Threat Modelling with Cybersecurity Impact in 5G Core Networks and OPEN RAN

Sharique Ahmad*, Maik Holzhey*, Elif Tasdemir†, Mehmet Akif Kurt†, Frank H.P. Fitzek†‡
*IABG, Einsteinstraße 20, 85521 Ottobrunn, Germany
†Deutsche Telekom Chair of Communication Networks, Technische Universität Dresden, 01062, Germany
‡ Centre for Tactile Internet with Human-in-the-Loop (CeTI)
Ahmad@iabg.de, Holzhey@iabg.de, elif.tasdemir@tu-dresden.de, mehmet_akif.kurt@tu-dresden.de, frank.fitzek@tu-dresden.de

***Abstract*—Open interfaces in 5G Radio Access Network architecture allow flexibility, multi-vendor options and agile development. Open RAN architecture uses open source software (OSS) and proprietary products. The OSS allows many developers to be involved in the Open RAN technology, and offers testing capability for interoperability and security assessment. Using the advantage of openness of the software, developers can test code flaws, and overlooked vulnerabilities in the software. In order strength the security of the open source software, particularly OpenAirInterface (OAI) , we have modelled six possible threats for 5G Core and RAN network. These threats were implemented on dedicated test-beds. Risk and impact of these threats have been explained to provide valuable insight in preventing these threats from being executed. In summary, our evaluations and findings will increase technical capabilities of a resilient 5G system include a combination of reliability, availability, robustness and security, whilst protecting overall privacy.**

***Index Terms*—Open RAN, open source, security assessment, OpenAirInterface, interfaces**

I. Introduction

Open Radio Access Network (RAN) architecture enables to split monolithic RAN into different components based on the various split options. The interfaces between RAN components and core network are standardized so that mixing the components from the different vendors becomes possible. In Addition to these also new innovations is developed , e.g, Radio Intelligent Controller (RIC) to manage RAN resources, slicing the network to divide physical network into multiple virtual networks. Further it achieves the decoupling of software from hardware and enables the usage of general purpose hardware.

Although Open RAN allows flexibility, it offers vendors to develop and specialize in separate network components. This provides advancement in network softwarization, however this also brings new security and privacy challenges. The security challenges have been classified into six categories [1]: Misconfiguration in SMO and RIC, missing ciphering of data through open interfaces, decision conflict about low layer split options, trust issues towards multi-vendor support, disaggregation of hardware and software impeding security measures, and the implementation of the open source software.

In this paper, we consider security issues relevant to the implementation of open source software. As summarized in [2], the open source software related to Open RAN risks potentially uses software which is untrusted or vulnerable including backdoors, lack of standards for trusted available codes. Since it is expected to have open source code in Open RAN system, it is very critical to assess vulnerabilities in open source software.

Most of the work done to assess security of open source software for Open RAN is reviewing the possible scenarios as presented in the next section. Different than these, in this work we present threat modelling for well known threats e.g., brute-forcing, backdoor, unauthorized links for data transfer, interference on RF signals and fuzzing to assess vulnerabilities in network functions. Furhermore, we implement these steps in dedicated security test-beds and evaluate the impact to assess robustness of the open source software and suggest resiliency measures.

II. Related Work

The projects and alliances have embraced the open source software and frameworks as well as hardware and testbeds in which these software runs for Open RAN architecture, recently reviewed in [3]. The stakeholders for security regarding Open RAN deployment, corresponding threat surface and related countermeasures in O-RAN Alliance are discussed in [4]. Authors in [2] provide a threat overview in Open RAN and classify the threats in four categories: Process, people, technology and global threats. They classify open-source related risk in a people related category and risk related on virtual/cloud network functions in the global category. The authors also discuss possible security solutions and present an overview of general mistakes, consequences and mitigation. However this paper is a survey and there is no practical implementation. Moreover, provided solutions are very genear and just give an overview insight. Another comprehensive security evaluation,

This work was supported by the French-German project 5G-OPERA which is funded by the German Federal Ministry of Economic Affairs and Climate Action (BMWK), grant 01MJ22008A, and the German Research Foundation (DFG, Deutsche Forschungsgemeinschaft) as part of Germany's Excellence Strategy—EXC 2050/1—Cluster of Excellence "Centre for Tactile Internet with Human-in-the-Loop" (CeTI) of Technische Universität Dresden under Project ID 390696704 and by IABG mBH, Munich Germany for contribution and work related approaches on Security testing to reduce risk of 5G Open RAN private networks.

risk analysis, threat analysis and future direction to improve security of Open RAN architecture is presented in [5]. The authors group risk areas in five categories such as cellular infrastructure, architectural openness, cloud/virtualization, machine learning and 5G architecture threats. A comprehensive security evaluation is proposed in a future work item.

Despite Open RAN introducing new vulnerable surfaces, at the same time, it also gives opportunity to strengthen the security aspect of Open RAN as emphasized here [6]. Some dedicated security assessment is done for open fronthaul interface which has a standard protocol between radio unit and distributed unit. The results are given by [7]. Another detailed security analysis of the fronthaul is conducted in [8]. The authors present a detailed security analysis and describe the threats and vulnerabilities seen in fronthaul. They study the applicability, benefit and limitations of Media Access Control Security (MACsec) which is a security protocol for fronthaul. Further they asssess the feasibility of the proposed MACsec hardware architecture on Field Programmable Gate Array (FPGA) devices. In Addition to this, the authors in [9] develop a programmable control plane xApp for RIC to detect Layer-3 vulnerability in the Open RAN. Although there are few practical works done to test robustness of Open RAN components for fronthaul and higer layer of RAN, there is no practical assessment/evaluation done for surfaces/interfaces between core network and RAN using open source software.

Hence, we present the possible threat models with cybersecurity impact for the surface between 5G Core and RAN network for the Open RAN community to make open source software more resilient against cybersecurity threats.

A. Background

This section gives a brief definition of the functionality of the tools and threat model used to test vulnerability in the OpenRAN, Open-Source 5G system testbed and further we evaluate the risk level of threats based on Open Worldwide Application Security Project (OWASP) used for the Risk-Rating methodology.

B. Definition of Tools Used for Testing the Threat Models

Hydra is a form of password guessing or password cracking tool. Different username and password pairs are given repeatedly until the correct credentials are found. This is also referenced as password spraying. Similarly, *Metasploit* threat is used for brute-forcing with an additional backdoor being present. *Very Secure File Transfer Protocol Daemon (VSFTPD)* leads to unauthorized access to sensitive data or the execution of malevolent commands and it encompasses the exploitation of vulnerabilities inherent within the VSFTPD software, a prevalent FTP server employed for file transfers within networked environments. *Data Exfiltration* has similar aim as VSFTPD, i.e., unauthorized extraction, transfer, or theft of sensitive or confidential data with various methods beyond FTP servers. In a different way, *Jamming* works by interfering the transmission signal with a device emitting radio frequency signals in the same frequency band as the target network.

TABLE I
RANKING TABLE

Threat	**Likelihood**						**Impact**
	Thread Agent Factors		Vulnerability Factors				Technical Impact
	Skill Level	Opportunity	Ease of Discovery	Ease of Exploit	Awareness	Average	Loss of CIAA
Hydra	3	1	1	3	9	3.4	5
Metasploit	3	1	2	3	9	3.6	5
VSFTP	6	1	2	3	9	4.2	5
Data Exfiltration	6	1	2	3	9	4.2	3
Jamming	3	0	0	3	5	2.2	8
Fuzzing	8	4	5	3	9	5.8	8

Fuzzing is a software testing technique to detect security flaws in software applications, such as bugs, or vulnerabilities of the program.

C. Risk evaluation procedure of the threats

After explaining risk evaluation of the threats introduced above, we derive a ranking in Table I from OWASP Risk-Rating methodology [10] to estimate the likelihood of the risks and the impacts of successful adversary. Likelihood consists of Threat Agent Factors and Vulnerability Factors. Threat Agent Factors are formed from these criteria: *Skill Level* assessing the technical proficiency of a potential threat, *Motivation* showing the motivation level of intruder *Opportunity* identifying the required resources and opportunities that the intruder discovers the vulnerabilities, *Size* showing how large the cyber intrusions group is. On the other hand, the Vulnerability Factors consists of *Ease of Discovery* showing how easy the discovery of the vulnerabilities for the intruder, *Ease of Exploit* showing how easy it is exploiting the vulnerabilities for the intruder, *Awareness* describing how much the vulnerability is known by the intruder, *Intrusion Detection* describing possibilities to detect an exploit ongoing. The Technical Impacts of a realized threat is classified as *Loss of Confidentiality* measuring the sensitivity of data, *Loss of Integrity* showing the corruption level and damage on the data. *Loss of Availability* describing how the service is effected, and how vital it is. *Loss of Accountability* measuring how much the actions of intruders are traceable. In OWASP, all the criteria provided above are scored between 0 and 9. The interval is divided into three sub-intervals as $[0, 3)$, $[3, 6)$, $[6, 9]$, and these sub-intervals represent low, medium and high risk levels, respectively. To evaluate a threat, the average scores are calculated for the criteria in the likelihood estimation and impact estimation, separately. In our evaluation, we consider the provided criteria in Table I for the likelihood estimation, and we assess the criteria under technical impact to investigate the impact of threats.

III. TACTICS AND TECHNIQUES USED TO TEST THREATS

This section describes the tactics, techniques and sub-techniques of the implementation of the threats based on the Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK) framework. MITRE ATT&CK framework is developed by MITRE corporation to help organizations understand and classify adversaries. So that organizations have better understanding of the detection, response and mitigation

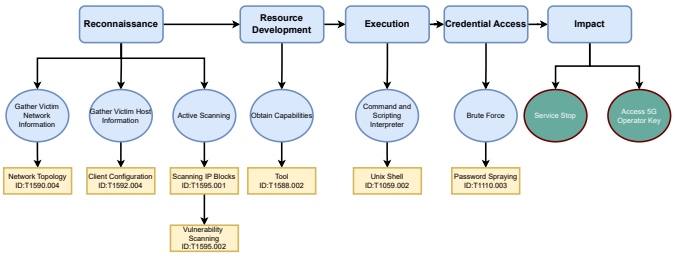

Fig. 1. Tactics and techniques followed to test Hydra.

of threats. Definition, differentiation of these tactics and techniques are well explained in [11].

Before explaining tactics and techniques selected for tested threats, we chose in figures of this section, to use rounded rectangles indicating tactics, circles showing techniques, while rectangles with yellow color are for sub-techniques with MITRE ID numbers. Techniques with green color are the sub-techniques that are newly found in this work after implementing different threat models on 5G Core and RAN. Then, implementation and explanation phases follow this procedure. Impacts and comprehensive evaluation is provided in Section V.

A. Hydra Threat Modelling

The Hydra model starts with sub-technique Network Topology to do IP scanning in order to look for open ports as illustrated in Figure 1. After gathering information about open ports, the threat flow continues for gathering Client Configuration sub-technique using Gather Victim Host Information technique in order to receive the IP address of the machines with the open ports. Afterwards, Scanning IP Blocks and Vulnerability Scanning sub-techniques are implemented in order to map IP blocks on a logical level and to exploit username and password database in KALI OS, respectively. The aim is to narrow down the potential target machine. The sub-technique is the tool to obtain capabilities belonging the Resource Development tactic. The goal is to spray credentials using the username and password database on the 5G Core infratsructure without using any backdoor. The flow follows the Execution tactic and to implement Unix- Shell sub-technique to execute commands. In this scenario, SSH protocol is used. Finally, to get the valid account, Password Spraying sub-technique is implemented with executing the command that receives files for username and password. Impact of this threat once a intruder gain credential information of 5G sytsem might be a Service Stop for the operator or the Access to the 5G Operator Key, which is new to MITRE ATT&CK framework.

B. Metasploit

The Metaploit threat model has been illustrated as given in Figure 2. Since the metasploit model requires a backdoor server allowing the intruder to access the victim remotely, the threat model starts with two Web Services sub-technique having different MITRE IDs. The first step is to download Tomcat Apache web service as a backdoor and install. The next step is giving permission as executable to web service in the victim machine. Subsequently, Meterpreter performs a vulnerability scanning to initialize a web service backdoor. As a further step, NMAP (Network Mapper) tool is activated in the remote Tomcat Apache to scan open ports. After this, MSFconsole runs to exploit the public facing applications for the Initial Access tactic. The last technique followed is Initial Access for valid Accounts to search Tomcat as a local backdoor.

Further the Exploitation for Client Execution, the Exploitation for Credential Access, and Content Injection techniques are following to deploy the payload which is shell code, to configure the payload parameters such as Setting IP, port numbers, username and password of victim machine which hosts the 5G Core infrastructure, and run the exploit which is a module executing a set of commands. During Exfiltration once the intruder accesses the reverse shell taking advantage of the target system's vulnerability and allows to access the victim's machine. The Impact of this threat might be vital like Resource Hijacking and System Shutdown/Reboot for mobile operators hosting the 5G systems.

C. VSFTPD

The threat model for VSFTPD based on the MITRE ATT&CK framework is shown in Figure 3. It is very similiar to metasploit but uses a different protocol (FTP) and not (SSH). We explain the steps implemented for each sub-techniques. Test scenario for VSFTPD are starting with Vulnerability Scanning to scan protocols such as FTP. Then victim IP address is gathered for Reconnaissance tactic. In the Resource Development tactic, first a script is created to compromise the infrastructure such as installing VSFTPD tool and upgrading the tool in a Server sub-technique. A Cron Job is created ((/bin/bash -i /dev/tcp/192.168.xxx.xx/8228 0—1)) to automate the task that runs as a shell script. Afterwards in tactics Initial Access this "Cron-Job" on the KALI OS virtual machine and also a reverse shell ((Ncat -nlvp 8228)) is listening on port 8228. The script is prepared to allow anonymous deletion, renaming, or logins. In sub-technique Launch Daemon, a FTP connection between victim and intruder machine is setup. Subsequently, in technique Forced Authentication, Lateral Tool Transfer, and Scheduled Transfer the directory of the Cron Job is changed, so that the Cron Job is executed with a new name. Hence a reverse shell is activated by the Cron Job to connect to the victim machine. As the Impact, we see that Data Manipulation is realized to insert, delete, or manipulate data of the 5G Core infrastructure hosted on the victim machine.

D. Data Exfiltration

As seen in Figure 4, for data exfiltration the initial access phase is skipped since the adversary is an insider and has access to 5G infrastructure. Hence, the first step is to import/install libraries to be able to run Python scripts. Afterwards, in the sub-technique using python script to discover the NGAP, NAS, and OAI messages, a script is shared with

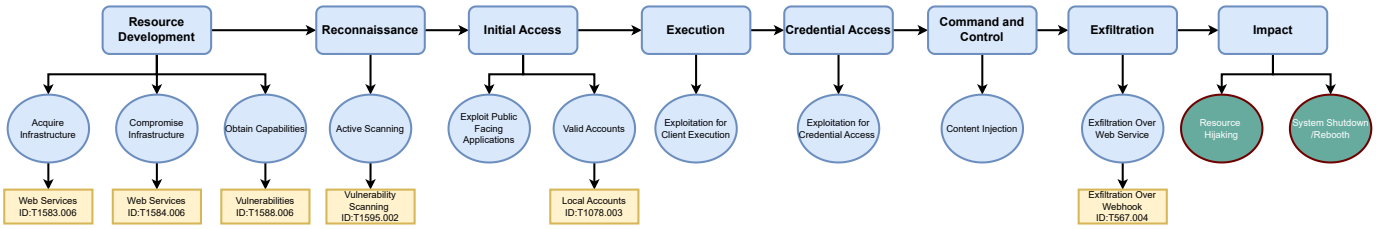

Fig. 2. Tactics and techniques followed to test the threat based on the Metasploit framework.

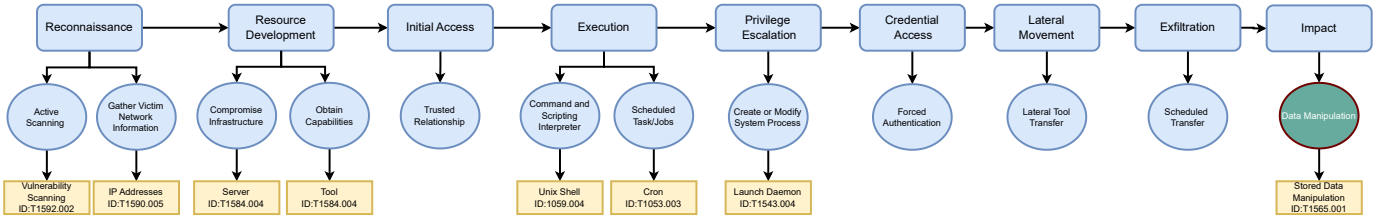

Fig. 3. Tactics and techniques followed to assess system for VSFTPD vulnerability.

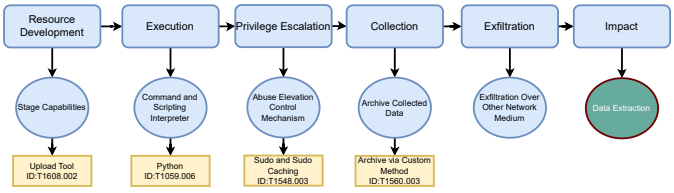

Fig. 4. Tactics and techniques followed to test Data Exfiltration.

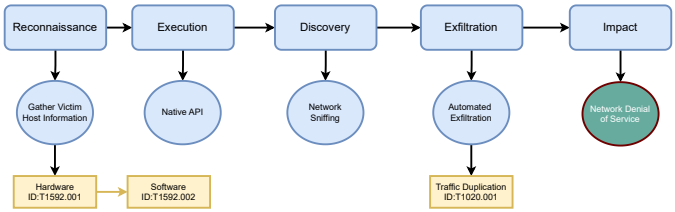

Fig. 5. Tactics and techniques followed to test Jamming.

the root user. Subsequently, the script runs with root privileges in Privilege Escalation tactic. Then, custom information such as security key, and PLMN ID's are collected in the Collection phase. Finally in the Exfiltration step confidential network operator informations is obtained.

E. Jamming

As illustrated in Figure 5, the sub-technique Gathering Victim Host Information begins the threat model and starts with Hardware and Software used to scan radio transmission using a cell scanner to discover frequency, channel bandwidth, and cell tower information. Then, HackRF One GNU Radio-companion is executed, which is an API to run in a virtual machine. Afterwards, we configure PLMN, center frequency of OAI used spectrum band ((n78=2.685G)) and ((Band-width=5Mhz)) with other cell tower information which is done to reconfigure GNU radio parameters with scanned parameters in the Network Sniffing phase. This step is followed by Traffic Duplication with an increase of power in step size of 10dB using Gaussian noise in the signal to create interference in the air interface.

F. Fuzzing

Fuzzing is a type of test in which malformed or unexpected data packets are sent to a system to detect to vulnerabilities such as crashes, memory leak, or unexpected behaviors. In 5G Network Fuzzing we target core network, gNB, or UE as well as various protocols such as Next Generation Application Protocol (NGAP), Non Access Stratum Protocol (NAS) and Stream Control Transmission Protocol (SCTP). In this section we explain fuzzing for 5G core and RAN side.

1) 5G Core Network Steps: For Fuzzing test on 5G core network, we used the 5GReplay tool [12]. It is a open source tool behavior which can be controlled by user defined rules allowing forwarding or modifying the packets. A configuration file with XML format is prepared to specify default actions. In this work, the rules applied to packets are illustrated in Figure 6. More specifically, fuzzing testing the core network sources involves sending malformed NGAP/NAS messages to scrutinize the AMF function's source code. The aim is to generate packets valid enough to evade parser rejection yet flawed enough to trigger errors. Random malformations include altering Procedure Codes and UE IDs. 5GReplay facilitates packet filtration via deep packet inspection, adjusting rule files accordingly. Manipulating NGAP PDU present attributes determining the packet type. Packets are dispatched to specified network interfaces or IPs via configuration files, which dictate actions on filtered packets and rule compilation.

The steps following to test vulnerabilities are : a) *Preparation*: In the machine having the core network functions installed, we set up and install the necessary tools and libraries, i.e., cloning and installing 5GReplay tool and MMT-Deep Packet Inspection tool as well as the necessary tool for

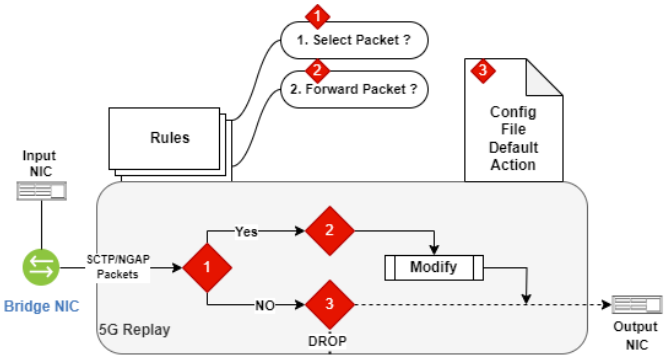

Fig. 6. Rules applied to the captured packets. This figure is inspired from [12].

building the software. b) *Running 5G system*: To implement the threat, only a running 5G core network is necessary. gNB and UE are optional components. c) *Tracking the logs*: With a network packet analyzer, e.g., Wireshark target network interface should be selected and the desired protocols needs to be filtered to capture the .pcap files to run the 5GReplay tool. d) *Modifying packets*: 5GReplay tool runs in the command line with the necessary input parameters, e.g., with target port number, IP address and target protocol.

2) 5G RAN Steps: In order to asses vulnerability of a legitimate gNB, another gNB is set to behave as adversary gNB. Once the adversary gNB is sufficiently close to the target UE and the Received Signal Strength Indicator (RSSI) of the adversarial gNB is higher than the one of legitimate gNB, the target UE will automatically connect to the adversarial gNB and the connection with the actual access radio node is completely lost. We test what kind of cell tower connection parameters are vulnerable. The steps following to test the vulnerabilities are: a) *Preparation*: We used 5GHOUL to exploit vulnerabilities to deceive 5G-capable devices into connecting with a malicious base station. This is accomplished by exposing an Adversary-Controlled Downlink channel that can arbitrarily inject and/or modify 5G NR Downlink packets generated by a real 5G OpenAirInterface. Installation involves downloading the 5GHOUL repository and adjusting configurations. b) *Running 5G system*: The vulnerable targets used in our evaluation and their corresponding Quectel modem firmware of the 5G device which is connected to 5G OpenAirInterface. c) *Tracking the logs*: The attack process includes starting the core network, establishing UE-gNB connection, launching 5GHOUL, and initiating OTA attacks. Disconnecting UE-gNB connection can be achieved through airplane mode or jamming. Following attacks, reset 5GHOUL configurations. d) *Modifying packets*: This results in Qualcomm 5G USB Modems being impacted in dropped connections by a range of previously unknown vulnerabilities in the handling of MAC/RLC, RRC and NAS messages with high severity. RRC Attach procedure, which contains the RRC Connection Setup message, is the key element of most vulnerabilities and device freezing.

IV. Implementation and Test-beds

In this section, we explain hardware and software, security testing tools, interfaces, 5G set up components used for threat modelling the test scenarios.

A. Testbed used for to test threat modelling

In our implementation set up, there is a host computer having 5G Stand Alone (SA) network installed. This host computer with 5G setup is used for Hydra, Metasploit, Data Exfiltration, VSFTPD as seen in Figure 7, while for jamming and fuzzing analysis we used another testbed as seen in Figure 8. This host computer has Ubuntu 20.04 installed with Intel Gen. 10 core and 3.30 GHz CPU, 32 GB memory and 1 TB storage. Two virtual machines (VMs) are installed on this host. One has KALI operating system (OS) to provide security testing tools, such as Hydra, Metasploit, VSFTPD, Data Exfiltration, NMAP and futhermore. The KALI OS VM is used as intruder machine. THe other adversary node has Ubuntu OS. OpenAirInterface (OAI) software [13] is used to set up core network, gNB and UE. This software enables users to have a complete 5G system which is used by numerous researchers, such as are [14], [15]. The used version of OAI is v1.5.1. The bridge seen in the figures are from OAI (demo_oai) and used to connect all Network Functions (NFs) as well as the logical router as a bridge from VMware on NAT. As seen in figures, the USRP x310 is connected to the 5G SA host computer. Since split option 8 is used from OAI, the USRP is used with an antenna for RF transmission. In addition to these, in Figure 8, there are two(2) SDR set up and using GRC GNU-Radio intentionally to create a radio interfere signal on the same centre frequency ((band n78=2.685GHz)) and 5MHz bandwidth as used by the victim SDR USRP x310. The GRC running in another intruder machine connected to USRP B210 support up to 40 MHz. For testing the air-interface Quectel Module connected to a PC used for controlling and setting up UE User equipment connected to Open 5G Radio Access Network via an open, self programmed U-SIM inside the Quectel Module.

The list of installed 5G core NFs are: a) *Core Components*: Access and Mobility Management (AMF), Session and Management Function (SMF), User Plane Function (UPF), Network Repository Function (NRF), Unified Data Repository (UDR), Authentication Server Function (AUSF), Unified Data Management (UDM) together with external Data Network to generate traffic and SQL data base. b) *Interfaces*: NGAP is found on the N2 reference point between the gNB and the AMF. NGAP is also used to convey downlink and uplink NAS (Non Access Stratum) messages as a payload that operate at the upper layer of the 5G system architecture, above the access stratum (AS) that deals with the radio interface. The N3 interface is used to connect the UPF to the Serving Gateway for data forwarding. N6: The N6 interface is used to connect the UPF to the Data Network (DN) responsible for forwarding data packets. c) *RAN Components*: It is a gNB in a 5G Stand-Alone network on general purpose x86 computing hardware and COTS Software Defined Radio

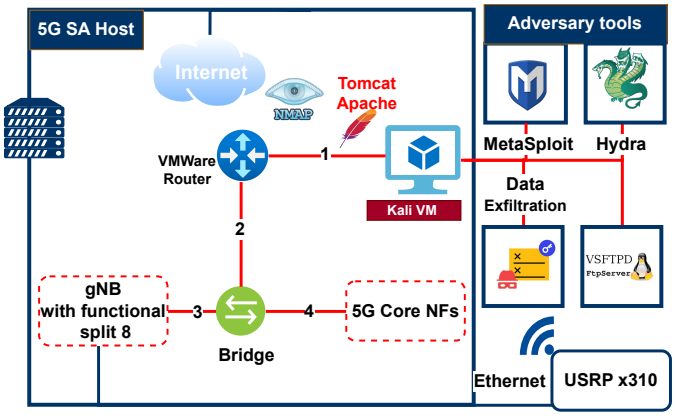

Fig. 7. Logical and physical connections used for testbed used for Hydra, Metasploit, Data Exfiltration, and VSFTPD.

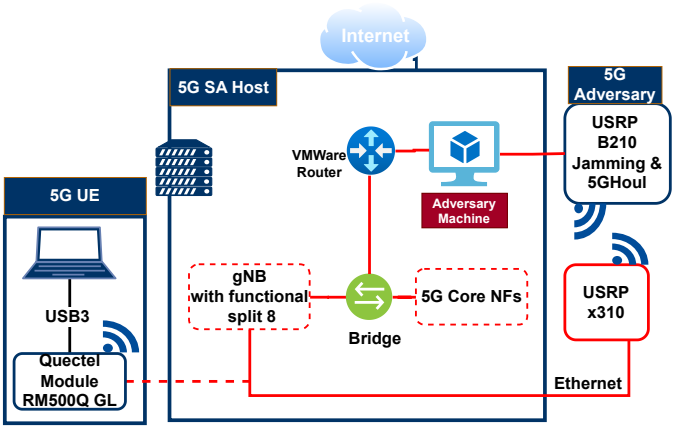

Fig. 8. Logical and physical connections used for testbed used for jamming and fuzzing attacks.

(SDR) such as the Universal Software Radio Peripheral (USRP B210 and USRP X310) which system performs most of the signal processing receiver bandwidths of a few 10 MHz can be realized.

B. Thread implementation

For testing threat models of Hydra and Metasploit, KALI OS VM is the adversary node and 5G Core NFs are victim nodes. The path followed for these two attacks is the line 1, then line 2 and line 4 as illustrated in Figure 7. On the other hand, Data Exfiltration and VSFTPD threat models have been tested following lines 1, 2, 3, and 4, hence both 5G Core and gNB are the victim nodes. The path followed to implement jamming attacks is shown in Figure 8. The affected interface is the air interface between UE(Quectel module) and gNB. The USRP B120 is connected to the adversary VM to interfere with the airinterface. To assess the vulnerability of the 5G Core network for fuzzing, the set up in Figure 8 has been used. The adversary VM has 5GReplay tool installed and connected to OAI 5G core network. On the other hand, to investigate the fuzzing threat in gNB, the 5GHOUL open source software is used. OAI gNB's legitimate node, and 5GHOUL container ((sudo bin/5gfuzzer –MCC=xxx –MNC=xx –GlobalTimeout=false –EnableMutation=false)) is the adversary node. We start the rogue base station without any attack. When the UE (Quectel Modem) losses the connection with Real gNB, achieved either by Jamming or Signal-to-Noise Ratio dropped by certain thresholds, then 5GHOUL uses the provided MCC and MNC to connect to this rogue base station by inserting a compatible testing USIM card, an attack is launched. The terminal will print messages such as ((”Malformed rrc setup sent)). Finally, target (Quectel Modem) is not responding and no communication with the smartphone is possible after 45 seconds- Here the mac-sch-rrc-setup-crash-var is exploited which has been reported in CVE-2023-33042. In summary the victim and adversary nodes, interfaces are summarized in Table II.

TABLE II
NODES AND INTERFACE USED IN THREAT MODELING

Attack Components	Hydra	Metasploit	VSFTPD	Data Exfiltration	Jamming	Fuzzing
Attack Device	Kali VM	Kali VM	Kali VM	Script-Phishing Attack	External Machine	5GReplay(Core) & 5G RAN (Ghoul)
Vulnerability Node	5G Core (OAI)	5G Core (OAI)	5G Core (OAI)	5G Core (OIA) & 5G RAN	5G RAN & Air Interface	5G RAN & Air Interface
Primary Impacted Interface	N6	N6	N6	N14	UE/Air Interface	UE/Air Interface
Secondary Impacted Interface	N2& N3	N2 & N3	N2 & N3	N4	N1 & N2	N1 & N2

V. EVALUATION

This section presents vulnerabilities found for each threat model in summary presented in Table III. In the threat model done with Hydra tool, availability and confidentiality has been compromised. It is observed that it is possible to access OAI 5G core network with Hydra tool with SSH protocol. Similarly, Confidentiality and Availability are also compromized in Metasploit threat model. This implies that the adversary has attained ROOT Access privileges, thereby assuming control as SUDO users of the vulnerable machine. This exploitation is facilitated through the exploitation of a backdoor Apache Tomcat server, which provides remote access to the 5G Open Air Interface core. Consequently, the breach significantly compromizes the ”Confidentiality” aspect of the 5G Standalone (SA) network, enabling the adversary to manipulate the security framework and take over control. In VSFTPD, with predefined username and password, a backdoor is triggered. With this backdoor a listening socket is opened and an access to a new port is established. This access allows to execute commands. Possible outcomes encompass data theft, website defacement, server hijacking, installation of additional malware, or the utilization of the server as a launching pad for subsequent vulnerabilities. The data exfiltration did not disrupt the ongoing transaction between core and RAN, so availability was not disrupted. On the other hand, the intruder was able to obtain information about the ”Ciphering Key”, the ”Security Key”, also known as the operator key, defined in the database, and the PLMN information is obtained from the Mobile Network Code (MNC) and the Mobile Country Code

TABLE III
RESULT AND IMPACT

C-I-A-A	Hydra	Metasploit	VSFTPD	Data Exfiltration	Jamming	Fuzzing
Confidentiality	Affected	Affected	Affected	Affected		
Integrity	Affected			Affected		
Availability					Affected	Affected
Authenticity		Affected	Affected	Affected		

(MCC). This shows that the confidentiality and integrity of the 5G standalone network has been breached. The adversary therefore impacts the confidentiality, integrity and authenticity of the 5G network.

Jamming compromises the availability of the network by blocking the target with loss of signal coverage. For fuzzing threat model on the 5G Core network side, a vulnerability in SCTP protocol has been observed. A memory overflow has been observed with exit flag 139. A denial of service is realized. On the other hand on 5G RAN side, a vulnerability is observed for the RRC message.

VI. OUTLOOK AND EVOLUTION

For future study cases we plan to develop resiliency measures to make 5G Core Network and Open RAN technologies with Open-Source software more secure and robust against cybersecurity threats. To implement future-proof and goal-oriented resilience measures to reduce risks 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 systems and executed on not totally trustworthy nodes, like end devices or edge components.

REFERENCES

[1] A. S. Abdalla, P. S. Upadhyaya, V. K. Shah, and V. Marojevic, "Toward next generation open radio access networks: What o-ran can and cannot do!" *IEEE Network*, vol. 36, no. 6, pp. 206–213, 2022.

[2] M. Liyanage, A. Braeken, S. Shahabuddin, and P. Ranaweera, "Open ran security: Challenges and opportunities," *Journal of Network and Computer Applications*, vol. 214, p. 103621, 2023.

[3] L. Bonati, M. Polese, S. D'Oro, S. Basagni, and T. Melodia, "Open, programmable, and virtualized 5g networks: State-of-the-art and the road ahead," *Computer Networks*, vol. 182, p. 107516, 2020.

[4] M. Polese, L. Bonati, S. D'oro, S. Basagni, and T. Melodia, "Understanding o-ran: Architecture, interfaces, algorithms, security, and research challenges," *IEEE Communications Surveys & Tutorials*, 2023.

[5] D. Mimran, R. Bitton, Y. Kfir, E. Klevansky, O. Brodt, H. Lehmann, Y. Elovici, and A. Shabtai, "Security of open radio access networks," *Computers & Security*, vol. 122, p. 102890, 2022.

[6] A. Zwarico, "O-ran security," *Open RAN: The Definitive Guide*, pp. 121–136, 2023.

[7] J. Y. Cho and A. Sergeev, "Secure open fronthaul interface for 5g networks," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–6.

[8] D. Dik and M. S. Berger, "Open-ran fronthaul transport security architecture and implementation," *IEEE Access*, 2023.

[9] H. Wen, P. Porras, V. Yegneswaran, A. Gehani, and Z. Lin, "5g-spector: An o-ran compliant layer-3 cellular attack detection service," 2024.

[10] "OWASP Risk Rating Methodology," https://owasp.org/, Accessed: 2024-04-16.

[11] "MITRE ATT&CK," https://attack.mitre.org/, Accessed:2024-04-16.

[12] Z. Salazar, H. N. Nguyen, W. Mallouli, A. R. Cavalli, and E. Montes de Oca, "5greplay: A 5g network traffic fuzzer-application to attack injection," in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 2021, pp. 1–8.

[13] "OPENAIRINTERFACE," https://openairinterface.org/, Accessed: 2024-04-18.

[14] F. Kaltenberger, R. Knopp, N. Nikaein, D. Nussbaum, L. Gauthier, and C. Bonnet, "Openairinterface: Open-source software radio solution for 5g," in *European Conference on Networks and Communications (EUCNC), Paris, France*, 2015.

[15] F. Kaltenberger, A. P. Silva, A. Gosain, L. Wang, and T.-T. Nguyen, "Openairinterface: Democratizing innovation in the 5g era," *Computer Networks*, vol. 176, p. 107284, 2020.