Generating Full-stack 5G Security Datasets: IP-layer and Core Network Persistent PDU Session Attacks

George Amponis[a,b], Panagiotis Radoglou-Grammatikis[a,c], Thomas Lagkas[b], Savas Ouzounidis[a], Maria Zevgara[a], Ioannis Moscholios[d], Sotirios Goudos[e] and Panagiotis Sarigiannidis[c,*]

[a]*Department of Research and Development, K3Y Ltd., Sofia, 1000, Bulgaria*
[b]*Department of Computer Science, International Hellenic University, Kavala Campus, 65404, Greece*
[c]*Department of Electrical and Computer Engineering, University of Western Macedonia, Kozani, 50100, Greece*
[d]*Department Informatics & Telecommunications, University of Peloponnese, Tripolis, 22131, Greece*
[e]*Department of Physics, Aristotle University of Thessaloniki, Thessaloniki, 54124, Greece*

ARTICLE INFO

Keywords:
5G Testbed
Cybersecurity Events
PFCP
Radio Access Networks
5G Datasets

ABSTRACT

With the increasing number of users accessing the Internet over 5G systems, security concerns have become a major challenge that needs to be addressed. This paper proposes a solution to this challenge by proposing a system to train defenders to handle cyber attacks and develop intrusion detection systems that can timely notify of security events, also within the 5G core itself. This paper builds on our previous contributions on a containerized 5G testbed and proposes a novel set of full-stack attacks targeting networked hosts and 5G Network Functions (NFs) alike. Importantly, we identify the potential to generate persistent Packet Forwarding and Control Protocol (PFCP) Denial of Service (DoS) attacks to deprive end users of connectivity to the data network, even in the event of a handover to another gNodeB. This framework is envisaged to facilitate the generation of highly diverse and realistic datasets, containing malicious GPRS Tunneling Protocol (GTP) and PFCP traffic captured over 5G interfaces, thereby enhancing the security of next-generation networks.

1. Introduction

In this paper, we address the pressing issue of ensuring secure and reliable connectivity in 5G networks by investigating and mitigating potential attacks on the control-plane signaling between the Session Management Function (SMF) and the User Plane Function (UPF). Our motivation stems from the increasing reliance on 5G networks and the criticality of maintaining uninterrupted user connectivity. Building upon existing approaches, we present innovative techniques to detect and mitigate unauthorized control-plane signaling attacks, such as Session Deletion and Session Modification attacks. These attacks aim to disrupt user connectivity to the Data Network (DN) by targeting session parameters and packet handling settings within the UPF. Through a comprehensive evaluation on a real-world testbed, we showcase the effectiveness of our proposed mechanisms in mitigating these attacks, highlighting their superiority over current approaches. Our contributions extend beyond existing methods, providing enhanced security measures and ensuring the robustness of 5G network connectivity in the face of malicious control-plane signaling activities.

Building on our previous work entitled "Towards Securing Next-Generation Networks: Attacking 5G Core/RAN Testbed" presented in the 2022 Panhellenic Conference on Electronics and Telecommunications (PACET) (1), we extend our research to cover a new set of 5G-specific attacks targeting not only 5G-connected hosts but also key components of the 5G core itself, with the end-goal of depriving users from access to the internet. We consider a set of N4 interface-targeting attacks which we first proposed in (2) and extend them to enable persistence and increase

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952672 (SANCUS).

*Corresponding author
gamponis@k3y.bg (G. Amponis); geaboni@cs.ihu.gr (G. Amponis); pradoglou@k3y.bg (P. Radoglou-Grammatikis); tlagkas@cs.ihu.gr (T. Lagkas); souzounidis@k3y.bg (S. Ouzounidis); mzevgara@k3y.bg (M. Zevgara); idm@uop.gr (I. Moscholios); sgoudo@physics.auth.gr (S. Goudos); psarigiannidis@uowm.gr (P. Sarigiannidis)
ORCID(s): 0000-0001-6411-0485 (G. Amponis); 0000-0003-1605-9413 (P. Radoglou-Grammatikis); 0000-0002-0749-9794 (T. Lagkas); 0000-0002-6648-4728 (S. Ouzounidis); 0000-0002-5804-1003 (M. Zevgara); 0000-0003-3656-277X (I. Moscholios); 0000-0001-5981-5683 (S. Goudos); 0000-0001-6042-0355 (P. Sarigiannidis)

the attack severity. The end goal of this research is to generate valuable 5G datasets for training Intrusion Detection Systems (IDSs) that can serve the whole 5G stack.

Training defenders and detection systems capable of handling and detecting cybersecurity events in 5G networks is pivotal for enabling the undisturbed flow of information and minimizing downtime in critical and sensitive applications such as aerial communications (3), remote sensing, and industrial monitoring.

The communications transformation brought by next-generation cellular networks has already redefined existing connectivity and service reliability models so as to include pivotal security-by-design principles. These are deemed an absolute necessity to enable 5G to achieve its promise (4). It is important to embed security capabilities to both classical networking and 5G-specific attack detection and prevention systems. Moreover, training defenders in the current networking landscape and keeping them up-to-date with the latest developments is proving to be increasingly difficult (5).

New security requirements have risen and are required to address the needs of different adjacent layers of the 5G architecture, namely physical, network, and application layer. Defensive systems and engineers need to implement new risk management frameworks so as to consider the evolving security threats landscape (6). Thus, 5G networks should consider additional security requirements, while at the same time, should address the need to maintain some level of modularity and flexibility, to train defenders and improve resilience and reliability (7). To that end, we aspire to address the issue of lack of defense training baseline by introducing an integrated yet modular, all-in-one testbed capable of modelling cybersecurity events on a spectrum of layers, ranging from the 5G core (i.e., attacks specifically implemented within the 5G core network, against targeted NFs) to the RAN and the applications layer.

5G networks present a unique set of security challenges due to their increased complexity and the integration of diverse technologies. As the backbone of critical applications such as aerial communications, remote sensing, and industrial monitoring, the security of 5G networks is of paramount importance. However, the rapid growth of 5G technology also brings about an evolving threat landscape, with sophisticated attacks targeting different layers of the network architecture. From physical layer vulnerabilities to network and application layer exploits, 5G networks must address a wide range of security concerns to ensure the confidentiality, integrity, and availability of data and services. Robust defense mechanisms and detection systems are essential in mitigating these risks and protecting against malicious activities. (8) Traditional security solutions are no longer sufficient in this dynamic environment, necessitating the development of advanced intrusion detection systems (IDS) capable of identifying and preventing emerging threats. By addressing these specific security challenges, our research aims to contribute to the development of effective defense strategies for 5G networks, enabling the undisturbed flow of information and the safeguarding of critical applications.

The rest of the paper has the following structure. Section 2 overviews the related work on testbeds for 5G systems. Implementation information about the proposed modular 5G testbed is provided in Section 3. The emulated 5G cybersecurity attacks are described in Section 4. Lastly, Section 5 concludes the paper and provides future directions.

2. Related work

Authors in (9) propose a 5G testbed which allows the user to study performance issues and attacks on network slices. The aim of the authors is to provide a tool for a research study of network slicing; their proposed testbed uses OpenAirInterface for adding core and radio-level 5G elements to the testbed. More specifically, the UE and the AN are simulated through the OAI Simulator. In this case, instead of representing network functions (NFs), docker containers represent entire network slices. The authors' work can be considered complementary to ours, from a technical point of view, as we deal with individual containerized NFs. In comparison to this work, our research goes beyond the state of the art by focusing on the detection and mitigation of unauthorized control-plane signaling attacks in 5G networks. While the referenced work primarily centers around the development of a 5G testbed for network slicing evaluation, our study delves into the specific challenges associated with the control-plane signaling between the SMF and UPF. We propose innovative techniques to identify and counteract attacks such as Session Deletion and Session Modification, which aim to disrupt user connectivity to the DN. Moreover, our research includes a comprehensive evaluation on a real-world testbed, showcasing the effectiveness of our proposed mechanisms in mitigating these attacks. By addressing the critical issue of secure and reliable connectivity, we contribute to advancing the state of the art in ensuring the robustness of 5G networks against malicious control-plane signaling activities.

Authors in (10) engage in an in-depth study of the platforms and frameworks available to implement the 5G core network. The authors compare three open-source platforms, namely Magma, Open5GS and Free5GC.

The core idea behind this comparative analysis is to address development and computational demands concerning flexibility, scalability and the appropriate use of available resources to deliver performance and various functions. We considered the outputs of this work to implement our own integrated testbed, electing Open5GS as the core network implementation, along with UERANSIM to implement the RAN.

Authors in (11) investigate the process and deployment aspects concerning 5G testbed structures and architectures. The authors also research the usage of an AI-based RAN slicing module and virtual network function (VNF) placement algorithm. The authors work is complementary to ours, as it concerns deployment and orchestration aspects of 5G testbeds leveraging AI. In their paper titled (12), S. Gupta et al. examine the fundamental processes involved in 5G network handover, with a particular focus on the security implications related to handovers between base stations. Meanwhile, I. Ahmad et al. provide a comprehensive overview of the significant security challenges and privacy concerns in 5G networks, in their paper titled (13).

In our own previous work in (2) we investigated how scapy-crafted PFCP session control messages can be used in a malicious context in order to disconnect legitimate users from the internet by high-jacking the N4 interface of the 5G core. The previously proposed set of attacks was successfully implemented and tested using the same testbed as the one we proposed in (1).

Authors in (14) demonstrate the practical application of a cyber range platform for training cybersecurity defenders. The study focuses on the integration of a machine learning-driven security threat analytics module within the SPIDER cyber range platform. By leveraging automated network orchestration and machine learning techniques, the platform enables realistic network traffic generation and the detection of attacker connections. The authors deduct that trainees can improve their skills in identifying and mitigating cybersecurity risks, enhancing their ability to protect critical systems and networks. The authors highlight the importance of such training environments in preparing defenders to address the evolving challenges in the cybersecurity landscape.

This paper distinguishes itself from the above-mentioned related works by presenting a novel and comprehensive approach to training and evaluating cybersecurity defenders in a realistic 5G network environment, considering both 5G-specific and network related security events. While existing studies focus on generic cyber range platforms or testbeds, our work specifically targets the unique security challenges and vulnerabilities inherent in 5G networks. We provide a containerized 5G testbed that allows for the emulation of various network functions and the implementation of specific attack scenarios. Our testbed integrates Open5GS and UERANSIM tools, enabling the examination of both classical networking attacks and 5G-specific threats. Additionally, our proposed work incorporates a set of PFCP attack generators capable of generating persistent 5G-specific security events affecting internal 5G core interfaces. Moreover, we contribute to the field by generating malicious datasets, containing traffic corresponding to both classical and 5G-specific attacks. Said datasets serve as valuable resources for training artificial intelligence and machine learning systems to preemptively recognize and respond to attacks in cellular networks. An already outputted such dataset can be found in (15). By showcasing the applicability of our approach and validating our work through successful tests of cyberattacks, we demonstrate the effectiveness and practicality of our proposed testbed for enhancing the defense and security of 5G networks

3. Containerized 5G Testbed

The testbed proposed and implemented in the context of this paper utilizes a slight modification of Open5GS as the cellular core (16), and UERANSIM as RAN component of the overall synthesis (17). The architecture of the testbed, allows for a great degree of modularity and extensibility, while its containerized nature supports minimal-overhead instantiation of tests and cybersecurity events, in a scalable, fully automated and near zero-touch manner. Moreover, the testbed's modularity allows for a set of attacks to be implemented simultaneously. Adding to the above-mentioned tools, we have incorporated a set of custom-built sniffers and packet generating tools, capable of formulating 5G control-plane traffic which is transmitted at the N4 interface effectively disrupting user sessions in a UE-targeting manner.

The testbed has been successfully tested with a set of cyberattacks, of both classical networking and 5G-specific nature. This paper focuses on performing a man-in-the-middle (MITM) and a brute force (BF) attack for eavesdropping traffic over a 5G tunnel and obtaining illegitimate access across a next generation cellular network.

The proposed emulation framework presented in this paper provides support for a wide range of network functions (NFs) required for implementing cellular connectivity. These NFs include the Access and Mobility Management Function (AMF), Session Management Function (SMF), User Plane Function (UPF), Network Slice Selection Function

(NSSF), Network Exposure Function (NEF), Network Repository Function (NRF), Policy Control Function (PCF), Unified Data Management (UDM), Application Function (AF), Authentication Server Function (AUSF), DN, Radio Access Network (RAN), and User Equipment (UE). By incorporating these NFs into the testbed architecture, we ensure the comprehensive coverage of key components necessary for simulating a realistic 5G network environment. This allows for accurate emulation and evaluation of cybersecurity events and attacks in the context of cellular connectivity.

The proposed work pioneers in the domain of generating malicious datasets, containing traffic corresponding to both classical and 5G-specific attacks. This will allow us to train artificial intelligence (AI) and machine learning (ML) systems to recognise preemptively take action against attacks, in cellular networks. To showcase the applicability of our approach, we validate our work by capturing malicious 5G traffic at both a core and a RAN level. The architecture of the testbed can be seen in Figure 1.

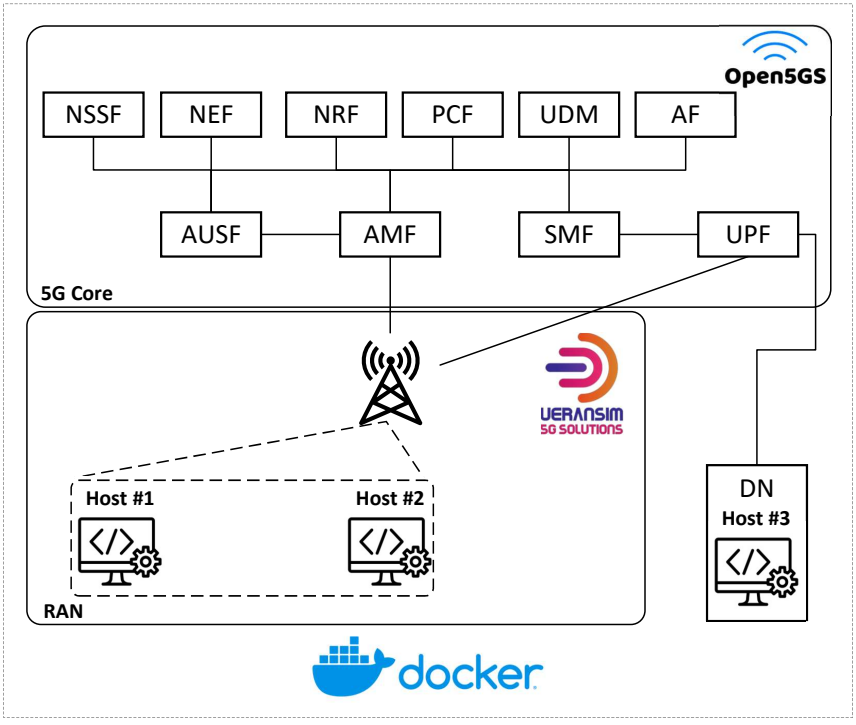

Figure 1: Architecture of the testbed.

To implement the aforementioned attack scenarios, we have networked three pivotal containers, namely the Server, the Attacker and the Victim. The Server is accessible by the Victim through a 5G connection to the DN, while the Attacker and the Victim are directly networked at the RAN layer, and they constitute UE devices of UERANSIM.

The developed testbed can be instantiated with a single docker-compose command. The overall automated process is as follows. After starting all the appropriate containers implementing the above-mentioned NFs, the UEs are registered. This needs to be done prior to starting the UERANSIM simulation and is implemented so as to allow the proper exchange of handshakes with the emulated cellular antennas. This initial registration can either be done graphically via the included Open5GS webui, or by using a command-line interface (CLI) tool directly at the database handling user registrations. As this method is easier to automate, we chose it as a better alternative. The attributes needed to register a new user are the International mobile subscriber identity (IMSI), the unique Key, and the Operator Code (OPC).

For the purpose of automating the overall setup, we wrote a script to perform the relevant actions. The registration prompt seen below concerns the core network domain and needs to be implemented prior to the establishment of a RAN session. The return message seen below can be used as a reference for the successful registration of UEs in the mobile core network. Assuming that the registrations have been successful, the registry holding the relevant user data (in our case the mongodb database) will return:

```
WriteResult({
        "nMatched" : 0,
        "nUpserted" : 1,
        "nModified" : 0,
        "_id" : ObjectId("62711caaf...")
})
```

After registering the UEs using the above-mentioned method, the emulator launches all radio-layer processes. First it launches the gNB emulation using `./nr-gnb -c ./oai-gnb.yaml`, and then the UE emulation(s) using `./nr-ue -c ./oai-ue.yaml`. The individual subscribers can now successfully establish GTP-U tunnels with the third illustrated host entity (Host #3), using the newly created `uesimtun` interface. To facilitate the implementation and execution of the testbed, specific commands are provided in the text for executing the gNB and UEs with their respective configuration files. These commands and configuration files are essential for initializing the necessary network functions and emulated user equipment. While the detailed discussion of these commands and configuration files may be specific to the software used in the testbed, they serve as a practical guide for researchers and practitioners interested in replicating and utilizing the proposed framework. Additionally, the uesimtun interface mentioned in the commands represents the virtual network interface that connects the emulated user equipment with the core network components. It enables the exchange of data packets between the UEs and the network functions. The inclusion of these details aims to provide readers with a comprehensive understanding of the testbed setup and its operational aspects.

Summarizing, the testbed for our research comprises several key building blocks. Firstly, it utilizes a modified version of Open5GS as the cellular core and incorporates UERANSIM as the RAN component. The architecture of the testbed is modular and containerized, facilitating scalability and automation. Custom-built sniffers and packet generating tools are integrated to formulate 5G control-plane traffic for targeted disruption. The testbed incorporates various network functions essential for cellular connectivity, such as AMF, SMF, UPF, NSSF, NEF, NRF, PCF, UDM, AF, AUSF, DN, RAN, and UE. This comprehensive integration ensures the realistic simulation of a 5G network environment. The testbed also generates malicious datasets containing classical and 5G-specific attacks, enabling the training of AI and ML systems for proactive threat detection and response. Overall, the testbed's architecture and components provide a solid foundation for conducting cybersecurity events and evaluating the security and resilience of 5G networks.

4. Cyberattack Scenarios

4.1. Scenario 1: MITM attack

The MITM scenario involves three nodes (Host 1, Host 2 and Host 3), where a malicious user intercepts and eavesdrops traffic exchanged between two legitimate hosts over a 5G tunnel. The participating entities are:

- User: this is the "victim" of the MITM attack. It attempts to load the contents of a web page by accessing a server located at the DN. The container corresponding to this entity has Firefox running on it, so that a user can test

Table 1
PFCP Session Management Message Types

PFCP SessionManagement Messages		
Message Type Value (dec)	**Message Type**	**Description**
50	Session Establishment Request.	Used by the SMF to request establishment of a new PFCP session with the UPF.
51	Session Establishment Response.	Sent by the UPF to acknowledge the request and establish the PFCP session.
52	Session Modification Request.	Used by the SMF to request modifications to an existing PFCP session.
53	Session Modification Response.	Sent by the UPF to acknowledge the modification request.
54	Session Deletion Request.	Used by the SMF to request deletion of an existing PFCP session.
55	Session Deletion Response.	Sent by the UPF to acknowledge the deletion request.
56	Session Report Request.	Used by the SMF to request a report of the session information from the UPF.
57	Session Report Response.	Sent by the UPF in response to a session report request, containing the requested information.
58 to 99	For future use.	Not implemented.

connectivity to the web page of interest. The idea behind this configuration is that an actual user can navigate graphically, and access the Server's contents over a virtualized 5G connection. To connect to firefox from the host, the user can visit `localhost:5800`.

- Server: this entity is hosting an http server, serving the files contained in is internal directory. This server uses http instead of https and can thus be used to demonstrate genuine data interception.
- Attacker: this entity is meant to be used as an illegitimate user instantiating the attack. This container comes ready with a set of scripts used to automate the attack process when required.

In this scenario, the hosts shown in Figure 1 interact as described below: Host 1 assumes the role of the legitimate user (i.e., the victim of the attack), while Host 2 assumes the role of the attacker and Host 3 assumes the role of the server (since it is accessible only through the DN). The steps followed to automatically implement the MITM attack are as described below. Firstly, the attacker (Host 2) discovers the IPs of the victim (Host 1) and the server (Host 3). The commands used by the automated script are `dig mitm_victim` and `dig mitm_server`. Secondly, with this information, the attacker will run arpspoof twice, once for each flow direction concurrently; the commands used by the script are `arpspoof -t <server_ip> <victim_ip>` and `arpspoof -t <victim_ip> <server_ip>`. Thirdly, the emulator adds a forwarding rule to the attacker entity with `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080`. This will add a rule to iptables to forward every packet with destination port 80 (therefore HTTP traffic) to the proxy. Fourthly, the attacker starts the transparent (i.e., non-blocking) interception process with the command `mitmproxy -m transparent`. Checking the output of the mitm proxy will show the POST and GET requests from and to the server. Alternatively, the malicious host can use any relevant tool to monitor and store the traffic (i.e., `tshark`). The mitigation process of the attack has also been implemented in an automatic manner by the emulator. This process involves utilizing `macchanger` to undo the above-mentioned arp cache poisoning.

4.2. Scenario 2: BF attack

The BF scenario involves two nodes (Host 1 and Host 3), where a malicious user attempts to gain access to a vulnerable service-component of the ONAP Software Defined Networking Controller (SDNC) Directed Graph (DG) Editor. ONAP in this context can be used to deploy other 5G network slices (18) in an on-demand fashion, where a user can instantiate and define an appropriate network topology. The participating entities are:

- SDNC DG builder: this entity is the victim of the BF attack. This is the container exposing the ONAP DG service to the end-user. It is located outside of the networking scope of the attacker host, and is only accessible through the emulated 5G tunnel. This is done to ensure that we can obtain flow-level metrics, which can subsequently be utilized to train AI-based intrusion detection and prevention systems (IDPS), using solely 5G core-level datasets.
- SDNC Ansible: An Ansible server enabling the underlying ONAP SDN controller offer the DG service.
- SDNC Controller: this entity is SDNC controller which implements the logic of the targeted service
- Attacker: this entity is meant to be used as an illegitimate user, attempting to take control of the targeted service via a dictionary attack. The target is located at the DN, and as such, all traffic and connection requests will pass

through the emulated 5G core network. The exploited vulnerability is that the ONAP SDNC DG Builder service uses basic authentication for its front-end, without any form of login rate-limitations being in place.

For the purpose of this scenario, we will only consider the ONAP SDNC DG builder entity as the target of the attack, for simplicity, mainly since the other networked entities of the ONAP SDNC service are purely supportive and are not directly targeted by the attacker. In this scenario, the hosts shown in Figure 1 interact as described below: Host 1 assumes the role of the attacker and Host 3 assumes the role of the scenario's target, i.e., the SDNC DG builder. The steps followed to automatically implement the BF attack are as described below. Firstly, the attacker (Host 1) performs an nmap to check for open ports at the target using the command `nmap -p- <target-IP>`. Port `3100` should be is open, running the opcon-xps service. A user can access the targeted service by visiting `<target_ip>:3100`. The authentication method is https-get. Secondly, considering the above remarks, the attacker runs hydra (19) using the command `hydra -L <usr_list> -P <pass_list> https-get://target_ip:3100/ -t 4`. If the attack has been successful, the command will return the correct credential combination. The attack can be mitigated by re-configuring the target entity to drop all packets originating from the attacker by adding the malicious address to a prohibition list.

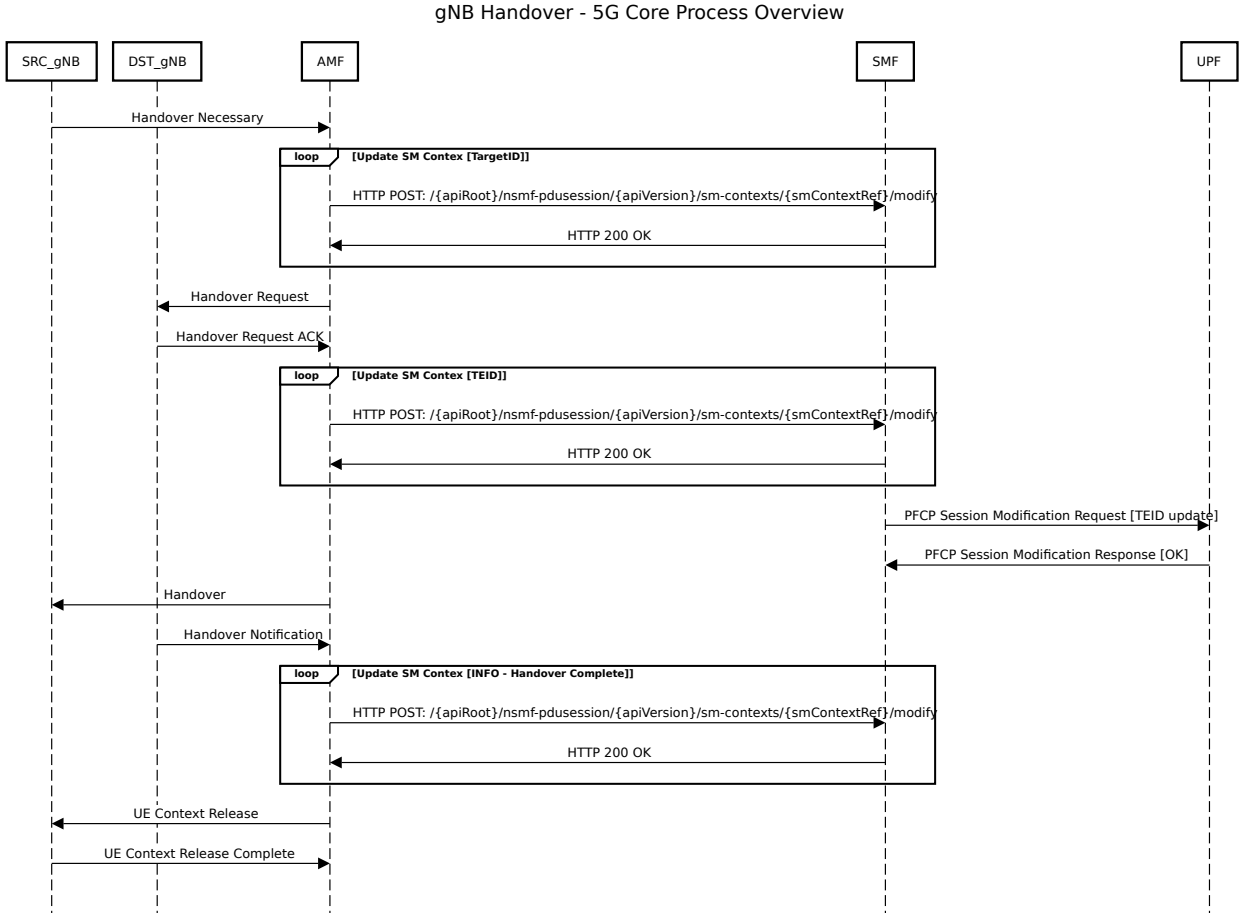

Figure 2: Handover procedure for 5G core elements.

4.3. Scenario 3: Persistent PDU Session Attacks

The third scenario presented in this paper concerns a PDU session interruption attack, which happens within the 5G core itself. As we have shown in our relevant work targeting attacks at the N4 interface (2), it is possible for a malicious entity to impede the connectivity of an end user to the DN. This is implemented through gaining access to the SMF and transmitting fraudulent Packet Forwarding and Control Protocol (PFCP) messages to the UPF.

PFCP is a protocol specified by 3GPP, which plays a critical role in 5G core networks. The protocol is used for the communication between the control plane (SMF) and the user plane (UPF) on the N4 interface. This protocol is designed to regulate and compartmentalize the interactions between SMF and UPF. It is an application-layer protocol that usesthe User Datagram Protocol (UDP) and operates on port number 8805 by default. PFCP messages can be divided into three categories: Node-related messages, Session-related messages, and Error Indication messages. The Session-related messages are particularly important for the creation, updating, and deletion of sessions and associations among PFCP nodes. In this paper, we focus on the PFCP session-related messages as they are critical for managing subscribers' sessions. Table 1 provides more details about PFCP session management messages, as well as a short description for each message type.

From the above-described messages two types of session management messages which the SMF utilizes in order to control user sessions handled by the UPF: PFCP Session Deletion messages, and PFCP Session Modification messages. Building on our previously published work on PFCP attacks, we showcase a method to extend our previously proposed session-targeting attacks into more sophisticated IP-targeting attacks.

Implementing this attack persistence can be done with relative ease, by checking the correlation between the target UE's IP address and the newly assigned SEID, which is computed by the SMF and sent to the UPF in a Session Modification Request upon session handover. This implies that the SMF must persistently store a table with the assigned SEIDs and their corresponding IP addresses at the User Plane level. The process describing a session handover in 5G networks is described in Figure 2. In greater detail, our approach in the work at hand fundamentally enhances our results obtained in (2) by introducing the idea that a loss of connectivity can "follow" an affected subscriber UE, despite them having altered SEIDs, IP addresses or TEIDs. This newly introduced layer or persistence necessitates a more intricate and convoluted approach towards implementing the session manipulation tactics described in our works.

The PFCP Session Establishment message includes the updated SEID, as well as other relevant information such as the F-TEID and the N4 interface endpoint. Using this data, we are proposing a set of persistent PDU session attacks targeting not just a specific SEID, as we have already showcased in (2), but also enabling persistence through using the new assigned SEID sent by the UPF upon completion of the 5G handover, effectively targeting specific IP addresses instead of session endpoints. The information needed to correlate the distinct and unique SEID and IP address of each UE can be found in the following fields:

The new unique assigned SEID can be found in the `SEID` field of the `F-SEID` PFCP layer. The IPv4 address of t he UE can be found at the `IPv4 address` field at the `UE IP Address layer`, which in turn resides within the `PDI` layer of the `Create PDR` field.

After transmitting a Session Deletion request or a Session Modification request with a DROP flag, the user packets are dropped due to the following mechanisms. In the case of a Session Deletion request, the unauthorized request is sent from the SMF to the UPF, triggering the deletion of the Tunnel Endpoint Identifier (TEID) and IP address of the gNB from the UPF's records. As a result, when user packets arrive at the UPF for forwarding to the DN, the UPF can no longer associate these packets with the corresponding session and destination. Consequently, the UPF discards these packets, effectively dropping them and preventing their transmission to the DN.

Similarly, when a Session Modification request with a DROP flag is transmitted, the malicious request instructs the UPF to apply a "DROP" action in the Forwarding Action Rules (FAR) of the affected session. As a result, when user packets associated with that session arrive at the UPF, the UPF identifies the corresponding FAR with the "DROP" flag and immediately discards the packets without forwarding them to the DN. This behavior effectively drops the user packets, preventing their delivery to the intended destination. These mechanisms demonstrate how the unauthorized control-plane signaling disrupts the normal flow of user packets, leading to their intentional dropping by the UPF. By manipulating the session records or introducing "DROP" actions, the attacker effectively prevents the transmission of user packets to the DN, resulting in a disruption of connectivity for the affected user. Tests conducted with our proposed testbed indeed validate both above statements.

4.3.1. Persistent Session Deletion

For this attack scenario, the PFCP Session Deletion messages are used to delete a targeted PFCP session, and thus disconnect a specific UE from the DN - it must be noted that while removing a UE's radio-layer association from the network will result in a PFCP session deletion, the reverse is not true: a PFCP session deletion done directly at the N4 interface will result in the network maintaining the connection to the 5G RAN and core network intact, as we have shown in (2). Although the UE is still connected to the 5G RAN and core network, the UE is no longer able to connect to the DN. This message type uses a unique identifier to target specific sessions, namely the Session Endpoint Identifier

(SEID). Assuming that the affected UE doesn't relocate to the range of a new gNB, connectivity remains disrupted indefinitely. If the affected UE changes its serving gNB through, namely in the case of a 5G handover its possible that both the SEID and the Tunnel Endpoint Identifier (TEID) change (20). When a UE performs a gNB handover, it initiates a new PDU session with the target antenna. As a result, a new SEID is assigned to the session between the UE and the target gNB entity. However, the data traffic is still transmitted through the existing data tunnel between the UE and the source UPF, and thus the TEID remains the same. Once the handover is completed, the source gNodeB releases the old data tunnel and the target gNodeB establishes a new data tunnel with the UPF. At this point, the TEID also changes to reflect the new data tunnel.

4.3.2. Persistent Session Modification

In the case of this attack scenario, we are proposing an extension of the PFCP Session Modification attack we showcased in our previous work. The attack utilizes the DROP flag, which is enabled in order to disrupt a specific UE's connectivity to the DN by modifying its PFCP session and making the UPF drop all packet handling rules for the affected session. As is the case with the previous attack, deleting or modifying a UE's radio-layer association will result in a PFCP session deletion, but a PFCP session modification (or in this case packet handling rules drop) done directly at the N4 interface will not necessarily result in disconnection from the 5G RAN and core network. Again, the SEID is used as a unique identifier to target specific sessions. If the affected UE undergoes a gNB handover, the new SEID assigned by the SMF to the session shall be recorded and correlated with the UE's IP address. When the Session Modification message is successfully received and parsed by the UPF, it will drop all packet handling rules for the affected SEID. Effectively, this means that without removing the session at a PFCP or RAN layer, we are able to deprive a given UE of access to the DN.

5. Conclusions

This paper has built on the results presented in (2) and (1), where we showcased a containerized and integrated testbed, incorporating all necessary networking elements to achieve connectivity over 5G, while also supporting the implementation of and mitigation against different attacks, as seen in (21). In the work at hand, we further investigate a set of PFCP attacks, and enhance them in terms of SEID-persistence. The proposed testbed and set of attacks, can successfully generate rich and diverse datasets mainly targeting the GTP and PFCP protocols. Regarding mitigating actions against the 5G-specific PFCP attack, limited actions can be taken by potential victims. However, at the 5G core level, there indeed can exist defensive measures. The most important defensive action which can be taken by a defensive entity within the 5G core is to enable the cascading of session-affecting events not only from the RAN to the 5G core NFs (implemented inherently) but also vise-versa, through the implementation of context-aware inter-plane acknowledgements. While this wouldn't directly secure victims, this implementation would allow session-affecting events to cascade "downwards", and having their effects projected to the UEs' radio sessions. For instance, a session deletion event initiated at the mobile core layer should cascade, resulting in a session context removal at the radio layer. This will allow a user to be notified of alterations to their PDU session context. Another defensive measure would be for PFCP traffic between the SMF and UPF to be encrypted, or alternatively the UE IP addresses (which are currently carried in clear text in the `IPv4 address` field, within the `UE IP Address` field of the `PDI [Grouped IE]`, which lies nested within the `Create PDR` PFCP layer). Encrypting sensitive UE-specific data would hinder a malicious entity from implementing session-persistence in their attacks, as described in this paper.

Using the proposed testbed, we were able to extract useful datasets at various levels, containing 5G traffic corresponding to cyberattacks and nominal traffic alike. We have published a such example, which can be found in IEEE DataPort (15). The examined scenarios can provide valuable data on the targeted application-layer attacks both for defenders and AI-enabled detection systems. For example, an AI-enabled IDPS can be trained on such datasets, so as to timely terminate the appropriate communication links and potentially secure an otherwise vulnerable host. For the MITM attack, the captured datasets, as expected, contain malicious traffic, accessible through the N3 and N4 5G interfaces. Similarly, in the case of the BF attack, since the attack exclusively concerned traffic exchanged through the 5G tunnel, we were able the extract valuable metrics at a 5G core level. Specifically, by observing the typology and transport-layer characteristics of the GTP-U packets exchanged between the emulated cellular tower and the UPF, we were able to discern and pinpoint the timestamp at which the attack begins. Regarding the persistent PDU session attacks, we showcase an enhancement to previously proposed 5G attacks, enabling a malicious entity to deprive an end user of connectivity to the DN even in the event of a 5G handover and subsequent change in SEID/TEID.

Acknowledgment

A preliminary version of this work is published in the 2022 Panhellenic Conference on Electronics and Telecommunications (PACET) (1).

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952672 (SANCUS).

Notes

This publication constitutes an extension of the conference paper entitled "Towards Securing Next-Generation Networks: Attacking 5 Core/RAN Testbed" (1).

References

[1] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, S. Ouzounidis, M. Zevgara, I. Moscholios, S. Goudos, and P. Sarigiannidis, "Towards Securing Next-Generation Networks: Attacking 5G Core/RAN Testbed," in *2022 Panhellenic Conference on Electronics & Telecommunications (PACET)*, pp. 1–4, 2022.

[2] G. Amponis, P. Radoglou-Grammatikis, T. Lagkas, W. Mallouli, A. Cavalli, D. Klonidis, E. Markakis, and P. Sarigiannidis, "Threatening the 5G core via PFCP DoS attacks: the case of blocking UAV communications," *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, p. 124, Dec 2022.

[3] G. Amponis, T. Lagkas, M. Zevgara, G. Katsikas, T. Xirofotos, I. Moscholios, and P. Sarigiannidis, "Drones in B5G/6G Networks as Flying Base Stations," *Drones*, vol. 6, no. 2, 2022.

[4] A. Dutta and E. Hammad, "5G Security Challenges and Opportunities: A System Approach," in *2020 IEEE 3rd 5G World Forum (5GWF)*, pp. 109–114, 2020.

[5] F. Rebecchi, A. Pastor, A. Mozo, C. Lombardo, R. Bruschi, I. Aliferis, R. Doriguzzi-Corin, P. Gouvas, A. Alvarez Romero, A. Angelogianni, I. Politis, and C. Xenakis, "A Digital Twin for the 5G Era: the SPIDER Cyber Range," in *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, pp. 567–572, 2022.

[6] C. Liu, Y. Xie, H. Li, Y. Wang, and Y. Zhang, "A Framework for Assessing the Resilience of 5G Mobile Communication Networks," in *2022 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, pp. 1077–1081, 2022.

[7] G. Iashvili, M. Iavich, R. Bocu, R. Odarchenko, and S. Gnatyuk, "Intrusion Detection System for 5G with a Focus on DOS/DDOS Attacks," in *2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, vol. 2, pp. 861–864, 2021.

[8] T. A. Ahanger and A. Aljumah, "Internet of Things: A Comprehensive Study of Security Issues and Defense Mechanisms," *IEEE Access*, vol. 7, pp. 11020–11028, 2019.

[9] A. Shorov, "5G Testbed Development for Network Slicing Evaluation," in *2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, pp. 39–44, 2019.

[10] F. J. De Souza Neto, E. Amatucci, N. A. Nassif, and P. A. Marques Farias, "Analysis for Comparison of Framework for 5G Core Implementation," in *2021 International Conference on Information Science and Communications Technologies (ICISCT)*, pp. 1–5, 2021.

[11] C. V. Nahum, L. De Nóvoa Martins Pinto, V. B. Tavares, P. Batista, S. Lins, N. Linder, and A. Klautau, "Testbed for 5G Connected Artificial Intelligence on Virtualized Networks," *IEEE Access*, vol. 8, pp. 223202–223213, 2020.

[12] S. Gupta, B. L. Parne, and N. S. Chaudhari, "Security Vulnerabilities in Handover Authentication Mechanism of 5G Network," in *2018 First International Conference on Secure Cyber Computing and Communication (ICSCCC)*, pp. 369–374, 2018.

[13] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," in *2017 IEEE Conference on Standards for Communications and Networking (CSCN)*, pp. 193–199, 2017.

[14] S. Vakaruk, A. Mozo, A. Pastor, and D. R. López, "A digital twin network for security training in 5g industrial environments," in *2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI)*, pp. 395–398, 2021.

[15] G. Amponis, P. Radoglou-Grammatikis, G. Nakas, M. Zevgara, S. Giannakidou, S. Ouzounidis, G. Kakamoukas, and A. Sarigiannidis, "5GC PFCP Intrusion Detection Dataset," 2023.

[16] P. Kiri Taksande, P. Jha, A. Karandikar, and P. Chaporkar, "Open5G: A Software-Defined Networking Protocol for 5G Multi-RAT Wireless Networks," in *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pp. 1–6, 2020.

[17] K.-L. Lee, C.-N. Lee, and M.-F. Lee, "Realizing 5G Network Slicing Provisioning with Open Source Software," in *2021 Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (APSIPA ASC)*, pp. 1923–1930, 2021.

[18] V. Q. Rodriguez, F. Guillemin, and A. Boubendir, "Automating the deployment of 5G Network Slices using ONAP," in *2019 10th International Conference on Networks of the Future (NoF)*, pp. 32–39, 2019.

[19] J. Aiken and S. Scott-Hayward, "Investigating Adversarial Attacks against Network Intrusion Detection Systems in SDNs," in *2019 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN)*, pp. 1–7, 2019.

[20] "Interface between the Control Plane and the User Plane nodes," Tech. Rep. TS 29.244, 3GPP, 2020-11.

[21] P. R. Grammatikis, P. Sarigiannidis, C. Dalamagkas, Y. Spyridis, T. Lagkas, G. Efstathopoulos, A. Sesis, I. L. Pavon, R. T. Burgos, R. Diaz, A. Sarigiannidis, D. Papamartzivanos, S. A. Menesidou, G. Ledakis, A. Pasias, T. Kotsiopoulos, A. Drosou, O. Mavropoulos, A. C. Subirachs,

P. P. Sola, J. L. Domínguez-García, M. Escalante, M. M. Alberto, B. Caracuel, F. Ramos, V. Gkioulos, S. Katsikas, H. C. Bolstad, D.-E. Archer, N. Paunovic, R. Gallart, T. Rokkas, and A. Arce, "SDN-Based Resilient Smart Grid: The SDN-microSENSE Architecture," *Digital*, vol. 1, no. 4, pp. 173–187, 2021.