Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G

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

Nils Fürste
Software Radio Systems
Barcelona, Spain
nils.fuerste@srs.io

David Rupprecht
Radix Security
Bochum, Germany
david@radix-security.com

Katharina Kohls
Radboud University
Nijmegen, Netherlands
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 numerous 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, current research 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 mitigations and analyze their specification and implementation in phones and 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.

CCS CONCEPTS

• **Security and privacy → Mobile and wireless security**.

KEYWORDS

Bidding-Down, Downgrade, Fake Base Station, 4G, 5G

ACM Reference Format:
Bedran Karakoc, Nils Fürste, David Rupprecht, and Katharina Kohls. 2023. Never Let Me Down Again: Bidding-Down Attacks and Mitigations in 5G and 4G. In *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '23), May 29-June 1, 2023, Guildford, United Kingdom.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3558482.3581774

WiSec '23, May 29-June 1, 2023, Guildford, United Kingdom

ACM ISBN 978-1-4503-9859-6/23/05.
https://doi.org/10.1145/3558482.3581774

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 [26]. 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 [36]. 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 a generation. For example, when an adversary makes the network believe that the victim's phone only supports null algorithms, 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 [39] or how connections can be manipulated into using null encryption [7, 38], 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 [22, 25, 35] or specifications [6, 19, 20], 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 [3, 4]. 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 protocols. To the best of our knowledge, the current state of the art provides either isolated security analyses of individual attack concepts or conducts generic security analyses of specifications. However, it cannot offer a structured comparison of UE- and network-based attack vectors.

In this work, we provide a systematization of bidding-down attacks and their attack vectors. Based on this extensive overview of attacks, we extend existing security test cases by 24 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 [10, 23, 28], 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 or missing security features enabled in phones and public networks. Further, we demonstrate a full 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 through the GSMA CVD program [14]. We further notified manufacturers about implementation flaws to contribute to timely fixes.

2 PRELIMINARIES

From a high-level view, we distinguish between three parts of a mobile network. 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.

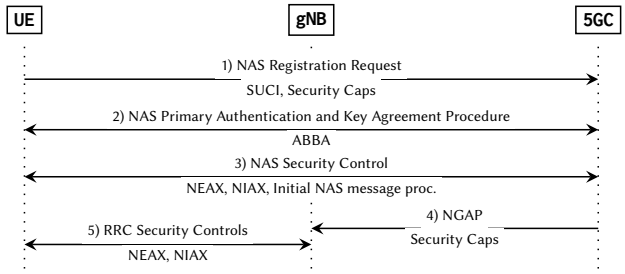

Figure 1: Simplified security context establishment between UE and 5GC core network in 5G SA.

2.1 Security Establishment

The UE and the network are responsible for establishing the security context for a connection (cf. Figure 1). Exemplary for 5G Standalone (SA), we describe each step in this procedure.

1) The UE sends the `Registration Request` containing all supported, currently four, security algorithms. One of them is the null algorithm which does not provide any security.

2) Based on the UE identity, the 5GC 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 Non-Access Stratum (NAS) connection and sends its response in the `Security Mode Command` including a replay of the initial `UE Security Capabilities`.

4) & 5) The core network sends the `UE Security Capabilities` to the gNB, which subsequently chooses a security algorithm for the radio connection. Those are then established via the Radio Resource Control (RRC) security control procedure.

It is important to note that the pre-authentication traffic before the security establishment is unprotected, which means that the UE is unable to verify the legitimacy of messages at first.

2.2 Deployment Scenarios

We focus on 4G and 5G implementations and define the following deployment scenarios. In 4G, the UE connects to the Evolved NodeB (eNB) via the air interface, which is connected to the 4G core network. A 5G Non Standalone (NSA) network has multiple deployment options [13], whereas we focus on the widely used NSA option E-UTRAN New Radio Dual Connectivity (ENDC) [41]. In an ENDC deployment, the UE connects to a main eNB and secondary Next Generation NodeB (gNB), both of which are connected to a 4G core network. We refer to ENDC as 5G NSA. In 5G 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.

2.3 Threat Model

We consider the following attack and attacker characteristics.

Bidding-Down Attacks. In a bidding-down attack, an adversary attempts to downgrade the security of a network connection. This can 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. We focus on analyzing the feasibility of bidding-down attacks against different implementations of UEs and core networks.

Security Assessment. The 3GPP defines a basic set of security tests in their Security Assurance Specification (SCAS) including the expected behavior for different components of a mobile network infrastructure. 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 towards the UE and towards the network. 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 (cf. §3).

3 BIDDING-DOWN ATTACKS

In the following, we first introduce our categorization characteristics and then assess two major classes of attacks.

3.1 Categorization

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

Class. We distinguish between intra-generation (cf. §3.2) and inter-generation (cf. §3.3) attacks.

Attack Vector. To specify this further, we distinguish *attack vectors* that enable the bidding-down attacks. To this end, we focus on message types and features that can be exploited for an attack.

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 enables an attacker to impact the overall security of the connection.

Specification. We inspect the attack vectors for each mobile generation and derive the potential for a bidding-down related security risk. Detailed and unambiguous specifications ✔only yield further experiments if preliminary experiments indicate potential issues. Whenever the specification leaves room for speculation ✖, we verify the security of specific implementations. We manually analyze the specification to scope our analysis on the bidding down relevant parts more efficiently. The targeted analysis allows a more in-depth coverage and elaboration of the interrelationships of the bidding down attack vectors and mitigations.

UE, Networks. To cover both UEs and networks, 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 the case of the network, we send critical messages from the UE and analyze the network's reaction. Vulnerabilities are documented as ● in cases where at least one of the tested systems yielded a test failure. Tests are successful ❍ 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 target are noted as –.

3.2 Intra-Generation

We classify the feasibility of intra-generation attacks through five different attack vectors (cf. Table 1) and their features.

3.2.1 UE Security Capabilities. The UE uses the security capabilities to signal the 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. To this end, we focus on two scenarios. First, manipulated setups with null algorithms result in security-critical plaintext submissions. Second, we must consider that a subset of algorithms may be compromised in the future.

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 individual implementation of each vendor.

Vulnerable Vendor Implementation. If the vendor's implementation does not reject invalid 5G NSA UE Security Capabilities, bidding-down attacks on the 5G NSA connection are possible.

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. This is particularly relevant for the 5G NSA case, where the specification does not describe a detection mechanism for the core network.

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.

3.2.2 Network Capabilities. Current security features in the 5G standard might get compromised in the future, e. g., a broken cryptographic algorithm, and will be replaced by more secure versions. The 5G standard introduces Anti-Bidding down Between Architectures (ABBA) parameter that allows the core network to prevent the UE from using compromised features.

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	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	✖	–	–

ABBA Parameter: 5G SA. The ABBA parameter is sent unprotected from the network to the UE [4]. However, it is guarded against manipulation, as it is one of the input parameters of the initial Authentication and Key Agreement (AKA) protocol.

UE Responsibility. The UE is responsible for enforcing the policy of the explicit ABBA parameter value set by the network.

3.2.3 Initial NAS Message Protection. The `Initial NAS Message` initiates the establishment of a connection between the UE and the core network. Prior to the security context establishment, this is either an `Attach Request` (4G) or a `Registration Request` (5G). Besides the `UE Security Capabilities`, the `Initial NAS Message` contains additional parameters with security implications. The 4G and 5G specifications include different mechanisms to counteract tampering with the `Initial NAS Message`.

Retransmission of Initial NAS Message: 5G SA. After the security context is established, the UE must retransmit the `Initial NAS Message` [1, 5.4.2.3]. The network then uses the retransmitted `Initial NAS Message` instead of the earlier unprotected version.

HashMME: 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` ciphered and integrity protected. 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. If protection of the `Initial NAS Message` is implemented incorrectly, bidding-down attacks are possible by tampering with the included security-relevant parameters.

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. The 5G standard has introduced the Subscription Permanent Identifier (SUPI) as a permanent identifier which, unlike the IMSI, can be sent encrypted and thus provides protection against IMSI catchers.

Pre-authenticated 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 Subscriber Concealed Identifier (SUCI) in 5G or the IMSI in 4G. However, the network may additionally request the International Mobile Station Equipment Identity (IMEI) of the UE instead. The IMEI is an additional unique identifier to the IMSI and identifies the corresponding hardware of the UE. By the 4G and 5G specifications, the UE is not allowed to send the IMEI in cleartext prior to the establishment of the security context to prevent tracking attacks.

Cleartext Extraction of IMEI. Vulnerable UE devices enable an attacker to extract the cleartext IMEI and completely bypass the identity protection provided by the encrypted SUPI.

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 re-sent by an adversary.

NAS Count: 4G, 5G SA. The NAS count is a sequence number that is sent with all ciphered and integrity-protected messages, and it is an input parameter to the Message Authentication Code (MAC) for integrity protection. The UE and the network increment a corresponding count value for each message sent and received.

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

We define two types of inter-generation attack vectors and discuss their individual features.

3.3.1 DoS / Downgrade. A DoS can either be a standalone attack, or is the entry point for a follow-up downgrade. 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.

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* unprotected reject messages 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 and can be exploited to initiate a downgrade attack.

3.3.2 Redirection. Base stations use a redirection mechanism to send a UE into a cell in another frequency or network generation. In a malicious context, redirections target a specific fake base station and thus increase the success chances for a downgrade attack.

RRC Release with Redirection: 5G, 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. As the release procedure can be initiated before the radio connection is secured, the following redirections are possible.

5G → 4G. In 5G, the UE must 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 specification does not provide any countermeasures to prevent a pre-authenticated RRC redirection from 4G to 3G.

4G → 2G. 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 specification does not provide any countermeasures to prevent a pre-authenticated RRC redirection from 3G to 2G.

Redirection. While 5G prevents insecure redirections by default, 4G networks require additional operational steps to provide protection against redirection attacks

4 EXPERIMENTS AND RESULTS

Our experiments focus on the security of networks (cf. Table 2) and commercial UEs (cf. Table 3). While we apply a *full* set of test cases to the systems under test (cf. Appendix, Tables 5 and 6), we focus our documentation and results only on those tests in which we observed an open attack vector. We perform a total of 47 tests, including 34 for the UEs and 14 for the networks. We find vulnerabilities in 16 tests for the UEs and 11 tests for the networks. In the following, we describe the experimental setup used for all tests, describe the adjustments in place for individual experiments, and document the network (§4.2) and UE (§4.3) tests and their results.

4.1 Experimental Setup

Our experimental setup 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` [32] and the eNB/gNB implementation `srsENB`[1], which is provided by the `srsRAN` [12] open-source software radio suite.

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. To achieve this, we use a modified version of `CoreScope` [27], which is a testing tool that combines a 5G UE and gNB architecture and requires no additional radio front-end. The tests in the commercial networks are done using a rooted phone with SCAT [16] and `srsUE`.

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. All devices support the newest 5G standard and receive the latest security updates.

[1]For a subset of test cases, we exchange the `srsENB` with the eNB/gNB provided by an `Amarisoft Callbox` [5] due to technical limitations.

For the network tests, we use four different core networks in our lab setup and further conduct experiments with three commercial networks. The lab setup consists of the open-source implementations `open5gs` [32], `OAI5GCN`[2] [33], `Free5GC`[2] [11] and a closed-source commercial solution. For the public networks, we are limited to 4G and 5G NSA, because no local provider in our reach has deployed 5G SA networks at the time of writing.

Ethical Considerations. We conducted all UE tests in a shielded environment to not interfere with commercial networks and users. Before testing in the operator networks, we conducted preliminary experiments in the operator lab with the corresponding commercial equipment. We comprehensively verified the network equipment's internal logfiles, and PCAP captures to exclude any undefined behavior. Finally, the attacks presented in the case studies were limited to our shielded lab network.

4.2 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` to the core network. We then verify whether the core network accepts the capabilities and the selected algorithms in the `Security Mode Command`. Our permutations 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 and 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. Consequently, 4G security issues [7] have been inherited by 5G.

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* lab and public networks fail the test case.

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 manipulated by an adversary.

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

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 Replay Protection. To test a system's vulnerability against replayed NAS messages, we send messages that always trigger a response from the network and verify if the network responds to the subsequent replay of those messages.

TC8: Replay PDU Session Est. Request. In 5G, 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 core networks do not implement replay protection.

TC9: Replay PDN Connectivity Request. Analog to **TC8**, we replay 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.

4.2.4 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.

TC10, TC11: 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.

Conclusion Network Experiments. The results of our network experiments are devastating. In total, we found security issues in five different mitigations that affect both open-source networks and publicly available commercial networks. 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 5 in the Appendix. The full name of the UEs and the baseband models are listed in Table 4.

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`

Table 2: Network Test Results. ❍ Success, ● Failure, – Not applicable, ✔ Spec. complete, ✖ Spec. 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	✔	❍	–	–	❍	●	●	●
Replay Protection	5G SA	8	✔	●	●	●	❍	–	–	–
	4G	9	✔	●	–	–	❍	❍	❍	❍
Redirection	4G	10	✔	●	–	–	●	●	●	●
		11	✔	●	–	–	●	●	●	●

Table 3: UE Test Results. ❍ Success ● Failure ✔ Spec. complete ✖ Spec. issues

Mitigation	G	TC	Spec.	OP 10 Pro 5G	iPhone SE 2022	P40 Pro 5G	S22	Pixel 6 Pro	A22	F50+
UE Sec. Caps.	5G NSA	1	✔	❍	❍	❍	●	●	❍	❍
		2	✔	●	●	❍	●	●	❍	❍
		3	✖	●	●	●	●	●	❍	●
		4	✖	●	●	●	●	●	●	●
Initial NAS Msg. Prot.	4G	5	✔	❍	❍	●	●	●	❍	●
Identity Bidding-Down	5G SA	6	✔	❍	❍	❍	●	●	❍	❍
	4G	7	✔	❍	❍	❍	●	●	❍	❍
Replay Protection	5G SA	8	✔	❍	❍	❍	●	●	●	❍
	4G	9	✔	❍	❍	❍	●	●	●	●
Redirection	4G	10	✔	❍	❍	❍	●	●	❍	❍
Downgrade	5G SA	11	✖	●	●	●	●	●	●	●
		12	✖	●	●	●	●	●	●	●
		13	✖	❍	❍	❍	●	●	●	●
	4G	14	✖	●	●	●	●	●	●	●
		15	✖	●	●	❍	❍	❍	●	❍
		16	✖	❍	❍	●	●	●	●	●

message. Our experiments show two UEs that *fail* the test case and do not verify the replayed message in the `Security Mode Reject`. 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 (TC3), 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 security capabilities. *All* devices except for one *fail* this test case.

Finally, we check the UE behavior when the network does not replay the UE Additional Security Capabilities but still instructs the UE to establish a connection with the gNB (TC4). 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. *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 $Hash_{MME}$ in the `Security Mode Command` and send it to the UE. A UE with correct implementation should verify the invalid hash and then retransmit its `Initial NAS Message` in the protected `Security Mode Complete`. Two devices *fail* this test and ignore the invalid $Hash_{MME}$ value.

The verification of the replayed security capabilities (TC1-TC4) or the $Hash_{MME}$ (TC5) is the last checkpoint to prevent a bidding-down attack. Unfortunately, for the majority of devices, implementation flaws prevent the UE from identifying malicious behavior.

TC6, TC7: 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 cleartext IMEI to the unauthenticated requests in 4G and 5G.

Despite being known for several years [30], 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.

4.3.3 Replay Protection. Replay protection must be implemented correctly on both endpoints of the connection. To verify the side of the UE, we repeat the network test cases TC8 and TC9.

TC8, TC9: Replay of Security Mode Command. To audit the replay protection of the individual UEs, we replay a `Security Mode Command` message to the UE. Our experiments show three devices for 5G and four devices for 4G 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 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, 19].

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

TC10: 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 test network has correctly deployed the network policy, the implementation flaw in the vulnerable UEs completely nullifies the protection and enables redirection attacks [18].

4.3.5 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.

TC11, TC12, TC13: Registration Reject. In our lab setup, we operate legitimate 5G and 4G networks. The UE selects the 5G cell as it is the highest available generation. We then run a 5G fake base station and attempt to lure the UE into initiating a registration procedure. 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` (TC11), 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` (TC12) triggers a downgrade in two UEs and causes a DoS in five UE models. With the cause `11: PLMN Not Allowed` (TC13), we cause a downgrade in one and a DoS in three devices.

TC14, TC15, TC16: 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` (TC14). 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, three UEs downgraded to the 2G network if they are rejected with cause `7: EPS services not allowed` (TC15). Further, we test cause `8: EPS services and non-EPS services not allowed` (TC16), which causes a DoS 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 4G, bypassing all of the latest security features. Furthermore, we identify a new reject cause that enables a downgrade from 4G to a lower generation. This reject cause triggers a downgrade more reliably than causes discussed in prior work [18, 24, 39].

Conclusion UE Experiments. Our findings have severe consequences for the security of the end users, as we find various individual attack vectors that can be exploited by an adversary. Our case studies in section 5 demonstrate how these flaws can be exploited to forge bidding-down attacks that impair the security of a connection. Furthermore, we can derive certain characteristics from the test results that have an influence on the realization of security features.

Vendor Dependency. A device's security depends on the specific implementation of a baseband vendor. Devices from different manufacturers that share basebands from the same vendor, e. g., OP 10 Pro and iPhone SE, are likely to share the same implementation flaws. Further, the test results emphasize that the number of vulnerabilities found varies depending on the vendor, as each vendor may interpret and implement the specification differently. Consequently, we see mixed results for test cases in which the specification is complete (e. g. TC 5-11) and observe a tendency of test failures for individual vendors. However, in the cases where the specification is incomplete or ambiguous (e. g. TC 2-4), most devices fail the tests. Furthermore, the differences in the outcome of the downgrade tests may indicate that certain vendors have implemented custom protection measures.

Synergy between UE and Network. The test results clearly show that connection security is a two-sided problem. Given a secure behavior by the 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

We demonstrate the feasibility of two full attack procedures, i. e., a Downgrade Dance (§5.1, **ATK1**), and a NEA0 Bidding-Down (§5.2, **ATK2**) in case studies with 7 UEs (cf. Table 4).

5.1 Downgrade Dance 5G → 2G

The attack aims to *downgrade* a victim from a 5G network to 2G. To achieve this, the adversary conducts step-by-step exploits of the pre-authentication phase of all generations (§3.3.1, §4.3.5).

Table 4: UEs analyzed in the bidding-down case studies. The check (✔) denotes a successful attack on the device.

Phone	Baseband	ATK1	ATK2
Samsung S22	Exynos	✔	✔
Google Pixel 6 Pro	Exynos	✔	✔
iPhone SE 2022	Qualcomm	✔	✖
One Plus 10 Pro	Qualcomm	✔	✖
Huawei P40 Pro 5G	HiSilicon	✔	✖
Hisense F50+	UNISOC	✔	✖
Samsung A22 5G	Mediatek	✔	✖

5.1.1 Prerequisites and Attacker Model. We assume that the victim is registered in the legitimate 5G test 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 SIM card and letting it connect to the legitimate network. To simulate the attack, we manipulate the gain of our fake base station and the legitimate 5G gNB. In reality, the attacker must use more sophisticated hardware and techniques, such as the use of a jammer to disturb the legitimate transmission and force the UE to another 5G cell.

5.1.2 Attack Procedure. While the victim connects to the legitimate 5G SA cell, we trigger a cell re-selection to the 5G SA fake base station by increasing its signal gain (cf. Appendix 3). 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 4G cells. Repeating the same procedure, we can downgrade the UE step-by-step to 2G. 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 in 5G NSA, we must combine exploits for the network and the UE. On the network side, a UE with invalid `UE Additional Security Capabilities` shall not be rejected. At the same time, the $Hash_{MME}$ and the replayed `UE Additional Security Capabilities` are not checked in vulnerable devices.

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. 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) (cf. Appendix 2). The network receives and then replays the `UE Additional Security Capabilities` back to the UE in the *integrity protected* `NAS Security Mode Command` message. As the manipulated capabilities are not checked by the vulnerable 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 `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. 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. 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 [29]. *However, such verification cannot be a replacement for the security assessment of implementations.*

6.2 Improvements

Our observations indicate different improvements for the specification and implementation of network components.

6.2.1 Specification. The following improvements help to overcome security-relevant ambiguities in the specification.

- **High-Impact Reject Causes.** We suggest that NAS reject causes with security implications shall only be accepted by the UE after *authentication* with the network. Despite the additional authentication procedure, we gain significant protection against bidding-down attacks. However, all security-related causes must be covered and ensured that no cause is required before authentication in order not to break any edge cases.
- **RRC Redirection Mitigation Missing.** In the latest release, 4G (optionally) prevents 4G → 2G RRC redirection attacks while the downgrades from 4G → 3G and from 3G → 2G are still possible. We suggest that the 4G specification implements a similar prevention mechanism to prevent attacks from 4G → 3G.
- **Rejection HashMME mismatch.** The UE does not reject the connection establishment, if $Hash_{MME}$ and $Hash_{UE}$ do not match although it is a sign of manipulation. The specification argues that this is obsolete, as the UE has already

checked the `UE Security Capabilities` before. We suggest that the UE should reject the connection immediately if the hashes mismatch.

- **UE Additional Security Capabilities in 5G NSA.** The exchange of `UE Additional Security Capabilities` and the security algorithm negotiation is not securely specified for the 5G NSA case. The specification must determine how the MME shall handle insecure and invalid `UE Additional Security Capabilities`.

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, it is certified regarding its radio and protocol conformance. Those UE conformance tests lack a security focus. In contrast, the GSMA NESAS scheme solely focuses on the security of network components [15]. 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 following, we discuss previous work related to bidding-down vulnerabilities and systematic security analysis approaches.

7.1 Bidding-Down Specification Flaws

Specification flaws are particularly relevant, as they affect *all* network equipment that strictly follows the specification in their implementation [19, 20, 40]. Shaik et al. [39] and Jover [24] demonstrated downgrade attacks on 4G using pre-authenticated NAS reject messages. We extend this by considering *all* existing reject causes. Further, previous work [20, 37] indicates that security issues regarding pre-authenticated NAS messages might be inherited to the 5G standard. Moreover, Hussain et al. [21] proposed additional methods to solve the underlying problem of unauthenticated pre-authenticated traffic. Other variants of downgrade attacks use RRC redirections [18] that should be mitigated through features of the specification. However, our results show that networks remain vulnerable.

7.2 Bidding-Down Implementation Flaws

Attackers can exploit implementation flaws to forge different types of bidding-down or downgrade attacks, e. g., accepting weak algorithms [35, 38]. Our findings support these observations for the latest generations. Identity bidding-down vulnerabilities have been revealed [30, 35], 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 [9, 31, 36], 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. [8] demonstrated that SUCI catcher attacks are still possible, although being less practicable and require far more effort than 4G IMSI catching techniques. We analyze the corresponding measures and find UEs revealing their IMEI in unauthenticated requests in 5G. Furthermore, our test results underline the correlation between detected implementation flaws and individual baseband vendors and align with findings by Palamà et al. [34].

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. Prior work provides analysis frameworks [34, 35], studies on commercial networks [7], or tests for the control plane of UEs and networks [25]. However, there is a lack of past work thoroughly analyzing bidding-down mitigations.

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.

ACKNOWLEDGMENTS

We sincerely thank our shepherd and the anonymous reviewers for their valuable and helpful feedback. This work was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CASA – 390781972.

REFERENCES

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

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

[3] 3GPP. 2022. *3GPP System Architecture Evolution (SAE); Security architecture.* Technical Specification (TS) 33.401. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/33401.htm Version 17.2.0.

[4] 3GPP. 2022. *Security architecture and procedures for 5G System.* Technical Specification (TS) 33.501. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/33501.htm Version 17.6.0.

[5] Amarisoft. 2022. The 4G/5G network on your desk. https://www.amarisoft.com/products/test-measurements/amari-lte-callbox/ [Online; accessed 18-Nov-2022].

[6] Yi Chen, Yepeng Yao, XiaoFeng Wang, Dandan Xu, Chang Yue, Xiaozhong Liu, Kai Chen, Haixu Tang, and Baoxu Liu. 2021. Bookworm Game: Automatic Discovery of LTE Vulnerabilities Through Documentation Analysis. In *2021 IEEE Symposium on Security and Privacy (SP)*. ieee, online, 1197–1214. https://doi.org/10.1109/SP40001.2021.00104

[7] 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* (Miami, Florida) *(WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 261–266. https://doi.org/10.1145/3317549.3324927

[8] 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* (Abu Dhabi, United Arab Emirates) *(WiSec '21)*. Association for Computing Machinery, New York, NY, USA, 359–364. https://doi.org/10.1145/3448300.3467826

[9] 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* (New Orleans, Louisiana, USA) *(ACSAC '14)*. Association for Computing Machinery, New York, NY, USA, 246–255. https://doi.org/10.1145/2664243.2664272

[10] Firecell. 2022. 4G and 5G Private Networks made simple. https://firecell.io/

[11] free5GC. 2022. *free5GC: open-source project for 5th generation mobile core networks*. free5GC. https://www.free5gc.org/

[12] 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* (New York City, New York) *(WiNTECH '16)*. Association for Computing Machinery, New York, NY, USA, 25–32. https://doi.org/10.1145/2980159.2980163

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

[14] GSMA. 2022. GSMA Coordinated Vulnerability Disclosure Programme. https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/

[15] GSMA. 2022. GSMA Network Equipment Security Assurance Scheme. https://www.gsma.com/security/network-equipment-security-assurance-scheme/

[16] Byeongdo Hong, Shinjo Park, Hongil Kim, Dongkwan Kim, Hyunwook Hong, Hyunwoo Choi, Jean-Pierre Seifert, Sung-Ju Lee, and Yongdae Kim. 2018. Peeking Over the Cellular Walled Gardens - A Method for Closed Network Diagnosis -. *IEEE Transactions on Mobile Computing* 17, 10 (2018), 2366–2380. https://doi.org/10.1109/TMC.2018.2804913

[17] Xinxin Hu, Caixia Liu, Shuxin Liu, Wei You, Yingle Li, and Yu Zhao. 2019. A Systematic Analysis Method for 5G Non-Access Stratum Signalling Security. *IEEE Access* 7 (2019), 125424–125441. https://doi.org/10.1109/ACCESS.2019.2937997

[18] Lin Huang. 2016. Forcing a Targeted LTE Cellphone into an Eavesdropping Network. https://conference.hitb.org/hitbsecconf2016ams/sessions/forcing-a-targeted-lte-cellphone-into-an-eavesdropping-network/

[19] 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*. isoc-ndss, San Diego, CA, USA. https://doi.org/10.14722/ndss.2018.23319

[20] 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 *Conference on Computer and Communications Security (CCS)* (London, United Kingdom) *(CCS '19)*. Association for Computing Machinery, New York, NY, USA, 669–684. https://doi.org/10.1145/3319535.3354263

[21] Syed Rafiul Hussain, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino. 2019. Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks* (Miami, Florida) *(WiSec '19)*. Association for Computing Machinery, New York, NY, USA, 1–11. https://doi.org/10.1145/3317549.3323402

[22] Syed Rafiul Hussain, Imtiaz Karim, Abdullah Al Ishtiaq, Omar Chowdhury, and Elisa Bertino. 2021. Noncompliance as Deviant Behavior: An Automated Black-Box Noncompliance Checker for 4G LTE Cellular Devices. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security* (Virtual Event, Republic of Korea) *(CCS '21)*. Association for Computing Machinery, New York, NY, USA, 1082–1099. https://doi.org/10.1145/3460120.3485388

[23] NextEPC Inc. 2021. Build your own 5G and LTE networks with NextEPC. https://nextepc.com/

[24] Roger Piqueras Jover. 2016. LTE Security, Protocol Exploits and Location Tracking Experimentation with Low-Cost Software Radio. *CoRR* abs/1607.05171 (2016). arXiv:1607.05171 http://arxiv.org/abs/1607.05171

[25] Hongil Kim, Jiho Lee, Eunkyu Lee, and Yongdae Kim. 2019. Touching the Untouchables: Dynamic Security Analysis of the LTE Control Plane. In *2019 IEEE Symposium on Security and Privacy (SP)*. IEEE, San Francisco, CA, 1153–1168. https://doi.org/10.1109/SP.2019.00038

[26] Sebastian Lambert. 2022. Number of Internet Users in 2022/2023: Statistics, Current Trends, and Predictions. https://financesonline.com/number-of-internet-users/

[27] Software Radio Systems Ltd. 2021. CoreScope: 5G core testing solution . https://github.com/srsran/corescope

[28] Magma. 2022. *A modern mobile core network solution*. Magma. https://magmacore.org/

[29] Simon Meier, Benedikt Schmidt, Cas Cremers, and David Basin. 2013. The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In *Computer Aided Verification*, Natasha Sharygina and Helmut Veith (Eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, 696–701.

[30] 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)*.

[31] Stig F. Mjølsnes and Ruxandra F. Olimid. 2017. Easy 4G/LTE IMSI Catchers for Non-Programmers. https://doi.org/10.48550/ARXIV.1702.04434

[32] Open5GS. 2022. Open source project of 5GC and EPC. https://open5gs.org/

[33] OpenAirInterfaceTM Software Alliance (OSA). 2022. *OpenAirInterface (OAI) - 5G Software Alliance for Democratising Wireless Innovation*. [Online; accessed 15-Nov-2022].

[34] Ivan Palamà, Francesco Gringoli, Giuseppe Bianchi, and Nicola Melazzi. 2021. IMSI Catchers in the wild: A real world 4G/5G assessment. *Computer Networks* 194 (05 2021), 108137. https://doi.org/10.1016/j.comnet.2021.108137

[35] 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)*. USENIX Association, Boston, MA, 1325–1342. https://www.usenix.org/conference/usenixsecurity22/presentation/park-cheoljun

[36] 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* (London, United Kingdom) *(WPES'19)*. Association for Computing Machinery, New York, NY, USA, 74–86. https://doi.org/10.1145/3338498.3358649

[37] Roger Piqueras Jover and Vuk Marojevic. 2019. Security and Protocol Exploit Analysis of the 5G Specifications. *IEEE Access* 7 (2019), 24956–24963. https://doi.org/10.1109/ACCESS.2019.2899254

[38] David Rupprecht, Kai Jansen, and Christina Pöpper. 2016. Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness. In *Proceedings of the 10th USENIX Conference on Offensive Technologies* (Austin, TX) *(WOOT'16)*. USENIX Association, USA, 40–51.

[39] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2016. Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. In *Symposium on Network and Distributed System Security (NDSS)*. ISOC.

[40] Guan-Hua Tu, Yuanjie Li, Chunyi Peng, Chiyu Li, Hongyi Wang, and Songwu Lu. 2014. Control-Plane Protocol Interactions in Cellular Networks. *ACM SIGCOMM Computer Communication Review* 44 (08 2014). https://doi.org/10.1145/2619239.2626302

[41] Wikipedia. 2021. List of 5G NR networks. https://en.wikipedia.org/wiki/List_of_5G_NR_networks

A ATTACK PROTOCOL FLOWS

Figure 3 documents the steps necessary to conduct a full downgrade attack from 5G to 2G. Figure 2 documents the protocol flow for the 5G NSA encryption bidding-down attack.

B TEST CASES

In our experiments, we focus on those test cases that lead to a finding (assigned with a test case code TC). Tables 5 and 6 document the *full* set of test cases including those that we applied and that did not yield a security-critical result.

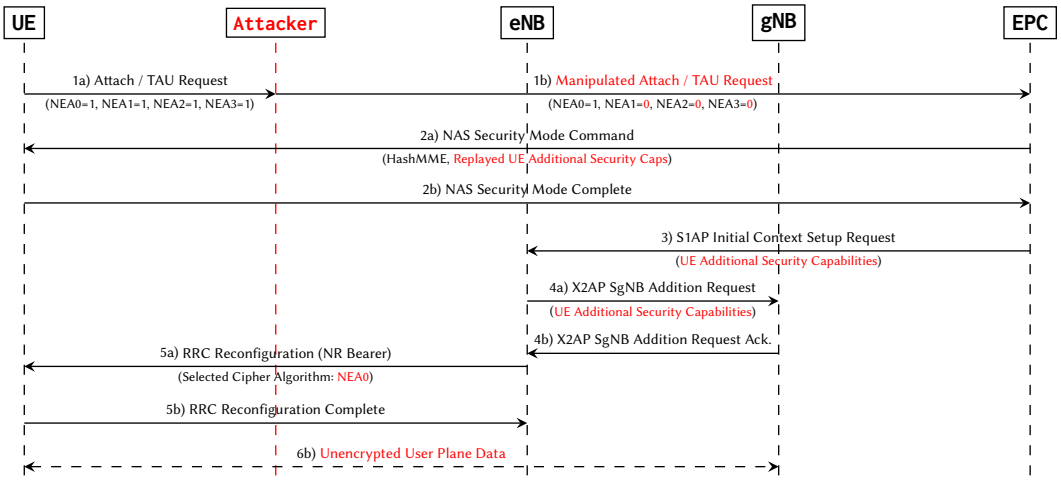

Figure 2: 5G NSA NEA0 Bidding-Down Attack.

Table 5: 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. w/o replay of Add. Sec. Caps	-	5G SA	No
	Replay invalid Add. Sec. Caps.	1	5G NSA	Yes
	Replay invalid Add. Sec. Caps. with HashMME	2	5G NSA	Yes
	Replay Add. Sec. Caps. when 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	Unauthenticated IMEI Identity Request	6	5G SA	Yes
	Unauthenticated 5G-GUTI Identity Request	-	5G SA	No
	Unauthenticated IMEI Identity Request	7	4G	Yes
Replay Protection	Replay Security Mode Command	8	5G SA	Yes
	Replay Security Mode Command	9	4G	Yes
Redirection	Unauth. RRC Release with redirection	-	5G SA	No
	Unauth. Redirection to 2G with policy bit	10	4G	Yes
Downgrade	Registration Reject with Cause 27	11	5G SA	Yes
	Registration Reject with Cause 7	12	5G SA	Yes
	Registration Reject with Cause 11	13	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	14	4G	Yes
	TAU Reject with Cause 7	15	4G	Yes
	TAU Reject with Cause 8	16	4G	Yes
	TAU Reject with Cause 17	-	4G	No
	TAU Reject with Cause 22	-	4G	No
	TAU Reject with Cause 24	-	4G	No

Table 6: 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
Replay Protection	Replay PDU Session Establishment Request	8	5G SA	Yes
	Replay PDN Connectivity Request	9	4G	Yes
Redirection	Presence of Policy Bit	10	4G	Yes
	Presence of Policy Bit without VoLTE	11	4G	Yes

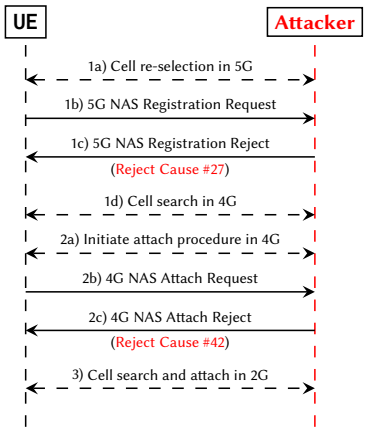

Figure 3: Protocol flow of downgrade dance from 5G to 2G.

Acronyms

PLMN Public Land Mobile Network
SUCI Subscriber Concealed Identifier
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
RAN Radio Access Network
RRC Radio Resource Control
SA Standalone
SUPI Subscription Permanent Identifier
UE User Equipment