

European 5G Security in the Wild: Reality versus Expectations

Oscar Lasierra
oscar.lasierra@i2cat.net
i2CAT Foundation

Gines Garcia-Aviles
gines.garcia@i2cat.net
i2CAT Foundation

Esteban Municio
esteban.municio@i2cat.net
i2CAT Foundation

Antonio Skarmeta
skarmeta@um.es
University of Murcia

Xavier Costa-Pérez
xavier.costa@i2cat.net
i2CAT Foundation and ICREA
NEC Laboratories Europe

ABSTRACT

5G cellular systems are slowly being deployed worldwide delivering the promised unprecedented levels of throughput and latency to hundreds of millions of users. At such scale security is crucial, and consequently, the 5G standard includes a new series of features to improve the security of its predecessors (i.e., 3G and 4G). In this work, we evaluate the actual deployment in practice of the promised 5G security features by analysing current commercial 5G networks from several European operators. By collecting 5G signalling traffic in the wild in several cities in Spain, we i) fact-check which 5G security enhancements are actually implemented in current deployments, ii) provide a rich overview of the implementation status of each 5G security feature in a wide range of 5G commercial networks in Europe and compare it with previous results in China, iii) analyse the implications of optional features not being deployed, and iv) discuss on the still remaining 4G-inherited vulnerabilities. Our results show that in European 5G commercial networks, the deployment of the 5G security features is still on the works. This is well aligned with results previously reported from China [16] and keeps these networks vulnerable to some 4G attacks, during their migration period from 4G to 5G.

CCS CONCEPTS

• Security and privacy → Mobile and wireless security.

KEYWORDS

5G, security, subscriber anonymity, subscriber privacy, experimental data collection

1 INTRODUCTION

The arrival of the fifth generation of mobile networks (5G) is substantially changing the way networks are designed and deployed. From the subscribers perspective, 5G effectively provides an improved performance compared with their predecessors, increasing available bandwidth (e.g., to provide on-demand high-quality video services) and reducing end-to-end latency (e.g., to provide real-time augmented/virtual reality applications). By the end of 2021, more than 176 commercial 5G networks have been deployed worldwide, of which only 22 were already 5G Stand Alone (SA) networks. [11]. Unfortunately, such growing figures also bring greater risks in terms of security.

However, unlike previous mobile generations such as 3G/4G which are subject to a number of known attacks [13, 15, 21, 22], 5G provides security enhancements through a series of new generation specifications defined by the 3rd Generation Partnership Project (3GPP), including TS 33.501 [3] and TS 33.511 [1]. Despite this, while current real-world 5G deployments follow the same architectural security framework reference, neither all of them implement the same 5G security mechanisms enabled by the new specifications, nor they do it in the same way. This is usually caused by the optionality of some mechanisms and by the operators' inherent constraints (cost, compatibility, or performance) [16].

In this work, we report a hands-on security analysis of currently deployed 5G networks, fact-checking security mechanisms compliance and identifying still existing vulnerabilities in current 5G deployments. For those non-compliant or partially-compliant deployments, we identify and provide an in-depth characterisation of the attacks they are vulnerable to.

In order to perform such analysis, we collect and study signalling messages between various 5G networks and the User Equipment (UE) through commercial cellular traffic sniffers focusing on currently deployed 5G networks from different network operators in urban and suburban areas of various cities in the east coast of Spain. These traces include information about the User Plane (UP) and Control Plane (CP) security activation, the subscriber identifiers exchanged and the Authentication procedures performed for accessing the network.

Our measurements show that although commercial deployments do not implement all user authentication mechanisms specified in the standard, the confidentiality and integrity implementation at the UE does always seem to comply with the standard. However, unlike previously reported in [16] for Chinese 5G deployments in Beijing, the majority of the observed networks are still exposed to 4G-inherited vulnerabilities such as identity and user data leakage and Denial of Service (DoS) attacks because of the yet general absence of Standalone (SA) 5G network deployments. Note that this is as expected due to practical deployment reasons; which is aligned with the roadmap specified by operators towards the adoption of 5G not just in Europe but worldwide. GSMA forecasts a 44% average adoption of 5G within Europe by 2025 [10]. So the migration path from 4G to 5G is on the works but will take some years still to be completed.

Therefore, the main contributions of this work are i) a comprehensive compliance analysis for different 5G networks deployed in Spain in order to fact-check and evaluate the actual security and privacy mechanisms implemented by vendors and operators

in a typical European 5G network deployment¹; and ii) a study of the available security vulnerabilities in current commercial 5G networks.

The rest of this work is structured as follows. In Section 2 we briefly provide the necessary background on 5G NR. Section 3 describes the corresponding security mechanisms included in the 5G standard and identifies the most common security threats. In Section 4 we detail the methodology followed for data collection and its subsequent analysis and in Section 5 we report the results, extensively discussing the capabilities, standard compliance, and vulnerabilities observed in the different 5G networks. Finally, Section 6 concludes this work.

2 BACKGROUND

2.1 5G Outline

The architecture of 5G cellular networks can be logically separated into three main components, User Equipment (UE), the Radio Access Network (RAN), and the mobile Core Network (CN). The UEs establish a wireless connection with the RAN to be able to reach the CN, which acts as i) an authentication entity, allowing/denying devices to access the network; and ii) acting as an ingress/egress point of the traffic generated from/to the internet.

Within the 5G context, UEs are essentially defined as a combination of two components. First, the Universal Subscriber Identity Module (USIM) card, which is used to store user identification data, such as the public/private keys and the Subscriber Permanent Identifier (SUPI), known as the International Mobile Subscriber Identity (IMSI) in 4G. Second, the Mobile Equipment (ME) hardware itself, is identified by the International Mobile Equipment Identity (IMEI).

The RAN manages the wireless connectivity through the 5G base stations (gNBs), replacing or coexisting with legacy 4G base stations (eNBs). LTE/NR coexistence is ensured through the 5G Non-standalone (NSA) mode or EUTRA NR Dual Connectivity (ENDC), which allows UEs to configure a 5G secondary node for data plane transmissions. This mode keeps 4G eNBs as master nodes which are in charge of carrying control plane traffic. In contrast, 5G Standalone (SA) mode adopts the gNB as the master node of the connection to jointly manage both data and control planes traffic. The interaction between the UE and the RAN is one of the most vulnerable parts in the network, and therefore, the main security features imposed by the 5G standard come to solve some of the major risks and pitfalls in the wireless domain [5, 8, 17, 22].

Similarly to 4G, the 5G core network (CN) provides the UEs with external packet data network connectivity. It consists of various network functions to manage different fundamental processes such as session control (SMF), authentication (AUSF and SEAF), access and mobility (AMF), etc.

2.2 Critical NR Procedures: Initial Attachment and Registration

The initial procedures performed by 5G NR carry essential information required to establish a stable and secure communication through the RAN. These processes are based on the exchange of

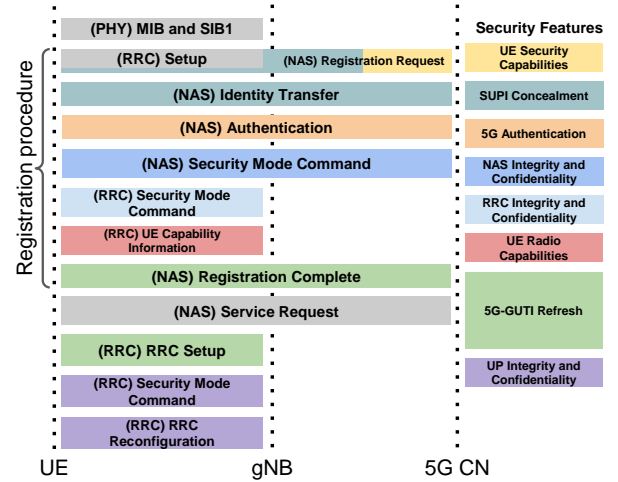


Figure 1: 5G NR Initial Registration Procedure

information between parties: *UE-gNB* for the radio link and *UE-gNB-CN* for a higher-level communication layer. Both processes must be performed in a way that preserves security and confidentiality, avoiding third-party observers to gather the exchanged information, and hence bypassing security leaks in subsequent communications.

2.2.1 Broadcast Channel and Random Access: To effectively establish a connection, the UE must perform a set of interactions with the gNB before starting with the registration procedure itself, the Cell search and the Random Access Channel (RACH).

The Cell Search procedure allows the UE to acquire time and frequency synchronisation within cells with the goal of retrieving cell parameters and system information from the Master Information Block (MIB) and the System Information Block (SIB). Synchronisation is obtained by detecting Synchronisation Signal Block (SSB) and decoding Primary and Secondary Synchronisation Signals (PSS and SSS) located on the synchronisation raster. Then, MIB is decoded from the Physical Broadcast Channel (PBCH) from the same synchronisation raster to subsequently configure the Control resource set zero (CORESET0) and SearchSpace. With this information, the UE can perform the blind decode of the Physical Downlink Control Channel (PDCCH) and configure the remaining parameters to find and decode SIB1 in the Physical Downlink Shared Channel (PDSCH) (full procedure defined in 3GPP 38.104 [2]).

RACH procedure allows the UE to configure UL synchronisation and obtain an identifier for the radio communication. If BeamForming is supported, the UE shall detect, choose and synchronise with the best beam to start the communication with the gNB.

2.2.2 Radio Resource Control: After the Random Access procedure, if the UE is not attached to the network, it has to initiate the registration procedure. Otherwise, the UE initiates the tracking area update if it has changed since the last update. For initiating any NAS procedure, the UE needs to establish a Radio Resource Control (RRC) connection with the gNB. The main purpose of this procedure is to establish an active connection with the gNB, enabling the acquisition of radio resources for the communication. RRC connection establishment involves the creation of the Signalling Radio Bearer one (SRB1) for the RRC messages exchange.

¹The network operators considered in this work operate in about 70% of the countries in the EU with similar 5G deployments

The last message of this process can carry the initial Non-Access Stratum (NAS) message from the UE to the Access and Mobility Management Function (AMF) via the gNB (Mobility Management Entity (MME) via the eNB for NSA deployments).

2.2.3 Non-Access-Stratum: To get Non-Access Stratum (NAS)-level services (e.g. internet connectivity), NAS nodes in the network need to know about the UE. To facilitate this, the UE has to initiate the Attach Procedure, which is mandatory to be performed by the UE at boot time (or by setting Airplane mode off). Once the attach procedure succeeds, a context is established for the UE in the core, and a default bearer is established between the UE and the Packet Data Network Gateway (PDN GW). This results in the allocation of an available IP address to the UE, enabling IP-based internet services in the 5G device.

3 SECURITY IN 5G NR

Security in cellular networks has been evolving during the different mobile generations in order to address the open threads identified during their operation. The enhancements brought by the 5G standard [3] are depicted in Figure 1 and summarised next.

3.1 UE credentials and identifiers

One of the major enhancements introduced in 5G SA networks is the concealment of the SUPI. In previous generations, subscriber permanent identifiers (which in some cases contain relevant information such as the phone number) were sent in clear text and thus, attackers could retrieve this information and perform impersonation attacks [15, 21]. In 5G, the UE sends a concealed version of the SUPI called Subscription Concealed Identifier (SUCI) generated by using asymmetric cryptography (the private key is securely stored in the USIM). However, 5G SUCI-Catching attacks are still possible as reported in [7]. In this sense, in order to avoid sending the subscriber identifier over the radio link, temporal identifiers were added in 4G (Globally Unique Temporary Identity, GUTI and the Temporary Mobile Subscriber Identity, TMSI) but their refresh rate was sub-optimal, failing on providing confidentiality and anonymity to users. 5G networks also use temporary identifiers but 3GPP imposes specific guidelines dealing with aforementioned vulnerabilities.

3.2 Enhanced Authentication and Privacy

The 5G Authentication and Key Agreement (5G-AKA) protocol is a security protocol introduced in the 5G standard to provide mutual authentication between all the components in the communication, i.e., UE, Serving Network (SN) and Home Network (HN) with privacy-preserving policies (i.e., providing user ID confidentiality and preventing from user tracking). Similarly to AKA protocols of previous generations, 5G-AKA allows two end-points to establish the root keys from which new keys in subsequent security procedures will be derived [19]. However previous authentication protocols, such as 4G-AKA, failed to provide anonymity to the user because a) the IMSI of the user was sent in plain text and b) when replacing the ID of the user with temporary identifiers they are usually static and persistent, hence predictable as studied in [12]. 5G-AKA adopts the use of the 5G-GUTI to address this issue. Additionally, 5G-AKA enables Non-3GPP accesses (authentication is no longer related to one specific access technology) and allows the

	UE	4G-AKA	5G-AKA
Confidentiality	SN HN	USIM MME HSS	USIM AMF/SEAF AUSF
UE Identity		IMSI/GUTI	SUCI/5G-GUTI
Trust Model		Shared Symmetric Key	Shared Symmetric Key
UE Authentication		No information to HN	Inform HN

Table 1: 5G-AKA Security Enhancements

Serving Network and the Home Network to mutually authenticate themselves by cross-verification (i.e., by the AMF and SEAF in the Serving Network and by the AUSF in the Home Network) [14]. Table 1 summarizes the 5G-AKA security enhancements along with the new 5G UE identifiers, in contrast with the previous 4G-AKA protocol.

3.3 Improved Confidentiality and Integrity

Previous generations of cellular networks failed on providing confidentiality/integrity protection on some pre-authentication signalling messages, allowing attackers to exploit multiple vulnerabilities [20]. For that reason, 5G introduces novel protection mechanisms specifically designed for signalling and user data. Besides increasing the length of the key algorithms (to 256-bit expected for future 3GPP releases), 5G forces mandatory integrity support of the user plane, and extends confidentiality and integrity protection to the initial NAS messages. Table 3 summarises in column *Standard* the requirements in terms of confidentiality and integrity protection as defined in [3].

5G also secures the UE network capabilities, a field within the initial NAS message, which is used to allow UEs to report to the AMF about the supported integrity and encryption algorithms in the initial NAS message.

In addition to backward compatibility, 5G UEs shall implement New Radio Encryption Algorithm (NEA) 0, 128-NEA1 and 128-NEA2 for confidentiality protection and New Radio Integrity Algorithm (NIA) 0, 128-NIA1 and 128-NIA2 for integrity protection. However, the implementation of the 128-NEA3 and 128-NIA3 is optional [3]. In 4G, the UE security capabilities are exchanged with integrity protection only when the UE has already established a security context. An attacker entity could capture this message and gain substantial information, e.g., the technologies supported by the UE or the device model in the best-case scenario. In order to prevent this, 5G includes both integrity and confidentiality protection in the initial registration NAS message to protect the *UE capability* field. However, for both 4G and 5G, if the UE does not have an established security context (i.e., the first registration attempt), the *UE capability* field is sent in clear. This information allows an attacker to read/modify the exchanged information and perform multiple attacks (e.g., user identification and power drain [23]).

3.4 UE Radio Capabilities transfer

Before establishing the connection, the UE needs to provide the gNB its capabilities for radio access (e.g., supported frequency bands, EN-DC support, etc.). In previous generations, this information was sent without establishing CP security directives, and hence, an adversary could hijack this information and perform bidding down attacks [23]. 5G ensures its protection by sending them in the *RRC UE Capability Information* message after enabling security directives.

City	Murcia	Alicante	Valencia	Castellon	Tarragona	Barcelona
Population	450.000	330.000	790.000	170.000	170.000	1.62M

Table 2: Cities covered for data collection

4 METRICS IN THE WILD

4.1 Data Collection Methodology

In order to characterise 5G commercial deployments we have used a commercial protocol analyser with two different SIM cards from two different network operators². The commercial protocol analyser is a *Keysight NEMO Handy Handheld*³ which includes a debugging tool used for wireless diagnostics. We have collected data traces from six Spanish cities: Barcelona (B), Tarragona (T), Castellón de la Plana (C), Valencia (V), Alicante (A) and Murcia (M) (see Table 2).

Then, to homogenise the data collection process, we have defined an experimentation methodology consisting on the following steps:

- (1) **Airplane mode ON:** The terminal will always start with airplane mode activated.
- (2) **Start data collection:** Once the airplane mode of the terminal is active, we start the data collection tool at the device.
- (3) **Airplane mode OFF:** Disabling the airplane mode will allow the device to initiate the registration process to establish an active session with the mobile operator.
- (4) **Initial registration:** At this phase, we wait until the registration process is complete.
- (5) **Traffic generation:** This phase consists on the generation of ICMP traffic to check the connectivity status and to force a possible reconfiguration of the radio channel.
- (6) **Stop data collection:** Finally, we stop the data collection tool as well as the collected data of the experiment.

Finally, to effectively study the temporary identifiers, we replace the *Traffic Generation* step with *ON-OFF Switch*, where airplane mode is activated and deactivated during the traffic gathering. Both types of experiments were performed on each geographical place with an average duration of 15 minutes. It is important to highlight the non-intrusive nature of the data collection process, where we only collect data transmitted openly over the air in a *passive* manner, i.e. without performing any interaction with the network or users.

4.2 Data Evaluation Methodology

Traces extracted from the communication process contains all the information required for the evaluation of 5G networks security features introduced in Section 3. We look into the RRC and NAS messages to identify the status of the security enhancements.

Deployment type identification. The first step in the evaluation process is to identify the type of deployment at which the user was connecting to. The incremental approach followed by operators towards the deployment of 5G networks results in two different types of deployments: i) 5G NSA and 5G SA (see Sec. 2). The identification between NSA and SA will be performed by using the Information Elements (IEs) carried by the MIB. More specifically, in 5G SA deployments the gNB will include *pdccch-ConfigSIB1*, *ssb-SubcarrierOffset* or *dmrs-TypeA-Position* IEs, which will not be present on a 5G NSA deployment.

Authentication procedure. The evaluation of the authentication procedure will be performed after the RRC connection establishment. Apart from the different messages exchange from other authentication procedures, there are other indicators within the messages that allow the proper identification of 5G AKA. For example, after the *RRCSetupComplete* message, the UE sends a *NAS RegistrationRequest* initiating the authentication procedure and hence, disclosing the underlying authentication procedure (e.g. "5GS registration type" field, 5G-GUTI as *TypeOfIdentity*, or the inclusion of the 5G-TMSI).

Privacy and Anonymity. Privacy and anonymity of terminals depend on whether UE identity is accessible by third-party observers or not. There are two types of parameters devoted to identify UEs within the authentication process: i) the permanent subscriber identifiers, which must be securely transmitted; and ii) temporal subscriber identifiers, which must be periodically updated in order to avoid their correlation with UEs. The permanent subscriber identifier can be found in the *NAS RegistrationRequest* (within the *5GS Mobile Identity* IE), when the UE starts a registration procedure or in the *NAS IdentityResponse* after receiving a *NAS IdentityRequest* from the network. Then, we focus on measuring the refresh rate of the temporal identifiers (5G-GUTI and 5G-TMSI). Their values must be updated after each registration procedure within *NAS Registration Accept* message and after *NAS Service Request* in the subsequent *RRC Connection Request* message where a new value for 5G-TMSI shall be assigned by the gNB.

In order to assess the implementation of the new 5G security features, we will check if the security of the permanent identifiers and the refresh period was applied to the temporal subscriber identifiers by checking their value within the aforementioned messages.

Confidentiality and Integrity. To assess confidentiality and integrity in the Control Plane we need to look into the RRC and *NAS SecurityModeCommand* messages, where the algorithms to provide protection are selected and activated. For the UP, we have first located the *NAS Service Request* and the subsequent *RRC SecurityModeCommand* messages, which activate the Data Radio Bearer (DRB) and the algorithms. However, the UP security is established with the *RRCReconfiguration* message, which carries information about the algorithms used for the service to provide integrity and confidentiality protection per DRB.

UE Supported Capabilities. UE network capabilities are always sent in the *NAS Registration Request* message within the UE network capability and UE additional security capability fields. In these both fields, all the security algorithms supported by the UE regarding each mobile technology are sent to the base station. In the case of NSA deployments, this information is carried by the *UECapabilityInformation* message sent by the UE.

UE Radio Capabilities Transfer. UE radio capabilities are sent in the *RRC UE Capability Information* message. Following the registration procedure time events in the traces, we verify that in some networks this message is sent before the *RRC Security Mode Command* without confidentiality or integrity protection.

²For anonymity reasons, we will refer to them as Operator A and Operator B.

³<https://www.keysight.com/us/en/product/NTH00000B/nemo-handy-handheld-measurement-solution.html>

Source			Standard	Commercial										[16]					
				Operator A					Operator B					C	D	E			
Operator				M	A	V	C	T	B	M	A	V	C	T	B	Beijing			
Location																			
User Authentication	5G AKA																		
	SUCI																		
	GUTI Refresh	After Registration After Service Req.																	
UE Radio	Capabilities Transfer																		
UE Network	Security Capabilities																		
Confidentiality Protection	NAS Signalling																		
	RRC Signalling																		
	User Data																		
Integrity Protection	NAS Signalling																		
	RRC Signalling																		
	User Data																		
Confidentiality Mechanisms	Supported by UE																		
Integrity Mechanisms	Supported by UE																		

■ 5G SA Mandatory (TS 33.501 [3]) |
 ■ 5G SA Optional (TS 33.501 [3]) |
 ■ 5G Compliant |
 ■ No 5G Compliant

Table 3: 5G Security mechanisms availability on current network deployments

5 EVALUATION

5.1 Reality Check, is current 5G Really Improving Security?

The results of the analysis following the methodology introduced in Section 4.2 are summarised in Table 3. Each row of the table represents the different security features under study, and being the columns, the standard view of each feature, the results obtained for two different operators and the results obtained in [16] respectively.

The first result to highlight is the complete absence of 5G SA deployments. Both operators are offering 5G coverage by means of 5G NSA deployments which essentially rely on existing 4G infrastructures. Hence, there is no enhancement on the Authentication and Key Agreement process.

Ciphering of Permanent Identifiers: We have checked that no concealment of permanent identifiers has been done by capturing the permanent IMSI and IMEI values which are sent without protection within the *NAS Identity Response* message.

Temporary Identifier and GUTI Refresh: We have verified along the different traces, after receiving the *NAS Attach Accept* and *RRC Connection Request* messages, the freshness of *m-TMSI* value within GUTI. *m-TMSI* shall change its value after these messages, however, only during the Registration procedure the temporary identifier is updated.

Confidentiality and Integrity: In terms of confidentiality, on the one hand the *nr-RadioBearerConfig-r15* IE to establish the DRB points to the *NEA2* algorithm in all the traces except for Operator B in the city of Tarragona. This algorithm indicates that User Data confidentiality is effectively met even if the standard marks it as optional. In contrast, Tarragona does not accomplish confidentiality protection of user data due to the lack of a 5G DRB in this area. On the other hand, confidentiality protection for the initial NAS and RRC messages is not yet implemented using 5G NEA algorithms.

In contrast to confidentiality in data transmissions, integrity is a mandatory feature for signalling messages. Nevertheless, the configured data and signalling radio bearers do not show any of the mandatory algorithms in the *IntegrityProtAlgorithm* field within

the IEs. Instead, they use algorithms from previous generations (i.e., eia2) which do not provide the required security level.

UE Network security capabilities: Moreover, we have verified the supported algorithms in the UE by checking the UE security capabilities within *NAS Attach Request* message. Despite only using 5G NEA algorithm for securing the UP, the UE supports both 5G NEA and NIA plus legacy 4G and 3G algorithms.

UE Radio capabilities: We found that only in Operator B, four access networks are sending the radio capabilities before initialising the security environment for the CP messages.

Although there is a clear trend in the reported results, note that there might be other operators/deployments (not covered in this measurement campaign) exhibiting better security results if they are more advanced in their migration path from 4G to 5G.

5.2 Effective Attacks on current 5G Deployments

Subscriber credentials (identity attacks): Since none of the studied networks implement concealment of the permanent identifier, the legacy *IMSI* catching attacks can still be deployed [9] as well as more sophisticated attacks that exploit subscriber credentials *leakability* [7] [18]. Moreover, temporary identifiers can be found in all captures (updated every time the Registration Procedure is performed), enabling identity mapping and tracking attacks by correlating temporary identifiers with UEs.

Authentication vulnerabilities (activity monitoring): Our previous section revealed the complete absence of 5G-AKA protocol and hence, the presence of UEs and their consumed mobile services can be inferred. Authors in [4] propose novel privacy attacks against all variants of AKA protocol which also affect the studied scenarios.

UP Confidentiality and Integrity: As highlighted in the evaluation section, confidentiality protection is enabled in most of the studied deployments while integrity protection is completely missing. This absence allows an adversary to perform data manipulation, identity mapping and impersonation attacks (i.e., *MitM* attacks) even if confidentiality is active [13, 20, 21].

Security Field	5G NSA Vulnerability	Threats and Attacks	5G SA Enhancement
Subscriber Credentials	No concealment of permanent identifiers No specific policies for GUTI reallocation	[7], [18], [9] [20], [22]	Concealment of SUPI, the SUCI GUTI reallocation after Registration and Service Request
Authentication procedure	Lack of randomness and the use of XOR in AUTS	[4]	—
UP Confidentiality	Optional Support	[20], [22]	UE and gNB Mandatory Support
UP Integrity	Optional Support	[20], [21], [13]	UE and gNB Mandatory Support
UE Capabilities	No security transfer of UE Capabilities	[23]	CP Security before transfer of Capabilities

Table 4: Overview of vulnerabilities and attacks

UE Radio Capabilities: Transmitting radio capabilities information before the CP security activation (*Security Mode Command* message) could lead to Identification, Binding Down and Battery Drain attacks [23]. Given the obtained results, most of the deployments enclosed by Operator B are susceptible to these attacks.

The implementation of active data collection methodologies (e.g. [6], [7]) would enrich the obtained results, allowing an in-depth analysis of the security features not only from a network subscriber perspective but from the view of an active attacker willing to exploit the available vulnerabilities.

6 CONCLUSIONS

5G networks are expected to significantly improve the security of mobile users, thanks to the newly introduced mandatory features which address identified 4G vulnerabilities. In this paper, we analysed the progress of current 5G European commercial networks deployments with respect to the expected security features. In order to do so, we collected a dataset comprising 5G measurements from two different operators in Spain, six different cities and both urban and suburban scenarios. The two major network operators considered in our study operate in 70% of the European countries and, due to economies of scale, our results can be reasonably expected to be applicable to other European countries served by the same operators. Our results show that current 5G network deployments miss expectations on i) providing improved privacy and anonymity to subscriber identifiers (transmitting them in clear text), ii) refreshing often enough temporal subscriber identifiers (facilitating subscriber identification and tracking), iii) additional confidentiality protection (inheriting security vulnerabilities from previous generations) and iv) UE radio capabilities are sometimes transferred without protection (enabling bidding down and battery drain attacks).

As already reported in [10], we are in the midst of the 4G to 5G migration, expected to be mature by 2025. Thus, as we get closer to this date, we expect operators to increasingly deploy 5G security features accordingly, covering the gaps identified by our work.

7 ACKNOWLEDGMENTS

This work has been supported by the Spanish Ministry of Economic Affairs and Digital Transformation and the European Union – NextGeneration EU, in the framework of the Recovery Plan, Transformation and Resilience (PRTR) (Call UNICO I+D 5G 2021, ref. number TSI-063000-2021-6-Open6G), and by the CERCA Programme from the Generalitat de Catalunya.

REFERENCES

- [1] 3GPP. 2021. TS 33.511: Security Assurance Specification (SCAS) for the next generation Node B (gNodeB) network product class (Release 16). https://www.3gpp.org/ftp/Specs/archive/33/_series/33.511
- [2] 3GPP. 2021. TS 38.104: Base Station (BS) radio transmission and reception: Section 5.4.3 Synchronization Raster (Release 15). https://www.etsi.org/deliver/etsi_ts/138100_138199/138104/15.14.00_60/ts_138104v151400p.pdf
- [3] 3GPP. 2022. TS 33.501: Security architecture and procedures for 5G system (Release 17). https://www.3gpp.org/ftp/Specs/archive/33/_series/33.501/
- [4] Ravishankar Bargaonkar et al. 2019. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019).
- [5] Ya-Chu Cheng and Chung-An Shen. 2022. A New Tracking-Attack Scenario Based on the Vulnerability and Privacy Violation of 5G AKA Protocol. *IEEE Access* 10 (2022), 77679–77687.
- [6] Merlin Chlosta et al. 2019. LTE security disabled: misconfiguration in commercial networks. In *Proceedings of the 12th conference on security and privacy in wireless and mobile networks*. 261–266.
- [7] Merlin Chlosta et al. 2021. 5G SUCI-catchers: still catching them all?. In *Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 359–364.
- [8] Zhiwei Cui et al. 2022. Security Threats to Voice Services in 5G Standalone Networks. *Security and Communication Networks* 2022 (2022).
- [9] Adrian Dabrowski et al. 2014. IMSI-catch me if you can: IMSI-catcher-catchers. <https://doi.org/10.1145/2664243.2664272>
- [10] GSMA. 2022. The future of 5G connectivity in Europe. Product. <https://www.gsma.com/gsmmaeurope/news/the-future-of-5g-in-europe/>
- [11] GSMA. 2022. The Mobile Economy 2022. White Paper. <https://data.gsmaintelligence.com/api-web/v2/research-file-download?id=69042315&file=280222-The-Mobile-Economy-2022.pdf>
- [12] Byeongdo Hong et al. 2018. GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier.. In *NDSS*.
- [13] Katharina Kohls et al. 2019. Lost traffic encryption: fingerprinting LTE/4G traffic on layer two. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 249–260.
- [14] Adrien Koutsos. 2019. The 5G-AKA authentication protocol privacy. In *2019 IEEE European Symposium on Security and Privacy (EuroS&P)*. IEEE, 464–479.
- [15] Stig F Mjøltnes and Ruxandra F Olimid. 2017. Easy 4G/LTE IMSI catchers for non-programmers. In *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*. Springer, 235–246.
- [16] Shiyue Nie et al. 2022. Measuring the Deployment of 5G Security Enhancement. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 169–174.
- [17] Ivan Palamà et al. 2021. IMSI catchers in the wild: A real world 4G/5G assessment. *Computer Networks* 194 (2021), 108137.
- [18] John Preuß Mattsson and Prajwol Kumar Nakarmi. 2021. Nori: Concealing the Concealed Identifier in 5G. In *The 16th International Conference on Availability, Reliability and Security*. 1–7.
- [19] Stefan Rommer et al. 2020. Chapter 8 - Security. In *5G Core Networks*, Stefan Rommer et al. (Eds.). Academic Press, 171–201. <https://doi.org/10.1016/B978-0-08-103009-7.00008-9>
- [20] David Rupperecht et al. 2019. Breaking LTE on Layer Two. In *IEEE Symposium on Security & Privacy (SP)*. IEEE.
- [21] David Rupperecht et al. 2020. IMP4GT: IMPersonation Attacks in 4G NeTworks.. In *NDSS*.
- [22] Altaf Shaik et al. 2015. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. *arXiv preprint arXiv:1510.07563* (2015).
- [23] Altaf Shaik et al. 2019. New vulnerabilities in 4G and 5G cellular access network protocols: exposing device capabilities. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*. 221–231.