TU WIEN Informatics

Countering SUCI-Catcher

Practical Implementation, Evaluation and Mitigation Against SUCI Replay Attacks in 5G Networks

DIPLOMARBEIT

zur Erlangung des akademischen Grades

Diplom-Ingenieur

im Rahmen des Studiums

Software Engineering und Internet Computing

eingereicht von

Maximilian Braunschmied, BSc
Matrikelnummer 01633001

an der Fakultät für Informatik

der Technischen Universität Wien

Betreuung: Univ.Prof. Dipl.-Ing. Dr.techn. Thomas Grechenig

Wien, 11. April 2025

Maximilian Braunschmied

Thomas Grechenig

Technische Universität Wien
A-1040 Wien ▪ Karlsplatz 13 ▪ Tel. +43-1-58801-0 ▪ www.tuwien.at

Informatics

Countering SUCI-Catcher

Practical Implementation, Evaluation and Mitigation Against SUCI Replay Attacks in 5G Networks

DIPLOMA THESIS

submitted in partial fulfillment of the requirements for the degree of

Diplom-Ingenieur

in

Software Engineering and Internet Computing

by

Maximilian Braunschmied, BSc
Registration Number 01633001

to the Faculty of Informatics

at the TU Wien

Advisor: Univ.Prof. Dipl.-Ing. Dr.techn. Thomas Grechenig

Vienna, April 11, 2025

Maximilian Braunschmied

Thomas Grechenig

Erklärung zur Verfassung der Arbeit

Maximilian Braunschmied, BSc

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst habe, dass ich die verwendeten Quellen und Hilfsmittel vollständig angegeben habe und dass ich die Stellen der Arbeit – einschließlich Tabellen, Karten und Abbildungen –, die anderen Werken oder dem Internet im Wortlaut oder dem Sinn nach entnommen sind, auf jeden Fall unter Angabe der Quelle als Entlehnung kenntlich gemacht habe.

Wien, 11. April 2025

Maximilian Braunschmied

Danksagung

An dieser Stelle möchte ich mich bei allen bedanken, die mich während der Entstehung dieser wissenschaftlichen Arbeit unterstützt haben.

Mein besonderer Dank gilt Thomas Grechenig und Clemens Hlauschek für die fortlaufende Betreuung und Unterstützung, die konstruktiven Rückmeldungen sowie die fachliche Begleitung meiner Arbeit. Ebenso danke ich dem ESSE (Establishing Security) Team, insbesondere für die Bereitstellung der benötigten Hardware, die für die Durchführung des praktischen Teils von zentraler Bedeutung war.

Ein großer Dank geht auch an meine Familie, die mir mein Studium überhaupt erst ermöglicht hat. Eure Unterstützung – vor allem in der Anfangszeit meines Studiums – hat mir viele Lasten abgenommen. Ihr habt mir mit Geduld und Verständnis zur Seite gestanden, was für mich von unschätzbarem Wert war. Besonders möchte ich meiner Partnerin Dušica danken, die in schwierigen Phasen mein Fels in der Brandung war – und das Wort *Diplomarbeit* sicherlich mehr als nur einmal zu viel gehört hat. Auch meinem Hund Buddy gilt mein Dank: Er hat mich zuverlässig zu wohlverdienten Pausen in der Natur gezwungen und so für Ausgleich gesorgt.

Ich danke auch meinen Freunden, insbesondere Bernhard und Alex, die ich ohne mein Studium wohl nie kennengelernt hätte und mit denen vor allem der Studienbeginn deutlich leichter fiel.

Abschließend möchte ich meine Dankbarkeit dafür ausdrücken, in einem politischen System leben zu dürfen, das Bildung fördert und unterstützt. Die finanzielle Hilfe durch das Studienabschlussstipendium hat es mir ermöglicht, mich voll und ganz auf diese Arbeit zu konzentrieren.

Acknowledgements

I would like to take this opportunity to thank everyone who supported me during the development of this scientific work.

My special thanks go to Thomas Grechenig and Clemens Hlauschek for their ongoing support, constructive feedback and expert guidance. I would also like to thank the ESSE (Establishing Security) team, especially for providing the necessary hardware, which was of central importance for carrying out the practical part.

A big thank you goes to my family, who made my studies possible in the first place. Your support – especially at the beginning of my studies – took a lot of the burden off my shoulders. You stood by me with patience and understanding, which was invaluable to me. I would especially like to thank my partner Dušica, who has been my rock in difficult phases – and has certainly heard the word *thesis* more than one too many times. I would also like to thank my dog Buddy: he reliably forced me to take well-deserved breaks in nature, providing me with balance.

I would also like to thank my friends, especially Bernhard and Alex, whom I would probably never have met without my studies and with whom, above all, the start of my studies was much easier.

Finally, I would like to express my gratitude for being able to live in a political system that promotes and supports education. The financial help provided by the graduation scholarship has enabled me to concentrate fully on this work.

Kurzfassung

Die fünfte Generation von Mobilfunknetzen (5G) bringt gegenüber ihrem Vorgänger, Long Term Evolution (LTE), bedeutende Verbesserungen mit sich, insbesondere im Hinblick auf den Datenschutz von Netzwerkteilnehmern. Eine zentrale Neuerung ist die Einführung des Subscription Concealed Identifier (SUCI), welche die dauerhafte Teilnehmerkennung, den International Mobile Subscriber Identity (IMSI), durch Public-Key-Verschlüsselung schützt. Damit wird eine bekannte Schwachstelle früherer Mobilfunkgenerationen adressiert, bei der Angreifer mittels sogenannter IMSI-Catcher die im Klartext übermittelten IMSIs abfangen und zur Ortung und Identifikation von Nutzern verwenden konnten. Obwohl der SUCI den Datenschutz in Mobilfunknetzwerken erheblich verbessert, haben aktuelle Studien Schwachstellen in seiner praktischen Umsetzung aufgezeigt – insbesondere den sogenannten SUCI-Catcher-Angriff.

Diese Arbeit untersucht bestehende Datenschutzlücken in 5G-Netzen mit besonderem Fokus auf den SUCI-Catcher-Angriff. In einer kontrollierten 5G-Testumgebung demonstrieren wir, wie ein Angreifer SUCI-Werte abfangen und das Authentifizierungsprotokoll 5G Authentication and Key Agreement (5G-AKA) ausnutzen kann, um Netzwerkteilnehmer zu deanonymisieren. Darüber hinaus analysieren wir von 3rd Generation Partnership Project (3GPP) vorgeschlagene Gegenmaßnahmen und zeigen deren Einschränkungen auf – insbesondere im Hinblick auf die Erkennung von SUCI-Replay-Angriffen.

Als Reaktion auf diese Schwächen entwickeln und implementieren wir eine neuartige, netzwerkseitige Abwehrstrategie innerhalb eines Open-Source-5G Core Network (5GC). Unsere Lösung erkennt erfolgreich eine Variante des SUCI-Catcher-Angriffs, verursacht keine nennenswerten Leistungseinbußen, erfordert keine Änderungen auf der Client-Seite und bleibt vollständig kompatibel mit bestehenden 5G-Standards und -Infrastrukturen.

Diese Arbeit leistet einen Beitrag zur Weiterentwicklung der 5G-Sicherheit, indem sie eine umfassende Analyse von Datenschutzrisiken für Netzwerkteilnehmer liefert und eine praxistaugliche, standardkonforme Gegenmaßnahme für einen Angriff vorstellt.

Keywords: *5G*, *SUCI-Catcher*, *Bloom Filter*, *Security*, *Privacy*, *Open5GS*, *srsRAN*

Abstract

The fifth generation of mobile networks (5G) introduces substantial improvements over its predecessor, Long Term Evolution (LTE), particularly in the area of subscriber privacy. A key enhancement is the introduction of the Subscription Concealed Identifier (SUCI) mechanism, a privacy feature which protects the subscriber's permanent identifier, the International Mobile Subscriber Identity (IMSI), through public key encryption. This addresses a well-known vulnerability in previous network generations where attackers could easily track network subscribers by capturing IMSIs transmitted in plaintext using IMSI-Catchers. While the introduction of the SUCI significantly improves privacy, recent research has identified weaknesses in its implementation, including the emergence of the SUCI-Catcher attack.

This thesis explores privacy vulnerabilities in 5G networks, with a particular focus on the SUCI-Catcher attack. Within a controlled 5G network environment, we demonstrate how an adversary can intercept SUCI values and exploit the 5G Authentication and Key Agreement (5G-AKA) to deanonymize subscribers. We also analyze mitigation approaches proposed by the 3rd Generation Partnership Project (3GPP), highlighting their limitations – with respect to SUCI replay detection.

To address these shortcomings, we propose and implement a novel, network-sided mitigation strategy within an open-source 5G Core Network (5GC). Our solution successfully detects a variant of the SUCI-Catcher attack without imposing significant performance overhead or requiring changes on the client side, while preserving full compatibility with existing 5G standards and infrastructure.

This research contributes to the ongoing development of 5G security by providing an in-depth analysis of subscriber privacy risks and presenting a practical, non-intrusive countermeasure.

Keywords: *5G*, *SUCI-Catcher*, *Bloom Filter*, *Security*, *Privacy*, *Open5GS*, *srsRAN*

Contents

CHAPTER 1

Introduction

This chapter provides an introduction to the thesis. It begins with a presentation of the SUCI-Catcher vulnerability in 5G networks and the privacy implications that motivate this research. This is followed by a definition of the specific objectives of the thesis and an outline of the research methodology used. The chapter concludes with a structural overview of the thesis.

1.1 Problem Statement and Motivation

The emergence of 5G technology signifies an advancement in the field of telecommunications, offering improvements in data transmission rates, reliability as well as connectivity. Additionally, security enhancements have been implemented to address some threats faced in former mobile network generations. Among these improvements is the protection of the permanent subscriber identity, the International Mobile Subscriber Identity (IMSI). It is replaced by the Subscription Concealed Identifier (SUCI) as the unique identifier for a subscriber in 5G networks. The SUCI provides a mechanism to encrypt parts of the subscriber identifier, thus protecting the confidentiality of initial messages between a phone and the network. As a result, tracking subscribers using former attack methodologies is not possible anymore in 5G networks; impeding the use of IMSI-Catchers, surveillance devices used to intercept and track mobile phone communications. In the past these devices have been used by public authorities such as the swedish police [Naa16] to track individuals, leading to potential misuse and abuse.

Despite those measures taken, proof-of-concept studies [CRPH21, HEC^{+}19, PMN21] have shown that the newly introduced SUCI is insufficient for protecting the subscriber's privacy from malicious parties. Chlosta et al. [CRPH21] have demonstrated that it is still possible to deanonymize network participants using the SUCI-Catcher attack. Although their proof-of-concept attack requires significantly more effort than conventional IMSI-Catchers in older generations of networks, it is particularly suitable for tracking selected persons of interest. Ultimately, this poses a significant threat to the privacy and security of mobile phone users in 5G networks.

1.2 Aim of the Thesis

The aim of this thesis is to develop an effective solution to mitigate the SUCI-Catcher attack identified by Chlosta et al. [CRPH21]. This includes the evaluation of existing mitigation approaches, analyzing their respective strengths and limitations. The author aims to design a mitigation strategy that addresses identified shortcomings, followed by a practical implementation within an open-source core network to demonstrate its effectiveness and feasibility.

1.3 Methodology

The goals outlined in Section 1.2 will be accomplished through a systematic methodology involving following key steps:

1. **Research and Literature Review**: Conduct an extensive literature review to understand existing attacks targeting subscriber privacy. The focus will be on Long Term Evolution (LTE) and 5G vulnerabilities. This will serve as the foundation for the research.

2. **Setup of 5G Network Environment**: Establish a simulated 5G Standalone (SA) network environment by setting up a Base Station (BS) a Core Network (CN) and User Equipment (UE). This not only allows for replicating a real-world scenario, but also provides an environment for controlled experimentation.

3. **Attack Simulation**: Execute the SUCI-Catcher attack within the simulated 5G environment to assess its feasibility.

4. **Attack Mitigation**: Based on the findings, propose mitigation strategies aimed at neutralizing the identified vulnerabilities. This includes the identification of gaps and limitations in existing approaches. Ultimately, modifications are implemented in the code base of the open-source software used for network simulation.

5. **Mitigation Evaluation**: Identify potential shortcomings of the proposed mitigation approach through analysis and recommend improvements that could address remaining limitations.

6. **Documentation and Reporting**: Document the findings as well as the proposed solution approach comprehensively in the master thesis.

1.4 Structure of the Thesis

The thesis is structured as follows: Chapter 2 provides essential background information, summarizing the evolution of mobile network generations and their security mechanisms throughout the years, with particular emphasis on LTE and 5G. Chapter 3 presents an evaluation of subscriber privacy in current 5G networks, describing deanonymization attacks and analyzing their underlying vulnerabilities, while evaluating general enhancements to address these issues. Chapter 4 focuses on the practical aspects of the research, demonstrating the replication of the SUCI-Catcher attack within a simulated 5G network environment. Chapter 5 concentrates on the mitigation of the SUCI-Catcher attack. This includes the implementation of the author's own mitigation strategy. Chapter 6 contextualizes the research by reviewing related work in the field, and Chapter 7 presents the conclusions and outlines directions for future research.

CHAPTER 2

Background

This chapter provides the foundation for understanding mobile network security. It begins with an overview of mobile network generations, from early systems to current technologies, examining the evolution of authentication procedures and security architectures. The focus lies on Long Term Evolution (LTE) and 5G networks. The chapter then proceeds to analyze signaling protocols, highlighting their roles in secure communications within the mobile network. This background information serves as a prerequisite for understanding the security challenges and solutions discussed in subsequent chapters.

2.1 Legacy Network Technologies

Mobile communications technology has evolved through several generations over the last few decades. Currently, the fourth and fifth generations are the most widely used worldwide, while older generations are gradually disappearing. This section provides a brief overview of the older generations of mobile networks, from the first to the third generation, and their security.

2.1.1 First Generation (1G)

1G refers to the first generation of mobile communications and was introduced in the 1980s. Data transmission on 1G networks was analogue and lacked any security measures. Text messaging (SMS) was not possible under 1G, only voice calls could be made. The last operating 1G network was reportedly shut down in Russia in 2017 [Lip].

2.1.2 Global System for Mobile Communications (2G)

The second generation (2G), also known as Global System for Mobile Communication (GSM), was introduced in 1991. It introduced the transmission of text, multimedia messages (MMS) and data.

GSM improved network security by introducing authentication and encryption algorithms into its protocol. Most of its cryptographic algorithms were not publicly disclosed, following the principle of *Security through obscurity*[1]. This proved to be a problem for the security of GSM, and as a result its algorithms are not considered secure today [TB08]. For example, A5/1, the stream cipher used to encrypt over-the-air transmissions in GSM, has been cracked in real time using a set of rainbow tables [Noh]. In addition, the authentication process in GSM networks is one-way, requiring the subscriber to authenticate to the network, but not vice versa [CMP13]. This poses a significant risk of Man-in-the-Middle (MitM) attacks (see Section 3.3.3).

Although GSM is now considered insecure and a generally outdated technology, there are no plans to shut down GSM networks in Austria [Pro]. The main reason for this is their wide coverage and availability in rural areas.

2.1.3 Universal Mobile Telecommunications System (3G)

The third generation (3G), also known as Universal Mobile Telecommunications System (UMTS), was introduced in 2000. The goal of UMTS was to offer increased data rates as well as significantly improved audio and video transmission capabilities.

UMTS was based on the security architecture of GSM but had several improvements, such as the integration of the Authentication and Key Agreement (AKA). The AKA enables mutual authentication of the handset and the network combating man-in-the-middle attacks and the use of false base stations [CMP13]. Additionally, integrity protection was introduced to the entirety of signalling messages, significantly improving the security of UMTS by preventing message tampering [3GP22d].

2.2 Long Term Evolution (4G)

Long Term Evolution (LTE) or 4G was introduced around 2010. It represents a radical step in mobile network technology, aiming to provide a highly efficient, low-latency, packet-optimized and more secure service. At the network layer, LTE is based on Internet Protocol (IP).

2.2.1 Network Architecture

A LTE network involves three major components for the establishment of signaling protocols between a subscriber and a Base Station (BS):

- The Evolved Packet Core (EPC) which manages core network functions.
- The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) which handles radio communications.

[1] Security through obscurity is the reliance on secrecy as the primary method of providing security to a system.

- The User Equipment (UE) which is the subscriber's device connecting to the network.

Evolved Packet Core (EPC)

The EPC, the Core Network (CN) of LTE, consists of the following components [3GP22c]:

- The Mobility Management Entity (MME) facilitates the authentication and allocation of resources to UEs. It is used for Control Plane (CP) messages between the UE and the network.
- The Home Subscriber Server (HSS) contains subscription-related information, such as identifiers or cryptographic keys, used to handle calls and sessions within the network.
- The Serving Gateway (SGW) is used for signalling conversion and the routing of IP packets between UE and the network. Unlike the MME, the SGW handles User Plane (UP) messages.
- The Packet Data Network Gateway (PDN-GW) connects the EPC to external IP networks.
- The Policy and Charging Rules Function (PCRF) is responsible for the Quality of Service (QoS) of the LTE network. It ensures that subscribers receive services and are charged accordingly.

Evolved Universal Terrestrial Radio Access Network (E-UTRAN)

The E-UTRAN, also referred to as the Radio Access Network (RAN), handles communication between the UE and the EPC. It is composed out of multiple Base Stations (BSs). In LTE architecture, a BS is specifically designated as a Evolved Node B (eNB). Each eNB is responsible for critical functions including data connectivity, over-the-air security implementation, radio resource management, as well as managing handovers[2] and location updates. eNBs maintain connections with both the MME and the SGW, serving as the interface between a UE and the CN. [Vac19]

User Equipment (UE)

The UE refers to the subscriber's communication device, typically a smartphone. Each UE contains a Universal Subscriber Identity Module (USIM) which securely stores authentication credentials and subscriber-specific information. Among the subscriber information stored are various identifiers used for secure and efficient communication with

[2] Handover refers to the process of transferring an ongoing communication session from one base station to another without interruption.

the network. The identifiers play a crucial role in authentication and session management procedures. They are specified in the following section.

2.2.2 Identifiers

In mobile networks, identifiers serve the function of uniquely identifying and addressing both the UE and and its USIM. The LTE architecture employs two categories of identifiers: long-term (permanent) and short-term (temporary) identifiers. Permanent identifiers, including the International Mobile Equipment Identifier (IMEI) and the International Mobile Subscriber Identity (IMSI), contain sensitive subscriber information and are therefore not intended to be transmitted in clear over the air interface. This serves as a privacy protection measure for subscribers, as will be shown later in the thesis. Temporary identifiers, including the Globally Unique Temporary ID (GUTI), are used for the majority of communications. This section gives an overview of the identifiers used in LTE networks.

Mobile Subscriber Integrated Services Digital Network Number (MSISDN)

The Mobile Station International Subscriber Directory Number (MSISDN), also referred to as Generic Public Subscription Identifier (GPSI), serves as the primary public identifier for a subscriber. Within the network system, a secure mapping is maintained between the MSISDN and the IMSI, enabling the routing of communication. The MSISDN is composed of a country code, indicating where the USIM is registered, a network code that identifies the network operator providing the service and a unique subscriber number that identifies the user within the network. [3GP23]

International Mobile Equipment Identity (IMEI)

The IMEI is a 15-digit number that uniquely identifies each UE in mobile networks. It serves as a device fingerprint that is independent of subscriber information and enables the network operator to trace the equipment to its origin of production. The IMEI encodes device attributes, such as the device's country of origin, the manufacturer and specific model number. [3GP22b]

International Mobile Subscriber Identity (IMSI)

The IMSI is a 15-digit number that uniquely identifies each subscriber within mobile networks. Unlike the MSISDN, which serves as the public contact point, the IMSI functions as the private identity of a USIM. It used for authentication and authorization within the network. According to TS 123 003 [3GP23], the IMSI is composed of three parts, namely:

- The Mobile Country Code (MCC), a three-digit number that uniquely identifies the network's country of operation.

- The Mobile Network Code (MNC), a two or three-digit number that uniquely identifies the network's operator within the MCC.
- The Mobile Subscriber Identification Number (MSIN), a 9 or 10 digit number that identifies a subscriber within the network.

The combination of MCC and MNC is also referred to as the Public Land Mobile Network (PLMN) or the Home Network Identity (HNI). The structure of the IMSI is illustrated in Fig. 2.1.

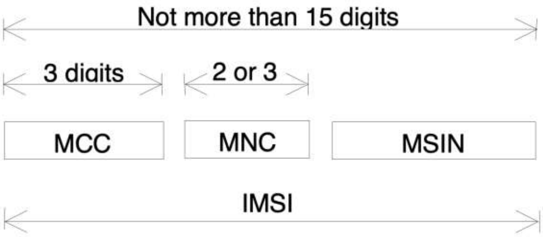

Figure 2.1: The structure of the IMSI. [3GP23]

Globally Unique Temporary Identifier (GUTI)

The GUTI serves as a temporary identifier designed to protect the subscriber's identity in LTE networks. It is assigned to the UE by the serving MME only after the security context has been established through the authentication procedure. Following this, the GUTI replaces the permanent identifiers in all subsequent communication between the network and the UE.

The GUTI consists of two components [3GP23]:

- The Globally Unique Mobility Management Entity Identifier (GUMMEI) combines the PLMN and the Mobile Management Entity ID (MME ID) – a code that specifically identifies the MME that assigned the current GUTI to the UE.
- The MME-Temporary Mobile Subscriber Identity (M-TMSI) is a temporary value that identifies the UE within its assigned MME.

To enhance subscriber privacy, the MME refreshes the GUTI on a regular basis [HBK18]. This is also referred to as *GUTI reallocation*. In TS 124 301 [3GP24e], the 3GPP recommends reallocating the GUTI in following situations:

- When the UE processes the attachment procedure or the update location procedure.
- When the GUTI provided by the UE was assigned by another MME, i.e. the MME changes.
- When the network issues the `GUTI reallocation` command.

2.2.3 Authentication

Similarly to the AKA in UMTS, LTE implements the Evolved Packet System Authentication and Key Agreement (EPS-AKA) protocol to ensure mutual authentication between the network and the UE. The EPS-AKA has two primary objectives [PGBBM21]:

1. To derive a set of ephemeral keys used for encrypting the exchanged traffic and ensuring its integrity.
2. To create the GUTI.

The EPS-AKA is based on the challenge-response mechanism where the challenge consists of a random number (RAND) and the authentication token (AUTH). The detailed protocol operation is described below.

EPS Authentication and Key Agreement (EPS-AKA)

As illustrated in Fig. 2.2, the EPS-AKA authentication procedure follows these steps [PGBBM21]:

1. The UE initiates the process by sending an `Attach Request` to the MME. In the initial `Attach Request` the UE sends its IMSI, in any subsequent communication its previously assigned GUTI is used.
2. The MME forwards an `Authentication Request` to the HSS, containing the UE's identifier (either IMSI or GUTI) along with its own network identifier.
3. The HSS generates multiple Authentication Vectors (AVs) using the UE's secret key (K_i) and transmits these back to the MME within an `Authentication Response` message.
4. From the received vectors, the MME extracts the AUTH token and the Expected Response (XRES) field. The MME then forwards the AUTH token to the UE.
5. The UE uses the copy of K_i that is stored within its USIM to verify the received AUTH token. If the verification succeeds, the UE generates a Response (RES) and sends it back to the MME.
6. The MME compares the received RES with its stored XRES. If the values match, the authentication is considered mutually successful, and both entities generate and cache the UE's GUTI for subsequent communications. If authentication fails (RES does not match XRES), the UE marks the cell as barred for a specified duration, preventing further connection attempts to that cell [PGBBM21].

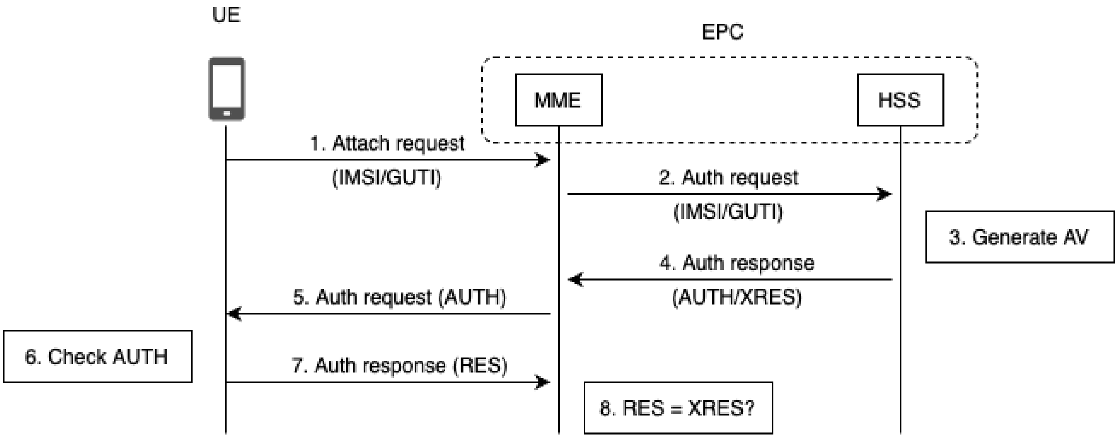

Figure 2.2: The EPS-AKA protocol of the LTE network.

2.3 5G New Radio

5G is the fifth-generation mobile communication standard and the most advanced wireless technology currently in commercial deployment. Its global rollout began in 2019 [Tea], introducing significant improvements over its predecessor LTE. 5G offers a higher bandwidth and connectivity improving the quality of internet services in densely populated areas. In addition, the 5G standard reduces end-to-end latency meeting the needs of time-sensitive applications. The core radio technology used in 5G, New Radio (NR), has been established as the global standard for a unified air interface.

Release 15 defines the specifications for the first phase of 5G and represents the baseline of the protocol, while Release 18, also known as 5G-Advanced, is still under development. Release 17 defines the latest specification to be used in commercial networks. [3GP]

2.3.1 Network Architecture

5G networks can be deployed in two architectural configurations, according to TS 123 501 [3GP24c]: Standalone (SA) and Non-Standalone (NSA). In the NSA implementation, the network utilizes a 5G-RAN while maintaining an LTE CN. This hybrid approach simplifies the deployment of 5G by leveraging existing LTE infrastructure. As a result, 5G-NSA networks do not adopt the advanced authentication mechanisms and security improvements associated with the full 5G standard.

On the other side, the SA configuration represents a full end-to-end 5G network, comprising both a 5G-RAN and a dedicated 5GC and fully implementing the enhanced authentication and security protocols defined in the 5G specifications.

UEs operating within 5G-NSA networks maintain the ability to connect to both LTE and 5G BSs. In this architecture, the LTE infrastructure typically handles the Control Plane (CP) functions (signaling, authentication, mobility management), while the 5G infrastructure handles the User Plane (UP) functions. The two architectural configurations are illustrated in Fig. 2.3.

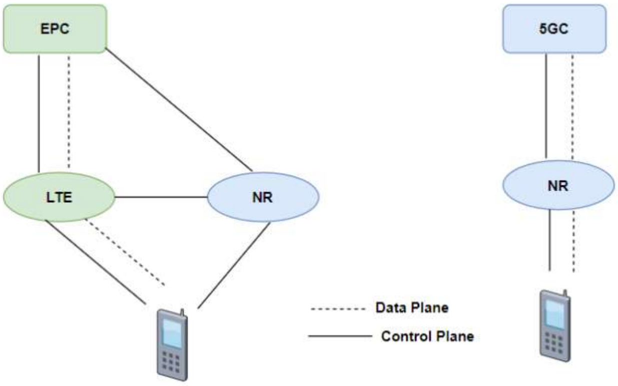

Figure 2.3: The two architectural configurations in 5G: Non-Standalone is displayed on the left, Standalone on the right. [FO22]

Similar to the LTE architecture, a 5G network can be conceptually broken down into three primary components:

- The 5G Radio Access Network (5G-RAN).
- The 5G Core Network (5GC)
- The User Equipment (UE).

Alternatively, it can be divided into the Serving Network (SN), the Home Network (HN) and the User Equipment (UE). In this case, the HN represents the network operator with whom the subscriber has established a service contract and that maintains its credentials. The SN refers to the network infrastructure, including the BSs the UE connects to. [3GP24c]

5G Radio Access Network (5G-RAN)

In 5G architecture, a BS is referred to as Next-Generation Node B (gNB). In a 5G-SA network, the 5G-RAN consists of several gNBs, in a 5G-NSA network it may contain both gNBs and eNBs. Most of the 5G-RAN's functionality is similar to the E-UTRAN in LTE. There are some advancements, such as the support for network slicing which enables the creation of multiple logical networks within a single physical network infrastructure [3GP23].

5G Core Network (5GC)

In contrast to the EPC in LTE, the 5GC implements a service-oriented architecture. In this architecture, each component is referred to as a Network Function (NF) which provides its services to other authorized NFs through standardized interfaces. An innovation in 5G is the clear separation of CP functions are from UP functions, enabling independent scalability and decoupled technical evolution [Bro17].

The 5GC contains following key components [3GP24c]:

- The Access and Mobility Management Function (AMF) is the primary entry point for the UE in the 5GC and responsible for managing access and mobility:
  - The AMF hosts the Security Anchor Function (SEAF) which acts as the middleman between the UE and its HN.
- The Authentication Server Function (AUSF) executes the authentication process with the UE.
- The Unified Data Management (UDM) hosts two key functions:
  - The Authentication Credential Repository and Processing Function (ARPF) selects the authentication method and computes the authentication vectors and keying material for the AUSF.
  - The Subscription Identifier De-concealing Function (SIDF) decrypts the SUCI to retrieve the UE's SUPI. It is the only entity with access to the private key used for decryption. In Section 2.3.2, the SUPI and SUCI are specified.
- The Policy Control Function (PCF) is responsible for the QoS of the 5G network, enforcing network policies and service-level agreements.

User Equipment (UE)

The UE in 5G is enhanced to support the protocol's improved speeds and features. Its USIM holds new identifiers (see Section 2.3.2) that play a crucial role in the authentication and communication within the 5G network.

2.3.2 Identifiers

In addition to maintaining compatbility with identifiers from previous generations, the 5G standard introduces significant enhancements to subscriber privacy through two new identifiers:

1. The Subscription Permanent Identifier (SUPI).
2. The Subscription Concealed Identifier (SUCI).

The GUTI is replaced by the 5G Globally Unique Temporary Identifier (5G-GUTI).

Subscription Permanent Identifier (SUPI)

Under 5G the SUPI replaces the IMSI as the subscriber's permanent identity. The SUPI can exist in one of two formats: It may either be an IMSI (maintaining compatibility with previous network generations) or take the form of a Network Access Identifier (NAI). Except for a few individual cases (see Section 2.3.2, SUCI), the SUPI shall never be transmitted in plaintext. [3GP24b]

Subscription Concealed Identifier (SUCI)

The Subscription Concealed Identifier (SUCI) is a privacy preserving identifier, containing an enciphered version of the SUPI. Using an Elliptic Curve Integrated Encryption Scheme (ECIES)-based protection scheme, either the UE or its USIM generate the SUCI with the public key of its corresponding HN.

According to TS 133 501 [3GP24b], the SUCI is composed of following fields:

- SUCI Type – This field indicates the type of SUCI, i.e. whether it's an IMSI or a NAI.
- Home Network Identifier – This field identifies the HN of the subscriber. This corresponds to the PLMN in case the SUCI type is of the form IMSI.
- Routing Indicator – This field is used for selecting the right UDM or AUSF for serving a subscriber.
- Protection Scheme ID – This field refers to the protection scheme used to generate the SUCI. There are following values defined:
    - Null Scheme – This scheme does not conceal the SUPI and thus provides no privacy protection.
    - Profile A & Profile B – These schemes rely on the ECIES but differ in the parameters used. The specifics can be found in TS 33.501 C.3.4.1 and C.3.4.2 [3GP24b], respectively.
- Home Network Public Key ID – This field indicates the public/private key pair used for concealment and deconcealment of the SUPI. It is set to 0, when the Null Scheme is used.
- Scheme Output – Depending on the used protection scheme, this field consists of a string of characters with variable length. It represents the output of the SUPI concealment. [3GP23]

There are cases in which the UE shall generate a SUCI using the Null Scheme [3GP24b]:

- The UE initiates an unauthenticated emergency session and does not have a 5G-GUTI that is consistent with the given PLMN.
- The HN has been configured to use the Null Scheme.
- The HN has not provisioned a public key for generating the SUCI.

The structure of the SUCI is shown in Fig. 2.4.

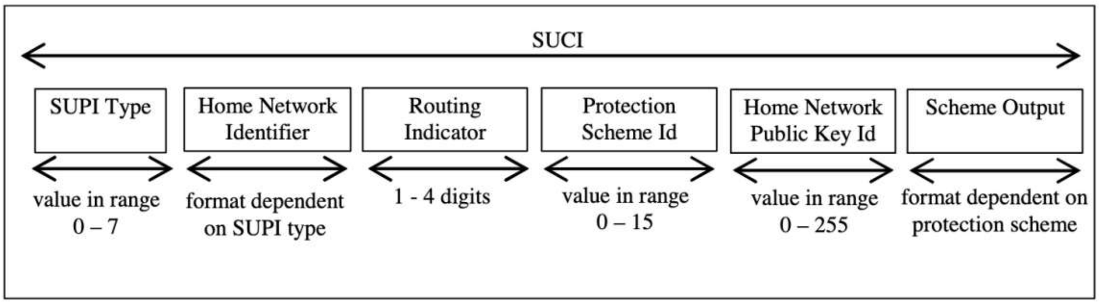

Figure 2.4: The structure of the SUCI. [3GP23]

5G Globally Unique Temporary Identifier (5G-GUTI)

The 5G-GUTI serves as the evolved counterpart to the GUTI in LTE networks. It is assigned to the UE by the AMF only after a security context has been established through authentication. The 5G-GUTI is composed of following two components [3GP24b]:

- The Globally Unique AMF Identifier (GUAMI) is constructed from the PLMN and the AMF Identifier (AMFI). The AMFI identifies the AMF that assigned the current 5G-GUTI to the UE.
- The 5G-TMSI, a temporary value used for identifying the UE within the assigned AMF.

The 5G-TMSI should follow the best practices of unpredictable identifier generation. The 5G S-Temporary Mobile Subscription Identity (5G-S-TMSI) is the shortened form of the 5G-GUTI and used for optimizing signalling procedures, including Paging.

The 5G-GUTI is required to be refreshed in following situations [3GP24b]:

- When the UE sends a `Registration Request` message of the type *initial registration* or *mobility registration update*.
- When the UE sends a `Service Request` message in response to a Paging message.

Moreover, it is recommended by the 3GPP that the 5G-GUTI is refreshed in following situation [3GP24b]:

- When the UE sends a `Registration Request` message of the type *periodic registration update*.

2.3.3 Authentication

The 5G standard introduces two authentication protocols: the 5G Authentication and Key Agreement (5G-AKA) and the Extensible Authentication Protocol-AKA (EAP-AKA). While these protocols share many similarities, this analysis focuses specifically on the 5G-AKA. Like its predecessors, the 5G-AKA provides mutual authentication between the network and the UE while establishing root keys necessary for securing subsequent communication.

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

The 5G-AKA introduces several changes compared to the AKA in LTE [Cab19]:

- Service-Based Architecture: The entities involved in the authentication process differ. Particularly, 5G introduces the SIDF which does not exist in LTE.
- Subscriber Identity Protection: The UE uses the public key of the HN to encrypt its permanent identifier (see Section 2.3.2). In LTE, the permanent identifier is sent in clear before a security context is established.
- Enhanced Home Network Control: In the AKA, the network is consulted only to generate AVs. In 5G, the AUSF participates in the actual authentication decision process. The UDM receives and logs these authentication results.
- Key Hierarchy: 5G introduces a more complex key hierarchy with intermediate keys, including K_{AUSF} and K_{AMF}. This strengthens security by limiting the impact of key compromise.

As illustrated in Fig. 2.5 [Cab19] the 5G-AKA, follows these steps [3GP24b]:

1. The UE initiates the process by sending a signaling message to the SEAF. This message contains either a 5G-GUTI (if previously assigned) or a SUCI if no temporary identifier has been allocated. The message also includes the name of the SN.
2. The SEAF forwards an authentication request to the AUSF, which first verifies the authorization status of the SN.
3. Upon SN verification, the AUSF forwards the request to the UDM. Within the UDM:

   - The SIDF decrypts the SUCI to obtain the SUPI.
   - The ARPF selects the 5G-AKA as the authentication protocol and generates the 5G Home Environment Authentication Vector (5G HE AV) including the SN's name and the SUPI.

4. The UDM sends the 5G HE AV to the AUSF. The AUSF:
   - Buffers the XRES.
   - Calculates the hash of the XRES (HXRES).
   - Creates a modified authentication vector by replacing XRES with HXRES and removing K_{AUSF}.
   - Forwards the vector to the SEAF.

5. The SEAF:
   - Calculates the hash of the response (HRES) from the received RES.
   - Compares the HRES with its stored HXRES.
   - If both are matching, it forwards the RES to the AUSF.

6. The AUSF compares the RES with the stored XRES and informs the UDM of the result.

7. Upon successful authentication, the anchor key (K_{AUSF}) and the SUPI are transmitted to the SEAF. This key serves as the foundation for securing all subsequent communications between entities.

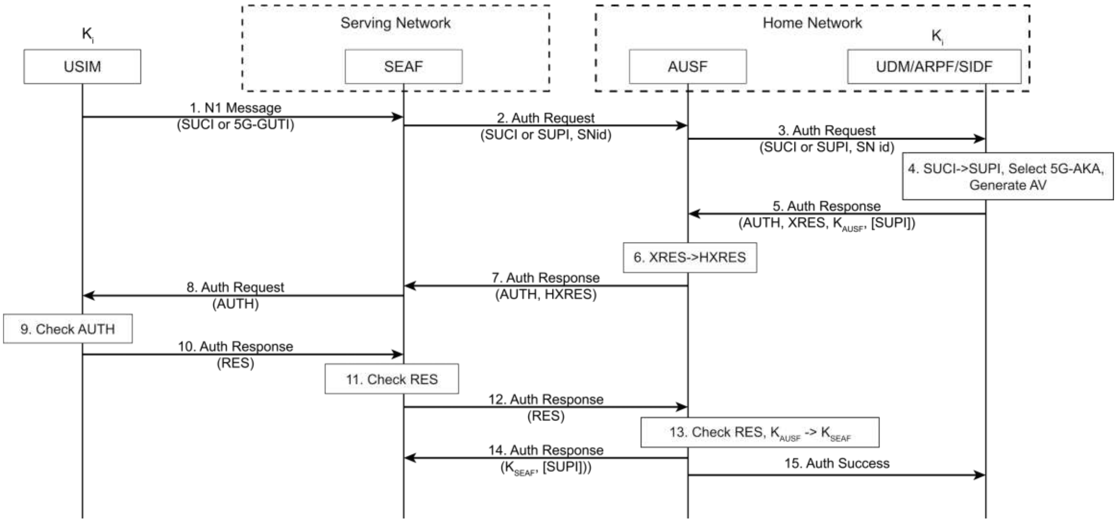
Serving Network
Home Network
K_i
USIM
SEAF
AUSF
K_i
UDM/ARPF/SIDF
1. N1 Message (SUCI or 5G-GUTI)
2. Auth Request (SUCI or SUPI, SNid)
3. Auth Request (SUCI or SUPI, SN id)
4. SUCI->SUPI, Select 5G-AKA, Generate AV
5. Auth Response (AUTH, XRES, K_AUSF, [SUPI])
6. XRES->HXRES
7. Auth Response (AUTH, HXRES)
8. Auth Request (AUTH)
9. Check AUTH
10. Auth Response (RES)
11. Check RES
12. Auth Response (RES)
13. Check RES, K_AUSF -> K_SEAF
14. Auth Response (K_SEAF, [SUPI])
15. Auth Success

Figure 2.5: The 5G-AKA protocol.

Elliptic Curve Integrated Encryption Scheme (ECIES)

The Elliptic Curve Integrated Encryption Scheme (ECIES) is implemented in 5G networks to conceal the SUPI, thereby protecting subscriber privacy. It uses several concepts from modern cryptography [3GP24b, MO19]:

- Public Key Cryptography: The ECIES maintains a long-term key pair. The USIM is pre-provisioned with the public key of the HN and the UE generates fresh ephemeral key pairs for each SUCI transmission.
- Diffie-Hellman Key Exchange: The UE uses its ephemeral private key and the public key of the HN to derive a shared secret. The HN, on the other hand, uses the ephemeral public key of the UE and its own private key to derive the same secret. In this way, keys can be exchanged without transmitting sensitive information.
- Key Derivation: The shared secret is fed into a key derivation function and produces encryption keys and Message Authentication Codes (MACs).
- Integrity Protection: Verification of the MACs ensures that the data has not been tampered with.

The ECIES and its two variants, referred to as *Profiles*, are described in TS 133 501 [3GP24b]. An illustration of the concealment of the SUPI using the ECIES is shown in Fig. 2.6.

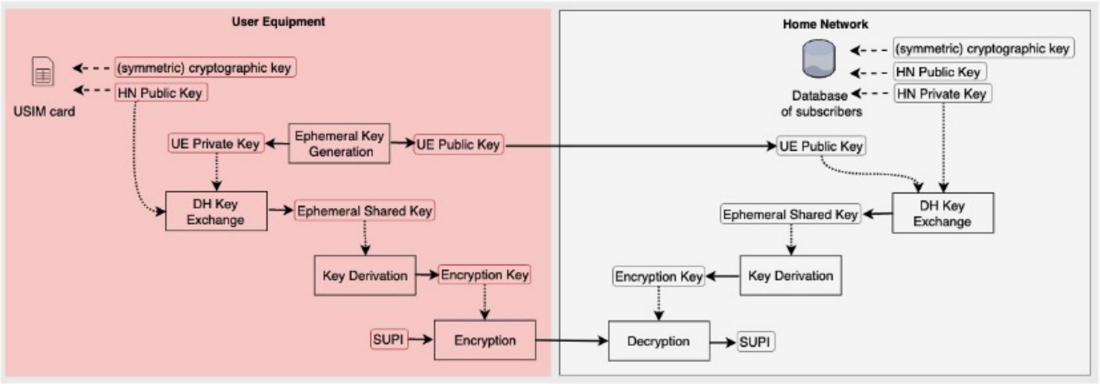

Figure 2.6: Concealment of the SUPI using the ECIES. [MO19]

2.4 Signalling Messages

In LTE and 5G, signalling procedures are essential for establishing and maintaining connections and managing mobility. These procedures represent the CP within the network architecture.

Signalling messages are composed of three parts [PBO+22]:

- Message Type: Each type serves specific functional purposes. For example, an `Identity Request` type is used by the NAS identification procedure to request identity information from the UE.
- Information Element (IE): These elements carry specific values according to their defined length and value type. Depending on the message type, a message can contain a single or multiple IEs.
- Security Components: A message is encapsuled by security components for integrity protection and encryption:
  - Security Header Type: Defines the level of protection using following values [3GP25a]:
    - 0: There is no security protection. The message is sent plain.
    - 1: The message is integrity protected.
    - 2: The message is integrity protected and ciphered.
    - 3 & 4: These values are dedicated for certain message types.
  - Message Authentication Code (MAC): If the security header type is not 0, the message contains a MAC to verify integrity.
  - Sequence Number (SQN): This number is used as a protection against replay attacks for the UE.

Among various protocols, the Non-Access Stratum (NAS) and Radio Resource Control (RRC) protocols play a crucial role in handling radio-specific functionality. Both NAS and RRC serve different functions in the network, as illustrated in Fig. 2.7.

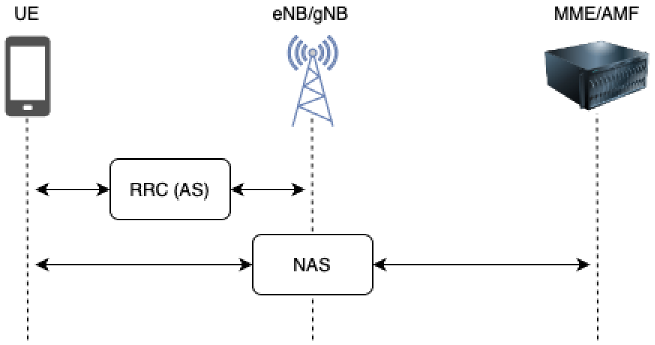

Figure 2.7: RRC and NAS signalling visualized.

2.4.1 Radio Resource Control (RRC)

The RRC represents the highest layer in the Access Stratum (AS) and controls communication between the UE and the eNB or gNB in 5G. The protocol is specified in TS 136 331 [3GP25e] for LTE and TS 138 331 [3GP25c] for 5G, respectively. The major functions of the RRC include:

- Establishment, release and reconfiguration of RRC connections.
- Broadcast of system information.
- Paging
- RRC connection mobility.

Paging

The paging procedure is described in TS 136 304 [3GP24d] for LTE and TS 138 300 [3GP25b] for 5G, respectively. Paging is used to deliver pending services, such as incoming calls or SMS messages, to the UE. This process is initiated by the CN which sends a paging request and awaits a response from the UE within a set time frame (T3413). The UE, on the other hand, listens for incoming paging messages.

Continuously monitoring the paging channels can reduce the battery life of UEs significantly. To optimize battery life, UEs operate in `RRC idle` mode, where they are not actively transmitting or receiving any data. The time interval in which the UE monitors the paging channel is referred to as Paging Occasion (PO).

Paging messages contain identifiers to target specific UEs. In LTE, the identifier is derived from the IMSI [3GP24d], while in 5G, it is derived from the 5G-S-TMSI [3GP25b]. The paging procedure is illustrated in Fig. 2.8.

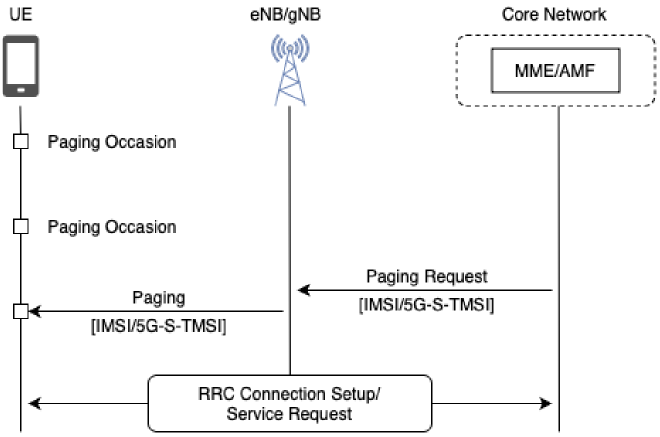

Figure 2.8: The paging procedure illustrated, adapted from Singla et al. [SHC+20].

2.4.2 Non-Access Stratum (NAS)

The NAS signalling manages communication between the UE and the MME in LTE or AMF in 5G. It is specified in TS 124 301 [3GP24e]. Its primary functions include:

1. Supporting UE mobility including common procedures such as authentication.

2. Supporting session management procedures to establish and maintain connectivity between the UE and the network.
3. Providing NAS transport procedures, such as SMS delivery.

2.4.3 Security

After successful execution of the AKA (or 5G-AKA) and establishment of a security context, signalling messages are protected according to their Security Header Type. In TS 138 331, Annex B.1 [3GP25c], the 3GPP, however, specifies several RRC and NAS messages that can be transmitted without (integrity) protection, particularly before the security activation.

CHAPTER 3

Subscriber Privacy in 5G Networks

Privacy is one of the security objectives defined by the 3GPP [3GP24b]. It encompasses the protection of users' sensitive information. This includes not only obvious personal data, but also information that can be derived from habits, profiling, tracing or inferred from location services [SRCP20]. In mobile networks, privacy is particularly important as mobile phones have become more widespread than ever before. UEs constantly exchange information that has the potential to draw conclusions about the subscriber. The aim is to protect this data from being accessed and misused by unauthorized parties. The first generation (1G) of mobile networks did not intend to provide security or privacy to its subscribers. As a result, organizations such as the 3GPP have iteratively added security and privacy features with each subsequent generation of mobile networks. These changes are recorded in reports referred to as *Releases*. Releases provide a platform for developers to implement features and allow new functionality to be added [3GP]. With Release 15, the 3GPP specified the first revision of 5G. It represents a significant step forward in terms of end-user privacy compared to previous generations of networks. This chapter assesses the current state of subscriber privacy in 5G.

3.1 Requirements

In TS 133 102 [3GP22d], the 3GPP specifies the security properties necessary to ensure subscriber privacy, or in its words *user identity confidentiality*. In particular, the 3GPP identifies three essential requirements, namely user identity confidentiality, user location confidentiality and user untraceability.

3.1.1 User Identity Confidentiality

This property defines that the persistent identity of a subscriber cannot be intercepted [3GP22d]. User identity confidentiality can be subdivided into subscriber identity confidentiality and device identity confidentiality.

Subscriber Identity Confidentiality

In subscriber identity confidentiality, threats can arise when the user's permanent subscription identifier, the IMSI in LTE or the SUPI in 5G, is exposed. An adversary could learn the IMSI of any person of interest (PoI) and thus link a subscriber's real life identity to their network subscription identity. An obvious solution to this problem would be to encrypt the IMSI and use of enhanced pseudo-identifiers, i.e. identifiers that do not infer the identity of the subscriber.

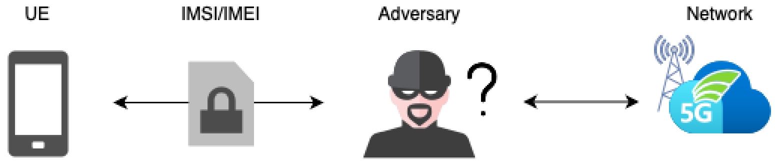

Figure 3.1: User identity confidentiality visualized.

Device Identity Confidentiality

Device identity confidentiality aims to protect the identifier of the UE, namely the IMEI. While a subscriber can change USIMs to prevent their real identity from being linked to their leaked IMSI, changing the IMEI would require replacing the entire UE. As with the IMSI, the IMEI should never be sent in clear.

3.1.2 User Location Confidentiality

This property defines that the presence or the arrival of a subscriber within a given area cannot be determined on the radio access link [3GP22d]. In order for user location confidentiality to be maintained, user identity confidentiality is required, as the most notorious way to determine a subscriber's presence is to leak their permanent identity.

Van den Broek et al. [FRJ15] identify two different objectives of location confidentiality attacks, namely monitoring and tracking. The two terms are illustrated in Fig. 3.2.

Monitoring

Monitoring refers to the mass retrieval of identifiers at a particular location. For example, a list of IMSIs caught at a protest can provide information about everyone who was in the vicinity, i.e. the participants in the protest [Int21]. In the context of international espionage, retrieving identifiers at political headquarters can provide information about its visitors [Sok18].

Tracking

Tracking is a targeted attack. The aim is to determine the exact or approximate GPS position of a person or, if this is not possible, to verify their presence within an area. This requires active interaction with the target. As the coverage area of a radio cell is limited, the tracking range is also limited. In order to track a person across multiple cells, an adversary needs either a mobile setup or a network of antennas [FRJ15].

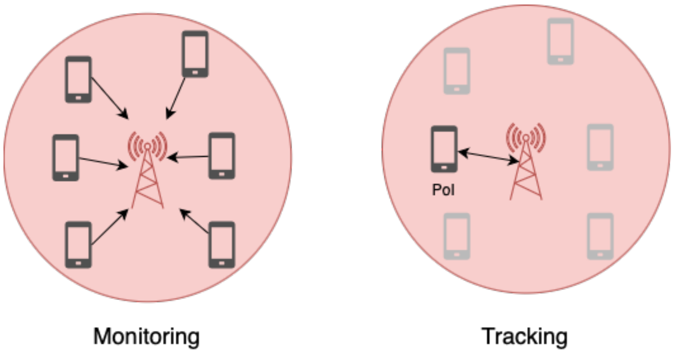

Figure 3.2: Monitoring and Tracking of UEs illustrated.

3.1.3 User Untraceability

User untraceability means that an adversary cannot deduce whether different services are being provided to the same subscriber by eavesdropping on the radio access link [3GP22d]. Similar to location confidentiality, untraceability is not given as long as a subscriber's IMSI can be disclosed. For example, an adversary only needs to group captured messages by their IMSI to determine whether they are generated or delivered to the same subscriber. As will be seen in the following sections, there are other ways to associate different messages with a single subscriber.

3.2 Vulnerabilities

Each generation of mobile networks has vulnerabilities that make them susceptible to privacy attacks. This section provides an overview of the past and present challenges in protecting the privacy of subscribers. First, it addresses the legacy privacy vulnerabilities that exist in LTE. Then, the author will evaluate the privacy improvements that the 3GPP has introduced with 5G in specifications up to Release 17. Finally, the unresolved issues in the current state of 5G are identified. An overview of the vulnerabilities as well as the privacy improvements in 5G and their impact is given in Tbl. 3.1.

3.2.1 Inherited Vulnerabilities

This section provides an overview of subscriber privacy vulnerabilities that exist in mobile network generations up to LTE.

Plain-Text IMSI

Up to LTE, there are cases where the IMSI is transmitted in clear over the air interface. This is the case with the EPS-AKA protocol, where authentication of the UE to the network requires initial user identification (see Section 2.2.3). The transmission of permanent or long-term subscription identifiers has been identified by the 3GPP in TR 33 899 [3GP17] as a key issue.

Inadequate BS Validation

In LTE, the UE receives some services such as paging while in `RRC idle mode`. When in *RRC idle mode*, the UE does not validate whether the eNB it wants to register with is authentic or fake. As a result, the UE may register with a rogue cell, leading to a number of location tracking and DoS attacks. This attack scenario is further explained in the 3.3.2 section. The 3GPP have recognized the vulnerability of rogue base stations [3GP17].

UE Measurement Reports

In LTE, measurement reports are used by network operators for cell selection and troubleshooting. The UE performs network measurements and sends them to the BS in RRC messages [SSB+16]. There are two types of measurement reports [KM20]:

1. The `Measurement Report` message is primarily used for handover procedures and allows the BS to specify the type of information to be measured by the UE. This can even include exact GPS coordinates [SSB+16]. In later versions of LTE, measurement reports can only be requested after a security context has been established [3GP25e].

2. Radio Link Failure (RLF) reports are used for troubleshooting signal coverage issues. These reports contain the identifiers of the serving and neighboring BSs together with their signal strength. By using a trilateration technique, as described by Caffery et al. [CS98], and using the signal strengths as inputs, the location of a subscriber can be inferred. The trilateration technique is illustrated in Fig. 3.3 [Wik05]. The 3GPP does not allow the transmission of RLF reports before a security context has been established [3GP25e]. However, Shaik et al. [SSB+16] found that LTE operators have failed to implement this security protection in the past.

While most privacy vulnerabilities are exploited for presence testing, UE measurement reports can be abused for fine-grained location tracking.

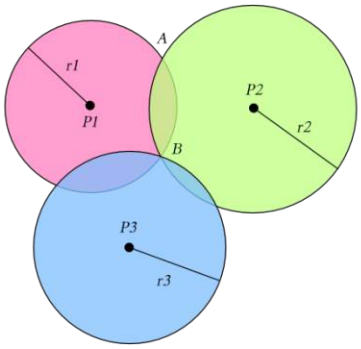

Figure 3.3: Trilateration in a plane.

GUTI Persistence

Temporary identifiers, including the GUTI in LTE and the 5G-GUTI in 5G, are used within 3GPP systems to protect subscriber privacy and mitigate location tracking by adversaries. In LTE, the GUTI should be reassigned in certain scenarios (see Section 2.2.2). However, network operators tend not to always change the GUTI by recommendation [SSB+16, BHPS18]. Furthermore, newly generated GUTIs are often based on previous ones with only minor and predictable modifications [FBB+23, BHPS18]. This has led to the emergence of attack scenarios [KKHK12, SSB+16] in which temporary identifiers are used to track subscribers. GUTI persistence has been identified by the 3GPP in TR 33 899 [3GP17] as a key issue.

IMSI-based Paging

The paging procedure is described in the 2.4.1 section. In LTE, paging events are usually derived from IMSI. During paging, no security context has been established between the UE and the eNB. This allows an adversary to passively monitor the occurrence of (parts of) the IMSI. The 3GPP identifies IMSI-based paging as a key issue in TR 33 899 [3GP17].

3.2.2 Privacy Improvements in 5G

Release 15 introduced several security features that significantly improve subscriber privacy. This section provides a summary of the most notable subscriber privacy improvements introduced with 5G. Release 17 of the 3GPP serves as the basis for this analysis.

Concealment of IMSI

The 3GPP decided to address the issue of IMSI exposure in Release 15 [3GP24b]. Unlike previous generations, the specifications do not allow clear text transmission of permanent identifiers over the radio interface. Instead, the SUCI, the ciphered version of the SUPI, is transmitted, providing protection against a number of deanonymization attacks.

Fake Base Station Detection

In Release 15 [3GP24b], the 3GPP specified a framework to counter the use of Fake Base Station (FBS), which is a precursor to various attacks. The framework is based on the analysis of measurement reports and could be used to make it significantly harder for FBS to remain stealthy. It works by detecting anomalies in the reports, such as unexpected radio access types, foreign mobile country codes, deployment inconsistencies and abnormal signal strengths. The status of the framework is purely informative. This means that there are no specific requirements on how to enable the detection system, and it is up to the operator to decide whether to implement it on the network. According to Khan et al. [KM20], the FBS detection framework should be transformed into a normative specification to ensure its adoption.

Refreshment of 5G-GUTI

With Release 15 of the 5G protocol [3GP24b], the 3GPP provides clear specifications for the refreshment of the 5G-GUTI (see Section 2.3.2, 5G-GUTI). This has made the correlation of 5G-GUTIs to identify subscribers impractical [Eri19].

Decoupling of IMSI from Paging

To reduce the exposure of the IMSI within paging messages, the 3GPP decided to decouple the IMSI and SUPI from the paging procedure with Release 16. The calculation of the paging frame index and paging occasions is now based on the 5G-S-TMSI [3GP25b]. The strict refreshment of the 5G-GUTI, which includes the 5G-TMSI and its shortened version, renders the vulnerability impractical.

Secure Radio Redirections

Redirection is used by BSs to send a UE to a cell in a different frequency or network generation [KFRK23]. In a malicious context, the redirection mechanism can be exploited to force a UE into older, less secure network generations. This is also known as a *downgrade attack*. In Release 15 [3GP25c], the 3GPP is specified to protect the integrity of RRC messages that redirect UEs. In addition, only redirection to LTE is possible [KFRK23].

3.2.3 Unresolved Vulnerabilities in 5G

Despite the improvements that 5G has introduced to protect subscriber privacy, there are issues that haven't been fully addressed by the 3GPP in the specifications up to Release

17. This section is a summary of unresolved and new vulnerabilities in the current state of 5G.

Unprotected NAS & RRC Messages

In 5G there are NAS and RRC messages that can be sent without (integrity) protection, at least before a security context has been established. This makes them vulnerable to various attacks [PGBBM21, BKS+23, HEC+19, CRPH21], targeting both UE and the network.

Replay Attacks

Because the ECIES scheme inherently lacks a mechanism to guarantee the freshness of messages to the network, the 5G protocol is vulnerable to replay attacks [KM20].

Linkability of AKA Failure Messages

This vulnerability originates from the fact that in the event of a failed authentication, the network exposes the reason for the authentication failure. Combined with the lack of replay protection, an adversary can replay some payload from a user's session against the UE or the network and observe the response. Depending on the nature of the failure, the adversary can check whether the previously observed network session belongs to a subscriber in their area. The 3GPP recognizes the linkability through AKA failure causes as a problem in TR 33 899 [3GP17].

Plaintext C-RNTI

The Cell Random Network Temporary Identifier (C-RNTI) is a physical layer identifier and is unique for each UE within a given cell. It is used to identify RRC connections. By monitoring packets over the air interface and exploiting the use of temporary identifiers in higher layers, an adversary can associate network traffic with a subscriber.

The 3GPP identify the use of the unprotected C-RNTI in TR 33 899 [3GP17] as a key issue but claim that the C-RNTI is too short-lived to have privacy implications. Research [RKHP19, LRN23] has shown that the C-RNTI can still be used in combination with the TMSI of the UE to track a subscriber in 5G. However, it is much more difficult than in LTE networks.

Post-Quantum Vulnerability in ECIES

The two protection schemes, Profile A & B, used to encrypt the SUPI in the SUCI are based on a ECIES-based scheme. ECIES-based schemes use ECC to provide user identity confidentiality. ECC is based on the hardness assumption of the discrete logarithm problem. Using Shor's algorithm, a quantum adversary could break the SUCI cryptography and thus deanonymize all of a network operator's subscribers [UPMS22, BR20].

The 3GPP acknowledges the threat that quantum computing poses to the cryptographic schemes used in 5G in TR 33 841 [3GP19]. They argue that a large-scale quantum computer with processing power could be built within the two decades that are within the life cycle of 5G systems. To mitigate this vulnerability, Ulitzsch et al. [UPMS22] propose a quantum-resistant scheme for SUCI computation.

Chosen SUPI Attacks

If the public key of the HN is known, the adversary can derive the SUCI of a UE himself. All he has to do is obtain the IMSI (SUPI) of a selected target to create the corresponding SUCI and perform the encryption himself. This procedure is described in more detail in Section the 4.2.2. The 3GPP acknowledged chosen SUPI attacks in TR 33 846 [3GP21].

Insecure Network Configurations

The inadequate implementation of the 3GPP specification by network operators is a weak point for various attacks, as shown by recent studies [NZW+22, FBB+23]. In addition, some important security features are marked as optional in the specifications and can therefore be bypassed.

Legend: ● = resolved, ◗ = partial effect

5G Privacy Enhancements	Inherited Vulnerabilities								
	Resolved					Unresolved			
	Plain-Text IMSI	Inadeq. BS Validation	UE Measurement Reports	GUTI Persistence	IMSI-based Paging	Unprotected Signalling	Replay Attacks	AKA Failure Messages	Plaintext C-RNTI
Concealment of IMSI	●					◗			
False Base Station Detection		●	●		◗	◗	◗	◗	
Refreshment of 5G-GUTI				●					◗
Decoupling of IMSI from Paging					●				
Secure Radio Redirections	◗		◗		◗	◗			

Table 3.1: An overview of the 5G privacy enhancements' effects on existing vulnerabilities, adapted from Khan et al. [KM20].

3.3 Attack Scenarios

The vulnerabilities described in the previous section can be exploited by adversaries to perform deanonymisation attacks on the UE. The attacks can be carried out in a number of ways. Typically, there are four scenarios in which an adversary might act:

(a) Passive.

(b) As a Fake Base Station (FBS),

(c) As a Man-in-the-Middle (MitM).

(d) By exploiting Signal Overshadowing.

The attack scenarios are illustrated in Fig. 3.4.

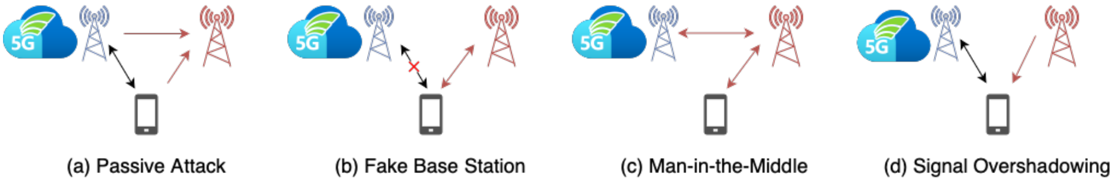

Figure 3.4: Typical attack scenarios, adapted from Bitsikas et al. [BKS+23].

3.3.1 Passive Attack

In a passive attack scenario, the adversary silently eavesdrops (*sniffs*) on over-the-air broadcast channels. All that is required is simple radio equipment, such as a Software Defined Radio (SDR), an antenna, a laptop computer and associated software [SSB+16]. By scanning for unprotected traffic, the adversary can record identifiers that occur. Permanent identifiers can be used to track the subscriber (see Section 3.4.1). Capturing temporary identifiers can be a prerequisite for a number of subsequent attacks.

3.3.2 Fake Base Station

FBS attacks involve the malicious attachment of a UE to an illegitimate BS for a limited period of time. This attack scenario differs from a classic MitM attack in that the FBS does not have the cryptographic keys to establish a full connection with the UE. Instead, an FBS attack relies on pre-authentication traffic and unprotected NAS and RRC messages to compromise its victims. [BKS+23]

FBS and MitM attacks require the UE to connect to the adversary in a process called *cell selection*. A number of privacy attacks using the FBS approach are discussed in Section 3.4.

Cell Selection

A UE can only register with one cell. To do this, it goes through a decision-making process to select a particular BS to which it wants to connect. As it goes on, the UE may find another BS with better conditions. It can then change BSs in a process called *cell reselection*. To do this, the UE continues to monitor the signal quality of the serving and neighboring BSs.

There are two types of cell reselection, according to TS 138 304 [3GP25d]:

1. Intra-frequency cell reselection.

2. Inter-frequency cell reselection.

Within intra-frequency cell reselection, the UE performs a ranking of all cells that fulfil a certain criterion. If a newly discovered BS achieves a better rank than the serving one, the UE will reselect it. Within the inter-frequency cell reselection, the UE uses a feature called *absolute priority based cell reselection*. The principle is that UEs should try to connect to BSs operating on high priority frequencies. These frequencies are defined in RRC messages sent by BSs.

A FBS can exploit the cell reselection process to trick the UE into connecting to it. Under GSM, it can exploit the fact that UEs tend to select the BS with the highest signal strength [3GP22a]. In later protocols, however, the UE does not scan for surrounding BSs when it is very close to a serving BS in order to save power. Thus, more sophisticated techniques, such as exploiting absolute priority based cell reselection, are required to achieve the desired effect [SSB+16].

3.3.3 Man-in-the-Middle (MitM)

The MitM approach allows the adversary to capture and control traffic even after a secure context has been established. This allows attacks on the User Plane (UP), making MitM attacks more powerful than FBS attacks [BKS+23].

Communication Interception

Unlike later generations, intercepting UP communication between the network and the UE is only possible when using GSM. The reasons for this are as follows:

1. Communication using the GSM protocol doesn't require encryption or mutual authentication [DPK+14].

2. Even when encryption is enabled, some encryption algorithms in GSM can be broken in real time, as discussed in Section 2.1.2.

One way to intercept UP traffic is described by Dabrowski et al. [DPW16]: The MitM places itself between the UE and a legitimate BS and convinces the network that it is the real subscriber. It can then tap into the cipher negotiation sequence to change the set of supported ciphers, i.e. either *null scheme* or a cipher that can be easily decrypted. As a result, the adversary has access to all user and data traffic between the UE and the network.

Communication Manipulation

While communication interception is the act of eavesdropping on over-the-air traffic, communication manipulation is the act of tampering messages without the knowledge of the network or the subscriber. An attacker can modify captured data packets at will if the messages can be sent without mandatory integrity protection. Communication manipulation can also occur in 5G, as will be seen later in the thesis.

3.3.4 Signal Overshadowing

Signal overshadowing refers to signal injection attacks that exploit unprotected signalling messages. These attacks are based on the fact that the UE will always decode a stronger signal when it receives multiple overlapping signals [YBS+19]. An adversary only needs simple radio equipment, such as a SDR, an antenna, a laptop and the appropriate software, to carry out signal overshadowing attacks [YBS+19, KEL+22].

The procedure is as follows: The adversary sends a message perfectly matched to the time and frequency of the BS message, but with a higher signal strength [KEL+22]. As a result, the original message is *overshadowed* by the adversary's message. The UE, on the other hand, cannot distinguish which message was sent by the legitimate BS.

Signal overshadowing attacks require precise timing and are therefore not the most common attack scenario. The author decided not to discuss them further in the thesis.

3.4 Privacy Attacks

After describing the privacy vulnerabilities and attack scenarios, this section looks at specific privacy attacks in 5G. The attacks, together with their feasibility and underlying vulnerabilities, are summarized in Tab. 3.2.

3.4.1 IMSI-Catching

IMSI-Catching is the most notorious privacy attack in mobile networks. It involves capturing identifiers to test the presence of network subscribers. Adversaries typically use the IMSI or IMEI of the UE to do this. IMSI-Catching can be done either passively or actively via a FBS.

In a passive attack, the attacker eavesdrops on communication channels by scanning for frequencies in use and listening for unencrypted messages. He then looks for IMSIs within the intercepted traffic. Passive IMSI-catching is mainly used for monitoring attacks involving multiple UEs. An adversary can also test the presence of a person if he already knows their IMSI. However, in this scenario the adversary cannot force the transmission of the IMSI and must wait for the UE to send it [FRJ15].

Active attacks use a FBS, which makes the attacks more sophisticated, but also more powerful. The FBS can request a specific identity by using the command `Identity Request`. The UE then responds with an `Identity Response` containing the requested identifier, as shown in the Fig. 3.5. According to the TS 124 301 [3GP24e], an `Identity Request` requesting an identifier other than the IMSI will be ignored unless the security context is established. However, in some cases [FRJ15] the UE will also send its TMSI and IMEI when requested. Active IMSI-Catching can be used to test the presence of a particular participant, provided that the person's IMSI is already known. Unlike passive monitoring, the adversary can retrieve the target's IMSI at any time.

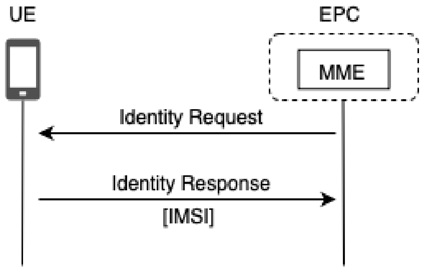

Figure 3.5: The identification procedure in LTE, adapted from the 3GPP [3GP24e].

IMSI-Catching attacks are a major problem in GSM, UMTS and LTE networks [SSB+16]. In the past, these attacks have been used for location tracking and mass surveillance. Reports [Naa16] [PE16][BS17] have shown the use of IMSI-Catching by law enforcement agencies under the pretext of serious crime and terrorism. Similarly, IMSI-Catching has been abused in the context of international espionage [Sok18]. The problem is so notorious that FBSs are also referred to as *IMSI-Catchers*.

The SUCI was introduced in 5G to prevent IMSI-Catching attacks. Addressing the UE with a concealed identifier prevents the adversary from directly inferring the identity of the subscriber. However, the use of downgrade attacks allows the adversary to disable the UE's 5G capabilities [KFRK23], making IMSI-Catching still possible under certain circumstances.

3.4.2 IMSI-Probing

The term *IMSI-Probing* covers attacks where the adversary already knows some identity of a subscriber and wants to check their presence within a geographical area. These attacks usually require additional effort from the adversary, making them less powerful than IMSI-Catching. Despite its name, IMSI-Probing is not limited to the IMSI and can use other identities to reveal a subscriber's location. Two IMSI-Probing attacks are described in more detail below.

3.4.3 Paging-based Probing

This attack is a form of IMSI-Probing that exploits paging. Using some identity of the subscriber, such as the MSIN or even a Facebook profile [SSB+16], the adversary triggers a certain number of paging messages to the subscriber's UE. The targeted UE must have no radio connection, i.e. be in `RRC idle mode` [FBB+23]. After sending the messages, the adversary monitors the paging channel and checks if there is an influx of traffic. If this is the case, the presence of the subscriber within the coverage area of the given BS is confirmed. If not, the attacker must change the cell area and repeat the procedure.

In addition to simple channel monitoring, the adversary can apply set intersection analysis, as proposed by Kune et al. [KKHK12], to the recorded traffic. This allows him to deduce the target's PO and the 5G-S-TMSI to which the paging messages are addressed. As a result, this attack can reveal the mapping between the UE's 5G-GUTI and its previously known identity.

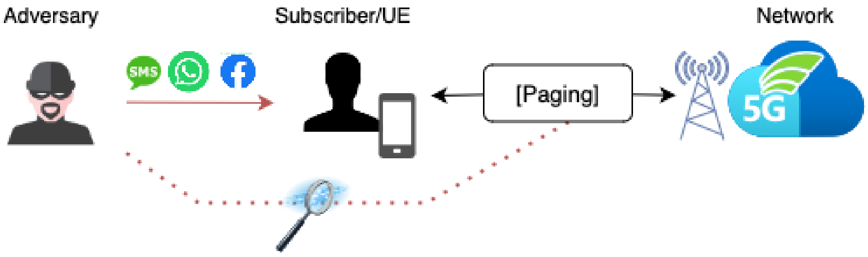

Figure 3.6: Paging-based Probing illustrated.

In paging-based probing, the adversary abuses external services to trigger paging messages. Most triggering methods result in a notification on the user interface of the UE application. However, by sending silent SMS [Cro12] or abusing the typing notification feature in the WhatsApp messenger [SSB+16], paging messages can be sent inconspicuously.

Testing for the presence of a targeted UE by triggering messages and monitoring communication channels is a known vulnerability that is not easily mitigated [KM20]. The feasibility of associating a GUTI with a previously known (permanent) identifier depends on the persistence of the GUTI (see Section 3.2.1). In 5G, the UE is strictly required to update the 5G-GUTI after the `Service Request` in the paging procedure. However, the exact implementation of the 5G-GUTI reallocation is left to the mobile operator and is not always implemented accordingly [FBB+23, NZW+22]. In addition to the 5G-GUTI, the C-RNTI can be used for this attack [LRN23].

Ultimately, the success rate for paging-based probing is highly dependent on the number of probes and detection algorithms used [FBB+23].

3.4.4 Session Linkability-based Probing

This attack is based on the linkability of error messages in the 5G-AKA mentioned in Section 3.2. It was first discovered by Basin et al. [BDH⁺18] and later implemented as a proof-of-work *SUCI-Catcher* by Chlosta et al. [CRPH21].

The process consists of two phases, a discovery phase and an attack phase. During the discovery phase, the adversary must obtain any SUCI of its target. In the attack phase, the adversary sends an `Authentication Request` to the network using the collected SUCI. The response is sent to every UE in the vicinity. Based on the response, the adversary can infer whether the targeted UE is within the cell's coverage area, making the attack viable for presence testing.

For the discovery phase, Chlosta et al. [CRPH21] mention two ways of obtaining the victim's SUCI:

1. Sniffing network traffic: The adversary can passively monitor the (initial) registration procedure and search for occurring SUCIs.

2. Deriving the SUCI from the IMSI: The adversary can perform the encryption of the IMSI on its own, as described in Section 3.2, Chosen SUPI Attacks.

For the attack phase, the adversary must establish a FBS: Whenever a UE connects to the FBS, the adversary tries to find out if the received SUCI belongs to this UE. The attack phase is visualized in Fig. 3.7, its procedure is as follows [CRPH21]:

1. The adversary inserts the searched-for SUCI into a `Registration Request` and sends it to the network. This is possible because this command can be sent without (integrity) protection. The network responds with an `Authentication Request`, which is forwarded by the adversary to all connecting UEs.

2. Depending on the UEs' given responses, the presence of the searched-for subscriber can be inferred:

   a) The obtained SUCI belongs to the UE: The UE either successfully authenticates to the network by responding with `Authentication Response`, or it returns `Authentication Failure` with the cause *Synch Failure*.

   b) The obtained SUCI does not belong to the UE: The UE returns an `Authentication Failure` message with the cause *MAC Failure*.

Following this procedure, the SUCI-Catcher is limited to testing for a single entity only, as the UE aborts further registration attempts after two consecutive authentication failures. To allow scaling and searching for multiple subscribers, the authors [CRPH21] extended the scheme with an additional reset stage. This allowed them to test 500 identities

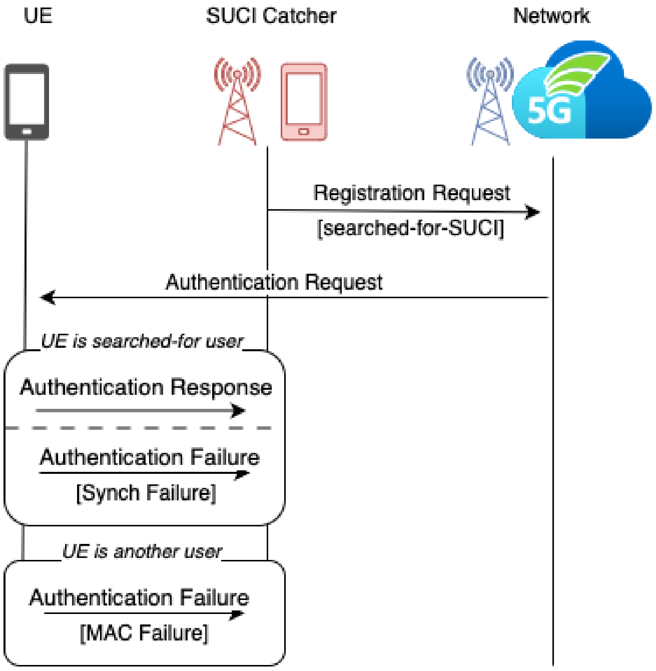

Figure 3.7: The SUCI-Catcher's attack phase, adapted from Chlosta et al. [CRPH21].

within 60 seconds in the lab experiment. However, taking into account the throttling of commercial networks, Chlosta et al. [CRPH21] advise limiting the attack to a small group. Verifying the presence of 10 people would take 20 seconds.

3.4.5 IMSI-Cracking

The IMSI-Cracking attack is a brute force attack that aims to guess the IMSI (SUPI) of a UE. Hussain et al. [HEC⁺19] propose two versions of this attack. The version applicable in 5G is discussed in this section and visualized in Fig. 3.8.

The IMSI-Cracking attack takes advantage of the following circumstances:

1. The first 5 to 6 digits of the IMSI consist of the MCC and the MNC. These codes identify the mobile operator and are publicly visible, leaving 9 or 10 digits for the adversary to *guess*.

2. The public key CN_{pk} of the network is known, allowing chosen SUPI attacks (see Section 3.2.3).

3. The NAS message `Registration Request` can be sent without (integrity) protection, at least before a security context has been established.

4. The network response to a `Registration Request` message depends on whether the message contains a valid IMSI. The UE's response to a `Authentication`

`Request` depends on whether it can solve the attached challenge. This behavior allows the linkability of failure messages (see Section 3.2.3)

To brute force the IMSI of a UE in 5G, the adversary makes a guess of the IMSI I_{guess} and calculates its corresponding SUCI, i.e. $SUCI_{guess} = f(I_{guess}, CN_{pk})$. It sends $SUCI_{guess}$ to the network within a `Registration Request`. If the IMSI is valid, the network responds with a `Authentication Request`. The adversary now knows if I_{guess} is the IMSI of any UE connected to this network. In the case of a valid IMSI, the adversary forwards the `Authentication Request` to the targeted UE. Based on the UE's response, the attacker can infer whether I_{guess} is the victim's IMSI.

The authors only validated the IMSI cracking attack in LTE. In their tests, it took them about 200,000 paging messages and 74 hours to crack the victim's IMSI [HEC+19]. It can be assumed that brute forcing the IMSI in 5G will take at least as much effort and time, making the IMSI cracking attack impractical for tracking attacks.

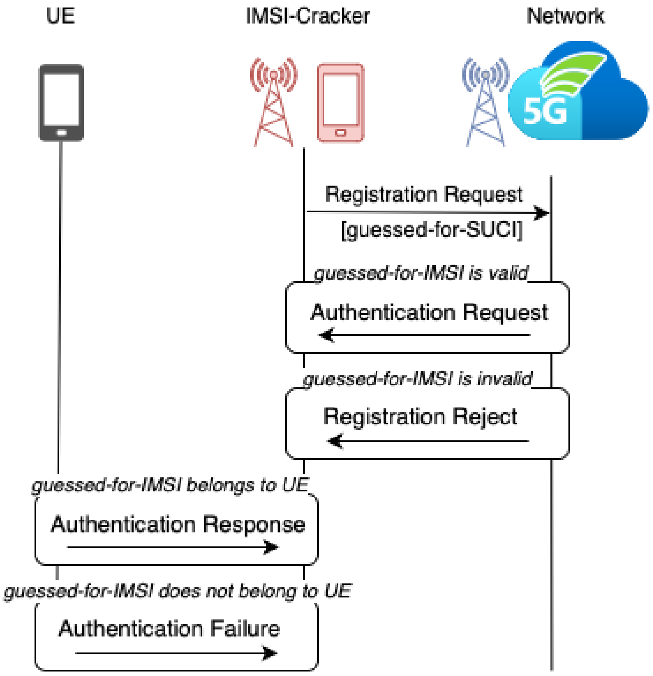

Figure 3.8: The IMSI-Cracking attack.

3.4.6 Denial of Service & Downgrading

Denial of Service (DoS) attacks in telecommunications aim to disrupt the availability of network services to subscribers. They can be either a stand-alone attack or an entry point for a subsequent downgrade attack. In a downgrade attack, also known as a *bidding-down attack*, the adversary tricks the UE into believing that access to its chosen network generation has been denied. The goal is to force a UE to connect to a cell on an older generation network, thus rendering the security enhancements of 5G useless. A downgrade attack from 5G SA to LTE is visualized in Fig. 3.9.

The simplest form of downgrade attack is to flood the radio frequencies in use with white noise, making it too noisy for UEs to connect to their preferred cell. There are also methods for targeting individual phones. Karakoc et al. [KFRK23] found that unprotected NAS messages can be exploited to instruct the UE to move to older network generations:

1. The adversary sets up a FBS and tricks the UE into connecting to it, i.e. initiating a registration procedure.

2. After receiving the `Registration Request`, the FBS immediately responds with a `Registration Reject` including the `Reject Cause`. The 5G specifications allow UEs to accept unprotected rejection messages, at least before a security context is activated [3GP25a].

3. Depending on the cause of the rejection, the UE may ignore all 5G networks and reselect LTE cells, rendering a downgrade attack.

Karakoc et al. [KFRK23] tested different types of `Reject Cause` on a number of 5G UEs. They were able to cause all UEs to disable their 5G capabilities and downgrade to LTE. This attack is a prerequisite for further downgrade attacks: The authors demonstrated a complete downgrade from 5G to GSM.

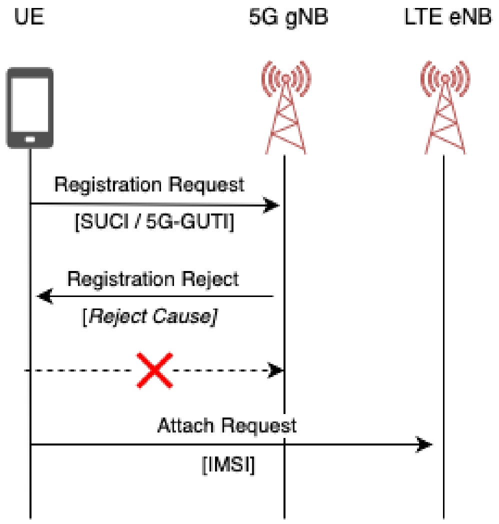

Figure 3.9: A downgrade attack from 5G SA to LTE visualized. The adversary operates two FBS and downgrades the UE from a 5G gNB to a LTE eNB.

Legend: ● = direct effect, ◗ = partial effect

5G Privacy Attacks	Underlying Vulnerabilities						Related Literature
	Unprotected Signalling	Replay Attacks	AKA Failure Messages	Plaintext C-RNTI	Chosen SUPI Attacks	Insecure Network Configurations	
IMSI-Catching	◗			◗		●	[FRJ15]
Paging-based Probing				◗		●	[SSB+16, FBB+23]
Linkability-based Probing	●	●	●		◗	◗	[CRPH21]
IMSI-Cracking	●		●		●		[HEC+19]
DoS & Downgrade	●					●	[KFRK23]

Table 3.2: A summary of the privacy attacks presented in this chapter, together with the underlying vulnerabilities.

3.5 Suggestions for Improvement

In this section, the author will mention general suggestions aimed at neutralizing the attacks mentioned above. A summary of the ideas, together with the estimated difficulty of their implementation and the underlying attacks, is given in Tbl. 3.3.

3.5.1 Public Key Infrastructure

One mitigation strategy would be to deploy a network-wide Public Key Infrastructure (PKI). This would encrypt pre-authentication traffic, making some of the above attacks impossible. Using a PKI infrastructure would require every USIM to have the public keys of every operator in the world. Mobile operators, on the other hand, would have to store their private keys securely. Arapinis et al. [AMRR17] propose their version of a PKI.

According to Jover et al. [PJM19], this form of key management is unlikely to be feasible as it is far outside the 3GPP specifications and would require a lot of effort to implement. In addition, the global scale would most likely lead to political disagreement and therefore lack of global adoption.

3.5.2 Strengthening 3GPP Security Requirements

It is recommended that the 3GPP further strengthens its security requirements by changing some security features from optional to mandatory [NZW+22]. Network operators are not required to implement certain protection mechanisms, which may, for example, enable the operation of FBSs.

Enforcing 5G-GUTI Refreshment

It is up to the network operator's implementation to reallocate 5G-GUTIs more frequently, for example after a `Service Request`. [KM20]. Enforcing frequent 5G-GUTI reallocation prevents adversaries from abusing traffic analysis for privacy attacks.

Mandatory Provision of Encryption Keys

As mentioned in Section 2.3.2, there are three cases where the SUCI can be generated with *Null Scheme*, one of which is when the mobile operator does not provide a public key for encryption. Nie et al. [NZW+22] found that mobile operators in China failed to configure 5G USIM with cipher suites for SUPI protection, exposing the subscriber's IMSI over the air interface.

3.5.3 Extending the ECIES Scheme

Extending the ECIES scheme could address some vulnerabilities in 5G. This would require changes to both the UE and the network. Some approaches are described in more detail in Section 5.1.

3.5.4 Increasing Paging Rate

According to Hussain et al. [HEC+19], increasing the current paging rate would require numerous pings from the adversary to sufficiently distinguish the victim's PO from others. This would make paging-based probing more difficult.

Injecting additional paging messages at each PO may be trivial to implement. However, depending on the additional rate of paging injections, this approach could result in significant overhead for the network and the UE.

3.5.5 Non-static C-RNTI

The static C-RNTI can be misused for correlation attacks with the UE's TMSI [LRN23]. It should therefore be reassigned regularly. According to Ludant et al. [LRN23], updating the C-RNTI could be trivially achieved by using the `newUE-Identity` field.

Legend: ● = direct effect, ◗ = partial effect
★ = low, ★★ = medium, ★★★ = high, ? = unknown

Improvements	Vulnerabilities/Attacks								Complexity Level
	Unprotected Signalling	Replay Attacks	AKA Failure Messages	Plaintext C-RNTI	Post-Quantum ECIES	Chosen SUPI Attacks	Insecure Network Configuration	Paging-based Probing	
Public-Key Infrastructure	●		●			●			★★★
Enforcing 3GPP Requirements		◗				◗	●		?
Extending the ECIES Scheme		●			●	●			★★
Increasing Paging Rate								●	★★
Non-static C-RNTI				●					★

Table 3.3: A summary of the presented mitigation strategies and their impact on 5G vulnerabilities or attacks. The complexity level indicates how complex the approach would be to implement.

CHAPTER 4

SUCI-Catcher Attack: Replication

This chapter focuses on replicating the SUCI-Catcher attack discussed in Section 3.4.4 in a simulated environment. The author implements the attack methodology described by Chlosta et al. [CRPH21] using an open-source 5G test bed and demonstrates its practical execution. The specific steps, configuration parameters and technical requirements are documented.

4.1 Establishment of a 5G Standalone Network

In this section, a 5G SA network environment is established using free and open-source software (FOSS) and off-the-shelf hardware. First, existing 5G-RAN and 5GC implementations suitable for 5G are discussed. As a result, the chosen software stack is justified. In addition to the software, the hardware used to build the network is also mentioned. Finally, the author will discuss the setup process and related configuration details.

4.1.1 Software Specification

This section describes the free and open-source software (FOSS) software used to simulate the 5G SA network, more specifically the 5G-RAN and 5GC.

Traditionally, mobile network deployments have a closed RAN architecture. More specifically, the RAN is based on monolithic building blocks and its interfaces are proprietary and largely undisclosed to third parties, eliminating the possibility of interoperability between vendors and limiting the flexibility of the network. To mitigate this problem, the concept of Open RAN (O-RAN) was introduced by the O-RAN Alliance [ALL24a]. Its aim is to define specifications for open interfaces and to abstract network elements and functions from the underlying hardware. [LBSR23]

There are two popular FOSS solutions that implement a complete RAN solution that conforms to the 3GPP and O-RAN Alliance (Release 17) specifications, namely srsRAN

Project (srsRAN) [(SR24] and OpenAirInterface (OAI) [All24b]. Both solutions are available for the research community to explore by providing a full version of the complete protocol stack for 5G networks. According to Mamushiane et al. [MLKM23] OAI offers better support for sub-carrier bandwidths and better throughput under signal interference than srsRAN. However, srsRAN provides better community support and documentation, and is easier to deploy. The author decided to use srsRAN as the RAN protocol stack.

There are several FOSS projects focused on implementing a 3GPP compliant 5GC. These include Free5GC [Fre25], Magma, OAI 5GC [All24b], OMEC and Open5GS [Ope]. All of these solutions are easy to deploy and generally have low system resource usage [MLKM23]. However, compared to its rivals, Open5GS is the most widely adopted and has the widest community support. The author decided to use Open5GS as the 5GC.

4.1.2 Hardware Specification

This section describes the hardware used to build the 5G SA network.

The following hardware configuration was used as the underlying test platform:

- Processor (CPU): AMD Ryzen 5 3600, 6 cores, 12 threads, 3.6 GHz base clock, 4.2 GHz boost clock.
- Memory (RAM): 16 GB DDR4, 3200 MHz.
- Operating System (OS): Ubuntu 24.04 LTS.

Two different SDRs were used as the radio hardware in the experiment:

- The Universal Software Radio Peripheral (USRP) B205mini [Cor], developed by National Instruments. It is a high-performance SDR with a frequency range of 70 MHz to 6 GHz, capable of full-duplex communication with a bandwidth of up to 56 MHz.
- The bladeRF 2.0 micro xA4 [Nua], developed by Nuand. It operates across the frequency range of 47 MHz to 6 GHz, capable of full-duplex communication with a bandwidth of up to 40 MHz.

To synchronise the radio signal, the two SDRs are connected to a global positioning system disciplined oscillator (GPSDO) from Leo Bodnar. The use of an external GPSDO is recommended in order to operate a stable 5G network [HLRM24, BKS+23].

The experiment used two commercial off-the-shelf (COTS) UEs capable of 5G connectivity, namely the OnePlus Nord N10 5G and the Apple iPhone 13 mini. In both devices a sysmocom sysmoISIM-SJA5-9FV [sfmcG] was used as the USIM.

An illustration of the system configuration can be seen in Figure 4.1. The system configuration in action (without the PC) can be seen in Figure 4.2

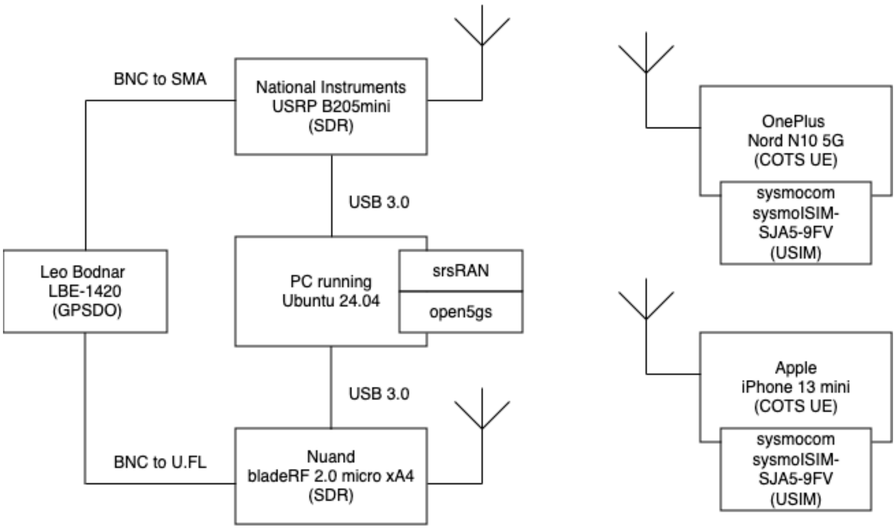

Figure 4.1: The system configuration used for establishing a 5G SA network in which the experiment could be executed.

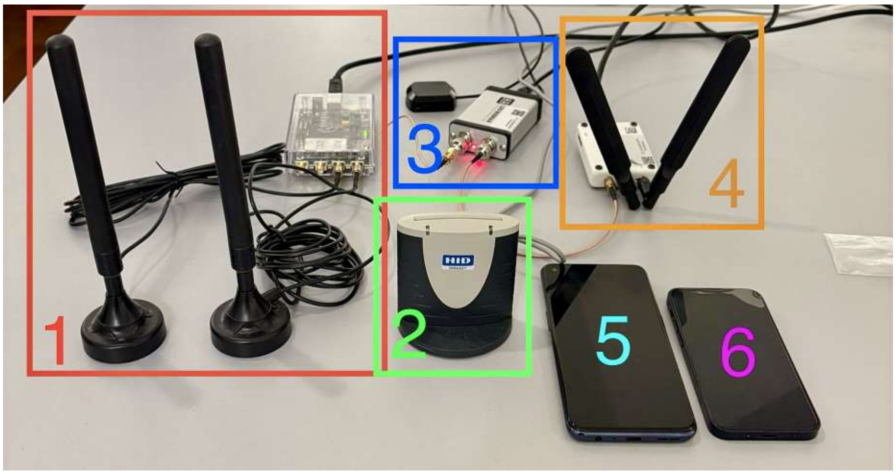

Figure 4.2: The system configuration in action. The PC running the software is not shown in this picture.

1: bladeRF xA4	2: HID Omnikey 3121
3: Leo Bodnar GPSDO	4: USRP b205mini
5: OnePlus Nord N10 5G	6: iPhone 13 mini

4.1.3 Preparatory Work

The following describes the preparatory work that needed to be done to conduct the experiment.

Network Configuration

Open5GS was used to simulate the 5GC. A fundamental feature of 5G SA networks is the encryption of the SUPI. By default, Open5GS is not configured for SUCI concealment. Therefore, private keys had to be generated for the ECIES profiles and specified in the UDM configuration files. The specific ECIES scheme depends on the desired SUCI profile. The author has specified keys for both SUCI profiles A and B, following this guide [Ish23].

Open5GS rejects `Registration Request` messages without integrity protection, preventing the modification of the message's identification fields and thus the SUCI-Catcher attack. However, this protection mechanism is not compliant with the 5G protocol specification: In TS 124 501, 4.4.4.3 [3GP25a], the 3GPP specifies that a `Registration Request` message must be processed by the AMF, even if it fails integrity checks. Therefore, the author decided to adapt the Open5GS code base to allow the processing of unprotected `Registration Request` messages.

One of the COTS UE used in this experiment is the Apple iPhone 13 mini. iPhones are selective in their support for private 5G networks [App24]. Open5GS had to be configured as follows to allow the iPhone to connect to the simulated network:

- The network needed to be configured with the MCC `999`.
- NAS encryption had to be explicitly enabled in the AMF configuration.

Before connecting the USIMs to the network, they had to be registered in the Open5GS database. This was done using the USIM key material sent by sysmocom after the cards were purchased.

Cell Configuration

Two instances of the srsRAN were used in this experiment. One instance used the USRP B205mini and the other instance used the bladeRF 2.0 micro xA4 as its RF front end. While the USRP worked out of the box with srsRAN, some modifications had to be made to the code base of the software to make it compatible with the bladeRF.

The gNB was configured as follows:

- The PLMN was set to the one configured in the AMF of Open5GS.
- The clock source used by the SDR was set to `external`.
  - This allows the gNB to use the Leo Bodnar GPSDO as a 10MHz reference.

Programming of SIM cards

The 3GPP defines two variants for enabling SUCI concealment on the subscriber side:

- Calculation of the SUCI on the UE, using the keys stored on the USIM.
- Calculation of the SUCI on the USIM itself.

By default, the sysmocom USIMs do not have SUCI concealment enabled. The specific USIM model used supports SUCI calculation on the UE. To enable this feature, the USIM needs to be reprogrammed as follows [MWM+23]:

- The USIM service 124 must be active.
- The USIM service 125 must be inactive.
- The network's public keys must be stored in `EF.SUCI_Calc_Info`.
  - The corresponding public keys of the private keys specified in the network's UDM have been used. The author configured the USIMs to prioritize Profile B for SUCI encryption.
- A routing indicator must be specified.
  - This has been set to `0x71`.

The USIMs were reprogrammed using an Omnikey 3121 smart card reader and pySim [Osm], a Python tool for reading and writing all types of USIM cards.

UE Configuration

To allow the COTS UEs to connect to the private network, the following steps had to be taken [Sys25]:

- Enable 5G SA mode.
- Enable data roaming.
- Disable VoLTE or VoNR.
- Configure the APN.
  - The `APN` option must be the same as the `DNN/APN` option in the Open5GS subscriber registration.
  - The options `APN protocol` and `APN roaming protocol` must be set to `IPv4`.

4.2 Attack Implementation

In this section, the author explains in detail the steps needed to replicate the SUCI-Catcher attack. All related code is available in the author's gitlab repository.

4.2.1 Test Environment

The test environment for the SUCI-Catcher attack was created using Docker containers. Specifically, one container running the Open5GS 5GC, two containers each running a srsRAN gNB container and a Man-in-the-Middle (MitM) container implemented by the author for the experiment. Both gNBs are connected to the AMF of the 5GC via the MitM container. In this scenario, the first gNB acts as the legitimate BS, while the second gNB acts as the malicious, i.e. the FBS. In the experiment the MitM is placed at the NGAP layer – a protocol used in the communication between gNB and AMF – rather than at the radio layer. This simplifies the attack compared to a *real* SUCI-Catcher operating in commercial networks. The setup is illustrated in figure 4.3.

4.2.2 Obtaining the SUCI

As mentioned in Section 3.4.4, there are two ways to obtain a SUCI before the actual probing attack.

Sniffing Network Traffic (Variant 1)

In this scenario, a SUCI is obtained by intercepting network traffic occurring between the UE and the gNB, i.e. NAS messages. To do this, the author's implementation monitors the initial registration procedure on the NGAP layer. The identification procedure can also be triggered by corrupting NAS messages with an unknown 5G-GUTI, as mentioned by the 3GPP in TR 33 846 [3GP21]. This method will be referred to as *Variant 1* in the following sections.

Deriving a SUCI from the IMSI (Variant 2)

In this scenario, the SUCI is derived from a previously known IMSI (or SUPI). Performing the ECIES on the SUPI requires knowledge of the network's public key. Among other methods, an IMSI can be obtained quite easily under LTE (see Section 3.4.1). The network's public key can be read from any USIM issued by the same network operator using a smart card reader, such as the HID Omnikey 3121. This only works if the SUCI calculation is done on the UE. In this implementation, the author takes advantage of the fact that the IMSI of both UEs and the public key of the network are already known. This method will be referred to as *Variant 2* in the following sections.

4.2.3 Configuring the Fake Base Station

Some configuration is required to get UEs within range to connect to the fake base station. Mjolsnes et al. [MO17] list important configuration steps for setting up a FBS in LTE:

1. The FBS must operate at a higher signal strength to be prioritized for cell selection.
2. The PLMN must match that of the target network operator to mimic the real network.

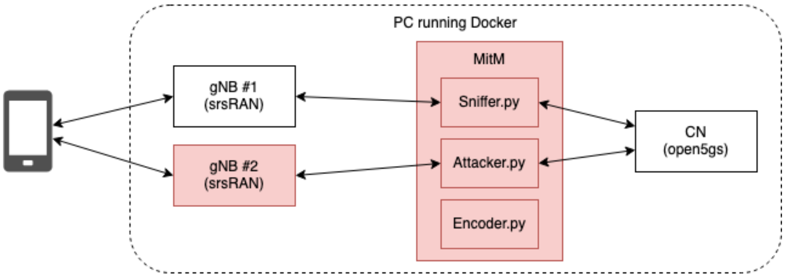

Figure 4.3: The setup of the Docker container illustrated. The red boxes represent the attacker's resources.

3. The Tracking Area Code (TAC) must be different from that of the target network. This will cause the UE to update its tracking area, triggering a `Registration Request` in 5G.

4. The DL_ARFCN must have the highest priority next to the channel being blocked. So if the DL_ARFCN of the target cell is 327340, the FBS should be configured with a slightly higher value, i.e. 327360.

4.2.4 Establishing a Man-in-the-Middle

To intercept and modify (unprotected) signalling messages between the gNBs and the 5GC, the author placed a MitM container on the NGAP layer between the two parties. The container runs three Python scripts that share one volume. Depending on the method used to obtain a SUCI, the scripts `Sniffer.py` or `Encoder.py` are executed. `Sniffer.py` is used to replicate Variant 1 while `Encoder.py` is used for Variant 2. The script `Attacker.py` performs the probing of the SUCI-Catcher attack.

Sniffer.py

The `Sniffer.py` script is responsible for monitoring the traffic between the target UE and the network in order to retrieve some SUCI of the target. The exact procedure is as follows

1. NAS messages are intercepted at the NGAP layer and the NGAP-PDU, the message data packet, is decoded.

2. The MitM looks for `Initial UE Message` or `Uplink NAS Transport` messages. These contain a decoded NAS-5G message sent to the network by the UE.

3. The NAS-5G message is decoded and its message type and IEs are checked. If the message is of the type `Registration Request`, the script will look for SUCIs in the corresponding IE.

4. If a SUCI is found, it is stored as a JSON file on the container's volume.

Encoder.py

The Encoder.py script takes an IMSI and the network's public key and derives a SUCI using Elliptic Curve Integrated Encryption Scheme (ECIES) encryption. Profile B is used as the protection scheme. The scheme input is constructed using the MSIN of the IMSI according to the 3GPP in TS 133 501, Appendix C.3.1 [3GP24b]. As with Sniffer.py, the resulting SUCI is stored as a JSON file on the container's volume.

Attacker.py

The Attacker.py script is responsible for probing the identity of a connecting UE by replacing its SUCI with the one previously collected (or generated) and analyzing the response. The exact procedure is as follows

1. Messages at the NGAP layer are intercepted and decoded analogous to the Sniffer.py script.
2. If a message of type Registration Request is found, the MitM disposes of it and creates a new (unprotected) Registration Request using a SUCI from the container's volume.
3. The network accepts the unprotected Registration Request (see Section 4.1.3) and sends an Authentication Request.
4. The MitM analyzes the response of the UE, i.e. whether the authentication was successful, and infers whether the connecting UE is the searched-for participant.

Both Sniffer.py and Attacker.py maintain the connection between the 5GC and the gNB by forwarding occurring traffic in both directions.

All three Python scripts make use of external libraries. CryptoMobile [mit] is used to perform the ECIES and derive the SUCI. Pycrate [Sec23] is used to decode and encode NAS messages, Pysctp [Sec22] is used to receive and send messages via Stream Control Transmission Protocol (SCTP).

4.2.5 Attack Execution

Once the test environment is set up, the SUCI-Catcher attack can be executed. Using the two available COTS UEs, the author was able to demonstrate both successful and failed probing attacks. The procedure is as follows:

1. The two UEs register on the network by performing the 5G-AKA and communicating with the first (legitimate) gNB. One of the UEs resembles the targeted subscriber.
2. The MitM either sniffs the SUCI of the targeted UE during the registration procedure or derives it from its known IMSI.

3. Once the UE is registered, the author starts the second (illegitimate) gNB using a specific configuration (see Section 4.2.3).

4. The UEs perform a handover to the second gNB. The MitM performs the probing attack.

5. The MitM analyzes the response of the UE and reports the results to the author. In this scenario, one probing attack succeeds and the other one fails.

A detailed visualization of the sequence of the SUCI-Catcher attack variants and the role of the MitM container can be seen in Fig. 8.1 and Fig. 8.2.

CHAPTER 5

SUCI-Catcher Attack: Mitigation

This chapter focuses on mitigating the SUCI-Catcher attack. First, existing solution approaches proposed by the 3GPP are analyzed, evaluating their implementation requirements, technical feasibility and potential effectiveness. In the second part, the author proposes and implements his own strategy to mitigate the SUCI-Catcher attack. This practical solution targets Variant 1 of the attack by identifying and preventing SUCI replay attempts.

5.1 Existing Strategies

Section 3.5 describes general proposals to improve the structure of the 5G protocol in order to eliminate one or more of the evaluated vulnerabilities. The following section describes specific approaches proposed by the 3GPP in TR 33 846 [3GP21] to mitigate the SUCI-Catcher attack. It assesses how difficult they may be to implement and which network components are affected. The 3GPP refers to each solution approach by a number. The number is given in the parentheses.

5.1.1 Keeping the Network's Public Key Secret

It is not possible for the attacker to generate his own SUCIs unless he has access to the network's public key. One way to keep the key secret would be to calculate SUCIs via the USIM instead of the UE. In this way, the key cannot be read out, preventing Variant 2 of the SUCI-Catcher attack.

Keeping the network's public key secret would be a trivial solution to prevent third parties from generating their own SUCIs. However, this approach requires that all USIMs issued comply with strict security requirements that adequately secure key material. This is proving difficult, as there is usually only one public key linked to a mobile operator and a single USIM would be sufficient for disclosure.

5.1.2 Assuring SUCI Generation by legitimate SUPI Owner (#2.8)

This solution approach introduces an additional key derivation step when generating the SUCI. The MAC tag in the SUCI is generated using a new MAC key MAC'_k:

$$MAC'_k = f(K_{SUCI}, MAC_k) \tag{5.1}$$

The function f combines the existing MAC key MAC_k with a specific key K_{SUCI}. K_{SUCI} can only be derived by knowing the long term key K_i used in the 5G-AKA (see Section 2.3.3), which effectively binds the SUCI generation to the legitimate key holder, i.e. the respective UE.

The introduction of the K_{SUCI} key adds complexity to the 5G-AKA and requires modification of the ECIES, affecting both the USIM and the network. Its implementation would mitigate Variant 2 of the SUCI-Catcher attack.

5.1.3 Detecting SUCI Replays by extending ECIES with Timestamp (#2.7)

In TR 33 846 [3GP21], the 3GPP proposes to extend the ECIES used for SUPI concealment with the field MESSAGE_TIME. MESSAGE_TIME represents the time at which the message was sent. By including the timestamp in the SUCI, the network can detect SUCI replays by comparing it with the current time, e.g. rejecting messages if MESSAGE_TIME is greater than some value MAX_DELAY.

This mitigation would counter Variant 1 of the SUCI-Catcher attack. It requires changes both to the USIM and the UDM in the core network. While the concept seems straightforward, the implementation of this approach would rely heavily on time synchronization between the UE and the network. Normally, time synchronization on the UE requires external network connectivity, e.g. via NTP server [Pro25]. This is not the case here, as the 5G-AKA is still in progress when the SUCI is sent.

5.1.4 Detecting SUCI Replays by storing SUCI and Timestamp (#2.2)

In TR 33 846 [3GP21], the 3GPP proposes to store occurring SUCIs together with the timestamp at which they were first received. When the network receives the SUCI again, it checks whether the difference between the current timestamp and the timestamp when the SUCI was first seen, is greater than the timer T3519. The UE runs the predefined timer T3519 when it sends a SUCI in a Registration Request or Identity Response message. It will not calculate a new SUCI for these type of messages, until the timer T3519 has expired. Its value is 60 seconds. The use of T3519 allows the network to detect replay attacks.

The approach mitigates Variant 1 of the SUCI-Catcher attack and can only be implemented on the network side without changing the ECIES. Depending on the size of the network, there may be a large storage overhead as each SUCI that occurs must be stored along with its timestamp. In addition, database queries can result in high latencies and delay the 5G-AKA. Cell level tracking is still possible within the `T3519` time window, although unlikely. The approach of detecting SUCI replays by storing SUCIs already in circulation, was the basis for the development of our own approach, specified in Section 5.3.

5.1.5 Detecting SUCI Replays using UE's Public Key (#2.11)

The 3GPP proposes to store the UE's public key on the network side when a transmitted SUCI is proven valid. The key can then be extracted from the received SUCI. If a public key occurs twice within a SUCI, the network infers that the SUCI in question has been replayed.

Similar to the previous approach, this would mitigate Variant 1 of the SUCI-Catcher attack and can only be implemented on the network side. There is also the issue of storage overhead as each ephemeral public key needs to be stored in the database.

5.1.6 Adding Randomness (#2.12)

This approach adds randomness and MAC verification to both the UE and the network. The UE sends a `Registration Request` containing the SUCI, a random number $RAND_{MS}$ and a key-based MAC function MAC_0. MAC_0 is specified as follows, where K is the long term key used in the 5G-AKA:

$$MAC_0 = f_0(K, SUCI, RAND_{MS}) \tag{5.2}$$

The network checks the resulting MAC and responds with its own random number $RAND_{HE}$ embedded within the authentication vector AV.

This modification to the 5G-AKA provides fresh randomness on both sides, preventing replay attacks and the Variant 1 of the SUCI-Catcher attack. It would require significant changes to the USIM, the network and cryptographic functions used within the 5G-AKA. Not only is this the most complex approach, but it also introduces an overhead in terms of the additional cryptographic operations required.

5.2 Limitations

The implementation of mitigation in our test bed is subject to certain limitations. These may be due to a lack of open source systems, the limitations of the 5G specification or the lack of system resources. This section describes the main limitations that may complicate the implementation of the mitigations presented in Section 5.1.

5.2.1 Deployment Challenges

Some mitigation approaches described in Section 5.1 require intervention in multiple network components. As this implementation of the SUCI-Catcher works with COTS smartphones and the baseband firmware of these devices is closed source [LZL+24], fundamental changes such as extending the ECIES cannot be made to the 5G protocol. As a result, the author focused on network-side changes in the proposed mitigation.

5.2.2 Limited Storage Space

Solutions #2.2 and #2.11 propose a data-driven approach where replay attacks are detected by comparing signatures or identifiers with previously stored historical data. This has the potential disadvantage of consuming a lot of storage space (see Section 5.3.1). As network storage space is limited, the author has taken care to implement a strategy to work around this problem.

5.2.3 Low Latency Requirements

Latency and delay of 5G networks is a key performance indicator (KPI) defined by the 3GPP [3GP24a]. Ultra-Reliable Low-Latency Communications (URLLC) has been introduced as a service in 5G to meet the requirement for latencies as low as 0.5ms [MVG+24]. Adding computationally intensive operations, such as expensive cryptographic functions, or querying large amounts of data could increase latency and degrade network performance. The author decided to use lightweight hash functions to overcome this limitation.

5.2.4 No Time Synchronization

Mitigation #2.7 relies heavily on time synchronization between the UE and the network, which requires an external network connection, as noted in Section 5.1.3. This is not the case, as the 5G-AKA is still running at the time the SUCI is sent. Instead of sending timestamps between the UE and the network, the author decided to use separate timers for synchronization in his mitigation.

5.3 Designing an Effective Strategy

In this section, the author describes the process of designing a mitigation strategy against the SUCI-Catcher attack. The mitigation is based on the strategy #2.2 proposed by the 3GPP. The analysis begins by identifying the limitations of the current draft through examination of an extreme case scenario. Following this assessment, the author introduces Bloom filters as an efficient mechanism for replay detection, highlighting both their beneficial and restricting properties.

5.3.1 Evaluating Limitations of the 3GPP Solution

As already mentioned in Section 5.2, the 3GPP's solution approach #2.2 has potential drawbacks. Storing all occurring SUCIs together with the timestamp at which they

Legend: ↯ = Conflict, ? = Limitation unknown

Mitigation Strategies	Limitations				Mitigates Variant
	Deployment Challenges	Limited Storage Space	Low Latency Requirements	No Time Synchronization	
Keeping Public Key Secret	?				**2**
Assuring Legitimate SUPI Owner	↯		↯		**2**
Extending ECIES with Timestamp	↯			↯	**1**
Storing SUCI and Timestamp		↯	↯		**1**
Storing UE's Public Key		↯	↯		**1**
Adding Randomness	↯		↯		**1**

Table 5.1: This table summarizes the proposed mitigation strategies by the 3GPP and its (potential) limitations. It also indicates which of the SUCI-Catcher's variants may be countered.

first occurred would result in large storage space requirements. The following example illustrates this:

Let's assume a medium-sized network serving 100,000 subscribers simultaneously. The network is configured to enforce periodic key rotation, which causes a SUCI renewal by the UE after timer `T3519` has elapsed, i.e. 60 seconds. After 24 hours, the number of records created would be as follows:

$$100,000 \cdot (24 \cdot 60) = 144,000,000 \text{ Records} \tag{5.3}$$

Assuming that a SUCI is 50 bytes and a timestamp is 8 bytes, each record requires 58 bytes of storage, giving the following storage requirements per day:

$$144,000,000 \cdot (50 + 8) = 8,352,000,000 \text{ Bytes} \; = 8.352 \text{ Gigabytes} \tag{5.4}$$

Given these dimensions and the fact that system memory is limited, it is obvious that ordinary in-memory objects or databases are not suitable for this purpose. However, relational databases require disk lookups, which are generally slower than in-memory operations. Depending on the amount of data that needs to be stored, disk-based databases can also be a significant cost factor.

It is true that the UE typically uses the 5G-GUTI instead of the SUCI for subsequent communication after a successful registration [3GP24b], so a mandatory update of the SUCI after the `T3519` timer expires is unlikely. However, this example is used to illustrate an extreme case.

5.3.2 Introducing Bloom Filters

In order to achieve fast lookup times and significantly reduce storage requirements, the author has decided to use Bloom filters to check for replayed SUCIs.

Bloom filters were developed by Burton H. Bloom in 1970 [Blo70] and are a space-efficient probabilistic data structure for testing the membership of an element. A Bloom filter consists of a bit array a of m bits, all of which are initially set to 0. When a new element is added to the set, the following operations are executed:

1. The new element e is hashed using k hash functions
2. Each output of the hash functions $h_1(e)...h_k(e)$ maps to a corresponding position $i_1...i_k$ in a bit array a.
3. The identified bits $a[i_1]...a[i_k]$ are set to 1.

To check the membership of an element e, the value of the corresponding bits is verified. If any bit is set to 0, e definitely is not a member of the Bloom filter. If all bits are set to 1, e is *probably* a member of the Bloom filter.

The time needed to add an element or to check whether an element is a member of a set is independent of the number of elements already in the set. It only depends on the performance of the hash functions used. Thus, the time complexity can be described as $O(k)$, where k is the maximum number of hash functions implemented.

Bloom filters require a fixed amount of memory per element, regardless of the size of the elements. The amount of space per element depends on the acceptable error rate. This is discussed in more detail in the next section.

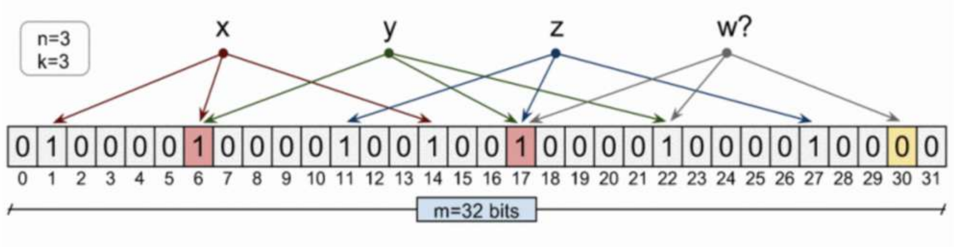

Figure 5.1: The Bloom filter illustrated. [TRL12]

False Positives

Bloom filters can tell you with certainty whether an element is *not* in the corresponding set. Conversely, membership testing can lead to false positives. False positives are elements that are not part of a set S but are reported as being in the set by the Bloom filter.

The reason for the occurrence of false positives lies in the fundamental design of the Bloom filter. Hash collisions can occur when calculating the positions in the bit array. When multiple elements are mapped to the same bit positions, the Bloom filter cannot distinguish between them.

According to Tarkoma et al. [TRL12], the probability of false positives (p) in a Bloom filter depends on the size of the bit array (m) the number of hash functions used (k), and the number of elements that are already in the set (n). While these three parameters play an important role in reducing the probability of hash collisions, the choice of hash function is also crucial. Hash functions with a good avalanche effect are preferred. A good avalanche effect means that for every change of an input bit i, each output bit j changes with 50% probability [HM24].

libbloom & Murmur2

libbloom [Vir22] is a simple open source implementation of a Bloom filter, written in plain C. The author embedded the project to use it in the Open5GS implementation. libbloom uses the non-cryptographic hash function Murmur2 [App] optimized for performance and speed. Murmur2 works through a series of simple operations [HM24]:

1. Split the input data into n 4-byte sized blocks.
2. Create a 4-byte sized initialization vector (IV).
3. For each block, perform bitwise operations such as `XOR`s, multiplications and bit rotations to obtain an intermediate value t_i. The calculation includes some constant value m.
4. Using multiplication and `XOR` again, the IV is combined with the intermediate value t_i.
5. After all the blocks have been read, the partial results $t_1 ... tn$ are mixed using `XOR`s, shifts and multiplication to produce the final hash.

Murmur2 is well known for its avalanche properties. Hayes et al. [HM24] showed that compared to other similar hash functions, Murmur2 is the best at avoiding collisions.

libbloom calculates the number of bits m and the number of hash functions k based on the number of items (n) the user wants to store in the Bloom filter and the acceptable false positive rate (p):

$$m = -\left\lceil \frac{n \cdot \ln(p)}{\ln(2)^2} \right\rceil \tag{5.5}$$

$$k = \text{round}\left(\frac{m}{n} \cdot \ln(2)\right) \tag{5.6}$$

The user therefore needs to know beforehand how many items he wants to store in the Bloom filter and how high the error rate can be when testing an item for membership. Using the values of the extreme example, with 144 million records per day and a false positive rate of 1:100,000 ($p = 0.00001$), the required storage space would be as follows:

$$m = -\left\lceil \frac{144,000,000 \cdot \ln(0.00001)}{\ln(2)^2} \right\rceil = 3,450,621,000 \text{ Bits } \approx 431.3 \text{ Megabytes} \tag{5.7}$$

It is clear that the trade-off between correctness and memory consumption plays a role in the design of the Bloom filter.

5.4 Our Approach

This section describes the operation of the author's mitigation approach and its impact on the network. All modifications necessary to implement the mitigation were made in the Open5GS codebase [Ope25]. To extend the project with Bloom filters, the C library libbloom [Vir22] was integrated. The mitigation aims to prevent Variant 1 of the SUCI-Catcher attack.

5.4.1 Network Impacts

To determine the starting point for the changes in the system, it's important to understand the interaction between the network functions in 5G. When an authentication procedure is initiated using a SUCI, the following process occurs [3GP24b, 3GP21]:

1. The UE sends the `Registration Request` containing the SUCI to the SEAF.
2. The SEAF sends a `Nausf_UEAuthentication_AuthenticateRequest` message containing the SUCI to the AUSF.
3. The AUSF sends a `Nudm_UEAuthentication_Get Request` message containing the SUCI to the UDM.
4. The SIDF of the UDM decrypts the SUCI to obtain the corresponding SUPI. Based on the SUPI, the UDM selects the authentication method and generates the AV. The authentication then continues according to the 5G-AKA (see Section 2.3.3).

The aim is to extend the UDM in such a way that in the case of a SUCI-Catcher attack according to Variant 1, the UDM rejects the authentication attempt for the UE. The exact communication exchange is illustrated in Fig. 5.2.

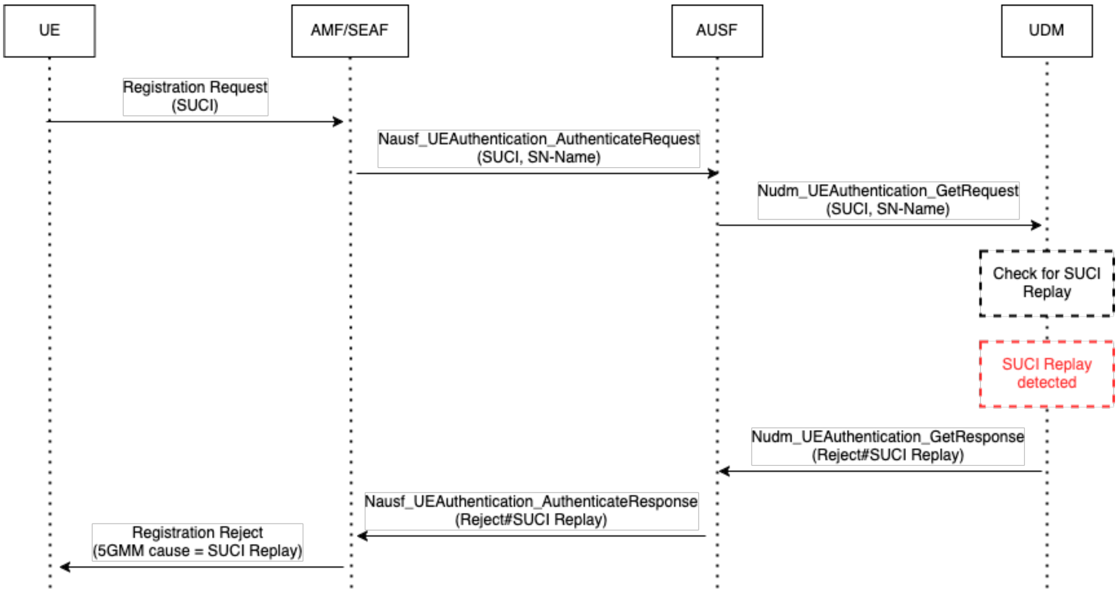
UE
AMF/SEAF
AUSF
UDM
Registration Request (SUCI)
Nausf_UEAuthentication_AuthenticateRequest (SUCI, SN-Name)
Nudm_UEAuthentication_GetRequest (SUCI, SN-Name)
Check for SUCI Replay
SUCI Replay detected
Nudm_UEAuthentication_GetResponse (Reject#SUCI Replay)
Nausf_UEAuthentication_AuthenticateResponse (Reject#SUCI Replay)
Registration Reject (5GMM cause = SUCI Replay)

Figure 5.2: The communication exchange between UE and UDM using our SUCI replay mitigation. The UE's registration attempt is rejected with cause `SUCI Replay`.

5.4.2 Implementation Details

In Open5GS, additional functionality is added to the UDM to handle incoming `Nudm_UEAuthentication_GetRequest` messages: When a SUCI is received, the network uses the Bloom filter – referred to as `bloom_filter` – to check if it has already been used for registration in the past. SUCIs are not added to the Bloom filter until after the `T3519` timer has expired. A hash set called `active_suci_hash` is used to keep track of active SUCIs whose timer has not expired. If a replay attack is detected, the UDM rejects the registration request with cause `SUCI Reject`.

The pseudocode seen in Alg. 5.1 illustrates the function responsible for detecting a replay attack, while the pseudocode in Alg. 5.2 represents the procedure to be executed at the end of a timer.

Fig. 5.3 illustrates the mitigation workflow. In order to avoid false positives, the author took care to use reasonable properties, including size and accuracy, when creating the Bloom filter. During implementation, attention was paid to dynamic memory allocation and thread safety. To avoid losing the data after a restart, the Bloom filter is saved before the application is closed and reloaded at startup. It has been ensured that resources such as instances of the `T3519` timer are deallocated after their completion.

Algorithm 5.1: SUCI Handler for Replay Detection

```
Function handle_suci(suci, bloom_filter, active_suci_hash):
    if bloom_filter.contains(suci) then
        print("Replay attack detected");
        return false ;     /* Registration Request gets rejected */
    end
    active_entry ⟵ active_suci_hash.get(suci);
    if active_entry = null then
        /* An entry consists of a SUCI and a T3519 timer     */
        new_entry ⟵ create_entry(suci);
        active_suci_hash.add(new_entry);
        start_timer(new_entry, 60);
    end
    return true ;                           /* 5G-AKA continues ...   */
```

Algorithm 5.2: Timer Callback Function

```
Function timer_callback(entry, bloom_filter, active_suci_hash):
    active_suci_hash.delete(entry);
    suci ⟵ entry.get_suci();
    bloom_filter.add(suci);
```

5.5 Identified Shortcomings

The proposed mitigation ensures that SUCI replays are detected by the network and can no longer be used within the SUCI-Catcher attack to deanonymize subscribers. The Bloom filters are a fast and resource-efficient way to check whether a SUCI has already been used. The introduction of `T3519` timers on the network side ensures that there is no need to store timestamps in addition to the identifiers. However, the addition of new functionality may introduce security vulnerabilities. The author has attempted to identify possible flaws in the proposed approach and their impact on the network.

5.5.1 Attacks inside T3519 Window

The mitigation presented prevents SUCI replay attacks from taking place after the `T3519` timer has expired. Before that, an attacker still has the opportunity to abuse the SUCI. However, the question is how useful an attack within the `T3519` window would be. The advantage of the SUCI-Catcher attack is that an attacker only needs to intercept a single SUCI from a participant to track their presence over an undefined period of time. Limiting the validity of the SUCI to 60 seconds makes this impossible and therefore invalidates the attack. Luring multiple UEs to one's fake base station and probing each of them against the network may also be time-consuming and simply not possible within

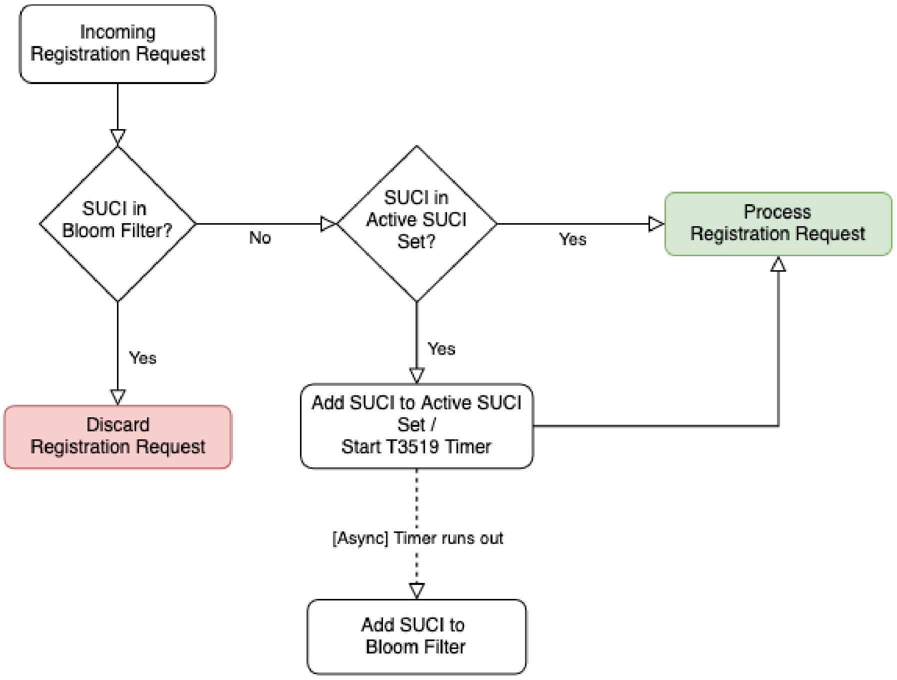

Figure 5.3: A diagram showing the workflow of our mitigation strategy using Bloom filters.

this relatively short time. According to Cabrera et al. [CG24], successful probing of a SUCI in a real network can take from 10 minutes to almost 7 hours.

5.5.2 Retention of Registration Requests

When intercepting a `Registration Request` message and its SUCI, an attacker can deliberately not forward the data to the network. This ensures that the network does not know about the SUCI, making the identifier usable in a replay attack. However, the identifier can only be used in a probing attack, as it is then known to the network. Since the attacker usually needs several attempts to successfully SUCI probe, it does not seem to make sense to keep SUCIs from the network. It also prevents long term tracking of a participant, similar to Section 5.5.1, Attacks within `T3519` window.

5.5.3 Denial of Service Attacks

The UDM creates and starts an instance of the `T3519` timer for each new SUCI it receives. An attacker could theoretically take advantage of this mechanism. By sending many registration requests with different SUCIs to the network in a short period of time, the attacker could claim too many of the system's resources, causing a Denial of Service (DoS) attack.

5.5.4 False Positives

As already mentioned in Section 5.3.2, Bloom filters can return false positives when testing an element for membership. While it is theoretically possible to take a Bloom filter and increase its size and hashing until the probability of a false positive is effectively zero, this would negate the primary benefit of the Bloom filter - its small size. It is therefore only possible to minimize the probability of false positives, and their occurrence must be taken into account.

5.5.5 UE Blacklisting Network

A false positive in the mitigation presented would mean that the network (mistakenly) rejected a legitimate request from some UE. Multiple unanswered requests could cause the UE to cancel registration attempts, essentially *blacklisting* the network [CRPH21]. This is a special case of the effects of false positives.

5.5.6 Static Filter Size

The size of the Bloom filter is static and must be determined during initialization. This can be a significant limitation, as the network operator needs to know in advance how many SUCIs to expect. To be on the safe side, the operator can choose a very large size for the Bloom filter. In this case, however, the main advantage of the Bloom filter - its relatively small memory footprint - may no longer apply.

5.6 Future Improvements and Extensions

This section describes possible improvements to our approach. The suggestions are aimed at addressing some weaknesses identified in Section 5.5. An illustration comparing drawbacks and improvements can be found in Tbl. 5.2.

5.6.1 Dynamic Bloom Filters

Guo et al. [GWC+10] introduced the idea of Dynamic Bloom Filters (DBFs). A DBF consists of several homogeneous Standard Bloom Filters (SBFs), i.e. regular Bloom filters. It starts with an active SBF and adds more SBFs as needed. New elements are only added to the active SBF. When the active SBF reaches its capacity, it becomes inactive and a new active SBF is added.

The library used, libbloom, has its own functions for saving, loading and merging Bloom filters. Therefore, it would not require many changes to the code base in order to add dynamic Bloom filters to our proposed mitigation. The procedure could be as follows:

1. When an active SBF becomes full, it becomes inactive and is persisted out of memory.

2. A new active SBF is created with a higher capacity, e.g. $2 * m$.

3. A background process loads up the recently inactive SBF and merges it into the active SBF.

4. When the inactive and active SBFs are fully merged, we can remove the inactive SBF from the persistent storage.

5.6.2 Stable Bloom Filters

Regular Bloom filters have the limitation that they cannot distinguish between newer and older items. Furthermore, it is not possible to forget old items and make room for new ones. Deng et al. [DR06] introduced the concept of Stable Bloom Filters (StaBFs), an extension of regular Bloom filters specifically designed for duplicate detection. As new items are added to the StaBF, both older and *unwanted* information (i.e. items that are not requested as often) have a higher probability of being discarded. This saves storage space, resulting in lower Bloom filter utilization and a lower false positive rate. The authors found that, for a given false positive rate, StaBFs were superior to the alternative methods in terms of both accuracy and time for a given amount of space.

In the case of SUCI replay detection, StaBFs can be a useful mitigation extension. Since cells in StaBFs consist of multiple bits acting as counters rather than single bits, this implementation requires fundamental changes to the (regular) Bloom filter.

5.6.3 Introducing a Delay Timer on UE

To prevent the UE from blacklisting the network in case of a false positive when checking its SUCI for membership, an additional timer T_{DELAY} could be introduced. If the network does not respond to the UE's `Registration Request` within the window of T_{DELAY}, the UE generates a new SUCI and uses it within its next request. This way, only one of the UE's request is discarded, as the occurrence of false positives across multiple SUCIs is very unlikely (p^2). That is, if the chosen probability p is low enough.

5.6.4 Allocating Timer after Authentication

As already discussed in Section 5.5.3, an attacker can flood the network with a numerous `Registration Request` messages, thus overloading the network system by creating many instances of the `T3519` timer. This is particularly the case with Variant 2 of the SUCI-Catcher, where an attacker can generate any number of SUCIs himself. To prevent this, it is important to distinguish malicious authentication requests from legitimate ones.

In addition to the known anomalies used to detect FBSs, the following property is of particular importance: An attacker who wants to initiate as many authentication processes as possible on the network is unlikely to respond to all the requests that the network sends subsequently. Therefore, to make our mitigation approach more resilient, the `T3519` timer could only be created after a UE has been successfully authenticated.

However, this would have the disadvantage that, in combination with request retention (see Section 5.5.2, Retention of Registration Requests), SUCIs can be used as often as desired for the probing attack as long as the 5G-AKA is not carried out.

5.6.5 Storing selected SUCI Components

Instead of storing all 50 bytes of a SUCI in the Bloom filter, certain parts of the identifier may be ignored. This is because some components are often constants or predictable values for a given network operator. These fields may include:

- SUPI Type: Usually a network will only accept one type of identifier.
- Home Network Identifier: A network usually has one identifying PLMN.
- Routing Indicator: This value can be a constant for participants in the same network slice.
- Protection Scheme ID: A network usually has only one protection scheme.
- Home Network Public Key Identifier: A network operator typically maintains a very limited number of public keys for SUCI encryption.

Other characters that are used for padding may also be removed, if necessary.

Since the memory requirements of the Bloom filter are independent of the size of its elements, reducing the SUCI to certain components has no direct effect in this regard. However, removing constant or predictable values from the Bloom filter would produce more distinct patterns in the underlying bit array and reduce the probability of hash collisions (see Section 5.3.2).

Legend: ● = direct effect, ◗ = partial effect
★ = low, ★★ = medium, ★★★ = high

Shortcomings	**Improvements**					**Impact**
	Dynamic Bloom Filters	Stable Bloom Filters	Delay Timer on UE	Timer after Authentication	Storing selected SUCI Components	
Attacks inside `T3519` Window						★
Retention of Registration Requests						★
Denial of Service Attacks				●		★★★
False Positives	◗	●	◗		◗	★★
UE Blacklisting Network	◗	◗	●		◗	★★★
Static Filter Size	●	◗				★★

Table 5.2: An overview of the identified shortcomings and the extent to which the described improvements can overcome them. The last column indicates the severity of the impact of the shortcoming on the functioning of the mitigation measure or network.

CHAPTER 6

Related Work

6.1 SUCI-Catcher Attack

This work is not the first attempt to implement and detect or rather mitigate the SUCI-Catcher attack:

Chlosta et al. [CRPH21] demonstrated the SUCI-Catcher attack in a standalone 5G network for the first time, referring to the work of Basin et al. [BDH+18] who had previously identified the underlying vulnerability. Their setup consists of the open source Free5GC [Fre25] 5G Core Network (5GC) and commercial Amarisoft solutions. In their lab conditions, the authors were able to test 500 identities within 60 seconds. To achieve this, they introduced a *Reset & Sync* phase to allow for multiple identity probing. In commercial networks, however, the attack resulted in throttling that limited its scalability. In their paper, Chlosta et al. did not provide any implementation details of their test setup. They concluded that SUCI-Catchers are particularly suitable for targeted tracking of small groups.

In addition to replicating the SUCI-Catcher attack, Barraud et al. [BCP+23] performed traffic analysis using rule-based and AI-based systems to detect ongoing attacks. For their test bed, the authors used UERANSIM [Gü25] to simulate User Equipment (UE) and Next-Generation Node B (gNB), and Free5GC as the 5GC. Similar to Chlosta et al., no implementation details are discussed in their work. Barraud et al. were able to effectively detect the SUCI-Catcher attack with detection times of less than 1 second.

Tucker et al. [TBK+25] have also worked on the detection of IMSI and SUCI catchers using traffic analysis: They identified 53 different messages across GSM to 5G networks that can expose IMSIs in LTE or SUCIs in 5G. They then monitored cellular downlink traffic, capturing each of the popular frequencies used in networks. By creating baseline profiles that define the regularity with which radio messages typically expose IMSIs, the authors were able to identify anomalies and detect the presence of IMSI-Catchers.

Parkin et al. [PT25] have developed a mitigation that uses an ephemeral identifier derived from the SUPI, rather than using the SUPI directly. Their approach has parallels to the ratcheting mechanism used in the Signal Protocol, but is applied to subscriber privacy. Parkin et al. were able to mitigate both variants of the SUCI-Catcher attack. Their solution is backwards-compatible with existing networks and requires modifications on USIMs only.

6.2 Fake Base Station Detection

The general detection of a Fake Base Station (FBS) in mobile networks is not part of this thesis. However, it plays an important role in preventing attacks such as the SUCI-Catcher. If a FBS can be detected at an early stage by the UE, an attack may not occur in the first place. Several researchers have worked on detecting rogue base stations in LTE and 5G:

Purification et al. [PWK$^+$24] investigated the detection and blacklisting of rogue base stations in cellular networks with a focus on LTE and 5G. They propose a novel detection scheme that tracks both connection setup time and the number of registration requests to identify malicious BSs that disrupt user connectivity, while avoiding false positives. Their solution builds on the 5G protocol and requires implementation on the UE only.

Mubasshir et al. [MKB25] present FBSDetector, a machine learning-based framework for detecting FBSs and Multi-Step Attacks (MSAs) in LTE networks. For FBS detection, they use packet-level classification using stateful LSTM with attention and trace-level classification for contextual analysis. For MSA detection, the framework uses graph learning to capture attack patterns by converting attack signatures into graphs. The final solution is deployed as a mobile application and detects FBSs with 96% accuracy and a false positive rate of 2.96%, as well as 21 different MSAs with 86% accuracy. FBSDetector outperforms similar solutions for FBS detection under LTE. It is purely software-based and does not require any changes to the protocol.

6.3 Bloom Filters for Replay Detection

Bloom filters are widely used in network security. Applications range from Firewalling to DoS attack detection to spam filtering [GA13]. In this work, Bloom filters were used to detect a variant of the SUCI-Catcher attack. Other types of replay attacks have also been detected in this way in the past:

Huang [Hua08] has used Bloom filters in wireless sensor networks to efficiently check the freshness of transmitted messages. His protocol, called *Low-Overhead Freshness Transmission* (LOFT), maintains a Bloom filter of the last w messages sent by a participant. Before checking the freshness of a message in detail, the receiver quickly checks whether the message appears in the Bloom filter of recent messages. If found in the filter, the message may be a replayed message and requires further verification.

Jinwala et al. [JPPD12] implemented an anti-replay mechanism at the link layer of wireless networks. Instead of storing hash values or counters of received packets, one of their approaches uses Bloom filters to reduce memory overhead. In this scenario, the received packets are fully hashed and inserted into the Bloom filter. This allows the network to determine if an incoming packet has been seen before. The authors conclude that the approach works well regardless of network size, but also address the issue of a higher chance of false positives as the number of packets increases.

6.4 5G Network Setup

In this thesis, a 5G SA test bed was set up using open source software and off-the-shelf hardware. This process and the associated challenges were documented in the course of the work. In addition to our contribution, other works addressed the process of setting up private 5G networks using open source software.

Mamushiane et al. [MLKM23] successfully deployed a 5G SA network using open source components, namely srsRAN as the 5G-RAN and Open5GS as the 5GC, on off-the-shelf hardware. Their work highlights significant challenges in integrating commercial UE, including device compatibility, USIM card programming and SDR configuration. With detailed troubleshooting solutions for common errors and performance issues, their work serves as a valuable guide for researchers looking to set up a 5G test bed.

Mukute et al. [MML+24] analysed three popular open source 5G core network implementations (OpenAirInterface, Open5GS and free5GC), focusing on their control plane performance. They assessed each implementation's maturity and compliance with 3GPP standards, as well as performance bottlenecks. Based on their findings, Open5GS demonstrated the best overall performance and the highest support for most NF operations.

6.5 Man-in-the-Middle Attack Prevention

In recent years, research has focused on preventing MitM attacks across various domains, including SSL/TLS and Spoofing-based MitM. SSL/TLS MitM is a form of active network eavesdropping where the attacker intercepts the communication channel between two victims.

In SSL/TLS MitM, the attacker usually intercepts the communication channel between the victim's browser and the web server. Karapanos et al. [KC14] examined SSL/TLS MitM attacks in web applications where attackers impersonate legitimate servers to compromise user account. They found that a Channel ID-based client authentication alone is insufficient to prevent MitM attacks, as those defenses can be bypassed by injecting malicious JavaScript, referred to as Man-in-the-Middle-Script-in-the-Browser (MITM-SITB). The authors propose a solution called Server Invariance with Strong

Client Authentication (SISCA) to prevent both conventional MitM and MITM-SITB atttacks without requiring complete server authentication.

Spoofing-based MitM refers to communication interception within the means of a spoofing attack, including ARP spoofing. ARP spoofing is a common attack where an attacker associates its MAC address with the IP address of a legitimate host. Morsy et al. [MN22] present a detection scheme for ARP spoofing attacks, titled D-ARP. D-ARP sends signed ARP packets in parallel with original packets, creating a correlation between requests and replies using injected keys. Their solution does not rely on a central server and has minimal overhead. In the tests, D-ARP successfully detected various ARP spoofing attacks while having zero false positives and negatives.

CHAPTER 7

Conclusion & Future Work

This thesis presents an investigation of the SUCI-Catcher attack, its replication in a controlled environment, and the implementation of a network-side mitigation strategy employing Bloom filters.

We started the research with an analysis of vulnerabilities in mobile networks, focussing on Long Term Evolution (LTE) and 5G systems. We looked at various attacks that exploit these vulnerabilities to deanonymize subscribers, compromising their privacy. Additionally, we evaluated potential improvements to the 5G protocol specifically designed to protect subscriber anonymity.

To replicate the SUCI-Catcher attack, we established a test environment consisting of a 5G Standalone (SA) network and a Man-in-the-Middle (MitM) using open-source software and commercial off-the-shelf (COTS) hardware. Furthermore, we employed two commercially available smartphones to simulate a real-world attack scenario. Throughout this process, we documented all implementation details, including system configurations and pitfalls that we encountered.

Our proposed mitigation strategy is based on Subscription Concealed Identifier (SUCI) replay detection implemented through Bloom filters. During the design phase of this detection mechanism, we evaluated existing approaches and considered the practical limitations imposed by real-world deployment scenarios. We successfully integrated our theoretical approach into a 5G Core Network (5GC) implementation of choice, namely Open5GS, and published the code base. Throughout this process, we assessed both the advantages and disadvantages of using Bloom filters for replay detection.

Within our established test bed, we demonstrated the effectiveness of our approach in detecting and countering Variant 1 of the SUCI-Catcher attack. Finally, we performed a critical analysis of our solution, identifying potential shortcomings and discussing improvements that could further enhance its robustness and applicability in 5G networks.

There is a scope for future research in this area. One direction would be to investigate Bloom filter extensions, such as Dynamic Bloom Filters (DBFs) or Stable Bloom Filters (StaBFs), more and conduct test scenarios to determine which Bloom filter implementation strategy is most effective for our mitigation approach. Another area requiring further examination is the behavior of the User Equipment (UE) when encountering false positives in the Bloom filter, which results in unanswered registration procedures. This could create problems during authentication and needs to be investigated. Additionally, the compatibility of our solution with 5G network slicing technology requires further exploration. Given the distributed nature of network slicing, implementing a synchronization mechanism between multiple Bloom filter instances may be necessary to maintain consistent replay protection across the network. With respect to Variant 2 of the SUCI-Catcher attack, a research direction would be to develop mechanisms to secure the network's public key stored on Universal Subscriber Identity Modules (USIMs) appropriately.

CHAPTER 8

Appendix

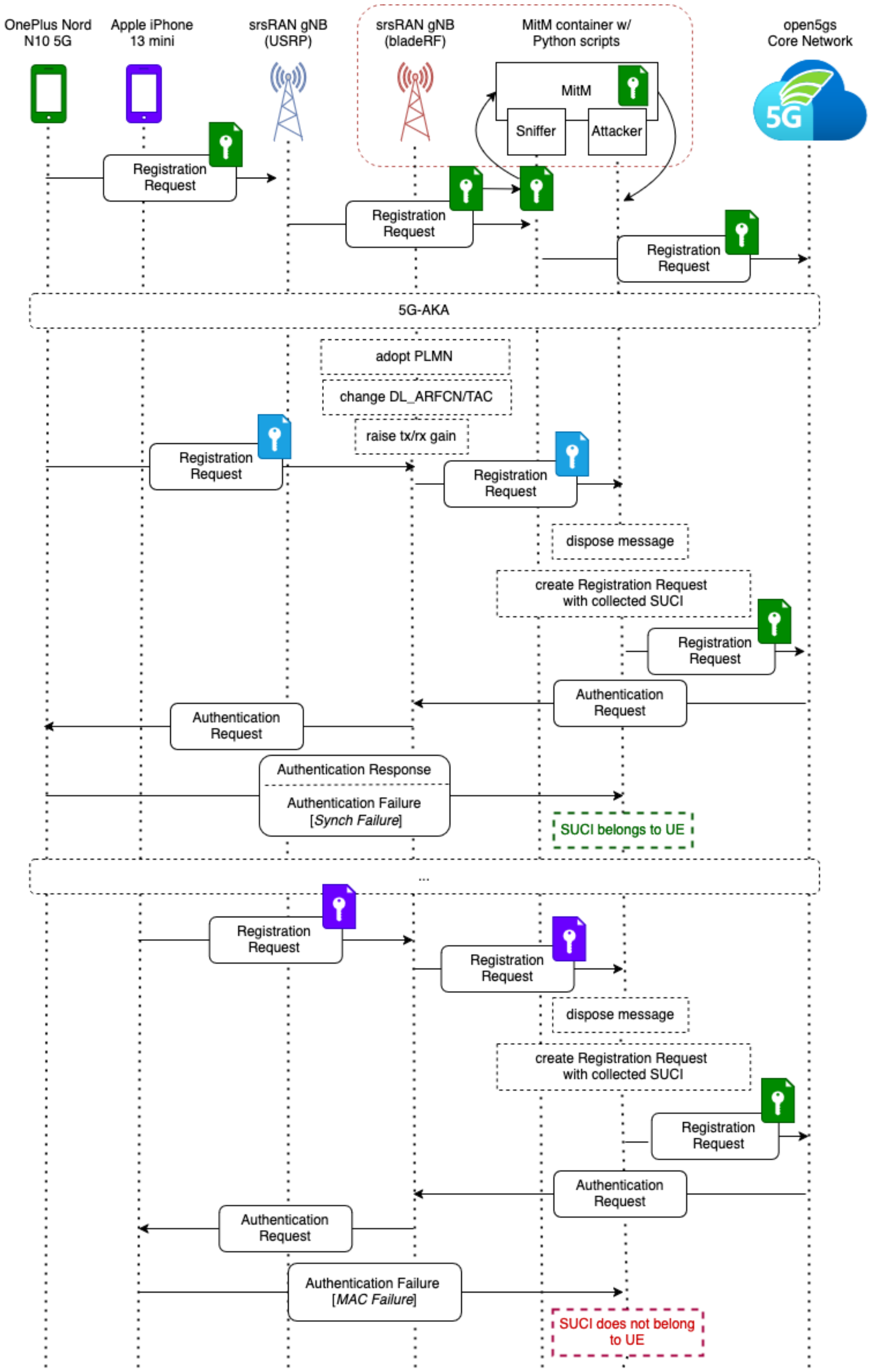

Figure 8.1: A detailed visualization of Variant 1 of the SUCI-Catcher's implementation in a 5G SA network. The searched-for UE as well as the respective SUCI are displayed in green. The malicious party is circled in red.

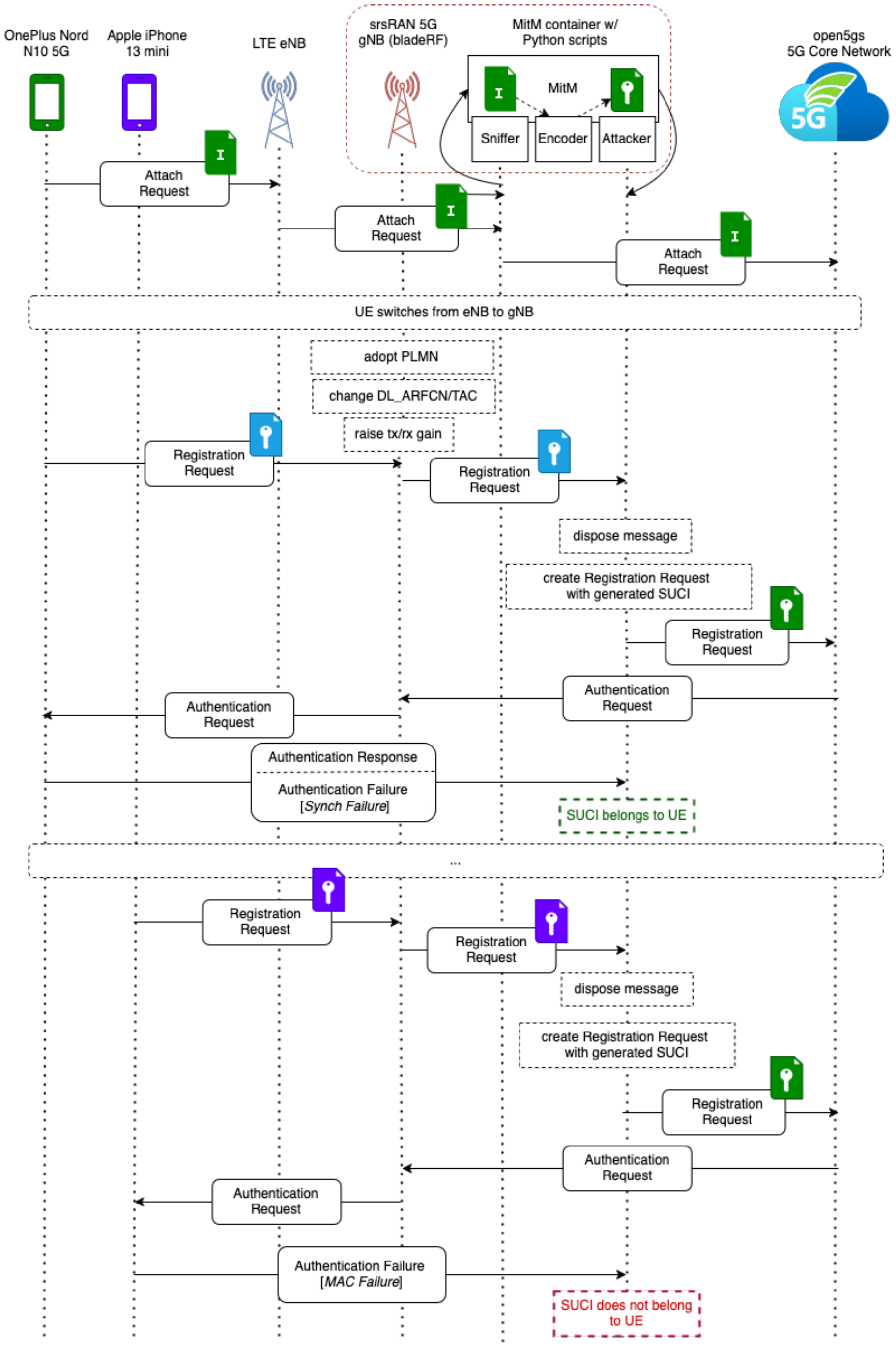

Figure 8.2: A detailed visualization of Variant 2 of the SUCI-Catcher's implementation in a 5G NSA network. The searched-for UE as well as the respective IMSI and generated SUCI are displayed in green. The malicious party is circled in red.

List of Figures

List of Tables

List of Algorithms

Acronyms

3GPP 3rd Generation Partnership Project. xi, xiii, 9, 16, 21, 23, 25–30, 40, 41, 43, 44, 46, 48, 50, 53–56, 71

5G-AKA 5G Authentication and Key Agreement. xi, xiii, 16, 17, 21, 36, 50, 54–56, 60, 66, 79

5G-GUTI 5G Globally Unique Temporary Identifier. 13, 15, 16, 27, 28, 35, 41, 48, 58

5G-RAN 5G Radio Access Network. 11, 12, 43, 71

5G-S-TMSI 5G S-Temporary Mobile Subscription Identity. 15, 20, 28, 35

5G-TMSI 5G Temporary Mobile Subscription Identity. 15, 28

5GC 5G Core Network. xi, xiii, 11–13, 43, 44, 46, 48–50, 69, 71, 73

AKA Authentication and Key Agreement. 6, 10, 16, 21, 29

AMF Access and Mobility Management Function. 13, 15, 20, 46, 48

AMFI AMF Identifier. 15

ARPF Authentication Credential Repository and Processing Function. 13, 17

AS Access Stratum. 19

AUSF Authentication Server Function. 13, 14, 16, 17, 60

AV Authentication Vector. 16

BS Base Station. 2, 6, 7, 11, 12, 26, 28, 31–33, 35, 48, 70

C-RNTI Cell Random Network Temporary Identifier. 29, 35, 41

CN Core Network. 2, 7, 11, 20

COTS commercial off-the-shelf. 44, 46, 47, 50, 55, 73

CP Control Plane. 7, 11, 13, 18

DBF Dynamic Bloom Filter. 64, 74

DoS Denial of Service. 26, 38, 63, 70

E-UTRAN Evolved UMTS Terrestrial Radio Access Network. 6, 7, 12

ECC Elliptic Curve Cryptography. 29

ECIES Elliptic Curve Integrated Encryption Scheme. 14, 18, 29, 41, 46, 48, 50, 54, 56, 79

eNB Evolved Node B. 7, 12, 19, 26, 27, 39, 79

EPC Evolved Packet Core. 6, 7, 13

EPS-AKA Evolved Packet System Authentication and Key Agreement. 10, 11, 26, 79

FBS Fake Base Station. 28, 31–34, 36, 39, 41, 48, 49, 65, 70, 79

FOSS free and open-source software. 43, 44

gNB Next-Generation Node B. 12, 19, 39, 46, 48–51, 69, 79

GPSDO global positioning system disciplined oscillator. 44, 46

GPSI Generic Public Subscription Identifier. 8

GSM Global System for Mobile Communication. 5, 6, 32, 34, 39, 69

GUAMI Globally Unique AMF Identifier. 15

GUMMEI Globally Unique Mobility Management Entity Identifier. 9

GUTI Globally Unique Temporary ID. 8–10, 13, 15, 27, 35

HN Home Network. 12–16, 18, 30

HNI Home Network Identity. 9

HSS Home Subscriber Server. 7, 10

IE Information Element. 19, 49

IMEI International Mobile Equipment Identifier. 8, 24, 33, 34

IMSI International Mobile Subscriber Identity. xi, xiii, 1, 8–10, 14, 20, 24–28, 30, 33–38, 41, 48, 50, 69, 79

IP Internet Protocol. 6, 7, 72

LTE Long Term Evolution. xi, xiii, 2, 5–13, 15, 16, 18–20, 24–29, 34, 38, 39, 48, 69, 70, 73, 79

M-TMSI MME-Temporary Mobile Subscriber Identity. 9

MAC Message Authentication Code. 18, 19, 54, 55, 72

MCC Mobile Country Code. 8, 9, 37, 46

MitM Man-in-the-Middle. 6, 31–33, 48–51, 71–73

MME Mobility Management Entity. 7, 9, 10, 20

MME ID Mobile Management Entity ID. 9

MNC Mobile Network Code. 9, 37

MSIN Mobile Subscriber Identification Number. 9, 35, 50

MSISDN Mobile Station International Subscriber Directory Number. 8

NAI Network Access Identifier. 14

NAS Non-Access Stratum. 19–21, 29, 31, 37, 39, 48–50, 79

NF Network Function. 13

NR New Radio. 11

NSA Non-Standalone. 11, 12, 77, 80

O-RAN Open RAN. 43

OAI OpenAirInterface. 44

PCF Policy Control Function. 13

PCRF Policy and Charging Rules Function. 7

PDN-GW Packet Data Network Gateway. 7

PLMN Public Land Mobile Network. 9, 14, 15, 46, 48, 66

PO Paging Occasion. 20, 35, 41

QoS Quality of Service. 7, 13

RAN Radio Access Network. 7, 43, 44

RF Radio Frequency. 46

RRC Radio Resource Control. 19–21, 26, 28, 29, 31, 32, 79

SA Standalone. 2, 11, 12, 39, 43–47, 71, 73, 76, 79, 80

SBF Standard Bloom Filter. 64, 65

SDR Software Defined Radio. 31, 33, 44, 46, 71

SEAF Security Anchor Function. 13, 16, 17, 60

SGW Serving Gateway. 7

SIDF Subscription Identifier De-concealing Function. 13, 16, 17, 60

SN Serving Network. 12, 16, 17

srsRAN srsRAN Project. 43, 44, 46, 48, 71

StaBF Stable Bloom Filter. 65, 74

SUCI Subscription Concealed Identifier. xi, xiii, 1, 13–18, 28–30, 34, 36, 38, 41, 46–50, 53–58, 60–66, 69, 73, 79

SUPI Subscription Permanent Identifier. 13, 14, 17, 18, 24, 28–30, 36, 37, 41, 46, 48, 54, 60, 66, 70, 79

TMSI Temporary Mobile Subscriber Identity. 29, 34, 41

UDM Unified Data Management. 13, 14, 16, 17, 46, 47, 60, 61, 63, 79

UE User Equipment. 2, 7–16, 18–21, 23–39, 41, 44, 46–51, 53–58, 60–62, 64, 65, 69–71, 74, 79

UMTS Universal Mobile Telecommunications System. 6, 10, 34

UP User Plane. 7, 12, 13, 32, 33

USIM Universal Subscriber Identity Module. 7, 8, 10, 13, 14, 18, 24, 40, 41, 44, 46–48, 53–55, 70, 71, 74

Bibliography

[3GP17] 3GPP. Study on the security aspects of the next generation system. Technical Report TR 33.899, 3rd Generation Partnership Project, August 2017. Release 14.

[3GP19] 3GPP. Study on the support of 256-bit algorithms for 5G. Technical Report TR 33.841, 3rd Generation Partnership Project, March 2019. Release 16.

[3GP21] 3GPP. Study on authentication enhancements in the 5G System (5GS). Technical Report TR 33.846, 3rd Generation Partnership Project, December 2021. Release 17.

[3GP22a] 3GPP. Digital cellular telecommunications system (Phase 2+) (GSM); GSM/EDGE Radio subsystem link control. Technical Specification TS 145 008, 3rd Generation Partnership Project, May 2022. Release 17.

[3GP22b] 3GPP. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; International Mobile station Equipment Identities (IMEI). Technical Specification TS 122 016, 3rd Generation Partnership Project, May 2022. Release 17.

[3GP22c] 3GPP. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Network architecture. Technical Specification TS 123 002, 3rd Generation Partnership Project, May 2022. Release 17.

[3GP22d] 3GPP. Digital cellular telecommunications system (Phase 2+) (GSM);Universal Mobile Telecommunications System (UMTS); LTE; 5G; 3G security; Security architecture, May 2022. Release 17.

[3GP23] 3GPP. Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification, July 2023. Release 17.

[3GP24a] 3GPP. 5G; Management and orchestration; 5G end to end Key Performance Indicators (KPI). Technical Specification TS 128 554, 3rd Generation Partnership Project, October 2024. Release 17.

[3GP24b] 3GPP. 5G; Security architecture and procedures for 5G System. Technical Specification TS 133 501, 3rd Generation Partnership Project, July 2024. Release 17.

[3GP24c] 3GPP. 5G; System architecture for the 5G System (5GS). Technical Specification TS 123 501, 3rd Generation Partnership Project, October 2024. Release 17.

[3GP24d] 3GPP. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode. Technical Specification TS 136 304, 3rd Generation Partnership Project, January 2024. Release 17.

[3GP24e] 3GPP. Universal Mobile Telecommunications System (UMTS); LTE; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3. Technical Specification TS 124 301, 3rd Generation Partnership Project, July 2024. Release 17.

[3GP25a] 3GPP. 5G; Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3. Technical Specification TS 124 501, 3rd Generation Partnership Project, March 2025. Release 17.

[3GP25b] 3GPP. 5G; NR; NR and NG-RAN Overall description; Stage-2. Technical Specification TS 138 300, 3rd Generation Partnership Project, April 2025. Release 17.

[3GP25c] 3GPP. 5G; NR; Radio Resource Control (RRC); Protocol specification. Technical Specification TS 138 331, 3rd Generation Partnership Project, 2025. Release 17.

[3GP25d] 3GPP. 5G; NR; User Equipment (UE) procedures in idle mode and in RRC Inactive state. Technical Specification TS 138 304, 3rd Generation Partnership Project, January 2025. Release 17.

[3GP25e] 3GPP. LTE; Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification. Technical Specification TS 136 331, 3rd Generation Partnership Project, April 2025. Release 17.

[AMRR17] Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, and Mark Dermot Ryan. Analysis of privacy in mobile telephony systems. *Int. J. Inf. Secur.*, 16(5):491–523, October 2017. doi: 10.1007/s10207-016-0338-9.

[BCP+23] Lorens Barraud, Francesco Caccavale, Jean-Baptiste Peyrat, Wissam Mallouli, Véronique Capdevielle, Hicham Khalife, and Ana Rosa Cavalli. 5G SUCI Catcher: Attack and Detection. In *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, pages 285–290, 2023. doi: 10.1109/CloudCom59040.2023.00053.

[BDH+18] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. A Formal Analysis of 5G Authentication. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1383–1396, New York, NY, USA, 2018. Association for Computing Machinery. doi: 10.1145/3243734.3243846.

[BHPS18] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols, 2018. doi: 10.2478/popets-2019-0039.

[BKS+23] Evangelos Bitsikas, Syed Khandker, Ahmad Salous, Aanjhan Ranganathan, Roger Piqueras Jover, and Christina Pöpper. UE Security Reloaded: Developing a 5G Standalone User-Side Security Testing Framework. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '23, pages 121–132. Association for Computing Machinery, 2023. doi: 10.1145/3558482.3590194.

[Blo70] Burton H. Bloom. Space/time trade-offs in hash coding with allowable errors. *Commun. ACM*, 13(7):422–426, July 1970. doi: 10.1145/362686.362692.

[BR20] Vaishali Bhatia and K.R. Ramkumar. An Efficient Quantum Computing technique for cracking RSA using Shor's Algorithm. In *2020 IEEE 5th International Conference on Computing Communication and Automation (ICCCA)*, pages 89–94, 2020. doi: 10.1109/ICCCA49541.2020.9250806.

[CG24] Pedro Cabrera and Miguel Gallego. 5G SUCI Probing in the Wild, 07 2024.

[CMP13] Giuseppe Cattaneo, Giancarlo Maio, and Umberto Petrillo. Security Issues and Attacks on the GSM Standard: a Review. *JOURNAL OF UNIVERSAL COMPUTER SCIENCE*, 19:2437–2452, 01 2013. doi: 10.3217/jucs-019-16-2437.

[Cro12] Neil Croft. On Forensics: A Silent SMS Attack. In *2012 Information Security for South Africa*, pages 1–4, 2012. doi: 10.1109/ISSA.2012.6320454.

[CRPH21] Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz. 5G SUCI-Catchers: Still Catching Them All? In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '21, pages 359–364. Association for Computing Machinery, 2021. doi: 10.1145/3448300.3467826.

[CS98] James J. Caffery and Gordon L. Stuber. Overview of radiolocation in CDMA cellular systems. *IEEE Communications Magazine*, 36(4):38–45, 1998. doi: 10.1109/35.667411.

[DPK+14] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. IMSI-Catch Me If You Can: IMSI-Catcher-Catchers. In

Proceedings of the 30th Annual Computer Security Applications Conference, ACSAC '14, pages 246–255. Association for Computing Machinery, 2014. doi: 10.1145/2664243.2664272.

[DPW16] Adrian Dabrowski, Georg Petzl, and Edgar Weippl. The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection. In *Research in Attacks, Intrusions, and Defenses*, volume 9854, pages 279–302, September 2016. doi: 10.1007/978-3-319-45719-2_13.

[DR06] Fan Deng and Davood Rafiei. Approximately detecting duplicates for streaming data using stable bloom filters. In *Proceedings of the 2006 ACM SIGMOD International Conference on Management of Data*, SIGMOD '06, page 25–36, New York, NY, USA, 2006. Association for Computing Machinery. doi: 10.1145/1142473.1142477.

[FBB+23] Daniel Fraunholz, Dominik Brunke, Simon Beidenhauser, Sebastian Berger, Hartmut Koenig, and Daniel Reti. IMSI Probing: Possibilities And Limitations. In *Secure IT Systems: 27th Nordic Conference, NordSec 2022, Reykjavic, Iceland, November 30–December 2, 2022, Proceedings*, pages 80–97. Springer-Verlag, 2023. doi: 10.1007/978-3-031-22295-5_5.

[FO22] Diyar Fadhil and Rodolfo Oliveira. Estimation of 5G Core and RAN End-to-End Delay through Gaussian Mixture Models. *Computers*, 11:184, December 2022. doi: 10.3390/computers11120184.

[FRJ15] Fabian van den Broek, Roel Verdult, and Joeri de Ruiter. Defeating IMSI Catchers. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Ccs '15, pages 340–351. Association for Computing Machinery, 2015. doi: 10.1145/2810103.2813615.

[GA13] Shahabeddin Geravand and Mahmood Ahmadi. Bloom filter applications in network security: A state-of-the-art survey. *Comput. Networks*, 57:4047–4064, 2013. doi: 10.1016/j.comnet.2013.09.003.

[GWC+10] Deke Guo, Jie Wu, Honghui Chen, Ye Yuan, and Xueshan Luo. The Dynamic Bloom Filters. *IEEE Transactions on Knowledge and Data Engineering*, 22(1):120–133, 2010. doi: 10.1109/TKDE.2009.57.

[HBK18] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier. In *Network and Distributed System Security Symposium*, 2018. doi: 10.14722/ndss.2018.23365.

[HEC+19] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. Privacy Attacks to the 4G and 5G Cellular Paging Protocols Using Side Channel Information. *Proceedings 2019 Network and Distributed System Security Symposium*, 2019. doi: 10.14722/ndss.2019.23442.

[HLRM24] Jan Erik Håkegård, Henrik Lundkvist, Ashish Rauniyar, and Peter Morris. Performance Evaluation of an Open Source Implementation of a 5G Standalone Platform. *IEEE access : practical innovations, open solutions*, 12:25809–25819, 2024. doi: 10.1109/ACCESS.2024.3367120.

[HM24] Catherine Hayes and David Malone. An Evaluation of FNV Non-Cryptographic Hash Functions. In *2024 35th Irish Signals and Systems Conference (ISSC)*, pages 1–8, 2024. doi: 10.1109/ISSC61953.2024.10603139.

[Hua08] Chin-Tser Huang. LOFT: Low-Overhead Freshness Transmission in Sensor Networks. In *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008)*, pages 241–248, 2008. doi: 10.1109/SUTC.2008.38.

[JPPD12] Devesh C. Jinwala, Dhiren R. Patel, Sankita Patel, and Kankar S. Dasgupta. Optimizing the Replay Protection at the Link Layer Security Framework in Wireless Sensor Networks, 2012. doi: 10.48550/arXiv.1203.4694.

[KC14] Nikolaos Karapanos and Srdjan Capkun. On the effective prevention of TLS man-in-the-middle attacks in web applications. In *Proceedings of the 23rd USENIX Conference on Security Symposium*, SEC'14, page 671–686, USA, 2014. USENIX Association. doi: 10.5555/2671225.2671268.

[KEL+22] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Capkun. LTrack: Stealthy Tracking of Mobile Phones in LTE. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1291–1306. USENIX Association, August 2022. doi: 10.48550/arXiv.2106.05007.

[KFRK23] Bedran Karakoc, Nils Fürste, David Rupprecht, and Katharina Kohls. Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '23, pages 97–108. Association for Computing Machinery, 2023. doi: 10.1145/3558482.3581774.

[KKHK12] Denis Foo Kune, John Kölndorfer, Nicholas Hopper, and Yongdae Kim. Location leaks over the GSM air interface. In *Network and Distributed System Security Symposium*, 2012.

[KM20] Haibat Khan and Keith Martin. A Survey of Subscription Privacy on the 5G Radio Interface - The Past, Present and Future. *Journal of Information Security and Applications*, 53:102537, August 2020. doi: 10.1016/j.jisa.2020.102537.

[LBSR23] Madhusanka Liyanage, An Braeken, Shahriar Shahabuddin, and Pasika Ranaweera. Open RAN Security: Challenges and Opportunities. *Journal of Network and Computer Applications*, 214:103621, 2023. doi: 10.1016/j.jnca.2023.103621.

[LRN23] Norbert Ludant, Pieter Robyns, and Guevara Noubir. From 5G Sniffing to Harvesting Leakages of Privacy-Preserving Messengers. In *2023 IEEE Symposium on Security and Privacy (SP)*, pages 3146–3161, 2023. doi: 10.1109/SP46215.2023.10179353.

[LZL+24] Yiming Liu, Cen Zhang, Feng Li, Yeting Li, Jianhua Zhou, Jian Wang, Lanlan Zhan, Yang Liu, and Wei Huo. Semantic-Enhanced Static Vulnerability Detection in Baseband Firmware. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, ICSE '24, New York, NY, USA, 2024. Association for Computing Machinery. doi: 10.1145/3597503.3639158.

[MKB25] Kazi Samin Mubasshir, Imtiaz Karim, and Elisa Bertino. Gotta Detect 'Em All: Fake Base Station and Multi-Step Attack Detection in Cellular Networks, 2025. doi: 10.48550/arXiv.2401.04958.

[MLKM23] Lusani Mamushiane, Albert Lysko, Hlabishi Kobo, and Joyce Mwangama. Deploying a Stable 5G SA Testbed Using srsRAN and Open5GS: UE Integration and Troubleshooting towards Network Slicing. In *2023 International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)*, pages 1–10, 2023. doi: 10.1109/icABCD59051.2023.10220512.

[MML+24] Tariro Mukute, Lusani Mamushiane, Albert A. Lysko, Elena-Ramona Modroiu, Thomas Magedanz, and Joyce Mwangama. Control Plane Performance Benchmarking and Feature Analysis of Popular Open-Source 5G Core Networks: OpenAirInterface, Open5GS, and free5GC. *IEEE Access*, 12:113336–113360, 2024. doi: 10.1109/ACCESS.2024.3441725.

[MN22] Sabah M. Morsy and Dalia Nashat. D-ARP: An Efficient Scheme to Detect and Prevent ARP Spoofing. *IEEE Access*, 10:49142–49153, 2022. doi: 10.1109/ACCESS.2022.3172329.

[MO17] Stig F. Mjølsnes and Ruxandra F. Olimid. Easy 4G/LTE IMSI Catchers for Non-Programmers. *arXiv e-prints*, page arXiv:1702.04434, February 2017. doi: 10.48550/arXiv.1702.04434.

[MO19] Stig Mjølsnes and Ruxandra Olimid. Private Identification of Subscribers in Mobile Networks: Status and Challenges. *IEEE Communications Magazine*, 57:138–144, 09 2019. doi: 10.1109/MCOM.2019.1800511.

[MVG+24] Arman Maghsoudnia, Eduard Vlad, Aoyu Gong, Dan Mihai Dumitriu, and Haitham Hassanieh. Ultra-Reliable Low-Latency in 5G: A Close Reality or a Distant Goal? In *Proceedings of the 23rd ACM Workshop on Hot Topics in Networks*, HotNets '24, page 111–120, New York, NY, USA, 2024. Association for Computing Machinery. doi: 10.1145/3696348.3696862.

[Naa16] Markus Naarttijärvi. Swedish police implementation of IMSI-catchers in a European law perspective. *Computer Law & Security Review*, 32(6):852–867, 2016. doi: 10.1016/j.clsr.2016.07.006.

[NZW+22] Shiyue Nie, Yiming Zhang, Tao Wan, Haixin Duan, and Song Li. Measuring the Deployment of 5G Security Enhancement. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '22, page 169–174, New York, NY, USA, 2022. Association for Computing Machinery. doi: 10.1145/3507657.3528559.

[PBO+22] CheolJun Park, Sangwook Bae, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, and Yongdae Kim. DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 1325–1342. USENIX Association, August 2022. isbn: 978-1-939133-31-1.

[PGBBM21] Ivan Palamà, Francesco Gringoli, Giuseppe Bianchi, and Nicola Blefari-Melazzi. IMSI Catchers in the Wild: A Real World 4G/5G Assessment. *Computer Networks*, 194:108137, 2021. doi: 10.1016/j.comnet.2021.108137.

[PJM19] Roger Piqueras Jover and Vuk Marojevic. Security and Protocol Exploit Analysis of the 5G Specifications. *IEEE access : practical innovations, open solutions*, 7:24956–24963, 2019. doi: 10.1109/ACCESS.2019.2899254.

[PMN21] John Preuß Mattsson and Prajwol Kumar Nakarmi. Nori: Concealing the Concealed Identifier in 5G. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, ARES '21. Association for Computing Machinery, 2021. doi: 10.1145/3465481.3470076.

[PT25] Julian Parkin and Mahesh Tripunitara. Countering Subscription Concealed Identifier (SUCI)-Catchers in Cellular Communications. In *Information Systems Security*, pages 107–126. Springer Nature Switzerland, 2025. doi: 10.1007/978-3-031-80020-7_6.

[PWK+24] Sourav Purification, Simeon Wuthier, Jinoh Kim, Jonghyun Kim, and Sang-Yoon Chang. Fake Base Station Detection and Blacklisting. In *2024 33rd International Conference on Computer Communications and Networks (ICCCN)*, pages 1–9, 2024. doi: 10.1109/ICCCN61486.2024.10637542.

[RKHP19] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. Breaking LTE on Layer Two. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 1121–1136, 2019. doi: 10.1109/SP.2019.00006.

[SHC+20] Ankush Singla, Syed Hussain, Omar Chowdhury, Elisa Bertino, and Ninghui Li. Protecting the 4G and 5G Cellular Paging Protocols against Security and Privacy Attacks. *Proceedings on Privacy Enhancing Technologies*, 2020:126–142, January 2020. doi: 10.2478/popets-2020-0008.

[SRCP20] Sabrina Sicari, Alessandra Rizzardi, and Alberto Coen-Porisini. 5G In the Internet of Things Era: An Overview on Security and Privacy Challenges. *Computer Networks*, 179:107345, 2020. doi: 10.1016/j.comnet.2020.107345.

[SSB+16] Altaf Shaik, Jean-Pierre Seifert, Ravishankar Borgaonkar, N. Asokan, and Valtteri Niemi. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In *23rd Annual Network and Distributed System Security Symposium NDSS*. The Internet Society, 2016. doi: 10.48550/arXiv.1510.07563.

[TB08] Mohsen Toorani and Seyed Ali Asghar Beheshti. Solutions to the GSM Security Weaknesses. In *2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies*, pages 576–581, 2008. doi: 10.1109/NGMAST.2008.88.

[TBK+25] Tyler Tucker, Nathaniel Bennett, Martin Kotuliak, Simon Erni, Srdjan Capkun, Kevin R. B. Butler, and Patrick Traynor. Detecting IMSI-Catchers by Characterizing Identity Exposing Messages in Cellular Traffic. *Proceedings 2025 Network and Distributed System Security Symposium*, 2025. doi: 10.14722/ndss.2025.241115.

[TRL12] Sasu Tarkoma, Christian Esteve Rothenberg, and Eemil Lagerspetz. Theory and Practice of Bloom Filters for Distributed Systems. *IEEE Communications Surveys& Tutorials*, 14(1):131–155, 2012. doi: 10.1109/SURV.2011.031611.00024.

[UPMS22] Vincent Quentin Ulitzsch, Shinjo Park, Soundes Marzougui, and Jean-Pierre Seifert. A Post-Quantum Secure Subscription Concealed Identifier for 6G. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, WiSec '22, pages 157–168. Association for Computing Machinery, 2022. doi: 10.1145/3507657.3528540.

[Vac19] Khyati Vachhani. Security Threats against LTE Networks: A Survey. In Sabu M. Thampi, Sanjay Madria, Guojun Wang, Danda B. Rawat, and Jose M. Alcaraz Calero, editors, *Security in Computing and Communications*, pages 242–256. Springer Singapore, 2019. doi: 10.1007/978-981-13-5826-5_18.

[YBS+19] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. Hiding in Plain Signal: Physical Signal Overshadowing Attack on LTE. In *28th USENIX Security Symposium USENIX Security 19)*, pages 55–72. USENIX Association, August 2019. isbn: 978-1-939133-06-9.

Online References

[3GP] 3GPP. Releases. https://www.3gpp.org/specifications-technologies/releases, Accessed: 02.05.2025.

[3GP23] 3GPP. 5G Network slice management, July 2023. https://www.3gpp.org/technologies/slice-management, Accessed: 02.05.2025.

[ALL24a] O-RAN ALLIANCE. O-RAN Alliance, 2024. https://www.o-ran.org/, Accessed: 02.05.2025.

[All24b] OpenAirInterface Software Alliance. OpenAirInterface, 2024. https://openairinterface.org/, Accessed: 02.05.2025.

[App] Austin Appleby. MurmurHash2. https://github.com/abrandoned/murmur2/blob/master/MurmurHash2.c, Accessed: 02.05.2025.

[App24] Apple. Apple device support for private 5G and LTE networks, September 2024. https://support.apple.com/en-ie/guide/deployment/depac6747317/web, Accessed: 02.05.2025.

[Bro17] Gabriel Brown. Service-Based Architecture for 5G Core Networks, 11 2017. https://www.3g4g.co.uk/5G/5Gtech_6004_2017_11_Service-Based-Architecture-for-5G-Core-Networks_HR_Huawei.pdf, Accessed: 02.05.2025.

[BS17] Matthew Braga and Dave Seglins. Cellphone surveillance technology being used by local police across Canada. *CBC/Radio-Canada*, April 2017. https://www.cbc.ca/news/science/cellphone-surveillance-police-canada-imsi-catcher-privacy-1.4066527, Accessed: 02.05.2025.

[Cab19] CableLabs. A Comparative Introduction to 4G and 5G Authentication, 2019. https://www.cablelabs.com/insights/a-comparative-introduction-to-4g-and-5g-authentication, Accessed: 02.05.2025.

[Cor] National Instruments Corp. Ettus Research USRP B205mini-i. https://www.ettus.com/all-products/usrp-b205mini-i/, Accessed: 02.05.2025.

[Eri19] Ericsson. 3GPP Release 15: An end to the battle against false base stations?, January 2019. https://www.ericsson.com/en/blog/2019/1/3gpp-release15, Accessed: 02.05.2025.

[Fre25] Free5GC. free5gc, 2025. https://github.com/free5gc/free5gc, Accessed: 02.05.2025.

[Gü25] Ali Güngör. UERANSIM, February 2025. https://github.com/aligungr/UERANSIM, Accessed: 02.05.2025.

[Int21] Privacy International. How IMSI catchers can be used at a protest, May 2021. https://privacyinternational.org/explainer/4492/how-imsi-catchers-can-be-used-protest, Accessed: 02.05.2025.

[Ish23] Shigeru Ishida. A Note for 5G SUCI Profile A/B Scheme, 2023. https://github.com/s5uishida/note_5g_suci_profile_ab, Accessed: 02.05.2025.

[Lip] Paul Lipscombe. Why telcos are switching off legacy networks, and what it means for 5G. https://www.datacenterdynamics.com/en/analysis/why-telcos-are-switching-off-legacy-networks-and-what-it-means-for-5g/, Accessed: 02.05.2025.

[mit] mitshell. CryptoMobile. https://github.com/mitshell/CryptoMobile, Accessed: 02.05.2025.

[MWM+23] Sylvain Munaut, Harald Welte, Philipp Maier, Supreeth Herle, and Merlin Chlosta. Guide: Enabling 5G SUCI, 2023. https://downloads.osmocom.org/docs/pysim/master/html/suci-tutorial.html, Accessed: 02.05.2025.

[Noh] Karsten Nohl. Attacking Phone Privacy.

[Nua] Nuand. bladeRF 2.0 micro xA4. https://www.nuand.com/product/bladerf-xa4/, Accessed: 02.05.2025.

[Ope] Open5GS. open5gs. https://open5gs.org/, Accessed: 02.05.2025.

[Ope25] Open5GS. open5gs, 2025. https://github.com/open5gs/open5gs, Accessed: 02.05.2025.

[Osm] Osmocom. pySim. https://github.com/osmocom/pysim, Accessed: 02.05.2025.

[PE16] David Pegg and Rob Evans. Controversial snooping technology ‘used by at least seven police forces’. *The Guardian*, Oktober 2016. https://www.theguardian.com/world/2016/oct/10/controversial-phone-snooping-technology-imsi-catcher-seven-police-forces, Accessed: 02.05.2025.

[Pro] Andreas Proschofksy. 2G-Mobilfunk: Notorisch unsicher, extrem veraltet und doch kein Ende in Sicht. https://www.derstandard.at/story/2000132732535/2g-mobilfunk-notorisch-unsicher-extrem-veraltet-und-doch-kein-ende, Accessed: 02.05.2025.

[Pro25] Android Open Source Project. Network time detection, February 2025. https://source.android.com/docs/core/connect/time/network-time-detection, Accessed: 02.05.2025.

[Sec22] P1 Security. pysctp, November 2022. https://github.com/P1sec/pysctp, Accessed: 02.05.2025.

[Sec23] P1 Security. pycrate, November 2023. https://github.com/P1sec/pycrate, Accessed: 02.05.2025.

[sfmcG] systems for mobile communications GmbH. sysmoISIM-SJA5 programmable SIM/USIM/ISIM/HPSIM cards. https://sysmocom.de/products/sim/sysmoisim-sja5/index.html, Accessed: 02.05.2025.

[Sok18] Daniel AJ Sokolov. US-Heimatschutz lässt illegale IMSI-Catcher unbehelligt, 2018. https://www.heise.de/news/US-Heimatschutz-laesst-illegale-IMSI-Catcher-unbehelligt-4011143.html, Accessed: 02.05.2025.

[(SR24] Software Radio Systems (SRS). srsRAN Project – Open Source RAN, 2024. https://www.srslte.com/, Accessed: 02.05.2025.

[Sys25] Software Radio Systems. srsRAN gNB with COTS UEs, 2025. https://docs.srsran.com/projects/project/en/latest/tutorials/source/cotsUE/source/index.html,Accessed: 02.05.2025.

[Tea] GSMA Future Networks Team. 2019 saw 5G become a commercial reality – 2020 will take it to the mass market. https://www.gsma.com/futurenetworks/digest/5g-in-2019/, Accessed: 02.05.2025.

[Vir22] Jyri J. Virkki. libbloom, September 2022. https://github.com/jvirkki/libbloom, Accessed: 02.05.2025.

[Wik05] Wikimedia Commons. Trilateration, 2005. https://commons.wikimedia.org/wiki/File:Trilateration.png, Accessed: 02.05.2025.