Demystifying Privacy in 5G Stand Alone Networks

Stavros Eleftherakis*
stavros.eleftherakis@imdea.org
Imdea Networks Institute
Universidad Carlos III de Madrid
Madrid, Spain

Timothy Otim
timothy.otim@imdea.org
Imdea Networks Institute
Madrid, Spain

Giuseppe Santaromita
giuseppe.santaromita@imdea.org
Imdea Networks Institute
Madrid, Spain

Almudena Diaz Zayas
adz@uma.es
Universidad de Málaga
Málaga, Spain

Domenico Giustiniano
domenico.giustiniano@imdea.org
Imdea Networks Institute
Madrid, Spain

Nicolas Kourtellis
nicolas.kourtellis@telefonica.com
Telefonica Research
Barcelona, Spain

ABSTRACT

Ensuring user privacy remains critical in mobile networks, particularly with the rise of connected devices and denser 5G infrastructure. Privacy concerns have persisted across 2G, 3G, and 4G/LTE networks. Recognizing these concerns, the 3rd Generation Partnership Project (3GPP) has made privacy enhancements in 5G Release 15. However, the extent of operator adoption remains unclear, especially as most networks operate in 5G Non Stand Alone (NSA) mode, relying on 4G Core Networks. This study provides the first qualitative and experimental comparison between 5G NSA and Stand Alone (SA) in real operator networks, focusing on privacy enhancements addressing top eight pre-5G attacks based on recent academic literature. Additionally, it evaluates the privacy levels of OpenAirInterface (OAI), a leading open-source software for 5G, against real network deployments for the same attacks. The analysis reveals two new 5G privacy vulnerabilities, underscoring the need for further research and stricter standards.

KEYWORDS

5G, Wireless Networks, OpenAirInterface, Network Identifiers, Security, Privacy

ACM Reference Format:
Stavros Eleftherakis, Timothy Otim, Giuseppe Santaromita, Almudena Diaz Zayas, Domenico Giustiniano, and Nicolas Kourtellis. 2024. Demystifying Privacy in 5G Stand Alone Networks. In *The 30th Annual International Conference on Mobile Computing and Networking (ACM MobiCom '24), November 18–22, 2024, Washington D.C., DC, USA.* ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3636534.3690696

*This work was carried out during S. Eleftherakis' internship at Telefonica Research, Barcelona.

ACM MobiCom '24, November 18–22, 2024, Washington D.C., DC, USA

1 INTRODUCTION

Telecommunication companies worldwide are rapidly rolling out 5G technology, with projections already suggesting billions of active 5G connections based on 3GPP Release 15 [19]. This faster, denser, and larger-bandwidth cellular technology is being used by the ever increasing number of IoT, smartphone, and other connected devices, estimated to be 15 billion by the end of 2023, and projected to reach 30 billions by 2030 [18]. However, the pressure to fast deploy 5G networks comes at a cost. Although operators started to deploy and use 5G networks, a lot of these are 5G Non Stand Alone (NSA), i.e., they rely on 4G Core Networks to operate. For example, in Europe in 2022, the 5G Stand Alone (SA) deployment had reached only a 38% with respect to the total number of 5G Networks, although this is increasing [81]. In fact, 2024 is expected to be the year that 5G SA deployment will accelerate [85].

Continued reliance on 5G NSA technology poses a significant security and privacy (S&P) challenge, stemming from unresolved adversarial issues carried over from pre-5G networks. Despite efforts to address these S&P issues with the introduction of 5G, transitional 5G NSA networks still exhibit vulnerabilities. Prior research on pre-5G networks has revealed numerous S&P concerns regarding user confidentiality, authentication, integrity, location privacy, anonymity, and user unlinkability [23, 27, 53, 64, 89, 90]. Indeed, while 3GPP incorporated some of these findings to enhance 5G S&P features in Release 15 (Rel. 15), the promise of improved S&P mainly applies to 5G SA, not NSA networks. In fact, NSA's reliance on 4G core infrastructure increases the potential attack surface.

Given the proliferation of connected devices and shift from 5G NSA to SA, several key questions motivate this

study: 1) What are the core differences in S&P aspects between 5G NSA and SA networks? 2) How have industry standards and academic literature addressed pre-5G vulnerabilities in 5G real deployments, and what methods have been employed for enhancement? 3) Do current open-source tools, readily available to the research community such as OpenAirInterface (OAI) [15], adequately support and enable proper measurement capabilities for evaluating these 5G SA enhancements? 4) Are there any novel S&P flaws in 5G SA that remain unidentified and unresolved? With this work, we dive into the S&P aspects of 5G SA and NSA networks in Rel. 15 and, to the best of our knowledge, make the following contributions:

- We are the first to perform a head-on qualitative and experimental comparison between 5G NSA and SA in real operator networks, and study enhancements introduced in 5G to address 8 top pre-5G attacks as described in recent literature [25, 38, 54, 55, 86, 96].
- We are the first to perform a study on the security aspects of real 5G SA networks in Europe and the second in the world.
- We are the first to show the implementation of SUCI in a real 5G network.
- We are the first to examine the S&P levels offered by OpenAirInterface (OAI), the de facto open source software for 5G, and experimentally compare them with 5G NSA and SA real deployments for the same attacks.
- We highlight two new 5G S&P vulnerabilities that merit further research and stricter 5G standards.
- We discuss 9 key takeaways from our overall analysis.

2 BACKGROUND

2.1 5G Cellular Network Architecture

We provide an overview of the main infrastructure of a 5G Cellular Network: User Equipment (UE), New Generation Radio Access Network (NG-RAN), and Core Network (CN).

User Equipment (UE): The UE consists of the Mobile Equipment (ME) and the Universal Subscriber Identity Module (USIM) card. It is used by consumers to access mobile services and applications. The USIM card pays a pivotal role in authentication, key generation and subscriber information management.

New Generation Radio Access Network (NG-RAN): The New Generation Radio Access Network (NG-RAN) encompasses a network of Base Stations (BSs), known as gNBs in 5G, that are organized into distinct Tracking Areas (TAs). The RRC (Radio Resource Control) protocol [12] plays a critical role in establishing, maintaining, and terminating radio connections between UEs and the NG-RAN.

Core Network (CN): The CN comprises diverse entities known as Network Functions (NFs), each tasked with delivering different network services and functionalities such as mobility management, authentication, subscriber data management, session establishment and control, etc. The Non-Access Stratum (NAS) protocol serves as the pathway facilitating signaling procedures and the exchange of messages between the UE and the CN and a comprehensive analysis of NAS protocol can be found in [6].

2.2 UE Identifiers

There are various identifiers used in the Cellular Network, responsible for the identification of different entities participating in the system, and especially of the UE at hand. In general, they are divided into permanent and temporary identifiers. Permanent identifiers are global and are considered as extremely sensitive in terms of privacy. Temporary identifiers are used in order to minimize the transmission of permanent ones, thus enhancing UE privacy, but certain rules should be followed for them as well.

To begin with, 5G introduced Subscription Unique Permanent Identifier (SUPI) in the clause 5.9.2 of the 3GPP 5G technical specifications for security architecture and procedures [5]. SUPI is the permanent identity of the USIM card and must never be submitted plaintext, except for emergency cases, as denoted in the clause 5.2.5 of [9]. SUPI should not be used for the authentication of the UE.

Another important permanent identifier is the Permanent Equipment Identity (PEI), manufactured on the ME device during its production as analyzed in Sec. 6.4 of [4]. PEI should only be transmitted in a secure channel, after integrity and ciphering have been enabled, and cannot be used for the authentication of the UE by the network. Intuitively, SUPI and PEI are equivalent to the International Mobile Subscriber Identity (IMSI) and International Mobile Equipment Identity (IMEI), respectively in previous generations.

The second important category of identifiers are temporary. First, 5G introduces the Subscription Unique Concealed Identifier (SUCI) in the clause 5.9.2a of [5]. SUCI is an elliptic, cryptography-based concealed version of SUPI that is constructed by the USIM card and is used for the authentication of the UE by the network. The concept of SUCI is new in 5G and nothing equivalent exist in previous generations.

Furthermore, the CN assigns a temporary identifier to the UE for the communication between the UE and the CN, called 5G-GUTI (5G Globally Unique Temporary Identifier) as defined in the clause 5.9.4 of [5]. In 2G and 3G, 5G-GUTI was called Temporary Mobile Subscriber Identity (TMSI), whereas in 4G it was called GUTI or TMSI. For the rest of this paper, we denote this temporary identifier as TMSI for previous to 5G cellular generations. Finally, the UE is also assigned a temporary identifier called Cell Radio Network

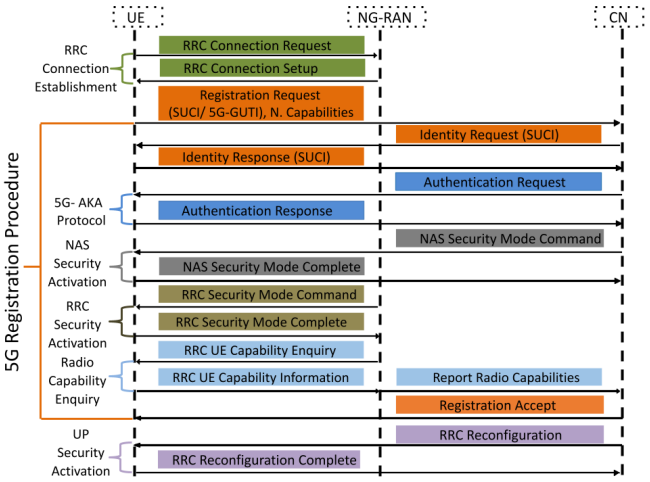


Figure 1: High Level Representation of 5G messages exchange flow.

Temporary Identity (C-RNTI) from the RAN, facilitating the communication between the UE and the RAN.

2.3 UE Capabilities

The capabilities of an UE can be separated into network capabilities [6] and radio access capabilities [11]. The network capabilities indicate general UE characteristics, such as the security algorithms supported by the UE for integrity and ciphering protection, and are transmitted as a NAS message.

As for the security algorithms, 5G UEs shall support New Radio Encryption Algorithm (NEA) 0, 128-NEA1 and 128-NEA2 for ciphering (confidentiality) protection and New Radio Integrity Algorithm (NIA) 0, 128-NIA1 and 128-NIA2 for integrity protection (Secs. 5.2.2 and 5.2.3 of [9]).

The radio access capabilities contain information regarding the radio capabilities of the UE, such as the supported frequency bands of the UE, and are transmitted as an RRC message. As explained next, the UE reports its capabilities to the network during the registration procedure. Further information about the UE capabilities can be found in [89, 90].

2.4 5G Message Exchange Flow

This section describes some basic message exchange flow regarding some critical procedures in 5G, as introduced in the 3GPP 5G specifications [9] and illustrated in Figure 1. First, the UE establishes an RRC Connection with the NG-RAN, and afterwards transmits a registration request message including a subscriber identity (SUCI or 5G-GUTI) and its network capabilities. If the 5G-GUTI was transmitted by the UE and the CN cannot resolve it, it sends to the UE an Identity Request message. The UE transmits the SUCI in a Identity Response message, and then the Authentication and Key Agreement Protocol (AKA) is initiated by the CN. We highlight that both EPS-AKA (Evolved Packet System Authentication and Key Agreement) and 5G-AKA (5G Authentication and Key Agreement) can be used, but since the differences are out of scope for this paper, 5G-AKA (Sec. 6.1.3.2 of [9]) is referred. Further information about the 5G-AKA protocol can be found in [24, 62, 93].

After a successful authentication response sent by the UE, NAS Security Mode Command (SMC) is transmitted in order to initiate the activation of a secure channel for the NAS protocol messages, providing integrity and ciphering protection. As analyzed in the Sec. 6.7.2 of [9] an enhanced NAS SMC procedure is followed, where the CN replays the Network capabilities received in the first Registration message to ensure that they were not modified. Furthermore, a Message Authentication Code (MAC) is included to ensure the integrity of the NAS SMC message. The UE verifies the correctness of the Network capabilities and the integrity of the NAS SMC message and if everything is fine, a secure NAS channel is established.

The same procedure is followed for the RRC messages, exchanged between the UE and the NG-RAN, for the activation of a secure channel for them as well. Then, the UE radio capabilities are transmitted to the 5G network, *after the establishment of a secure RRC channel* (see Figure 1). This is in contrast to prior cellular generations, where radio capabilities were sent before the establishment of a secure channel between the UE and the RAN. Finally, integrity and ciphering for the User Plane (UP) messages are activated through the RRC Reconfiguration message.

2.5 Paging Procedure

The paging mechanism notifies the receiving UE for incoming data transmissions or phone calls. These paging messages are primarily transmitted by the base station (RRC paging), broadcasting the UE's identity and indicating the recipient of incoming data or a call via the paging channel. After data or an SMS are sent to a UE, the paging procedure is activated at the incoming or receiving UE, prompting all UEs within the cell to monitor the paging channel and respond if their identity matches. Similarly for phone calls, this process occurs at a TA level. As discussed later, the paging mechanism posed significant privacy concerns across various cellular generations, as it relied on IMSI, potentially enabling adversaries to compromise the UE's permanent identity.

3 METHODOLOGY

In this section, we describe the methodology of our work. First, in Sec. 3.1, we define User Identity Confidentiality and its properties. Then, Sec. 3.2 provides an end-to-end overview of the Framework we use, thereby navigating the reader for the rest of this paper. Finally, Sec. 3.3 describes the different 5G SA and NSA deployment scenarios, and the common experimental process used in various experiments executed.

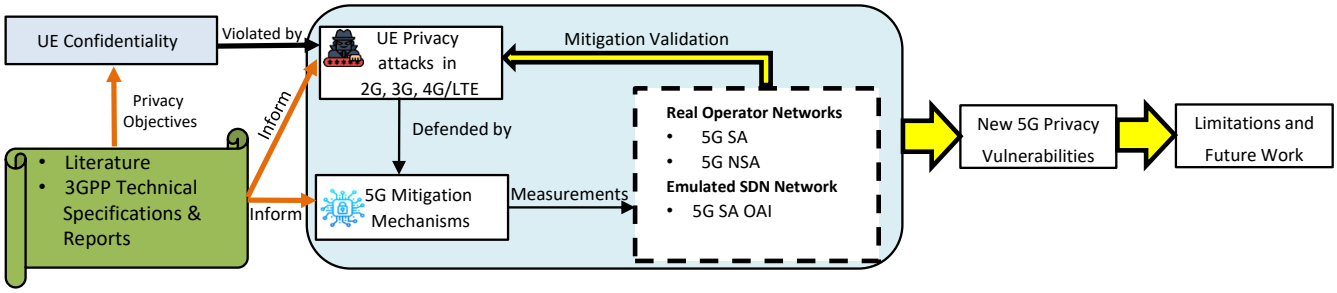


Figure 2: Framework followed to study pre-5G attacks in real 5G NSA & SA deployments, and an OAI testbed.

3.1 User Identity Confidentiality

It is crucial to establish certain S&P objectives about the confidentiality of the user identity in mobile networks. Thus, Sec. 5.1.1 of [7] describes some important security characteristics that should be met by cellular networks. In fact, as previous works [28, 38, 54, 55] considered them, the following properties are necessary for the protection of the user identity confidentiality:

(1) UE Identity Privacy: "the permanent user identity (IMSI) of a user to whom a services is delivered cannot be eavesdropped on the radio access link".
(2) UE Location Privacy: "the presence or the arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link".
(3) UE Untraceability: "an intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link".

3.2 Framework

The framework followed in this paper is outlined in Figure 2: First, we search in related surveys [38, 55, 59, 86] for pre-5G related attacks that violated UE Confidentiality. Then, in Sec. 4, we identify the corresponding 5G Security mechanisms that have been planted in 5G to mitigate these attacks, again by looking into related literature (e.g., [65, 75]) and 5G 3GPP Technical Specifications (e.g., [9]). Afterwards, we perform measurements in five different deployment scenarios (outlined in Sec. 3.3 below). In Sec. 4, we make a qualitative analysis of these measurements examining if the mitigation mechanisms embedded in 5G are implemented correctly, thus mitigating the above-mentioned attacks, inherited from past generations of cellular networks. Building on this knowledge, Sec. 5 outlines two new privacy vulnerabilities that we identified through the measurements in the real operator networks. Finally, Sec. 7 discusses lessons learned and directions for future research work, regulation and standardization. We remark that the proposed framework is the first that compares 5G SA and 5G NSA resilience against well-known pre-5G attacks in the same operator's networks. It is also the first framework that identified novel 5G privacy attacks in 5G SA real operator networks and the first that analyzed OAI privacy compliance.

We mention that our framework can be used for analyzing the existence of the specific pre-5G (Sec. 4) or new 5G attacks (Sec. 5) in different operators' networks as well. Indeed, the specifics of which messages and actions need to be checked for each attack are further analyzed experimentally in the main body of Secs. 4 and 5, and can be repeated by other researchers/operators. Finally, the following Sec. 3.3.3 (Data Collection Approach) attempts to homogenize the experimental process in order to facilitate in higher degree the reproduction of our framework.

3.3 Experimental & Deployment Scenarios

Next, we describe the different 5G testbeds that were used for our experiments. Further, we explain the data collection approach during experiments.

3.3.1 Operator's networks testbed: Real private 5G SA and NSA networks from a large operator in a city of Spain. We test three 5G SA networks and one 5G NSA. All networks are based on 5G Rel. 15, operate in a single TA and only data transmission is supported. We use an Asus exp21 5G smartphone equipped with a 5G USIM card to connect to these networks. The smartphone is equipped with the Nemo Handy diagnostic tool [17], that allows measuring information on wireless diagnostics of air interface and mobile application quality-of-service and quality-of-experience.

3.3.2 5G SA in OpenAirInterface (OAI):. A SDN testbed based on OAI in a lab setting. We connect a Google Pixel 7 with a 5G USIM card. Our analysis is based on CN and gNB log files and wireshark captures. OAI has been chosen for this work because it has become the de facto open-source software solution for 5G applications. To build the SA network, the gNB consisted of an Ettus N310 SDR and a high-performance Intel Core i7-8700k 3.7 GHz CPU work station. To establish the 5G CN, an Intel Core i7-8700k 3.7 GHz CPU workstation with Linux operating systems serving as the host as used. This workstation emulated all the required functionalities of a 5G NR CN. When the smartphone connected to the OAI

5G network, the CN and gNB log files were saved for post processing analysis.

3.3.3 Data Collection Approach. To facilitate and homogenize the data collection procedure, the following experimental process has been followed across experiments:

- Step 1: Airplane mode ON: The terminal will always start with airplane mode activated.
- Step 2: Start data collection: Once the airplane mode of the UE is deactivated, the data collection starts.
- Step 3: Time duration of the experiment: Based on the nature of the experiment, we wait from some seconds to some days.
- Step 4: Airplane mode ON: End of experiment and stop of data collection process.

4 PRE-5G ATTACKS & 5G ENHANCEMENT

We focus on 8 top adversarial attacks in pre-5G cellular networks, that have been documented extensively in academic literature [25, 38, 54, 55, 86, 96]. These attacks attempt to break either the whole set or a portion of the UE Confidentiality properties described in Sec. 3.1. Here, and for each attack, we first outline the attack and then refer to the corresponding 5G mitigation mechanisms as analyzed in [38, 55, 86, 96]. Then, we examine the existence and correct implementation of each specific 5G mitigation mechanisms across the different deployment scenarios described earlier in Sec. 3.3. In Table 1, we summarize our findings for all attacks.

4.1 Attacks on Permanent Identifiers

4.1.1 ***IMSI Catching:*** In this section, we refer to attacks that aim to steal the IMSI of the UE, known as IMSI catching attacks [42, 67, 74, 84]. Indeed, the attacker uses a device called IMSI Catcher consisting of a fake base station, thus being easily deployable and affordable [34, 78, 79]. A fake base station can be constructed by using a Universal Software Radio Peripheral (USRP) [14] with a modified code of open-source projects like OpenLTE [3], srsRAN [13, 44], gr-LTE [2, 35], or OAI [15, 76]. In fact, IMSI Catching [42, 67, 74] has been a persistent attack in 2G [72], 3G [20] and 4G [73]. The adversary has two different ways to steal the IMSI of the UE. First, and more usual, an IMSI catcher takes advantage of the victim's phone behavior to connect to the Cell that offers the strongest signal power. When the UE connects to the IMSI catcher device, the adversary sends an Identity Request message. Then, the UE answers with an Identity Response message, including the IMSI without encryption (plaintext), thus, leading to UE identity disclosure.

As an alternative, signal overshadowing techniques have been used as well [95]. This kind of attacks require time and frequency synchronization with the legitimate Base Station (BS), offering signal strength slightly stronger [95] or slightly weaker [69] than the legitimate one. In fact, IMSI catching based on signal overshadowing [39, 61] is stealthier compared to the traditional, fake-BS-based attack, since it uses a normal signal strength, thus making its detection even more difficult.

A lot of different solutions to IMSI catchers had been proposed in the literature for IMSI Catcher detection, but all of them suffer from practicality problems. A first set of solutions proposed either the usage of multiple IMSIs [57, 71] or the introduction of a new pseudonym instead of the IMSI [77, 92], but both of them suffer from synchronization problems between the USIM and the network as described in [48, 58]. Furthermore, other solutions [32, 36, 37, 43, 66, 97] proposed significant changes to the AKA protocol, thus making their implementation impractical. Finally, Dabrowski et all. [33, 34] proposed an IMSI Catcher detection framework based on possible network abnormalities (e.g., strange Cell frequencies, unusual Cell locations and Cell IDs, signal noise level, unusual network parameters) that could have been created by the existence of an IMSI Catcher. It is unclear if such a detection framework has been implemented by any operator. Based on this outlook, the plaintext IMSI transmission was characterized as a key vulnerability in the clause 6.1.3 of 3GPP Specifications [8].

5G Enhancement 1: SUPI Concealment
SUPI is the corresponding Identifier to IMSI in 5G networks. In order to avoid the plaintext transmission of SUPI, Subscriber Unique Concealed Identifier (SUCI) is introduced as an *encrypted* form of SUPI, based on elliptic cryptography. In fact, SUCI can be mainly used for authentication if the temporary identifier, 5G-GUTI, is not available. SUCI is an optional feature based on 3GPP TSs.

Experimental Validation: We performed multiple UE registrations in all the different deployment scenarios available and analyzed the Identity Request message content, as depicted in Fig. 3. First, we find that the 5G NSA operator's implementation does not support SUCI, transmitting the Identity Request with IMSI as illustrated in Fig. 3a, and thus being vulnerable to IMSI catchers attacks. Then, as illustrated in Fig. 3b and Fig. 3c, all operator's 5G SA implementations and OAI support SUCI, thereby eliminating the privacy risks imposed by IMSI Catchers. To the best of our knowledge, ours is the first study showing that an operators' network supports this important optional feature, since a previous study among Chinese 5G SA networks showed that SUCI was not supported [75].

Existing literature has emulated some attacks against SUCI. For instance, a SUCI probing or SUCI replay attack [31] tried to obtain the victim's SUCI and verify if a Person of Interest (PoI) is in a current location or not. 3GPP characterized

Attack Name	5G Security		Operator's Implementations Supported Features		Emulated SDN Testbed
	Mitigation Mechanisms	Optional or Mandatory	5G NSA	5G SA*	OAI 5G SA
IMSI Catching [39, 42, 49, 61, 72, 74, 79, 91]	SUCI	O	No	Yes	Yes
IMSI Paging [23, 27, 64, 89]	5G-TMSI based paging	M	Yes	Yes	Yes
IMEI Catching [34, 73, 78, 82]	IMEI in secure channel	M	Yes	Yes	Yes
TMSI Deanonymity [21, 22, 47, 64]	GUTI reallocation mechanism	M	No	Yes	No
C-RNTI Tracking [51, 52, 87, 88]	RRC Ciphering	O	No	No	No
UE Measurements reports [26, 78, 89]	RRC Ciphering	O	No	No	No
Security capabilities bidding down attack [53, 89, 90]	Enhanced NAS process	M	Weak	Weak	Yes
Radio Capabilities bidding down attack [53, 90]	Radio Capabilities in a Secured Channel	M	Yes	Yes	Yes

∗: tested over three different 5G SA networks. The best result achieved among them is reported.

Table 1: Summary of pre-5G attacks, 5G mitigation strategies, and employment in different testbeds and networks.

this attack (Key Issue #2.2 of [10]) as low risk and no normative measures are needed. The reason behind this is that obtaining the actual identity of the user cannot be revealed by the SUCI, thus, there is no threat of UE identification. Furthermore, SUPI guessing attacks have been discussed in the literature as well [54, 68]. The adversaries first guess a SUPI and generate SUCIs from this. Then, the produced SUCIs are sent to potential victims, trying to verify if the guessed SUPI belongs to the victim user. Such attacks have been analyzed as a Key Issue #3.2 in [10], concluding that no normative measures should be taken against them since the likelihood of their accuracy is small.

Takeaway 1: The SUCI mechanism significantly improves the identity privacy of UEs; it is crucial that real operator CNs support this privacy-enhancing feature.

4.1.2 ***Attacks based on IMSI Paging:*** Paging procedure is initiated when the network searches for an UE in order to deliver a service to the device, such as a phone call or an SMS. In general, the temporary identifier (TMSI) is used for paging, but in previous generations to 5G, there are cases where (e.g., TMSI cannot be resolved by the network) IMSI can be used as well. The fact that IMSI could be sent in cleartext in paging messages made the paging process vulnerable, as were shown in 2G [64], 3G [21, 23] and 4G [27, 89]. The attacker initiates the paging process by sending messages, or making phone calls to the victim and at the same time a sniffer [29, 40, 46, 63, 70] can observe the unencrypted downlink paging messages and identify the IMSI of the victim's UE.

5G Enhancement 2: Decoupling IMSI from paging The above-mentioned problem was taken into consideration in 5G and the decoupling of the IMSI/SUPI from the paging mechanism is proposed. Indeed, in 5G paging takes place with a shortened version of 5G-GUTI, called 5G-S-TMSI (5G S-Temporary Mobile Subscription Identifier) as mentioned in Sec. 2.10.1 of [4]. 5G-S-TMSI is derived from 5G-GUTI, so its strict update mechanism as analyzed in the Section 4.2 holds for 5G-S-TMSI as well.

Experimental Validation: To verify this functionality, we sent messages to the victim's phone, while it was connected to each network, through the Messenger application [16]. All of our networks used 5G-S-TMSI for the paging message transmission. After many different experiments, IMSI or SUPI were never used for paging.

Takeaway 2: Both 5G NSA and SA real networks, and the OAI open-source implementation properly follow the related 5G specification to decouple IMSI from paging [4].

4.1.3 ***IMEI Catching:*** IMEI (or Permanent Equipment Identity (PEI) in 5G) is another sensitive permanent identifier, corresponding to the Mobile Equipment (ME). In previous

```
LAYER 3 SIGNALING MESSAGE
Time: 13:23:50.443

IDENTITY REQUEST       3GPP TS 24.301 ver 15.4.0 Rel 15    (8.2.18)

M Protocol Discriminator (hex data: 7)
     (0x7) EPS mobility management messages
M Security header type (hex data: 0)
     Security header type value: Plain NAS message, not security protected
M Message Type (hex data: 55)
     Message number: 85
M Identity type (hex data: 1)
     Identity type: IMSI
M Spare Half Octet (hex data: 0)
```

(a) IMSI based Identity Request in 5G NSA operator's network.

```
LAYER 3 SIGNALING MESSAGE
Time: 10:25:13.598

IDENTITY REQUEST       3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.21)

M Extended protocol discriminator (hex data: 7e)
     EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
     Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 5b)
     Message number: 91
M Identity type (hex data: 1)
     Type of identity: SUCI
```

(b) SUCI based Identity Request in 5G SA operator's networks.

```
Non-Access-Stratum 5GS (NAS)PDU
  Plain NAS 5GS Message
      Extended protocol discriminator: 5G mobility management messages (126)
      0000 .... = Spare Half Octet: 0
      .... 0000 = Security header type: Plain NAS message, not security protected (0)
      Message type: Identity request (0x5b)
      0000 .... = Spare Half Octet: 0
    5GS identity type
        .... .001 = Type of identity: SUCI (1)
```

(c) SUCI based Identity Request in OAI based SA network.

Figure 3: Identity Request in 5G NSA, SA and OAI networks.

mobile generations, the cleartext transmission of this identifier was permitted as a response to an Identity Request Message. Thus, an active adversary using a fake base station, similar to IMSI catchers' adversaries, could send an Identity Request using the IMEI instead of the IMSI, and steal the IMEI of the ME [33, 34].

5G Enhancement 3: Secrecy of PEI
PEI is the corresponding identity to IMEI, that was used in previous generations. As denoted in the clause 5.2.5 of [9]: "the UE shall only send the PEI in the NAS protocol, after NAS security context is established, unless during emergency registration when no NAS security context can be established". Therefore, the PEI should not be used in authentication in a normal scenario.

Experimental Validation: As shown in Fig. 3, SUCI or IMSI are used for UE authentication. PEI is requested by the network in the Security Mode Command and transmitted by UE to the CN in the Security Mode Complete message.

Takeaway 3: All operator's networks and OAI open-source implementation properly follow the appropriate steps in terms of complying with the 3GPP protocols and procedures for PEI as described in [9].

4.2 TMSI Deanonymity attack

The main reason for using the temporary identifier (TMSI) is the minimization of permanent identifiers transmission, offering better anonymity to the UE. In theory, TMSI has to be periodically updated by the network to avoid UE be easily tracked and identified [22]. However, as was shown in [21, 22], in some cases the TMSI remained constant even for three days, in 2G [64] and 3G [47] during experiments that took place in different European countries. Similar results were obtained in LTE networks [47, 89] as well. An adversary, consisting of a passive sniffer and a phone that sends (silent) calls or messages to the victim's UE, leads to linkability of the victim's phone number with its TMSI, and consequently location tracking.

5G Enhancement 4: Strict 5G-GUTI update method
5G-GUTI is the corresponding identifier to TMSI in previous cellular network generations. As analyzed before, previous generations faced serious privacy problems due to the infrequent or miss-configured refreshment of this temporary identifier. Based on this outlook, 5G strictly defines when the 5G-GUTI should be updated or refreshed by the Core Network in the clause 6.12.3 of [9]:

- Upon receiving Registration Request message of type "initial registration" or "mobility registration update" from a UE.
- Upon receiving Service Request message sent by the UE in response to a Paging message.
- Upon receiving Registration Request message of type "periodic registration update" from a UE.
- Upon receiving an indication from the lower layers that the RRC connection has been resumed for a UE in 5GMM IDLE mode with suspend indication in response to a Paging message.
- Even more frequently, based on the implementation of the operator.

In addition, it is denoted in the same 3GPP document that 5G-GUTI should be generated in an *unpredictable* way.

Experimental Validation: Regarding the operator's deployment scenarios, important differences were observed between the different networks. First, in terms of initial registration, all three 5G SA networks as well as the 5G NSA network, assign a new, unpredictable value of 5G-GUTI. Afterwards, we observed significant differences between the four networks in terms of 5G-GUTI update policy during paging. The 5G NSA and one out of three 5G SA implementations never assigned a new 5G-GUTI value after paging. On the other hand, two 5G SA implementations always assigned a new and unpredictable 5G-GUTI value. As for the

implementation of each operator, the 5G NSA and one 5G SA networks kept the same 5G-GUTI even for 2 days, whereas the other two 5G SA networks assigned a new value after a time ranging between 90 minutes and 2 hours, even if neither paging nor a new registration had been made in this period. As for the emulated, OAI-based testbed, it fails to generate a new and unpredictable 5G-GUTI value. For instance, even after a new UE registration, either the previous 5G-GUTI value was used, or a new one almost equal to the previous one.

Takeaway 4: The 5G SA and NSA Networks can be 3GPP compliant if properly implementing the 5G-GUTI update mechanism. Only two out of the three tested 5G SA Networks were compliant, whereas the third 5G SA, the NSA and the OAI Networks were found to be weak in terms of implementation of the 5G-GUTI update policy; future work should improve this weakness.

4.3 Attacks based on lack of ciphering

4.3.1 ***C-RNTI Tracking:*** C-RNTI is local to the users' serving BS and is used for the communication between the UE and the RAN as mentioned in Sec. 2.2. C-RNTIs can be found in both Uplink (UL) and Downlink (DL) RRC messages. Interestingly, [52] passively analyzed the traffic in LTE and found that the C-RNTI is included without encryption in the header of every single packet, regardless of whether it is signaling or user traffic. Ultimately, C-RNTI based attacks take advantage of the lack of RRC ciphering, gaining information about the UE location [51, 52, 60, 87, 88]. Linkability between the C-RNTI and the victim's phone number or a social network account (e.g., Messenger [16]) can be easily done by the adversary with a few messages or calls. After that, decoding the DL messages including the C-RNTI can be done using passive sniffers that are available [29, 40, 63]. C-RNTI attacks lead to location tracking of the victim UE. Concluding, the lack of ciphering in RRC messages is the privacy weakness behind this attack.

4.3.2 ***UE Measurement reports:*** To make matters worse, a more fine-grained attack called UE Measurements reports attack [78] take advantage of the un-ciphered RRC messages, including measurements made by the UE, such as the signal strength of nearby cells, thereby localizing the UE with triangulation. Compared to the C-RNTI tracking that localizes in a BS level, this attack can estimate the exact coordinates of the UE. Concluding, the lack of ciphering in RRC messages is the privacy weakness that leads to this attack.

5G Enhancement 5: Ciphering of RRC messages
At the gnB level, current 5G Systems are expected to implement New Radio Encryption Algorithm (NEA) 0, 128-NEA1 and 128-NEA2 for confidentiality (ciphering) protection as analyzed in Sec. 5.2.2 of [9]. Ciphering of RRC messages is optional, so it is up to the operator if it is enabled or not.

Experimental Validation: Looking into the RRC Security Mode Command message, we can find the information related to the RRC ciphering. All setups we examined (i.e., OAI, 5G SA and NSA operator networks) use NEA 0 (Null ciphering) for the ciphering of RRC messages.

Takeaway 5: Null Ciphering is 3GPP compliant, but we highlight it is not a safe option: the network is vulnerable to C-RNTI tracking and UE measurement reports attacks.

4.4 Attacks based on lack of integrity

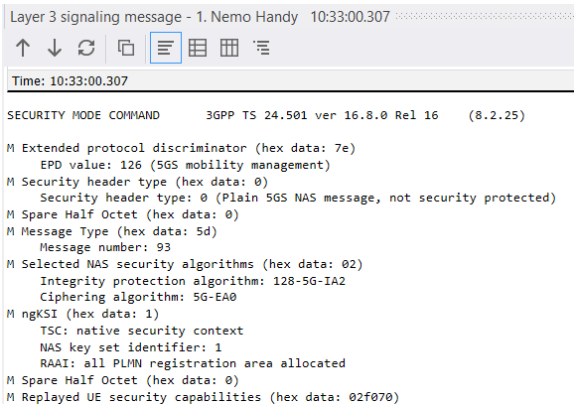
In this section, we discuss bidding-down attacks [53, 89, 90] that take advantage of the lack of integrity in messages including the Security and Radio capabilities. As the name suggests, a bidding-down attack forces the UE to use lower-quality network protocols and mechanisms, resulting, among others, in degradation of user privacy.

4.4.1 ***Radio Capabilities attack:*** In [89, 90], they analyze an attack based on the UE radio capabilities. The adversary, using a rogue base station, intercepts the UE radio capabilities message that is transmitted up to 4G, before the establishment of a secure channel, thus with no integrity protection activated. The adversary modifies appropriately their characteristics (e.g., modify the frequencies supported by the UE Modem), thus, managing to downgrade the UE to use a lower-level cellular network generation.

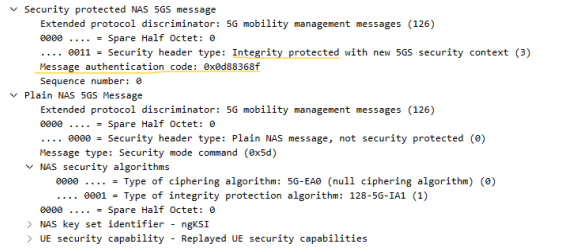
5G Enhancement 6: Transmission of Radio Capabilities over a Secured Channel
The UE radio capabilities were transmitted before the establishment of the RRC security channel, enabling bidding down attacks in 3G and 4G. This mistaken flow was corrected in 5G, as already mentioned in Sec. 2.4, and depicted in Fig. 1. This is because the RRC UE Capability Inquiry is transmitted after the RRC Security Mode Complete, when integrity protection is enabled. Based on this outlook, the bidding-down attacks based on UE Radio capabilities are eliminated.

Experimental Validation: All different real operator networks, and the OAI testbed asked for the Radio Capabilities after the establishment of an RRC secure channel.

Takeaway 6: The transmission of the Radio Capabilities after the establishment of an RRC secure channel indicates the elimination of the problem caused in previous generations [89, 90].



(a) Enhanced SMC in 5G SA networks. Similar in 5G NSA implementation.



(b) OAI enhanced SMC.

Figure 4: Enhanced SMC Procedure between operator's implementation and OAI.

4.4.2 ***Security Capabilities attack:*** To begin with, the adversaries described in [89, 90] exploit the security capabilities in the first registration message. The fact that the integrity protection of NAS messages is mandatory is not enough for the initial NAS message protection, since at this stage the UE and the network have not yet defined the algorithms that will be used for integrity and ciphering. An active adversary with a rogue base station can intercept the Registration Request message, modify the UE Security Capabilities (e.g., disable them) and release the modified message to the legitimate network. As a result the UE obtains weaker security compared to the one that their phone can support.

5G Enhancement 7: Enhanced SMC Privacy
A new, enhanced and integrity-protected initial NAS message transmission procedure has been introduced in the Sec. 6.7.2 of [9] to defend the bidding-down attacks, described in [53, 89, 90]. This procedure applies in the NAS Security Mode Command (SMC) message. In fact, the CN initiates the integrity protection and transmits among others a Message Authentication Code (MAC), the UE replayed the Security Capabilities that were received in the initial Registration Request message by the UE, and the security algorithms that will be used for integrity and ciphering. The UE uses the MAC to verify the integrity of the NAS SMC message and if the integrity verification is successful. Then, it verifies that the Security Capabilities replayed by the CN are the ones that had been originally transmitted in the Registration Request message. If everything is correct, the UE answers with a NAS Security Mode Complete and the establishment of a secure NAS channel is completed. After that, any attempt of the adversary to modify any NAS message is futile, since NAS integrity is mandatory, as mentioned earlier.

Experimental Validation: We verified the NAS Security mode command in all of our networks. We observed that all replay the initially transmitted security capabilities but only OAI follows the procedure described in the Sec. 6.7.2 of [9] correctly. As shown in Fig. 4a, all operator's networks omit the MAC code integrity protections and simply replay the UE network capabilities received in the registration message and mention the algorithms used for integrity and ciphering. On the other hand, Fig. 4b shows that OAI follows the enhanced SMC Privacy procedure accurately, transmitting the replayed UE Capabilities, and the chosen security algorithms along with the MAC code that ensures the integrity protection.

Takeaway 7: All of the implemented solutions defend the Security Capabilities bidding-down attack as mentioned in [89, 90], but all operator's implementations (NSA and SA) are vulnerable to another, novel attack, as will be explained next in Sec. 5.2.

5 NEW VULNERABILITIES OF 5G

In this section, we analyze two new vulnerabilities based on the measurement studies described earlier.

5.1 GUTI Reallocation Command Attack

As shown earlier, two out of three 5G SA networks always assign a new, unpredictable 5G-GUTI value to the UE. This new value is transmitted to the UE through a NAS Configuration Update Command message. Unfortunately, these two 5G SA networks transmit this command without security protection, neither in terms of integrity nor of ciphering, to the UE causing a significant privacy risk. Fig. 5 illustrates the Nemo Handy capture that demonstrates the aforementioned privacy vulnerability. We highlight that Arapinis et al. [22] had referred to this danger in previous generations, but later the same authors characterized this attack as a mere theoretical one [23], since the previous generations were not assigning new 5G-GUTI values. As we saw in our experiments, 5G SA assigns new 5G-GUTI values. Thus, we demonstrate this vulnerability in a real scenario for the first time.

A potential adversary can take advantage of two vulnerabilities leading to two different types of attacks. First, the lack

of integrity means that the content of the above mentioned message can be modified. Therefore, a Man-in-the-Middle (MiTM) attacker can intercept a Configuration Update Command message and modify the 5G-GUTI value to a different one. Then, when the UE tries to reestablish some content with the network, using this modified 5G-GUTI value, the network will not be able to recognize him/her, thus leading to a Denial of Service (DoS) attack. On the other hand, we stress that an attack called GUTI Refreshment Neutralization that was presented in 5G networks as a proof of concept in [50], exploits the Configuration Update Command as well. In that work, the authors took advantage of the lack of Acknowledgment (ACK) request in the Configuration Update Command. The lack of this parameter means that the UE does not send a Configuration Complete message as an answer to the Configuration Update Command. As a result, the adversary was capable of intercepting or dropping the Configuration Update Command without having to send an Acknowledgment Request to the CN. The UE was never obtaining the Configuration Update Commands, and as a result, its GUTI remained the same. As we see in Fig. 5, an ACK is requested, so the GUTI Refreshment Neutralization attack is not applicable as opposed to our attack that exploits the lack of integrity in the Configuration Update Command message.

Furthermore, the adversary can take advantage of the lack of ciphering in the 5G-GUTI Reallocation Command, aiming to track the victim's location. First, the adversary can send silent messages or perform silent calls to the victim. A silent call or message is one that does not trigger any notification to the recipient UE [47]. After making (sending) these silent calls (messages), the paging mechanism is triggered either in Cell or TA level, followed by the unencrypted Configuration Update Command including the new victim's 5G-GUTI value. The adversary can sniff the downlink paging channel and search for the victim's unencrypted 5G-GUTI value, thus verifying the victim's presence in a specific cell or TA. The realization of this attack in a large scale network, where many devices are connected, is difficult. By the time the adversary sends the message to the PoI, other devices in the same area can receive messages as well, so the adversary may see many different Configuration Update Commands. To enhance the attack's accuracy, the attacker can send messages with a specific frequency (timing attack) aiming to estimate the victim's paging time, or during non-busy time windows in terms of traffic (e.g., very late at night), or by avoiding to search for the victim in very crowded areas. Unfortunately, with the current experimental setting it was impossible to verify the accuracy of this attack in the private operator deployments, since the traffic from UEs was minimal.

Based on related 3GPP documents [6, 9], the responsibility behind these attacks can be placed to two factors. First, the operator **must not** transmit NAS messages without integrity.

```
LAYER 3 SIGNALING MESSAGE
Time: 11:12:47.975

CONFIGURATION UPDATE COMMAND        3GPP TS 24.501 ver 16.8.0 Rel 16    (8.2.19)

M Extended protocol discriminator (hex data: 7e)
     EPD value: 126 (5GS mobility management)
M Security header type (hex data: 0)
     Security header type: 0 (Plain 5GS NAS message, not security protected)
M Spare Half Octet (hex data: 0)
M Message Type (hex data: 54)
     Message number: 84
O Configuration update indication (hex data: d1)
     ACK: acknowledgement requested
     RED: registration not requested
O 5G-GUTI (hex data: 77000bf2 00f11001 00413cbd 5e7b)
     Type of identity: 5G-GUTI
     MCC: 1
     MNC: 1
     AMF Region ID: 1
     AMF Set ID: 1
     AMF Pointer: 16
     5G-TMSI: 0x3cbd5e7b
```

Figure 5: 5G-GUTI Reallocation Command in 5G SA operator's networks.

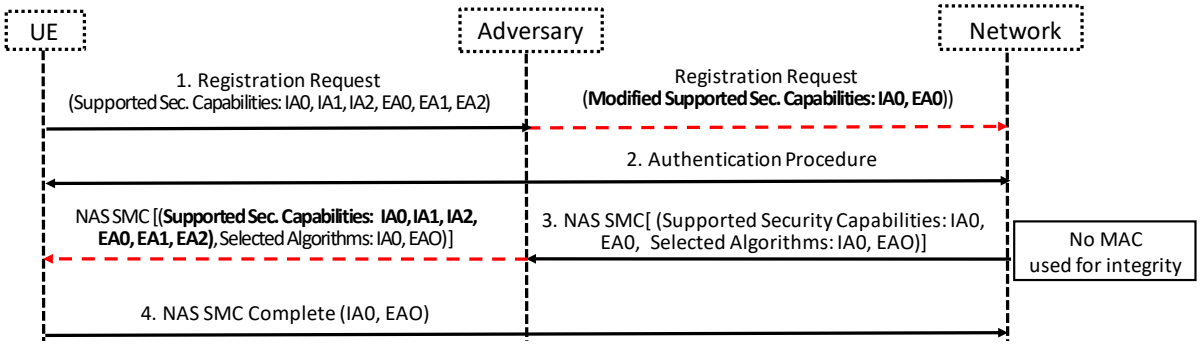
In fact, as shown in Fig. 4a, during the establishment of the NAS Security Channel, integrity was used. Unfortunately, when the UE switched from "Idle" to "Connected" state, due to the activation of the paging mechanism, the operator lost the NAS Security context and did not reestablish it with a NAS SMC message. Second, the lack of ciphering comes from an omission in 3GPP documents. As explicitly written in Sec. 5.5.1 of [9]: "NAS confidentiality is optional to use", also similarly stated in Sec. 4.4.1 of [6]: "The use of ciphering in a network is an operator option. Operation of a network without ciphering is achieved by configuring the AMF so that it always selects the "null ciphering algorithm", 5G-EA0".

Takeaway 8: This is a potential future threat to address: it is not the best strategy to transmit the Configuration Update Command, including the reallocated value of the privacy-sensitive identifier 5G-GUTI, without integrity and encryption.

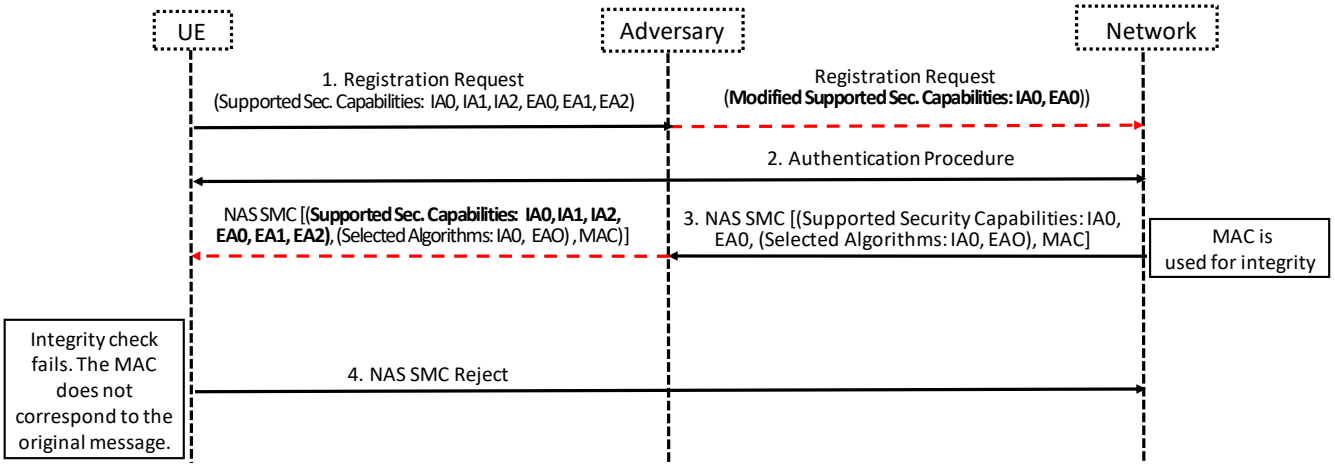
5.2 Security Capabilities Bidding-Down Attack

As it was shown in Sec. 4.4.2, the enhanced NAS Security Mode Command procedure followed by all different operator's implementations (5G NSA and three 5G SA networks), and shown in Fig. 4a, is weaker compared to the one presented in the 3GPP TS. 33.501 [9]. However, the same procedure is implemented correctly in OAI, as shown in Fig. 4b. Here, we discuss a proof of concept of a Bidding-Down attack that works as an extension to the initially presented ones [89, 90], and can lead to privacy deterioration.

First, as shown in both Figures 6a and 6b, the UE sends a Registration Request indicating the supported Security Capabilities for ciphering (encryption) algorithms (e.g., EAO, EA1, EA2) and integrity algorithms (IAO, IA1, IA2) to the network. An active MiTM adversary intercepts this message



(a) Successful Security Capabilities Bidding-Down attack in operator's 5G SA and NSA networks.



(b) Unsuccessful Security Capabilities Bidding-Down attack in OAI emulated network.

Figure 6: The importance of the MAC code in the NAS SMC Enhanced Procedure.

similarly to [89, 90] and modifies the supported security algorithms using the weakest ones, in this case IA0 with EA0. Afterwards, an authentication procedure based on 5G-AKA is followed as described in the Sec. 2.4. When the authentication is completed, the CN sends a NAS Security Mode Command (SMC) to the UE. The 5G NSA and SA operator's networks include only the replayed security capabilities and the selected security algorithms, as illustrated in Fig. 6a. As explained, the OAI implementation follows exactly the 3GPP related documentation transmitting the NAS SMC message with its corresponding Message Authentication Code (MAC) for integrity protection.

Afterwards, the adversary modifies again the supported capabilities, as we see in both Figures 6a and 6b, so that the UE cannot understand the difference between the Supported Security Capabilities as transmitted in the first Registration message and the ones received in the NAS SMC message. In all different 5G SA and NSA operator's implementations, there is not a MAC code, so the integrity of the NAS SMC message cannot be verified by the UE. As a result, the UE accepts the NAS SMC procedure and the weakest security algorithms are used for integrity and ciphering, leading to a successful biding-down attack. Given that the OAI implementation includes the MAC code in the process, the UE can verify the integrity of the NAS SMC message though the MAC code using its private key. The adversary cannot have access to this key, so it cannot modify the MAC code. As a result, the UE understands the NAS SMC message modification by the adversary, the integrity check fails and the UE rejects the NAS SMC.

Takeaway 9: An operator CN implementation may omit the transmission of the Message Authentication Code (MAC) in the NAS Security Mode Command, potentially making both vulnerable to a Security Capabilities-based bidding-down attack. The OAI implementation is adjusted to 3GPP specifications and can mitigate this attack.

6 RELATED WORK

Next, we cover related studies grouped into four main areas, and outline how they compare to our work.

Measurement Studies: There are some experimental studies in 5G NSA and SA networks, mentioning the privacy vulnerabilities of these network infrastructures. For instance, [65, 80, 83, 94] focused only on 5G NSA networks' security vulnerabilities, whereas [75] focused only on 5G SA networks' ones. In contrast to them, we compare 5G SA and NSA operator networks under the same operating settings, analyzing a wide range of security features and their corresponding privacy attacks, thus providing a more concrete and complete work on this topic than the previously mentioned works. We also include in our study a 5G SA OAI open source framework setup, showing the degree of its compliance with the 3GPP standards, and thus its utility to the research community studying these issues.

Attacks on permanent UE IDs: Many different adversaries have tried to steal the UE IMSI, either through an IMSI catching attack [39, 49, 61, 72, 80, 91], or via an IMSI paging attack [23, 27, 64, 89]. Our work shows that IMSI catching attack, as described in Sec. 4.1.1, exists only in 5G NSA networks, since in 5G SA networks SUCI security characteristic is implemented. In fact, *we are the first to show that SUCI can be supported by a real operator 5G SA CN.* As for the IMSI paging attack, as described in Sec. 4.1.2 it is mitigated in both 5G SA and NSA networks, since IMSI was never used for paging. Also, IMEI catching was of primary interest to previous generations' adversaries [34, 73, 78, 82], but as shown in our work in Sec. 4.1.3, both 5G SA and NSA networks have eliminated the vulnerabilities that led to this attack.

Attacks based on TMSI/GUTI and lack of ciphering: Previous cellular network generations focused on TMSI-related attacks [21, 22, 47, 64], taking advantage of the weak TMSI reallocation mechanism. As analyzed in Sec. 4.2, these attacks cannot be deployed in a 5G SA network that follows the 3GPP standards for the reallocation of 5G-GUTI. Also, C-RNTI tracking [51, 52, 70, 87, 88] and the UE measurements reports attacks [26, 78, 89] took advantage of the lack of ciphering, as analyzed in Sec. 4.3. Our work shows that this kind of problems continue to exist in 5G networks, and thus, 3GPP should think of mandating ciphering. Finally, a recent work in 5G [50] theoretically showed potential problems with the GUTI reallocation procedure due to the lack of ACK request. As shown in Sec. 5.1, even if the ACK request is included in the Configuration Update Command, another privacy vulnerability can persist in the GUTI reallocation process, due to lack of integrity and ciphering.

Bidding-Down Attacks: There are a few works focusing on bidding-down attacks based on Security Capabilities as presented in Sec. 4.4.2. First, [89] introduced this attack as in LTE networks, proposing the replay of the Security capabilities for its mitigation. Then, [30] and [53] showed the lack of a replay mechanism for security capabilities in 4G, and the lack of enhanced initial NAS message protection in 5G NSA networks, respectively. Our work shows the replay of security capabilities has been done in both 5G NSA and SA, but as explained in Sec. 5.2, it is not enough. In fact, we are the first to stress the importance of Message Authentication Code (MAC) process in the NAS SMC command, and show its correct implementation in an OAI emulated network.

7 DISCUSSION

Based on the qualitative and experimental analysis presented in Sec. 4, and the corresponding summary made in Table 1, we draw important lessons about 5G privacy. First, all three deployment setups (operator's 5G SA and 5G NSA networks, and OAI 5G SA SDN network) have mitigated traditional attacks caused by the IMSI paging and IMEI or Radio Capabilities transmission, following the corresponding mitigation mechanisms, as mentioned in Takeaways 2, 3 and 6. Second, the 5G SA operator's implementations and the OAI 5G SA SDN testbed support SUCI mechanism (Takeaway 1), thus, mitigating IMSI Catchers attack and offering better UE identity privacy, as opposed to the 5G NSA infrastructure. Third, the 5G-GUTI update mechanism is implemented accurately in two out of three 5G SA operator's networks, thus, mitigating the TMSI Deanonymity attack, in contrast to the 5G NSA operator network and OAI SDN based one (Takeaway 4). Unfortunately, C-RNTI tracking and UE measurement reports attacks are still existent in all of the examined networks. Therefore, stricter 3GPP regulations are needed, mandating the ciphering of RRC messages (Takeaway 5). Finally, NAS SMC procedure is partially implemented by all 5G SA networks and the 5G NSA network as well, whereas OAI followed exactly the 3GPP TSs., adding the MAC in corresponding messages (Takeaway 7).

Our work also presented two new 5G vulnerabilities that can be potential privacy risks in future 5G networks. As explained in Sec. 5.1 and summarized in Takeaway 8, 5G SA networks transmit the Configuration Update Command without integrity and ciphering, thus, risking DoS attacks and potential UE tracking. We believe that measures should be taken against this problem, both from the operators (integrity protection) and 3GPP community (mandatory ciphering) sides. Moreover, in Sec. 5.2, another novel privacy attack was outlined, taking advantage of the NAS SMC vulnerability of all operator's networks. As shown, including the MAC in the NAS SMC message, similarly to what OAI implementation does, is of paramount importance for being safe against bidding-down attacks (Takeaway 9).

Next, we discuss why these privacy problems arose. Regarding the use of RRC ciphering, as explained in 3GPP-related documents [9] and discussed earlier (Sec. 4), it is a functionality that remains optional for the operator. This can explain its lack of activation during our experiments, even if it is supported by the gNBs. This finding aligns well

with earlier reports [30, 65], that showed operators are often unwilling to activate such optional security features that add computational overhead to the network. As for the attack described in Sec. 5.1, the different CNs lost the integrity protection that had been activated before with the NAS Security Command message (Fig. 4a). We confirmed this was a result of a CN mis-configuration. Further, the lack of NAS ciphering is an operator's choice (Sec. 5.1), and similar to RRC ciphering, it was not activated by the different CNs for similar reasons. Finally, the 5G bidding-down attack, described in Sec. 5.2, exploits another CN mis-implementation, which is the lack of MAC in the NAS Security Mode Command message. We remark that the 3GPP-related document [9] does not sufficiently explain the importance and use of this MAC in this process, and therefore, the operators/vendors may under-estimate its critical role. As shown in Sec. 5, both new attacks were applicable to different 5G networks, indicating common CN mis-configurations/mis-implementations for the specific operator and vendors. We stress the importance of our findings: same vendors of 5G CN solutions can be providers to network operators in various countries, and therefore, such privacy attacks can be applicable to other CNs beyond the ones tested.

To summarize, 5G SA followed almost all of the 3GPP privacy enhancements mentioned in Sec. 4 and is more privacy-preserving than the 5G NSA network, which inherently missed SUCI and 5G-GUTI update mechanisms. Furthermore, stricter policies are needed from the 3GPP community, mandating ciphering and mitigating the corresponding privacy attacks. Operators and 3GPP community should take into consideration the attacks mentioned in Sec. 5 and make the appropriate adjustments to their implementations and Technical Specifications, respectively. Finally, OAI showed almost excellent results in terms of privacy, considering that it is an open source project, missing only the 5G-GUTI update mechanism and can be used for privacy studies by the research and industry 5G community, while the considerations from the present study are taken into account.

We mention that all of our findings in the private operator's 5G NSA and SA networks have been reported to the operator for further assessment. Besides, the weakness of 5G-GUTI update mechanism has been communicated to OAI development team as well, together with details on the procedure to correct it.

AKA Protocol Linkability attack: We have not discussed here the AKA protocol linkability attack [21, 23, 45, 56]. This attack was common since 3G (no AKA protocol in 2G), performing location tracking by linking two AKA sessions of the same user. Recent papers [41, 50, 62, 93] verified it in 5G. The 3GPP community analyzed this attack in Sec. 6.2 of [1], proposing modifications to the 5G AKA protocol, such as ciphering of different 5G-AKA parameters. These modifications can mitigate this problem, but are still not included in the 5G Systems Security protocols and procedures in 3GPP 5G Specifications [9]. Thus, until now, there is no official 3GPP mitigation mechanism against this attack.

8 CONCLUSION

In this paper, we presented a first of its kind, head-on comparison between 5G stand alone (SA) and non-stand alone (NSA) cellular networks, in terms of security and privacy capabilities across 8 different top pre-5G attacks. As shown, 5G SA offers higher identity privacy, since SUCI identifier and 5G-GUTI reallocation mechanism are properly supported. On the other hand, problems inherited by the previous cellular generations, and caused by the lack of ciphering continue to exist, since ciphering is still optional in 3GPP documentation, making both of the 5G implementations (SA and NSA) vulnerable to NAS and RRC based protocol attacks. Our in-depth analysis also revealed two new potential attacks against UE privacy. The first exploits the lack of ciphering and integrity of the Configuration Update Command used for updating the 5G-GUTI value. The second is a security capabilities bidding-down attack, exploiting the lack of inclusion of Message Authentication Code (MAC) in the NAS Security Mode Command. Finally, privacy features of OAI were analyzed showing that it can be considered for privacy studies, as only the 5G-GUTI update mechanism is missing.

ACKNOWLEDGEMENTS

This research was partially supported by: The Ministry of Economic Affairs and Digital Transformation of Spain and the European Union-Next Generation EU programme for the Recovery, Transformation and Resilience Plan and the Recovery and Resilience Mechanism under agreements TSI-063000-2021-63 (MAP-6G), TSI-063000-2021-142 and TSI-063000-2021-147 (6G-RIEMANN); The European Union Horizon 2020 program under grant agreements 101021808 (SPATIAL), 101096435 (CONFIDENTIAL6G) and 101139067 (ELASTIC). The views and opinions expressed are those of the authors only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them. The authors thank Maria del Mar Moreno, Javier Jimemez, Manuel Palacios Trapero for their help during the experiments.

REFERENCES

[1] 2021. 3GPP TS 33.846, "Study on authentication enhancements in the 5G System (5GS)," version 17.0.0 Rel. 17. https://www.3gpp.org/. Accessed: 2024-02.

[2] 2021. gr-LTE: GNU Radio LTE receiver. https://github.com/kit-cel/gr-lte/. Accessed 2024-02.

[3] 2021. OpenLTE: An open source 3GPP LTE implementation. https://sourceforge.net/projects/openlte/. Accessed 2024-02.

[4] 2023. 3GPP TS 23.003, "Numbering, addressing and identification," version 18.2.0 Rel. 18. https://www.3gpp.org/. Accessed: 2024-02.

[5] 2023. 3GPP TS 23.501, "System architecture for the 5G System (5GS)," version 18.3.0 Rel. 18. https://www.3gpp.org/. Accessed: 2024-02.

[6] 2023. 3GPP TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS)," version 18.4.0 Rel. 18. https://www.3gpp.org/. Accessed: 2024-02.

[7] 2023. 3GPP TS 33.102, "3G Security; Security Architecture," version 17.0.0 Rel. 17. https://www.3gpp.org/. Accessed: 2024-02.

[8] 2023. 3GPP TS 33.401, "3GPP System Architecture Evolution (SAE); Security architecture," version 17.4.0 Rel. 17. https://www.3gpp.org/. Accessed: 2024-02.

[9] 2023. 3GPP TS 33.501, "Security architecture and procedures for 5G system," version 18.2.0 Rel. 18. https://www.3gpp.org/. Accessed: 2024-02.

[10] 2023. 3GPP TS 33.846, "Study on authentication enhancements in the 5G System (5GS)," version 17.0.0 Rel. 17. https://www.3gpp.org/. Accessed: 2024-02.

[11] 2023. 3GPP TS 38.306, "NR; User Equipment (UE) radio access capabilities," version 18.0.0 Rel. 18. https://www.3gpp.org/. Accessed: 2024-02.

[12] 2023. 3GPP TS 38.331, "NR; Radio Resource Control (RRC) protocol specification," version 17.6.0 Rel. 17. https://www.3gpp.org/. Accessed: 2024-02.

[13] 2023. srsRAN: an open source 4G software radio suite developed by SRS. https://github.com/srsran/srsRAN_4G/. Accessed 2024-02.

[14] 2024. Ettus. USRP. https://www.ettus.com/products/. Accessed 2024-02.

[15] 2024. OpenAirInterface Source Code for Next Generation Cellular Standard. https://gitlab.eurecom.fr/oai/. Accessed 2024-02.

[16] Messenger application. 2024. https://www.messenger.com/. Accessed: 03-2024.

[17] Nemo Handy Handheld Measurement Solution. 2024. https://www.keysight.com/us/en/product/NTH50047B/nemo-handy-handheld-measurement-solution.html/. Accessed: 03-2024.

[18] Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030. 2023. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide//. Accessed: 03-2024.

[19] 5GAmericas. 2023. Global 5G Connections Increase 76% Annually and Now Reaches 1.05 Billion. https://www.5gamericas.org/global-5g-connections-increase-76-annually-and-now-reaches-1-05-billion/. Accessed: 2024-02.

[20] Zahra Ahmadian, Somayeh Salimi, and Ahmad Salahi. 2009. New attacks on UMTS network access. In *2009 Wireless Telecommunications Symposium*. IEEE, 1–6.

[21] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kevin Redon, and Ravishankar Borgaonkar. 2012. New privacy issues in mobile telephony: fix and verification. In *Proceedings of the 2012 ACM conference on Computer and communications security*. 205–216.

[22] Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, and Mark Ryan. 2014. Privacy through Pseudonymity in Mobile Telephony Systems.. In *NDSS*.

[23] Myrto Arapinis, Loretta Ilaria Mancini, Eike Ritter, and Mark Dermot Ryan. 2017. Analysis of privacy in mobile telephony systems. *International Journal of Information Security* 16 (2017), 491–523.

[24] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. 2018. A formal analysis of 5G authentication. In *Proceedings of the 2018 ACM SIGSAC conference on computer and communications security*. 1383–1396.

[25] Shanay Behrad, Emmanuel Bertin, and Noel Crespi. 2018. Securing authentication for mobile networks, a survey on 4G issues and 5G answers. In *2018 21st conference on innovation in clouds, internet and networks and workshops (ICIN)*. IEEE, 1–8.

[26] Evangelos Bitsikas and Christina Pöpper. 2021. Don't hand it over: Vulnerabilities in the handover procedure of cellular telecommunications. In *Annual Computer Security Applications Conference*. 900–915.

[27] Iva Bojic, Yuji Yoshimura, and Carlo Ratti. 2017. Opportunities and challenges of trip generation data collection techniques using cellular networks. *IEEE Communications Magazine* 55, 3 (2017), 204–209.

[28] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. 2018. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. *Cryptology ePrint Archive* (2018).

[29] Nicola Bui and Joerg Widmer. 2016. OWL: A reliable online watcher for LTE control channel measurements. In *Proceedings of the 5th Workshop on All Things Cellular: Operations, Applications and Challenges*. 25–30.

[30] Merlin Chlosta, David Rupprecht, Thorsten Holz, and Christina Pöpper. 2019. LTE security disabled: misconfiguration in commercial networks. In *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*. 261–266.

[31] Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz. 2021. 5G SUCI-Catchers: Still catching them all?. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 359–364.

[32] Hiten Choudhury, Basav Roychoudhury, and Dilip Kr Saikia. 2012. Enhancing user identity privacy in LTE. In *2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications*. IEEE, 949–957.

[33] Adrian Dabrowski, Georg Petzl, and Edgar R Weippl. 2016. The messenger shoots back: Network operator based IMSI catcher detection. In *Research in Attacks, Intrusions, and Defenses: 19th International Symposium, RAID 2016, Paris, France, September 19-21, 2016, Proceedings 19*. Springer, 279–302.

[34] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. 2014. IMSI-catch me if you can: IMSI-catcher-catchers. In *Proceedings of the 30th annual computer security applications Conference*. 246–255.

[35] Johannes Demel, Sebastian Koslowski, and Friedrich K Jondral. 2015. A LTE receiver framework using GNU Radio. *Journal of Signal Processing Systems* 78 (2015), 313–320.

[36] Yaping Deng, Hong Fu, Xianzhong Xie, Jihua Zhou, Yucheng Zhang, and Jinling Shi. 2009. A novel 3GPP SAE authentication and key agreement protocol. In *2009 IEEE International Conference on Network Infrastructure and Digital Content*. IEEE, 557–561.

[37] Okoye Emmanuel Ekene, Ron Ruhl, and Pavol Zavarsky. 2016. Enhanced user security and privacy protection in 4G LTE network. In *2016 IEEE 40th Annual Computer Software and Applications Conference (COMPSAC)*, Vol. 2. IEEE, 443–448.

[38] Stavros Eleftherakis, Domenico Giustiniano, and Nicolas Kourtellis. 2024. SoK: Evaluating 5G Protocols Against Legacy and Emerging Privacy and Security Attacks. arXiv:2409.06360 [cs.CR] https://arxiv.org/abs/2409.06360

[39] Simon Erni, Martin Kotuliak, Patrick Leu, Marc Roeschlin, and Srdjan Capkun. 2022. AdaptOver: adaptive overshadowing attacks in cellular networks. In *Proceedings of the 28th Annual International Conference*

on Mobile Computing And Networking. 743–755.

[40] Robert Falkenberg and Christian Wietfeld. 2019. FALCON: An accurate real-time monitor for client-based mobile network data analytics. In *2019 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 1–7.

[41] Teng Fei and Wenye Wang. 2023. The vulnerability and enhancement of AKA protocol for mobile authentication in LTE/5G networks. *Computer Networks* 228 (2023), 109685.

[42] Joachim Frick and Rainer Bott. 2000. Method for identifying a mobile phone user or for eavesdropping on outgoing calls. Patent, Rohde & Schwarz, EP 1051053.

[43] M Køien Geir et al. 2013. Privacy enhanced mutual authentication in LTE. In *2013 IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 614–621.

[44] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D Sutton, Pablo Serrano, Cristina Cano, and Doug J Leith. 2016. srsLTE: An open-source platform for LTE evolution and experimentation. In *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*. 25–32.

[45] Changhee Hahn, Hyunsoo Kwon, Daeyoung Kim, Kyungtae Kang, and Junbeom Hur. 2014. A privacy threat in 4th generation mobile telephony and its countermeasure. In *Wireless Algorithms, Systems, and Applications: 9th International Conference, WASA 2014, Harbin, China, June 23-25, 2014. Proceedings 9*. Springer, 624–635.

[46] Tuan Dinh Hoang, CheolJun Park, Mincheol Son, Taekkyung Oh, Sangwook Bae, Junho Ahn, Beomseok Oh, and Yongdae Kim. 2023. LTESniffer: An Open-source LTE Downlink/Uplink Eavesdropper. (2023).

[47] Byeongdo Hong, Sangwook Bae, and Yongdae Kim. 2018. GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier.. In *NDSS*.

[48] Syed Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A systematic approach for adversarial testing of 4G LTE. In *Network and Distributed Systems Security (NDSS) Symposium 2018*.

[49] Syed Rafiul Hussain, Mitziu Echeverria, Omar Chowdhury, Ninghui Li, and Elisa Bertino. 2019. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information. *Network and distributed systems security (NDSS) symposium2019* (2019).

[50] Syed Rafiul Hussain, Mitziu Echeverria, Imtiaz Karim, Omar Chowdhury, and Elisa Bertino. 2019. 5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 669–684.

[51] Roger Piqueras Jover. 2016. LTE security and protocol exploits. *Shmoocon 2016* (2016).

[52] Roger Piqueras Jover. 2016. LTE security, protocol exploits and location tracking experimentation with low-cost software radio. *arXiv preprint arXiv:1607.05171* (2016).

[53] Bedran Karakoc, Nils Fürste, David Rupprecht, and Katharina Kohls. 2023. Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G. (2023).

[54] Haibat Khan, Benjamin Dowling, and Keith M Martin. 2018. Identity confidentiality in 5G mobile telephony systems. In *International Conference on Research in Security Standardisation*. Springer, 120–142.

[55] Haibat Khan and Keith M Martin. 2020. A survey of subscription privacy on the 5G radio interface-the past, present and future. *Journal of Information Security and Applications* 53 (2020), 102537.

[56] Mohammed Shafiul Alam Khan and Chris J Mitchell. 2014. Another look at privacy threats in 3G mobile telephony. In *Australasian Conference on Information Security and Privacy*. Springer, 386–396.

[57] Mohammed Shafiul Alam Khan and Chris J Mitchell. 2015. Improving air interface user privacy in mobile telephony. In *Security Standardisation Research: Second International Conference, SSR 2015, Tokyo, Japan, December 15-16, 2015, Proceedings 2*. Springer, 165–184.

[58] Mohammed Shafiul Alam Khan and Chris J Mitchell. 2017. Trashing IMSI catchers in mobile networks. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 207–218.

[59] Rabia Khan, Pardeep Kumar, Dushantha Nalin K Jayakody, and Madhusanka Liyanage. 2019. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Communications Surveys & Tutorials* 22, 1 (2019), 196–248.

[60] Katharina Kohls, David Rupprecht, Thorsten Holz, and Christina Pöpper. 2019. Lost traffic encryption: fingerprinting LTE/4G traffic on layer two. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 249–260.

[61] Martin Kotuliak, Simon Erni, Patrick Leu, Marc Röschlin, and Srdjan Čapkun. 2022. {LTrack}: Stealthy tracking of mobile phones in {LTE}. In *31st USENIX Security Symposium (USENIX Security 22)*. 1291–1306.

[62] Adrien Koutsos. 2019. The 5G-AKA authentication protocol privacy. In *2019 IEEE European symposium on security and privacy (EuroS&P)*. IEEE, 464–479.

[63] Swarun Kumar, Ezzeldin Hamed, Dina Katabi, and Li Erran Li. 2014. LTE radio analytics made easy and accessible. *ACM SIGCOMM Computer Communication Review* 44, 4 (2014), 211–222.

[64] Denis Foo Kune, John Koelndorfer, Nicholas Hopper, and Yongdae Kim. 2012. Location leaks on the GSM air interface. *ISOC NDSS (Feb 2012)* (2012).

[65] Oscar Lasierra, Gines Garcia-Aviles, Esteban Municio, Antonio Skarmeta, and Xavier Costa-Pérez. 2023. European 5G Security in the Wild: Reality versus Expectations. *arXiv preprint arXiv:2305.08635* (2023).

[66] Xiehua Li and Yongjun Wang. 2011. Security enhanced authentication and key agreement protocol for LTE/SAE network. In *2011 7th International Conference on Wireless Communications, Networking and Mobile Computing*. IEEE, 1–4.

[67] Andy Lilly. 2017. IMSI catchers: hacking mobile communications. *Network Security* 2017, 2 (2017), 5–7.

[68] Fuwen Liu, Li Su, Bo Yang, Haitao Du, Minpeng Qi, and Shen He. 2021. Security Enhancements to Subscriber Privacy Protection Scheme in 5G Systems. In *2021 International Wireless Communications and Mobile Computing (IWCMC)*. IEEE, 451–456.

[69] Norbert Ludant and Guevara Noubir. 2021. SigUnder: a stealthy 5G low power attack and defenses. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 250–260.

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

[71] Ian Marsden and Paul Marshall. 2014. Multi IMSI system and method. US Patent App. 13/966,350.

[72] Ulrike Meyer and Susanne Wetzel. 2004. A man-in-the-middle attack on UMTS. In *Proceedings of the 3rd ACM workshop on Wireless security*. 90–97.

[73] Benoit Michau and Christophe Devine. 2016. How to not break LTE crypto. In *ANSSI Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*.

[74] Chris Mitchell. 2001. The security of the GSM air interface protocol. *Univ. of London, Royal Holloway, RHUL-MA-2001-3* (2001).

[75] Shiyue Nie, Yiming Zhang, Tao Wan, Haixin Duan, and Song Li. 2022. Measuring the deployment of 5g security enhancement. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 169–174.

[76] Navid Nikaein, Mahesh K Marina, Saravana Manickam, Alex Dawson, Raymond Knopp, and Christian Bonnet. 2014. OpenAirInterface: A

flexible platform for 5G research. *ACM SIGCOMM Computer Communication Review* 44, 5 (2014), 33–38.

[77] Karl Norrman, Mats Näslund, and Elena Dubrova. 2016. Protecting IMSI and user privacy in 5G networks. In *Proceedings of the 9th EAI international conference on mobile multimedia communications*. 159–166.

[78] Ruxandra F Olimid and Stig F Mjølsnes. 2017. On LowCost Privacy Exposure Attacks in LTE Mobile Communication. *Proceedings of the Romanian Academy Series AMathematics Physics Technical Sciences Information Science* 18 (2017), 361–370.

[79] Chris Paget. 2010. Practical cellphone spying. *Def Con* 18 (2010).

[80] Ivan Palamà, Francesco Gringoli, Giuseppe Bianchi, and Nicola Blefari-Melazzi. 2021. IMSI Catchers in the wild: A real world 4G/5G assessment. *Computer Networks* 194 (2021), 108137.

[81] Pier Luigi Parcu, Anna Renata Pisarkiewicz, Chiara Carrozza, and Niccolò Innocenti. 2023. The future of 5G and beyond: Leadership, deployment and European policies. *Telecommunications Policy* 47, 9 (2023), 102622. https://doi.org/10.1016/j.telpol.2023.102622

[82] CheolJun Park, Sangwook Bae, BeomSeok Oh, Jiho Lee, Eunkyu Lee, Insu Yun, and Yongdae Kim. 2022. {DoLTEst}: In-depth Downlink Negative Testing Framework for {LTE} Devices. In *31st USENIX Security Symposium (USENIX Security 22)*. 1325–1342.

[83] Seongmin Park, Daeun Kim, Youngkwon Park, Hyungjin Cho, Dowon Kim, and Sungmoon Kwon. 2021. 5G security threat assessment in real networks. *Sensors* 21, 16 (2021), 5524.

[84] Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, and Jean-Pierre Seifert. 2019. Anatomy of commercial IMSI catchers and detectors. In *Proceedings of the 18th ACM Workshop on Privacy in the Electronic Society*. 74–86.

[85] RCRWirelessNews. 2024. 2024 will be a catalyst for accelerating 5G Standalone/5G Core deployments. https://www.rcrwireless.com/20240130/opinion/readerforum/2024-will-be-a-catalyst-for-accelerating-5g-standalone-5g-core-deployments-reader-forum. Accessed: 2024-02.

[86] David Rupprecht, Adrian Dabrowski, Thorsten Holz, Edgar Weippl, and Christina Pöpper. 2018. On security research towards future mobile network generations. *IEEE Communications Surveys & Tutorials* 20, 3 (2018), 2518–2542.

[87] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2019. Breaking LTE on layer two. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, 1121–1136.

[88] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2020. Call me maybe: Eavesdropping encrypted {LTE} calls with {ReVoLTE}. In *29th USENIX security symposium (USENIX security 20)*. 73–88.

[89] Altaf Shaik, Ravishankar Borgaonkar, N Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2015. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *arXiv preprint arXiv:1510.07563* (2015).

[90] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 221–231.

[91] Daehyun Strobel. 2007. IMSI catcher. *Chair for Communication Security, Ruhr-Universität Bochum* 14 (2007).

[92] Fabian Van Den Broek, Roel Verdult, and Joeri De Ruiter. 2015. Defeating IMSI catchers. In *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*. 340–351.

[93] Yuchen Wang, Zhenfeng Zhang, and Yongquan Xie. 2021. {Privacy-Preserving} and {Standard-Compatible}{AKA} Protocol for 5G. In *30th USENIX Security Symposium (USENIX Security 21)*. 3595–3612.

[94] Mohamad Saalim Wani, Michael Rademacher, Thorsten Horstmann, and Mathias Kretschmer. 2024. Security Vulnerabilities in 5G Non-Stand-Alone Networks: A Systematic Analysis and Attack Taxonomy. *Journal of Cybersecurity and Privacy* 4, 1 (2024), 23–40.

[95] Hojoon Yang, Sangwook Bae, Mincheol Son, Hongil Kim, Song Min Kim, and Yongdae Kim. 2019. Hiding in plain signal: Physical signal overshadowing attack on {LTE}. In *28th USENIX Security Symposium (USENIX Security 19)*. 55–72.

[96] Chuan Yu, Shuhui Chen, Fei Wang, and Ziling Wei. 2021. Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers. *Computer Networks* 201 (2021), 108532.

[97] Muxiang Zhang and Yuguang Fang. 2005. Security analysis and enhancements of 3GPP authentication and key agreement protocol. *IEEE Transactions on wireless communications* 4, 2 (2005), 734–742.