Measuring the Deployment of 5G Security Enhancement

Shiyue Nie[1], Yiming Zhang[1], Tao Wan[2], Haixin Duan[1,3]✉, Song Li[1]✉
[1] Tsinghua University, China
[2] CableLabs and Carleton University
[3] QI-ANXIN Technology Research Institute, China

ABSTRACT

The fifth-generation(5G) cellular network is entering an era of rapid development. Not only is 5G supposed to be fast, it also offers enhanced security based on 5G security specifications developed by the 3rd Generation Partnership Project (3GPP). However, little is known about 5G security in real world deployment. This paper analyzes 5G security features and measures their implementation in commercial 5G networks. By collecting and analyzing signaling messages between a cell phone and several commercial 5G networks, we measured multiple aspects of 5G security in real world deployment including, crypto algorithms used in the control plane, user plane (UP) security activation, subscriber identifier protection, and initial None-Access Stratum(NAS) message protection. We evaluated the compliance of commercial 5G networks with 5G security specifications. The results show that major discrepancy exists between 5G security standards and real world deployment, especially in the areas of UP protection and subscriber identifier protection. Therefore, well-known security risks, such as user data leakage, location exposure and Denial-of-Service(DoS) attacks, still apply to 5G commercial networks.

CCS CONCEPTS

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

KEYWORDS

5G security enhancement, measurement, subscriber privacy

ACM Reference Format:
Shiyue Nie[1], Yiming Zhang[1], Tao Wan[2], Haixin Duan[1,3]✉, Song Li[1]✉. 2022. Measuring the Deployment of 5G Security Enhancement. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '22), May 16–19, 2022, San Antonio, TX, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3507657.3528559

1 INTRODUCTION

5G is the latest mobile communication standard that has been globally deployed. By March 2021, more than 150 commercial 5G networks have been deployed worldwide, covering every region[2]. As the largest 5G market, three major operators in China have installed more than 1.3 million 5G base stations, serving 497 million 5G users[21]. The global deployment of 5G is still accelerating.

At a time when 5G cellular networks are showing explosive growth, 5G security is of particular importance. Prior generations of mobile communication systems are known to be subject to a wide variety of attacks. In the early 2G network, User Equipment (UE) is subject to False Base Station (FBS) attacks such as communication hijacking and location tracking, primarily due to the lack of mutual authentication between UE and the network and the use of weak encryption algorithms. In 3G and 4G networks, security has been gradually improved, but many attacks are still possible, such as Man-In-The-Middle (MITM) [10, 13, 17, 18] and DoS attack [9, 15, 19, 22, 23]. These attacks are mainly due to the lack of protection for subscriber identity and initial control messages. In 5G systems, a series of new specifications, primarily TS 33.501[1], have been developed to further enhance 5G security.

However, not all security enhancements in 3GPP specifications can meet their prospects in reality. The reasons are: (1) many provisions in the security standards are optional to deploy rather than mandatory, allowing operators to ignore them; (2) even for mandatory security provisions, stakeholders may skip them for practical reasons, such as performance, cost, compatibility, etc.

Prior work[4, 7, 12, 16] showed that non-compliant implementations of security features would make the protection ineffective in 4G and expose the network to risks. However, no studies have yet explored the implementation of 5G security enhancements. In this work, we aim to fill this gap by answering three questions: *What are the key security features of 5G? How can their deployment be measured? Does the current commercial network meet the requirements (safer than prior networks)?*

Our study focuses on 5G security features over the New Radio (NR) interface. Core network related features are not considered, as they could not be easily measured and also not easily exploited by attackers. Specifically, we performed a measurement of the commercial 5G network in China to verify its security compliance with 3GPP specifications. Based on the 5G security specifications, we systematically analyzed the 5G security features in three aspects: confidentiality and integrity protection, subscriber identifier protection, and initial NAS message protection. Using 5G commercial handsets and special tools capable of intercepting signaling messages, our measurement covered three popular network operators in China. Our testing results show that the enhanced security mechanisms in 5G specifications are not fully deployed in the current commercial 5G networks in terms of (1) UP data protection, (2) user identity protection and (3) initial NAS message encryption. 5G subscribers are still exposed to risks such as user data leakage, identity privacy stealing, tracking, and DoS attacks. To summarize, this paper makes the following contributions:

- We present a comprehensive study on the new security features of 5G networks over the NR interface. We extract and concisely summarize the security enhancements and their

WiSec '22, May 16–19, 2022, San Antonio, TX, USA

ACM ISBN 978-1-4503-9216-7/22/05…$15.00
https://doi.org/10.1145/3507657.3528559

corresponding deployment requirements from the complex 5G standards.

- To the best of our knowledge, this work performs the first evaluation of the commercial 5G networks by collecting and decoding signaling messages interacting between 5G UEs and the 5G network.
- We discover several deployment vulnerabilities of commercial 5G networks in terms of user data protection and subscriber privacy protection, which would lead to attacks as user data leakage, location tracking, and DoS.

2 5G BACKGROUND

In this section, we present the 5G network architecture and signaling interaction flow to facilitate understanding of our work.

2.1 5G Network Architecture

A cellular network consists of User Equipment (UE), Radio Access Network (RAN), and Core Network (CN).

UE: A UE consists of mobile equipment(ME) and a Universal Subscriber Identity Module (USIM) issued by a network operator. USIM is used to store subscriber identification information, such as the Subscriber Permannent Identifier (SUPI) in 5G, root key, and public keys shared with the network operator.

RAN: A RAN consists of several base stations (e.g., g-NodeBs/gNBs in 5G) that allocate radio resources for the UE to access the cellular network via radio interfaces. After establishing the Radio Resource Control(RRC) layer connection, the UE can continue to establish a NAS connection to interact with the network at the service level.

CN: The core network in 5G consists of a number of network functions including the Access and Mobility Management Function (AMF), the Authentication Server Function (AUSF), the Unified Data Management (UDM), the Session Management Function (SMF) and the User Plane Function (UPF), among others.

Non-Stand Alone (NSA) architecture and Stand-Alone (SA) architectures currently coexist in 5G networks. NSA is also referred to as "E-UTRA-NR Dual Connectivity" (ENDC). The main difference between NSA and SA is that NSA anchors the control signaling of 5G Radio Networks to the 4G Core, while the SA scheme connects the 5G Radio directly to the 5G core network. This paper focuses on pure 5G security deployment in SA mode (the network architecture is shown in Figure 1).

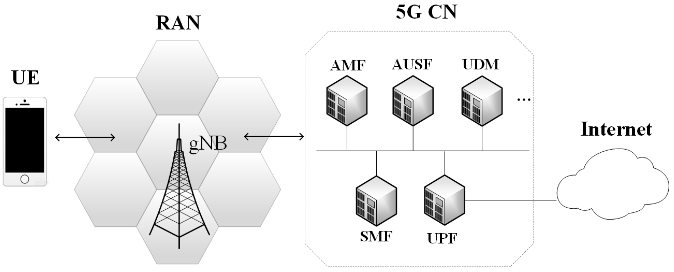

Figure 1: 5G network architecture in SA mode.

2.2 5G Signal Exchange Flow

Figure 2 illustrates the basic message exchange flow in several critical procedures in 5G. When a UE accesses the 5G system, it first sends a registration request to the core network, which contains its subscriber identifier (5G Globally Unique Temporary Identifier, i.e., 5G-GUTI, or Subscription Concealed Identifier, i.e., SUCI). Then the subscriber identification procedure may be invoked by the CN when the UE cannot be identified by a temporary identity (5G-GUTI). Subsequently, the Authentication and Key Agreement (AKA) procedure mutually authenticates the user and the network. The Security Mode Command(SMC) procedure accomplishes the activation of security in the NAS layer and RRC layer. Finally, the CN sends a registration accept message to indicate a successful registration, after which the UE can perform services like calling, texting, and Internet access. The relationship between the 5G security features studied in this work and the procedures/messages they involved is colored in Figure 2. Details will be described in the next section.

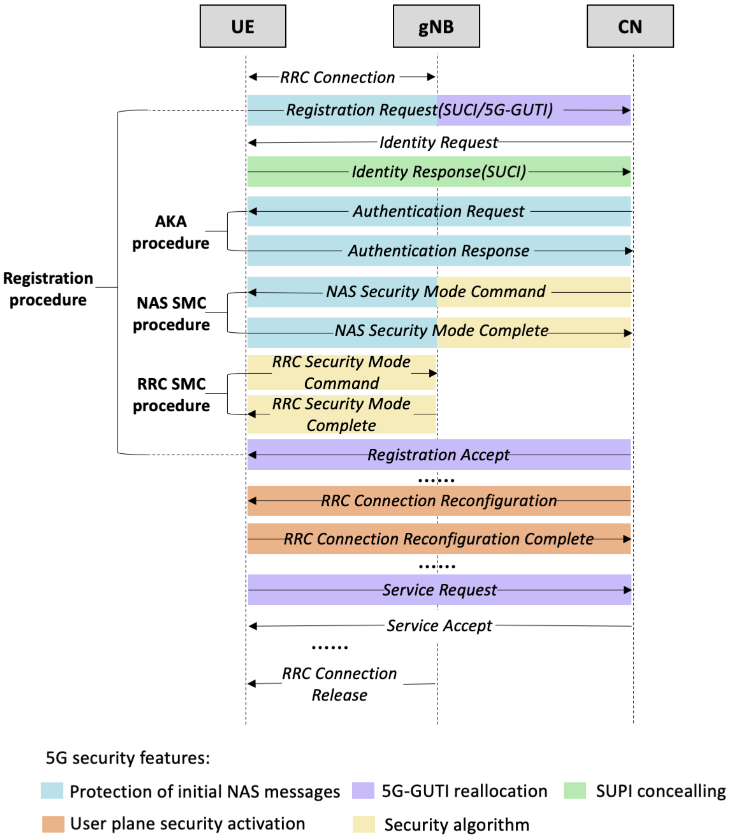

Figure 2: 5G signal exchange flow.

3 SECURITY FEATURES IN 5G

In this section, we provide a comprehensive overview of the new 5G security features introduced in 3GPP specifications (see Table 1), with a focus on the security of the access network.

3.1 Confidentiality and Integrity Protection

3.1.1 Crypto Algorithms. 5G crypto algorithms for confidentiality and integrity protection are named NR Encryption Algorithm (NEA) and NR Integrity Algorithm (NIA) respectively. NEA/NIA algorithms include NEA0/NIA0 (no crypto protection), NEA1/NIA1 (SNOW 3G), NEA2/NIA2 (AES), and NEA3/NIA3 (ZUC). According

Table 1: An overview on 5G security features

Issues	4G	5G Security Enhancements	Mitigated Security Threats	Refrences
Confidentiality and Integrity Protection	128-bit algorithms supported	256-bit algorithms supported	−−	TS 33.501 5.2.2, 5.2.3, 5.3.2, 5.3.3, 5.5.1, 5.5.2
	support control layer encryption and integrity protection, as well as user plane encryption	in addition to 4G security, mandatory support for UP integrity protection	unauthorized disclosure and tampering of user data	TS 33.501 6.6.1, 6.6.2 TS 38.331 5.3.5, 6.3.2 TR 33.853
Subscriber Privacy	subscriber Identifier sent in plaintext	SUPI concealment	imsi-catcher, location exposure, user tracking	TS 33.501 5.2.5, 6.12.2, 6.12.4 TS 23.003 2.2
	does not specify guidelines for when and how to update the temporary identity(GUTI)	well-defined timing of 5G-GUTI redistribution		TS 33.501 6.12.3 TS 23.003 2.10
NAS Security	initial NAS messages are not encrypted	protecting the confidentiality of the initial NAS messages between the UE and the network	spoofing networks, message hijacking, DoS attacks	TS 33.501 6.4.6 TS 24.501 4.4.6

to 3GPP TS 33.501, the UE/gNB/AMF shall at least support the first three algorithms, while the fourth (NEA3/NIA3) is optional.

3.1.2 Control Plane Protection. Based on 3GPP TS 33.501, integrity protection is mandatory to be both supported (by products) and used (by operators) for control plane including both RRC and NAS signaling. Confidentiality is mandatory to be supported (by products) but optional to use (by operators).

3.1.3 User Plane Protection. In 5G systems, the user-plane and control-plane are rigorously separated, enabling independent enhancement of functionality in each plane, and facilitating to sink the UP closer to users to reduce network latency. Although 4G supports confidentiality and integrity protection of RRC and NAS messages, it lacks integrity protection of UP due to perceived performance overhead on devices. In comparison, as a new security feature, 5G mandates the support of both confidentiality and integrity protection for UP by UE and gNB. However, both UP confidentiality and integrity protection are optional to use by the network operator.

The protection of user-plane in 5G is signalled from SMF to gNB and then from gNB to UE. More specifically, (1) SMF to gNB: The SMF shall provide UP security policy to the gNB to indicate whether UP confidentiality and/or UP integrity protection shall be activated or not for all each Data Radio Bearers(DRBs) in the Packet Data Unit(PDU) session, and the gNB shall not overrule the policy provided by the SMF; (2) gNB to UE: according to the UP security policy received, the gNB shall send the RRC Connection Reconfiguration message to the UE for UP security activation, indicating the activation of UP integrity protection and ciphering for each DRB.

3.2 Protection of Subscriber Identifiers

3.2.1 SUPI Concealing. In a cellular communication system, each subscriber has a unique and permanent identifier to distinguish them from each other. As for GSM/UMTS/EPS systems, a unique International Mobile Subscription Identity (IMSI) is allocated to each mobile subscriber. The feature of IMSI being transmitted in clear text over the air interface causes it to be easily intercepted by FBSs or stingrays (also called IMSI-Catchers) to facilitate attacks such as locating, tracking and signal hijacking. 5G addresses this vulnerability by various optimizations, among which the most important is the concealed subscriber identifier.

In 5G, the globally unique long-term subscription identifier is called SUPI. The SUCI is a privacy-preserving identifier containing the concealed SUPI. The UE generates SUCI using a protection scheme with the raw public key securely provisioned under the control of the home network. To support 5G protection of subscriber identity, the public key and the protection mechanism identifier need to be stored in the USIM. Otherwise, the ME will select the "null-scheme" mechanism, at which point SUPI will not be discreetly protected. As clarified in the TS33.501, the UE shall only generate a SUCI using "null-scheme" in the following three cases:

- if the UE is making an unauthenticated emergency session and it does not have a 5G-GUTI to the chosen network.
- if the home network has configured "null-scheme" to be used.
- if the home network has not provisioned the public key needed to generate a SUCI.

3.2.2 5G-GUTI Reallocation. In addition to encrypting the permanent user identifiers, mobile networks also prevent privacy breaches by assigning temporary unique identifiers to subscribers, such as Temporary Mobile Subscriber Identity (TMSI) in 2G/3G, and GUTI in 4G/5G. These temporary identifiers would be changed frequently, and used for identification before establishing a secure channel. This mechanism increases the difficulty for attackers to identify or track mobile users, thus providing a better protection of user privacy. However, no specific requirements of updating temporary identifiers have been imposed in 4G standards, and mobile operators have also been reported to update GUTI infrequently[7], resulting in inefficient protection of user privacy. As an enhancement, 5G provides clear specifications of the timing to re-allocate 5G-GUTI in TS33.501, including:

- Upon receiving Registration Request message of "initial registration" or "mobility registration update" from a UE.
- Upon receiving Registration Request message of "periodic registration update" from a UE.
- Upon receiving Service Request message sent by the UE in the response to a Paging message.

3.3 Protection of Initial NAS Messages

In 4G systems, all initial NAS messages are not encrypted, as encrypted initial NAS messages cannot be decrypted by the Mobility Management Entity(MME). In contrast, 5G systems encrypt the complete initial NAS message in the NAS container. Although the encrypted messages may not be decrypted by the AMF, the AMF can request the UE to resend the initial NAS message after authentication. This is where the security resides: the complete initial NAS message is sent to the AMF only after the security context is established, thus preventing fake networks from hijacking the non-encrypted initial NAS messages and sending fake NAS rejection messages to the UE, which could lead to DoS attacks.

Specifically, in 5G systems, the initial NAS message is the first NAS message sent to the AMF after the UE transitions from the idle state. If the UE does not have a NAS security context, the initial NAS message contains only the plaintext IE, i.e., subscription identifier, UE security capability, ngKSI, etc. If the UE has a security context, the full initial NAS message encrypted in the NAS message container shall be included additionally. If the AMF does not have the same security context from the local or last accessed AMF, it could not decrypt the NAS message container. Then the AMF needs to authenticate with the UE and sends the initial NAS message request identifier. The UE should then reply with a NAS Security Mode Complete message containing the full encrypted initial NAS message. It is only after the above process that the AMF responds to the initial NAS message.

4 MEASUREMENT METHODOLOGY

In this section, we introduce the various components of the measurement experiment.

5G networks. We tested commercial 5G networks of three mobile operators in China, termed as Operators A, B, and C. Collectively, they serve hundreds of millions of 5G subscribers.

Test tools. The experiment was conducted by Pilot Pioneer[6], a commercial 5G radio testing software. The software runs on a nuc host which is connected to the UE through the USB debugging port. It is capable of monitoring and decoding UE-side 5G signaling at the control layer in real-time. The data logs could be captured and stored for offline analysis. The software also provides the functionality to customize test templates, which enables us to automate multiple test cases in a configured order. As for the test UE, we choose one mainstream 5G smartphone, Samsung S20, and test it with commercial 5G sim cards from operators A, B, and C respectively.

Location. We perform our measurement in Beijing - one of the first cities in the world to deploy commercial 5G networks. Before the main test, we first investigate whether the network architecture of 5G would differ between different locations in Beijing. Two typical locations are selected: (1) the urban center, where 5G base stations are well built; (2) the urban edge, where few 5G base stations are deployed and signals are less stable relatively. The results show that in the city center, 5G is always in NR mode. While at the urban edge, the UE would first connect to the NR network during the initial registration phase, and switch to ENDC once the registration has been completed, which means that the 5G network at that area is NSA mode. We then perform the security enhancement measurement at both locations separately. However, at least for the three operators we choose, their deployment status of NR security policies are found with no difference in these two locations.

Dataset. The 5G signaling collection experiments were conducted three times a day, in the morning, afternoon, and evening, lasting for three days (two working days and one rest day). In each experiment, we would (1) trigger an average of about 30 registration procedures, (2) send about 20 SMS messages during the RRC idle phase, and (3) make 5 phone calls. Data collections for three operators were carried out independently, taking about one hour each time. All signaling data sent and received by the test UE would be captured for analysis.

Table 2: Crypto algorithms in 5G commercial networks

	NAS		RRC	
Operator A	NEA 0	NIA 2	NEA 2	NIA 2
Operator B	NEA 0	NIA 1	NEA 2	NIA 2
Operator C	NEA 1	NIA 2	NEA 2	NIA 2

Methodology. We performed (1) signaling-specific analysis, and (2) scenario-specific analysis based on the collected dataset. Specifically, we analyzed critical signaling messages that interacted between handsets and networks, including: Security Mode Command message for the selection of security algorithms, RRC Connection Reconfiguration message for UP security activation status, Identity Response for SUPI concealing, Registration accept for 5G-GUTI reallocation and Registration request for the protection of initial NAS message.

In addition, as the reallocation of 5G-GUTI needs to be triggered under certain conditions, we performed a statistical analysis of the 5G-GUTI values in different scenarios. According to specifications, 5G-GUTI should be refreshed after (1) UE's registration to the network and (2) UE sending a service request message in response to a paging message. For the former, we configured the UE to automatically register and deregister to the network at an average frequency of 30 times per hour by our test tool. For the latter, we continuously sent Short Messaging Service(SMS) messages (about 20 times in 1 hour) to the test UE, triggering it to send Service Request messages to the network. The changes of 5G-GUTI during the above processes would be used to evaluated the implementation of reallocation.

5 RESULT ANALYSIS

In this section, we analyze the experimental results and discuss the deployment status of commercial 5G networks .

5.1 Crypto Algorithms

The crypto algorithms configured by each operator during the SMC process are summarized in Table 2. It could be seen that, the support of crypto algorithms in all three 5G networks is basically compliant with 3GPP specifications, both for RRC and NAS. Specifically, all three operators support integrity protection of signaling data (via NIA1 or NIA2). The only absence is the protection for NAS of operator A and B, but it is still compatible as confidentiality protection is specified as optional. However, the lack of confidentiality protection would lead to the interception of status and authorization data between the UE and gNB/AMF, posing risks of attacks such as location tracking[8]. Therefore, the implementations of operator A and B are compliant but unsafe (marked as red in Table 2).

5.2 UP Protection

According to the mechanism of UP protection, the activation of protection is performed by the gNB sending RRC Connection Reconfiguration messages to the UE. Therefore, we carefully analyzed each field in RRC messages to clarify whether it is used for user-level security. Finally, we found two key fields used to reconfigure Packet Data Convergence Protocol(PDCP) for additional encryption and integrity protection, which are:

- `cipheringDisabled`, indicates whether cyphering is disabled for this DRB. Note that this field only appears when the UE is connected to 5G CN. Otherwise, it is absent.
- `intergrityProtection`, indicates whether integrity protection is configured for this radio bearer.

We examined the states and values of the above two fields in each operator's signaling flow. The results show that operators B and C do not have UP confidentiality protection activated, and all three operators do not support integrity protection. It suggests that 5G operators may have no robust security initiatives to enhance user-plane security, which makes data vulnerable to interception and may lead to malicious alteration of user data[10].

5.3 SUPI Concealing

Unfortunately, all three operators use SUCI with Null-scheme in identity responses, i.e., the unique and permanent subscriber identifier is transmitted in clear text on the air interface without any protection. Therefore, in the commercial 5G networks we tested, an attacker could still disguise as a fake base station and send identity requests to the targeted UE and steal its subscriber identity information for further attacks such as location tracking. As we performed the tests by 5G SIM cards, the results indicate that all the three operators either fail to configure their 5G SIMs with cipher suites for SUPI protection, or their networks are not enabled for SUPI concealing. In any case, their implementations are insecure to protect the most important subscriber identifier.

5.4 5G-GUTI Reallocation

In previous generations of networks, untimely updates of temporary user identifications rendered their privacy protection null and void, which triggers a security threat that can expose a victim's location[9, 14]. To prevent such failures, 5G standards set out explicit requirements on the timing of the temporary user identification reallocation. However, our measurement results show that commercial 5G networks do not strictly adhere to the standards, only updating the temporary identity after registrations while not after sending service requests.

The 5G-GUTI consists of Globally Unique AMF Identifier (GUAMI) and 5G-TMSI. As GUAMI (MCC, MNC, AMF Identifier) can be considered as constant, in this work, we only focused on the value of 5G-TMSI (32-bit). Based on the collected signaling messages, we found that each time the UE sends a registration request and activates the NAS security through SMC procedure, a new 5G-GUTI would be allocated via the DLinformation transfer message or Registration accept message(see Table 3 for an example). According to hundreds of repeated registration tests per day, we found that all three operators have sufficiently randomized the reallocated GUTIs, with no obvious patterns or fixed values identified. In short, during the procedure of registration, 5G-GUTI has been implemented with compliant reallocation.

According to the 5G security specification, 5G-GUTI should also be reallocated after the core network receives a Service Request message from the UE in response to paging messages. However, our results show that the 5G-TMSI value is not refreshed in the above scenario in all the three tested networks. Then we tried to figure out how long the value of 5G-GUTI would be maintained due to this implementation vulnerability. Unfortunately, we found that after a UE is registered to the network, the GUTI would not be updated as long as the subscriber does not make a call or switch networks for re-registrations. Previous studies [14] have confirmed that, if the temporary identifier remains unchanged, an attacker with prior knowledge of the victim's phone number could obtain an exact mapping between the temporary identifier and the phone number, and then track the victim's location. Such attacks require only a few (usually 2 or 3) spam messages to be sent to the target UE and sniffing to the public wireless channel.

5.5 Protection of Initial NAS Messages

When measuring the deployment of initial NAS message protection mechanisms in commercial networks, we focused on: (1) What is the specific signaling interaction flow between UE and AMF in commercial networks, and is it consistent with the 5G specification? (2) How are the initial NAS message encrypted?

As for the signaling interaction flow, all three operators performed the retransmission mechanism of the initial NAS message after authentication, which is compatible with the security standard. Further, we carefully investigated the encryption of the initial NAS messages. Basically, the initial NAS message is a registration request message or service request. When a phone with a security context sends a registration request to the network, the NAS message contains not only plaintext IEs (i.e., subscriber identifier), but also a NAS message container. Notably, 5G requires the NAS container to be encrypted for protection. However, the measurement results showed that Operators A and B just transmit the NAS container in plaintext. Only Operator C strictly encrypted the NAS message container. Obviously, the non-compliant implementation of Operators A and B would lead to certain security risks - when the content of the NAS message container is not protected, in addition to user-side information such as 5GS mobile identity, other sensitive information such as 5GMM capabilitity can also be leaked, posing the risk of fake network and DoS attacks[24].

6 DISCUSSION

Ethical Considerations. Our experiment only passively collects cellular signals and analyzes security features, and does not actively send out any jamming signals. Therefore, the real cellular networks or other users would not be affected. We have reported these vulnerabilities to the China National Vulnerability Database (CNVD), and expect to contact with the three operators via this institution. We've also present our findings to the GSM Association (GSMA) for mitigation. They responded that they will engage with all three of the Chinese network operators to discuss our findings.

Related Work. Academic research on 5G security is at an early stage. Most existed works focus on survey study[11], formal analysis[3, 25], and proof-of-concept attack discussions[5, 20]. They either look for programmatic vulnerabilities in 5G simulation platforms, or analyze 5G protocol issues on a theoretical level only. Instead, this work is concerned on the security features of commercial 5G networks, which has stronger real-world impact.

Table 3: 5G-GUTI fields in the registration message: 5G-TMSI is redistributed in adjacent registration messages

	Length-of-5GS-Mobile -Identity-Contents	Type-of -Identity	MCC	MNC	AMF-RegionID	AMF-SetID	AMF-Pointer	5G-TMSI
Registration Request	11	2	460	1	1	0	1	774A710D
Registration Accept	11	2	460	1	1	0	1	A0BC4A70

Table 4: Summary of commercial 5G measurements

Operators:		A	B	C
Security Algorithm Selection	NAS Confidentiality Protection	-	-	✓
	NAS Integrity Protection	✓	✓	✓
	AS Confidentiality Protection	✓	✓	✓
	AS Integrity Protection	✓	✓	✓
UP Security Activation	Ciphering Protection	✓	-	-
	Integrity Protection	-	-	-
SUPI Concealing		-	-	-
5G-GUTI Reallocation	After Registration	✓	✓	✓
	After Service Request	-	-	-
Initial NAS Message Protection		-	-	✓

- : vulnerable configuration

Besides, prior work on LTE networks[4, 7, 12, 16] also inspires our study. [7] evaluated the implementation of GUTI reallocation mechanism in the LTE network. [4] tested the security algorithm selection in LTE network and exposed multiple cases of misconfiguration. [12] presented a systematical approach for detecting implementation flaws, leading to 36 vulnerabilities in phones and network components. In contrast, we focus on 5G NR implementation, which is relatively nascent and more complicated.

7 CONCLUSION

This paper measures the security of commercial 5G deployment, especially the implementation of new 5G security features (see Table 4 for a summary). By collecting and analyzing the signaling messages transmitted over 5G air interface, we found insecure configurations in 5G networks in terms of user privacy protection and user data protection. We strongly recommend 3GPP to further strengthen its security requirements by changing important security features such as UP integrity protection and SUPI concealment from optional to mandatory to use. We also recommend operators to adopt stronger security policies by implementing some important optional security features and also fix the deployment flaws discovered in this paper to create a more secure 5G network environment.

ACKNOWLEDGEMENT

We thank the anonymous reviewers for their valuable comments to help improve this paper. This work was supported in part by the National Natural Science Foundation of China (U1836213, U19B2034).

REFERENCES

[1] 3GPP. 2022. *Security architecture and procedures for 5G System*. Technical Standard (TS) 33.501. 3rd Generation Partnership Project (3GPP). Version 16.9.0.

[2] GSM Association. [n.d.]. The Mobile Economy 2021. https://www.gsma.com/mobileeconomy/wp-content/uploads/2021/07/GSMA_MobileEconomy2021_3.pdf.

[3] David A. Basin, Jannik Dreier, Lucca Hirschi, Sasa Radomirovic, Ralf Sasse, and Vincent Stettler. 2018. Formal Analysis of 5G Authentication. *CoRR* abs/1806.10360 (2018). arXiv:1806.10360 http://arxiv.org/abs/1806.10360

[4] 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

[5] Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz. 2021. 5G SUCI-Catchers: Still catching them all? (2021).

[6] Ltd. DingLi Corp. [n.d.]. *Pilot Pioneer - The specialized field test solution for directed radio access network troubleshooting and optimization.* https://www.dingli.com/PilotPioneer.php

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

[8] 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.

[9] Lin Huang. 2016. Forcing Targeted LTE Cellphone into Unsafe Network. In *HITB AMS Security Conference*.

[10] 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*.

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

[12] 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)*. 1153–1168. https://doi.org/10.1109/SP.2019.00038

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

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

[15] Stig F Mjølsnes 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] David Rupprecht, Kai Jansen, and Christina Pöpper. 2016. Putting LTE Security Functions to the Test: A Framework to Evaluate Implementation Correctness. In *10th USENIX Workshop on Offensive Technologies (WOOT 16)*. USENIX Association, Austin, TX. https://www.usenix.org/conference/woot16/workshop-program/presentation/rupprecht

[17] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2020. IMP4GT: IMPersonation Attacks in 4G NeTworks.. In *NDSS*.

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

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

[20] Vui Huang Tea. 2020. Unmasking Concealed 5G Privacy Identity with Machine Learning and GPU in 12 mins. https://doi.org/10.36227/techrxiv.13187636.v1

[21] Juan Pedro Tomás. [n.d.]. *China reaches over 1.3 million 5G base stations nationwide: Report.* https://www.rcrwireless.com/20211227/5g/china-reaches-over-million-5g-base-stations-nationwide-report

[22] Guan-Hua Tu, Chi-Yu Li, Chunyi Peng, and Songwu Lu. 2015. How voice call technology poses security threats in 4G LTE networks. In *2015 IEEE Conference on Communications and Network Security (CNS)*. 442–450. https://doi.org/10.1109/CNS.2015.7346856

[23] Chuan Yu, Shuhui Chen, and Zhiping Cai. 2019. Lte phone number catcher: A practical attack against mobile privacy. *Security and Communication Networks* 2019 (2019).

[24] Chuan Yu, Shuhui Chen, Fei Wang, and Ziling Wei. 2021. Improving 4G/5G air interface security: A survey of existing attacks on different LTE layers. *Computer Networks* 201 (2021), 108532. https://doi.org/10.1016/j.comnet.2021.108532

[25] J. Zhang, L. Yang, W. Cao, and Q. Wang. 2020. Formal Analysis of 5G EAP-TLS Authentication Protocol Using ProVerif. *IEEE Access* PP, 99 (2020), 1–1.