Never let me down again: Bidding-Down Attacks and Mitigations in 5G and 4G

Bedran Karakoc
Ruhr University Bochum
bedran.karakoc@rub.de

Nils Fürste
Software Radio Systems
nils.fuerste@srs.io

David Rupprecht
Ruhr University Bochum
david.rupprecht@rub.de

Katharina Kohls
Radboud University Nijmegen
kkohls@cs.ru.nl

***Abstract*—Bidding-down attacks reduce the security of a mobile network connection. Weaker encryption algorithms or even downgrades to prior network generations enable an adversary to exploit several attack vectors and harm the users of a network. The problem of bidding down attacks has been known for generations, and various mitigations are integrated into the latest 4G and 5G specifications. However, the current state lacks a systematic identification and analysis of the variety of potential attack vectors. In this work, we classify an extensive set of bidding-down attack vectors and analyze their specification and implementation. We test different commercial phones and networks in a controlled lab setup and in public networks. Our results demonstrate vulnerabilities for all attacks and devices, including the latest mobile generation 5G and recent flagship phones. To further prove how the identified attack vectors can be exploited in sophisticated attacks, we conduct two case studies in which we apply a full downgrade attack from 5G SA to 2G and bid down a 5G NSA connection by enforcing null encryption. Again, we find a majority of systems vulnerable. With this paper, we hope to improve the state of bidding down mitigations in the specification and implementation.**

1. Introduction

Mobile communication is an integral part of our daily lives. It has an essential role in casual use cases, e. g., approximately 4.66 billion people worldwide use the Internet, and 92.6 percent are online with mobile devices [24]. Besides, mobile networks are a fundamental building block in industrial contexts, critical infrastructures, and for first-responder communication. Due to this ubiquitous integration into our lives, we do not only depend on the reliable performance of networks, but we are also directly affected by security flaws. Although every new generation of a mobile network introduces security features that overcome prior weaknesses, backward compatibility with older generations preserves severe attack vectors. Bidding-down attacks exploit this fact and degrade the security of a connection. The entry points for such attacks are diverse, which hinders the deployment of a generic mitigation technique.

The most prominent examples of bidding-downs are downgrade attacks that force a phone into a connection with an older, more insecure generation. Those inter-generation bidding-down attacks exploit legitimate protocol functionality and are common entry points for IMSI catchers [32]. In this case, a bidding-down attack enables an attacker to completely circumvent the latest security mechanisms and allows them to eavesdrop on calls or text messages. However, bidding-down attacks can also exist within (intra) a generation. For example, when the phone makes the network believe that only null algorithms are supported, which upon acceptance leads to an unencrypted connection.

Given this concrete threat, prior work addresses individual attack vectors. While this allows us to learn more about downgrade attacks [34] or how connections can be manipulated into using null encryption [5], [33], these works are focused on a *single* type of attack. As bidding-down attacks can be diverse, this isolated view is insufficient to fully understand the current threat of bidding-down in the latest mobile generations. Although we already see publications on automatic test suites for implementations [31], [23], [20] or specifications [18], [4], [17], we lack a systematic and targeted analysis of different classes of bidding-down attacks. Consequently, we cannot be sure about the efficiency of mitigation techniques that are in place at the moment. This leaves us with a significant blind spot regarding a severe security threat in our deployed networks.

The threat of bidding-down attacks is well-known and recognized by the 3GPP, which is the organization responsible for specifying mobile networks. The latest generation 5G defines the prevention of such attacks as a fundamental security requirement. Consequently, different aspects of the architecture and protocols include bidding-down mitigations that should prevent any kind of attack. However, the sheer diversity of potential entry points for a bidding-down attack mandates a systematic analysis of mobile networks. To the best of our knowledge, the current state of the art provides mostly isolated security analyses of individual attack concepts, but it cannot offer a structured comparison of UE- and network-based attack vectors.

We provide a systematic categorization of intra- and inter-generation bidding-down attacks and their attack vectors. Based on this extensive systematization of attacks, we extend existing security test cases by 29 new tests that allow us to analyze the effectiveness of 5G and 4G bidding-down mitigations. We conduct these experiments with seven commercial phones, four open-source core networks with commercial licensing options, and three public networks. *Our*

findings are concerning: For all classes of bidding-down attacks, we find vulnerable UEs and networks, i. e., multiple open attack vectors exist for intra- and inter-generation bidding-down attacks. This includes transmissions with null encryption, missing security features enabled in phones and public networks. Further, we are the first to demonstrate a downgrade from 5G to 2G, affecting all tested phones.

To contribute to the security of current and future releases of mobile networks, we share a detailed description of test cases that can be used to audit the implementation of bidding-down mitigations before a market release. Further, we analyze possible flaws and ambiguities in the current specifications. In a detailed discussion, we elaborate on our findings and propose ways to improve the current situation. With our publication, we emphasize the need for an effective prevention mechanism against bidding-down attacks in the current generation and hope that these findings enhance the specification and implementation. In summary, we provide four key contributions:

- We provide a systematic classification of bidding-down attacks, their attack vectors, and the specific features that can be exploited in different generations. The result is an extensive attack classification.
- We systematically review the specification based on the attack classification. Our analysis reviews specification flaws and ambiguities that contribute to the feasibility of bidding-down attacks.
- We extend existing test cases to comprehensively cover all classified attack vectors and conduct a systematic security analysis of phones and networks. Our results indicate that *all* systems under test are vulnerable to intra- and inter-generation attacks up to a total downgrade from 5G to 2G.
- We provide a detailed discussion that elaborates on the current shortcomings and proposes improvements for specification and implementation flaws.

Responsible Disclosure. At the time of submission, we started the responsible disclosure process to ensure that the implementation issues are fixed as soon as possible and that the specification issues are addressed appropriately by the specification bodies. We used the GSMA CVD program [11] to officially communicate our findings for all flaws, including those found in public networks. We further notify manufacturers about implementation flaws to contribute to timely fixes.

2. Preliminaries

In preparation for the systematic analysis of bidding-down vulnerabilities, we introduce the background of mobile networks and document existing security testing approaches. Finally, we provide a problem statement that specifies the scope of this work.

2.1. Mobile Network Architecture

From a high-level view, we separate the mobile network into three parts. The **User Equipment (UE)** is the end-device that connects to base stations (eNB/gNB) through the Radio Access Network (RAN). The RAN is responsible for managing the radio layer resources and encrypting the user data. The **core network** consists of various components and is responsible for authentication and mobility management. An example of such a component in a 5G network is the Access and Mobility Management Function (AMF), which is the entry point for the UE to the core network.

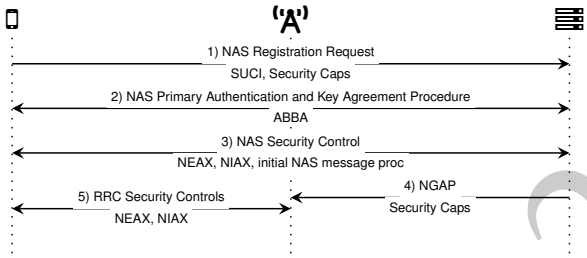

Figure 1. Simplified security context establishment between UE and core network in 5G SA.

Mobile networks employ protocols to abstract tasks and responsibilities. For the radio connection, the Packet Data Convergence Protocol (PDCP) and Radio Resource Control (RRC) are particularly security-relevant. For the connection between the UE and the core network, the Non-Access Stratum (NAS) protocol is responsible for establishing a secure connection with the Authentication and Key Agreement (AKA) procedure.

2.2. Security Establishment

In the security establishment, the UE and the network establish a security context for the connection (cf. Figure 1). Exemplary for 5G, we describe each step in this procedure. The procedure is similar for older mobile network generations but uses different terminology.

1) The UE sends the `Registration Request` containing all supported security algorithms. Currently, four security algorithms for encryption and integrity protection are specified. One of them is the null algorithm which does not provide any security. Optionally, the request contains the encrypted Subscriber Concealed Identifier (SUCI) as an identifier (5G-specific).

2) Based on the UE identity, the core network performs an authentication procedure that establishes mutual authentication. The authentication request also contains the so-called Anti-Bidding down Between Architectures (ABBA) parameter that shall prevent bidding-down attacks in the future (5G-specific).

3) Once authenticated, the core network selects the security algorithm used for the NAS connection and sends its response in the `Security Mode Command` including a replay of the initial `UE Security Capabilities`.

4) & 5) Further, the core network sends the `UE Security Capabilities` to the Next Generation NodeB (gNB), which subsequently chooses a security algorithm used for

the radio connection. Those are then established via the RRC security control procedure.

It is important to note that the pre-authentication traffic before the security establishment is completely unprotected, which means that the UE is unable to verify the legitimacy of messages. This opens up an attack vector that enables fake base station attacks.

2.3. Deployment Scenarios

Mobile communications can be deployed in a variety of ways. With respect to this paper, we focus on 4G and 5G implementations. In 4G, the UE connects to the Evolved NodeB (eNB) via the air interface, which is connected to the 4G core network. The 5G Non Standalone (NSA) networks can be installed in multiple deployment options [13]. For the scope of this paper, we analyze the widely used NSA option E-UTRAN New Radio Dual Connectivity (ENDC) [37]. In an ENDC deployment, the UE connects to an main eNB and secondary gNB, which are connected to a 4G core network. In the following, we refer to ENDC as 5G NSA. In 5G Standalone (SA), the UE connects via the air interface to a gNB, which is exclusively connected to the 5G core network. We refer to 5G SA as 5G if not stated otherwise.

2.4. Problem Statement

We consider a mobile network consisting of the infrastructure maintained by the mobile network operator (base stations and a core network component) and the UEs of end-users. The capabilities of all components in this setting depend on their implementations and can differ depending on their individual hardware. We assume that the end-users and network operators are honest and that an external adversary is interested in conducting any form of a bidding-down as a stepping-stone for follow-up attacks.

Bidding-down Attacks. In a bidding-down attack, an adversary attempts to reduce the security capabilities of a network connection. This can either result in an intra-generation bidding-down, where the mobile generation remains the same and the internal security measures are weakened on purpose. In an inter-generation bidding-down, the adversary forces the connection from one mobile generation into another. As older generations tend to have more known flaws, this weakens the overall security of the connection. Our main focus is on analyzing the feasibility of bidding-down attacks against the different implementations of UEs and core networks. To this end, we build a versatile experimental setup that involves commercial and open-source network components.

Security Assessment. The 3GPP defines a basic set of security tests in their Security Assurance Specification (SCAS). These test cases define the expected behavior for different components of a mobile network infrastructure, i. e., a failing test case indicates a potential security issue in a component. While SCAS serves as a foundation for the assessment of mobile network security, we point out numerous shortcomings in the existing test specifications and identify further relevant test cases that are currently not covered.

Attacker Model. We assume an *active* adversary capable of sending and receiving messages on the radio layer. This includes interaction on each layer of the protocol stack in both directions, i. e., towards the UE and towards the network. In practice, such a setting can be implemented through a software-defined radio and a software stack implementation of the mobile network generation(s) under attack. We further assume that the adversary has no knowledge about any internal information of the core network and the UE, e. g., key material. The goal of the adversary is to conduct a bidding-down attack of any kind. To this end, the different attack vectors introduced in Section 3 are exploited.

3. Bidding-Down Attacks

The feasibility of a bidding-down attack mainly depends on its individual attack vector and if or how it can be exploited in an implementation. In the following, we first introduce our categorization characteristics and then assess the two major classes of attacks.

3.1. Categorization

We categorize the different bidding-down attacks according to the following characteristics.

Class. We distinguish between two general *classes* of bidding-down attacks. Intra-generation bidding-down attacks decrease the security level within a generation, e. g., when an attacker can lower the used security algorithm. In contrast, inter-generation attacks enable a downgrade to an older generation, e. g., an attacker can downgrade a connection with a specific message from a 4G connection to a more insecure 2G connection. We further detail the attack classes in Sections 3.2 and 3.3.

Attack Vector. In the next step, we distinguish different types of *attack vectors* that can be exploited to achieve the bidding-down. Each of these attack vectors implies a specific mechanism or characteristic of mobile networks that can be generalized across multiple different mobile generations. Furthermore, we distinguish different types of messages and features that can be exploited for an attack vector.

Feature. For each general attack, a specific *feature* defines the introduction point for the bidding-down attack. All features have in common that they are related to the connection establishment and the negotiation of the `UE Security Capabilities`. Interfering with these mechanisms might enable an attacker to impact the overall security of the connection. In some cases, the feature is generation-specific. In other cases, a mechanism is present across multiple generations (denoted as **G**).

Spec. The specification is the starting point for our analyses. More precisely, we inspect the characteristics of the attack vector and feature for each mobile generation and interpret the potential for a bidding-down related security

risk. In some cases, the specification provides a detailed and unambiguous documentation of requirements ✔. In these cases, we only conduct further tests if related experiments indicate their relevance. In cases where the specification leaves room for speculation ✖, we verify the security of specific implementations.

UE, Networks. For each individual feature and generation in our attack classification, we decide whether it is reasonable and possible to implement a test case. We test the radio connection from both possible directions. In the case of the UE, we test incoming messages from the network side and analyze its reaction. In case of the network, we send critical messages from the UE and analyze the network's reaction. The results documented in the *UE* and *Networks* columns summarize the results of the each set of tests. More precisely, we document vulnerabilities as ● in cases where at least one of the tested systems yielded a test failure. We document successful tests as ○ in case *all* tested devices exposed secure behavior. Settings in which a technical limitation prohibited us from testing or if the test was not applicable to the particular test component are noted as ━.

3.2. Intra-Generation

An intra-generation bidding-down attack allows an attacker to bid down a security feature *within* the same generation. To analyze the feasibility of intra-generation attacks, we classify five different attack vectors (cf. Table 1) and introduce their specific features.

3.2.1. UE Security Capabilities. The UE uses the `UE Security Capabilities` to signal supported algorithms for ciphering and integrity protection, and the core network then chooses an algorithm based on that list. The capabilities are transmitted without protection if no security context is established, which makes tampering protection essential. Avoiding and detecting manipulation is particularly relevant in cases where the attacker removes all except for the null algorithms that would result in plaintext transmissions without integrity protection. Further, while the non-null algorithms in 4G and 5G are currently considered secure, they may be compromised in the future, and thus an attacker should not be able to bid down the capabilities in order to enforce the use of insecure algorithms.

Invalid UE Security Capabilities: 4G+5G SA/NSA. The core network is required to reject incoming security capabilities that are invalid, i. e., if they do not contain all mandatory algorithms or if the information element is incorrect (wrong length or syntax). While the specification is clear about the handling of invalid `UE Security Capabilities` in 4G and 5G, it *lacks* a description for the 5G NSA case. As a result, the behavior of the core network solely depends on the implementation of the vendors.

Vulnerable Vendor Implementation. If the vendor's implementation does not reject 5G NSA `UE Security Capabilities`, this can open doors for bidding-down attacks on the 5G NSA connection.

Replay of UE Security Capabilities: 4G+5G SA/NSA. An additional layer of protection is provided by the replay of the `UE Security Capabilities` from the core network back to the UE with applied integrity protection. The verification of the replayed capabilities is the only mechanism where the UE can detect manipulation of its capabilities independently from the network. The importance of the UE checking the replayed `UE Security Capabilities` is particularly important in the 5G NSA case, where the specification includes no mechanism for the core network to detect invalid capabilities.

Discrepancies across Connections. The 5G NSA connection does not provide the same security mechanisms as 5G SA and lacks a detection mechanism for invalid capabilities. Consequently, the same level of security cannot be assumed for NSA versus SA connections. This discrepancy arises from a blind spot in the specification.

3.2.2. Network Capabilities. Current security features in the 5G standard might get compromised in the future and will be replaced by more secure versions. The typical case would be a broken cryptographic algorithm. The 5G standard introduces a new feature that allows the core network to prohibit the UE the use of those compromised security features.

ABBA Parameter: 5G SA. The Anti-Bidding down Between Architectures (ABBA) parameter is used to indicate security features that became insecure over time. The ABBA parameter is sent unprotected from the network to the UE. However, it is guarded against manipulation, as it is one of the input parameters of the initial AKA protocol.

ABBA Parameter. The ABBA parameter is set by the network. Despite being used as an input to the AKA, the UE is responsible for enforcing the policy of the parameter. Consequently, the network can suggest a secure connection but the UE might ignore this input.

3.2.3. Initial NAS Message Protection. The `Initial NAS Message` initiates the establishment of a connection between the UE and the core network. In 4G, this is commonly the `Attach Request` and in 5G the `Registration Request`. These messages are usually sent prior to the security context establishment and are not ciphered or integrity protected. Besides the `UE Security Capabilities`, the `Initial NAS Message` contains additional parameters, some of which also have security implications. The 4G and 5G specifications include different mechanisms to counteract tampering with the `Initial NAS Message`.

TABLE 1. OVERVIEW OF BIDDING-DOWN ATTACKS AND MITIGATION.
● VULNERABLE, ○ NOT VULNERABLE, ━ TEST CASE NOT APPLICABLE, ✔ SPECIFICATION COMPLETE ,✖ SPECIFICATION CONTAINS SECURITY ISSUES

Class	Attack Vector	Feature	G	Spec.	UE	Networks
Intra-Generation	UE Security Capabilities 3.2.1	Handling Invalid Security Capabilities	5G	✔	○	●
			4G	✔	○	○
			5G NSA	✖	●	●
		Replay of Security Caps.	5G	✔	○	○
			4G	✔	○	○
			5G NSA	✔	●	●
	Network Capabilities 3.2.2	ABBA Parameter	5G	✔	○	━
	Initial NAS Message Protection 3.2.3	Retransmission of Initial NAS Message	5G	✔	○	○
		$Hash_{MME}$	4G	✔	●	●
	Identity Bidding-Down 3.2.4	SUPI Encryption	5G	✔	●	●
		IMEI Identity Request	5G	✔	●	━
			4G	✔	●	━
	Replay Protection 3.2.5	NAS Count	4G	✔	●	●
			5G	✔	●	●
Inter-Generation	DoS / Downgrade 3.3.1	NAS Reject Messages	5G	✖	●	━
			4G	✖	●	━
	Redirections 3.3.2	RRC Release with Redirection	5G → 4G	✔	○	━
			4G → 3G	✖	●	━
			4G → 2G	✔	●	●
			3G → 2G	✖	━	━

Retransmission of Initial NAS Message: 5G SA. After the security context is established, the UE must retransmit the `Initial NAS Message`, which was previously sent unprotected [1, 5.4.2.3]. The network must then use the retransmitted `Initial NAS Message` instead of the earlier unprotected version. This ensures that the network does not process manipulated parameters included in the `Initial NAS Message` for following procedures.

$Hash_{MME}$: 4G. After the core network receives the `Initial NAS Message` from the UE, it calculates a hash ($Hash_{MME}$) [2, 8.2.20.5] of the message and forwards it with applied integrity protection to the UE. The UE then independently calculates a hash of its `Initial NAS Message` and compares it with the received $Hash_{MME}$. If the two hashes do not match, the UE retransmits its `Initial NAS Message` back in a ciphered and integrity-protected transmission. From this point, the core network must only process the contents from the retransmitted version of the message. It is worth noting that the specification explicitly states that the UE should not terminate the connection if the hashes do not match due to the fact that the included `UE Security Capabilities` have already been checked for tampering before. We discuss this characteristic further in Section 6.

Initial NAS Message. The possibility to bypass the protection of the `Initial NAS Message` depends on the implementation. If the potential victim connects to a vulnerable network, a bidding-down is possible.

3.2.4. Identity Bidding-Down. The 4G standard offers no identity protection as the International Mobile Subscriber Identity (IMSI) can be requested in cleartext before authentication. Victims can be identified and located in the network using IMSI catching techniques. With 5G, new security features were introduced in order to defeat IMSI catchers and protect the identity of the users.

Subscription Permanent Identifier (SUPI) Encryption: 5G SA. The SUPI is the permanent identifier of the UE and can be encrypted to conceal the identity of the UE. This is realized by providing the Universal Subscriber Identity Module (USIM) card with the public key of the home network, which is then used for the encryption of the SUPI. The encrypted SUPI is called SUCI. The feature is optional and requires support from the USIM card, the UE, and the network. In case one of the three mentioned instances does not support the SUPI encryption, the identifier is transmitted in the cleartext.

Deployment of SUPI encryption. The specification does not guarantee identity protection, as the deployment of the SUCI feature is optional and additionally requires support from the USIM card. Without SUPI encryption, 5G suffers from the same bidding-down risks as 4G.

Pre-authenticated International Mobile Station Equipment Identity (IMEI) Identity Requests: 4G+5G SA. An identity request is sent from the network to the UE to obtain a chosen identity, which is usually the SUCI in 5G or the IMSI in 4G. However, the network may additionally request the IMEI of the UE instead. In 4G and 5G, the UE is not allowed to expose the IMEI to a pre-authenticated `Identity Request`.

3.2.5. Replay Protection. Replay protection is applied to all NAS messages exchanged after establishing the security context and prevents the UE or network from accepting messages that were intercepted and re-sent by an adversary to the corresponding receiver. Not rejecting replayed messages can create different attack vectors for bidding-down attacks.

NAS Count: 4G, 5G SA. The NAS count is a sequence number that is sent with all ciphered and integrity-protected messages. Further, the count is used as an input parameter to generate and verify the Message Authentication Code (MAC) for integrity protection. The UE and the network increment a corresponding count value for each message sent and received. For example, an attacker can re-assign old temporary identifiers to the UE by replaying the corresponding messages. Reusing temporary identifiers bear identity and privacy risks [14].

Improper Check of NAS Count. Without a correct NAS count implementation, replaying messages becomes possible. This enables an adversary to inject previously sent messages with potentially insecure `UE Security Capabilities`.

3.3. Inter-Generation Downgrade

In an inter-generation attack, the connection is downgraded from a newer to an older mobile network generation. We define two types of attack vectors and discuss their individual features to analyze the feasibility of these attacks.

3.3.1. DoS / Downgrade. A DoS is the entry point for every downgrade attack. An attacker aims to make the UE believe that access to the selected network is denied, which can force the UE to re-select older and insecure network generations. There are different mechanisms in 4G and 5G which can be exploited by an adversary to execute downgrade attacks against UEs. A DoS does not necessarily lead to a downgrade, e. g., a UE can also refuse the service completely without switching to an older generation.

NAS Reject Messages: 4G, 5G SA. Reject messages on the NAS layer are used to deny the UE access to network services in case the NAS attach is not accepted by the network. These messages always include a specific cause that informs the UE about how to behave when rejected by the network. The UE is allowed to *accept* the reject messages unprotected if it receives them before the establishment of the security context.

High-Impact Reject Causes. Some NAS reject causes instruct a UE to completely disable support for the current network generation. These reject causes can be exploited by an attacker to force the UE to downgrade to a lower and more insecure network generation.

3.3.2. Redirection. Base stations use a redirection mechanism to redirect a UE into a cell in another frequency or network generation. Typical use cases are load balancing and fallbacks to 2G/3G networks for phone calls or SMS, e. g., in case Voice over LTE is not available. In contrast to downgrade attacks, redirections target a specific fake base station and thus increase the success chances.

RRC Release with Redirection: 5G SA, 4G, 3G. The base station uses the RRC Release procedure to release the radio connection with a UE, e. g., if the UE switches into idle mode. In addition, the RRC release can be used to instruct the UE to re-select a cell in another frequency or an older generation network. The RRC release procedure is a viable attack vector for downgrade attacks, as the message can be sent before the security on the radio connection has been activated. We discuss the mechanisms of individual generations as follows.

5G → 4G. In 5G, the UE has to ignore the redirection field in a pre-authenticated RRC Release message in any case. Further, only a redirection to 4G is possible.

4G → 3G. The 3GPP specifications do not provide any countermeasures to prevent a pre-authenticated RRC redirection from 4G to 3G.

4G → 2G. Until the 3GPP release 15.3.0 the specification did not include any prevention mechanism against pre-authenticated redirections from 4G → 2G. However, since release 15.3.0, the core network can explicitly forbid the UE to accept an unauthenticated RRC Connection Release message with a redirection field in 4G by using an optional NAS flag during the attach procedure. If the flag is not used, an insecure redirection from 4G to 2G is always possible.

3G → 2G. The 3GPP specifications do not provide any countermeasures to prevent a pre-authenticated RRC redirection from 3G to 2G.

Redirection. While 5G SA does not allow insecure redirections by default, 4G networks require additional operational steps to provide protection. If these mitigations are not correctly deployed, an attacker can perform enhanced downgrade attacks by redirecting a UE to the exact frequency of a fake base station.

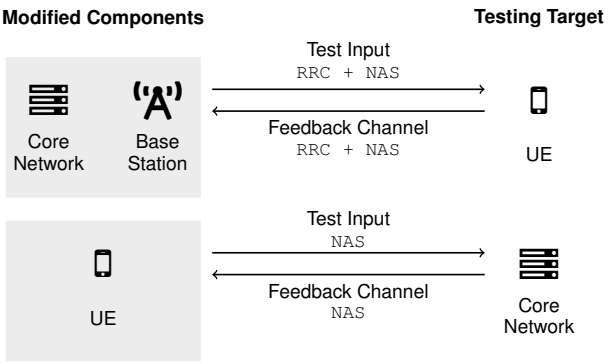

Figure 2. General overview of the testing setup for UE and network. For the UE tests, we modify the core network and the base station and perform our analysis on the RRC and NAS layers. Further, we perform the network tests with a modified UE component and then analyze the message exchange on the NAS layer.

4. Experiments and Results

Based on the observations of our systematic classification of bidding-down attacks, we define test cases that enable us to analyze the security of networks (cf. Table 2) and commercial UEs (cf. Table 3) regarding open attack vectors. While we apply a *full* set of test cases to the systems under test (cf. Appendix, Tables 6 and 7), we focus our documentation and results only on those tests in which we observed a test failure, i. e., identified an open attack vector. We perform a total of 49 tests, including 34 for the UEs and 15 for the networks. We find vulnerabilities in 17 tests for the UEs and 12 tests for the networks. In the following, we describe the experimental setup used for all tests and describe the adjustments in place for individual experiments. We then document the network (§4.2) and UE (§4.3) tests and their results.

4.1. Experimental Setup

Our experimental setup involves all components of a full mobile network (cf. Figure 2). As we either test the behavior of the UE or the core network, we always define a test target (system under test) and control the complementary component to apply test cases. We document the different setups as follows.

General Setup. Our testbed consists of a UE component, a base station, and a core network component. The UE and core network are either represented through an open source software implementation, or we refer to commercial devices/networks. In case we make use of a base station, we use the USRP X300 and B210 software-defined radio models for the radio connection.

UE Testing. When analyzing the behavior of a UE, we control the core network component to trigger certain states and behaviors. To this end, we use a modified version of the 4G/5G core network implementation `open5gs` [28] and the eNB/gNB implementation `srsENB`[1], which is provided by the `srsRAN` [10] open-source software radio suite. This setup of a core and base station component enables us to control the network connection of the UE, i. e., we can use it to analyze the behavior of commercial UEs. All UE tests were conducted isolated inside a Faraday cage.

Network Testing. When analyzing the behavior of the core networks in our lab setup, we control the UE component and can directly interfere with the functions of the core network. Consequently, it is not necessary to use a physical radio layer connection as we can directly connect to the core network interfaces. To achieve this, we use a modified version of `CoreScope` [35], which is a testing tool that combines a 5G UE and gNB architecture and requires no additional radio front-end. For the public commercial network tests, we use the UE implementation `srsUE` provided by the `srsRAN` software suite and modify it depending on our needs.

Results Analysis. For deriving the test results, we manually inspect recordings of each test run. We use the PCAP traces to derive a success or failure result for the test case.

Testing Targets. For the analysis of UEs, we test seven different commercial phones that are equipped with baseband modems from five different vendors (cf. Table 5). All devices support the newest 5G standard[2] and receive the latest security updates.

For the network tests, we use four different core networks in our lab setup and further conduct experiments with three commercial and publicly available networks. The lab setup consist of the open-source implementations `open5gs` [28], `Openairinterface5GCN`[3] [29], `Free5GC`[3] [8] and a closed-source commercial solution. For the public networks, we are limited to 4G and 5G NSA, because no local provider has deployed 5G SA networks at the time of writing.

4.2. Network Experiments

In the network experiments, we test core network implementations in controlled lab setups as well as public networks. All test results involving a test failure and potential security threat are documented in Table 2; a full set of test cases is listed in Table 6 in the Appendix.

4.2.1. UE Security Capabilities. An adversary may attempt to manipulate the UEs security capabilities to bait the network into selecting weak algorithms from the invalidated capability set.

5G SA: TC1, TC2, TC3. We send a `Registration Request` with invalid `UE Security Capabilities`

1. For a subset of test cases, we exchange the `srsENB` with the eNB/gNB provided by an `Amarisoft Callbox` [3] due to technical limitations.

2. Due to a vendor lock, the Huawei P40 Lite 5G was not able to connect to our 5G testbed, although it theoretically supports the standard.

3. These core networks are excluded from the 4G/5G NSA tests as they only provide a 5G SA implementation

TABLE 2. NETWORK TEST RESULTS.
○ TEST SUCCESS, ● TEST FAILURE, ━ TEST CASE NOT APPLICABLE, ✔ SPECIFICATION COMPLETE ,✖ SPECIFICATION CONTAINS SECURITY ISSUES

Mitigation	G	TC	Spec.	Open5GS	OAI 5G CN	Free5GC	Commercial Core	Pub-1	Pub-2	Pub-3
UE Sec. Cap.	5G SA	1	✔	○	●	●	●	━	━	━
		2	✔	○	●	●	●	━	━	━
		3	✔	○	●	●	●	━	━	━
	5G NSA	4	✖	●	●	●	●	●	●	●
		5	✖	●	●	●	●	●	●	●
		6	✖	●	●	●	●	●	●	●
Initial NAS Msg. Prot.	4G	7	✔	○	━	━	○	●	●	●
Identity Bidding Down	5G SA	8	✔	●	○	○	○	━	━	━
Replay Protection	5G SA	9	✔	●	●	●	○	━	━	━
	4G	10	✔	●	━	━	○	○	○	○
Redirection	4G	11	✔	━	━	━	●	●	●	●
		12	✔	●	━	━	●	●	●	●

to the core network. We then verify whether the core network accepts the capabilities and what algorithms were selected in the `Security Mode Command` message. Our permutations of invalid `UE Security Capabilities` involve settings that only support null algorithms (TC1), cover only non-mandatory algorithms (TC2), or do not support any algorithms at all (TC3). Three core networks *fail* these tests, i. e., we observe in all three test cases that the implementations fall back to null encryption and integrity.

Despite a clear indication through the specification, the majority of core networks fail the test cases and establish insecure connections. While similar findings have been made in 4G [5], the test results show that these security issues were also inherited by 5G SA networks.

5G NSA: TC4, TC5, TC6. For the 5G NSA tests, we send an `Attach Request` including invalid permutations of the `UE Additional Security Capabilities`. These capabilities are exclusively used in 5G NSA networks to negotiate the encryption algorithm between the UE and the secondary gNB. If the capabilities are accepted, the network chooses one algorithm from the capability set for the user plane data exchanged between UE and gNB.

Similar to the previous set of test cases, we send null (TC4), non-mandatory (TC5), or unsupported (TC6) algorithms. Our results show that *all* core networks in our lab setup fail the test cases and accept an insecure connection. We observe the same behavior for all *public* networks.

All open-source and public commercial networks share the same implementation flaws. The root cause for these security issues is an incomplete specification that does not address the handling of invalid `UE Additional Security Capabilities`.

4.2.2. Initial NAS Message Protection.

When the `Initial NAS Message` is sent before the security context establishment, it can be tampered with by an adversary.

TC7: $Hash_{MME}$ Protection. In 4G, the core network must actively use the $Hash_{MME}$ parameter to protect the `Initial NAS Message`. We perform the standard attach with a UE and check if the `Security Mode Command` sent by the network includes the $Hash_{MME}$. While the tested lab core networks make use of the $Hash_{MME}$, all tested public networks *fail* the test case.

The lack of $Hash_{MME}$ protection in public commercial networks is a threat to numerous real-world users, as it is currently the only countermeasure against manipulation attacks on the `Initial NAS Message` in 4G.

4.2.3. Identity Bidding-Down.

To protect the UE's identity, the core network must support the concealment of the UEs unique identifier by implementing SUPI encryption.

TC8: Support of SUPI Encryption. We send a `Registration Request` with an encrypted `SUCI` and the applied scheme to the core network. For one core network the test case *fails*, as it only supports clear SUPI transmissions.

If the encryption schemes for the SUCI are not supported by the network, the SUPI will be transmitted in clear text similar to the IMSI in 4G. This opens the door for tracking and identification attacks known from the context of 4G.

4.2.4. Replay Protection.

To ensure that replay attacks are mitigated, we investigate if the networks implement measures to detect replayed NAS messages. To execute our test case, we choose messages that always trigger a response from the network and verify if the network responds to the subsequent replay of those messages.

TC9: PDU Session Establishment Request. In 5G SA, we replay a `PDU Session Establishment Request` message multiple times. If the network does not check the count value of each replayed message, it will send a response to each request message. Three out of four tested 5G SA core networks do not implement replay protection properly.

TC10: Replay of PDN Connectivity Request. Analog to **TC9**, we perform a replay of a `PDN Connectivity Request` message to the 4G core networks and check if we get a response for every request. Our results show one core network that *fails* the test.

4.2.5. Redirection. In contrast to 5G SA, unauthenticated UE redirection to insecure 2G networks is not prohibited by default in 4G, but can be enabled by the operator.

TC11, TC12: Presence of Policy Bit. We attach to the networks and check if the `Attach Accept` message includes the `Network Policy` information element with the `Unsecured redirection to GERAN not allowed` bit [2, 9.9.3.52] set to `true`. All core networks under test *fail* this test case and enable redirection. We repeat the same test with Voice over LTE disabled, as this would require a UE to fall back to a 2G/3G connection for phone calls. Again, all tested networks *fail* the test.

In our experiments, no network prohibits a redirection to 2G, which enables an attacker to navigate the UE to the exact frequency of a 2G fake base station. Multiple known security flaws in 2G render this a severe vulnerability.

Conclusion Network Experiments. The results of our network experiments are devastating. In total, we found security issues in five different mitigation techniques that affect both open-source networks and publicly available commercial networks. This includes 5G SA and NSA connections, i. e., the latest and seemingly most secure mobile generation. The result is surprising, as in most cases the specification suggests secure behavior.

4.3. UE Experiments

We analyze the security of seven commercial UEs and document the analysis results in Table 3; the full set of applied test cases is listed in Table 6 in the Appendix.

4.3.1. UE Security Capabilities. On the UE side, we focus on the replay of the `UE Additional Security Capabilities` and investigate if each individual UE model detects the manipulation.

TC1, TC2, TC3, TC4: Additional Security Capability Experiments. In the first step, we replay tampered `UE Additional Security Capabilities` (TC1) in the `Security Mode Command` message. Our experiments show two UEs that *fail* the test case and do not verify the replayed message in the `Security Mode Reject`. They continue the now insecure connection establishment.

We repeat the same test *with* $Hash_{MME}$ (TC2) to check whether the $Hash_{MME}$ triggers the UE to ignore the replay, as it should provide protection for the complete `Initial NAS Message`. Four devices *fail* the test case and do not verify the replayed message.

In the next step, we replay security capabilities that were not initially sent in the `Attach Request` (e. g., due to disabled 5G NSA). The UE should reject the `Security Mode Command`, as it contains unknown credentials. *All* devices in our set *fail* this test case.

Finally, we check the behavior if the network does not replay the `UE Additional Security Capabilities` at all while we still instruct the UE to establish a connection with the gNB. As this behaviour is not specified, the UE should not accept a radio connection to the gNB because the network will use an encryption algorithm from a capability set that the UE did not verify. Again, *all* devices *fail* the test case.

4.3.2. Initial NAS Message Protection. In addition to the network mechanisms, the UE is also responsible for a correct `Initial NAS Message` Protection including a verification of the $Hash_{MME}$.

TC5: Verification of $Hash_{MME}$. We modify the core network to include an invalid $Hash_{MME}$ with the value zero in the `Security Mode Command` and send it to the UE. A UE with correct implementation should verify and then transmit its `Initial NAS Message` in the `Security Mode Complete`. Two devices *fail* this test and ignore the invalid $Hash_{MME}$ value.

The UE verifying replayed `UE Security Capabilities` (TC1-TC4) or the $Hash_{MME}$ (TC5) is the last checkpoint to prevent against a bidding-down attack. Unfortunately, for the majority of devices and test cases, implementation flaws prevent the UE from identifying malicious behavior.

4.3.3. Identity Bidding-Down. Even if the USIM card and the core network support SUPI encryption, the identifier is transmitted in clear text if the UE does not implement the encryption.

TC6: SUPI Encryption Support. In this test case the USIM card and the core network support SUPI encryption. To verify the enabled encryption, we inspect the `Registration Request`. One out of seven devices *fails* the test and attaches with a cleartext SUPI identifier.

TC7, TC8: Unauthenticated IMEI Identity Request. To verify if the UEs expose their IMEI to unauthenticated requests by an adversary, we respond to the `Registration Request` with a `Identity Request` with the identity type set to `IMEI`. Two UEs *fail* the test and respond with an `Identity Response` containing their IMEI to the unauthenticated requests in 4G and 5G.

Despite being known for several years [26], identity bidding-down attacks remain a problem in 4G and 5G. We find security flaws in the current 5G flagship UEs that break newly introduced security features in the latest 5G standard. These vulnerabilities have severe consequences for the privacy of users.

4.3.4. Replay Protection. Replay protection is a mitigation that must be implemented correctly on both endpoints of the connection. To verify the side of the UE, we repeat the network test cases TC9 and TC10.

TC9, TC10: Replay of Security Mode Command. To audit the replay protection of the individual UEs, we replay a previously accepted `Security Mode Command` message to the UE. Our experiments show three 5G devices and four 4G devices that *fail* the test and respond to a replayed message with a `Security Mode Complete`.

Without replay protection in place, the UE is vulnerable to incoming messages that can cause a bidding-down. With

TABLE 3. UE TEST RESULTS.
○ TEST SUCCESS, ● TEST FAILURE, ━ TEST CASE NOT APPLICABLE, ✔ SPECIFICATION COMPLETE ,✖ SPECIFICATION CONTAINS SECURITY ISSUES

Mitigation	G	TC	Spec.	OP 10 Pro 5G	OP 8	P40 lite 5G	S22	S21	A22	F50+
UE Sec. Caps.	5G NSA	1	✔	○	○	○	●	●	○	○
		2	✔	●	●	○	●	●	○	○
		3	✖	●	●	●	●	●	●	●
		4	✖	●	●	●	●	●	●	●
Initial Message Prot.	4G	5	✔	○	○	●	●	●	○	●
Identity Bidding-Down	5G SA	6	✔	○	○	━	○	○	○	●
	5G SA	7	✔	○	○	━	●	●	○	○
	4G	8	✔	○	○	○	●	●	○	○
Replay Protection	5G SA	9	✔	○	○	━	●	●	●	○
	4G	10	✔	○	○	○	●	●	●	●
Redirection	4G	11	✔	○	○	○	●	●	○	○
Downgrade	5G SA	12	✖	●	●	━	●	●	●	●
		13	✖	●	●	━	●	●	●	●
		14	✖	○	○	●	●	○	●	●
	4G	15	✖	●	●	●	●	●	●	●
		16	✖	●	●	●	○	○	●	○
		17	✖	○	○	●	●	●	●	●

the problem being split across the network and the UE, a connection can only be considered secure if both sides provide a correct implementation. Prior work demonstrates how this attack vector is a stepping-stone to tracking attacks [17], [15].

4.3.5. Redirection. To protect against redirection on the UE side, we verify if devices apply the security policy and reject an unauthenticated redirection to 2G.

TC11: Unauthenticated Redirection to 2G with Policy Bit. In our core network, we explicitly set the `Network Policy` bit in the `Attach Accept` to prohibit an unauthenticated redirection through a `RRC Connection Release`. We then lure the UE into connecting to a 4G fake base station and immediately send an unauthenticated `RRC Connection Release` with redirection to a 2G fake base station we operate. Two tested UEs *fail* the test and accepted the redirection.

Although the network has correctly deployed the `Network Policy`, the implementation flaw in the vulnerable UEs completely nullifies the protection and enables redirection attacks.

4.3.6. Downgrade. In the context of downgrade attacks, we focus on various reject causes that have not been discussed in the context of 5G and those that are uncovered for 4G setups.

TC12, TC13, TC14: Registration Reject. In our lab setup, we operate a legitimate 5G and 4G network; the UE selects the 5G cell as the highest available generation. We then run a 5G fake base station and attempt a registration procedure to lure the UE into a new connection. After our fake base station receives the `Registration Request`, it immediately replies with a `Registration Reject` including a specific `Reject Cause`. If the UE ignores all 5G networks after the reject and re-selects the 4G cell, we classify that specific cause as viable for a downgrade attack. Using the cause `27: N1 Mode Not Allowed` (TC12), we are able to downgrade all tested UEs from 5G to 4G. This cause instructs the UE to disable its capabilities for 5G SA altogether [1, 5.5.1.2.5]. The reject cause `7: 5GS Services Not Allowed` (TC13) triggers a downgrade in two UEs and causes a DoS in three UE models. With the cause `11: PLMN Not Allowed` (TC14), we cause one DoS and one downgrade.

TC15, TC16, TC17: Tracking Area Update (TAU) Reject. We use a similar setup for 4G downgrades by deploying a legitimate 4G network, a 4G fake base station, and a 2G fake base station. After connecting to the legitimate 4G network, the UEs are lured into the 4G fake base station and send `Tracking Area Update Request` message. The fake base station responds with a `Tracking Area Update Reject` message and includes a specific `Reject Cause`. We then examine if the UE downgrades to the 2G fake base station. All UEs downgrade to the 2G network if rejected with the cause `42: Severe network failure` (TC15). This cause explicitly instructs the UE to ignore all 4G networks of the current Public Land Mobile Network (PLMN) [2, 5.5.1.3.5] and was not tested in previous work. In addition, four UEs downgraded to the 2G network if they are rejected with cause `7: EPS services not allowed` (TC16). Further, we test cause `8: EPS services and non-EPS services not allowed` (TC17), which causes a DoS

TABLE 4. UEs ANALYZED IN THE BIDDING-DOWN CASE STUDIES

Phone	Baseband	ATK1	ATK2
Samsung S22	Exynos	✔	✔
Samsung S21	Exynos	✔	✔
One Plus 8	Qualcomm	✔	✖
One Plus 10 Pro	Qualcomm	✔	✖
Huawei P40 Lite 5G	HiSilicon	✔	✖
Hisense F50+	UNISOC	✔	✖
Samsung A22 5G	Mediatek	✔	✖

in five UEs.

We show that well-known downgrades also affect the latest 5G standard, as it was possible to downgrade all tested UEs to 5G, bypassing all of the latest security features. Furthermore, we identify a new reject cause that enables a downgrade from 4G to a lower generation. They are more successful than causes of prior work [34], [21], [16].

Conclusion UE Experiments. The security of a device highly depends on the specific implementation of a vendor. Consequently, we see mixed results for test cases in which the specification is complete, e. g., we observe a tendency of test failures for individual vendors that is not visible to others. In cases where the specification contains security issues, the majority of devices fail the test cases. This has severe consequences, as we find various individual attack vectors that can be exploited to harm the security of a connection.

Furthermore, we observe that connection security is a two-sided problem. Given a secure network, implementation flaws in the UE still enable an adversary to conduct bidding-down attacks. This adds complexity to the problem statement, as the diversity of UEs leads to more differences across devices.

5. Case Studies

While the targeted test cases of Section 3 indicate the existence of attack vectors in UEs and networks, a full bidding-down attack can be more complex. To demonstrate the feasibility of *full attacks*, we test 7 UEs (cf. Table 4) against two specific bidding-down attacks, i. e., a Downgrade Dance (§5.1, **ATK1**), and a NEA0 Bidding-Down (§5.2, **ATK2**).

5.1. Downgrade Dance 5G → 2G

The attack aims to *downgrade* a victim from a seemingly secure 5G SA network to 2G. To achieve this, the adversary conducts step-by-step exploits of the pre-authentication phase of all generations (§3.3.1, §4.3.6). When reaching the 2G connection, follow-up attacks enable eavesdropping, interceptions, and localization.

5.1.1. Prerequisites and Attacker Model. We assume that the victim is registered in the legitimate 5G SA network and has an active radio connection with the gNB. There are legitimate networks of all generations except 3G, which is the case in most European countries. The attacker operates a fake base station with a higher signal strength for every generation mimicking the legitimate network by broadcasting the same identity (PLMN).

In the lab setup, we create the conditions by equipping the victim's UE with a programmed USIM card and let it connect to the legitimate network (PLMN: 00101). Further, we operate multiple fake base stations with different software and hardware solutions. To simulate the attack, we manipulate the gain of our fake base station and the legitimate 5G gNB. In reality, the attacker can use a jammer to disturb the legitimate transmission and force the UE to another 5G cell.

5.1.2. Attack Procedure. We describe the attack procedure step by step. An illustration of the protocol flow can be found in the Appendix in Figure 3. While the victim connects to the legitimate 5G SA, we trigger a cell re-selection to the 5G SA fake base station by increasing its signal gain. This involves sending a `NAS Registration Request`, which is answered with a `NAS Registration Reject` with cause 27. This causes the UE to disable its 5G capabilities [1, 5.5.1.2.5], and it eventually searches for new cells in 4G. Repeating the same procedure, we can downgrade the UE step-by-step to 2G.

Our proof-of-concept demonstrates a full downgrade-dance in a controlled lab environment. In a real-world scenario, an attacker can refer to jamming attacks to increase the chances of the victim connecting to the fake base station. Furthermore, it is possible to combine the downgrade attack with the RRC redirection attacks described in Section 3.3.2.

5.2. 5G NSA NEA0 Bidding-Down Attack

To conduct a full bidding-down to null encryption, we must combine exploits for the network and the UE. On the network side, a UE with invalid `UE Additional Security Capabilities` must not be rejected. At the same time, the $Hash_{MME}$ and the replayed `UE Additional Security Capabilities` are not checked in vulnerable devices. To demonstrate the feasibility of the attack, we combine all attack vectors and aim for an established connection with null encryption.

5.2.1. Prerequisites and Attacker Model. We assume that the UE is not attached nor has an active radio connection to the legitimate network. The attack requires the adversary to manipulate messages between the UE and the eNB, which can be achieved by deploying a MitM attacker between the victim and the network.

5.2.2. Attack Procedure. The simplified attack is illustrated in the Appendix in Figure 8. In a NSA deployment, the UE starts by sending an Attach Request, which is intercepted by the MitM attacker to manipulate the included `UE Additional Security Capabilities` to only support null ciphering (NEA0). The network receives,

stores, and then replays the `UE Additional Security Capabilities` back to the UE in the *integrity protected* `NAS Security Mode Command` message. If the capabilities are not checked by the UE, it continues with a `Security Mode Complete`. In addition, the UE does not retransmit the `Attach Request` as the $Hash_{MME}$ is not verified correctly.

In the next phase, the Mobility Management Entity (MME) informs the target gNB about `UE Additional Security Capabilities` of the UE via the S1AP and X2AP interface. As the only available ciphering algorithm now left in the 5G capability set is NEA0, the eNB instructs the UE to establish an unencrypted radio connection to the secondary gNB via the `RRC Connection Reconfiguration` message. The UE acknowledges the establishment of the unencrypted radio connection via the RRC Reconfiguration Complete message.

6. Discussion

Despite being known for years, the threat of bidding-down attacks remains very real even for the latest flagship phones and multiple deployed networks. Being able to conduct a full downgrade from 5G to 2G is a devastating finding regarding our latest mobile network generation. Our experiments emphasize the complexity of this problem by pointing out various attack vectors for different types of bidding-down attacks. They all have in common that they are caused by implementation flaws, sometimes triggered through an incomplete specification. In the following, we discuss the security implications of our findings and suggest improvements that will contribute to the security of millions of users.

6.1. Complexity

Due to new requirements and features, the complexity of security protocols increases further, affecting the likelihood of implementation flaws. For example, the security establishment for 5G SA connections includes handling the `UE Security Capabilities` of multiple parties, which we have shown to be flawed on both the network and UE side. *To prevent under-specifying or even falsely specifying the security protocol, we suggest that protocols are verified before the specification, e. g., with a protocol verification tool like Tamarin [25]. Implementation flaws can only be prevented through detailed and systematic testing. Such verification helps to provide a better foundation, but it is not a replacement for security-focused implementation testing.*

6.2. Improvements

In the following, we discuss potential improvements to the specification, implementation, and operational aspects.

6.2.1. Specification. On the one side, the 5G security specification requires that bidding-down attacks are no longer possible. In contrast, other parts of the specification mandate that the network is operational and therefore demand a mechanism to reject a UE with specific causes. For example, the cause `N1 Mode Not allowed` switches 5G off because the subscription or operator policy does not allow the UE to operate 5G mode. However, an attacker can also exploit this cause to perform a downgrade. *This underlying conflict between the security and operational requirements needs to be resolved to make 5G secure.*

We discuss further details of the specification as follows:

- **High-Impact Reject Causes.** We suggest that NAS reject messages with the potential to disable capabilities shall only be accepted if the network authenticates them. Although this requires the network and UE to run through an additional authentication procedure, we gain a significant advantage in the protection against bidding-down attacks.
- **RRC Redirection Mitigation Missing.** In the latest release, 4G (optionally) prevents 4G $\rightarrow$ 2G RRC redirection attacks. However, the downgrades from 4G $\rightarrow$ 3G and from 3G $\rightarrow$ 2G are still possible. Consequently, an attacker can circumvent the Radio Resource Control (RRC) (4G $\rightarrow$ 2G) redirection prevention by using an extra step over 3G. Therefore, we suggest that the 4G specification implements a similar prevention mechanism to prevent attacks from 4G $\rightarrow$ 3G.
- **Rejection HashMME mismatch.** The UE does not reject the connection establishment, if $Hash_{MME}$ and $Hash_{UE}$ do not match. The specification argues that this is obsolete, as the UE has already checked the `UE Security Capabilities` before. However, a mismatch of both hash values is a clear sign of active manipulation. Further, the `Initial NAS Message` does contain other security-relevant parameters. Therefore, we suggest that the UE should reject the connection immediately if the hashes mismatch.
- **UE Additional Security Capabilities in ENDC.** The exchange of `UE Security Capabilities` and the security algorithm negotiation are not securely specified for the ENDC case. Further, releases must determine how the MME shall handle invalid `UE Security Capabilities` and how the UE shall behave in case of a mismatch in the replayed `UE Additional Security Capabilities`. This needs to be done before the actual 5G connection is built up.

6.2.2. Implementation. We found no operator using the flag to prevent redirections from 4G to 2G. Further, those operators did not use pre-authentication redirection from 4G to 2G. The first fact puts users at unnecessary risk of redirection attacks. The second indicates that they can effortlessly enable this feature without breaking any functionality. We highly recommend operators use the flag to protect their users from threatening redirection attacks.

6.2.3. Operational. Before a phone is launched to the market, it is certified regarding its radio and protocol con-

formance [9]. Those UE conformance tests lack a security focus. In contrast, the GSMA NESAS scheme solely focuses on the security of network components [12]. Only if *both* sides (UE and network) are sufficiently tested prior to their launch, we can increase the security of the system as a whole. Therefore, we plead to perform extensive UE security testing. The tests derived in this paper are a starting point to *extend* the baseline security of existing schemes.

7. Related Work

In the context of this work, we are mainly interested in prior work that addresses bidding-down attacks caused by specification and implementation flaws and in approaches for systematic UE and network testing.

7.1. Bidding-Down Specification Flaws

Past work has demonstrated that bidding-down attacks exploit mechanisms provided by the 3GPP specifications. Specification flaws are particularly relevant, as they affect *all* network equipment that strictly follows the specification in their implementation. Shaik et al. [34] and Jover [21] demonstrated downgrade attacks on 4G using pre-authenticated NAS reject messages. Both use a specific reject cause to disable 4G services and force the UE into a lower-generation network. In our experiments, we extend this by considering *all* existing reject causes and present multiple additional reject causes that an attacker can use to downgrade a UE to 3G or 2G networks. Further, previous work [22] indicated that security issues regarding pre-authenticated NAS messages might be inherited to the 5G standard. Our results show that downgrade attacks triggered by pre-authenticated NAS reject messages are possible in 5G networks. We present a proof-of-concept for a 5G downgrade attack and demonstrate a full downgrade dance from 5G down to 2G networks. The underlying problem of unauthenticated pre-authenticated traffic can be addressed by signing broadcast messages as suggested by Hussain et al. [19]. However, it is not foreseeable that such a feature will be integrated into the specification soon. Huang [16] presented another variant of a 4G downgrade attack using RRC redirections that enable an attacker to redirect a victim from 4G to 2G networks. Meanwhile, newer specification releases introduced security mechanisms to mitigate unauthenticated redirections. We investigate the deployment of these mitigations in the commercial networks and show that operators do not apply these measures, resulting in RRC redirection attacks still being possible. Furthermore, we show that some devices do not even consider the flag and are still vulnerable despite the countermeasures. Hussain et al. [17], [18] and Tu et al. [36] proposed methods to analyze the 4G protocol and found multiple design flaws in the standard. We emphasize the importance of doing a security analysis of the specification in the context of bidding-down protection and show that vulnerabilities that have been known for many years in the older standards still apply to the latest generation 5G.

7.2. Bidding-Down Implementation Flaws

Attackers can exploit implementation flaws to forge different types of bidding-down or downgrade attacks. Rupprecht et al. [33] revealed an implementation flaw that caused UEs to accept null ciphering and integrity algorithms. Park et al. [31] presented similar findings in more recent phone models. The authors demonstrated how an attacker could exploit the vulnerabilities to bid down the encryption and eavesdrop on a victim's 4G communication. Our findings include implementation flaws that leave affected UEs vulnerable to 5G NSA encryption bidding-down attacks. Identity bidding-down vulnerabilities have been revealed [26], [31], where UEs responded to unauthenticated IMEI requests in 4G. However, as the 4G standard has no proper mitigation against IMSI catchers in the first place [30], [32], [27], [7], complete identity protection cannot be assured. The 5G standard attempted to counteract this issue by introducing SUPI encryption, which replaces the cleartext IMSI. Chlosta et al. [6] demonstrated that SUCI catcher attacks are still possible, although being less practicable and requiring far more effort than 4G IMSI catching techniques. We analyze the corresponding measures and find UEs revealing their IMEI in unauthenticated requests in 5G. Consequently, IMEI catchers can be used in 5G networks to identify users and bypass the protection provided by SUPI encryption. Further, one device did not implement SUPI encryption at all. Although bidding-down mitigations improved with the release of the latest 5G standard, our findings highlight the necessity for correct implementation to ensure that these countermeasures are applied accordingly.

7.3. Systematic UE and Network Testing

Many bidding-down mitigations require the participation of both the UE and the network in order to offer appropriate protection. Thus, it is essential to systematically test both components to assess their security. Park et al. [31] present a negative testing framework for 4G, supporting multiple test cases to discover implementation flaws in UEs equipped with different baseband chipsets. Palamà et al. [30] systematically analyzed the behavior of different UEs when being attacked by IMSI catchers. Chlosta et al. [5] tested commercial 4G networks and found that multiple operators deployed insecure configurations in their networks. Further, Kim et al. [23] tested different UEs and networks in their implementation of security procedures with a focus on the control plane. However, there is a lack of past work thoroughly analyzing bidding-down mitigations. Thus, we focus on systematically reviewing those security features in UEs and networks for 4G and 5G.

8. Conclusion

Bidding-down attacks are a persisting threat against mobile networks, as they enable an adversary to drastically lower the security of a connection. Although mitigations

against different types of attacks are specified for newer mobile generations, the sheer variety of attack vectors makes it difficult to fully avoid the threat. In this work, we introduced the first systematic classification of bidding-down attacks and identified their attack vectors. In extensive experiments, we analyze the security of numerous commercial phones and networks and assess their protection against bidding-down attacks. Our results reveal that flagship phones and commercial networks alike are vulnerable against *multiple* bidding-down attacks, including a full downgrade from 5G to 2G. Our findings emphasize the challenges of providing secure specifications and implementing them in our everyday devices. Through the responsible disclosure of our findings and a detailed discussion of potential security improvements, we hope to contribute to the long-term security of our mobile networks.

Appendix

In the following, we provide additional information regarding detailed protocol flows of bidding down attacks, the test cases, and device specifications.

Protocol Flows. To illustrate the attack procedures of our case studies, we document the protocol flows and the adversary's interaction in two diagrams. Figure 3 documents the steps necessary to downgrade a UE from one generation to an older one. By repeating these steps for multiple generations, it is possible to conduct a full downgrade from 5G to 2G. Figure 8 documents the protocol flow for the null-encryption bidding down. In this process, we combine exploits towards the network and the UE to establish a connection without any encryption enabled.

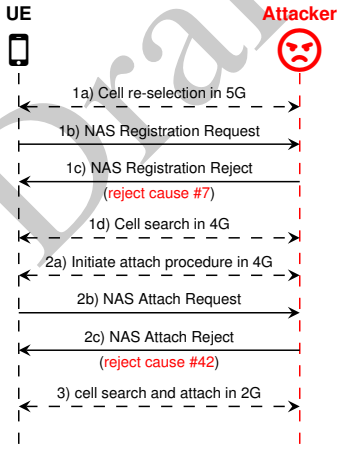

Figure 3. Protocol flow of downgrade dance from 5G to 2G. The attacker sequentially downgrades the victim from 5G to 4G and from 4G to 2G. For this, the attacker uses a fake base station for the corresponding generations and sends a NAS reject with reject causes that trigger the UE to downgrade to a lower generation.

UE Specification

In all UE experiments and in the case studies, we refer to a set of seven commercial phones. Table 5 provides an overview of the device models, their baseband vendors, and the model and version, respectively.

TABLE 5. SPECIFICATION OF UES.

Phone	Baseband Vendor	Model	Version
OnePlus 10 Pro 5G	Qualcomm	SM8450 (X60)	Q_V1_P14,Q_V1_P14
OnePlus 8	Qualcomm	SM8250 (X55)	MPSS.HI.2.0.c4l00028SDX55_RMTEFS_PACK1.375089.1.381005.3
Huawei P40 lite 5G	HiSilicon	Kirin 820	21C93B376S000C000,21C93B376S000C000
Samsung S22	Samsung	Exynos 2200	S901BXXU2AVG6
Samsung S21	Samsung	Exynos 2100	G991BXXU5CVG3
Samsung A22	Mediatek	MT6833	A226BXXS4AVD5
Hisense F50+	Unisoc	Tiger T7510	N1760.6.03.06.B3HZ

Test Cases

In our experiments, we focus on those test cases that lead to a finding (assigned with a test case code TC). Tables 6 and 7 document the *full* set of test cases including those that we applied and that did not yield a security-critical result.

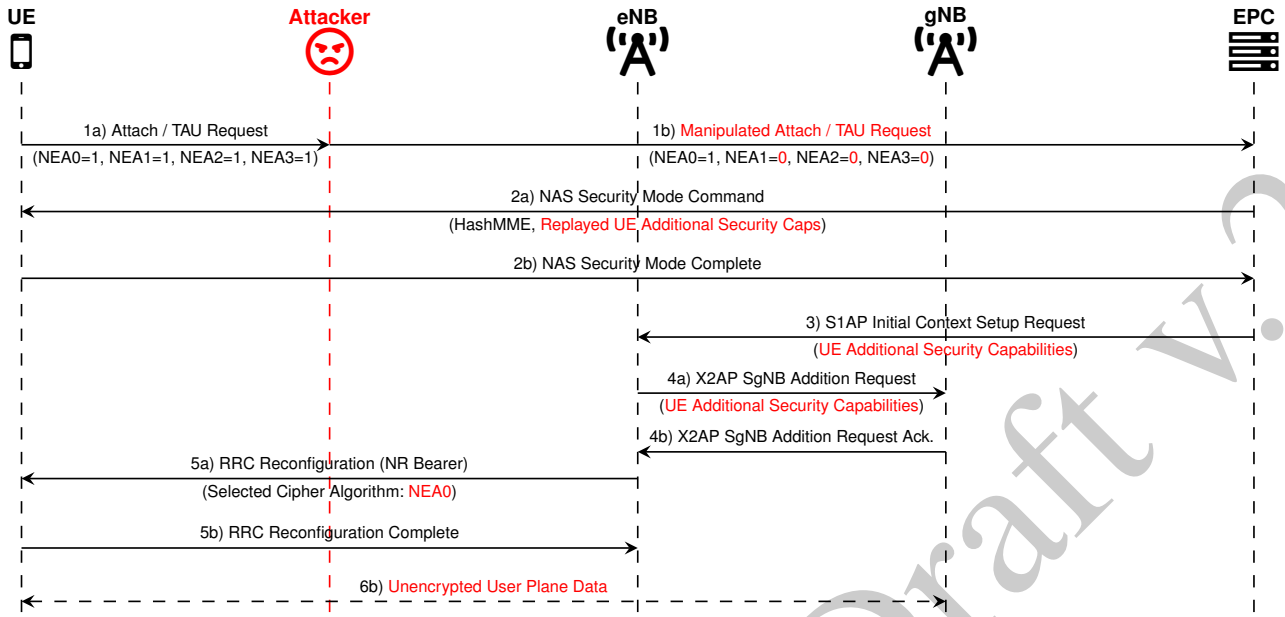

Figure 4. 5G NSA NEA0 bidding-down attack. The attacker manipulates the UEs additional security capabilities and enforces null encryption on the 5G NSA connection between UE and gNB. Due to multiple implementation flaws in UE and core network, the attack can not be detected.

TABLE 6. COMPLETE SET OF UE TEST CASES

Type	Test Case	Code	G	Issues Found
UE Security Capabilities	Replay invalid Sec. Caps.	-	5G SA	No
	NAS Security Mode Command with NIA0	-	5G SA	No
	RRC Security Mode Command with NIA0	-	5G SA	No
	NR Bearer Est., no replay of Add. Sec. Caps	-	5G SA	No
	Replay Add. Sec. Caps.	1	5G NSA	Yes
	Replay Add. Sec. Caps. with HashMME	2	5G NSA	Yes
	Replay Add. Sec. Caps., UE has not sent any	3	5G NSA	Yes
	NR Bearer Est., no replay of Add. Sec. Caps	4	5G NSA	Yes
	Replay invalid Sec. Caps.	-	4G	No
	NAS Security Mode Command with NIA0	-	4G	No
	RRC Security Mode Command with NIA0	-	4G	No
Network Capabilities	ABBA Value from Network	-	5G SA	No
Initial NAS Prot.	Retransmission of Initial NAS Message	-	5G SA	No
	Verifies HashMME	5	4G	Yes
Identity Bidding Down	Supports SUPI Encryption	6	5G SA	Yes
	Unauthenticated IMEI Identity Request	7	5G SA	Yes
	Unauthenticated 5G-GUTI Identity Request	-	5G SA	No
	Unauthenticated IMEI Identity Request	8	4G	Yes
Replay Protection	Replay Security Mode Command	9	5G SA	Yes
	Replay Security Mode Command	10	4G	Yes
Redirection	Unauth. RRC Release with redirection	-	5G SA	No
	Unauth. Redirection to 2G with policy bit	11	4G	Yes
Downgrade	Registration Reject with Cause 27	12	5G SA	Yes
	Registration Reject with Cause 7	13	5G SA	Yes
	Registration Reject with Cause 11	14	5G SA	Yes
	Registration Reject with Cause 12	-	5G SA	No
	Registration Reject with Cause 15	-	5G SA	No
	Registration Reject with Cause 25	-	5G SA	No
	TAU Reject with Cause 42	15	4G	Yes
	TAU Reject with Cause 7	16	4G	Yes
	TAU Reject with Cause 8	17	4G	Yes
	TAU Reject with Cause 17	-	4G	No
	TAU Reject with Cause 22	-	4G	No
	TAU Reject with Cause 24	-	4G	No

TABLE 7. COMPLETE SET OF NETWORK TEST CASES

Type	Test Case	Code	G	Issues Found
UE Sec. Cap.	UE Sec. Cap. with null algorithms	1	5G SA	Yes
	UE Sec. Cap. with non-mandatory algorithms	2	5G SA	Yes
	UE Sec. Cap. with no algorithm	3	5G SA	Yes
	UE Add. Sec. Cap. with null algorithms	4	5G NSA	Yes
	UE Add. Sec. Cap. with non-mandatory algorithms	5	5G NSA	Yes
	UE Add. Sec. Cap. with no algorithm	6	5G NSA	Yes
	UE Sec. Cap. with null algorithms	-	4G	No
	UE Sec. Cap. with non-mandatory algorithms	-	4G	No
	UE Sec. Cap. with no algorithm	-	4G	No
Initial NAS Message Prot.	Presence of $Hash_{MME}$	7	4G	Yes
Identity Bidding-Down	Supports SUPI Encryption	8	5G SA	Yes
Replay Protection	Replay PDU Session Establishment Request	9	5G SA	Yes
	Replay PDN Connectivity Request	10	4G	Yes
Redirection	Presence of Policy Bit	11	4G	Yes
	Presence of Policy Bit without VoLTE	12	4G	Yes

Acronyms

PLMN Public Land Mobile Network
SUCI Subscriber Concealed Identifier
AMF Access and Mobility Management Function
ABBA Anti-Bidding down Between Architectures
AKA Authentication and Key Agreement
eNB Evolved NodeB
ENDC E-UTRAN New Radio Dual Connectivity
gNB Next Generation NodeB
IMEI International Mobile Station Equipment Identity
IMSI International Mobile Subscriber Identity
MAC Message Authentication Code
MME Mobility Management Entity
NAS Non-Access Stratum
NSA Non Standalone
PDCP Packet Data Convergence Protocol
RAN Radio Access Network
RRC Radio Resource Control
SA Standalone
SUPI Subscription Permanent Identifier
UE User Equipment
USIM Universal Subscriber Identity Module

References

[1] 3GPP, "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 24.501, 2020, version 16.7.0. [Online]. Available: http://www.3gpp.org/DynaReport/24501.htm

[2] ——, "Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3," 3rd Generation Partnership Project (3GPP), Technical Specification (TS) 24.301, 2020, version 16.7.0. [Online]. Available: http://www.3gpp.org/DynaReport/24301.htm

[3] "The 4G/5G network on your desk," Amarisoft. [Online]. Available: https://www.amarisoft.com/products/test-measurements/amari-lte-callbox/

[4] Y. Chen, Y. Yao, X. Wang, D. Xu, C. Yue, X. Liu, K. Chen, H. Tang, and B. Liu, "Bookworm game: Automatic discovery of lte vulnerabilities through documentation analysis," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2021.

[5] M. Chlosta, D. Rupprecht, T. Holz, and C. Pöpper, "LTE Security Disabled — Misconfiguration in Commercial Networks," in *Conference on Security & Privacy in Wireless and Mobile Networks (WiSec)*. ACM, 2019.

[6] M. Chlosta, D. Rupprecht, C. Pöpper, and T. Holz, "5G SUCI-catchers: still catching them all?" *Conference on Security & Privacy in Wireless and Mobile Networks (WiSec)*, 2021.

[7] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," in *ACM Annual Computer Security Applications Conference (ACSAC)*. ACM, 2014.

[8] "free5GC: open-source project for 5th generation mobile core networks," free5GC. [Online]. Available: https://www.free5gc.org/

[9] G. C. F. (GCF), "3GPP Certifications." [Online]. Available: https://www.globalcertificationforum.org/services/3gpp-certifications.html

[10] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, "srsLTE: An Open-Source Platform for LTE Evolution and Experimentation," in *ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH)*. ACM, 2016, pp. 25–32.

[11] GSMA, "GSMA Coordinated Vulnerability Disclosure Programme." [Online]. Available: https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

[12] ——, "GSMA Network Equipment Security Assurance Scheme." [Online]. Available: https://www.gsma.com/security/network-equipment-security-assurance-scheme/

[13] ——, "Road to 5G: Introduction and Migration." [Online]. Available: https://www.gsma.com/futurenetworks/wp-content/uploads/2018/04/Road-to-5G-Introduction-and-Migration_FINAL.pdf

[14] B. Hong, S. Bae, and Y. Kim, "GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier," in *Symposium on Network and Distributed System Security (NDSS)*. ISOC, 2018.

[15] X. Hu, C. Liu, S. Liu, W. You, Y. Li, and Y. Zhao, "A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security," *IEEE Access*, 08 2019.

[16] L. Huang, "Forcing a Targeted LTE Cellphone into an Eavesdropping Network," 05 2016. [Online]. Available: https://conference.hitb.org/hitbsecconf2016ams/sessions/forcing-a-targeted-lte-cellphone-into-an-eavesdropping-network/

[17] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE," in *Symposium on Network and Distributed System Security (NDSS)*. ISOC, 2018.

[18] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5GReasoner: A Property-Directed Security and Privacy Analysis Framework for 5G Cellular Network Protocol," in *Conference on Computer and Communications Security (CCS)*. ACM, 2019.

[19] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil," in *Conference on Security & Privacy in Wireless and Mobile Networks (WiSec)*. ACM, 2019.

[20] S. R. Hussain, I. Karim, A. A. Ishtiaq, O. Chowdhury, and E. Bertino, "Noncompliance as Deviant Behavior: An Automated Black-box Noncompliance Checker for 4G LTE Cellular Devices," in *Conference on Computer and Communications Security (CCS)*, 2021, pp. 1082–1099.

[21] R. P. Jover, "LTE Security, Protocol Exploits and Location Tracking Experimentation with Low-Cost Software Radio," *CoRR*, vol. abs/1607.05171, 2016. [Online]. Available: http://arxiv.org/abs/1607.05171

[22] R. P. Jover and V. Marojevic, "Security and Protocol Exploit Analysis of the 5G Specifications," *arXiv preprint arXiv:1809.06925*, 2018.

[23] H. Kim, J. Lee, E. Lee, and Y. Kim, "Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane," in *IEEE Symposium on Security and Privacy (SP)*. IEEE, 2019.

[24] S. Lambert, "Number of Internet Users in 2022/2023: Statistics, Current Trends, and Predictions." [Online]. Available: https://financesonline.com/number-of-internet-users/

[25] S. Meier, B. Schmidt, C. Cremers, and D. Basin, "The TAMARIN Prover for the Symbolic Analysis of Security Protocols," in *International Conference on Computer Aided Verification*. Springer, 2013.

[26] B. Michau and C. Devine, "How to not Break LTE Crypto," in *ANSSI Symposium sur la sécurité des technologies de l'information et des communications (SSTIC)*, 2016.

[27] S. F. Mjølsnes and R. F. Olimid, "Easy 4G/LTE IMSI Catchers for Non-Programmers," in *Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS)*. Springer, 2017.

[28] "Open source project of 5GC and EPC," Open5GS. [Online]. Available: https://open5gs.org/

[29] "OpenAirInterface (OAI) - 5G Software Alliance for Democratising Wireless Innovation," http://www.openairinterface.org/, OpenAirInterfaceTM Software Alliance (OSA), [Online; accessed 15-Nov-2019].

[30] I. Palamà, F. Gringoli, G. Bianchi, and N. Melazzi, "IMSI Catchers in the wild: A real world 4G/5G assessment," *Computer Networks*, vol. 194, p. 108137, 05 2021.

[31] C. Park, S. Bae, B. Oh, J. Lee, I. Lee, Eunkyu Yun, and Y. Kim, "DoLTEst: In-depth Downlink Negative Testing Framework for LTE Devices," in *USENIX Security Symposium (SSYM)*, 2022.

[32] S. Park, A. Shaik, R. Borgaonkar, and J.-P. Seifert, "Anatomy of Commercial IMSI Catchers and Detectors," in *Workshop on Privacy in the Electronic Society*, ser. WPES'19, 2019, pp. 74–86.

[33] D. Rupprecht, K. Jansen, and C. Pöpper, "Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness," in *Workshop on Offensive Technologies (WOOT)*. USENIX Association, 2016.

[34] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems," in *Symposium on Network and Distributed System Security (NDSS)*. ISOC, 2016.

[35] "CoreScope: 5G core testing solution ," Software Radio Systems Ltd. [Online]. Available: https://github.com/srsran/corescope

[36] G.-H. Tu, Y. Li, C. Peng, C. Li, H. Wang, and S. Lu, "Control-Plane Protocol Interactions in Cellular Networks," *ACM SIGCOMM Computer Communication Review*, vol. 44, 08 2014.

[37] Wikipedia, "List of 5G NR networks." [Online]. Available: https://en.wikipedia.org/wiki/List_of_5G_NR_networks