

Research Article

Security Threats to Voice Services in 5G Standalone Networks

Zhiwei Cui ¹, Baojiang Cui ¹, Junsong Fu ¹, and Renhai Dong ²

¹The School of Cyberspace Security and National Engineering Lab for Mobile Network Technology, Beijing University of Posts and Telecommunications, Beijing, China

²The School of Computer Science (National Pilot Software Engineering School), Beijing University of Posts and Telecommunications, Beijing, China

Correspondence should be addressed to Baojiang Cui; cuibj@bupt.edu.cn

Received 19 April 2022; Accepted 27 July 2022; Published 4 September 2022

Academic Editor: Marimuthu Karupiah

Copyright © 2022 Zhiwei Cui et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

With the rapid development of 5G SA (standalone) networks, increasing subscribers are motivated to make calls through 5G. To support voice services critical to mobile users, 5G SA networks adopt two solutions: VoNR (Voice Over New Radio) and EPS (Evolved Packet System) fallback. At this stage, 5G SA networks provide voice services through EPS fallback, which leverages 4G networks to support voice calls for 5G users. This switch between cellular network systems may expose vulnerabilities to adversaries. However, there is a lack of security research on voice services in the 5G SA network. In this paper, we analyze the security of EPS fallback and its closely related IMS from the perspective of the protocol and the practices of the carriers. We uncover two protocol design vulnerabilities and two implementation flaws. In addition, we exploit them to design three attacks: voice DoS, voice monitoring, and SMS spoofing and interception. We validated these vulnerabilities and attacks using SDR (software-defined radio) tools and a set of open-source software in three mobile carriers. Our analysis reveals that the problems stem from both specifications and carrier networks. We finally propose several potential countermeasures to defend these attacks.

1. Introduction

5G has been rapidly developing in recent years. As 5G can provide higher bandwidth, faster speeds, and on-demand services, increasing subscribers are motivated to choose 5G networks. Nearly half of mobile subscribers will use the 5G network by 2027 [1]. 5G is designed to gradually phase out the current networks, such as 3G and 4G networks. To support voice services critical to mobile users and operators, 5G SA networks adopt two solutions: VoNR and EPS fallback. VoNR supports voice calls directly in the 5G system and is the IMS (IP Multimedia System) based voice service based on 5G access. In contrast, EPS fallback transfers the voice request from the 5G network to the 4G system when a call is made. Then the 4G networks use IMS-based VoLTE (voice over LTE) to provide voice services.

VoNR is the target solution for voice services in the 5G SA network. However, it is currently in the initial stage of 5G network construction, and VoNR has not yet been commercialized due to factors such as network coverage and

technology. At the current stage, the 5G SA network uses EPS fallback to provide voice services. And even if VoNR is commercialized in the future, there will be many mobile phones that do not support VoNR, and they still have to use EPS fallback to complete voice services. Under the premise of adopting EPS fallback, 2G/3G is needed to ensure voice service if 4G cannot provide voice services due to some reasons, such as turning off VoLTE (voice over LTE) and poor signal coverage. Voice services are essential to users. If the voice services are attacked, users' privacy is jeopardized. Therefore, considering the importance of voice services and the complexity of the initial 5G voice solution, it is necessary to study the security of 5G voice services.

Recently, there have been some exploratory studies on the security of voice services in cellular networks. The IMS-based voice services in 4G networks have been pointed out to be vulnerable due to unsafe implementation [2–4]. The authors in the work [5] analyze security issues on voice services of the 5G NSA (non-standalone) network system. As the 5G NSA network is using the 4G LTE core network,

they verified whether the vulnerabilities of 4G LTE are valid for the 5G NSA and presented countermeasures against the vulnerabilities. The work in [6] also carried out similar tests on the security of voice services in 5G NSA networks. However, to the best of our knowledge, there is a lack of security research on 5G voice services in the 5G SA network. Our work studies the security of voice services in 5G SA networks from the perspective of the protocol and the practices of the carriers as a complement to this research area.

In this paper, we have analyzed the standards of EPS fallback and verified the current voice solutions under the 5G SA network of three operators through experiments. We find that these operators all adopt EPS fallback to provide voice services. This solution means that mobile users will fall back to the 4G network when consuming voice services. Although the 5G standard defines relevant security measures to mitigate downgrade attacks, this kind of voice solution naturally introduces the risk of downgrade attacks. In addition, we have performed security analysis on the authentication protocol and implementation of IMS, which is closely related to EPS fallback. First, we analyze the possible problems in the implementation of the operators' IMS server and identify two vulnerabilities, one of which is new. Second, we find a flaw in the protocol design after careful analysis of the standards of the IMS authentication protocol. Combining all the above vulnerabilities, we have designed three attacks: voice DoS (A1), voice monitoring (A2), and SMS (Short Message Service) spoofing and interception (A3). The first attack causes a DoS on the victim's voice service, and the last two attacks can be exploited to steal the victim's privacy. Table 1 summarizes our findings. We denote the three operators as OP-I, OP-II, and OP-III for the privacy concern. Note that our assumed attack model is relatively simple. The attacker has no control over the operators and can launch the first two attacks without knowing the victim's information. In addition, the attacker can carry out the third attack after getting the victim's mobile phone number. In conclusion, we analyze the causes of these problems and present several countermeasures against these vulnerabilities and attacks.

In more detail, our contributions are as follows:

- (i) We present a security study on the EPS fallback in 5G SA networks and discover a protocol flaw. Furthermore, we found a protocol vulnerability and two implementation vulnerabilities of IMS closely related to EPS fallback.
- (ii) We exploit the vulnerabilities to design three attacks and validate these attacks using SDR tools and a set of open-source software in three mobile carriers.
- (iii) We analyze the root causes of the vulnerabilities and propose several potential countermeasures to defend against attacks.

The rest of this paper is organized as follows: We summarize the related work in Section 2. Section 3 describes the preliminaries of the system model, IMS registration process, and EPS fallback that are relevant to the vulnerabilities and

TABLE 1: Summary of our findings on 5G voice service vulnerabilities and attacks.

Attack	OP-I	OP-II	OP-III	Vulnerability
A1	✓	✓	✓	EPS fallback
A2	✓	✓	✗	EPS fallback
A3	✗	✗	✓	EPS fallback, IMS server, IMS AKA

attacks. We present the threat model and experimental setup in Section 4. The security threats from IMS-Based voice services are discussed in Section 5. Then we design three attack scenarios as described in Section 6. Section 7 discusses the causes, advantages, and possible limitations of these attacks. Several countermeasures are presented in Section 8. We describe the future research challenges in Section 9. At last, Section 10 concludes this paper.

2. Related Work

We present the related work in the security areas of mobile networks, IMS-based voice services, and SMS, as summarized in Table 2.

Vulnerabilities in mobile networks have been found in some existing studies. 2G/GSM (Global System for Mobile Communications) is known to be plagued by authentication vulnerabilities, which allow the attacker to send spam messages and get the phone numbers of victims [7, 8]. While the introduction of the mutual authentication mechanism makes 3G/4G more secure, they suffer from shortcomings that enable the tracking of users [9–11]. Chlosta et al. demonstrated a proof-of-concept identification attack in a 5G standalone network [14]. Hussain et al. proposed a property-directed formal verification framework for the 5G network protocol in [15], and they have identified 11 design weaknesses, which can be exploited to break the security of 5G networks. Although the mobile network continues to evolve, the original insecure network will still take some time to be abandoned. Based on this, an attacker can force devices in the 3G/4G environment to downgrade to insecure 2G and exploit the authentication vulnerabilities to steal privacy [12, 13]. However, there are not many studies on downgrade attacks on 5G networks. Our recent work reveals the feasibility of the attack on 5G and complements this research field.

Several previous studies have exposed the security issues of IMS-based voice services. Tu et al. analyzed two voice solutions for the 4G network from a security perspective [2], which is similar to the work of this paper. Li et al. conducted the first study on the security of VoLTE and identified several vulnerabilities of the VoLTE device and network, which can be exploited to gain free data service and launch the DoS attack against VoLTE [3]. Kim et al. found similar vulnerabilities and proposed a caller spoofing attack [4]. Security issues of voice services in 5G NSA networks have been discussed in [5, 6]. Different from them, we focus on EPS fallback in 5G SA networks.

The security issues of SMS have been an active research area in recent years. There are many works [16–19] that focus

TABLE 2: Summary of the related work.

Area	Network	Attack
Mobile networks	2G/GSM	Send spam messages [7] Get the phone numbers [8]
	3G/4G	Location privacy leakage [9–11] Downgrade to GSM [12, 13]
	5G SA	Identification attack [14, 15]
		Speed up the battery consumption [2]
IMS-based voice services	4G	DoS attacks [2, 3] Gain free data service [3] Caller spoofing attack [4]
	5G NSA	Eavesdropping [5] Charging avoidance attack [6]
	2G/GSM	Spamming SMS [16–21]
	4G	SMS spoofing [22]

on the (in) security of CS-based SMS. The FBS (fake base station) has been exploited by criminals to send spamming SMS to mobile users [20]. The authors in the work [21] present the first characterization of the FBS spam ecosystem and provide new insights into mitigating spamming SMS. Guan-Hua Tu et al. studied the security vulnerabilities of IMS-based SMS services for the first time [22]. To the best of our knowledge, most of the vulnerabilities in [22] have been fixed. However, our work uncovers new vulnerabilities, which can be exploited to send and receive SMS impersonating the victim's identity.

3. Background

In this section, we briefly review the system model, IMS registration process, and EPS fallback that are relevant to the vulnerabilities and attacks discussed in this paper.

3.1. System Model. In this paper, we analyze the security of EPS fallback voice service in the 5G SA network. Therefore, the system model we studied is the network architecture supporting EPS fallback voice service. As shown in Figure 1, the system model involves mainly three entities: the RAN (radio access network), the core network, and IMS.

The major components of the RAN are base stations (5G: gNB, 4G: eNB), which provide the wireless network for UEs to access the core network. The 4G core network has three critical components: MME (Mobility Management Entity), HSS (Home Subscriber Server), and PGW (Packet Data Network Gateway). The important network elements of the 5G core network relevant to the discussion in this paper include AMF (Access and Mobility Management Function), UDM (Unified Data Management), and UPF (User Plane Function).

The MME and AMF provide mobility management for the UE and at the same time use the stored authentication credentials (5G: UDM, 4G: HSS) for mutual authentication with the UE. The UPF and the PGW bridge the core network and external networks, such as IMS. It is worth mentioning the N26 interface between the MME and the AMF, which is used for 4G and 5G interoperability. The EPS fallback involves this interface when switching networks.

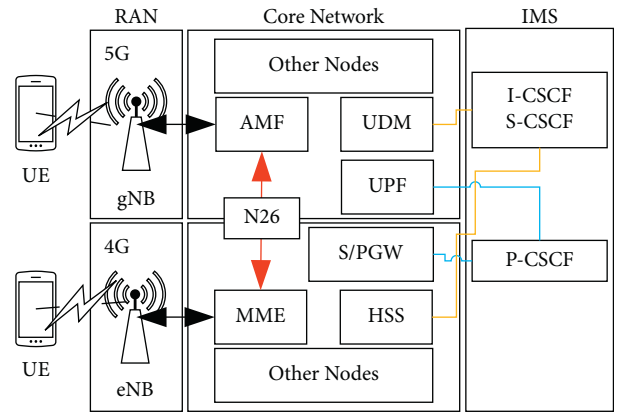


FIGURE 1: The system model supporting EPS fallback voice service.

The IMS is the standard solution for providing multimedia services in mobile networks. It changes voice and SMS from the traditional CS (circuit-switched) technology to the PS (packet-switched) design. Subscribers communicate with each other in the form of SMS or calls through IMS. The IMS has three main CSCF (Call Session Control Function) network elements: P-CSCF (Proxy-CSCF), I-CSCF (Interrogating-CSCF), and S-CSCF (Serving CSCF). The P-CSCF is the entry point for a UE to request services provided by an IMS server. The I-CSCF is responsible for querying and locating the S-CSCF. The S-CSCF handles user registration and services, and it requests the user's authentication data from the UDM or HSS.

From the system model, we can easily get the problems that need to be studied. First, EPS fallback voice service involves network switching. If the protocol is not secure, this mechanism may cause security problems. Second, it is worth exploring whether there are vulnerabilities in the implementation of IMS involved in voice services. Next, we will introduce the process of registering with IMS and the EPS fallback in detail.

3.2. IMS Registration Process. Figure 2 describes the process of registering to IMS. As defined in the 3GPP (3rd Generation Partnership Project) specification, mobile users need to carry out two mutual authentication steps to consume the

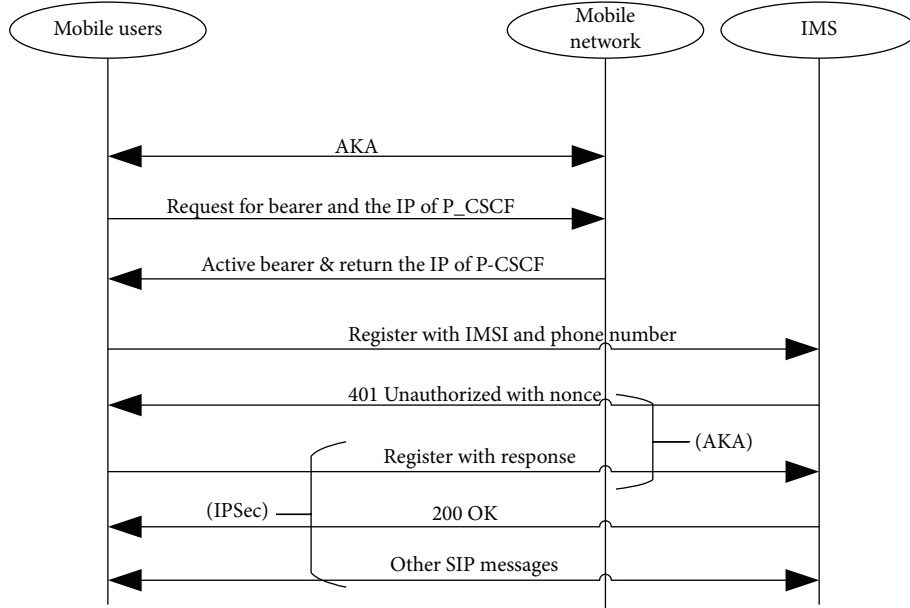


FIGURE 2: The process of registering to IMS.

multimedia services provided by IMS. The two mutual authentication steps use the same root key and similar AKA (Authentication and Key Agreement) algorithms. AKA uses the “question/answer” mode to realize the mutual authentication between the user and the network and can negotiate keys to ensure the confidentiality and integrity of subsequent communications. The IMS server uses the keys generated through negotiation required by IPSec to provide security protection for subsequent communications. First, the user and the mobile network complete mutual authentication. If the authentication is successful, the mobile network establishes a bearer between the user and IMS and returns the IP of P-CSCF to the user. Then the user sends a registration message with IMSI and phone number to the IMS server and will receive a 401 Unauthorized message containing nonce as the question of AKA. After parsing the nonce from the message, the user uses the AKA algorithm to calculate the response and generate the keys required by IPSec to provide security protection for SIP messages. Then, the user uses SIP messages protected by IPSec to complete the subsequent interaction and then consumes the services provided by IMS. It is worth mentioning that the authentication mechanism of IMS follows the principles and core algorithms of 3G AKA.

3.3. EPS Fallback. EPS fallback is a key enabling technology for 5G SA networks to provide voice services, regardless of whether VoNR is widely commercialized or not. EPS fallback chooses to switch or redirect to EPS based on the existence of the N26 interface [23]. Figure 3 describes the EPS fallback procedure for IMS voice in the Appendix. EPS fallback has the following steps:

- (1) UE registers to the 5G system and initiates the establishment of the IMS voice session.
- (2) The NG-RAN (NG Radio Access Network) receives a PDU (Packet Data Unit) session modification

request initiated by the network to set up QoS flow for IMS voice.

- (3) Taking into account UE capability, N26 availability configuration, and LTE radio conditions, the NG-RAN is configured to support EPS fallback and decides to trigger the fallback to EPS.
- (4) The NG-RAN denies PDU session modification requests.
- (5) The NG-RAN initiates handover or redirection to EPS based on terminal capacity and deployment.
- (6) In the case of handover via the N26 interface, the UE initiates the TAU (tracking area update) procedure. If there is no N26 interface, UE will be redirected to EPS and initiate the attach process with request type “handover.”
- (7) After the network initiates PDN connection modification to set up a dedicated bearer for voice, UE can consume voice services.

4. Threat Model and Experimental Setup

In this section, we introduce a threat model and an experimental setup. First, we present the threat model, which describes the attacker’s capabilities and security assumptions. Next, we build the experimental setup, which is exploited for vulnerability and attack verification.

4.1. Threat Model. The victims are mobile users who have connected to the 5G network. The moment they consume voice services is the moment they are attacked. The attacker has full knowledge of mobile networks, including 2G, 3G, LTE, and 5G. In addition, the attacker should have basic programming skills. We assume that the attacker is near the victim and the attacker does not need to know any information about the victim.

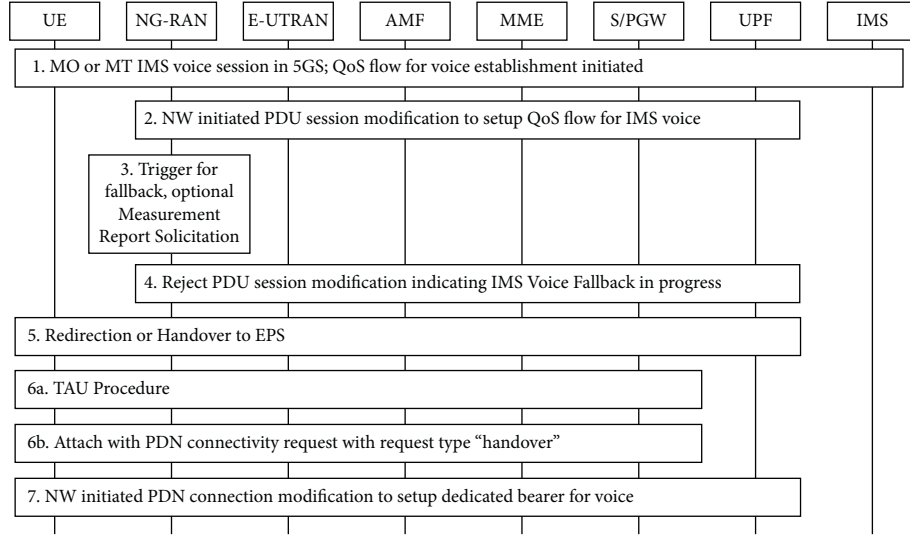


FIGURE 3: The procedure of EPS fallback [23].

The attacker can silently sniff over air interfaces and get some parameters of the operator's 2G, 3G, and LTE networks. In addition, the attacker can establish an FBS and a malicious UE. The most important is that the attacker is able to change some parameters to play as real operators. For example, the attacker can adjust the LTE FBS's frequency band, PLMN (Public Land Mobile Network) number, and TAC (Tracking Area Code) to be consistent with the operator. Mobile phones tend to select the base station with the strongest signal to access, and the signal strength of the FBS is generally greater than that of the legitimate base station nearby. Therefore, the victim's phone will choose to access the FBS.

We keep in mind that some vulnerability validations and attack evaluations may affect operators and mobile users. Therefore, we adopted two measures to conduct this research in a responsible manner. First, we only use our mobile phones as victims. Second, we reduce the power of the fake base stations and perform experiments in an environment that shields wireless signals to reduce the impact on other mobile users.

4.2. Experimental Setup. Software-defined radio is a system for wireless communication where the components are implemented completely by software. Traditional communication system equipment needs to be realized with expensive proprietary hardware. However, SDR has been widely used in various mobile communication systems due to its modifiability and flexibility. In addition, many open-source projects for mobile communication systems using SDR have been developed, such as srsLTE [24], OpenBTS-UMTS [25], and gr-gsm [26]. These excellent open-source projects provide analysis and testing tools for mobile security researchers. The following are the open-source projects used in our work:

- (1) *srsLTE*. It is a high-performance 4G/5G software radio suite including srsUE, srsENB, and srsEPC. We

use srsENB and srsEPC to build a fake LTE network. The srsUE can access the operator's LTE network using a real USIM card. Meanwhile, srsUE is the solution for establishing a bearer with the operator's IMS server. After the srsUE accesses the LTE network with a USIM card, we can remove the USIM card because the security context has been stored in the computer. This is one of the differences between srsUE and real mobile phones.

- (2) *OpenBTS-UMTS*. It is an application that uses SDR to present a UMTS network. We build it as a fake 3G network and modify it to complete our test requirements.
- (3) *gr-gsm*. The purpose of the gr-gsm project is to provide a set of tools to receive the signals transmitted by GSM devices. It is widely used in voice and SMS sniffing under the GSM network in the research field. In our work, we use it to monitor the content of the calls under the 2G network.

Figure 4 depicts the experimental hardware setup in our work including two computers, three USRP devices, two test mobile phones, and six USIM cards (excluding the monitor and other peripherals).

The following is a detailed description of these hardware packages:

- (1) *Computers*. Two desktop computers (Intel NUC8-BEH) with the 64 bit Ubuntu 16.04 LTS system are used in our experiment. Both computers are loaded with open-source projects required for the experiments, including srsLTE, OpenBTS-UMTS, and gr-gsm. In addition, the two computers need to be connected by a network cable to ensure that data can be transmitted to each other in subsequent experiments.
- (2) *SDR*. Three USRP B210 devices [27] act as the radio transceiver hardware. B210 is connected to the

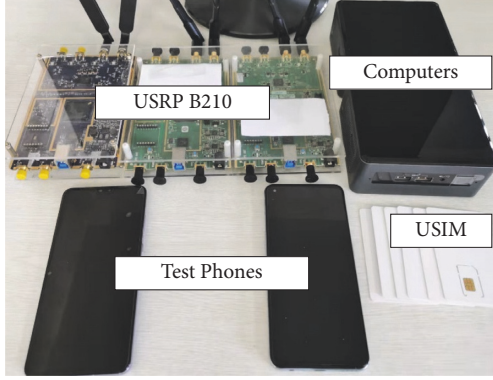


FIGURE 4: Experimental hardware setup.

computer via USB 3.0 and cooperates with the above-mentioned open-source projects to complete the data transmission. We can change the radio frequency at which B210 transmits and receives signals by modifying the configuration file.

- (3) *Test Phones*. Two commercial 5G mobile phones are needed to complete our tests. One Realme GT supporting all 5G, LTE, 3G, and GSM frequency bands works as the victim UE. One Huawei Mate 30 5G works as the callee. Two USIM (Universal Subscriber Identity Module) cards per carrier are used to accomplish different tasks.

5. Security Threats

In this section, we introduce security threats to IMS-based voice services in 5G SA networks. We have systematically analyzed the security issues of the IMS-based voice services by considering EPS fallback and IMS. Our work has discovered four vulnerabilities. Two are caused by flaws in the EPS fallback mechanism and IMS AKA, respectively, and the remaining two are implementation flaws in the IMS server. They enable an adversary to monitor the content of a call or launch the DoS attack against voice service. More threateningly, an attacker can exploit the vulnerabilities to send and receive SMS as a victim. Then the attacker may use the SMS verification code to log in to the victim's application to steal privacy. We validated these vulnerabilities in three carriers.

5.1. EPS Fallback Vulnerability. EPS fallback enables mobile users who have been registered to the 5G network to fall back to 4G when making or receiving calls and use VoLTE for voice services. The three operators related to our work are currently using EPS fallback to implement voice calls under 5G.

When one UE consumes voice services in 5G networks, it will receive RRC release signaling carrying the frequency list of the target LTE base station for the operator, as shown in Figure 5. Then the UE selects the frequency with the highest priority to access the base station and sends tracking area update request signaling to LTE networks for the operator. Whether an AKA process occurs when the UE accesses the LTE network can determine whether the operator's 5G network transmits the UE's security context through the N26

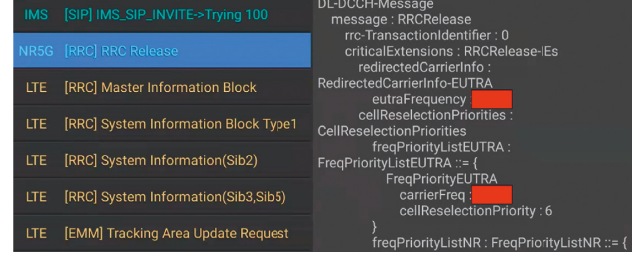


FIGURE 5: The validation of EPS fallback vulnerability.

interface. For OP-I, it will submit the UE's security context in the 5G network to LTE network through the N26 interface, while OP-II and OP-III will not. Although the implementations of the EPS fallback of the three operators are different, all of them may suffer from 4G FBS. Assuming that there is a 4G FBS near a victim registered to the 5G network, the victim will access the FBS when making or answering phones.

Validation. We use srsEPC and srsENB to build a 4G FBS for the three operators. First, we gather the operator's LTE network information such as the PLMN number, TAC, and EARFCN (E-UTRA Absolute Radio Frequency Channel Number) [28]. It is worth noting that the TAC and EARFCN are the parameters of the highest priority cell in the experimental area. Second, we configure the network information of the FBS to be consistent with the operator. Then we use the commercial mobile phone that is already stationed on the 5G network to make and answer calls. As expected, the phone is successfully connected to the FBS. In addition, the mobile phones of the three operators will try to access the 2G/3G network when they find that they cannot register to the 4G network to complete the call. For OP-I and OP-II, the phone finishes calls via the 2G network. For OP-III, 3G is the ultimate guarantee for voice service. Moreover, for these three operators, we have tested whether there is a lack of authentication in the CSFB (Circuit Switched Fallback) technology, which is one of the major voice solutions in the 4G network [29]. In the CSFB scheme, when there is a voice call, the phone will migrate from 4G to 2G/3G. If the authentication step is missing in this process, it can be exploited by attackers to launch impersonation attacks. Specifically, we use a rooted OPPO R11 to access the operator's 4G network and disable the VoLTE. Then we make a call and grab the signaling messages as shown in Figure 6. The result indicates that the authentication step has been enforced in the process of CSFB.

5.2. IMS Server Vulnerabilities. We have identified two implementation vulnerabilities at the IMS server for OP-III. First, the SIP session between the client on the phone and the IMS server should be protected by IPSec. If IPSec is not used, the SIP messages between the UE and IMS server may be protected by AS security. However, this approach may not achieve the desired goal [30]. The authors in [22] have pointed out the serious consequences of not mandating the use of IPSec. Although there are some studies about this vulnerability, we find that the SIP messages can still be plain-

LTE	[EMM] Extended Service Request
GSM	[MM] CM Service Request
GSM	[MM] Authentication Request

FIGURE 6: The validation of CSFB vulnerability.

text for OP-III. Therefore, the messages are easily injected into the SIP session by the attacker. Second, the owner of a bearer for registering to the IMS server can be different from the actual registered person using the bearer. An attacker can set up a bearer in advance and then register to the IMS as a victim to enjoy SMS services by exploiting the vulnerability. Our work is not the same as the spoofable SMS message attack described in [22]. In addition, we verify that this attack has been defended by OP-III.

Validation. We make some effort to discover these vulnerabilities for OP-III. First, we modify srsUE to request to establish an IMS bearer and obtain the IP of P-CSCF. We can use the modified srsUE with external USIM and one USRP B210 to register to OP-III. Second, we record the plain-text SIP messages on the iPhone XS through the open-source tool rvi_capture [31]. Third, we have implemented a simple but effective IMS client in the C language. The client completes the construction of legal SIP messages by modifying some fields in the captured SIP packets. The IMS client and the srsUE are independent processes. The client uses the IMS bearer established by the srsUE to interact with the operator's IMS server by using the IPv6 socket and needs the IMSI, phone number, and authentication response of a USIM card. The client can use the same USIM to register to the IMS server and send SMS. In this process, the SIP messages are not protected by IPSec, which proves that it is allowed not to use IPSec for OP-III. In addition, we send a spoofed SMS, where the specified sender number is changed. However, the SMS failed to be sent with the cause "invalid user." This shows that the attack described in [22] no longer exists for OP-III. Then we use the client with another USIM rather than the USIM used to establish the bearer to register to the IMS server and send SMS as shown in Figure 7. This proves the vulnerability we found. OP-III does not check whether the user who established the IMS bearer is the same as the one registered to the IMS via the bearer.

5.3. IMS AKA Vulnerability. Through a careful analysis of IMS AKA-related standards, we found the vulnerability of IMS AKA. The IMS AKA mechanism is implemented based on the SIP protocol. In the IMS registration process, SIP signaling carrying AKA parameters is interacted between the UE and the IMS server, and the AKA parameters are transmitted and negotiated according to the AKA mechanism. It is worth noting that the authentication mechanism

adopted by IMS follows the principles and core algorithms of AKA in 3G networks. The difference is that IMS AKA uses base64 to encode the authentication parameters. Therefore, we analyze whether the authentication vectors assigned to 3G and IMS domains can be mixed:

- (1) *Authentication Key.* The UE accesses the IMS through the USIM. When a USIM is used for IMS access, the authentication key and functions and the sequence number checking mechanism are shared with 3G [32].
- (2) *Sequence Number (SQN).* SQN is used to prevent replay attacks of authentication vectors. SQN ensures the freshness of the authentication vector through a series of verification mechanisms [33]. The SQN is maintained jointly by the network and the USIM card. Each time a mutual authentication is completed, the SQN maintained by both sides will increase by 1. Therefore, both sides can detect whether the authentication message is replayed. Since the authentication mechanism of IMS is the AKA algorithm, it can resist replay attacks. Specifically, SQN consists of two parts $SQN = SEQ || IND$, where IND is a 5-bit long index. USIM maintains an array of previously accepted SEQs. To verify that the sequence number SQN is fresh, the USIM shall compare the SEQ of the received SQN with the sequence number in the array indexed by the index value IND contained in the SQN [33]. Although the standard suggests that authentication vectors for different service domains should always have different INDs, there is no clear definition. USIM can only detect whether the authentication vector is generated by the home network, but cannot determine whether the received authentication vector is applied by the requested service network domain.
- (3) *AMF Field.* AMF (authentication management field) is a 16-bit field. The first bit is called the "AMF separation bit" [33]. If the "separation bit" is set to 0, the authentication vector can be used in 3G or IMS. However, the vector is useable in 4G and 5G that require the bit to be set to 1.

Based on the above analysis, we conclude that the authentication parameters carried in the SIP message can be parsed and then encapsulated into standard authentication signaling that the UE in the 3G network considers legal.

srsUE	IMS Client
Protocol Info	Source Dest: Prot Info
NAS-EPS Attach request, PDN connectivity request	24... 24... SIP Request: REGISTER sip:ims.mn...3gppnetwork.org
NAS-EPS Authentication request	24... 24... SIP Status: 401 Unauthorized
NAS-EPS Authentication response	24... 24... SIP Request: REGISTER sip:ims.mn...3gppnetwork.org
NAS-EPS Security mode command	24... 24... SIP Status: 200 OK (1 binding)
NAS-EPS Security mode complete	> Session Initiation Protocol (200)
NAS-EPS Attach accept, Activate default EPS bearer context request	> Status-Line: SIP/2.0 200 OK
NAS-EPS Attach complete, Activate default EPS bearer context accept	> Message Header
<div> <div>EPS mobile identity</div> <div>Length: 8</div> <div>.... 1... = Odd/even indicatio</div> <div>.... .001 = Type of identity:</div> <div>IMSI: ...5316</div> </div>	> Via: SIP/2.0/TCP [...FB14:FF46:856B]:55122;branc
	Call-ID: fpkLDAhLWVlffcYtOVXACIXm
	[Generated Call-ID: fpkLDAhLWVlffcYtOVXACIXm]
	> From: <sip: ...9404@ims.mn...3gppnetwork.org>;tag=1M5c
	> To: <sip: ...9404@ims.mn...3gppnetwork.org>;tag=bofify
<div> <div>Protocol or Container ID: P-CSCF IPv6 Address</div> <div>Length: 0x10 (16)</div> <div>IPv6: 24...1::ff:f070</div> </div>	

FIGURE 7: The validation of IMS server vulnerabilities.

Validation. First, we use srsUE equipped with a legal USIM card to register to the operator and establish an IMS bearer. Then, we use our simple IMS client to register to the IMS server with the same identity to obtain the SIP signaling containing the authentication information. Next, we parse the authentication parameters from SIP signaling and use OpenBTS-UMTS to build a fake 3G network. Then the mobile phone equipped with the USIM card is connected to our fake 3G network. Finally, the 3G FBS uses the parsed parameters to encapsulate the authentication request signaling and send it to the mobile phone, and the mobile phone responds normally. This proves our conjecture. In addition, we use the same method to test whether the IMS AKA parameters can be used in the 4G network, but it failed due to differences in the AMF field.

6. Attack Scenarios

In this section, we devise three representative attacks based on the vulnerabilities described above: (1) voice DoS, (2) voice monitoring, and (3) SMS spoofing and interception. The first attack can be launched on the three operators. The second attack is feasible in OP-I and OP-II, and the third attack only applies to OP-III. The two attacks, voice DoS and voice monitoring, only require the LTE fake base station. However, the other one can be launched from the attacker equipped with the 3G FBS, LTE FBS, and LTE UE.

Since we reduce the power of the FBS to avoid affecting other normal UEs as described in Section 4, we have to keep the victim UE close to the fake base stations to ensure that the UE will connect to the FBS. We completely executed the three attacks several times and always got the results that we expected.

6.1. Voice DoS. In this attack, the LTE FBS can launch a DoS attack on voice services of mobile users in 5G networks. 5G subscribers near the FBS cannot consume voice services. Moreover, the attacker can count the number of calls of the victim UE and corresponds to their identity through IMSI.

Attack Procedure. Figure 8 shows the voice client DoS attack flow. When the victim UE registered to the 5G network

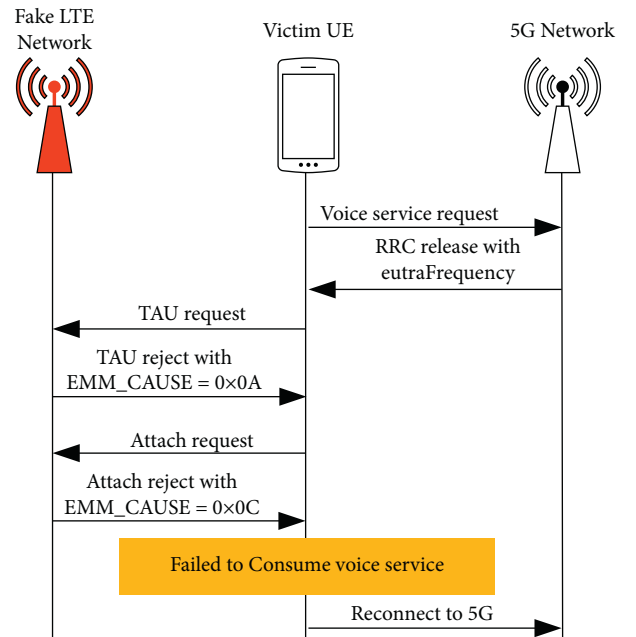


FIGURE 8: The procedure of voice DoS attack.

initiates a voice service request, the network sends RRC release message containing 4G network frequencies and corresponding priorities to the UE. The UE will select the frequency with the highest priority to connect to the LTE base station. First, we use srsUE to capture broadcast messages to get the highest priority frequency. Next, we use srsEPC and srsENB to complete the construction of the fake LTE network and keep the parameters consistent with the real network. Especially, the frequency of the base station is set to the highest priority frequency. Then the UE will be lured to the LTE FBS that is set to the frequency. Then the victim UE sends a TAU request signaling to the LTE FBS. The attacker will reply to the UE with the TAU reject message and set EMM_CAUSE to $0 \times 0A$, which means that TAU requests are not handled yet [34]. After receiving this message, the UE will continue to initiate an attach request to the LTE FBS. Since there is no key to complete the mutual authentication and security establishment with the victim,

the LTE FBS rejects the UE and sets EMM_CAUSE to $0 \times 0C$. According to our assessment, the UE will continue to try to connect to the FBS. After several failures, the voice program on the phone will return because it has not received a response for a long time. Finally, the UE failed to consume voice service and reconnect to the 5G network. Through the above steps, the attacker can realize a DoS attack on the voice service of the victim.

6.2. Voice Monitoring. In this attack, the attacker can monitor the victim's call. The ultimate goal of the attack is to lure the victim UE to an insecure GSM network. There is much research on security in GSM networks. The authors in [14] show the feasibility of the LTE mobile phone number catcher by downgrading UE in the LTE network to the GSM network. Although many attacks can be launched after downgrading UE to GSM networks, we only focus attacks on voice. Our work proves that it is also possible to launch an attack to monitor calls by downgrading UE in 5G networks to GSM networks.

Attack Procedure. Figure 9 shows the voice monitoring attack steps. We build the fake LTE network in the same way as above. The steps of connecting the victim UE initiating a voice service request in a 5G network to the LTE FBS are the same as those described in the voice client DoS attack. The slight difference is that EMM_CAUSE carried by the TAU reject signaling sent by the FBS is set to $0 \times 0F$ instead of $0 \times 0A$. UE may take different behaviors for different EMM_CAUSES [34]. It is worth mentioning that different types of terminals pairing the same EMM_CAUSE may perform different actions. EMM_CAUSES we use may only apply to our experiments. Then the UE in OP-I and OP-II connect to GSM networks to consume voice service. Furthermore, we find that the GSM network of OP-I does not use encryption. Moreover, even with weak encryption algorithms (A5/1), the voice monitoring attack can still be launched [29]. We use gr-gsm to sniff the information transmitted by GSM equipment and then successfully restore the call content.

6.3. SMS Spoofing and Interception. In this attack, the attacker can register to IMS as the victim and receive or send SMS during the attack. As described above, OP-III will eventually use 3G to provide voice services. Since 3G has adopted mutual authentication and stronger encryption algorithms, voice monitoring does not apply to OP-III. However, combining the implementation vulnerabilities of the IMS server of OP-III and the logic vulnerability of IMS AKA described above, we designed a new attack. In addition, the attacker needs to know the victim's mobile phone number.

Attack Procedure. Figure 10 shows the attack procedure. (1) Use the steps described in voice monitoring to connect the victim UE to the 3G FBS (OpenBTS-UMTS). The LTE FBS can send identity request signaling to get the victim's IMSI. In addition, the attacker needs to build srsUE and the IMS

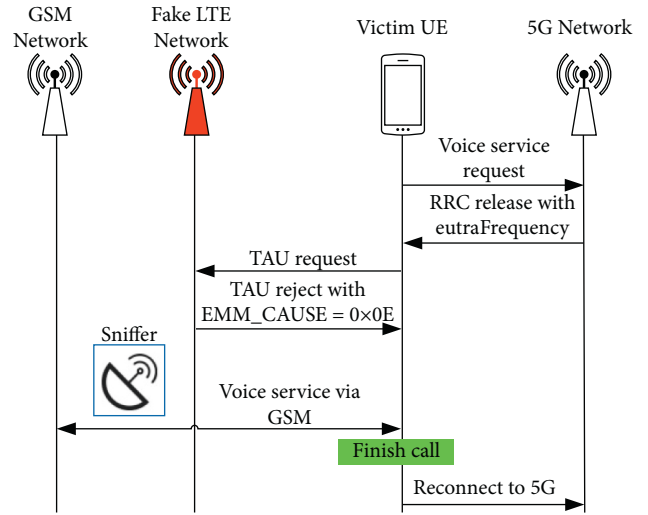


FIGURE 9: The procedure of voice monitoring attack.

client on a computer and ensure that the computer can transmit data through sockets with the computer running the 3G FBS. (2) The attacker used the modified srsUE equipped with a legal USIM to access the LTE network and establish the IMS bearer. (3) The attacker uses the IMS client to send a registration message with the victim's IMSI and phone number to the IMS through this bearer. (4) The IMS server will return a 401 Unauthorized message containing nonce as the AKA authentication challenge to the attacker. The attacker parses the authentication parameters such as RAND and AUTN from the message and sends them to the 3G FBS. (5) After the 3G FBS receives the authentication parameters, it encapsulates them into authentication request signaling and sends them to the victim. (6) The 3G FBS parses the authentication result from the signaling returned by the victim and sends it to the attacker. (7) The attacker encapsulates the parameters received from the 3G FBS into SIP signaling and sends it to the IMS server to complete the authentication and the subsequent registration process. Finally, the attacker accesses the IMS as the victim and can send or receive SMS. Figure 11 shows a packet of SMS spoofing.

7. Discussion

In this section, we discuss these attacks from three perspectives: causes, advantages, and possible limitations:

Voice DoS. The attack exploits a lack of protection in the EPS fallback process. The attack has good concealment and only works when the victim consumes voice service in a 5G network. Moreover, we found that even though the mobile phone was not always on the 5G network during the entire attack, the signal of the phone was always displayed as 5G. The victim may think it is the operator's problem rather than the attack.

Voice Monitoring. The attack exploits the vulnerability of EPS fallback and the insecurity of the encryption algorithm in the GSM network. The attack also has

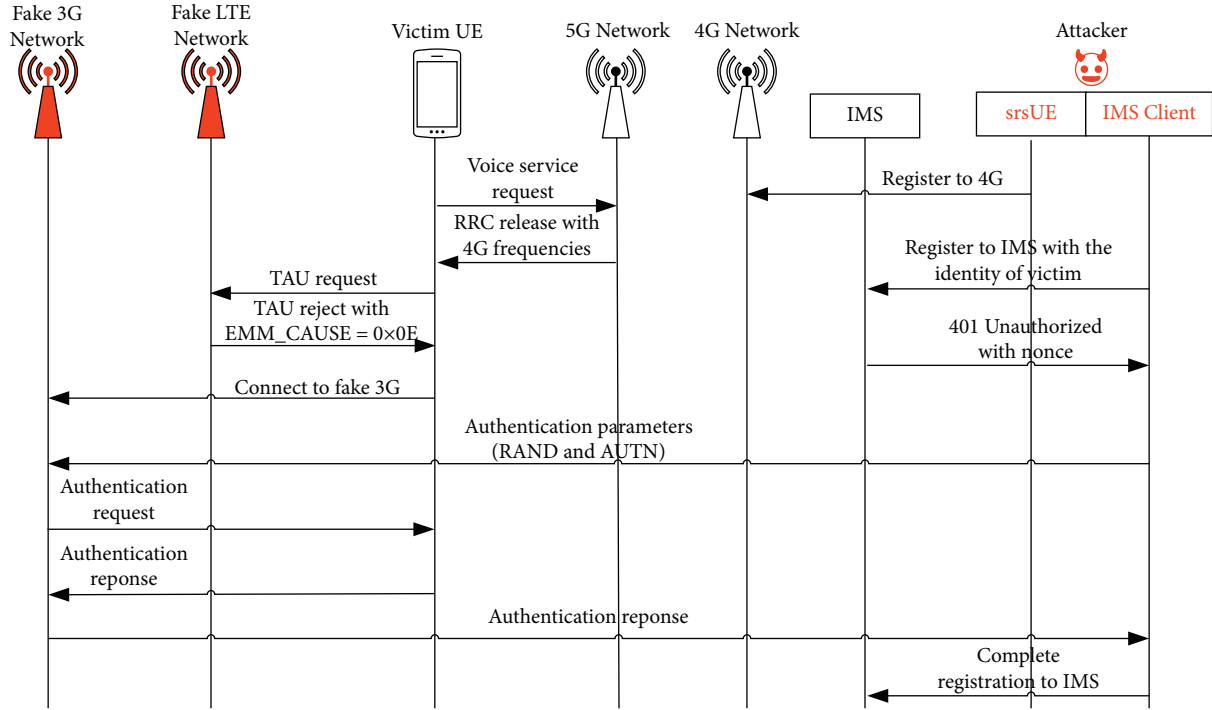


FIGURE 10: The procedure of SMS spoofing and interception attack.

```

Protocol Info
GSM SMS Request: MESSAGE tel: [redacted] | (RP) RP-DATA (MS to Network)
SIP Status: 202 Accepted |
SIP Request: MESSAGE sip: [redacted]
SIP Status: 200 OK |
- Session Initiation Protocol (MESSAGE)
  - Request-Line: MESSAGE tel: [redacted] SIP/2.0
  - Message Header
  - Message Body
    - GSM A-I/F RP - RP-DATA (MS to Network)
      - GSM SMS TPDU (GSM 03.40) SMS-SUBMIT
        0... .. = TP-RP: TP Reply Path parameter is not set in t
        .0.. .. = TP-UDHI: The TP UD field contains only the sho
        ..0. .. = TP-SRR: A status report is not requested
        ...1 0... = TP-VPF: TP-VP field present - relative format
        ....0... = TP-RD: Instruct SC to accept duplicates
        ....01 = TP-MTI: SMS-SUBMIT (1)
        TP-MR: 140
        - TP-Destination-Address - ([redacted])
        - TP-PID: 0
        - TP-DCS: 0
        TP-Validity-Period: 63 week(s)
        TP-User-Data-Length: (6) depends on Data-Coding-Scheme
      - TP-User-Data
        SMS text: hi ya
  
```

FIGURE 11: The packet of SMS spoofing.

strong concealment. Our tests show that the delay caused by our attack to the establishment of a voice call is only 3-4 seconds. More seriously, the monitoring of call content poses a threat to the privacy of mobile users.

SMS Spoofing and Interception. First, due to the vulnerability of IMS AKA, an attacker can use 3G FBS to complete the authentication initiated by the IMS server. Second, since it is not mandatory to use IPSec, the attacker can send messages in plain text after completing the IMS authentication without requiring a key to complete the encryption and integrity protection.

Finally, it is not checked whether the IMS bearer creator is consistent with the user so that the attacker can register to the IMS as the victim. Through this attack, the attacker can use the SMS verification code to log in to the victim's account to steal privacy. This poses a serious threat to mobile users' privacy and property. However, since the attack involves multiple interactive processes, it will cause a delay in the process of registering to the IMS. Considering the attack procedure, the delay mainly occurs between the IMS clients receiving the 401 Unauthorized message and sending the second registration message. To this end, we have tested

the maximum delay allowed by the OP-III. We add different delays (e.g., 2 s, 11 s, 32 s, and 33 s) to the processing logic of these two messages by the IMS client. Figure 12 shows the results of four tests with different delays. When the delay is set to 33 seconds, the second registration message sent by the IMS client will not be processed by the IMS server. Therefore, the maximum delay allowed by OP-III is 32 seconds, which is quite sufficient for launching the SMS spoofing and interception attack.

8. Countermeasure

In this section, we analyze the root causes of the vulnerabilities and propose several potential countermeasures to defend against attacks temporarily or permanently. In addition, we have informed the relevant operators, and the implementation vulnerabilities have been fixed:

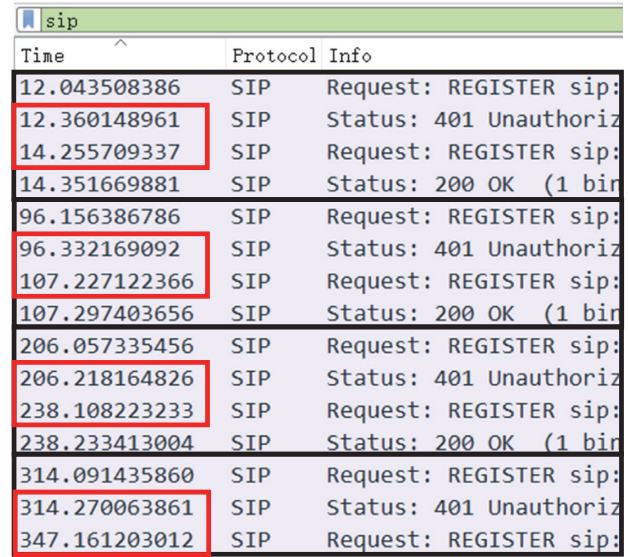
EPS Fallback Vulnerability. 5G is currently in the early stages of construction and cannot be independent of 4G. The inherent downgrade will make attacks using 4G FBS still useable. Operators should speed up the 5G construction and complete the full commercialization of VoNR as soon as possible. In addition, a security mechanism can be implemented to prevent UE from accessing the FBS [35].

IMS Server Vulnerabilities. First, encryption and integrity protection should be set to be mandatory to protect SIP messages for operators [36–38]. Otherwise, it is easy for an attacker to obtain privacy or inject forged messages through plain-text SIP messages. Second, there is no secure binding between the owner of the IMS bearer and the user registered to the IMS server via the bearer. The operator's IMS server should check whether the two identities are the same. In addition, the security and trustworthiness of the IMS server should also be ensured [39, 40].

IMS AKA Vulnerability. There is no difference between the AKA parameters of the 3G network and the IMS, which may lead to the abuse of the authentication vector. We suggest that the AMF field in these parameters can be used to set different values to distinguish the authentication vectors of different domains. The UE determines whether the authentication vector is from the requested service domain by checking this field. Since the AMF field is in plain text in the authentication request signaling, this solution can be implemented by upgrading the protocol stacks in the baseband without changing the USIM card.

9. Future Research Challenges

The voice solutions in the 5G SA network are divided into the VoNR and the EPS fallback. In this paper, we have made the first step towards the security analysis of voice services in the 5G SA networks. However, our study only focuses on the EPS fallback. In the future, researchers can



Time	Protocol	Info
12.043508386	SIP	Request: REGISTER sip:
12.360148961	SIP	Status: 401 Unauthoriz
14.255709337	SIP	Request: REGISTER sip:
14.351669881	SIP	Status: 200 OK (1 bir
96.156386786	SIP	Request: REGISTER sip:
96.332169092	SIP	Status: 401 Unauthoriz
107.227122366	SIP	Request: REGISTER sip:
107.297403656	SIP	Status: 200 OK (1 bir
206.057335456	SIP	Request: REGISTER sip:
206.218164826	SIP	Status: 401 Unauthoriz
238.108223233	SIP	Request: REGISTER sip:
238.233413004	SIP	Status: 200 OK (1 bir
314.091435860	SIP	Request: REGISTER sip:
314.270063861	SIP	Status: 401 Unauthoriz
347.161203012	SIP	Request: REGISTER sip:

FIGURE 12: The packet of registering to IMS with different delays.

pay attention to the security of VoNR, which is the target solution for voice services in the 5G SA networks. More specifically, formal methods can be used to analyze the protocol of VoNR, and artificial intelligence methods (e.g., natural-language processing and machine learning techniques) should be considered for discovering the insecure implementation of operators. Furthermore, emerging services in 5G (e.g., rich communication suite and vehicle-to-everything) also require systematic security research to enhance 5G network's security assurance. In addition, since time-consuming and error-prone manual analysis is not suitable for complex and dynamic 5G networks, automatic discovery of security weaknesses will contribute to 5G security and will be investigated in our future research.

10. Conclusion

The security of voice services in 5G SA networks is critical to both mobile users and operators. Despite its importance, its security has not received widespread attention in the research community. Voice solutions in the 5G SA network include EPS fallback and VoNR. In this paper, we examine the security of voice services in 5G SA networks of three operators, which adopt EPS fallback to provide voice services. Several vulnerabilities are discovered from specifications and carrier networks. Our work proves that the vulnerabilities can be exploited to launch three attacks against mobile users in 5G SA networks. The users may suffer from the attacks of voice DoS and monitoring. More seriously, the attacker can send or receive SMS as a victim and then log in to the victim's application to steal privacy. Finally, we analyze the root causes of these vulnerabilities and propose some alleviation schemes. Our work inspires researchers to further study the limitations and feasibility of the reported attacks and motivates security testing of VoNR in the future.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (No. 62001055).

References

- [1] Ericsson, "Ericsson Mobility Report," 2021, <https://www.ericsson.com/zh-cn/reports-and-papers/mobility-report/reports/november-2021>.
- [2] G. H. Tu, C. Y. Li, C. Peng, and S. Lu, "How Voice Call Technology Poses Security Threats in 4g Lte networks," in *Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS)*, pp. 442–450, IEEE, Florence, Italy, September 2015.
- [3] C. Y. Li, G. H. Tu, C. Peng et al., "Insecurity of Voice Solution Volte in Lte mobile Networks," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, CO, USA, October 2015.
- [4] H. Kim, D. Kim, M. Kwon et al., "Breaking and Fixing Volte: Exploiting Hidden Data Channels and Mis-Implementations," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, Denver, CO, USA, October 2015.
- [5] S. Kwon, S. Park, H. J. Cho, Y. Park, D. Kim, and K. Yim, "Towards 5G-based IoT security analysis against Vo5G eavesdropping," *Computing*, vol. 103, no. 3, pp. 425–447, 2021.
- [6] H. Cho, S. Park, Y. Park, B. Choi, D. Kim, and K. Yim, "Analysis against security issues of voice over 5G," *IEICE - Transactions on Info and Systems*, vol. 104, no. 11, pp. 1850–1856, 2021.
- [7] Z. Li, W. Wang, C. Wilson et al., "FBS-radar: Uncovering Fake Base Stations at Scale in the Wild," in *Proceedings of the Network and Distributed System Security Symposium*, San Diego, CA, USA, January 2017.
- [8] Y. Song, X. Hu, and Z. Lan, "The GSM/UMTS phone number catcher," in *Proceedings of the 2011 third international conference on multimedia information networking and security*, pp. 520–523, IEEE, Shanghai, China, November 2011.
- [9] A. Lilly, "IMSI catchers: hacking mobile communications," *Network Security*, vol. 2017, no. 2, p. 7, 2017.
- [10] R. P. Jover, "LTE Security, Protocol Exploits and Location Tracking Experimentation with Low-Cost Software radio," 2016, <https://arxiv.org/abs/1607.05171>.
- [11] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "IMSI-catch me if you can: IMSI-catcher-catchers," in *Proceedings of the 30th Annual Computer Security Applications Conference*, pp. 246–255, New Orleans, Louisiana, USA, December 2014.
- [12] H. Lin, "LTE REDIRECTION: Forcing Targeted LTE Cell-phone into Unsafe Network," in *Proceedings of the Hack in the Box Security Conference*, Amsterdam, The Netherlands, May 2016.
- [13] C. Yu, S. Chen, and Z. Cai, "LTE Phone Number Catcher: A Practical Attack against mobile privacy," *Security and Communication Networks*, vol. 2019, Article ID 7425235, 10 pages, 2019.
- [14] M. Chlosta, D. Rupprecht, C. Pöpper, and T. Holz, "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, UAE, June 2021.
- [15] S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5GReasoner: a property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pp. 669–684, London, UK, November 2019.
- [16] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, "On the (In)security of mobile Two-Factor Authentication," in *Financial Cryptography and Data Security*, Springer, Berlin, Germany, 2014.
- [17] C. Mulliner, R. Borgaonkar, P. Stewin, and J.-P. Seifert, "Sms-based One-Time Passwords: Attacks and Defense," in *Detection of Intrusions and Malware, and Vulnerability Assessment*, Springer, Berlin, Germany, 2013.
- [18] E. Shablygin and S. Bratus, "How to Count to Two: What "two Factor Authentication" Misses," 2015, https://old.wwpas.com/wp-content/uploads/WWPas_HowToCount.pdf.
- [19] Y. Song, K. Zhou, and X. Chen, "Fake bts attacks of gsm system on software radio platform," *Journal of Networks*, vol. 7, no. 2, pp. 275–281, 2012.
- [20] M. Hadžialić, M. Škrbić, K. Huseinović et al., "An Approach to Analyze Security of GSM network," in *Proceedings of the 2014 22nd Telecommunications Forum Telfor (TELFOR)*, pp. 99–102, IEEE, Belgrade, Serbia, November 2014.
- [21] Y. Zhang, B. Liu, C. Lu et al., "Lies in the Air: Characterizing Fake-Base-Station Spam Ecosystem in China," in *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, pp. 521–534, USA, October 2020.
- [22] G. H. Tu, C. Y. Li, C. Peng, Y. Li, and S. Lu, "New security threats caused by IMS-based SMS service in 4G LTE networks," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1118–1130, Vienna, Austria, October 2016.
- [23] ETSI, "Procedures for the 5G System (5GS); Stage 2. Technical Specification (TS) 23.502. 3rd Generation Partnership Project (3GPP)," Tech. Rep. ETSI TS 123 502, ETSI, Sophia Antipolis, France, 2021.
- [24] SRS, "srsLTE," <https://www.softwareradiosystems.com/products/#srslte/>.
- [25] Github, "OpenBTS-Umts," 2019, <https://github.com/EurecatSecurity/OpenBTS-UMTS>.
- [26] P. Krysik, "Gr-Gsm," 2007, <https://github.com/ptrkrysik/gr-gsm>.
- [27] Ettus, "USRP B210," 2022, <https://www.ettus.com/all-products/ub210-kit/>.
- [28] S. F. Mjølunes and R. F. Olimid, "Easy 4G/LTE IMSI Catchers for non-programmers," in *Proceedings of the International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, pp. 235–246, Springer, Warsaw, Poland, August 2017.

- [29] Y. Zheng, L. Huang, H. Shan, J. Li, Q. Yang, and W. Xu, "Ghost Telephonist Impersonates You: Vulnerability in 4g LTE Cs fallback," in *Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS)*, pp. 1–9, IEEE, Las Vegas, NV, USA, October 2017.
- [30] M. Chlosta, D. Rupperecht, T. Holz, and C. Pöpper, "LTE Security Disabled: Misconfiguration in Commercial networks," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and mobile Networks*, pp. 261–266, Miami, FL, USA, May 2019.
- [31] gh2o, "rvi_capture," 2020, https://github.com/gh2o/rvi_capture.
- [32] ETSI, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Access security for IP-based services (Release 17)," Tech. Rep. 3GPP TS 33.203 V17.0.0, Sophia Antipolis, France, 2021.
- [33] ETSI, "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 16)," Tech. Rep. 3GPP TS 33.102 V16.0.0, ETSI, Sophia Antipolis, France, 2020.
- [34] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J. P. Seifert, "Practical Attacks against Privacy and Availability in 4G/LTE mobile Communication systems," 2015, <https://arxiv.org/abs/1510.07563>.
- [35] S. R. Hussain, M. Echeverria, A. Singla, O. Chowdhury, and E. Bertino, "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*, pp. 1–11, Miami FL, USA, May 2019.
- [36] T. Sivakumar, S. Veeramani, M. Pandi, and G. Gopal, "A novel encryption of text messages using two fold approach," *Recent Advances in Computer Science and Communications*, vol. 13, no. 6, pp. 1106–1112, 2021.
- [37] V. Muthukumaran, C.-H. Hsu, M. Karuppiah, Y.-C. Chung, and Y.-H. Chen, "Public key encryption with equality test for Industrial Internet of Things system in cloud computing," *Transactions on Emerging Telecommunications Technologies (Wiley)*, vol. 33, no. 3, 2021.
- [38] S. M. Nagarajan, U. Kumaran, M. Thirunavukkarasan, M. D. Alshehri, and S. Alkhalaf, "Secure data transmission in Internet of medical Things using RES-256 algorithm," *IEEE Transactions on Industrial Informatics*, vol. 99, 2021.
- [39] R. Saravanan and D. G. Gopal, "Selfish node detection based on evidence by trust authority and selfish replica allocation in DANET," *International Journal of Information and Communication Technology*, vol. 9, no. 4, p. 473, 2016.
- [40] X.-Z. Gao, A. Jafar, and A. Alzubi, "IoT and big data impact on various engineering applications," *Recent Patents on Engineering*, vol. 15, no. 2, pp. 119–120, <https://www.eurekaselect.com/190864/article>.