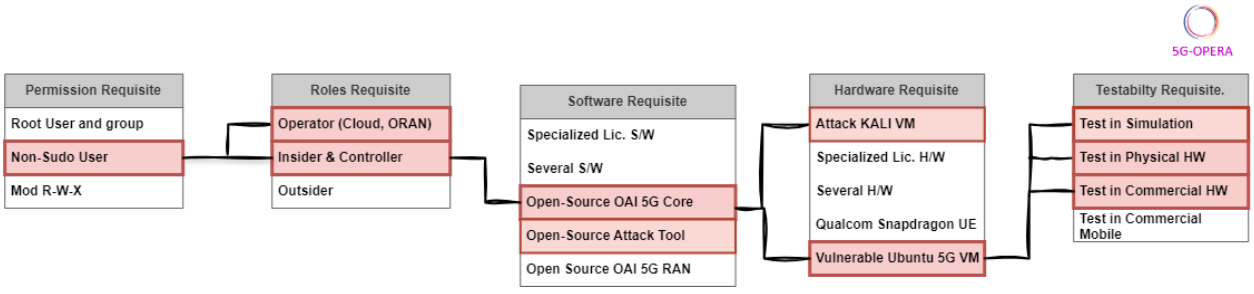

Figure 15 Requisite – Hydra Attack

9.2 Setup - Hydra Threat

1. The vulnerable machine 5G OAI Core should be up and running.

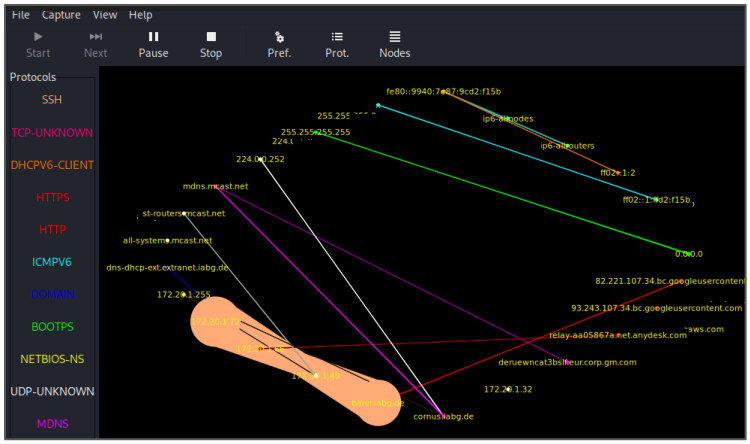

Figure 16 EtherApe Hydra Validation

2. The attacker machine should have KALI Operation System installed with Hydra Application
3. Attacker Machine:
    A. Initiate Hydra tool
    B. Initiate wordlist from user.txt
    C. Initiate wordlist from password.txt
4. Start password spraying.
5. Attack the vulnerable machine (5G Core)

9.3 MITRE ATT&CK Framework - Hydra Threat

- **TA**: TACTICS ID (MITRE Reference)
    - **Txxxx**: Technique ID (Threat ID) refer to table below, *Annex 1 MITRE ATT&CK Reference Hydra*
    - **Txxxx.xxx**: Sub Technique ID (Sub-Threat ID), refer to table below, Annex 2 MITRE ATT&CK Threat Reference Hydra

The Penetration testing team does “Grey Box” testing and identifies security risks on the Open-Air Interface of the 5G Network. We used the MITRE ATT&CK Framework refer to image below, Figure 17 MITRE ATT&CK Framework – Hydra Threat” for Enterprise Matrices to map the globally access adversaries’ tactics, techniques, and sub-techniques to our 5G Lab Network hacking. (21)

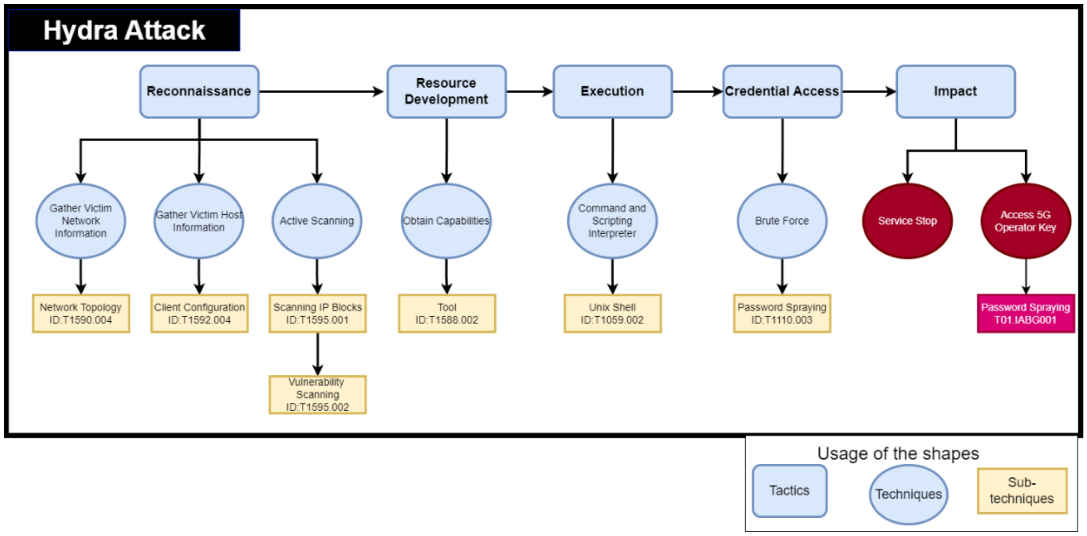

Figure 17 MITRE ATT&CK Framework – Hydra Threat

Summary of Attack Steps

Tactical Phase 1: Reconnaissance

- Gather Victim Network Information: Use IP scanning on port 22 (SSH) to collect network topology details.
- Gather Victim Host Information: Use IP scanning to identify vulnerable machines in the 5G Lab network.
- Active Scanning 1: Filter and map IP address ranges to identify client addresses.
- Active Scanning 2: Perform vulnerability scanning to access target IP and port ranges.

Tactical Phase 2: Resource Development

- Obtain Capabilities: Install and configure the HYDRA tool with user and password lists.

Tactical Phase 3: Execution

- Command and Scripting Interpreter: Use SSH and HYDRA to brute-force 5G Open Air Interface network credentials.

Tactical Phase 4: Credential Access

- Brute Force: Execute a password spraying script on port 22 to find valid accounts.

Tactical Phase 5: Impact

- Service Stop: Target availability by stopping services.
- Access 5G Operator Key: Compromise confidentiality by accessing the 5G operator key.

9.4 Annex Attached

Annex 1 MITRE ATT&CK Reference Hydra

Annex 2 MITRE ATT&CK Threat Reference Hydra

9.5 Result of Hydra Threat

The intruder breached the 5G Open Air Interface Network using Brute Force via SSH on port 22, compromising the confidentiality. By obtaining root credentials, the attacker could disrupt network availability or misuse services.

The result of Threat used Hydra refer to table below, Table 3 C-I-A-A Impact – Hydra Threat" and Table 4 Interfaces Impact – Hydra Threat" which is a tool for brute forcing network services like SSH. In our 5G lab, Hydra exploited vulnerabilities on port 22, rapidly increasing network traffic and prompting detection and countermeasures. Consequently, the 5G infrastructure's confidentiality and integrity were compromised. The 5G core network, operating on a Linux machine, was accessed through Hydra using the SSH protocol.

Threat Result and Impact (C-I-A-A)				
Threat Name	**"C" Confidentiality**	**"I" Integrity**	**"A" Availability**	**"A" Authenticity**
Hydra Threat	**affected**	**affected**		

Table 3 C-I-A-A Impact – Hydra Threat

Threat Node and Interfaces - 5G Threat Modelling				
Threat Name	**Threat Node**	**Vulnerable Node**	**Primary Affected - 5G Interface**	**Secondary Affected - 5G Interface**
Hydra Threat	**Kali VM without backdoor**	**5G Core**	**N6**	**N2 and N3**

Table 4 Interfaces Impact – Hydra Threat

10 Metasploit Threat

10.1 Introduction & Pre-Requisite - Metasploit Threat

Kali Linux, with its pre-built image and integrated Metasploit framework refers to image below Figure 18 Architecture Metasploit Threat", it offers over a hundred tools for vulnerability research in applications, networks, and servers. Metasploit's "msfconsole" interface allows users to scan and launch attacks on targets using various modules, including payloads, exploits, and post-exploitation tools. Version v6.2.9-dev includes 2230 exploits and 867 payloads. Meterpreter, a Metasploit payload, enables script execution and interaction without a GUI, though the paid Metasploit Pro version includes one. Metasploit helps identify and fix vulnerabilities before hackers exploit them, serving as a key tool for security professionals and hackers alike.

In our 5G lab, Apache Tomcat, a widely used Java application server, is installed on a vulnerable Ubuntu machine (VM1) with SSH enabled on port 22. This setup allows administrators to manage applications and acts as a backdoor for the attack machine (VM3), facilitating penetration testing. The Tomcat server on the 5G OAI Core provides a controlled entry point for security testing. (22)

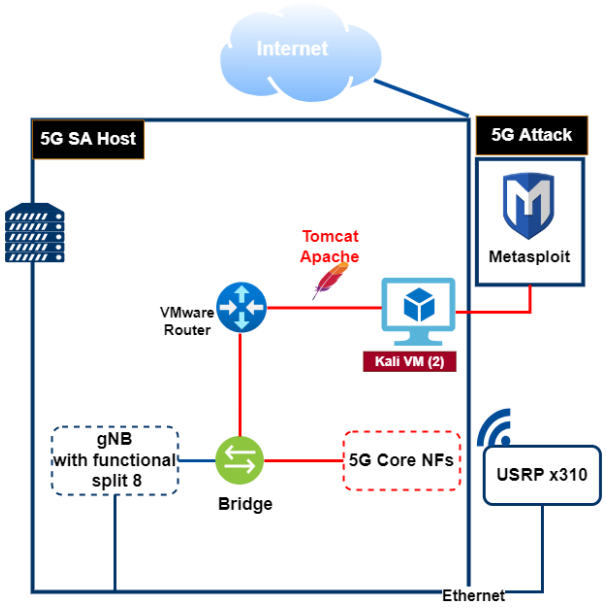

Figure 18 Architecture Metasploit Threat

The effective penetration testing requires refer to image below, Figure 19 Pre-Requisite Metasploit Threat" obtaining permission, defining roles, selecting appropriate hardware and software tools, and ensuring the test environment's testability to accurately assess the security posture of the target systems. (23)

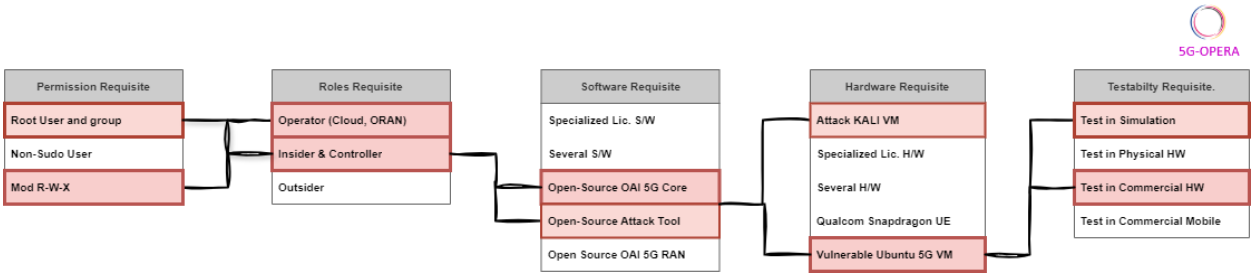

Figure 19 Pre-Requisite Metasploit Threat

10.2 Setup - Metasploit Threat

- The vulnerable machine 5G OAI Core should be up and running.
- The vulnerable machine must have a backdoor installed like Tomcat Apache Server, SQL, JAVA etc. In this threat scenario Tomcat Apache Web Server is used.
- The attacker machine should have KALI Operation System installed with Metasploit Hack application.
- Attacker Machine:
    - Initiate Metasploit MSFCONSOLE
    - Activate NMAP
    - Look for a backdoor entry
    - Deploy Payload
    - Configure Payload
    - Run the exploit
    - Get the reverse shell terminal
    - Attack the vulnerable machine (5G Core)

10.3 MITRE ATT&CK Framework - Metasploit Threat

- **TA**: TACTICS ID (MITRE Reference)
- **Txxxx**: Technique ID (Threat ID) refer to table below *Annex 3 MITRE ATT&CK Reference Metasploit* .
- **Txxxx.xxx**: Sub Technique ID (Sub-Threat ID), refer to table below, Annex 4 MITRE ATT&CK Threat Reference Metasploit

The penetration testing team does "Grey Box" testing and identifies security risks on the Open-Air Interface of the 5G Network. We used the MITTRE ATT&CK Framework refer to image below, Figure 20 MITRE ATT&CK Framework - Metasploit Threat" for Enterprise Matrices to map the globally access adversaries' tactics, techniques, and sub-techniques to our 5G Lab Network hacking.

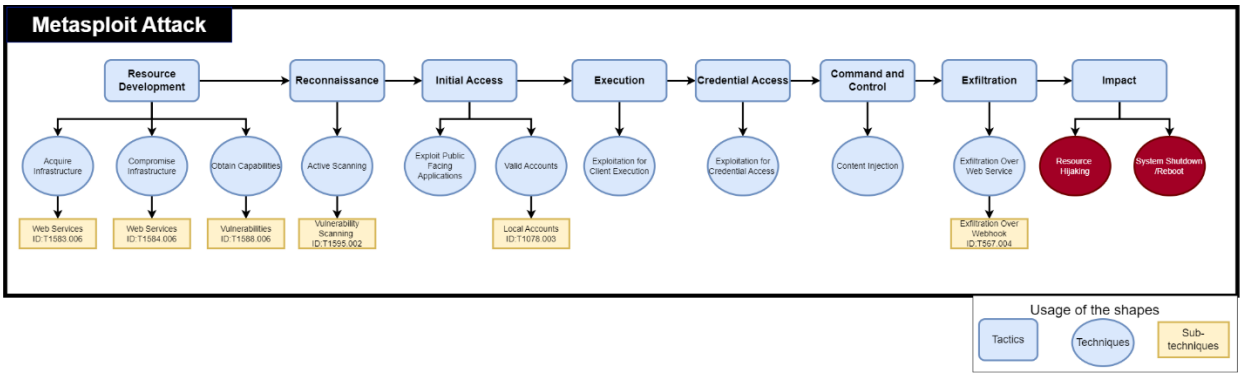

Figure 20 MITRE ATT&CK Framework - Metasploit Threat

Summary of Threat Steps

Phase 1: Resource Development
- Acquire Infrastructure: Download and install Apache Tomcat.
- Compromise Infrastructure: Set executable permissions for Tomcat.
- Obtain Capabilities: Initialize the Tomcat server with default credentials.

Phase 2: Reconnaissance
- Active Scanning: Use NMAP to scan the Apache Tomcat server.

Phase 3: Initial Access
- Exploit Public-Facing Application: Use Metasploit to target Tomcat.
- Valid Accounts: Search for Tomcat backdoor using Metasploit.

Phase 4: Execution
- Exploitation for Client Execution: Deploy the Metasploit payload.

Phase 5: Credential Access
- Exploitation for Credential Access: Configure payload parameters to gain access.

Phase 6: Command and Control
- Content Injection: Run the exploit to gain control and verify access.

Phase 7: Exfiltration
- Exfiltration over Web Services: Obtain a reverse shell from the vulnerable machine.

Phase 8: Impact
- Resource Hijacking: Use the compromised resources for malicious purposes.

- System Shutdown/Reboot: Reboot the system to disrupt operations.

10.4 Annex Attached

Annex 3 MITRE ATT&CK Reference Metasploit

Annex 4 MITRE ATT&CK Threat Reference Metasploit

10.5 Result of Metasploit Threat

The attacker successfully deployed a backdoor and gained root access as a sudo user on the vulnerable machine. This access through the Apache Tomcat server compromised the 5G Open Air Interface core, impacting the confidentiality and security of the 5G SA network refer to table below, Table 5 C-I-A-A Impact – Metasploit " and Table 6 Interfaces Impact - Metasploit ".

The attacker could manipulate the 5G VM1 machine and steal PLMN data (MCC, MNC, and IMSI IDs), affecting the network's accessibility.

Attack Result and Impact (C-I-A-A)				
Threat Name	**"C" Confidentiality**	**"I" Integrity**	**"A" Availability**	**"A" Authenticity**
Metasploit+NMAP Threat	**affected**			**affected**

Table 5 C-I-A-A Impact – Metasploit Attack

Attack Node and Interfaces - 5G Threat Modelling				
Attack Name	**Attack Node**	**Vulnerable Node**	**Primary Affected - 5G Interface**	**Secondary Affected - 5G Interface**
Metasploit+NMAP Attack	**Kali VM with backdoor**	**5G Core**	**N6**	**N2 and N3**

Table 6 Interfaces Impact - Metasploit Attack

11 VSFTPD Threat

11.1 Introduction & Pre-Requisite – VSFTPD Threat

The VSFTPD (Very Secure FTP Daemon) threat exploits vulnerabilities in the VSFTPD software refer to image below Figure 21 "*Architecture VSFTPD Threat*", commonly used for file transfers. Attackers use various methods to gain unauthorized access and execute malicious commands by exploiting software flaws, configuration issues, or outdated versions. (24)

Misconfigurations such as weak access controls and encryption make systems more vulnerable. In a 5G Standalone (SA) infrastructure on Ubuntu Server 20.0.4 LTS, attackers can install and configure VSFTPD to create vulnerabilities. They use a Cron Job to run a bash script continuously, monitoring and exploiting the system

through the default daemon port (8228). This allows attackers to gain root access via a reverse proxy, demonstrating the serious risks of VSFTPD vulnerabilities.

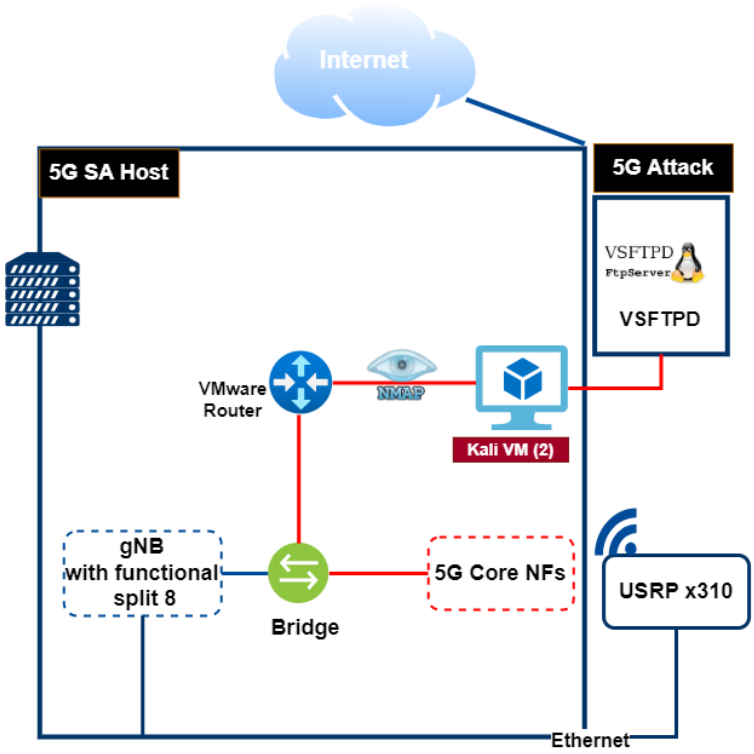

Figure 21 Architecture VSFTPD Attack

The effective penetration testing requires refer to image below **Error! Reference source not found.** *Figure 22 "Pre-Requisite – VSFTPD Threat"* obtaining permission, defining roles, selecting appropriate hardware and software tools, and ensuring the test environment's testability to accurately assess the security posture of the target systems.

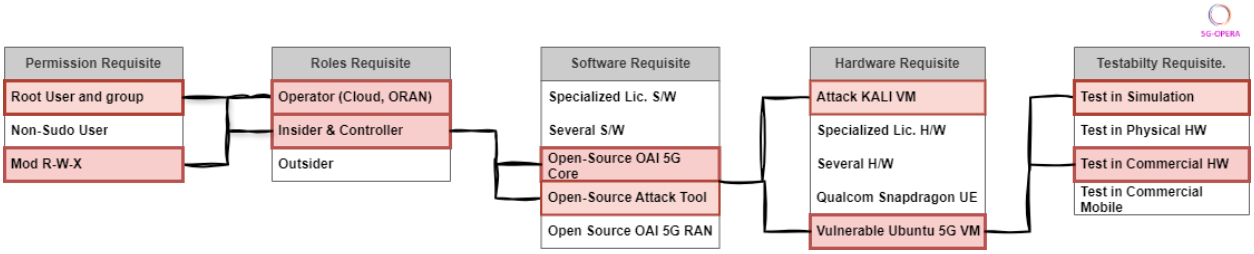

Figure 22 Pre-Requisite VSFTPD Attack

VSFTPD is the Very Secure FTP Daemon (FTP is the file transfer protocol). It is a secure and fast server, and we are using version 3.0. The normal FTP is a server process which uses TCP protocol and listen to port specified in the FTP. VSFTP is a GPL licensed FTP server. We can use VSFTP for many purposes.

- Virtual IP configurations
- Virtual Users
- Virtual networks

- BW Throttling for Stand Alone users.

- Just like any other server it has also got some backdoor vulnerability.
- The 5G Standalone machine was hosted on Ubuntu Server 20.0.4. LTS, the server already has FTP and VSFTPD daemon up and running.
- If the VSFTPD server is not installed, it can be installed for test purpose.
- After the installation we need to setup the configuration which can give right access to make the 5G SA machine vulnerable.
- We call this configuration file “vsftpd.conf”.

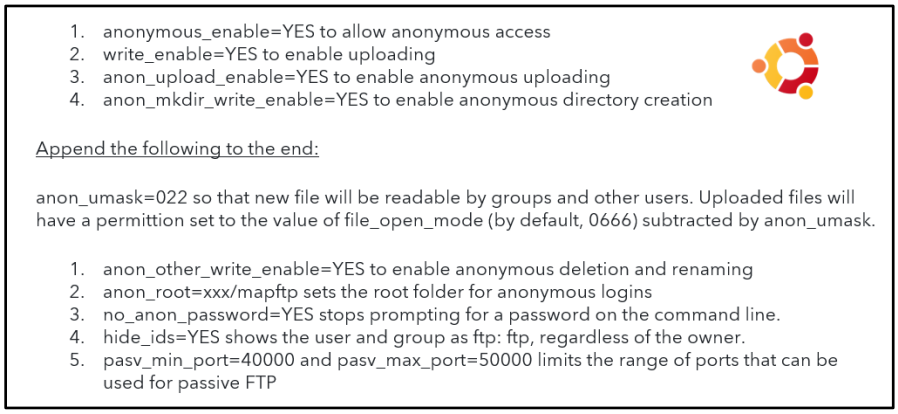

Figure 23 VSFTPD.conf.

- After the configuration is ready, a Cron Job must be build, which executes every 1 minute (we can custom it for 5 minutes too). The Cron job should be a bash script.
- VSFTPD has the daemon port 8228.

11.2 MITRE ATT&CK Framework - VSFTPD Threat

- **TA**: TACTICS ID (MITRE Reference)
- **Txxxx**: Technique ID (Threat ID) refer to table below, Annex 5 MITRE ATT&CK Reference VSFTPD **Txxxx.xxx**: Sub Technique ID (Sub-Threat ID), refer to table below, Annex 6 MITRE ATT&CK Threat Reference VSFTPD

The Penetration testing team does “Grey Box” testing and identifies security risks on the Open-Air Interface of the 5G Network. We used the MITRE ATT&CK Framework refer to image below, Attack, Figure 24 *“MITRE Framework-VSFTPD Threat”* for Enterprise Matrices to map the globally access adversaries’ tactics, techniques, and sub-techniques to our 5G Lab Network hacking.

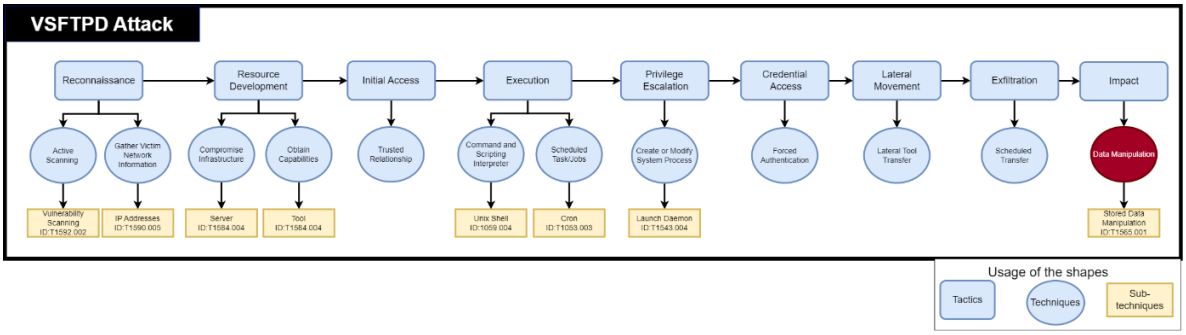

Figure 24 MITRE ATTACK Framework VSFTP Threat

Summary of Attack Steps

Tactical Phase 1: Reconnaissance
- Active Scanning
- Gather victim Network Information
- Vulnerability Scanning: Scanning for software vulnerabilities
- IP Addresses: Gathering victim's IP addresses

Tactical Phase 2: Resource Development
- Compromise Infrastructure
- Obtain Capabilities
- Server: Using or acquiring servers for staging attacks
- Tool: Acquiring or using tools for attacks

Tactical Phase 3: Initial Access
- Trusted Relationship: Exploiting third-party relationships for access

Tactical Phase 4: Execution
- Command and Scripting Interpreter
- Scheduled Task/Job
- Unix Shell: Using Unix shell commands for execution
- Cron: Using Cron jobs for scheduling malicious tasks

Tactical Phase 5: Privilege Escalation
- Create or Modify System Process
- Launch Daemon: Using launch daemons for persistence with elevated privileges

Tactical Phase 6: Credential Access
- Forced Authentication: Forcing users to provide authentication information

Tactical Phase 7: Lateral Movement
- Lateral Tool Transfer: Moving tools or files across compromised systems

Tactical Phase 8: Exfiltration
- Scheduled Transfer: Timing data exfiltration to blend with normal traffic

Tactical Phase 9: Impact
- Data Manipulation
- System Shutdown/Reboot
- Stored Data Manipulation: Altering data to affect outcomes or hide activities.

11.3 Annex Attached

Annex 5 MITRE ATT&CK Reference VSFTPD

Annex 6 MITRE ATT&CK Threat Reference VSFTPD

11.4 Result of VSFTPD Threat

The VSFTPD threat exploits vulnerabilities within the VSFTPD software, unfolding in stages:

- **Initial Compromise**: The attacker connects to the susceptible VSFTPD server, triggering a backdoor mechanism with a predefined username sequence.
- **Backdoor Activation**: Successful exploitation triggers a listening socket, enabling unauthorized access to the server.
- **Remote Control**: The attacker gains unauthorized remote control over the server, often with a shell or command execution environment.
- **Impact**: Potential outcomes include data theft, website defacement, server hijacking, malware installation, or using the server for further attacks.

Additionally, the attacker gains ROOT Access to the vulnerable system, compromising the confidentiality of the 5G SA and manipulating the 5G VM1 machine refer to table below, Table 7 C-I-A-A Impact - VSFTPD ” and Table 8 Interfaces Impact - VSFTPD ”. Data, including PLMN details, is exfiltrated, impacting the accessibility of the 5G SA Network.

Attack Result and Impact (C-I-A-A)				
Attack Name	**"C" Confidentiality**	**"I" Integrity**	**"A" Availability**	**"A" Authenticity**
VSFTPD Threat	**Affected**			**Affected**

Table 7 C-I-A-A Impact - VSFTPD Threat

Attack Node and Interfaces - 5G Threat Modelling				
Attack Name	**Attack Node**	**Vulnerable Node**	**Primary Affected - 5G Interface**	**Secondary Affected - 5G Interface**
VSFTPD Threat	**Kali VM with backdoor**	**5G Core**	**N6**	**N2 and N3**

Table 8 Interfaces Impact - VSFTPD Threat

12 Fuzzing Core

12.1 Introduction & Pre-Requisite – Fuzzing Core

The 5G network traffic open source fuzzer, using the 5GReplay tool, evaluates 5G components by replaying and modifying network traffic. Fuzz testing on the Open-Air Interface (OAI) source involved sending malformed NGAP/NAS-5GS protocol messages to assess the OAI-AMF function's resilience. The strategy was to create packets valid enough not to be discarded immediately but malformed enough to induce errors.

The 5GReplay tool refer to image below Figure 25 Architecture Fuzzing Core” allows packet selection and modification from captured network traffic using deep packet inspection. The impact was significant, with the OAI-

AMF function disengaging multiple times due to segmentation faults, suggesting potential disruption leading to Denial-of-Service scenarios. (25)

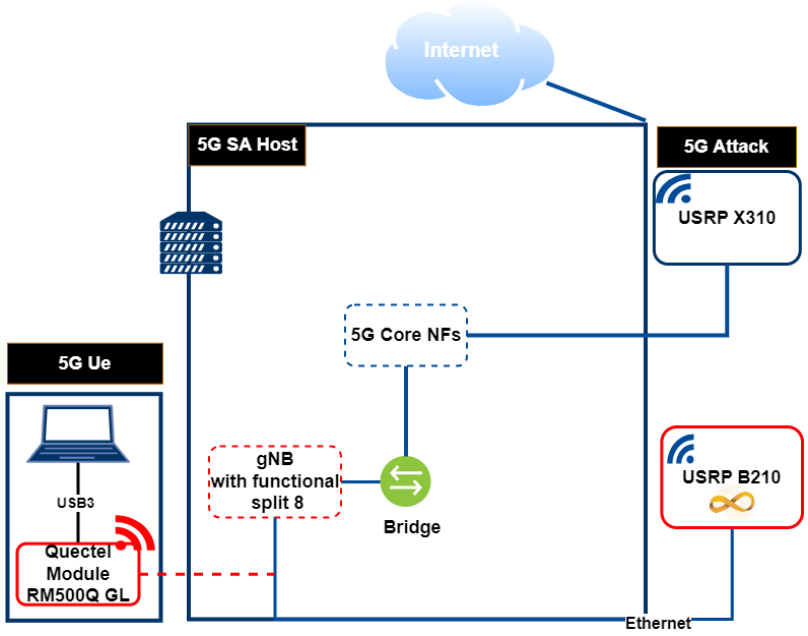

Figure 25 Architecture Fuzzing Core

The effective penetration testing requires refer to image below, **Error! Reference source not found.**" obtaining permission, defining roles, selecting appropriate hardware and software tools, and ensuring the test environment's testability to accurately assess the security posture of the target systems.

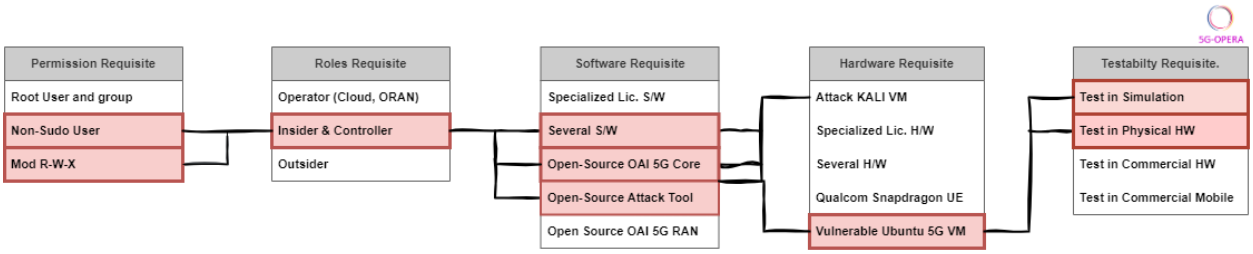

Figure 26 Pre-Requisite Fuzzing Core

12.2 Setup – Fuzzing Core

On an Ubuntu OAI 5G Core machine, to set up and compile the 5Greplay software along with mmt-dpi, follow these steps:

Preparation:

Update your system and install necessary tools and libraries such as gcc, make, git, libxml2-dev, libpcap-dev, libconfuse-dev, and libsctp-dev using the command `git clone` https://github.com/montimage/5greplay.git refer to image below, Figure 27 "RULE" & "CONFIG" File - Fuzzing Core.

Compilation & Installation

- Clean up previously compiled objects with make clean.
- Compile the software in its local directory using make.
- To compile sample rules in the rules folder, use make sample-rules.
- Enable debugging with GDB (The GNU Project Debugger) it allows you to see what is going inside the program by compiling with make DEBUG=1.
- For using Valgrind DRD (the threat error detector) it allows to detect error in multithreat C++ program compiler with make DEBUG=1 VALGRIND=1.

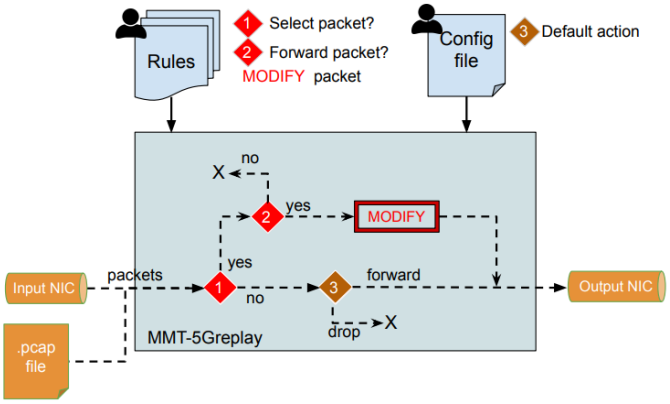

Figure 27 "RULE" & "CONFIG" File - Fuzzing Core

12.3 MITRE ATT&CK Framework – Fuzzing Core

- **TA**: TACTICS ID (MITRE Reference)
- **Txxxx**: Technique ID (Threat ID) refer to table below, *Annex 9 MITRE ATT&CK Reference Fuzzing Core*
- **Txxxx.xxx**: Sub Technique ID (Sub-Threat ID), refer to table below, *Annex 10 MITRE ATT&CK Threat Reference Fuzzing Core*

The Penetration testing team does “Grey Box” testing and identifies security risks on the Open-Air Interface of the 5G Network. We used the MITRE ATT&CK Framework refer to image below, Figure 28 MITRE ATT&CK Framework-Fuzzing Core for Enterprise Matrices to map the globally access adversaries’ tactics, techniques, and sub-techniques to our 5G Lab Network hacking.

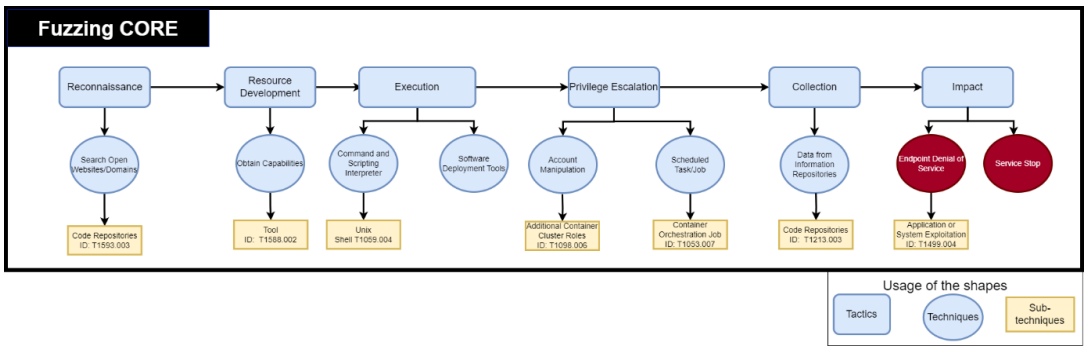

Figure 28 MITRE ATT&CK Framework-Fuzzing Core

Summary of Attack Steps

Tactical Phase 1- Reconnaissance

- Technical Step 1: Searching Open Websites/Domains to find the 5G Replay Core fuzzing tool.

Tactical Phase 2 - Resource Development

- Technical Step 2 Obtaining Capabilities by creating a bridge and rule file.

Tactical Phase 3 - Execution Phase

- Technical Step 3: Using Command and Scripting Interpreter to create a config file and install rules in offline mode.
- Technical Step 4: Using Software Deployment Tools to implement rules in online mode.

Tactical Phase 4 - Privilege Escalation Phase

- Technical Step 5: Account Manipulation by implementing RULE File for NGAP Fuzzing and compiling the config file for NGAP Fuzzing.
- Technical Step 6: Scheduling Task/Job to compile a rule file to Fuzz SCTP (transport layer).

Tactical Phase 5 - Collection Phase

- Technical Step 7: Gathering Data from Information Repositories, detecting a null pointer dereference in AMF, and accessing the value stored at a memory address.

Tactical Phase 6 - Impact Phase

- Technical Step 8: Causing Endpoint Denial of Service for Availability.
- Technical Step 9: Stopping Services for Availability.

12.4 Annex Attached

Annex 9 MITRE ATT&CK Reference Fuzzing Core

Annex 10 MITRE ATT&CK Threat Reference Fuzzing Core

12.5 Result of Fuzzing Core

A null pointer dereference was detected in AMF:

The 5G Core fuzzing impacts the **"Availability"** of 5G Radio access Network. And the Core cannot automatically connect to transmit and OAI-AMF container OAI gNB until hard reset / manual reset was done, refer to table below,

Table 9 C-I-A-A Impact: Fuzzing Core and *Table 10 Interfaces Impact: Fuzzing Core* The attack vector Denial of service was exploited when gNB resource was unavailable to its intended users indefinitely disrupting services of a host connected to a network.

Attack Result and Impact (C-I-A-A)				
Attack Name	**"C" Confidentiality**	**"I" Integrity**	**"A" Availability**	**"A" Authenticity**
Fuzzing Core			**Affected**	

Table 9 C-I-A-A Impact: Fuzzing Core

Attack Node and Interfaces - 5G Threat Modelling				
Attack Name	**Attack Node**	**Vulnerable Node**	**Primary Affected - 5G Interface**	**Secondary Affected - 5G Interface**
Fuzzing Core	**Ubuntu VM 5G Replay**	**5G Core**	**UE / Air Interface**	**N1 & N2**

Table 10 Interfaces Impact: Fuzzing Core

13 Fuzzing RAN

13.1 Introduction & Pre-Requisite – Fuzzing RAN

Fuzzing is an automated technique used to find software vulnerabilities by sending invalid or random inputs to cause crashes or malfunctions. In this case, a network protocol fuzzer was used to identify vulnerabilities in the 5G Radio Access Network (RAN) from the User Equipment (UE) or modem side, specifically using a Qualcomm chipset. The test environment employed open-source implementations of 5G Core and 5G RAN via OpenAirInterface and Open5GS. The attacker setup involved OpenAirInterface Core and Open5GS RAN, demonstrating that the RAN can completely freeze when a 5G connection is lost using the 5G Houl fuzzer refer to image below **Error! Reference source not found.**". (26)

The attack involved impersonating a legitimate gNB (5G base station) by using known cell tower connection parameters. Once the target UE connected to the adversarial gNB due to stronger signal strength, the actual connection was lost. The attacker could then manipulate downlink messages to the UE, enabling various attacks. These vulnerabilities can be exploited over-the-air by starting a malicious gNB within the target UE's radio range.

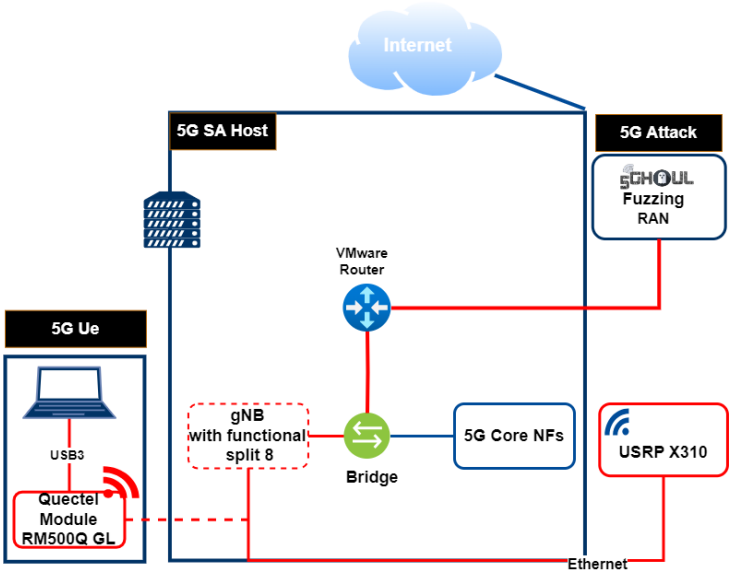

Figure 29 Architecture Fuzzing RAN

The effective penetration testing requires refer to image below, Figure 30 Pre-Requisite Fuzzing RAN" obtaining permission, defining roles, selecting appropriate hardware and software tools, and ensuring the test environment's testability to accurately assess the security posture of the target systems.

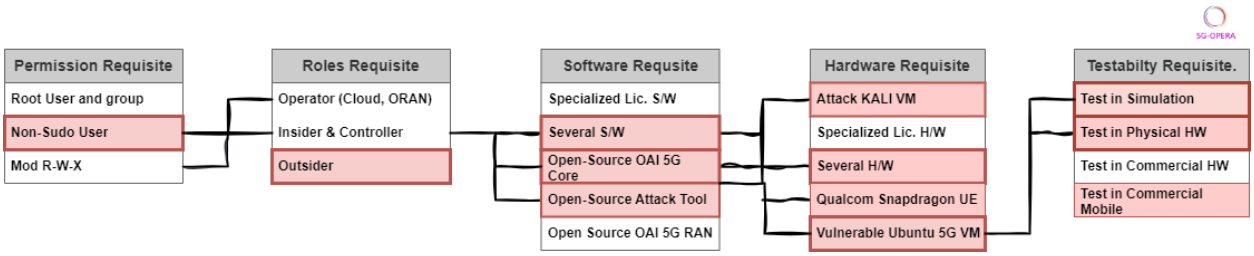

Figure 30 Pre-Requisite Fuzzing RAN

13.2 Setup – Fuzzing RAN

We use 5G Houl: When exploited, 5GHoul vulnerabilities aim to mislead UEs, such as smartphones and other 5G-capable devices, into connecting with a malicious base station (gNB) set up by 5GHoul in our LAB. After establishing a connection, these vulnerabilities could be leveraged to persistently initiate attacks that result in dropped connections, freezing of the device requiring a manual restart.

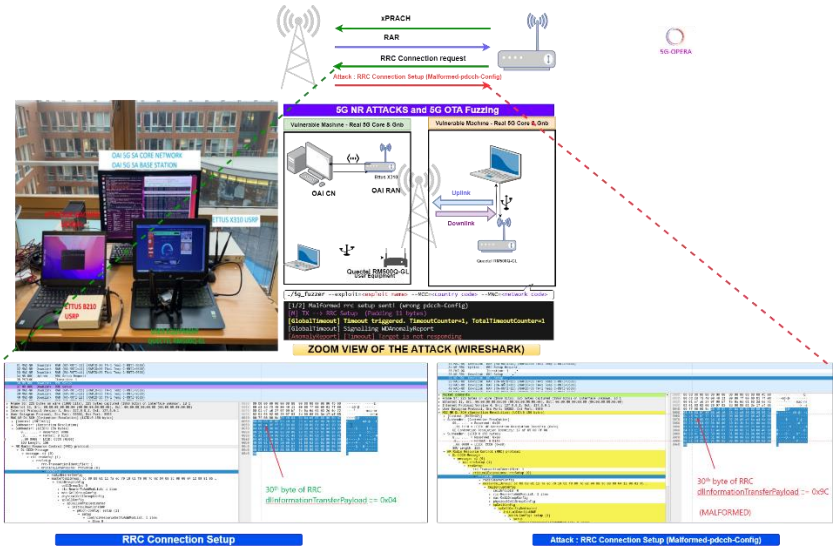

Figure 31 Lab-Setup Fuzzing RAN

- *mkdir 5ghoul* https://github.com/asset-group/5ghoul-5g-nr-attacks/raw/master/container.sh
- *chmod +x container.sh*
- *./container.sh run release-5g ##* ***opens wsdissector if successful installation.***

After the installation is complete refer to image above, **Error! Reference source not found.**, to perform the attack, configuration of the 5Ghoul must be adjusted with respect to OAI configuration. Since 5Ghoul attack machine mimics the original gNB, MCC, MNC, and APN name should be adjusted same with the OAI gNB.

The 5G cellular network architecture refer to image below, Figure 32 Connectivity Fuzzing RAN, is built around three primary components: the gNodeB (gNB), User Equipment (UE), and the Core Network. The gNB acts as the base station, facilitating wireless communication between the UE and the 5G core network. UEs encompass end-user devices like smartphones and tablets that are 5G-enabled and connect to the network via the gNB. The Core Network serves as the backbone of the 5G architecture, responsible for essential functions such as authentication, security, mobility management, session establishment, and routing data between network entities.

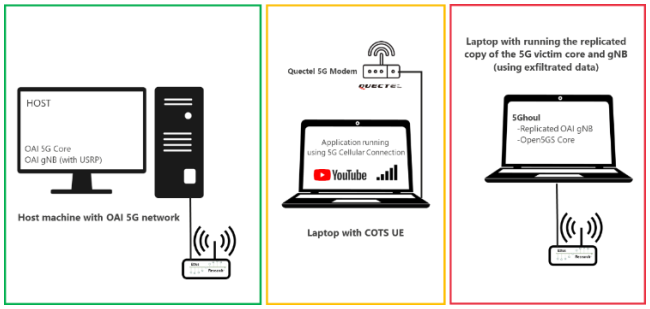

Figure 32 Connectivity Fuzzing RAN

On initiating the 5G Fuzzing RAN, do not forget to return the 5Ghoul to initial configurations refer to image below, Figure 33 Initiating 5G RAN Fuzzer with --EnableFuzzing=true is used, then after the attack, --EnableFuzzing=false should be done to return the 5Ghoul its initial configuration.

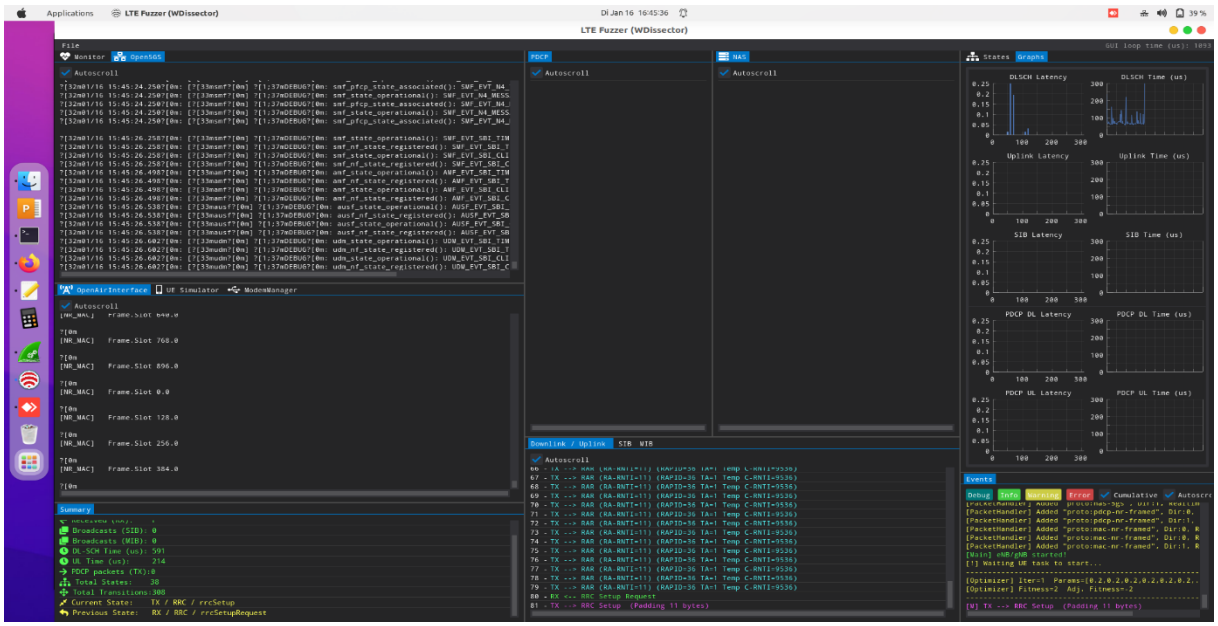

Figure 33 Initiating 5G RAN Fuzzer

13.3 MITRE ATT&CK Framework – Fuzzing RAN

- **TA**: TACTICS ID (MITRE Reference)
- **Txxxx**: Technique ID (Threat ID) refer to table below, *Annex 11 MITRE ATT&CK Reference Fuzzing RAN*
- **Txxxx.xxx**: Sub Technique ID (Sub-Threat ID), refer to table below, *Annex 12 MITRE ATT&CK Threat Reference Fuzzing RAN*

The IABG Penetration testing team does “Grey Box” testing and identifies security risks on the Open-Air Interface of the 5G Network. We used the MITTRE ATT&CK Framework refer to image below, Figure 34 MITRE ATT&CK Framework Fuzzing RAN”, for Enterprise Matrices to map the globally access adversaries’ tactics, techniques, and sub-techniques to our 5G Lab Network hacking.

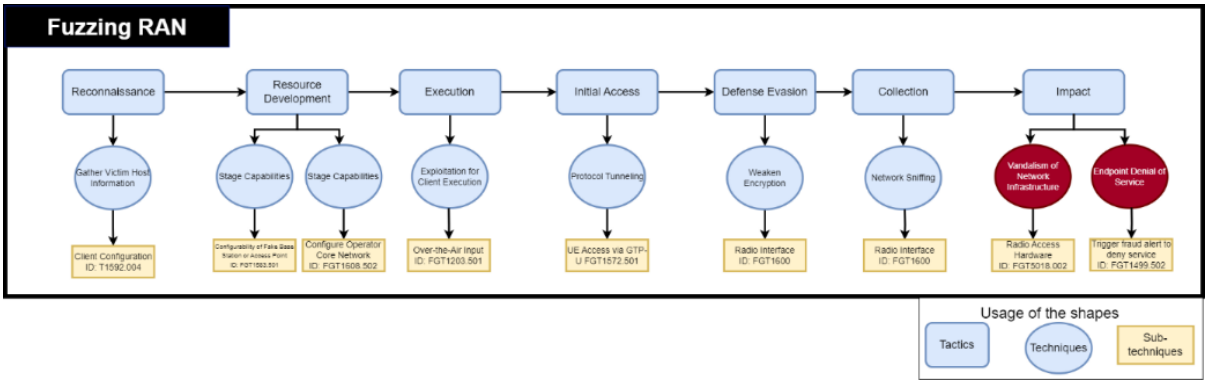

Figure 34 MITRE ATT&CK Framework Fuzzing RAN

Phase 1: Reconnaissance

- **Tactic:** Gather victim host information
- **Actions:** Start 5G Core OAI, 5G RAN OAI connect RM500Q-GL 5G HAT

Phase 2: Resource Development

- **Tactic:** Stage capabilities
- **Actions:** Configure fake base station and operator core network

Phase 3: Execution

- **Tactic:** Exploitation for client execution
- **Actions:** Initiate OAI 5G RAN and RAN fuzzing techniques

Phase 4: Initial Access

- **Tactic:** Protocol tunneling
- **Actions:** Follow GTPU packets to UPF

Phase 5: Initial Access (Repeated)

- **Tactic:** Protocol tunneling
- **Actions:** Follow GTPU packets to UPF

Phase 6: Defense Evasion

- **Tactic:** Weaken encryption
- **Actions:** Sign into attacker network, manipulate NAS PDU

Phase 7: Impact

- **Tactic:** Vandalism and denial of service
- **Actions:** Exploit radio access hardware vulnerabilities, trigger fraud alert.

13.4 Annex Attached

Annex 11 MITRE ATT&CK Reference Fuzzing RAN

Annex 12 MITRE ATT&CK Threat Reference Fuzzing RAN

13.5 Result of Fuzzing RAN

An attacker within radio range of Qualcomm's RM500Q-GL modems can downgrade 5G connectivity or block service by sending a corrupted RRC frame from a separate base station. This involves altering a specific byte in the NAS PDU during the RRC Attach Procedure, disrupting the modem's ability to connect to any 5G network.

Affected devices, such as smartphones and connected routers, cannot reconnect to 5G network until manually rebooted, as toggling airplane mode is ineffective. This vulnerability impacts a wide range of Qualcomm-enabled 5G devices, is easy to exploit without needing SIM card details, and occurs before security authentication. The attack disrupts the **availability** of the 5G Radio Access Network (RAN), causing a denial of service that prevents automatic reconnection until a hard reset, refer to table below, Table 11 C-I-A-A Impact: Fuzzing RAN *and* Table 12 Interfaces Impact: Fuzzing RAN. (27)

Attack Result and Impact (C-I-A-A)				
Attack Name	**"C" Confidentiality**	**"I" Integrity**	**"A" Availability**	**"A" Authenticity**
Fuzzing RAN			**affected**	

Table 11 C-I-A-A Impact: Fuzzing RAN

Attack Node and Interfaces - 5G Threat Modelling				
Attack Name	**Attack Node**	**Vulnerable Node**	**Primary Affected - 5G Interface**	**Secondary Affected - 5G Interface**
Fuzzing RAN	**Ubuntu machine with 5G Houl**	**5G RAN and Radio Interface**	**UE / Air Interface**	**N1 & N2**

Table 12 Interfaces Impact: Fuzzing RAN

14 Data-Exfiltration Threat

14.1 Introduction & Pre-Requisite – Data-Exfiltration Threat

Data-Exfiltration, also known as data extrusion or data exportation, involves the unauthorized extraction of data from vulnerable machines. In a 5G network scenario, a Python script was created to exfiltrate data via a data leak or breach, working in real-time or on recorded logs.

The attacker, an insider with user or group access to the 5G Core machine, already had initial access to the 5G network. The attack focused on the information exchange between the 5G Core network and the 5G RAN network, which is hosted on a virtual machine. The Python script discreetly extracted sensitive information, such as encryption keys, PLMN IDs, and ciphering algorithms, from System Information Blocks (SIBs) exchanged between Open RAN and the 5G Core refer to image below Figure 35 Architecture Data-Exfiltration The "initial access" phase was skipped in the MITRE ATT&CK Framework execution due to the attacker's pre-existing access.

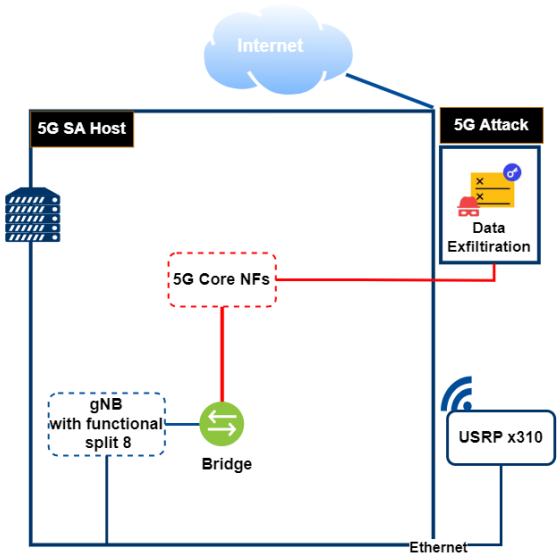

Figure 35 Architecture Data-Exfiltration

The effective penetration testing requires refer to image below, Figure 36 Pre-Requisites Data-Exfiltration Figure 36 Pre-Requisites Data-Exfiltration Threat obtaining permission, defining roles, selecting appropriate

hardware and software tools, and ensuring the test environment's testability to accurately assess the security posture of the target systems.

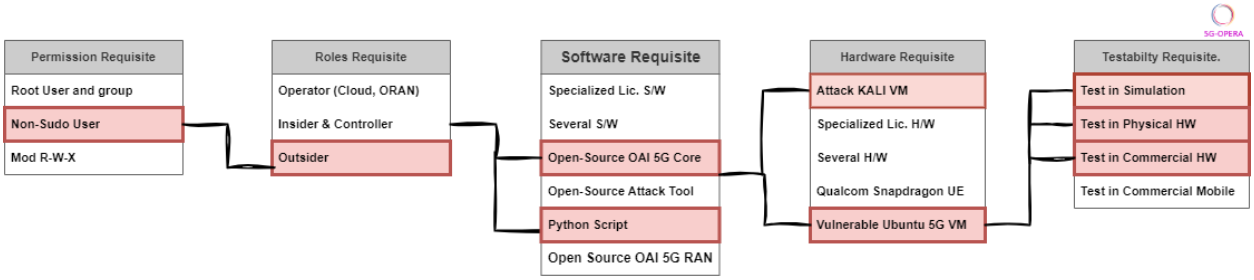

Figure 36 Pre-Requisites Data-Exfiltration Threat

14.2 Setup – Data-Exfiltration Threat

The vulnerable machine 5G OAI Core should be up and running. The attacker machine can be any Operation System installed, but should be able to transfer the Phishing script from attacker to Kali Machine

- Python Installed
- Python Lib [math, psutil, Pyshark, Socket]
- Python Script 1: Attack the vulnerable machine (5G RAN Live Network)
- Python Script 2: Attack the vulnerable machine (5G RAN Recorded Wireshark Logs)

During Execution, display Interfaces - It prints the list of interfaces with their corresponding indices for user selection, Check for NGAP Protocol: The function packet analyses checks if the packet contains the NGAP (Next Generation Application Protocol) layer. Extract MCC and MNC: If the NGAP layer contains Mobile Country Code (MCC) and Mobile Network Code (MNC) attributes, it extracts and prints these values along with the NGAP ID.

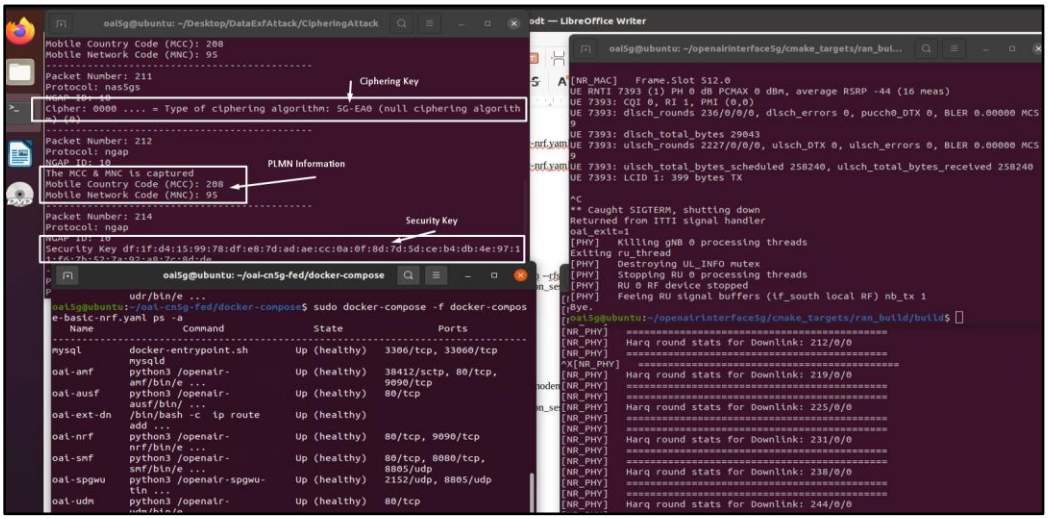

Figure 37 Result Data-Exfiltration Threat

14.3 MITRE ATT&CK Framework – Data-Exfiltration Threat

- **TA**: TACTICS ID (MITRE Reference)
- **Txxxx**: Technique ID (Threat ID) refer to table below, *Annex 13 MITRE ATT&CK Reference Data-Exfiltration*
- **Txxxx.xxx**: Sub Technique ID (Sub-Threat ID), refer to table below, *Annex 14 MITRE ATT&CK Threat Reference Data-Exfiltration*

The IABG Penetration testing team does “Grey Box” testing and identifies security risks on the Open-Air Interface of the 5G Network. We used the MITTRE ATT&CK Framework refer to image below, Figure 38 MITRE ATT&CK Data-Exfiltration " for Enterprise Matrices to map the globally access adversaries’ tactics, techniques, and sub-techniques to our 5G Lab Network hacking.

For the Data Exfiltration Threat, we filtered out 6 different Tactical Phases and 6 different Techniques with 5 different Sub-Techniques. For the Technique “Data Extraction” no convenient issue in the MITRE Reference tables is available, so we defined MITRE Reference T02.IABG and for Sub-Techniques T02.IABG.002.

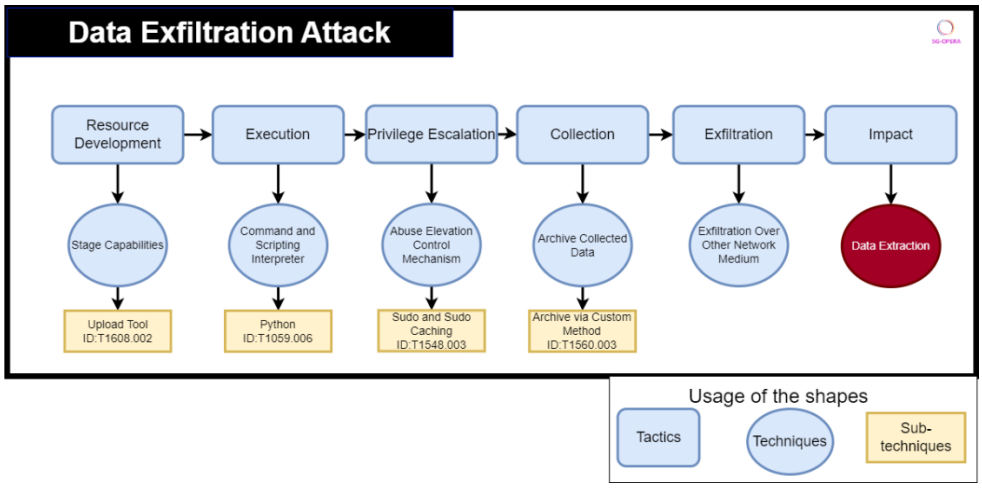

Figure 38 MITRE ATT&CK Data-Exfiltration Attack

Phase 1: Resource Development
- Upload tools and develop capabilities using Python script.

Phase 2: Execution
- Run the Python script with necessary libraries and discover network messages.

Phase 3: Privilege Escalation
- Run the script with ROOT (sudo) privileges.

Phase 4: Collection
- Exfiltrate and collect custom data from 5G SA protocols.

Phase 5: Exfiltration
- Extract and execute confidential information over network mediums.

Phase 6: Impact
- Extract critical network information and cause data theft.

14.4 Annex Attached

Annex 13 MITRE ATT&CK Reference Data-Exfiltration

Annex 14 MITRE ATT&CK Threat Reference Data-Exfiltration

14.5 Result of Data Exfiltration Threat

The script lists and displays available network interfaces using psutil, allowing user selection. It then captures live network traffic on the selected interface with pyshark. The packet analysis function checks for the NGAP layer in packets, extracting and printing details such as MCC, MNC, NGAP ID, encryption algorithms, and security keys.

This analysis aids in penetration testing and data exfiltration within a 5G network environment refer to table below, Table 13 C-I-A-A Impact: Data Exfiltration *and* Table 14 Interfaces Impact: Data-Exfiltration Threat.

Attack Result and Impact (C-I-A-A)				
Attack Name	**"C" Confidentiality**	**"I" Integrity**	**"A" Availability**	**"A" Authenticity**
Data Exfiltration	**affected**	**affected**		

Table 13 C-I-A-A Impact: Data Exfiltration Attack

Attack Node and Interfaces - 5G Threat Modelling				
Attack Name	**Attack Node**	**Vulnerable Node**	**Primary Affected - 5G Interface**	**Secondary Affected - 5G Interface**
Data Exfiltration	**Running Python Script**	**5G Core and RAN**	**N14**	**N4**

Table 14 Interfaces Impact: Data-Exfiltration Threat

15 Jamming Threat

15.1 Introduction & Pre-Requisite – Jamming Threat

This demonstration showcases a Denial of Service (DoS) attack using jamming to disrupt legitimate radio communication by introducing noise and causing external interference. The jammer overwrites the radio transmission signal with a target signal, impacting both military radar and commercial network communications. Jamming attacks target the physical layer of communication protocols by emitting radio frequency signals across the same frequency band as the targeted system refer to image below Figure 39 Architecture Jamming ".

The effects of such an attack can be severe, leading to communication outages, signal degradation, increased error rates, and complete loss of connectivity, which is critical for military communications, emergency services, and air traffic control.

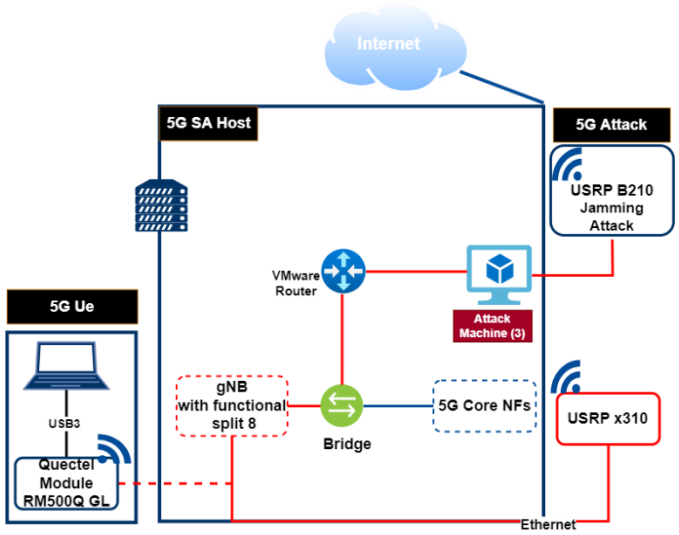

Figure 39 Architecture Jamming Threat

The effective penetration testing requires refer to image below, Figure 40 Pre-Requisite Jamming " obtaining permission, defining roles, selecting appropriate hardware and software tools, and ensuring the test environment's testability to accurately assess the security posture of the target systems.

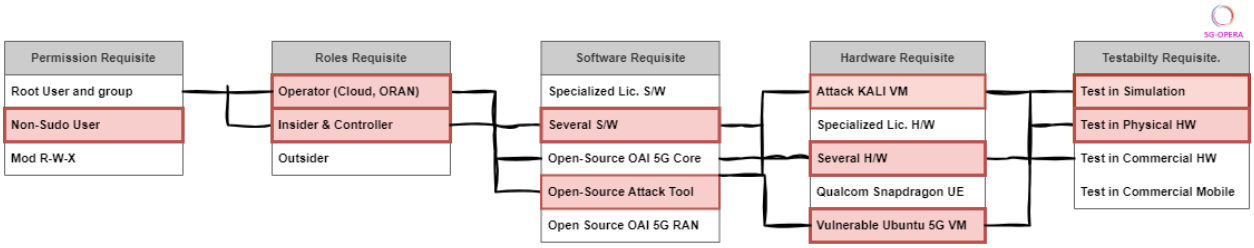

Figure 40 Pre-Requisite Jamming Attack

15.2 Setup – Jamming Threat

- The vulnerable machine 5G OAI Core should be up and running.
- The attacker machine should have Ubuntu Operation System installed with Python and GNU Radio Companion, application refer to image below, Figure 43 MITRE D3FEND for HYDRA Threat"
- Attacker Machine:
  - HackRF One attached as hardware which is a SDR
  - Initiate GNU RADIO
  - Increase power in step size of 10dB.

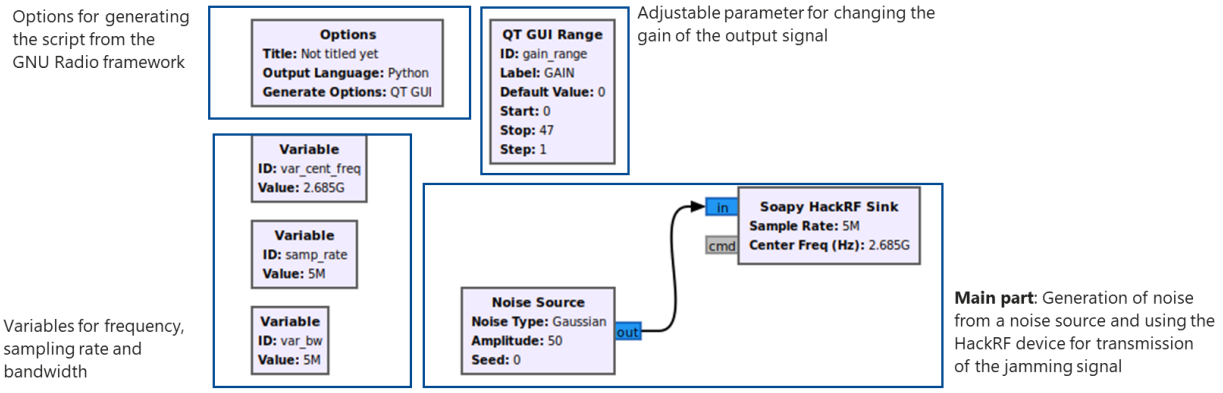

Figure 43 Jamming GNU Radio Companion

15.3 MITRE ATT&CK Framework – Jamming Threat

- **TA**: TACTICS ID (MITRE Reference)
- **Txxxx**: Technique ID (Threat ID) refer to table below, *Annex 7 MITRE ATT&CK Reference Jamming*
- **Txxxx.xxx**: Sub Technique ID (Sub-Threat ID), refer to table below, *Annex 8 MITRE ATT&CK Threat Reference Jamming*

The Penetration testing team does "Grey Box" testing and identifies security risks on the Open-Air Interface of the 5G Network. We used the MITRE ATT&CK Framework refer to image below, Figure 41 MITRE Framework - Jamming for Enterprise Matrices to map the globally access adversaries' tactics, techniques, and sub-techniques to our 5G Lab Network hacking.

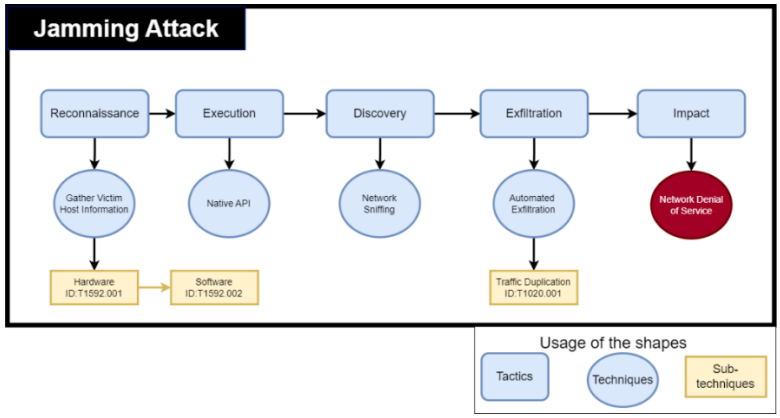

Figure 41 MITRE Framework - Jamming Threat

Phase 1: Reconnaissance

- Step 1: Gather Victim Host Information
  - Hardware: Used HACKRF One to scan frequency spectrum, channel bandwidth, and cell tower information.
  - Software: Used GNU Radio to gather software details and scan radio transmissions.

Phase 2: Execution

- Step 2: Native API
  - Executed HackRF ONE Radio in a virtual machine with Linux operating system.

Phase 3: Discovery

- Step 3: Network Sniffing
  - Configured GNU Radio with scanned PLMN and cell tower information.

Phase 4: Exfiltration

- Step 4: Automated Data-Exfiltration
  - Increased signal power to create interference and duplicated traffic using artificial noise.

Phase 5: Impact

- Step 5: Network Denial of Service
  - Conducted DoS attacks to block signal and coverage, causing service loss to UE.

15.4 Annex Attached

Annex 7 MITRE ATT&CK Reference Jamming

Annex 8 MITRE ATT&CK Threat Reference Jamming

15.5 Result of Jamming Threat

A jamming threat disrupts wireless communication by introducing constant noise, resulting in abnormal disconnections and a Denial of Service (DoS) attack. This interference degrades the Signal to Noise Ratio (SNR) between the User Equipment (UE) and the provider cell.

In our 5G lab, we used Quectel RM 500 GL modems. The jammer, placed nearby, increased interference, causing the 5G Standalone (SA) network to disconnect from the Quectel UE 5G modem refer to table below, Table 15 C-I-A-A Impact: Jamming Threat *and* Table 16 Interfaces Impact: Jamming Threat

Attack Result and Impact (C-I-A-A)				
Attack Name	**"C" Confidentiality**	**"I" Integrity**	**"A" Availability**	**"A" Authenticity**
Jamming			**affected**	

Table 15 C-I-A-A Impact: Jamming Threat

Attack Node and Interfaces - 5G Threat Modelling				
Attack Name	**Attack Node**	**Vulnerable Node**	**Primary Affected - 5G Interface**	**Secondary Affected - 5G Interface**
Jamming	**Ubuntu VM with GNU Radio**	**5G Radio Interface**	**UE / Air Interface**	**N1 & N2**

Table 16 Interfaces Impact: Jamming Threat

16 MITRE D3FEND Framework

To implement countermeasures against multiple attacks, as mentioned in chapter 7 subchapter 3, the MITRE D3FEND Framework provides proactive measures defined for specific already identified MITRE ATT&CK techniques, in the following subsections the description of the performed defense actions is explained. D3FEND Matrix | MITRE D3FEND™ (28)

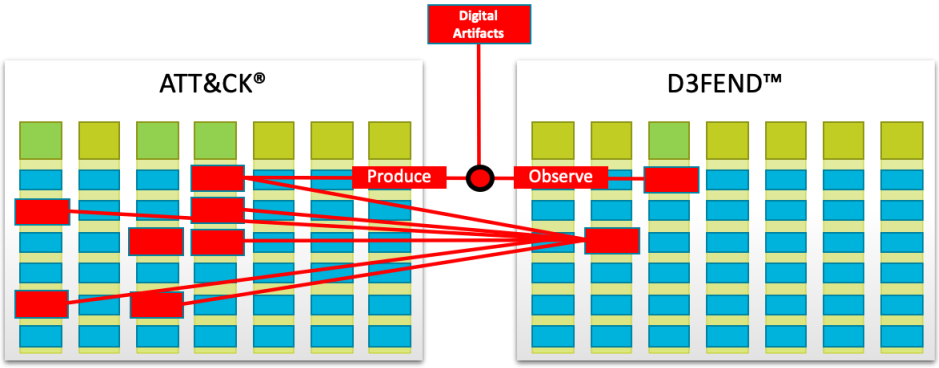

Figure 42 MITRE ATT&CK and D3FEND

16.1 Hydra Defend & Countermeasures

The MITRE D3FEND tactics show for mitigating Hydra attacks include Harden and Restore, including sub-techniques such as strong password policy, software updates, and account locking. Lastly, defensive suggestions based on general knowledge include rate limiting, regular security audits, and developing comprehensive cybersecurity policy. Please note that some attack preparation actions required to perform on the attacker's hardware, where access is not possible.

Countermeasures proposed

Develop Comprehensive Cybersecurity Policy
Provide Cybersecurity Training to employees
Avoid Sharing Personal Information on Insecure Website
Monitor Network Traffic & Implement Intrusion Detection System
Rate Limiting
Monitoring and Alerts
Regular Security Audits

Table 17 Countermeasures proposed against Hydra Threat.

Attack-Defend Artifacts

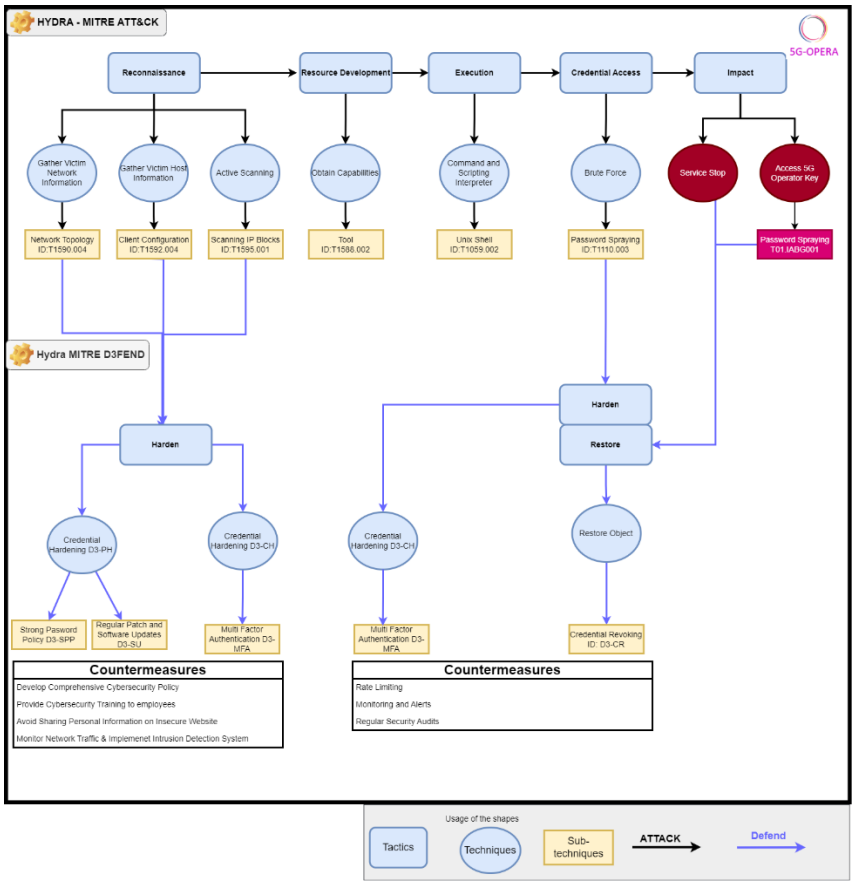

Figure 43 MITRE D3FEND for HYDRA Threat

Annex Attached

Annex 15 MITRE D3FEND Reference: Hydra

16.2 Metasploit MITRE D3FEND & Countermeasures

For the Metasploit threat case, the main mitigations are MITRE D3FEND Tactics include Harden, Detect, Isolate, and Restore, whereas actions (sub-techniques) are suggested as multifactor authentications, software update, remote session detection, and restoring network access. Additionally, it is noted that some steps that are needed to perform the attack are on the attacker side, where the defender cannot access, finally, in the so-called countermeasures, included are suggestions based on general knowledge in the cybersecurity field like secure SSH configuration and implement network security measures.

Countermeasures proposed

Secure SSH Configuration
Implement Network Security Measures
Rate Limiting and Account Lockout

Table 18 Countermeasures against Metasploit Threats

Attack-Defend Artifacts

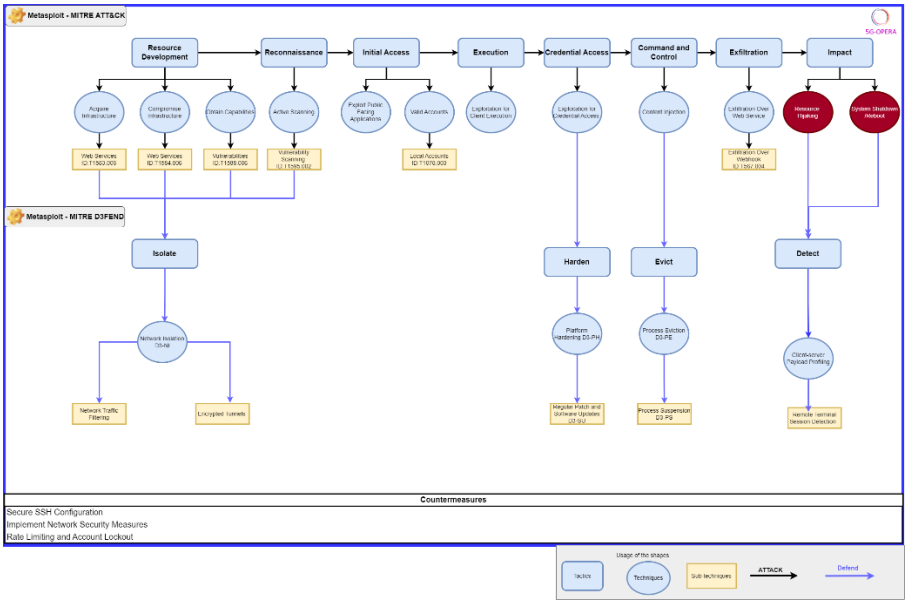

Figure 44 MITRE D3FEND Metasploit Threat

Annex Attached

Annex 16 MITRE D3FEND Reference: Metasploit

16.3 VSFTPD D3FEND & Countermeasures

Tactics included in MITRE D3FEND Framework that safeguard against the VSFTPD threat are Isolate, Detect and Restore, therefore action or sub-techniques suggested as encrypted tunnels, remote terminal sessions detection and user geolocation logon pattern analysis, moreover, the attacker performs some preparation on its side, ending with general suggestions such as intrusion detection and prevention, use of strong encryption and use of secure alternatives SFTP/FTPS for FTP services.

Countermeasure Proposed

Intrusion Detection and Prevention (Monitoring Tools and Log Analysis)
Implement Rate Limiting
Secure File Permissions (CHROOT JAIL and Set Permissions)
Firewall and Network Security (Restrict Ports and Limit IP Address)
Use Strong Encryption
Secure Configuration Disable Anonymous Access
Use Secure Alternatives SFTP/FTPS

Table 19 Countermeasures against VSFTPD Threat

Attack-Defend Artifacts

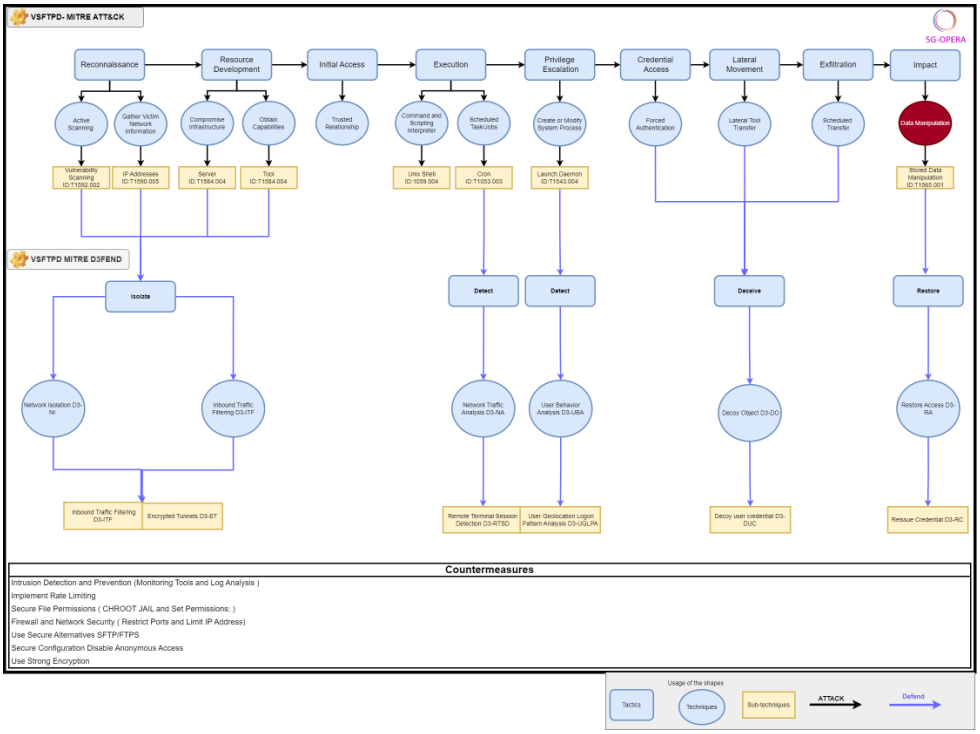

Figure 45 MITRE D3FEND VSFTPD Threat

Annex Attached

Annex 17 MITRE D3FEND Reference: VSFTPD

16.4 Jamming MITRE D3FEND & Countermeasures

To summarize the MITRE D3FEND tactics in a Jammer threat, we mention Detect, Isolate, and Restore, meanwhile, the sub-techniques needed like network community deviation, network traffic filtering, and restore access. In the end, most actions performed in this attack are in the attacker's hardware, nevertheless, some general knowledge suggestions can be included as signal detection and monitoring, network slicing, and enhanced security protocols in the whole infrastructure.

Countermeasures proposed

Network Slicing
Enhanced Security Protocols
Interference Mitigation Techniques
Physical and Infrastructure Security

Table 20 Countermeasures against Jamming Threat

Attack-Defend Artifacts

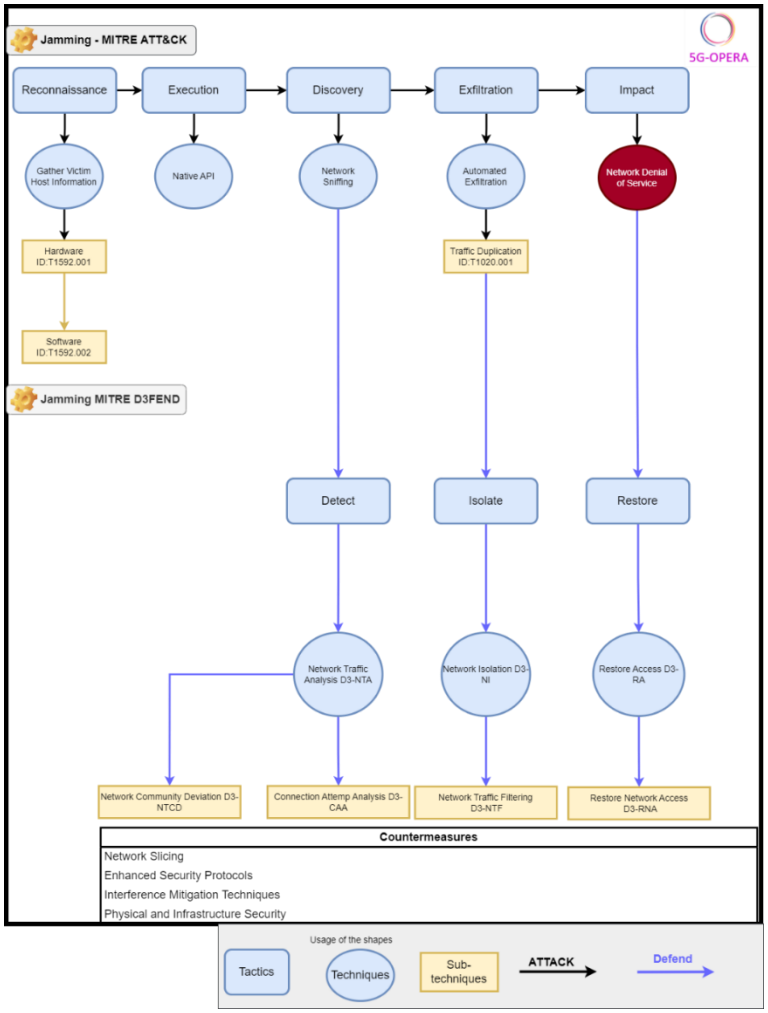

Figure 46 MITRE D3FEND Jamming Threat

Annex Attached

Annex 18 MITRE D3FEND Reference: Jamming

Jamming Detection

In this case study by TUD, Open RAN architectures, by their nature, enhance flexibility and innovation but also introduce new vulnerabilities to malicious activities like jamming. Detecting and mitigating such threats not only ensures uninterrupted communication but also safeguards the integrity and reliability of Open RAN deployment.

The authors in [2] study the detectability of DoS attacks, and they claimed that detecting classical computers by Turing machines (classical computers) is not possible. However, the DoS attacks secure

channels can be detected. They consider a communication scenario between transmitter (Alice) and receiver (Bob) as Figure 47 Communication model between Alice and Bob (Jammer with partial knowledge). In this communication scenario, Alice and Bob communicate with each other in the presence of Jammer with partial knowledge which means that Jammer knows encoding and decoding functions, however, it is not aware of the actual message M. Alice receives the message M, and converts it to the codeword X^n by using encoder. After the Arbitrarily Varying[1] Channel (AVC), Bob receives the codeword Y^n. Then, Bob decodes Y^n , and estimates the actual message as $\hat{M}$. The AVC between Alice and Bob expresses the transition probabilities from X^n to Y^n, and its entries vary between 0 and 1. It also worth to state that the AVC depends on the letter $\boldsymbol{x}$ in the X^n and the inserted jamming letter $\boldsymbol{s}$ in the jamming codeword S^n.

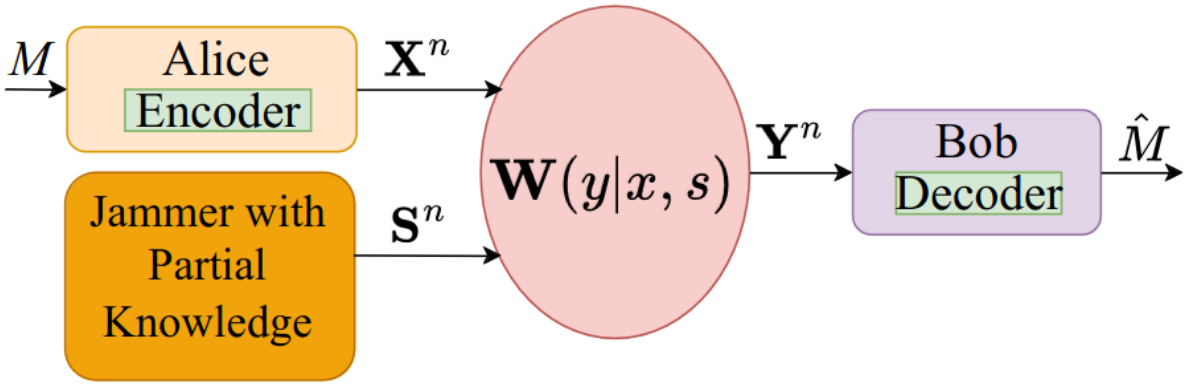

Figure 47 Communication model between Alice and Bob (Jammer with partial knowledge)

For the given communication scenario, if the AVC satisfies the equality in (1), it is called a symmetrizable AVC. In this case, the minimum channel capacity equals zero, and the AVC is open to DoS attacks.

On the other hand, if the AVC does not hold equality, it is called a non-symmetrical AVC. Then, the AVC is a DoS attack free channel since its minimum capacity is bigger than zero, $C_{min} = 0 C_{min} > 0$.

$$\sum_{i=1}^{|S|} \mathbf{W}(y|x, s_i)U(s_i|\hat{x}) = \sum_{i=1}^{|S|} \mathbf{W}(y|\hat{x}, s_i)U(s_l|x)$$

1 AVC Equality - Jamming Detection

As shown above, the detectability of DoS attack free channels is well-characterized theoretically in [2]. In our work, we focus on converting the theoretical background to the practical implementation. In this regard, we proposed an algorithm that checks the symmetrizability condition in (1) and returns 0 if the equality is held. Otherwise, the algorithm returns 1. Then, we implemented the algorithm in MATLAB, and we performed simulations for randomly generated AVC's. In our simulations, we took the algorithm's time consumption as a key performance indicator since it also affects the reliability of communication.

Figure 48 Time consumption results -Proposed algorithm for |X|=2,4,6 - below shows a time consumption result of the proposed algorithm for $|X| = 2$,$|X| = 4$, and$|X| = 6$ with varying $|Y|$ values. We

[1]

clearly see that increasing the size of the input alphabet, $|X|$, does not increase the time consumption of the algorithm dramatically.

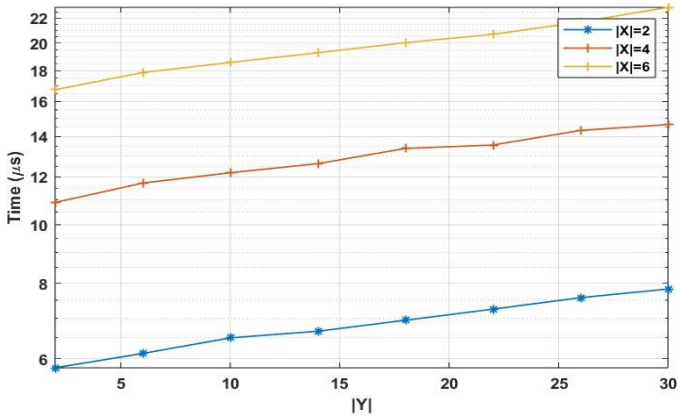

Figure 48 Time consumption results -Proposed algorithm for |X|=2,4,6

16.5 Data-Exfiltration MITRE D3FEND & Countermeasures

For Data-Exfiltration attacks the Isolate and Detect tactics in the MITRE D3FEND Framework are suggested, and then actions (sub-techniques) are required like network traffic filtering and protocol metadata anomaly detection. Lastly, suggestions based on general defense knowledge are included like phishing detection, network traffic monitoring, response mechanisms, and 5G network-specific countermeasures.

Countermeasures proposed

Phishing Detection
Network Traffic Monitoring
5G Network Specific Countermeasures (Implement strong encryption + Deploy anomaly detection systems)
Response Mechanisms

Table 21 Countermeasures against Data Exfiltration

Attack-Defend Artifacts

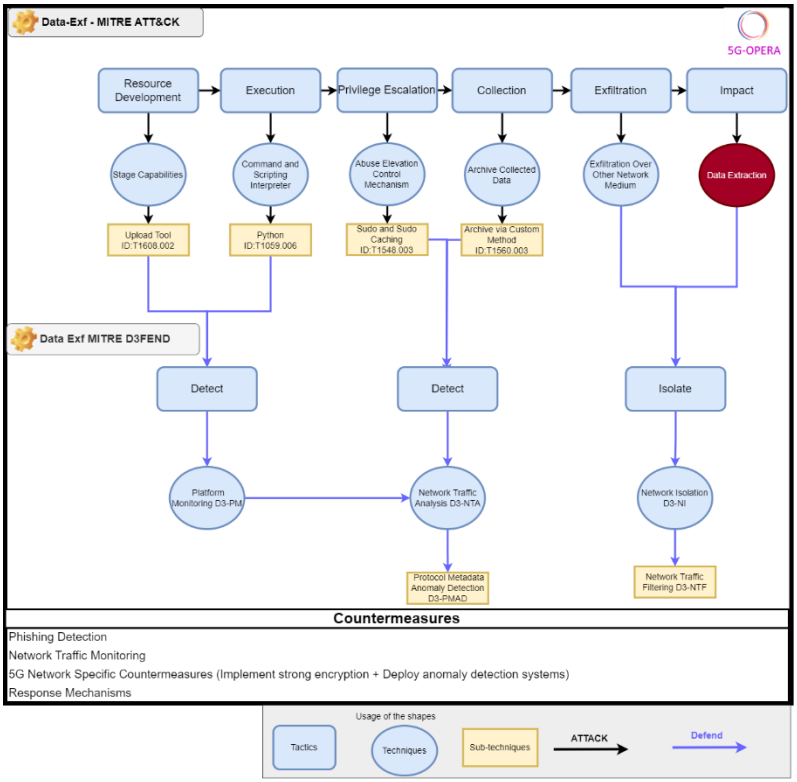

Figure 49 MITRE D3FEND Data-Exfiltration Threat

Annex Attached

Annex 19 MITRE D3FEND Reference: Data-Exfiltration

16.6 Fuzzing RAN MITRE D3FEND & Countermeasures

To start highlighting the Fuzzing RAN threat as a threat focused on 5G networks, and as in previous threats, preparation is required on the attacker infrastructure. Second, the MITRE D3FEND tactics involved in mitigation are Isolate, Detect and Restore, third, the technics part of the defense is platform monitoring, file analysis, restoring software and decoy files, and a final point the recommendations based on general defensive knowledge as login and monitoring, firmware security, intrusion detection and prevention system.

Countermeasures proposed

Logging and Monitoring
Modem Configuration - Access Control
Firmware Security (Regular Updates and Secure Boot)
Input Validation and Sanitization

Intrusion Detection and Prevention Systems (IDPS) - Network Monitoring

Table 22 Countermeasures against Fuzzing RAN

Attack-Defend Artifacts

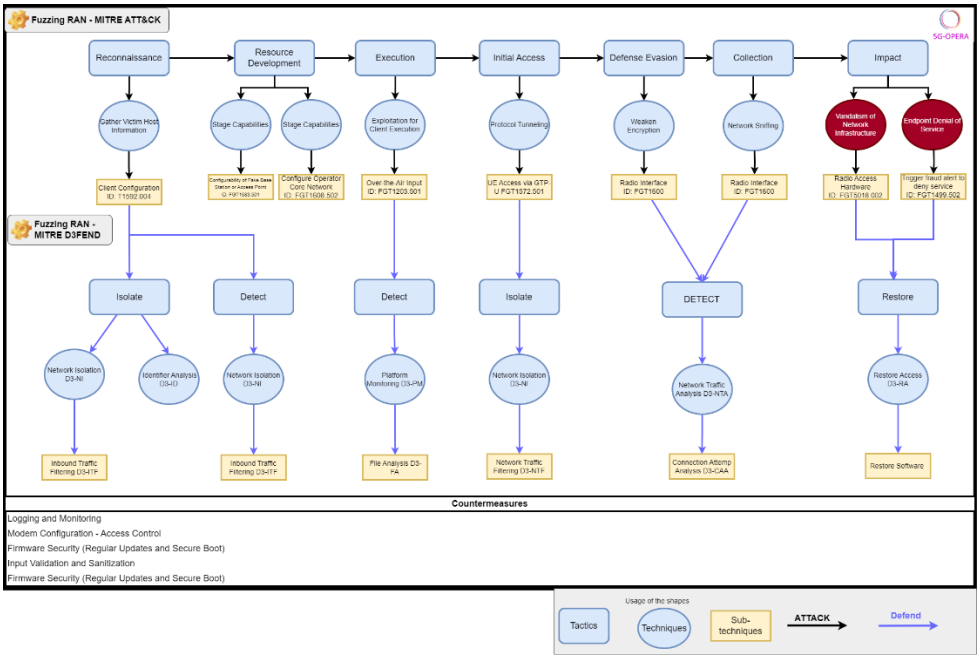

Figure 50 MITRE D3FEND Fuzzing RAN

Annex Attached

Annex 21 MITRE D3FEND Reference: Fuzzing RAN

16.7 Fuzzing Core & Countermeasures

Under MITRE D3FEND Framework the recommended tactics to mitigate Fuzzing Core attacks are Isolate, Harden, Evict, and Restore, further the sub-techniques suggested are inbound traffic filtering, encrypted tunnels, file encryption, file removal, and restoring network access, and finally, the general defensive knowledge recommendations are included like implement robust authentication and encryption, replay detection mechanisms, intrusion detection and prevention systems.

To conclude the main defensive recommendations to mitigate against general attacks that can be suggested are implementing robust authentication, intrusion detection and prevention systems (IDPS), schedule regular security audits and testing exercises to mitigate the vulnerabilities that attackers take advantage.

Countermeasures proposed

Implement Robust Authentication and Encryption (Mutual Authentication and Encryption)
Replay Detection Mechanisms
Intrusion Detection and Prevention Systems (IDPS)

Network Slicing and Isolation
Logging and Monitoring
Regular Security Audits and Testing

Table 23 Countermeasures against Fuzzing Core

Attack-Defend Artifacts

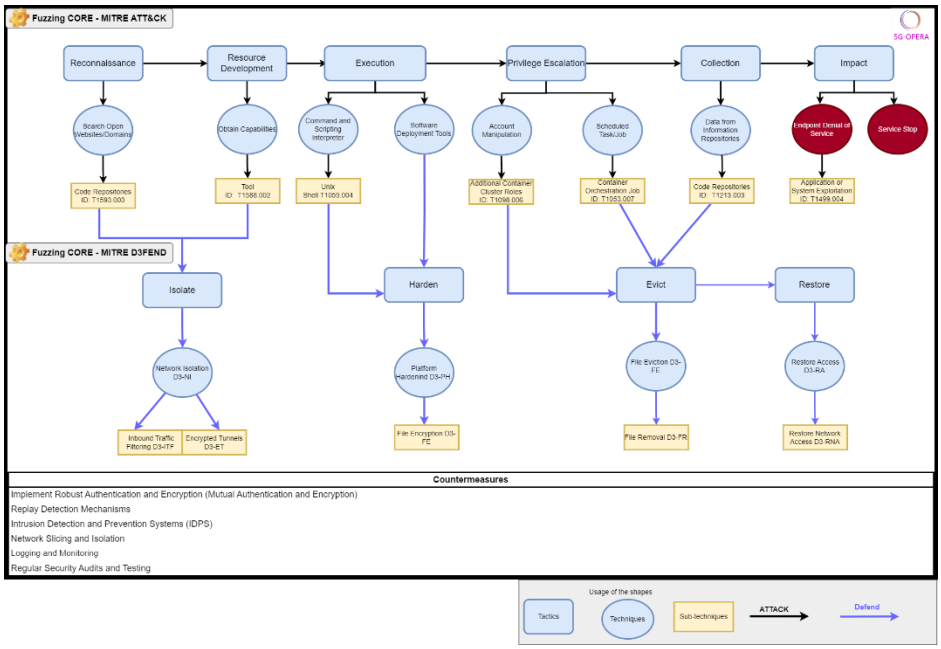

Figure 51 MITRE D3FEND Fuzzing Core

Annex Attached

Annex 20 MITRE D3FEND Reference: Fuzzing Core

17 ATTACK RATING

OWASP (Open Web Application Security Project) is an international non-profit organization focused on improving the security of software. Known for its practical guides, tools, and resources, OWASP aims to help developers, security professionals , and organizations enhance their software's security posture [1].

17.1 OWASP Risk Rating (ORR) Methodology

In OWASP risk rating methodology, the risk has two main components which are likelihood and impact as seen in *Figure 52 OWASP Ranking Criteria*., and is described as a multiplication of these two main components,

$$\text{Risk} = Likelihood * Impact$$

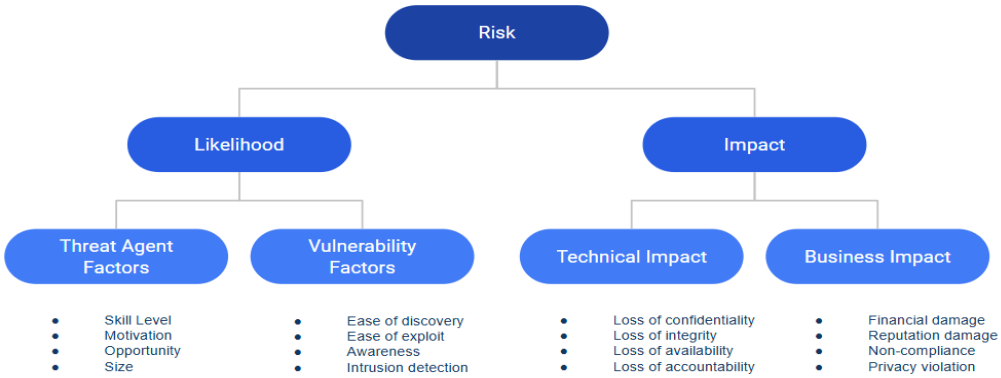

Figure 52 OWASP Ranking Criteria

When a potential risk is identified, the initial task is to estimate its "likelihood." This refers to how probable it is that the identified vulnerability could be discovered and exploited by an attacker. Several factors can aid in determining this likelihood. The first set of considerations revolves around the threat agents. The objective is to assess the probability of a successful attack by various potential attackers. Since multiple threat agents might exploit a given vulnerability, it's generally advisable to consider the worst-case scenario. For instance, an insider might pose a higher risk than an anonymous outsider, depending on various factors.

Each factor includes several options, each rated with a likelihood score ranging from 0 to 9. These ratings will be used later to compute the overall likelihood.

Threat Agent Factors

The first set of factors are related to the threat agent involved. The goal here is to estimate the likelihood of a successful attack by this group of threat agents. Use the worst-case threat agent.

- **Skill Level** - How technically skilled is this group of threat agents? No technical skills (1), some technical skills (3), advanced computer user (5), network and programming skills (6), security penetration skills (9)
- **Motive** - How motivated is this group of threat agents to find and exploit this vulnerability? Low or no reward (1), possible reward (4), high reward (9)
- **Opportunity** - What resources and opportunities are required for this group of threat agents to find and exploit this vulnerability? Full access or expensive resources required (0), special access or resources required (4), some access or resources required (7), no access or resources required (9)

- **Size** - How large is this group of threat agents? Developers (2), system administrators (2), intranet users (4), partners (5), authenticated users (6), anonymous Internet users (9)

Vulnerability Factors

The second part of likelihood estimation is related to the vulnerability factors. The purpose is to estimate the likelihood of the vulnerability involved being discovered and exploited. The vulnerability factors can be listed as below.

- **Ease of Discovery** - How easy is it for this group of threat agents to discover this vulnerability? Practically impossible (1), difficult (3), easy (7), automated tools available (9)
- **Ease of Exploit** - How easy is it for this group of threat agents to exploit this vulnerability? Theoretical (1), difficult (3), easy (5), automated tools available (9)
- **Awareness** - How well known is this vulnerability to this group of threat agents? Unknown (1), hidden (4), obvious (6), public knowledge (9)
- **Intrusion Detection** - How likely is an exploit to be detected? Active detection in application (1), logged and reviewed (3), logged without review (8), not logged (9)

When evaluating the consequences of a successful attack, it's crucial to understand that there are two distinct types of impacts. First is the "technical impact," which affects the application's integrity, the data it processes, and the functionalities it offers. Second is the "business impact," which influences the overall operations, reputation, and profitability of the organization managing the application. The technical impact factors are provided below in detail.

Technical Impact Factors

Technical impact can be broken down into factors aligned with the traditional security areas of concern: confidentiality, integrity, availability, and accountability. The goal is to estimate the magnitude of the impact on the system if the vulnerability were to be exploited.

- **Loss of Confidentiality** - How much data could be disclosed and how sensitive is it? Minimal non-sensitive data disclosed (2), minimal critical data disclosed (6), extensive non-sensitive data disclosed (6), extensive critical data disclosed (7), all data disclosed (9)
- **Loss of Integrity** - How much data could be corrupted and how damaged is it? Minimal slightly corrupt data (1), minimal seriously corrupt data (3), extensive slightly corrupt data (5), extensive seriously corrupt data (7), all data totally corrupt (9)
- **Loss of Availability** - How much service could be lost and how vital is it? Minimal secondary services interrupted (1), minimal primary services interrupted (5), extensive secondary services interrupted (5), extensive primary services interrupted (7), all services completely lost (9)
- **Loss of Accountability** - Are the threat agents' actions traceable to an individual? Fully traceable (1), possibly traceable (7), completely anonymous (9).

Upon completing the attack rating process, the tables shown in Table 24 Likelihood and Impact Level Table with Overall Risk Estimation are produced to finalize the risk analysis evaluation for the attack.

Likelihood and Impact Levels	
0 to <3	LOW
3 to <6	MEDIUM
6 to 9	HIGH

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

Table 24 Likelihood and Impact Level Table with Overall Risk Estimation

17.2 Common Criteria Ranking – CCR Mapping to OWASP

The risk evaluation criteria in CCR and ORR do not align perfectly. To address this, we propose a methodology for transitioning between CCR and ORR, illustrated Figure 53 Mapping OWASP to Common Criteria. The mapping procedure involves three steps: (29)

1. **Score Estimation:** Initially, we estimate the scores based on the criteria defined in CCR.
2. **Score Transfer:** Next, we transfer these estimated scores to the corresponding criteria in ORR.
3. **Score Scaling:** Finally, we scale the transferred scores, considering the highest and lowest values of the scales in both CCR and ORR.

Figure 53 Mapping OWASP to Common Criteria

This completes the risk rating mapping procedure. Conversely, confidentiality, integrity, availability, and accountability are common criteria examined in both CCR and ORR. The risk rating mapping procedure can also be applied to these criteria.

Common Criteria (CC) ISO/IEC 15408:2022 and evaluation methodology ISO/IEC 18045:2022. BSI is the only global mutually recognized product security standard. (30)

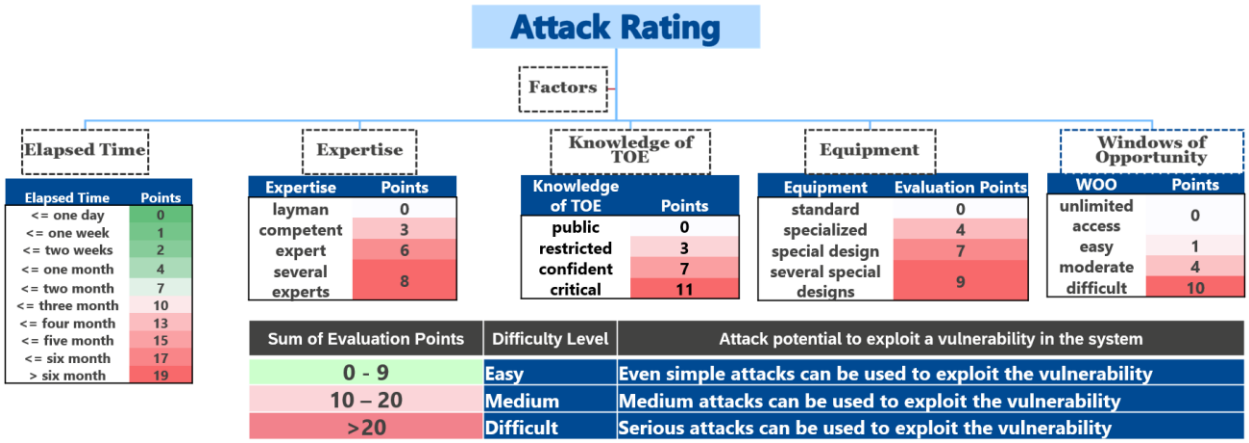

Figure 54 Common Criteria Methodology

17.3 Threat Rating Values

VSFTPD Threat

VSFTPD Threat	Elapsed Time	Expertise	Know of TOE	Equipment	WoO	Total
Factors	<= two week	Expert	Restricted	Standard	Easy	
Evaluation Points	2	6	3	0	1	12

Table 25 Rating - VSFTPD Threat

Hydra Threat

Hydra Threat	Elapsed Time	Expertise	Know of TOE	Equipment	WoO	Total
Factors	<= one week	Competent	Restricted	Standard	Easy	
Evaluation Points	1	3	3	0	1	8

Table 26 Rating - HYDRA Threat

Data-Exfiltration Threat

Data-Exf. Threat	Elapsed Time	Expertise	Know of TOE	Equipment	WoO	Total
Factors	<= two weeks	Expert	Restricted	Standard	easy	
Evaluation Points	2	6	3	0	1	12

Table 27 Rating Data-Exfiltration Threat

Fuzzing RAN

Fuzzing RAN	Elapsed Time	Expertise	Know of TOE	Equipment	WoO	Total
Factors	<=Three Months	Several Experts	Restricted	Standard	Moderate	
Evaluation Points	10	8	3	0	4	25

Table 28 Rating Fuzzing RAN

Jamming Threat

Jamming Threat	Elapsed Time	Expertise	Know of TOE	Equipment	WoO	Total
Factors	<=One day	Competent	Restricted	Specialized	Unlimited Access	
Evaluation Points	0	3	3	4	0	10

Table 29 Rating - Jamming Threat

Metasploit Threat

Metasploit Threat	Elapsed Time	Expertise	Know of TOE	Equipment	WoO	Total
Factors	<=Two weeks	Expert	Restricted	Standard	Easy	
Evaluation Points	2	3	3	0	1	9

Table 30 Rating - Metasploit Threat

Fuzzing Core

Fuzzing Core	Elapsed Time	Expertise	Know of TOE	Equipment	WoO	Total
Factors	<=Three Months	Several Expert	Restricted	Standard	Moderate	
Evaluation Points	10	8	3	0	4	25

Table 31 Rating - Fuzzing Core

18. 5G Security Stakeholder – OPERA Security Model (OSM)

For the project OPERA, we put best efforts to incorporate security and privacy considerations into all relevant aspects and phases of our product. Our efforts in this area follow internal control framework known as **OPERA Security Model (OSM)**. The OSM is an approach to achieve product security and privacy by design and type of deployment ambitions.

The Idea of OSM generates from ISO/IEC 27005 is an international standard that provides guidelines for information security management systems (ISMS).

Our approach to telecom security is built refer to image below, Figure 55 OSM – OPERA Security Model
Four key pillars:

A. Security Requirement Technical Specifications
B. Protocol Requirement Technical Specifications
C. Vulnerability Assessment
D. Threat Modelling Technical Specifications

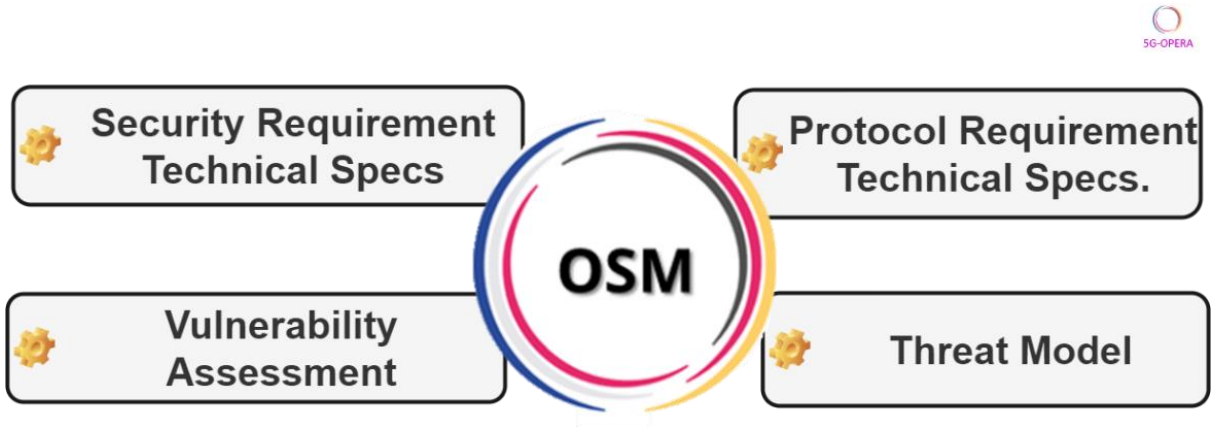

Figure 55 OSM – OPERA Security Model

18.1 Mapping ISO/IEC 27005: OSM – OPERA Security Model

The study follows ENISA's methodology for its annual Cyberthreat Landscape, starting with identifying relevant assets, then assessing vulnerabilities and threats to evaluate asset exposure. Security controls are then assigned to reduce the threat surface, refer to image below, *Figure 56 ISO 27005 – (OSM) OPERA Security Model: Mapping* illustrates the elements of cyberthreats and their relationship to risks. The report describes the relationships between assets, threats, and threat agents, with future versions to address vulnerabilities and countermeasures. (31)

Threats are crucial in risk assessment, defined by ISO 27005 as emerging when threats exploit asset vulnerabilities to harm the organization. The study identifies assets, threats, and threat agents, forming the core of the 5G Threat Landscape, based on specifications and literature. The relationship between threat agents and attack vectors is not yet covered due to rudimentary threat agent profiles and unknown 5G attack vectors.

- Context Establishment: Defining the scope, boundaries, and context of the risk management process.
- Risk Assessment: Identifying, analyzing, and evaluating risks.
- Risk Treatment: Selecting and implementing measures to mitigate identified risks.
- Risk Acceptance: Deciding which risks are acceptable and which need treatment.
- Risk Communication and Consultation: Ensuring all stakeholders are informed and consulted throughout the risk management process.
- Risk Monitoring and Review: Continuously monitoring and reviewing risks and the effectiveness of the risk management process.

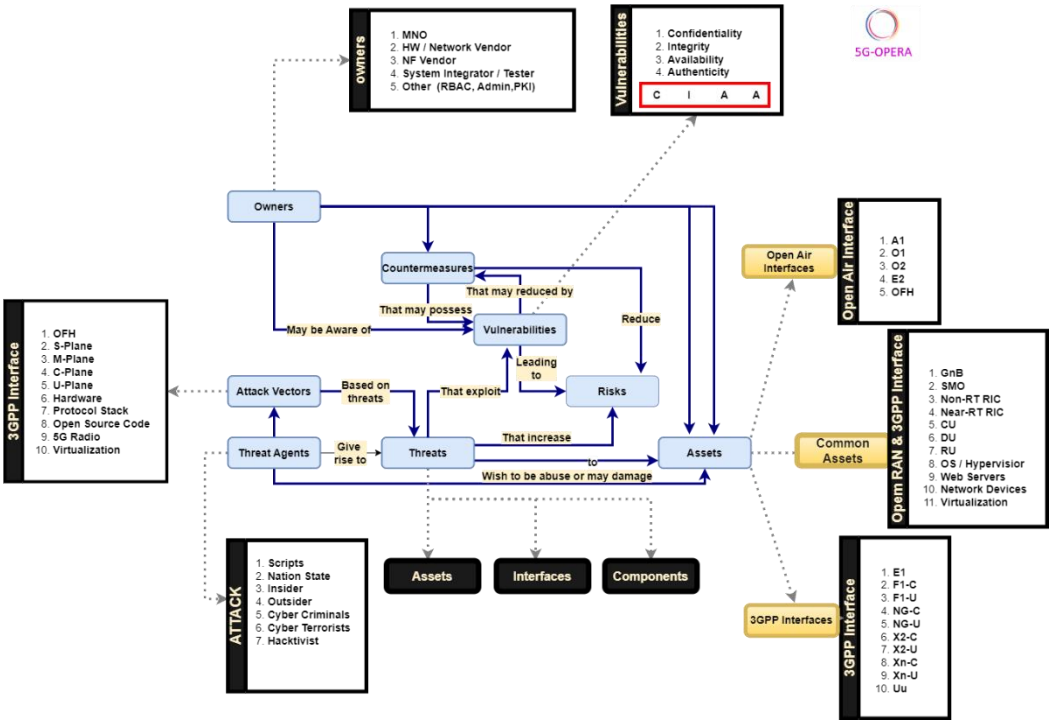

Figure 56 ISO 27005 – (OSM) OPERA Security Model: Mapping

19 Security Requirement Technical Specifications <A>

The OPERA Security Model (OSM) WP 5.4 Security specifications documents aims at specifying security requirements and security control per 5G defined OPERA interface and defined network function.
It also elaborates on OPERA Threats Analysis that identifies assets to be protected, analyses the OPERA interfaces components for vulnerabilities, examines potential threats associated with those vulnerabilities and provides security principles which stakeholders should address when building a secure end-to-end 5G OPERA system.

A threat actor is an individual, organization, or nation-state that carries out malicious activities against another entity. This section defines the most common types of threat actors and describes the threats they pose:

- **Cyber Criminals:** Professional hackers who attack systems for profit.
- **Hacktivists**: Individuals who use hacking to promote political or social agendas by defacing websites or disabling services.
- **Cyber Terrorists**: Experts motivated by political or religious beliefs who aim to create fear through large-scale disruption of telecommunications.
- **Cyber Warfare**: Government-employed individuals who infiltrate and damage information systems to gain confidential information from other governments.
- **Insider**: Threats from within an organization, including disgruntled or terminated employees and under-trained staff.
- **Script Kiddies**: Amateur hackers who use software and scripts developed by others to compromise systems.

Refer to table below, Table 32 5G OPERA Threat Actors and Agents" shows the mapping between the threat actors and the type of threats, as different types of actors have different motives.

	5G OPERA - Threat ACTOR / Threat AGENTS						
Type of Threats	5G-OPERA	Cyber Criminal	Hacktivist	Cyber Terrorist	Cyber Warfare	Insider	Script Kiddies
	Network Configuration Manipulation	Yes	No	Yes	Yes	Yes	Yes
	Hardware Manipulation	No	No	Yes	Yes	Yes	No
	Unauthorized Access	Yes	Yes	Yes	Yes	Yes	Yes
	Authentication Abuse	Yes	Yes	Yes	Yes	Yes	Yes
	Data Breach/ Eavesdropping	Yes	Yes	Yes	Yes	Yes	Yes
	Physical Attacks	No	No	Yes	Yes	No	No
	Accidental	No	No	No	No	Yes	Yes

Table 32 5G OPERA Threat Actors and Agents

19.1 Interfaces and Components

This describes the 5G OPERA Security Requirements for OPERA-maintained interfaces and network functions. Security Requirements specified in this document are built upon Security Principles defined and this intents to protect critical assets identified. Protection critical assets levels of as defined: (32)

[C-I-A-A]– **Confidentiality, Integrity, Authenticity, Availability.**

3GPP Interfaces & Components	Opera Components	Opera interfaces:
E1 F1-c F1-u NG-c NG-u X2-c X2-u Xn-c Xn-u Uu	Service Management and Orchestration (SMO) Non-RT RIC and rApps Near-RT RIC and xApps CU-CP and UP DU RU eNB / gNB	A1 Interface between Non-RT RIC and Near-RT RIC. O1 Interface connecting the SMO to the Near-RT RIC, one or more CU-CPs, one or more. CU-UPs, and one or more DUs. O2 Interface between the SMO and the Cloud E2 Interface connecting the Near-RT RIC and one or more CU-CPs, one or more CU-UPs, one or more DUs, and one or more eNBs. Open Fronthaul CUS-Plane Interface between RU and DU Open Fronthaul M-Plane Interface between RU and DU as well as between RU and SMO.

Table 33 C-I-A-A table for OPERA Interfaces

19.2 Security To-Do-OPERA-Tool List – ISO 27005

This OPERA Security To-Do-OPERA-Tool List as a tool with hope of the improving convenience, the security measures for OpenAirInterface networks. This security To-Do-OPERA-Tool List is formatted as a checklist and related information (vulnerability information, threat values, etc.) is added to improve visibility and operability.

- **Tool Name**: “To-Do-List Opera tool”.
- **Tool Description**: This tool covers 5G Open RAN architecture security must have actions.
- **Tool Scope**

<1> This tool assists in identifying and validating cybersecurity compliance.

<2> It focuses on system-level security, including CIAA mechanisms.
<3> Examines adherence to security policies, regulatory requirements.

- **Tool Assumption** Not Included in Tool: We assume that 3GPP security requirements are met. Therefore, the scope of this To-Do-List is not within for the 3GPP security requirements area.

19.2.1 To-Do-List OPERA tool.

Here is the detail list of parameters in To-Do-List-OPERA Tool:

[1] Item_____Security requirements count

[2] Assets_____Security requirements to be checked

[3] Threats_____Typical threat information

[4] Vulnerability_____Typical Vulnerability Information

[5] C-I-A-A_____Protection Level

[6] Threat _____This is the vulnerability ID

[7] Impact_____The degree of impact

[8] To-Do-List OPERA Tool_____Security requirements to be checked

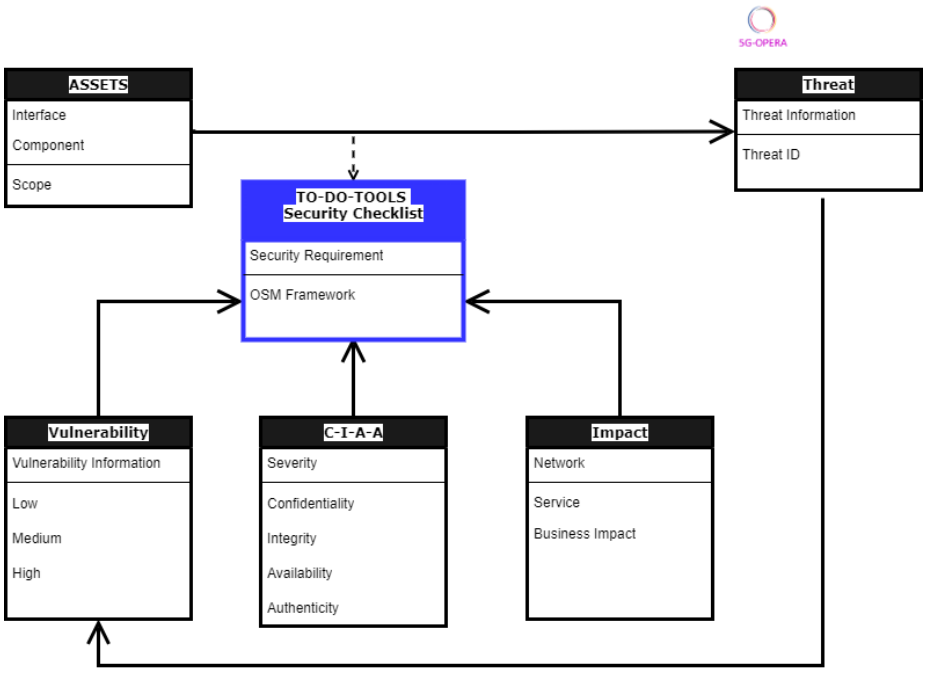

Table 34 Security To-Do-Tool

19.1 3GPP Security Specifications Requirement

gNB	**Annex 22 gNB Security Requirements**
Web Servers	**Annex 23 Web Servers Security** Requirements
Network Devices	**Annex 24 Network Devices Security Requirements**
Operating Systems	**Annex 25 Operating Systems Security Requirements**
Virtualization	**Annex 26 Virtualization Security Requirements**

19.2 OPERA Security Specifications Requirement

Non-RT RIC & rApps	**Annex 27 Non-RT RIC Security Requirements**
Near-RT RIC & xApps	**Annex 28 Near-RT RIC Security Requirements**
SMO-MANO	**Annex 29 MANO-SMO Security Requirements**
CU-DU-RU	**Annex 30 CU-DU-RU Security Requirements**
A1	**Annex 31 A1 Security Requirements**
E2	**Annex 32 E2 Security Requirements**
O1	**Annex 33 O1 Security Requirements**
O2	**Annex 34 O2** Security Requirements

20 Protocol Requirement Technical Specifications

This OPERA WP 5.4 Security specifications documents aims at specifying security requirements protocol per 5G defined OPERA interface only and defined network function. For future use the newer protocol mTLS with integrated authentication features and the newest TLS-Version must be used in Lab environments with all implemented security features depending on the tested tasks. Also, the QUIC protocol, which is used for speeding up web applications is recommended. Even SSH-2 could be a better protocol in future testing. But these newer Protocols are out of Scope of OPERA project and are not explained here.

<A> SSH

<B> TLS v1.2

<C> DTLS

<D> IPsec

<E> OAuth 2.0

<F> Cryptographic Operation

20.1 OPERA Protocol Specifications <A> SSH

The protocol operates in a client-server model, where the connection is initiated by the SSH client connecting to the SSH server. The SSH client manages the connection setup process and utilizes public key cryptography to verify the SSH server's identity. (33)

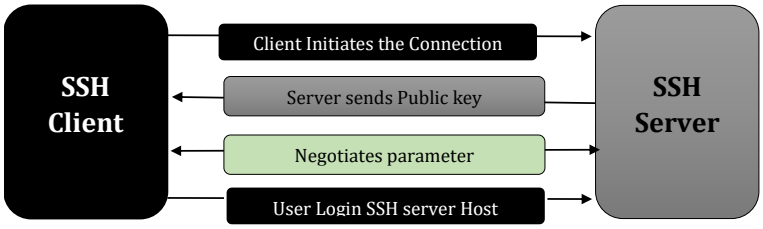

Figure 57 SSH Protocol Agreement

Following the setup phase, the SSH protocol employs strong symmetric encryption and hashing algorithms to ensure the privacy and integrity of the data exchanged between the client and server.

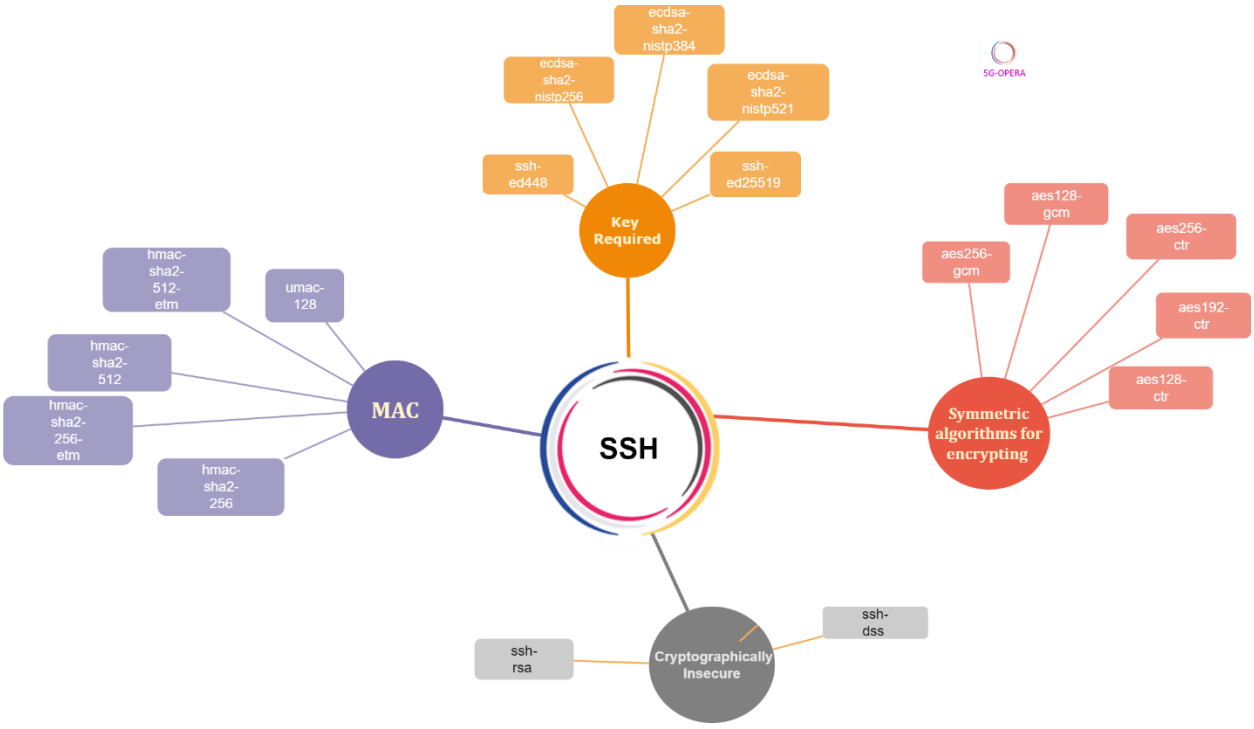

Figure 58 SSH - Key Agreement

20.2 OPERA Protocol Specifications <B> TLS v1.2

The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating applications. The protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. (34)

- **The connection is private**. Symmetric cryptography is used for data encryption (e.g., AES [AES], RC4 [SCH], etc.). The keys for this symmetric encryption are generated uniquely for each connection and are based on a secret negotiated by another protocol (such as the TLS Handshake Protocol).
- **The connection is reliable**. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g.SHA-1, etc.) are used for MAC computations. The Record Protocol can operate without a MAC but is generally only used in this mode while another protocol is using the Record Protocol as a transport for negotiating security parameters.

In Open-RAN interfaces that implement authentication, confidentiality and integrity using Transport Layer Security (TLS) shall:

- Support TLS 1.2.
- Configure the TLS 1.2 Intermediate server ciphers.
- Support TLS 1.3.
- Stay current with the latest release of the TLS software used to implement the protocol, such as OpenSSL.
- Provide an upgrade path for new software releases.
- Any version of SSL and any version of TLS below 1.2, shall not be supported.
- TLS 1.2 used on all interfaces except the Open Fronthaul interfaces shall support the TLS 1.2 profiles as defined by 3GPP TS 33.210.
- TLS 1.3 used on all interfaces except the Open Fronthaul interfaces shall support the TLS 1.3 profiles as defined by 3GPP TS 33.210.

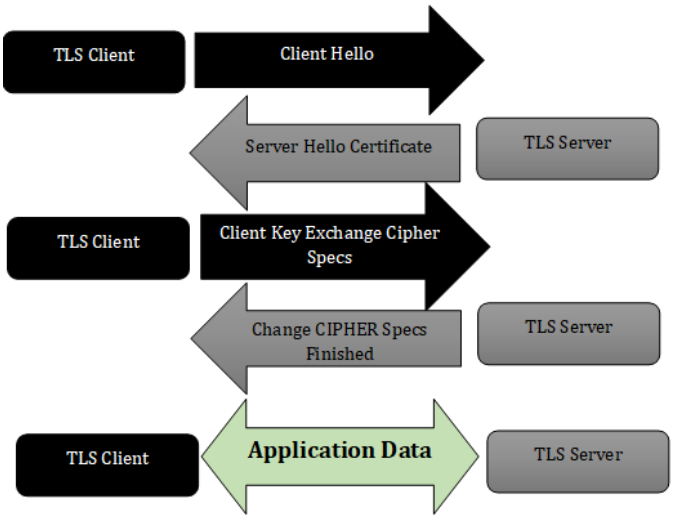

Figure 59 TLS Agreement

20.3 OPERA Protocol Specifications <C> DTLS

DTLS Datagram Transport Layer Security is intended for the delivery of application data that is authenticated and encrypted end-to-end but with lower latency than can be achieved when all application data delivery is guaranteed. DTLS is extremely like TLS and therefore allows reuse of pre-existing protocol infrastructure. DTLS Datagram transport Layer Security is a protocol that provides privacy for UDP communications. (35)

Open-RAN and 3GPP interfaces that implement mutual authentication, integrity protection, replay protection and confidentiality protection using Datagram Transport Layer Security (DTLS) shall:

- Support DTLS 1.2
- Support DTLS for Stream Control Transmission Protocol

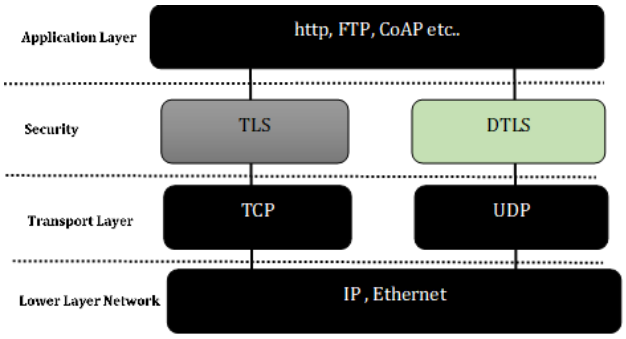

Figure 60 DTLS Agreement

20.4 OPERA Protocol Specifications <D> IPsec

IPsec is a group of protocols for securing connections between devices. IPsec helps keep data sent over public networks secure. IPsec is secure because it adds encryption and authentication to this process. (36)

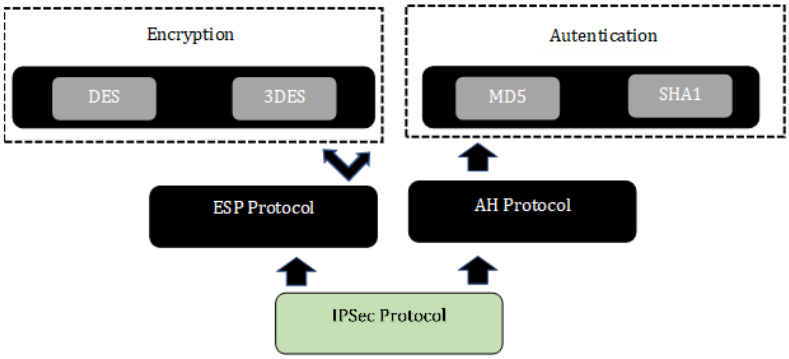

Figure 61 IPsec Agreement

- **Key exchange:** IPsec sets up keys with a key exchange between the connected devices, so that each device can decrypt the other device's messages.

- **Packet headers and trailers:** Packets contain both a payload, or the actual data being sent, and headers, IPsec adds several headers to data packets containing authentication and encryption information. IPsec also adds trailers.
- **Authentication:** IPsec provides authentication for each packet.
- **Encryption**: IPsec encrypts the payloads within each packet and each packet's IP header.
- **Transmission**: Encrypted IPsec packets travel across one or more networks to their destination using a transport protocol. TCP sets up dedicated connections between devices and ensures that all packets arrive.
- **FQDN**: Fully Qualified Domain Name (if DNS is supported)
- **Authentication**
  - X.509v3 digital certificates provided by a Certificate Authority solution.
  - Pre-shared Keys
  - Key exchange IKEv2
  - certificate-based authentication
- **Security Association**
  - Multiple IKE SAs (multiple IPsec tunnels)
  - Multiple IPsec SAs
  - Multiple IPsec SAs per IPsec tunnel

20.5 OPERA Protocol Specifications <E> AUTH2.0

OAuth 2 is an authorization framework that enables applications — such as Facebook, GitHub etc to obtain limited access to user accounts on an HTTP service. (37)

OAuth 2.0 defines a protocol for securing application access to protected resources, which are accessed through REST APIs. OAuth 2.0 relies on access tokens presented by client applications (on behalf of end-users or not) when requesting access to protected resources via APIs. These tokens must be obtained before the client application can get access to these resources. An access token contains a set of attributes and policies that relate to both the client application and the end-user, and these attributes are used for making authorization decisions at runtime.

OAuth 2.0 protocol supports several grant types for different use cases.

OAuth defines four roles:

[1] **Resource Owner:** The resource owner is the user who authorizes an application to access their account.
[2] **Client:** The client is the application that wants to access the user's account.
[3] **Resource Server:** The resource server hosts the protected user accounts.
[4] **Authorization Server:** The authorization server verifies the identity of the user then issues access tokens to the application.

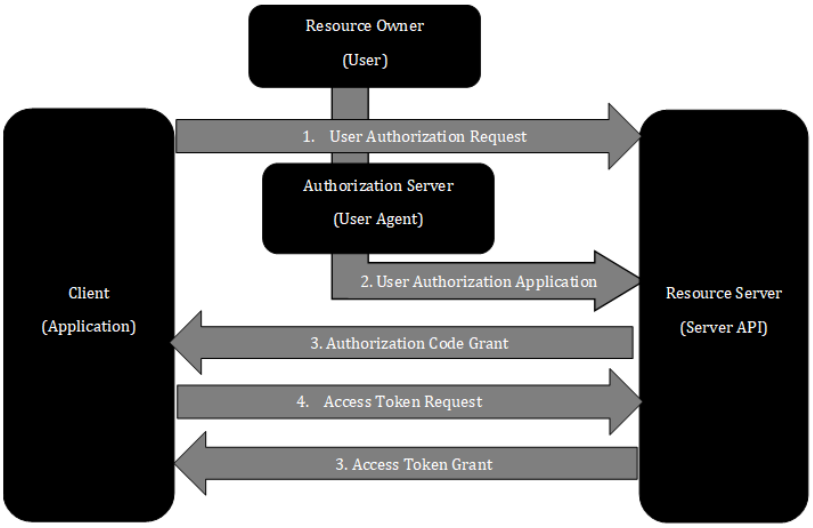

Figure 62 OAUTH2.0 Rules Agreement

20.6 OPERA Protocol Specifications <F> Cryptographic Operation

Core Network, DU, and CU packages for ensuring their integrity, authenticity, and confidentiality. the communication channel interfaces in terms of authenticity, confidentiality, and integrity. It contains the allowed list of algorithms, key sizes. (38)

The table below the outlines the main cryptographic operations involved in the protection:

Cryptographic operations	Algorithms	Key sizes	Usage
Signature generation and verification	RSASSA-PSS RSA_PKCS1_V1_5	>= 2048-bits	For ensuring the integrity and authenticity of Apps/VNF/CNF packages during delivery, onboarding, and instantiation phases
Signature generation and verification	ECDSA NIST-approved curves (P-256, P-384, or P-521)	>= 256-bits	
Symmetric Encryption/Decryption	AES_128, AES_192 and AES_256	128, 192 and 256 bits	For ensuring the confidentiality of sensitive artifacts
Asymmetric Encryption/Decryption	RSAES-OAEP	>= 2048-bits	
Hashing	SHA-2 family (SHA- 224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256) SHA-3 family (SHA3-224, SHA3-256, SHA3-384, and SHA3-512)		For ensuring the integrity of Apps/VNF/CNF packages

Table 35 Cryptographic Key and Algorithm Involved

Recommendation of Cryptographic Operations

The signature operation shall involve **X.509-based PKI certificates.**

1. For the protection of cryptographic keys, Hardware Security Modules (HSMs) should be used:

- An HSM is a specialized, highly trusted physical device.
- It is a network computer that performs major cryptographic operations, including encryption, decryption, authentication, key management, and key exchange.
- HSMs are tamper-resistant and utilize extremely secure cryptographic operations.

2. Along with HSMs, the principle of least privilege should be applied to keys, ensuring that only users who need access to the keys have it.

3. If a legacy system does not support ECDSA, RSA signing algorithms should be used instead. Otherwise, the use of Elliptic Curve signing algorithms is recommended.

4. If older libraries or frameworks do not support the PSS padding scheme, one of the RSA PKCS1 algorithms should be used instead. Otherwise, the use of one of the RSA PSS algorithms is recommended.

5. In general, the largest key size available for an algorithm family should be used:

- For RSA, the largest supported key size is 4096 bits.
- For ECDSA, the largest supported key size is 512 bits.
- For AES, the largest supported key size is 256 bits.

21 Threat Assessment Model – Technical Specifications

As we all know, a vulnerability is a flaw in a system's design, implementation, or operation that can be exploited to compromise its security. **Threat Assessment** helps identify potential threats to a system and provides a structured approach to mitigate them. It involves analyzing the system's architecture, data flows, and user roles to identify potential attack vectors and threat actors. The goal is to pinpoint and prioritize security risks so appropriate countermeasures can be implemented to mitigate them.

Threat assessment and penetration assessment are two essential methods for identifying and addressing security vulnerabilities in software systems. While they share similar goals, their approaches and scopes differ:

Threat assessment aims to identify potential threats before they can be exploited. It assesses the overall security posture of a system from a theoretical perspective and focuses on mitigating weaknesses.	**Penetration assessment** assesses the security of a system by attempting to exploit vulnerabilities, offering a practical, hands-on evaluation of system defenses through simulated attacks.

With multiple options available, choosing the best threat modeling framework can be challenging. Various frameworks are designed to address different needs and circumstances, such as SDL, **STRIDE**, DREAD, VAST, STRIKE, and PASTA. Selecting the right one depends on your specific requirements and the nature of the threats you face.

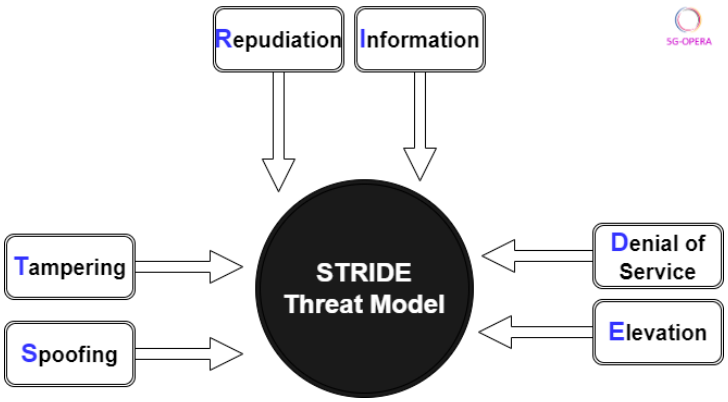

Figure 63 Threat Assessment Model

STRIDE Threat Definition

Spoofing
Spoofing involves an attacker impersonating a legitimate user, compromising the authentication aspect of the CIA triad. This can happen through techniques like ARP, IP, or DNS spoofing.

Tampering
Tampering means unauthorized modification of data or information, violating the integrity principle of the CIA triad. This includes any alteration of data by an attacker.

Repudiation
Repudiation is when an attacker denies involvement in malicious activities, evading accountability. This breaches the non-repudiation principle, often achieved by deleting logs and covering tracks.

Information Disclosure
Information disclosure refers to unauthorized access to confidential data, violating the confidentiality principle of the CIA triad. This includes data breaches and exfiltration by malicious users.

Denial of Service (DoS)
DoS attacks prevent legitimate users from accessing services by overwhelming network resources, violating the availability principle of the CIA triad.

Elevation/Escalation of Privilege
Privilege escalation involves gaining unauthorized access by increasing user privileges, breaching the authorization principle of the CIA triad.

22 Threat Assessment - TIER Approach

22.1.1 Endpoint Tier

This tier includes all the devices that connect to the 5G network. We're talking about mobile phones, drones, IoT gadgets, home appliances, autonomous vehicles, and network access points. The attack surface here is constantly

changing, with new threats like malware, worms, botnets, and advanced persistent threats (APTs) popping up regularly. If a breach happens, it can compromise user privacy or even lead to a massive attack on the network infrastructure and services.

22.1.2 Radio Tier

The 5G Radio Access Network (RAN) layer is what keeps all our devices wirelessly connected to the 5G core network and its services via 5G radio frequencies. This is crucial for applications like cloud gaming, AR/VR, autonomous driving, and fixed wireless access. The RAN is made up of transmitters, antennas, baseband (RAN Compute), and RAN software, delivering ultra-high speeds and enhanced mobility. 5G brings significant improvements to the RAN compared to 4G, like multiple antenna arrays, MIMO, and centralized or Cloud RAN (C-RAN). However, the RAN is still vulnerable to attacks such as unauthorized access, traffic sniffing, signaling storms, flooding, and jamming.

22.1.3 Edge Tier

The edge tier is where things get super-fast and responsive. It's what enables autonomous vehicles to navigate safely and allows surgeons to perform operations remotely with almost no delay. This is possible thanks to technologies like NFV (Network Function Virtualization) and SDN (Software Defined Networking). But despite its advancements, the edge layer is just as vulnerable to threats as any other part of the 5G network. Hackers might launch Denial of Service attacks, sneaky side-channel attacks, or tamper with virtual machines. So, while the edge layer brings us closer to a future of seamless connectivity, we must remain vigilant against potential threats.

22.1.4 Core Tier

The core tier is like the brain of the entire 5G operation, designed to be intelligent and flexible with its cloud-native setup and advanced technologies like NFV and SDN. This layer is packed with virtual functions, each handling specific tasks to keep everything running smoothly. Functions include authentication (making sure you're who you say you are), session management (keeping you connected), and more, with components like AMF, UPF, SMF, and AUSF. The core layer is built for flexibility and adaptability, featuring innovations like Control and User-Plane Separation (CUPS).

22.1.5 Service Tier

The service tier is where all the user action happens. It's the gateway to all the cool 5G services. Service providers define how we interact with these services through APIs. When it comes to security, the service provider plays a crucial role. They're like the guardians, ensuring everything runs smoothly and securely. They monitor for threats just like with any other internet-based applications. From authentication (confirming your identity) to authorization (deciding what you can access), and ensuring secrets stay safe and actions are undeniable (non-repudiation), they've got it all covered. (39)

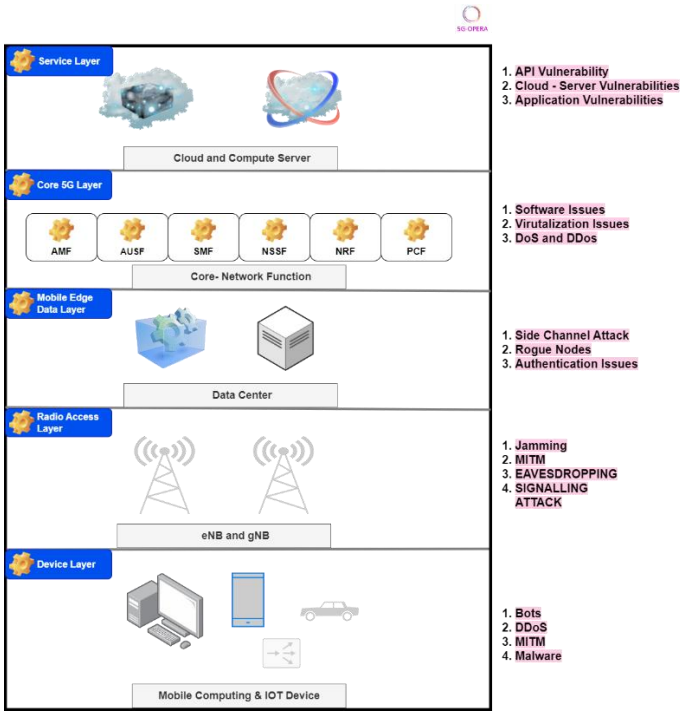

Figure 64 Tier Approach - Threat

23 Threat Assessment Mapping STRIDE - TIER Approach

In the OPERA Project 5G-network threats are studied at separate layers based on the impact these attacks have on different network functions and services. Another aspect of security threats is the enabling technology, which may be affected by the threats. Here, we classify the threats into categories and present the same in the form of Figure 65 LAYER Threat 5G Taxonomy https://bit.ly/5g_Threat_model_IABG maps the threats to each tier. (40)

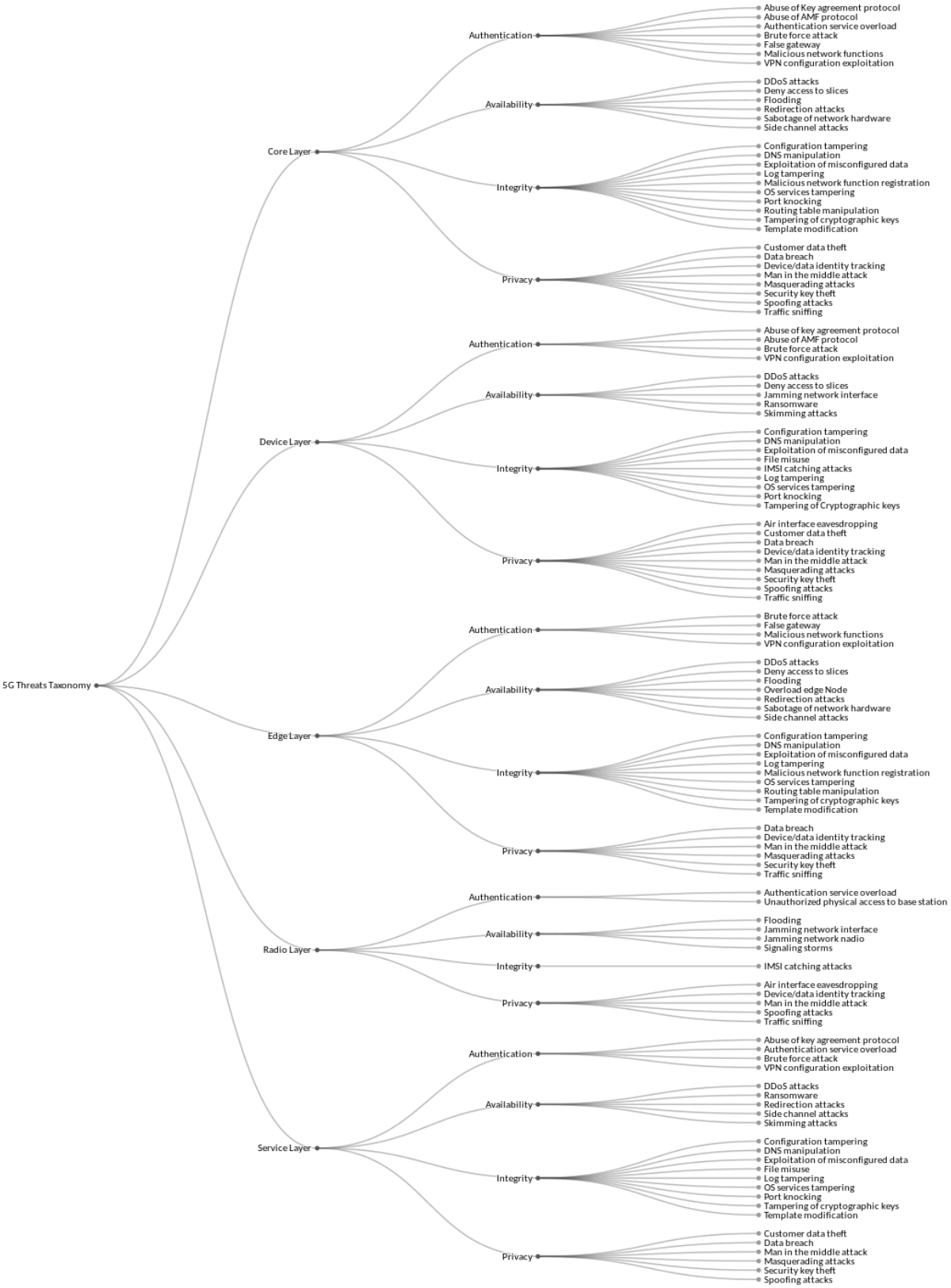

Figure 65 LAYER Threat 5G Taxonomy [(tool)]

23.1 Threat Assessment STRIDE Model – 5G Core

23.1.1 Spoofing

Spoofing (Jamming) involves attackers impersonating legitimate users or processes, posing a risk that seemingly legitimate traffic could be malicious. One common method is the Man-in-the-Middle (MitM) attack, where an attacker intercepts and manipulates traffic between two authentic nodes. For instance, an attacker could place himself between user equipment and a network slice, manipulating data and causing information disclosure, tampering, and denial of service. To mitigate these risks, mutual authentication using digital signatures and certificates is recommended, along with Transport Layer Security (TLS) and Mutual TLS (mTLS) to verify identities. Ensuring data integrity and encryption, and keeping sensitive network functions within a trusted environment, are crucial to minimizing the risk of such attacks. We have done a Jamming Penetration testing attack on 5G Opera Interface. (41)

Network Slice Management Function (NSMF) impersonating in the 5G network is highly dangerous, as it controls all network slices. If compromised, an attacker could manipulate or disrupt the entire network, risking tampering, repudiation, information disclosure, and privilege escalation. To mitigate this, use mutual authentication, digital signatures, TLS, and Mutual TLS (mTLS) to verify identities and protect communications.

Network Slice Selection Assistance Information (NSSAI) spoofing occurs when a user device sends a fake NSSAI to access a network slice without authorization. This can lead to information disclosure and tampering. To mitigate this, ensure that user device authentication and authorization are performed for each network slice.

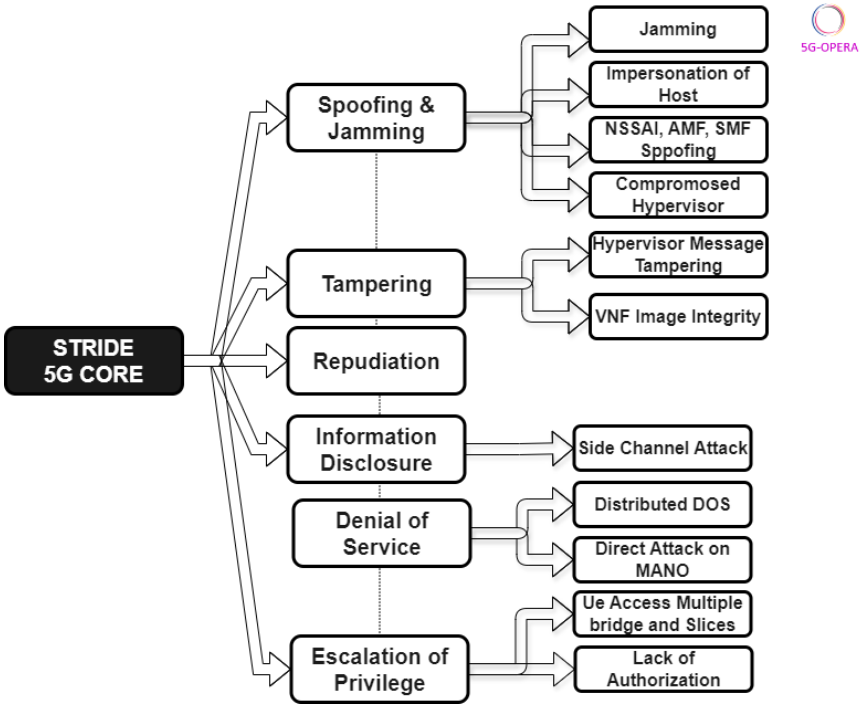

Figure 66 STRIDE Model

Hypervisor: A potential threat arises when untrusted hardware, potentially running other network functions or APIs, compromises the hypervisor, responsible for managing virtualization in 5G network slices. This "rogue hypervisor" scenario could lead to controlling the slices and intercepting traffic. Risks include information disclosure, denial of service, and privilege escalation. To mitigate, protocols and content should be verified, hypervisor software regularly updated and patched, and additional measures such as firewall isolation, intrusion detection systems, and a defense-in-depth approach to security should be implemented across the organization.

Authentication and Mobility Function (AMF) and Session Management Function (SMF) An attacker gaining control over the Session Management Function (SMF) could manipulate the Packet Forwarding Control Protocol (PCFP) session to the User Plane Function (UPF), potentially disrupting user connections to the internet. Risks include Denial of Service. To mitigate, ensure proper configuration of the N4 interface, restricting access from outside the operator's network.

23.1.2 Tampering

Virtual Network Function (VNF) images by tampering with them during download from the repository to the host platform. This could involve injecting malware or altering data. If the connection lacks encryption or integrity protection, attackers could intercept and modify the traffic, posing risks of information disclosure and privilege escalation. Mitigation involves verifying image signatures before execution and ensuring digital signatures for all stored images, assuming these signatures are trustworthy.

23.1.3 Repudiation

Repudiation, the ability to deny responsibility for actions, poses a significant risk to 5G core networks if actions are not logged or audited, making it impossible to trace their origin. While there's limited literature on direct threats to 5G core originating from repudiation attacks, the lack of traceability amplifies the potential damage from other attacks. Implementing measures like mutual authentication (mTLS) can enhance traceability and strengthen non-repudiation on the network, ensuring that all activities on the slice are authorized, authenticated, and logged for investigation in the event of an attack.

23.1.4 Information Disclosure

5G network function are susceptible to Side Channel Attacks exploit co-residency of Docker / Kubernetes of the same hardware, posing risks of information disclosure. These attacks encompass various methods, including mapping network topologies and extracting secret keys, leading to tampering and privilege escalation. Mitigation strategies from literature include increasing background noise, program analysis, cache flushing, and selective feature deactivation. However, no simple solution exists, with challenges arising from resource overhead and uncertainty in mitigating all attacks.

23.1.5 Denial of Service

Denial of Service (DoS) attacks hinder legitimate requests by overwhelming resources. Shared security mechanisms between slices, as in the Exhaustion of Shared Security Service attack, leave slices vulnerable once resources are depleted. Distributed Denial of Service (DDoS) attacks, facilitated by botnets, pose similar risks but on a larger scale, targeting critical interfaces like N4 and N6. Mitigation involves resource allocation and machine learning for traffic analysis. Direct attacks on Network

Functions Virtualization Management and Orchestration (NFV-MANO) jeopardize all slices, requiring regular updates, network isolation, and robust defense strategies.

23.1.1 Escalation of Privilege

Escalations of Privilege involves users gaining unauthorized access to more services than they are allowed. In one scenario, if a user accesses multiple network slices using the same credentials, a compromise in one slice could grant access to others, posing risks of information disclosure and tampering. Mitigation strategies include separate authentication for each slice or prohibiting credential reuse. Another concern arises from the lack of authorization between slice components, allowing unauthorized network functions to register, leading to risks such as information disclosure and denial of service. Mitigation involves implementing authorization mechanisms for network functions. Additionally, authentication relaxation for services may compromise security, leading to risks like spoofing and tampering. Countermeasures include maintaining a baseline security level across all network functions in 5G Core Networks.

23.2 Threat Assessment STRIDE Model – 5G Tiers

1. **Authentication Abuse**: Unauthorized access and integrity violations can occur, affecting services like AMF and NSSF. Example: Hyper jacking, where a malicious VM gains root access through hypervisor vulnerabilities. (42)

2. **Information Leakage**: Unauthorized access to sensitive data, such as user data and cryptographic keys, can occur across core, cloud, and edge layers. Example: VM hopping attacks that extract cryptographic keys.

3. **Denial of Service (DoS):** DoS attacks make services unavailable by overloading resources, targeting components like SDN, NFV, and RAN. Example: Flooding or jamming network interfaces.

4. **Network Configuration Manipulation**: DNS and routing table manipulation, exploiting misconfigured data, and tampering with cryptographic keys can impact 5G components like SDN and MANO. Example: Attackers exploiting misconfigured services.

5. **Malicious Software**: Injection attacks, worms, ransomware, and botnets can disrupt services and compromise data integrity at device, MEC, core, and service layers.

6. **Hardware Manipulation:** Attacks on user and MEC equipment and radio units can cause service unavailability and information destruction.

7. **Signaling Threats**: Malware or apps can launch signaling storms, overloading servers, and draining device batteries, affecting device, core, and cloud layers. Example: Signaling fraud compromising system integrity and confidentiality.

8. **Eavesdropping**: Attackers listen to network communications to access sensitive information, such as encryption keys and personal data. Example: Traffic sniffing, man-in-the-middle attacks, and session hijacking.

ISO27005 - Category	5G - Open RAN Tier Approach				
Attack	**CORE**	**Device**	**EDGE**	**RAN**	**Service**
Network Configuration Manipulation	IP Routing Table configuration Malicious network function reg. Tampering of Cryptographic keys	Exploitation of misconfigured data OS services tampering	IP Routing Table configuration Malicious network function registration	N/A	DNS manipulation Exploitation of misconfigured data Exploitation of misconfigured service Tampering of Cryptographic keys
Software Manipulation	Malicious network functions	Worms Ransomware Botnet	Malicious network functions	N/A	Worms Ransomware Botnet
Hardware Manipulation	Side channel attacks	N/A	Side Channel Attack	N/A	Side Channel Attack
Unauthorized Access	N/A	N/A	N/A	IMSI catching attacks	Brute force
Authentication Abuse	Authentication service overload Abuse of AMF and key agreement protocol	N/A N/A	N/A	N/A	Third party leakage/abuse
Physical Attacks	N/A	Theft	Attack Network hardware Terrorist attacks	Unauthorized physical access to base station Terrorist attacks	N/A
Network Slicing	Template modification Configuration tampering Configuration tampering, Fake slice creation Misuse of resources side channel attack	N/A N/A N/A N/A	Unauthorized access Side channel	Misuse of resources Side channel	Unauthorized access Side channel

Table 36 Threat Assessment Attack, All Tiers

24 Vulnerability Assessment

A vulnerability assessment in the context of open source 5G networks is an analysis of weaknesses within a 5G system at a specific point in time, aiming to identify and address these vulnerabilities before malicious actors can exploit them. Identifying these issues early is crucial to maintain the integrity and safety of open source 5G networks.

Before conducting a penetration test, we performed a vulnerability assessment on the open source 5G system. It's easy to confuse vulnerability assessments and penetration tests but the key difference lies in how the testing is conducted.

- **Vulnerability assessment** is an automated process where a tool scans the system and generates a report on identified issues whereas.
- **Penetration testing** on the other hand, is a manual process that relies on the expertise of a tester to find vulnerabilities in the system.

24.1 Vulnerability Assessment - Process

In the **Component Discovery** phase, we discover the vulnerabilities in a 5G Open RAN system which starts with deciding what you want to scan.

In **Component Priority** we selected to run a vulnerability assessment on a 5G Core system. In a perfect world, you would be running a vulnerability assessment regularly on all your systems. We selected based on host infrastructure which hold sensitive information like ID, MCC, MNC, encryption information etc.

In **Vulnerability Scanning** we used, Aqua Trivy which is an open-source tool that detects vulnerabilities and provides an explanation of risks so developers can decide which components they want to use in their applications and containers. Aqua Trivy has different scanners that look for different security issues, and different targets where it can find those issues. (43)

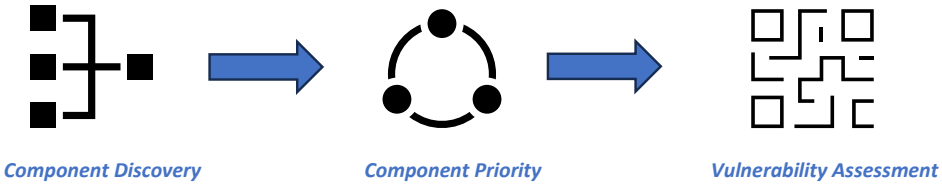

Figure 67 Vulnerability Assessment Steps

In case of 5G vulnerability analysis of 5G systems we tried to analyze different threats to various NFs. Comprehensive vulnerabilities can also be detailed categorized as below:

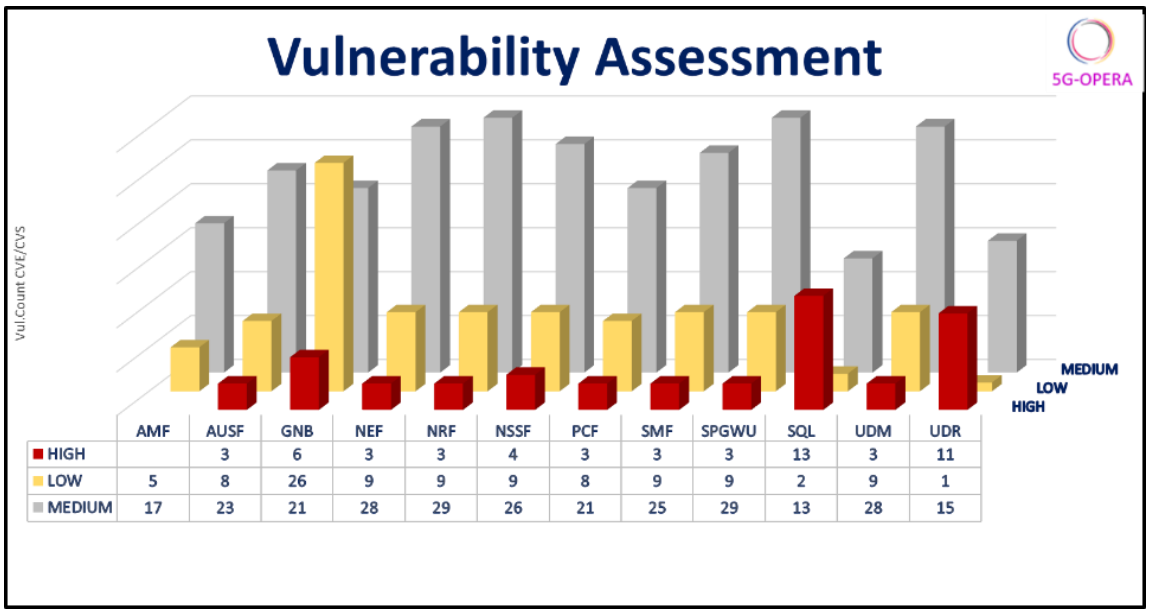

Figure 68 Vulnerability Assessment

24.1 AMF - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
AMF	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
AMF	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
AMF	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
AMF	liblzma5	CVE-2020-22916	MEDIUM	affected	6.2-0ubuntu2.1
AMF	libpcre3	CVE-2017-11164	LOW	affected	3.8.10-0ubuntu1~20.04.8
AMF	xz-utils	CVE-2023-39804	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 37 AMF Vulnerability

24.2 AUSF - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
AUSF	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
AUSF	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
AUSF	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
AUSF	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
AUSF	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1
AUSF	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.21
AUSF	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4
AUSF	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 38 AUSF Vulnerability

24.3 gNB - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
gNB	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
gNB	libapparmor1	CVE-2016-1585	MEDIUM	affected	2.13.3-7ubuntu5.2
gNB	libc6	CVE-2016-20013	LOW	affected	
gNB	libc6-dbg	CVE-2016-20013	LOW	affected	
gNB	libdbus-1-3	CVE-2023-34969	HIGH	affected	1.12.16-2ubuntu2.3
gNB	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
gNB	libpam-systemd	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.22
gNB	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1
gNB	libpython2.7-minimal	CVE-2021-4189	MEDIUM	affected	2.7.18-1~20.04.3
gNB	libpython3.8-minimal	CVE-2023-27043	MEDIUM	affected	
gNB	libpython3.8-stdlib	CVE-2023-27043	MEDIUM	affected	
gNB	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.22
gNB	ncurses-base	CVE-2023-50495	LOW	affected	6.2-0ubuntu2.1
gNB	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4
gNB	policykit-1	CVE-2016-2568	LOW	affected	0.105-26ubuntu1.3
gNB	python2.7	CVE-2021-4189	MEDIUM	affected	2.7.18-1~20.04.3
gNB	python3.8	CVE-2023-27043	MEDIUM	affected	3.8.10-0ubuntu1~20.04.8
gNB	python3.8-minimal	CVE-2023-27043	MEDIUM	affected	
gNB	systemd	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.22
gNB	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 39 gNB Vulnerability

24.4 NEF - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
NEF	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
NEF	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
NEF	libc6	CVE-2016-20013	LOW	affected	
NEF	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
NEF	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
NEF	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1

NEF	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.21
NEF	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4
NEF	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 40 NEF Vulnerability

24.5 NRF - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
NRF	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
NRF	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
NRF	libc6	CVE-2016-20013	LOW	affected	
NRF	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
NRF	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
NRF	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1
NRF	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.21
NRF	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4
NRF	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 41 NRF Vulnerability

24.6 NSSF - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
NSSF	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
NSSF	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
NSSF	libc6	CVE-2016-20013	LOW	affected	
NSSF	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
NSSF	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
NSSF	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1
NSSF	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.21
NSSF	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4
NSSF	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 42 NSSF Vulnerability

24.7 PCF - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
PCF	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
PCF	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
PCF	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
PCF	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
PCF	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1
PCF	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.21
PCF	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4

PCF	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 43 PCF Vulnerability

24.8 SMF - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
SMF	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
SMF	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
SMF	libc6	CVE-2016-20013	LOW	affected	
SMF	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
SMF	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
SMF	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1
SMF	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.21
SMF	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4
SMF	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 44 SMF Vulnerability

24.9 SPGWU - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
SPGWU	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
SPGWU	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
SPGWU	libc6	CVE-2016-20013	LOW	affected	
SPGWU	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
SPGWU	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
SPGWU	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1
SPGWU	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.21
SPGWU	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4
SPGWU	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 45 SPGWU Vulnerability

24.10 UDM - Vulnerability Discovery

5G Network Element	Library	Vulnerability	Severity	Status	Installed
UDM	coreutils	CVE-2016-2781	LOW	affected	8.30-3ubuntu2
UDM	libc-bin	CVE-2016-20013	LOW	affected	2.31-0ubuntu9.9
UDM	libc6	CVE-2016-20013	LOW	affected	
UDM	libexpat1	CVE-2023-52426	MEDIUM	affected	2.2.9-1ubuntu0.6
UDM	liblzma5	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1
UDM	libpcre3	CVE-2017-11164	LOW	affected	2:8.39-12ubuntu0.1
UDM	libsystemd0	CVE-2023-26604	LOW	affected	245.4-4ubuntu3.21
UDM	passwd	CVE-2013-4235	MEDIUM	affected	1:4.8.1-1ubuntu5.20.04.4
UDM	xz-utils	CVE-2020-22916	MEDIUM	affected	5.2.4-1ubuntu1.1

Table 46 UDM Vulnerability

25 Cryptography in Mobile Networks and Relevance on Post-Quantum Crypto

TLS, or Transport Layer Security, is a security protocol used to exchange information securely between two entities, usually called client and server. The main purpose of TLS is to provide privacy and data security for applications communicating over the internet. It works on top of TCP and is commonly used alongside HTTP on the application layer of the OSI model.

The TLS protocol comprises of 2 main phases: the TLS Handshake protocol and the TLS Record Protocol. In the first phase, the server gets authenticated (and optionally the client) and a set of keys for data integrity (through message authentication codes, MAC) and symmetric encryption of data is established. This keying material will then be used in the TLS Record Protocol phase for secure data exchange using symmetric cryptography, and for data integrity.

During the TLS Handshake phase, both parties will agree on a cipher suite to use for the communication, that is, the different cryptographic algorithms and protocols to be used during that communication instance/session. A critical point in this protocol phase is to determine which key encapsulation mechanisms (KEM) will be used to exchange or agree on the symmetric key used for data communication. Traditionally in TLS, KEMs based on RSA (Rivest-Shamir-Adleman) and DH (Diffie Hellman) have been used.

RSA is an asymmetric cipher used for data encryption and decryption based on the difficulty of the large integer factorization problem. An asymmetric cipher consists of a pair of keys, public and private key, an encryption procedure, and a decryption procedure. The public and private keys are mathematically related, but it is considered a mathematically hard problem to get the private key from the public key. When RSA is used in TLS for key exchange, the client chooses a symmetric key, it encrypts it with the server's public key, and sends it to the server. Once the message reaches the server, it decrypts the message with its private key and gets access to the key chosen by the client. At this point, both parties have a shared key, which they will use then to encrypt data symmetrically and communicate securely.

Diffie Hellman (DH) is a KEM used for two parties to agree on a shared secret without having to send the whole secret through the network at any point. Its security relies on the discrete logarithm problem, a mathematical hard problem which is thought to not be possible to solve efficiently by any traditional computer, no matter its computational power.

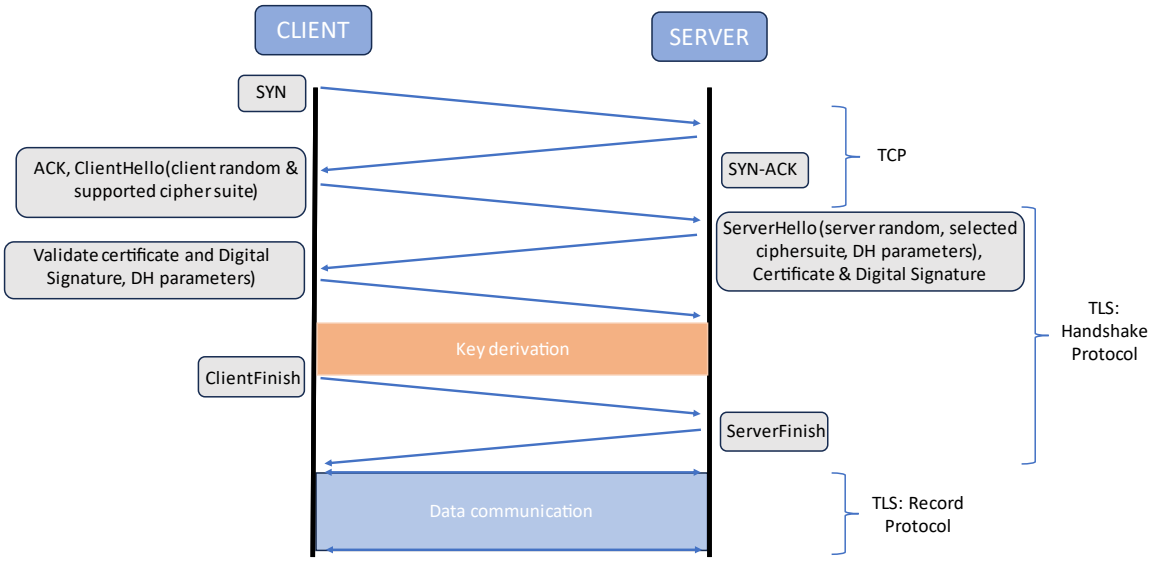

Figure 69 TLS communication establishment

As seen in Figure 69 TLS communication establishment (figure depicting the operation of TLS schematically), after agreeing on the cipher suite that both client and server will be using, the shared parameters for performing the key exchange/agreement are sent back and forth, and at the end of the TLS Handshake phase, both parties have a set of pairwise keys for secure communication, which are to be kept secret at all times.

These methods for agreeing on keying material are supposed to be secure if they are carefully implemented, and parameters with the enough length are chosen. However, the quantum computer era could jeopardize the security of systems using these schemes. It has been proven by Shor´s quantum algorithm that the hard problems on which RSA (large integer factorization) and DH (discrete logarithm) are based can be efficiently solved with a powerful enough quantum computer with only polynomial cost/complexity. Most of the cryptographic schemes being used in the present are, therefore, vulnerable to quantum computers adversary. Even if powerful enough quantum computers are not widely available in the market, the concept of “save now, decrypt later” is a concerning threat for data security, since once quantum computers powerful enough exist, those stored secrets could be revealed.

Particularly critical is the vulnerability of DH and DH-based KEM against quantum computer adversaries, given the fact that the majority of informatic systems around the world, and security protocol standards rely on and recommend this mechanism for establishing shared secrets. Therefore, security protocols that base their security on DH must be updated to support KEM resistant against quantum computers.

An approach to solve this problem is to develop new cryptographic techniques resistant to quantum computer attacks. In 2016, the National Institute of Standards and Technology (NIST) from the United States of America launched a worldwide competition for finding and standardizing quantum-resistant public-key cryptographic algorithms (44). This field is known as Post-Quantum Cryptography (PQC). After dozens of submissions and several testing and analysis rounds, in 2022, a list of candidate algorithms was chosen for standardization (45). For public-key encryption and key-establishment, CRYSTALS-KYBER was selected. For digital signatures, CRYSTALS-Dilithium, FALCON, and SPHINCS+ were chosen. These 4

algorithms are currently being standardized by NIST (46), and as of 2024 are in the draft standard of the Federal Information Processing Standard (FIPS). FIPS publications are issued by NIST.

The BSI (Bundesamt für Sicherheit in der Information Technik, or Federal Office for Information Security) elaborated a technical guideline with recommendations on cryptographic mechanisms for quantum-safe systems. In the previous report they suggest using the following quantum-resistant asymmetric mechanisms: FrodoKEM, Classic McEliece, and CRYSTALS KYBER (also known as Module-Lattice based KEM, ML-KEM).

Therefore, it is important to integrate these new suggested algorithms and mechanisms for making TLS secure against quantum adversaries. For implementing FrodoKEM into the TLS specifications, the following steps would have to be followed. First, both the client and the server should acknowledge their capability of using FrodoKEM for key agreement in the supported cipher suite list. Second, once this scheme is selected, client and server should exchange the FrodoKEM shared parameters and compute and generate their own secrets. Last, both parties will have the shared secret that will be used for secure communication using symmetric encryption. Following this procedure, a quantum-safe KEM could be implemented, in substitution of quantum-vulnerable schemas based on the RSA algorithm and versions of DH KEM.

However, given that the development and testing of quantum-secure key agreement and digital signature mechanisms are still on an early stage, it is advisable to transition to them with cautious. Due to the lack of testing of mentioned schemes, it is still possible that they are proven to be vulnerable to quantum computers, or even traditional computers currently widely available. An approach agreed upon academia (and a recommendation from the BSI) and the industry to overcome this issue is to develop hybrid systems (47). In such systems, both a traditional mechanism and a post-quantum safe mechanism are used, to ensure security in the present, as well as in the future.

Regarding the performance of Frodo KEM as a quantum-safe scheme in TLS, it is important to note the added overhead in most of the areas (connections per second, connection time) compared to traditional schemes is not critical, being always under the 2x mark (48). In the area of the handshake size, however, FrodoKEM uses significantly more resources than traditional schemes and other quantum-safe proposed schemes, on a scale of 1:20, with handshakes from traditional schemes needing around 1000 Bytes, while handshakes on PQC schemes take around 20.000 Bytes. Even when using FrodoKEM in hybrid cipher suites alongside with DH-based KEMs, the performance is not greatly affected (besides from the handshake size).

5G Opera components in which TLS is used can be found in Figure 59 TLS Agreement above section.

25.1 IPsec

IPsec, or Internet Protocol Security, is a set of protocols that contribute towards securing IP traffic on the network layer. The main protocol for establishing a secure communication between the communicating parties is called Internet Key Exchange (IKE). To have an end-to-end secure communication using IPsec, the following steps must be followed:

1. Initiate the communication. One of the two parties involved in the communication triggers the usage of IPsec.

2. IKE phase 1: during this phase, a secure channel for management traffic is established. The communicating peers negotiate and agree on a cipher suite, which always includes a DH group mechanism as a KEM and perform the key agreement. After a secure channel has been created, it is used for establishing a second secure channel in the following step.
3. IKE phase 2: the goal of the current phase is for the peers to negotiate, in a secure way (as opposed to default TLS), a set of rules such as the IPsec protocol to use for data exchange (related to the headers), the encapsulation mode, encryption and authentication algorithms and completing a new DH exchange, if desired. After the completion of this phase, the actual tunnel for secure data transmission is created.
4. Data communication. After the two IKE phases, the peers have all the information and shared secret keys to start communicating securely using symmetric encryption.

Figure 70 IPsec communication establishment summarizes the steps of IPsec for securing communications.

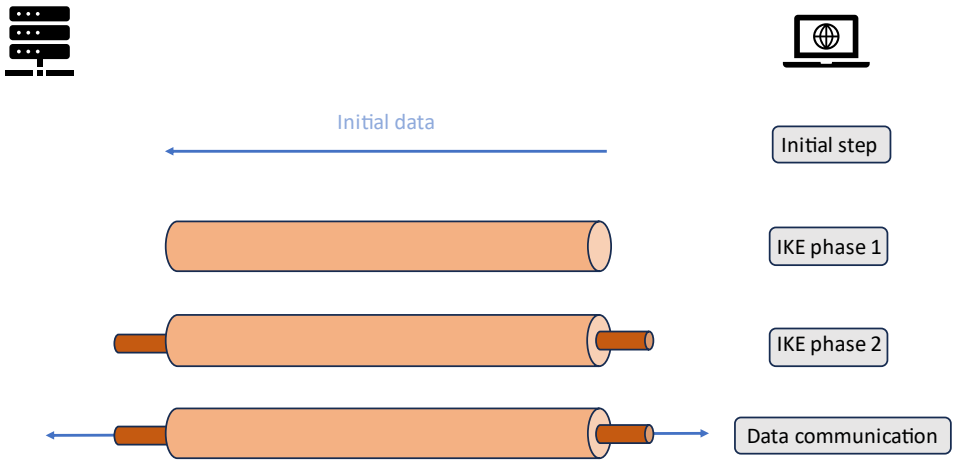

Figure 70 IPsec communication establishment

Therefore, to properly secure IPsec and make it resistant to quantum computers, it is necessary to substitute the DH KEM in both IKE phases for a scheme from the PQC field. The same suggestions and principles as those applied to TLS apply here, that is, substituting DH by CRYSTALS-Dilithium (49) (as recommended by NIST) or by FrodoKEM (50) (as suggested by the BSI). Both schemes would increase the security capabilities of the IPsec suite though enhancing the KEM used in IKE.

5G Opera components in which IPsec is used can be found in above section Figure 61 IPsec Agreement

25.2 Homomorphic Message Authentication Code (HMAC)

Homomorphic Message Authentication Codes (HMACs) represent a cryptographic solution that ensures both the security and integrity of network packets. HMACs provide a mechanism for authenticating messages and verifying data integrity, which is crucial for protecting network communications from tampering and unauthorized access. However, in scenarios where the packet pollution ratio is low,

individually verifying each packet can become inefficient and computationally expensive. To address this inefficiency, batch verification methods have been developed in the literature, allowing for the simultaneous verification of multiple packets as a group. This approach significantly reduces the complexity and resource requirements of the verification process, making it a practical solution for maintaining security and integrity in networks with high packet volumes or constrained computational resources.

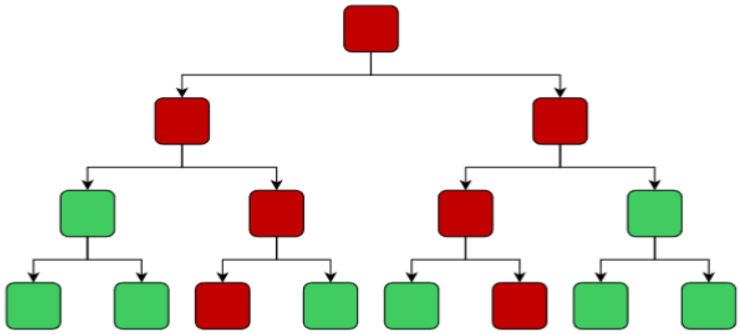

Figure 71. Binary Tree Verification Scheme

Binary tree-based verification scheme in Figure 71. Binary Tree Verification Scheme. is provided for homomorphic signature schemes to reduce verification complexity. In Figure 71 green and red boxes represent non-polluted and polluted packets, respectively. Additionally, the packets are linearly summed up to create the packet in the upper layer. At the end, the packet in the highest layer is the summation of the packets in the lowest layer. Then, the verification starts with the packet at the highest layer and continues with the leaves of the polluted packets (red boxes). This process continues until the lowest layer.

We implemented the idea for HMACs to evaluate the scheme's performance in terms of complexity. As seen in below graph, Tree Based verification scheme provides a low complex solution for the verification of the packets in the low pollution rate scenarios in the networks.

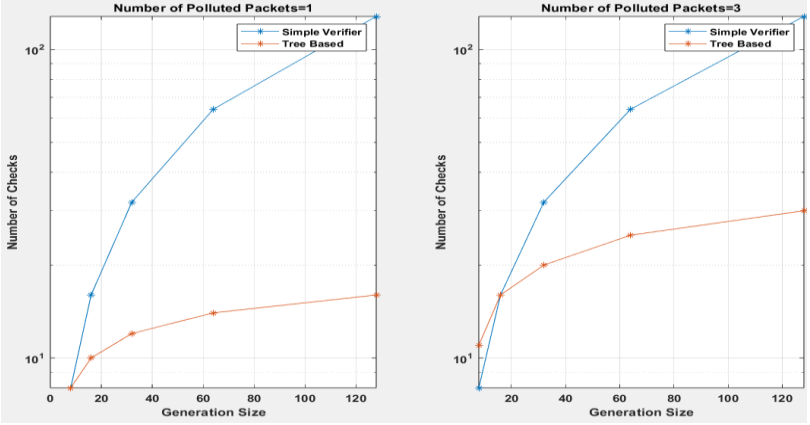

Figure 72 Comparison between Individual Packet Verification and Tree Based Verification

26 ML – based Mechanisms for Edge Security

In a case study done by NXP, even though 5G systems gain more visibility and participation in conventional communication scenarios (e.g., Internet and multimedia traffic) every day, other capabilities useful for automation and safe transportation such as URLLC are still not widely deployed. In that sense, 5G technologies are still nascent and have inherent complexity that pose some challenges to data security and privacy, as not all attack vectors on them are currently understood. Strategies of malicious actors are always evolving and increasingly call for approaches that leverage artificial intelligence to deal with the conquering attempts to take out critical communication infrastructure. The work to be presented in this section considers the premise that machine learning approaches are currently underexplored with regards to 5G network security and might help in closing security gaps in such communications systems. This report highlights that anomaly detection at the edge (i.e. RAN) shows promising results in identifying cyber-attacks by monitoring hardware performance counters (HPCs) at the Distributed Unit HW platform of a 5G private network.

26.1 Anomaly Detection Concept

Anomaly detection is the practice of detecting instances of a behavior that represent some deviation from a defined pattern considered normal (51). Such anomalous instances may also be regarded as outliers or novelties. A simple visualization of the anomaly detection approach is illustrated in where N1 and N2 represent the distribution of normal behavior, and O1-3 are potential anomalies or outliers. In other terms, anomaly detection differs from other machine learning applications, like image classification, in so far as that it does not try to match patterns but tries to model distributions of normal behavior. Data points that fall outside of this distribution of defined normality is deemed to be an anomaly.

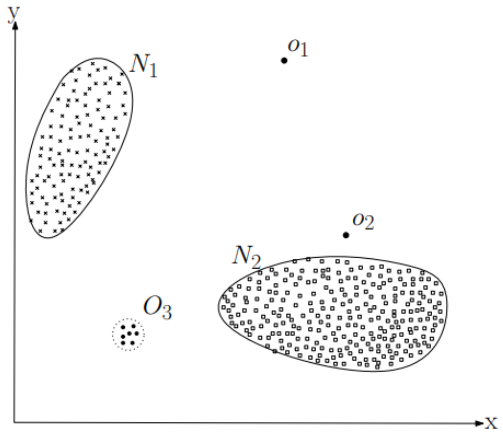

Figure 73. Example of anomaly detection (52)

Different from other strategies that explore using ML-based security mechanisms at the 5G Core Network or at architectural components outside the RAN, the solution proposed in 5G-OPERA aims at detecting anomalies at lower layers of the 5G communication stack, allowing for an earlier inference of attacks.

Since NXP's LX2160A processor enables the implementation of Distributed Units (O-DU) or even Radio Units (O-RU) in the project, that component was selected as the observed hardware to identify security risks close to the 5G Physical Layers.

The selected processor can eventually be attacked on both hardware and software level and there are possible exploits not yet known. The security challenges can be managed as an anomaly detection task, modeling normal behavior of the system, then creating a thorough distribution of what is deemed to be benign activity and later compare it to anomalous activity that is outside of that distribution. The additional benefit of such strategy is that it allows to combine two core strengths of NXP's edge-technology, namely: data processing and AI capabilities.

26.2 Implementation of Anomaly Detection at RAN

As contribution to the security extensions for open RAN 5G systems in 5G OPERA project, it is proposed the implementation of an anomaly detection system that consists of a data-mining toolkit specialized in scraping periodic snapshots of the current HPCs, storing each snapshot in an in-memory database (based on open-source Redis). Complementarily, different data collection procedures were implemented, for instance the execution of attacks targeting the hardware performance counters of the processor where the data-mining toolkit is running on. In addition, the system includes several end-to-end machine learning pipelines such as data processing or feature selection as well as the implementation of a variety of machine learning procedures selected to perform anomaly detection on different iterations of the collected datasets. Finally, since some of the used machine learning tend to need either engineering (OCSVM, KDE) to circumvent the disadvantages of dimensionality, or rigorous hyperparameter-tuning to avoid getting stuck in local minima (AE, VAE, etc.), one more contribution is the implementation of a generalized hyperparameter software tool that optimizes said machine learning procedures.

26.2.1 Set-Up

Since the implemented approach for detecting and classifying anomalous behavior requires custom data that to the best knowledge of the research team was not publicly available, a custom 5G system was deployed in NXP laboratories to simulate the ML-tool behavior in a real-life setting. The setup was also intended for validating the selected anomaly detection procedures on it. The 5G system includes a 5G CN and the data mining toolkit running on the LX2160 processor at the DU to continuously collect snapshots of the system in form of HPCs. The setup also includes a machine learning pipeline that implements end-to-end data processing, training, and evaluation of different anomaly detection models.

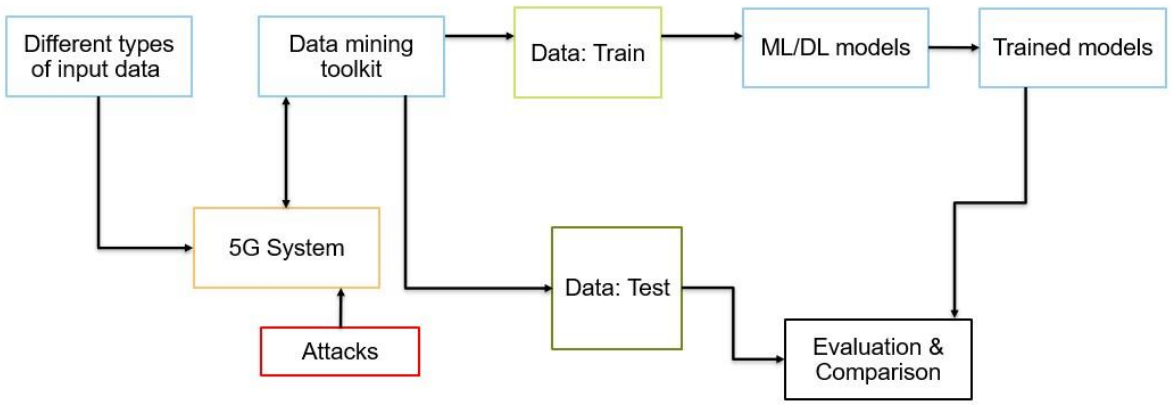

Figure 74. Model of our experimental data mining and anomaly detection setup

26.2.2 Data Mining Tool Kit

The data mining toolkit takes periodic snapshots of the HPCs from the LX2160 processor where the toolkit is running on, effectively providing a summary view of the chip's current state. Among the 234 features extracted with each snapshot, around 80 are related to the actual state of the CPU, cache, memory, etc. Notably, this data mining toolkit can run on any Linux distribution. Each snapshot is stored in a Redis database and subsequently processed for a downstream machine learning task. Since the goal is a system capable of doing real-time inference on the edge without degrading the data processing capabilities of the LX2160, discrete samples of the HPCs are taken rather than collecting a continuous stream of data. That is also compatible with the goal of detecting anomalous behavior from point anomalies alone.

26.2.3 Dataset

To effectively implement the ML-based anomaly detection system, custom datasets are needed to validate the methodology. Those datasets in general appeared to be not accessible to the public and, when accessible, they either were mostly outdated, or too specialized, or feature various deficiencies (53) reference section below, that make them unsuitable for the proposed task. To address this problem the above-described data mining toolkit was designed to build the needed datasets from scratch.

26.2.4 Machine Learning Pipelines

Implemented distance-based methods include K-Nearest Neighbor (KNN) (54), Local Outlier Factor (LOF) (55) and Random Forest (RF) (56). These methods served as comparative baselines to more sophisticated procedures deployed in further phases of the research. One-Class SVM method (OCSVM) (57) was implemented to compare against the more complex and deeper approaches. For the probabilistic component of the used methods, Kernel Density Estimation (KDE) with a gaussian RBF kernel (58) and VAE (59) were deployed, which are both a reconstruction and probabilistic method (60). Apart from PCA (61), the implemented reconstruction-based methods include AE (62) and VAE, which both make use of reconstruction score and threshold values to predict normal and anomalous behavior.

26.2.5 Hyper-Parameter Tuning

Some of deep methods implemented, such as Autoencoders (AE) and Variational Autoencoders (VAE) are prone to getting stuck in local minima, and thus tend to benefit greatly from optimization. A hyperparameter tuning toolkit was developed to search across all relevant variables of these models and assess the upper bound of performance on the custom datasets.

26.3 Results

Since the proposed anomaly detection system aims at modeling a given definition of normal behavior, the primary focus is to evaluate unsupervised or semi-supervised learning methods. The reconstruction-based approaches of the AE and the probabilistic reconstruction approach of VAE are well suited for learning non-linear relationships from a benign dataset. Because of this, it was concluded that those model architectures were most likely to perform well on achieving the goals. **Error! Reference source not found.**In summary, intermittent results have validated this informed guess so far, with both AE and VAE topping the charts of the implemented unsupervised and semi-supervised methods, with VAE almost reaching the perfect performance of the baseline supervised methods of RF and KNN.

Method Type	Learning Type	Model Name	AUC	AP
Distance	Unsupervised	LOF	0.5	0.164
Distance	Unsupervised	IsoForest	0.764	0.926
Reconstruction	Unsupervised	KMeans	0.765	0.922
Classification	Semi-supervised	OCSVM	0.8	0.803
Probabilistic	Unsupervised	KDE	0.829	0.882
Reconstruction	Semi-supervised	**AE**	**0.905**	**0.844**
Probabilistic	Semi-supervised	**VAE**	**0.978**	**0.969**
Distance	Supervised	KNN	1.0	1.0
Distance	Semi-supervised	RF	1.0	1.0

Table 47 AUC and AP detection performance for chosen methods on our custom HPC dataset.

To explore a preliminary assertion on why some of the implemented methods perform so well on the custom dataset, it is useful to look at a low-dimensional representation of the dataset in, the first two principal components of the linear dimensionality reduction method PCA, and the first two components of the non-linear dimensionality reduction method t-SNE provide an inside into the data distribution of the generated dataset. Both visualizations show that the distribution of normal and anomalous behavior can be differentiated, which matches the starting assumption.

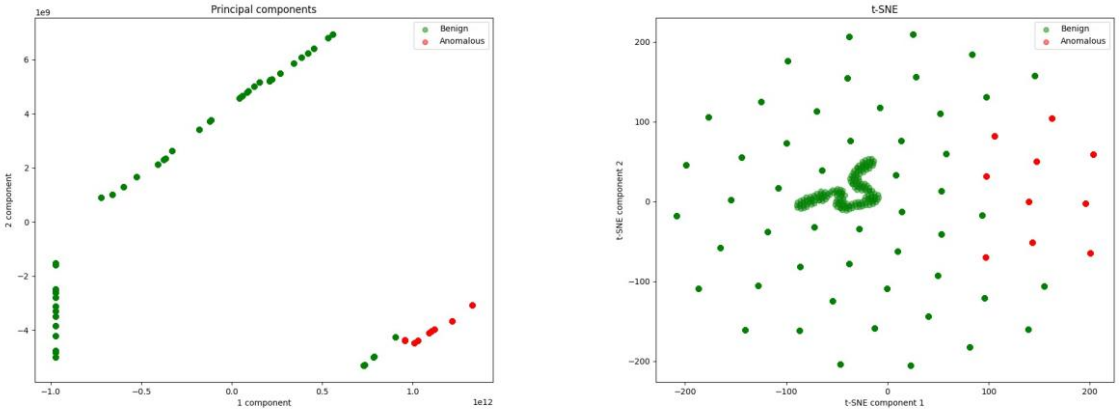

Figure 75 Linear reduction method PCA (left) and non-linear approach t-SNE (right)

27 Conclusion

The **"5G OPERA Security Specific Extension**" collaboratively undertaken by IABG, NXP-GE, and TU Dresden, has thoroughly analyzed the multifaceted security requirements and challenges associated with 5G standalone networks. This project underscores the significance of a robust security model to counteract diverse threats that 5G networks face, ensuring both their integrity and reliability.

In our detailed exploration, we dissected various attack vectors, meticulously identifying phases and corresponding countermeasures using the MITRE ATT&CK and D3FEND Frameworks. This approach facilitated the development of comprehensive strategies to safeguard 5G networks against potential breaches and disruptions. Our findings emphasize the necessity of deploying state-of-the-art security functionalities, such as firewalls, IDS/IDP systems, and zero-trust architectures, which are critical in minimizing the risk and impact of attacks by evaluating the Risk Rating for each attack.

Moreover, our recommendations for network security enhancements by implementing the “OPERA Security Model - OSM” including the implementation of stringent traffic management protocols and enforcing end-to-end encryption. These measures are designed to bolster the defense mechanisms, thereby mitigating the potential damage from both known and emerging threats.

Through the extensive use of the STRIDE model, we analyzed and prioritized threats based on their likelihood and impact, which enabled us to tailor our countermeasures effectively. Additionally, we also map the model to OPERA 5G Tiers and deep dive into these methodologies ensures a robust defense posture, providing a resilient framework capable of withstanding sophisticated cyber threats.

In conclusion, the successful execution of the 5G OPERA project highlights the critical role of collaborative efforts in advancing 5G security. By adopting the recommended security measures and continuously evolving to address new vulnerabilities, the 5G ecosystem can achieve a higher level of security, ensuring safe and reliable network operations for the future.

28 References

1. **3GPP.** 3GPP. [Online] ETSI. https://www.3gpp.org/.

2. **SA3, Portal 3GPP.** Portal 3GPP SA3 . [Online] https://portal.3gpp.org/Home.aspx?tbid=375&SubTB=386#/.

3. **ETSI.** ETSI. [Online] https://www.etsi.org/technologies/cyber-security.

4. **ITU-T.** ITU. [Online] https://www.itu.int/en/ITU-T/studygroups/2017-2020/17/Pages/default.aspx.

5. **IETF.** IETF - RFC's. [Online] https://www.ietf.org/rfc/.

6. **[Online] https://www.ieee.de/about/.**

7. NIST. NIST-Open RAN. [Online] https://www.nist.gov/programs-projects/open-ran-research-nist.

8. [Online] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

9. [Online] https://attack.mitre.org/techniques/enterprise/.

10. Chain, Lockheed Martin Cyberkill. Cyberkill Chain. [Online] https://www.ek.co/publications/the-7-steps-of-the-cyber-kill-chain/.

11. ATT&CK, MITRE. MITRE ATT&CK - Enterprise. [Online] https://attack.mitre.org/matrices/enterprise/.

12. —. MITRE ATT&CK - Mobile. [Online] https://attack.mitre.org/matrices/mobile/.

13. D3FEND, MITRE. MITRE D3FEND. [Online] https://d3fend.mitre.org/dao/.

14. Group, ORAN Security Working. O-RAN. [Online] https://www.o-ran.org/blog/the-o-ran-alliance-security-working-group-continues-to-advance-o-ran-security.

15. Testing, Security. Security Testing. [Online] https://www.viavisolutions.com/en-us/solutions/open-ran-security-test.

16. RAN, Mitgation - Open. Open RAN. Mitigation Methodology. [Online] https://link.springer.com/article/10.1007/s12243-024-01036-2.

17. wireless-communication, Test-and-Measurement. Rohde-Schwarz. [Online] https://www.rohde-schwarz.com/de/loesungen/test-and-measurement/wireless-communication/mobile-network-infrastructure-testing/open-ran-tests/open-ran-tests_255230.html.

18. Testing, Penthertz - Penetration. Penthertz - Penetration Testing. [Online] https://penthertz.com/blog/OpenRAN-New-classes-of-attack-against-mobile-operators-from-the-outside.html.

19. Attack, KALI - Hydra. KALI . [Online] https://www.kali.org/tools/hydra/.

20. Etherape, KALI. KALI Etherape. [Online] https://etherape.sourceforge.io/.

21. TTP's, MITRE ATT&CK -. MITRE ATT&CK - TTP's. [Online] https://attack.mitre.org/techniques/T1110/.

22. NMAP. KALI-NMAP. [Online] https://nmap.org/.

23. KALI-NMAP. Kali. [Online] https://nmap.org/.

24. Hawaii, VSFTPD - Uni of. VSFTPD. [Online] https://westoahu.hawaii.edu/cyber/forensics-weekly-executive-summmaries/8424-2/.

25. Resources, Fuzzing 5G replay - Git. Fuzzing 5G replay - Git Resources. [Online] https://github.com/Montimage/5Greplay.

26. *5GHOUL : Unleashing Chaos on 5G Edge Device.* (SUTD), Matheus E. Garbelini. 1.0, Matheus E. Garbelini (SUTD).

27. Garbelini1, Matheus E., et al. 5Ghoul : Unleashing Chaos on 5G Edge Devices. [Online] https://asset-group.github.io/disclosures/5ghoul/.

28. Do, Thoai Van. Threat Modelling Framework for 5G . [Online] https://www.duo.uio.no/bitstream/handle/10852/108537/1/thoaivd-final.pdf.

29. CCMB-2017-04-004. Common Methodology for Information Technology Security Evaluation. [Online] https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf.

30. Methodology, Evaluation. CEM-99/045. [Online] https://www.commoncriteriaportal.org/files/ccfiles/cemv10.pdf.

31. ENISA. ENISA.EUROPA.EU. [Online] https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_iso133352.html.

32. Overview, O-RAN Architecture. O-RAN Alliance. [Online] https://docs.o-ran-sc.org/en/latest/architecture/architecture.html.

33. Pentehrtz. Intruding 5G SA core networks from outside and inside. [Online] https://penthertz.com/blog/Intruding-5G-core-networks-from-outside-and_inside.html.

34. 501, ETSI TS 133. 5G; Security architecture and procedures for 5G System (3GPP TS 33.501 version 15.2.0 Release 15) . [Online] https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/15.02.00_60/ts_133501v150200p.pdf.

35. Parveen, Simpy, Safavi-Naini, Reihaneh and Kneppers, Marc. DTLS with Post-quantum Secure Source Authentication and Message Integrity. [Online] https://ieeexplore.ieee.org/document/9681952.

36. Qianran Wang, Jinhua Wang, and Chengbin HuangAuthors. The Optimization of IPSec VPN in 5G Mobile Communication Network. [Online] https://dl.acm.org/doi/10.1145/3605801.3605818.

37. Saleem, Imran. OAuth2.0 Security and Protocol Exploit Analysis in 5G Ecosystem. [Online] https://www.researchgate.net/publication/371401470_OAuth20_Security_and_Protocol_Exploit_Analysis_in_5G_Ecosystem.

38. Lanzenberger, David. Formal Analysis of 5G Protocols. [Online] https://ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/information-security-group-dam/research/software/5G_lanzenberger.pdf.

39. Muhammad Najmul Islam Farooqui, Junaid Arshad. A Layered Approach to Threat Modeling for 5G-Based Systems. [Online] https://www.mdpi.com/2079-9292/11/12/1819.

40. Sharique, Ahmad. GIT . https://github.com/shariquetelco/5g_Threat_model/blob/main/Threat%20Taxonomy%20-%20Categories%20(1).png. [Online] https://github.com/shariquetelco/5g_Threat_model/blob/main/Threat%20Taxonomy%20-%20Categories%20(1).png.

41. —. GIT . 5g_Threat_model. [Online] https://github.com/shariquetelco/5g_Threat_model/blob/main/Threat%20Taxonomy%20-%20Layered.png.

42. OPEN RAN SECURITY REPORT. www.ntia.gov. [Online] MAY 2023. https://www.ntia.gov/sites/default/files/publications/open_ran_security_report_full_report_0.pdf.

43. TRIVY. TRIVY. [Online] https://github.com/aquasecurity/trivy.

44. Division, I. T. L. Computer Security. *Call for proposals - Post-Quantum Cryptography | CSRC | CSRC.* s.l. : CSRC | NIST, https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals, Jan. 03, 2017.

45. I. T. L. Computer Security, Division. *Selected Algorithms 2022 - Post-Quantum Cryptography | CSRC | CSRC.* s.l. : CSRC | NIST, https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022, Jan. 03, 2017.

46. NIST. *NIST to Standardize Encryption Algorithms That Can Resist Attack by Quantum Computers.* s.l. : NIST. https://www.nist.gov/news-events/news/2023/08/nist-standardize-encryption-algorithms-can-resist-attack-quantum-computers, Aug. 2023.

47. BSI. *BSI - Technical Guideline.* s.l. : Available: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile&v=10.

48. J. Bos et et al., J. *Frodo: Take off the ring! Practical, Quantum-Secure Key Exchange from LWE.* s.l. : Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, doi: 10.1145/2976749.2978425., Oct. 24, 2016.

49. Cryptographic Suite for Algebraic Lattices. pq.crystals. [Online] https://csrc.nist.gov/CSRC/media/Presentations/Crystals-Dilithium/images-media/CRYSTALS-Dilithium-April2018.pdf.

50. MICROSOFT. FrodoKEM: Learning with Errors Key Encapsulation. [Online] https://github.com/microsoft/PQCrypto-LWEKE.

51. Lukas Ruff, Robert Vandermeulen, Nico Goernitz, Lucas Deecke, Shoaib Ahmed Siddiqui, Alexander Binder, Emmanuel Müller, and Marius Kloft. Deep one-class classification. ***Proceedings of the 35th International Conference on Machine Learning.*** **2018. Vol. 80, Proceedings of MAchine LEarning Research, PMLR.**

52. Varun Chandola, Arindam Banerjee, and Vipin Kumar. Anomaly detection: A survey. ***ACM Comput. Surv.*** **2009. 41.**

53. Ansam Khraisat, Iqbal Gondal, Peter Vamplew, and Joarder Kamruzzaman. Survey of intrusion detection systems: techniques, datasets and challenges. ***Cybersecurity.*** **2019. 2.**

54. Wikipedia, contributors. K-nearest neighbors algorithm. ***Wikipedia, the free encyclopedia.*** **[Online] [Cited: May 3, 2024.]**

55. Markus M. Breunig, Hans-Peter Kriegel, Raymond T. Ng, and Jörg Sander. Lof: identifying density-based local outliers. ***Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data.*** **New York : Association for Computing Machinery, 2000.**

56. Breiman, Leo. Random forests. ***Machine Learning.*** **2001. Vol. 45, 1.**

57. Bernhard Schölkopf, John C. Platt, John C. Shawe-Taylor, Alex J. Smola, and Robert C. Williamson. Estimating the support of a high-dimensional distribution. ***Neural Comput.*** **2001. Vol. 13, 7.**

58. Wikipedia, contributors. Density estimation. ***Wikipedia, the free encyclopedia.*** **[Online] [Cited: Apr 29, 2024.]**

59. Welling, Diederik P Kingma and Max. Auto-encoding variational bayes. 2022.

60. Lukas Ruff, Jacob R. Kauffmann, Robert A. Vandermeulen, Gregoire Montavon, Wojciechamek, Marius Kloft, Thomas G. Dietterich, and Klaus-Robert Muller. A unifying review of deep and shallow anomaly detection. ***Proceedings of the IEEE.*** **2021. Vol. 109, 5.**

61. Bishop, Christopher. Pattern Recognition and Machine Learning. s.l. : Springer, 2006.

62. Ian Goodfellow, Yoshua Bengio, and Aaron Courville. Deep Learning. 2016 : MIT Press.

29 ANNEX

Annex 1 MITRE ATT&CK Reference Hydra Threat

MITRE ATT&CK REF.						
	Tactical Phase	**1.Reconnaissance**	**2.Reconnaissance**	**3.Reconnaissance**	**4.Reconnaissance**	**5.Resource Development**
	Technique	Gather Victim Network Information	Gathering Victim Host Information	Active Scanning	Active Scanning	Obtain Capabilities
	Sub-Technique	Network Topology	Client Configuration;	Scanning IP Blocks	Vulnerability Scanning	Tool
	MITRE Reference	T1590.004	T1592.004	T1595.001	T1595.002	T1588.002
	Annex	---	---	---	Picture / Listing / Console Result	
	Tactical Phase	**6.Execution**	**7.Credential Access**	**8. Impact**	**9. Impact**	
	Technique	Command and Scripting Interpreter	Brute Force	Service Stop	Access 5G Operator Key	
	Sub-Technique	Unix Shell	Password Spraying	Service Stop	Access 5G Operator Key	
	MITRE Reference	T1059.004	T1110.003	T1489	---	
	Annex	Picture / Listing Console			Picture of OPKEY in amf.conf	

Annex 2 MITRE ATT&CK Threat Reference Hydra Threat

List of Threat ID´s

Tactics				
Reconnaissance	**Resource Development**	**Execution**	**Credential Access**	**Impact**
TA0043	TA0042	TA0002	TA0006	TA0040
18 October 2020	30 September 2020	19 July 2019	19 July 2019	25 July 2019
3 November 2023	3 November 2023	3 November 2023	3 November 2023	3 November 2023

Techniques			
Gather Victim Network Information	**Gather Victim Host Information**	**Active Scanning**	**Obtain Capabilities**
ID : T1590	ID : T1592	ID : T1595	ID : T1588
15 April 2021	17 October 2021	8 March 2022	18 October 2021
3 November 2023	3 November 2023	3 November 2023	3 November 2023
Command and Scripting Interpreter	**Brute Force**	**Service Stop**	**Access 5G Operator Key**
ID : T1059	ID : T1110	ID : T1489	**ID: TIABG.001**
27 March 2023	14 April 2023	28 July 2022	3 November 2023
3 November 2023	3 November 2023	3 November 2023	3 November 2023

Sub-Techniques						
Network Topology	**Client Configuration**	**Scanning IP-Blocks**	**Vulnerability Scanning**	**Tool**	**Unix Shell**	**Password Spraying**
ID : T1590.004	ID : T1592.004	ID : T1595.001	T1595.002	ID : T1588.002	ID : T1059.004	ID : T1110.003
15 April 2021	17 October 2021	15 April 2021	13 March 2023	17 October 2021	26 July 2021	16 October 2023
3 November 2023	3 November 2023	3 November 2023	3 November 2023	3 November 2023	3 November 2023	3 November 2023

ID: TIABG.001: The technique ID is not available in MITRE ATT&CK Framework status 3rd Nov 23.

Annex 3 MITRE ATT&CK Reference Metasploit Threat

MITRE ATT&CK Ref.							
	Tactical Phase	1. Resource Development	2. Resource Development	3. Resource Development	4. Reconnaissance	5. Initial Access	6. Initial Access
	Technique	Acquire Infrastructure	Compromise Infrastructure	Obtain Capabilities	Active Scanning	Exploit Public-Facing Application	Valid Accounts
	Sub-Technique	Web Services	Web Services	Vulnerabilities	Vulnerability Scanning	-	Local Accounts
	MITRE Reference	T1583.006	T1584.006	T1588.006	T1595.002	T1190	T1078.003
	Tactical Phase	7. Execution	8. Credential Access	9. Command and Control	10. Exfiltration	11. Impact	12. Impact
	Technique	Exploitation for Client Execution	Exploitation for Credential Access	Content Injection	Exfiltration Over Web Service	Resource Hijacking	System Shutdown/Reboot
	Sub-Technique	-	-	-	Exfiltration Over Webhook	-	-
	MITRE Reference	T1203	T1212	T1659	T1567.004	T1496	T1529

Annex 4 MITRE ATT&CK Threat Reference Metasploit Threat

List of Threat ID´s

Tactics							
Resource Development	**Reconnaissance**	**Initial Access**	**Execution**	**Credential Access**	**Command and Control**	**Exfiltration**	**Impact**
TA0042	TA0043	TA0001	TA0002	TA0006	TA0011	TA0010	TA0040
30 September 2020	18 October 2020	19 July 2019	19 July 2019	19 July 2019	19 July 2019	19 July 2019	25 July 2019
10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024

Techniques					
Acquire Infrastructure	**Compromise Infrastructure**	**Obtain Capabilities**	**Active Scanning**	**Exploit Public-Facing Application**	**Valid Accounts**
T1583	T1584	T1588	T1595	T1190	T1078
30 October 2023	2 October 2023	18 October 2021	8 March 2022	14 April 2022	30 March 2023
10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024

Techniques					
Exploitation for Client Execution	**Exploitation for Credential Access**	**Content Injection**	**Exfiltration Over Web Service**	**Resource Hijacking**	**System Shutdown/Reboot**
T1203	T1212	T1659	T1567	T1496	T1529
18 April 2022	15 October 2023	1 October 2023	5 September 2023	2 October 2023	2 March 2023
10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024

Sub-Techniques					
Web Services	**Web Services**	**Vulnerabilities**	**Vulnerability Scanning**	**Local Accounts**	**Exfiltration Over Webhook**
T1583.006	T1584.006	T1588.006	T1595.002	T1078.003	T1567.004
12 April 2023	12 April 2023	15 April 2021	13 March 2023	14 July 2023	12 October 2023
10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024	10 January 2024

Annex 5 MITRE ATT&CK Reference VSFTPD Threat

MITRE ATT&CK REF.						
	Tactical Phase	**1. Reconnaissance**	**2. Reconnaissance**	**3. Resource Development**	**4. Resource Development**	**5. Initial Access**
	Technique	Active Scanning	Gather Victim Network Information	Compromise Infrastructure	Obtain Capabilities	Trusted Relationship
	Sub-Technique	Vulnerability Scanning	IP Addresses	Server	Tool	´---
	MITRE Reference	ID: T1595.002	T1590.005	T1584.004	T1588.002	T1199
	Tactical Phase	**7. Execution**	**8. Execution**	**9. Privilege Escalation**	**10. Credential Access**	**11. Lateral Movement**
	Technique	Command and Scripting Interpreter	Scheduled Task/Job	Create or Modify System Process	Forced Authentication	Lateral Tool Transfer
	Sub-Technique	Unix Shell	Cron	Launch Daemon	´---	´---
	MITRE Reference	T1059.004	T1053.003	T1543.004	T1187	T1570
	Tactical Phase	**13.Impact**				
	Technique	Data Manipulation				
	Sub-Technique	Stored Data Manipulation				
	MITRE Reference	T1565.001				

Annex 6 MITRE ATT&CK Threat Reference VSFTPD Threat

List of Threat ID´s

Tactics				
Reconnaissance	Resource Development	Initial Access	Execution	Privilege Escalation
TA0043	TA0042	TA0001	TA0002	TA0004

Tactics			
Credential Access	Lateral Movement	Exfiltration	Impact
TA0006	TA0008	TA0010	TA0040

Techniques					
Active Scanning	Gather Victim Network Information	Compromise Infrastructure	Obtain Capabilities	Trusted Relationship	Command and Scripting Interpreter
T1595	T1590	T1584	T1588	T1199	T1059

Techniques					
Scheduled Task/Job	Create or Modify System Process	Forced Authentication	Lateral Tool Transfer	Scheduled Transfer	Data Manipulation
T1053	T1543	T1187	T1570	T1029	T1565

Sub-Techniques			
Vulnerability Scanning	'IP Addresses	Server	Tool
ID: T1595.002	T1590.005	T1584.004	T1588.002

Sub-Techniques			
Unix Shell	Cron	Launch Daemon	Stored Data Manipulation
T1059.004	T1053.003	T1543.004	T1565.001

Annex 7 MITRE ATT&CK Reference Jamming Threat

MITRE ATT&CK Ref.	Tactical Phase	1 Reconnaissance	1.2 Reconnaissance	2 Execution	3 Discovery	4 Exfiltration	5 Impact
	Technique	Gather Victim Host Information	Gathering Victim Host Information	Native API	Network Sniffing	Automated Exfiltration	Network Denial of Service
	Sub-Technique	Hardware	Software	-	-	Traffic Duplication	-
	MITRE Reference	T1592.001	T1592.002	T1106	T1040	T1020.001	T1464

Annex 8 MITRE ATT&CK Threat Reference Jamming Threat

List of Threat ID´s					
	Tactics				
	Reconnaissance	**Execution**	**Discovery**	**Exfiltration**	**Impact**
	ID:TA0043	ID : TA0002	ID : TA0007	ID : TA0010	ID : TA0034
	18.Oct 20	19-Jul-19	19-Jul-19	19-Jul-19	20.Mar 23
	01.Dec 23	01.Dec 23	01.Dec 23	01.Dec 23	01.Dec 23
	Techniques				
	Gather Victim Host Information	**Native API**	**Network Sniffing**	**Automated Exfiltration**	**Network Denial of Service**
	ID : T1592	ID : T1106	ID : T1040	ID : T1020	ID : T1464
	17.Oct 21	13.Oct 23	10-Jul-23	19-Apr-22	20.Mar 23
	01.Dec 23	01.Dec 23	01.Dec 23	01.Dec 23	01.Dec 23
	Sub-Techniques				
	Hardware	**Software**	**Traffic Duplication**		
	ID : T1592.001	ID : T1592.002	ID : T1020.001		
	17.Oct.21	17.Oct.21	14-Apr-23		
	01.Dec 23	01.Dec 23	01.Dec 23		

Network Denial of Service: The technique id is part of MITRE ATT&CK Framework from Mobile domain.

Annex 9 MITRE ATT&CK Reference Fuzzing Core

MITRE ATT&CK Ref.							
	Tactical Phase	**1.Reconnaissance**	**2.Reconnaissance**	**3.Resource Development**	**4.Execution**	**5.Execution**	**6.Privilege Escalation**
	Technique	Active Scanning	Search Open Websites/Domains	Obtain Capabilities	Command and Scripting Interpreter	Software Deployment Tools	Account Manipulation
	Sub-Technique	Scanning IP Blocks	Code Repositories	Tool	Unix Shell	-	Additional Container Cluster Roles
	MITRE Reference	T1595.001	T1593.003	T1588.002	T1059.004	T1072	T1098.006
	Tactical Phase	**7.Privilege Escalation**	**8.Collection**	**9.Impact**	**10.Impact**		
	Technique	Scheduled Task/Job	Data from Information Repositories	Endpoint Denial of Service	Service Stop		
	Sub-Technique	Container Orchestration Job	Code Repositories	Application or System Exploitation	-		
	MITRE Reference	T1053.007	T1213.003	T1499.004	T1489		

Annex 10 MITRE ATT&CK Threat Reference Fuzzing Core

List of Threat ID´s						
	Tactics					
	Reconnaissance	**Reconnaissance**	**Resource Development**	**Execution**	**Execution**	**Privilege Escalation**
	T1595	TA0043	TA0042	TA0002	TA0002	TA0004
	2-Oct-20	18-Oct-23	30-Sep-20	19-Jul-19	19-Jul-19	6-Jan-21
	13-Feb-24	13-Feb-24	13-Feb-24	13-Feb-24	13-Feb-24	13-Feb-24
	Privilege Escalation	**Collection**	**Impact**	**Impact**		
	TA0004	TA0009	TA0040	TA0040		
	6-Jan-21	19-Jul-19	25-Jul-19	25-Jul-19		
	13-Feb-24	13-Feb-24	13-Feb-24	13-Feb-24		
	Techniques					
	Active Scanning	**Search Open Websites/Domains**	**Obtain Capabilities**	**Command and Scripting Interpreter**	**Software Deployment Tools**	**Account Manipulation**
	T1595	T1593	T1588	T1059	T1072	T1098
	2-Oct-20	18-Oct-22	18-Oct-21	27-Mar-23	27-Sep-23	16-Oct-23
	13-Feb-24	13-Feb-24	13-Feb-24	13-Feb-24	13-Feb-24	13-Feb-24
	Scheduled Task/Job	**Data from Information Repositories**	**Endpoint Denial of Service**	**Service Stop**		
	T1053	T1213	T1499	T1489		
	20-Mar-23	11-Apr-22	30-Mar-23	28-Jul-22		
	13-Feb-24	13-Feb-24	13-Feb-24	13-Feb-24		
	Sub-Techniques					
	Reconnaissance	**Reconnaissance**	**Resource Development**	**Execution**	**Privilege Escalation**	**Privilege Escalation**
	T1595.001	T1593.003	T1588.002	T1059.004	T1098.006	ID: T1053.007
	2-Oct-20	26-Oct-21	17-Oct-21	26-Jul-21	16-Oct-23	15-Apr-23
	19-Feb-24	19-Feb-24	19-Feb-24	19-Feb-24	19-Feb-24	19-Feb-24
	Collection	**Impact**				
	ID: T1213.003	ID: T1499.004				
	18-Oct-22	25-Mar-22				
	19-Feb-24	19-Feb-24				

Annex 11 MITRE ATT&CK Reference Fuzzing RAN

MITRE ATT&CK REF.						
	Tactical Phase	**1.Reconnaissance**	**2.Resource Development**	**3.Resource Development**	**4.Execution**	**5.Initial Access**
	Technique	Gather Victim Host Information	Gathering Victim Host Information	Stage Capabilities	Exploitation for Client Execution	Protocol Tunneling
	Sub-Technique	Client Configurations	Configurability of Fake BS or Access	Configure Operator Core Network	Over-the-Air Input	UE Access via GTP-U
	MITRE Reference	T1592.004	FGT1583.501	FGT1608.502	FGT1203.501	FGT1572.501
	Annex	---	---	---	---	---
	Tactical Phase	**6.Defense Evasion**	**7.Collection**	**8. Impact**	**9. Impact**	
	Technique	Weaken Encryption	Collection	Vandalism of Network Infrastructure	Endpoint Denial of Service	
	Sub-Technique	Radio Interface	Radio Interface	Radio Access Hardware	Trigger fraud alert to deny of service	
	MITRE Reference	FGT1600	FGT1040.502	FGT5018.002	FGT1499.502	
	Annex	---	---	---	---	

TTP Id's starting with FGT is MITRE FiGHT Framework

Annex 12 MITRE ATT&CK Threat Reference Fuzzing RAN

List of Threat ID´s

Tactics						
Reconnaissance	Resource Development	Execution	Initial Access	Defense Evasion	Collection	Impact
TA0043	TA0042	TA0002	TA0001	FGT1600	TA0009	TA0040
18-Oct-20	30-Sep-21	19-Jul-19	19-Jul-19	-	19-Jul-19	25-Jul-19
12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24
-				-	-	-

Techniques			
Gather Victim Host Information	Stage Capabilities	Exploitation for Client Execution	Protocol Tunneling
T1592	FGT1608	FGT1203	FGT1572
17-Oct-21	-	-	-
12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24
Weaken Encryption	Network Sniffing	Vandalism of Network Infrastructure	Endpoint Denial of Service
FGT1600	FGT1040	FGT5018	FGT1499
-	-	-	-
12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24
-			

Sub-Techniques				
Client Configurations	Configurability of Fake Base Station or Access Point	Configure Operator Core Network	Over-the-Air Input	UE Access via GTP-U
T1592.004	FGT1608.501	FGT1608.502	FGT1203.501	FGT1572.501
17-Oct-21	-	-	-	-
12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24
Radio Interface	Radio interface	Radio Access Hardware	Trigger fraud alert to deny service	
FGT1600.501	FGT1040.501	FGT5018.002	FGT1499.502	
-	-	-	-	
12-Feb-24	12-Feb-24	12-Feb-24	12-Feb-24	

TTP Id’s starting with FGT is MITRE FiGHT Framework

Annex 13 MITRE ATT&CK Reference Data-Exfiltration Threat

MITRE ATT&CK REF.	Tactical Phase	1 Reconnaissance	1.2 Reconnaissance	2 Execution	3 Discovery	4 Exfiltration	5 Impact
	Technique	Gather Victim Host Information	Gathering Victim Host Information	Native API	Network Sniffing	Automated Exfiltration	Network Denial of Service
	Sub-Technique	Hardware	Software	-	-	Traffic Duplication	-
	MITRE Reference	T1592.001	T1592.002	T1106	T1040	T1020.001	T1464

Annex 14 MITRE ATT&CK Threat Reference Data-Exfiltration Threat

List of Threat ID´s					
	Tactics				
	Reconnaissance	**Execution**	**Discovery**	**Exfiltration**	**Impact**
	ID: TA0043	ID: TA0002	ID: TA0007	ID: TA0010	ID: TA0034
	18.Oct 20	19-Jul-19	19-Jul-19	19-Jul-19	20.Mar 23
	01.Dec 23	01.Dec 23	01.Dec 23	01.Dec 23	01.Dec 23
	Techniques				
	Gather Victim Host Information	**Native API**	**Network Sniffing**	**Automated Exfiltration**	**Network Denial of Service**
	ID: T1592	ID: T1106	ID: T1040	ID: T1020	ID: T1464
	17.Oct 21	13.Oct 23	10-Jul-23	19-Apr-22	20.Mar 23
	01.Dec 23	01.Dec 23	01.Dec 23	01.Dec 23	01.Dec 23
	Sub-Techniques				
	Hardware	**Software**	**Traffic Duplication**		
	ID: T1592.001	ID: T1592.002	ID: T1020.001		
	17.Oct.21	17.Oct.21	14-Apr-23		
	01.Dec 23	01.Dec 23	01.Dec 23		

Network Denial of Service: The technique id is part of MITRE ATT&CK Framework from Mobile domain.

Annex 15 MITRE D3FEND Reference: Hydra

MITRE ATT&CK Ref.	**Tactical Phase**	**1.Reconnaissance**	**2.Reconnaissance**	**3.Reconnaissance**	**4.Reconnaissance**	**5.Resource Development**	**6.Execution**	**7.Credential Access**	**8. Impact**	**9. Impact**
	Technique	Gather Victim Network Information	Gathering Victim Host Information	Active Scanning	Active Scanning	Obtain Capabilities	Command and Scripting Interpreter	Brute Force	Service Stop	Access 5G Operator Key
	Sub-Technique	Network Topology	Client Configuration;	Scanning IP Blocks	Vulnerability Scanning	Tool	Unix Shell	Password Spraying	Service Stop	Access 5G Operator Key
MITRE D3FEND Ref.	**MITRE D3FEND Tactics-Technique-Subtechnique**	HARDEN - Credential Hardening D3-PH - Strong Password Policy D3-SPP			ON ATTACKER MACHINE			HARDEN - Credential Hardening D3-CH- Multi Factor Authentication D3-MFA		
	MITRE D3FEND Tactics-Technique-Subtechnique	HARDEN - Credential Hardening D3-CH- Multi Factor Authentication D3-MFA						EVICT- Credential Eviction D3-CE - Account Locking D3-AL		
	MITRE D3FEND Tactics-Technique-Subtechnique	HARDEN - Platform Hardening D3-PH- Regular Patch and Software Updates D3-SU						EVICT - Credential Eviction D3-CE - Authentication Cache Invalidation D3-ANCI		

Annex 16 MITRE D3FEND Reference: Metasploit

Tactical Phase	1. Resource Development	2. Resource Development	3. Resource Development	4. Reconnaissance	5. Initial Access	6. Initial Access	7. Execution	8. Credential Access	9. Command and Control	10. Exfiltration	11. Impact	12. Impact
Technique	Acquire Infrastructure	Compromise Infrastructure	Obtain Capabilities	Active Scanning	Exploit Public-Facing Application	Valid Accounts	Exploitation for Client Execution	Exploitation for Credential Access	Content Injection	Exfiltration Over Web Service	Resource Hijacking	System Shutdown/Reboot
Sub-Technique	Web Services	Web Services	Vulnerabilities	Vulnerability Scanning	-	Local Accounts	-	-	-	Exfiltration Over Webhook	-	-
MITRE D3FEND Tactics-Technique-Subtechnique	HARDEN - Credential Hardening D3-CH- Multi Factor Authentication D3-MFA				ON ATTACKER MACHINE			HARDEN - Platform Hardening D3-PH- Regular Patch and Software Updates D3-SU		ON ATTACKER MACHINE	RESTORE - Restore Access D3-RA - Restore Network Access D3-RNA	
MITRE D3FEND Tactics-Technique-Subtechnique	HARDEN - Platform Hardening D3-PH- Regular Patch and Software Updates D3-SU							EVICT - Process Eviction D3-PE- Process Suspension D3-PS			DETECT - Network Traffic Analysis D3-NA - Remote Terminal Session Detection D3-RTSD	
MITRE D3FEND Tactics-Technique-Subtechnique	DETECT - Network Traffic Analysis D3-NA - Remote Terminal Session Detection D3-RTSD										ISOLATE -Network Traffic Isolation D3-NI - Network Traffic Filtering D3-NTF	
MITRE D3FEND Tactics-Technique-Subtechnique	ISOLATE -Network Isolation D3-NI – Encrypted Tunnels D3-ET											
MITRE D3FEND Tactics-Technique-	ISOLATE -Network Traffic Isolation D3-NI - Network Traffic Filtering D3-NTF											

Subtechnique					
MITRE D3FEND Tactics-Technique-Subtechnique	HARDEN - Platform Hardening D3-PH - Local File Permissions D3-LFP				
MITRE D3FEND Tactics-Technique-Subtechnique	DETECT - Identifier Analysis D3-ID - IP Reputation Analysis D3-IPRA				

Tactical Phase	**1. Reconnaissance**	**2. Reconnaissance**	**3. Resource Development**	**4. Resource Development**	**5. Initial Access**	**6. Execution**	**7. Execution**	**8. Privilege Escalation**	**9. Credential Access**	**10. Lateral Movement**	**11.Impact**
Technique	Active Scanning	Gather Victim Network Information	Compromise Infrastructure	Obtain Capabilities	Trusted Relationship	Command and Scripting Interpreter	Scheduled Task/Job	Create or Modify System Process	Forced Authentication	Lateral Tool Transfer	Data Manipulation
Sub-Technique	Vulnerability Scanning	IP Addresses	Server	Tool	´---	Unix Shell	Cron	Launch Daemon	´---	´---	Stored Data Manipulation

MITRE D3FEND Tactics-Technique-Subtechnique	ISOLATE- Network Isolation D3-NI - Inbound Traffic Filtering D3-ITF	ON ATTACKER MACHINE	DETECT - Network Traffic Analysis D3-NA - Remote Terminal Session Detection D3-RTSD

MITRE D3FEND Tactics-Technique-Subtechnique	ISOLATE - Network Isolation D3-NI - Encrypted Tunnels D3-ET		DETECT- User Behavior Analysis D3-UBA - User Geolocation Logon Pattern Analysis D3-UGLPA
MITRE D3FEND Tactics-Technique-Subtechnique			RESTORE - Restore Access D3- RA - Reissue Credential D3-RC
MITRE D3FEND Tactics-Technique-Subtechnique			DECEIVE - Decoy Object D3-DO - Decoy user credential D3-DUC

Annex 17 MITRE D3FEND Reference: VSFTPD

MITRE ATT&CK Ref.											
Tactical Phase	**1. Reconnaissance**	**2. Reconnaissance**	**3. Resource Development**	**4. Resource Development**	**5. Initial Access**	**6. Execution**	**7. Execution**	**8. Privilege Escalation**	**9. Credential Access**	**10. Lateral Movement**	**11.Impact**
Technique	Active Scanning	Gather Victim Network Information	Compromise Infrastructure	Obtain Capabilities	Trusted Relationship	Command and Scripting Interpreter	Scheduled Task/Job	Create or Modify System Process	Forced Authentication	Lateral Tool Transfer	Data Manipulation
Sub-Technique	Vulnerability Scanning	IP Addresses	Server	Tool	´---	Unix Shell	Cron	Launch Daemon	´---	´---	Stored Data Manipulation

MITRE D3FEND Ref.				
MITRE D3FEND Tactics-Technique-Subtechnique	ISOLATE- Network Isolation D3-NI - Inbound Traffic Filtering D3-ITF	ON ATTACKER MACHINE	DETECT - Network Traffic Analysis D3-NA - Remote Terminal Session Detection D3-RTSD
MITRE D3FEND Tactics-Technique-Subtechnique	ISOLATE - Network Isolation D3-NI - Encrypted Tunnels D3-ET		DETECT- User Behavior Analysis D3-UBA - User Geolocation Logon Pattern Analysis D3-UGLPA
MITRE D3FEND Tactics-Technique-Subtechnique			RESTORE - Restore Access D3- RA - Reissue Credential D3-RC
MITRE D3FEND Tactics-Technique-Subtechnique			DECEIVE - Decoy Object D3-DO - Decoy user credential D3-DUC

Annex 18 MITRE D3FEND Reference: Jamming

MITRE ATT&CK Ref.							
	Tactical Phase	**1 Reconnaissance**	**1.2 Reconnaissance**	**2 Execution**	**3 Discovery**	**4 Exfiltration**	**5 Impact**
	Technique	Gather Victim Host Information	Gathering Victim Host Information	Native API	Network Sniffing	Automated Exfiltration	Network Denial of Service
	Sub-Technique	Hardware	Software	-	-	Traffic Duplication	-

MITRE D3FEND Ref.			
	MITRE D3FEND Tactics-Technique- Subtechnique	ON ATTACKER MACHINE	DETECT - Network Traffic Analysis D3-NTA - Network Community Deviation D3-NTCD
	MITRE D3FEND Tactics-Technique- Subtechnique		DETECT - Network Traffic Analysis D3-NTA - Connection Attempt Analysis D3-CAA
	MITRE D3FEND Tactics-Technique- Subtechnique		ISOLATE -Network Traffic Isolation D3-NI - Network Traffic Filtering D3-NTF
	MITRE D3FEND Tactics-Technique- Subtechnique		RESTORE - Restore Access D3-RA - Restore Access D3-RA

Annex 19 MITRE D3FEND Reference: Data-Exfiltration

MITRE ATT&CK Ref.	Tactical Phase	1.Resource Development	2. Execution	3.Privilege Escalation	4 Collection	5.Exfiltiration	6. Impact
	Technique	Stage Capabilities	Command and Scripting Interpreter	Abuse Elevation Control Mechanism	Archive Collected Data	Exfiltration Over Other Network Medium	Data Extraction
	Sub-Technique	Upload Tool	Python	Sudo and Sudo Caching	Archive via Custom Method	---	…
MITRE D3FEND Ref.	MITRE D3FEND Tactics-Technique- Subtechnique	ISOLATE -Network Traffic Isolation D3-NI - Network Traffic Filtering D3-NTF					
	MITRE D3FEND Tactics-Technique- Subtechnique	DETECT -Network Traffic Analysis D3-NTA - Protocol Metadata Anomaly Detection D3-PMAD					
	MITRE D3FEND Tactics-Technique- Subtechnique	DETECT - Platform Monitoring D3-PM					

Annex 20 MITRE D3FEND Reference: Fuzzing Core

MITRE ATT&CK Ref.	Tactical Phase	Reconnaissance	Reconnaissance	Resource Development	Execution	Execution	Privilege Escalation	Collection	Impact	Impact	Privilege Escalation	Collection	Impact	Impact
	Technique	Active Scanning	Search Open Websites/Domains	Obtain Capabilities	Command and Scripting Interpreter	Software Deployment Tools	Account Manipulation	Data from Information Repositories	Endpoint Denial of Service	Service Stop	Scheduled Task/Job	Data from Information Repositories	Endpoint Denial of Service	Service Stop
	Sub-Technique	Scanning IP Blocks	Code Repositories	Tool	Unix Shell	-	Additional Container Cluster Roles	Code Repositories	Application or System Exploitation	-	Container Orchestration Job	Code Repositories	Application or System Exploitation	-

MITRE D3FEND Ref.				
	MITRE D3FEND Tactics-Technique-Subtechnique	ON ATTACKER MACHINE	ISOLATE- Network Isolation D3-NI - Inbound Traffic Filtering D3-ITF	ON ATTACKER MACHINE
	MITRE D3FEND Tactics-Technique-Subtechnique		ISOLATE - Network Isolation D3-NI - Encrypted Tunnels D3-ET	
	MITRE D3FEND Tactics-Technique-Subtechnique		HARDEN - Platform Hardening D3-PH - File Encryption D3-FE	
	MITRE D3FEND Tactics-Technique-Subtechnique		EVICT - File Eviction D3-FE- File Removal D3-FR	

	MITRE D3FEND Tactics-Technique-Subtechnique		RESTORE - Restore Access D3-RA - Restore Network Access D3-RNA	

Annex 21 MITRE D3FEND Reference: Fuzzing RAN

MITRE ATT&CK Ref.	**Tactical Phase**	**Reconnaissance**	**Resource Development**	**Resource Development**	**Execution**	**Initial Access**	**Defense Evasion**	**Collection**	**IMPACT**	**IMPACT**
	Technique	Gather Victim Host Information	Stage Capabilities	Stage Capabilities	Exploitation for Client Execution	Protocol Tunneling	Weaken Encryption	Network Sniffing	Vandalism of Network Infrastructure	Endpoint Denial of Service
	Sub-Technique	Client Configurations	Configurability of Fake Base Station or Access Point	Configure Operator Core Network	Over-the-Air Input	UE Access via GTP-U	Radio Interface	Radio interface	Radio Access Hardware	Trigger fraud alert to deny service
MITRE D3FEND Ref.	**MITRE D3FEND Tactics-Technique- Subtechnique**	ISOLATE- Network Isolation D3-NI - Inbound Traffic Filtering D3-ITF	ON ATTACKER MACHINE		DETECT - Platform Monitoring D3-PM					
	MITRE D3FEND Tactics-Technique- Subtechnique	DETECT - Identifier Analysis D3-ID			DETECT - File Analysis D3- FA					
	MITRE D3FEND Tactics-Technique- Subtechnique	ISOLATE- Network Isolation D3-NI - Inbound Traffic Filtering D3-ITF			ISOLATE- Network Isolation D3-NI - Network Traffic Filtering D3-NTF					
	MITRE D3FEND Tactics-Technique- Subtechnique	DECEIVE - Decoy Object D3-DO - Decoy File D3-DF			DETECT - Network Traffic Analysis D3-NTA - Connection Attempt Analysis D3-CAA					
	MITRE D3FEND Tactics-Technique- Subtechnique				RESTORE - Restore Access D3-RA - Restore Software D3-RS					

Annex 22 gNB Security Requirements

Item	Title	3GPP Security requirements	3GPP specifications and NESAS
gNB-Security Hardening Requirements			
#1	No unnecessary or insecure services / protocols	The network product shall only run protocol handlers and services which are needed for its operation, and which do not have any known security vulnerabilities.	TS 33.117 §4.3.2.1
#2	Restricted reachability of services	The network product shall restrict the reachability of services so that they can only be reached on interfaces where their usage is required. On interfaces where services are active, the reachability should be limited to legitimate communication peers.	TS 33.117 §4.3.2.2
#3	No unused software	Unused software components or parts of software which are not needed for operation or functionality of the network product shall not be installed or shall be deleted after installation.	TS 33.117 §4.3.2.3
#4	No unused functions	During installation of software and hardware often functions will be activated that are not required for operation or function of the system. Also, hardware functions which are not required for operation or function of the system (e.g., unused interfaces) shall be permanently deactivated. Permanently means that they shall not be reactivated again after network product reboot.	TS 33.117 §4.3.2.4
#5	No unsupported components	The network product shall not contain software and hardware components that are no longer supported by their vendor, producer, or developer, such as components that have reached end-of-life or end-of-support. Excluded are components that have a special support contract. This contract shall guarantee the correction of vulnerabilities over components' lifetime.	TS 33.117 §4.3.2.5
#6	Remote login restrictions for privileged users	Direct login as root or equivalent highest privileged user shall be limited to the system console only. Root user will not be allowed to login to the system remotely.	TS 33.117 §4.3.2.6
#7	Filesystem Authorization privileges	The system shall be designed to ensure that only users that are authorized to modify files, data, directories, or file systems have the necessary privileges to do so.	TS 33.117 §4.3.2.7

Annex 23 Web Servers Security Requirements

Item	Title	3GPP Security requirements	3GPP specifications and NESAS
Web Servers			
#1	No system privileges for web server	No web server processes shall run with system privileges. This is best achieved if the web server runs under an account that has minimum privileges. If a process is started by a user with system privileges, execution shall be transferred to a different user without system privileges after the start.	TS 33.117 §4.3.4.2
#2	Unused HTTP methods shall be deactivated	HTTP methods that are not required shall be deactivated. Standard requests to web servers only use GET, HEAD, and POST. If other methods are required, they shall not introduce security leaks such as TRACK or TRACE.	TS 33.117 §4.3.4.3
#3	Any add-ons and components that are not required shall be deactivated	All optional add-ons and components of the web server shall be deactivated if they are not required. In particular, CGI or other scripting components, Server Side Includes (SSI), and WebDAV shall be deactivated if they are not required.	TS 33.117 §4.3.4.4
#4	No compiler, interpreter, or shell via CGI or other server-side scripting	If CGI (Common Gateway Interface) or other scripting technology is used, the CGI directory - or other corresponding scripting directory - shall not include compilers or interpreters (e.g., PERL interpreter, PHP interpreter/compiler, Tcl interpreter/compiler or operating system shells).	TS 33.117 §4.3.4.5
#5	Access rights for web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges	Access rights for web server configuration files shall only be granted to the owner of the web server process or to a user with system privileges. Implementation example: Delete "read" and "write" access rights for "others." Only grant "write" access to the user who configures the web server.	TS 33.117 §4.3.4.8
#6	Information about the web server in HTTP headers shall be minimized	The HTTP header shall not include information on the version of the web server and the modules/add-ons used.	TS 33.117 §4.3.4.11
#7	File type- or script-mappings that are not required shall be deleted	File type- or script-mappings that are not required shall be deleted, e.g., php, phtml, js, sh, csh, bin, exe, pl, vbe, vbs.	TS 33.117 §4.3.4.13

Annex 24 Network Devices Security Requirements

Item	Title	3GPP Security requirements	3GPP specifications and NESAS
Network Devices			
#86	Traffic Separation	The network product shall support physical or logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 for further information.	TS 33.117 §4.3.5.1

Annex 25 Operating Systems Security Requirements

Item	Title	3GPP Security requirements	3GPP specifications and NESAS
Operating Systems			
#1	IP-Source address spoofing mitigation	Systems shall not process IP packets if their source address is not reachable via the incoming interface. Implementation example: Use of "Reverse Path Filter" (RPF) provides this function.	TS 33.117 §4.3.3.1.1
#2	Minimized kernel network functions	Kernel based network functions not needed for the operation of the network element shall be deactivated. In particular the following ones shall be disabled by default: - IP Packet Forwarding between different interfaces of the network product.	TS 33.117 §4.3.3.1.2
#3	No automatic launch of removable media	The network product shall not automatically launch any application when removable media device such as CD-, DVD-, USB-Sticks or USB-Storage drive is connected. If the operating system supports an automatic launch, it shall be deactivated unless it is required to support availability requirements.	TS 33.117 §4.3.3.1.3
#4	Syn Flood Prevention	The network product shall support a mechanism to prevent Syn Flood attacks (e.g., implement the TCP Syn Cookie technique in the TCP stack by setting net.ipv4.tcp_syncookies = 1 in the linux sysctl.conf file). This feature shall be enabled by default.	TS 33.117 §4.3.3.1.4
#5	Protection mechanisms against buffer overflows	The system shall support mechanisms for buffer overflow protection. Documentation which describes these buffer overflow mechanisms and also how to check that they have been enabled and/or implemented shall be provided.	TS 33.117 §4.3.3.1.5

Annex 26 Virtualization Security Requirements

Item	Title	3GPP Security requirements	3GPP specifications and NESAS
		Virtualization	
#1	VNF package and VNF image integrity	1) VNF package and image shall contain integrity validation value (e.g. MAC). 2) VNF package shall be integrity protected during onboarding and its integrity shall be validated by the NFVO.	TR 33.818 §5.2.5.5.3.3.5.1 TR 33.848 §5.18.3
#2	VNP lifecycle management security	1) VNF shall authenticate VNFM when VNFM initiates a communication to VNF. 2) VNF shall be able to establish securely protected connection with the VNFM. 3) VNF shall check whether VNFM has been authorized when VNFM access VNF's API. 4) VNF shall log VNFM's management operations for auditing.	TR 33.818 §5.2.5.5.7.1
#3	Secure executive environment provision	The VNF shall support to compare the owned resource state with the parsed resource state from VNFD (VNF Description) by the VNFM. The VNF can query the parsed resource state by the VNFM from the OAM. The VNF shall send an alarm to the OAM if the two resource states are inconsistent. This comparing process can be triggered periodically by the VNF, or the administrator can manually trigger the VNF to perform the comparing process.	TR 33.818 §5.2.5.5.7.2
#4	Traffic Separation	The virtualized network product shall support logical separation of traffic belonging to different network domains. For example, O&M traffic and control plane traffic belong to different network domains. See RFC 3871 for further information.	TR 33.818 §5.2.5.5.8.5.1
#5	Instantiating VNF from trusted VNF image	A VNF shall be initiated from a trusted VNF image which includes one or more than one images. The VNF image shall be signed by an authorized party. The authorized party is trusted by the operators.	TR 33.818 §5.2.5.6.6.1
#6	Secure virtualization resource management	To prevent a compromised VIM from changing the assigned virtualized resource, the VNF shall alert to the OAM. For example, when an instantiated VNF is running, a compromised VIM can delete a VM which is running VNFCI, the VNF shall alert to the OAM when the VNF cannot detect a VNFC message. A VNF shall log the access from the VIM. NOTE: The VIM manages the virtualization resource assignment and synchronization of virtualized resource state information. In the implementation, the VIM and the virtualization layer are coupled and provided by one vendor, they trust each other. Whether the VIM is trust or not is based on operator's decision.	TR 33.818 §5.2.5.6.7.1
#7	Secure hardware resource management	The VIM manages the hardware resource configuration and state information exchange. When the VIM is compromised to change the hardware resource configuration, an alert shall be triggered by the hardware. The administrator can check the alert and find the attack at latter.	TR 33.818 §5.2.5.7.7.1

#8	Trusted platform	The host system shall implement a Hardware-Based Root of Trust (HBRT) ((e.g., TPM, HSM)) as Initial Root of Trust **[1]**. The trust state of the platform shall be measured, and a trusted chain shall be built **[2]**.	TR 33.818 §5.2.5.7.7.3

Annex 27 Non-RT RIC Security Requirements

Item	Assets	Threats	Vulnerability	C-I-A-A	Impact	To-Do-List	Threat ID
Non-RT RIC							
#1	Non-RT RIC	An attacker may penetrate the non-RT RIC to cause a denial of service or degrade the performance.	Improper or missing authentication and authorization processes on the non-RT RIC.	A	LOW	Support authorization as a resource owner/server and client on the non-RT RIC.	I-OP-NONRTRIC-01
#2	Non-RT RIC	An attacker may bypass authentication and authorization	rApps may be misconfigured or compromised.	C-A-A	Medium	Ensure the Non-RT RIC Framework provides authorization to requests from rApps as a client.	I-OP-NONRTRIC-02
#3	Non-RT RIC	An attacker may bypass authentication and authorization using an injection attack.	rApps may be misconfigured or compromised. Failing or misconfigured authentication and authorization.	C-A-A	Medium	Ensure rApps provide client authorization requests to the Non-RT RIC Framework	I-OP-NONRTRIC-03
#4	Non-RT RIC	Conflicting rApps may maliciously impact performance or trigger a Denial of Service (DoS).	rApps from untrusted or unmaintained sources. rApps may be vulnerable to misbehavior or malicious intent.	C-I-A	High	Ensure rApps can recover without catastrophic failure from volumetric DDoS attacks across the R1 interface due to misbehavior or malicious intent.	I-OP-NONRTRIC-05

Annex 28 Near-RT RIC Security Requirements

Item	Assets	Threats	Vulnerability	C-I-A-A	Impact	To-Do-List	Threat ID
Near-RT RIC							
#1	Near-RT RIC	Attackers may exploit non-authenticated, weakly authenticated, or incorrectly authenticated Near-RT RIC APIs.	on-authenticated, weakly authenticated, or incorrectly authenticated Near-RT RIC APIs	C-A	Low	Ensure the Near-RT RIC authenticates xApp access to the Near-RT RIC database(s) during the Security Development Lifecycle (SDL) registration process.	I-OP-NEARRTRIC-01
#2	Near-RT RIC	An attacker exploits xApps vulnerabilities and misconfiguration.	xApp stems from an untrusted or unmaintained source.	C-I-A	High	xApp images shall be authenticated & validated during onboarding using a signature that is generated by the xApp Solution Provider and validated by the Service Provider.	I-OP-NEARRTRIC-02
#3	Near-RT RIC	Attackers exploit xApp vulnerabilities and misconfiguration	xApps from untrusted or unmaintained sources	C-A	Medium	Verify xApp images during onboarding using a signature validated by the Service Provider	I-OP-NEARRTRIC-03
#4	Near-RT RIC	Attackers exploit non-authorized Near-RT RIC APIs to access resources and services they're not entitled to use	Non-authorized Near-RT RIC APIs	C-A	Medium	Ensure the Near-RT RIC provides authorized access to Near-RT RIC database(s).	I-OP-NEARRTRIC-04
#5	Near-RT RIC	Attackers exploit non-authorized Near-RT RIC APIs to access resources and services they're not entitled to use.	Non-authorized RT RIC APIs	C-A	Medium	Implement authorization mechanisms in the Near-RT RIC Framework, supporting authorization as a resource owner/server (A1-P) and client (A1-EI)	I-OP-NEARRTRIC-05

#6	Near-RT RIC	Attackers exploit non authorized Near-RT RIC APIs to access to resources.	Non-authorized RT RIC APIs	C-A	Low	Ensure the Near-RT RIC can recover without catastrophic failure from a volumetric DDoS attack across the A1 interface.	I-OP-NEARRTRIC-06

Annex 29 MANO-SMO Security Requirements

Item	Assets	Threats	Vulnerability	C-I-A-A	Impact	To-Do-List	Threat ID
Service and Management Orchestration							
#1	SMO	Malicious actor views local logs	Missing or weak confidentiality protection of data at rest.	C	Low	Ensure SMO provides confidentiality protection for event logs over protected protocols to remote server.	I-OP-SMO-01
#2	SMO	External attacker exploits authorization weakness on SMO.	Missing or improperly configured authorization.	C-I-A	High	Ensure SMO can report to authorized external services.	I-OP-SMO-02
#3	SMO	External attacker exploits external interface to modify data in transit between SMO and external service	Missing integrity checking for data in transit.	C-I	Medium	Ensure SMO can record all security-related log events.	I-OP-SMO-03

#4	SMO	External attacker exploits missing or improperly configured authentication.	Missing or improperly configured authentication.	C-I	Medium	Ensure SMO does not permit configuration change to logging level(s) of any component on the SMO system without proper authorization	I-OP-SMO-04
#5	SMO	Malicious actor views security logs of SMO	Security logs of SMO should be separate from other system logs.	C	Low	Ensure SMO has separate security logs	I-OP-SMO-05

Annex 30 CU-DU-RU Security Requirements

Item	Assets	Threats	Vulnerability	C-I-A-A	Impact	To-Do-List	Threat ID
CU-DU-RU							
#1	CU-DU-RU	An attacker exploits insecure designs or lack of adoption	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	C-I-A	High	Must be updated	I-OP-CUDURU-01
#2	CU-DU-RU	An attacker stands up a false base station attack by attacking an O-RU.	False O-RU	C-I-A	High	Must be updated	I-OP-CUDURU-02
#3	CU-DU-RU	Developers use SW components with known vulnerabilities and untrusted libraries that can be exploited by an attacker through a backdoor attack	Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	C-I-A-A	High	Ensure digital signature must be provided.	I-OP-CUDURU-03

#4	CU-DU-RU	Attacks from the internet exploit weak authentication and access control.	Errors in the design and implementation of the network protocols (HTTP, P, TCP, UDP, application protocols).	C-I-A-A	High	Ensure transport protocols (IP, UDP, TCP, SCTP, SSH, HTTP, and HTTP2) must be able to withstand unexpected inputs that deviate from protocol specifications, including random protocol header and payload mutations, as well as targeted state-aware testing."	I-OP-CUDURU-04
#5	CU-DU-RU	Attacks from the internet exploit weak authentication and access control through a backdoor attack.	Errors in the design and implementation of the network protocols (HTTP, TCP, UDP) Lack of coding best practices. Modules with known vulnerabilities and untrusted libraries.	C-I-A-A	High	CU-DU-RU component vendors must implement robust password security measures to prevent brute-force attacks, unauthorized resets, man-in-the-middle attacks, and dictionary attacks.	I-OP-CUDURU-06

Annex 31 A1 Security Requirements

Item	Assets	Threats	Vulnerability	C-I-A-A	Impact	To-Do-List	Threat ID
A1							
#1	A1	Untrusted peering between Non-RT- RIC and Near-RT- RIC.	weak mutual authentication.	C-I-A	High	A1 interface shall support confidentiality, integrity, replay protection.	I-OP-A1-02
#2	A1	Untrusted peering between Non-RT- RIC and Near-RT- RIC.	weak mutual authentication.	C-I-A	High	A1 interface shall support mutual authentication and authorization.	I-OP-A1-01

+

Annex 32 E2 Security Requirements

Item	Assets	Threats	Vulnerability	C-I-A-A	Impact	To-Do-List	Threat ID
E2							
#1	E2	An attacker penetrates and compromises the system through the open fronthaul, O1, O2, A1, and E2.	Improper or missing authentication and authorization. Improper or missing ciphering and integrity checks. Improper or missing replay protection of sensitive data exchanged over E2 interfaces. Improper prevention of key reuse.	C-I-A	High	Ensure E2 interface shall support confidentiality, integrity, replay protection and data origin authentication.	I-OP-E2-01

Annex 33 O1 Security Requirements

Item	Assets	Threats	Vulnerability	C-I-A-A	Impact	To-Do-List	Threat ID
O1							
#1	O1	An attacker penetrates and compromises the O-RAN system through the open Fronthaul, O1, O2, A1, and E2	Improper or missing authentication and authorization. Improper or missing ciphering and integrity checks of sensitive data exchanged. Improper prevention of key reuse.	C-I-A	High	Confidentiality, Integrity and Authenticity Management Service providers and consumers that use TLS SHALL support TLS as specified.	I-OP-O1-01
#2	O1	An attacker exploits improper mechanisms for authentication and authorization to compromise O1 component	Unauthenticated access to O-RAN functions. Improper authentication mechanisms. Use of Predefined/ default accounts. Weak or missing password policy. Lack of mutual authentication. Failure to block consecutive failed login attempts. Improper authorization and access control policy.	C-I-A	High	The NETCONF implementation for O1 SHALL set the default values of the NACM Global Enforcement Controls as follows. • enable-nacm = true • read-default = permit • write-default = deny • exec-default = deny • enable-external-groups = true	I-OP-O1-02
#3	O1	An attacker exploits insecure designs or lack of adoption in O-RAN components	Outdated component from the lack of update or patch management. Poorly design architecture. Missing appropriate security hardening. Unnecessary or insecure function/protocol/component.	C-I-A	High	Users assigned to the O1_software_management group SHALL have permissions to install new software.	I-OP-O1-03

Annex 34 O2 Security Requirements

Item	Assets	Threats	Vulnerability	C-I-A-A	Impact	To-Do-List	Threat ID
O2							
#1	O2	MitM attacks on O2 interface between O-Cloud and SMO	Insecure O2 interface, lack authentication.	C-I-A	High	O2 interface shall support confidentiality, integrity, replay protection and data origin authentication.	I-OP-O2-01