Hindawi
Security and Communication Networks
Volume 2019, Article ID 7425235, 10 pages
https://doi.org/10.1155/2019/7425235

Research Article

LTE Phone Number Catcher: A Practical Attack against Mobile Privacy

Chuan Yu, Shuhui Chen, and Zhiping Cai

College of Computer, National University of Defense Technology, Changsha, Hunan 410073, China

Correspondence should be addressed to Shuhui Chen; shchen@nudt.edu.cn

Received 15 January 2019; Accepted 14 August 2019; Published 30 September 2019

Academic Editor: Jesús Díaz-Verdejo

Phone number is a unique identity code of a mobile subscriber, which plays a more important role in the mobile social network life than another identification number IMSI. Unlike the IMSI, a mobile device never transmits its own phone number to the network side in the radio. However, the mobile network may send a user's phone number to another mobile terminal when this user initiating a call or SMS service. Based on the above facts, with the help of an IMSI catcher and 2G man-in-the-middle attack, this paper implemented a practicable and effective phone number catcher prototype targeting at LTE mobile phones. We caught the LTE user's phone number within a few seconds after the device camped on our rogue station. This paper intends to verify that mobile privacy is also quite vulnerable even in LTE networks as long as the legacy GSM still exists. Moreover, we demonstrated that anyone with basic programming skills and the knowledge of GSM/LTE specifications can easily build a phone number catcher using SDR tools and commercial off-the-shelf devices. Hence, we hope the operators worldwide can completely disable the GSM mobile networks in the areas covered by 3G and 4G networks as soon as possible to reduce the possibility of attacks on higher-generation cellular networks. Several potential countermeasures are also discussed to temporarily or permanently defend the attack.

1. Introduction

5G/NR (New Radio), which has driven many new technologies like edge computing [1], now has been designed to gradually replace current mobile networks, such as 4G/LTE (Long Term Evolution), 3G/UMTS (Universal Mobile Telecommunications System), and 2G/GSM (Global System for Mobile Communications), but these remainders will still be used widely for a pretty long time due to the existing enormous mobile network infrastructures and terminals of 2G/3G/4G currently, just like 2G and 3G have coexisted with 4G networks for many years by far. Thus, it is still a required and significant work to study and fix the security and privacy problems in low-generation (compared to 5G) cellular networks.

The 2G mobile communication system has many security and privacy problems due to its inherent flaws in technical specifications, e.g., lack of mutual authentication between MSs (Mobile Stations) and the networks, difficulty to upgrade the weak cryptographic algorithms, and the MS always camps on the cell with the strongest radio signal power. Malicious people can easily set up fake base stations, known as IMSI (International Mobile Subscriber Identity) catchers, to spoof IMSIs and IMEIs (International Mobile Equipment Identity) of users, track their locations, and even intercept their calls and short messages by using the man-in-the-middle (MITM) attacks. 3G/UMTS and 4G/LTE were designed to sufficiently ensure the security and confidentiality, which motivating both to use much stronger cipher mechanism and mutual authentication. Even so, with the help of the accessible open source radio software tools, wireless security workers have disclosed more and more security and privacy vulnerabilities in LTE mobile networks such as protocol flaws and implementation flaws. One of the potential protocol flaws in LTE is that, the UE (User Equipment) may accept and process some signalling messages before the security context is established, according to 3GPP (Third Generation Partnership Project) specification [2], which can be exploited by the

stakeholders to attack both the UEs and the networks. For instance, the *Identity Request* NAS (Non-Access Stratum) message is an enabler for IMSI catchers, and the *Attach Reject* and *Tracking Area Update* (*TAU*) *Reject* messages are used to execute DoS (Denial of Service) attacks on the mobile terminals. In this paper, we utilized the unencrypted and none-integrity protected *RRCConnectionRelease* message to redirect LTE mobile phones to start up the phone number catching process.

The phone number, aka MSISDN (Mobile Subscriber ISDN Number) in terminology, is an important individual privacy of a mobile subscriber which is designed to identify the users in our real life, especially in the mobile social network life. According to the specifications, the mobile device does not send its own phone number to the network side in the radio. Thus, traditional IMSI catchers can only get the IMSI/IMEI from the user's mobile equipment by sending the signalling message *Identity Request* and hardly spoof the phone number. There is a unique mapping rule that nobody knows between the IMSI and the MSISDN, because all the subscriber's identity information as well as the mapping relations are only stored in the USIM (Universal Subscriber Identity Module) cards and the operator's database where both places are publicly acknowledged to be strongly secure. The operator's networks will translate the IMSI to the MSISDN in the core network when providing the users with call services or SMS (Short Message Service), which fact was exploited to implement our LTE phone number catcher.

In this paper, we came up with a phone number catcher model aiming for collecting the MSISDNs of LTE users. We also demonstrated that the phone number catcher can be easily set up by using available SDR (Software-Defined Radio) tools and commercial off-the-shelf devices only requiring basic coding skills and the knowledge of GSM/LTE specifications. We are the first phone number catcher that targeting at LTE mobile phones and fully implemented by SDR. The experimental results showed that we could catch an LTE device's phone number within a few seconds once the victim device camped on our fake station. The purpose of our work is to confirm that the LTE security and privacy can be also quite vulnerable as long as the legacy GSM still exists. Thus, this article hopes that the operators across the world can completely discard the 2G/GSM mobile network in the areas covered by 3G and 4G as soon as possible to guarantee the security and privacy for subscribers in higher-generation mobile networks, which is also considered to be the final solution to against this kind of phone number catcher.

2. Background

2.1. Mobile Communication Networks. Mobile communication networks play an important role in many scenarios of our lives; for example, they can be quite useful in the disaster rescue process when cooperated with other advanced technologies [3]. In the last decades, mobile communication network system has varied really a lot, and there appear many illustrious communication systems from the first generation (1G) to the latest 5G. 4G/LTE and 2G/GSM are two important and widely used modern wireless communication systems among them. In this paper, our LTE phone number catcher model is also based on the two mobile systems. So now we briefly describe their network structures and basic concepts which are helpful for understanding the paper next.

2.1.1. Global System for Mobile Communications. Global System for Mobile Communications (GSMs) is the first mobile communication system that uses digital communication technology instead of the analog which greatly reduced the body size of the mobile terminals. The general structure of GSM network is shown in Figure 1. There are several different components in a typical GSM network, which are MS, BTS (Base Transceiver Station), BSC (Base Station Controllers), MSC (Mobile Switching Center), and the databases (HLR/VLR/AuC/EIR) [4]. The MS can be a cell phone or other mobile terminal with a SIM card inserted in. The SIM card stores the subscriber's IMSI and MSISDN information which we aim to catch. The same identity information and their mapping relation also exist in the operator's database.

2.1.2. Long Term Evolution. Long Term Evolution (LTE) systems are the most popular mobile communication systems around the world for not only the higher access rate and lower latency but also the enhanced security and privacy scheme for users. The IP-based LTE mobile network has a flat and much simpler structure comparing to the GSM. Figure 2 shows the interface protocols among the network units as well as two main sections of LTE network structure: the EUTRAN (Evolved Universal Terrestrial Radio Access Network) and the EPC (Evolved Packet Core), and each of which comprises several subdivisions.

The LTE UE containing a USIM card is the target of our experiment. The eNodeB (Evolved Node B) refers to the base station that communicates with UEs using radio links and relays the NAS messages to the MME (Mobility Management Entity) who is responsible for authentication and resources allocation to UEs. HSS (Home Subscriber Server) is the operator's database which stores the authentication information and other important subscription data of subscribers.

2.1.3. Identity Codes. Identity Codes are widely used in mobile networks between UE and Network sides, such as IMSI, MSISDN, TAC, and PLMN number which appeared in our later experiment:

(i) *IMSI*. International Mobile Subscriber Identity is a global unique identification for subscriber's USIM card inserted in UE. It has been widely used in cellular communication systems since the birth of the early generation mobile network. It is transmitted to the Network in plain text when UE first initiates an attach procedure after the mobile

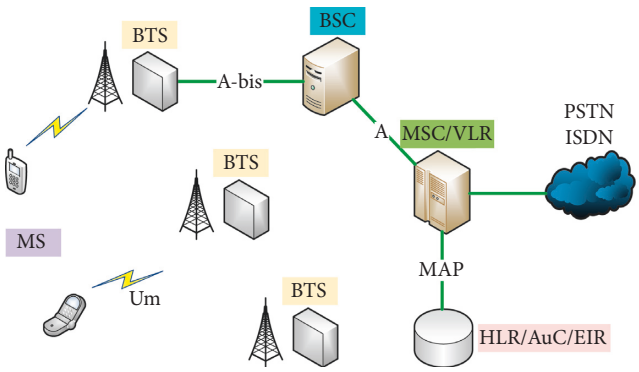

Figure 1: A general structure of GSM network.

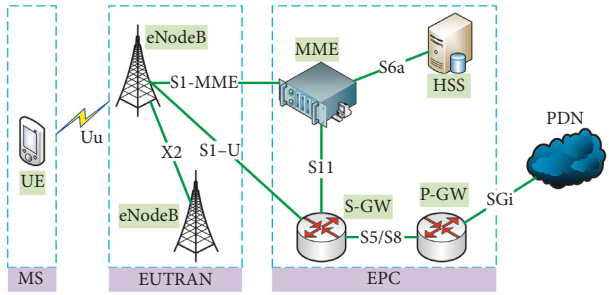

Figure 2: LTE network structure.

device powers on, or when the UE receives an *Identity Request* NAS message from the core network.

(ii) *MSISDN*. Mobile Subscriber ISDN (Integrated Services Digital Network) Number, also known as the phone number, is used to identify a specific user. It plays an important role in the mobile social network life; for example, we use it to register social accounts on different mobile apps. Nobody knows the mapping rule between a mobile user's IMSI and MSISDN except the USIM card and the operator. The UE never sends its own MSISDN to the network in the radio, but the network side may transmit the UE's phone number to another mobile device during the UE initiating service, because the mobile network operators will translate the UE's IMSI to MSISDN according to the mapping rule in the core networks to provide Caller ID service.

(iii) *PLMN*. Public Land Mobile Network code consists of the MCC (Mobile Country Code) and MNC (Mobile Network Code), which identifies an operator's particular mobile network in a country, e.g., one PLMN number of China Mobile is 46000.

(iv) *TAC*. Tracking Area Code is an identifier for a certain geographic area and all the eNodeBs and cells situated in the area own the same TAC.

2.2. Software-Defined Radio. Software-Defined Radio (SDR) is a wireless communication system where components are implemented completely by software on a general personal computer or embedded system rather than hardware [5]. SDR has become the analysis and testing tool for kinds of mobile communication systems due to its modifiability and flexibility over the last few years. Meanwhile, a great many of the open source projects have been developed. Such successful projects like srsLTE and OAI (OpenAirInterface) [6] for LTE, OpenBSC and OpenBTS for GSM have implemented most functions and protocol stacks of corresponding radio access network. Following are the open source projects which are used in our work:

(i) *srsLTE*. Software radio systems LTE is a high-performance LTE open source library for software-defined radio applications [7]. These applications including srsUE, srsENB, srsEPC, are fully compliant with LTE Release 8 which provide us an excellent LTE experimentation platform. We use this software to build a rogue LTE Network for redirecting the target LTE phone to our rogue GSM network implemented by OpenBSC.

(ii) *OpenBSC*. OpenBSC is a GSM open source project of Osmocom (Open Source Mobile Communication) community which is known as a collection of open source software projects in the area of mobile communications. OpenBSC aims to be a stable and all-in-one implementation system of the OsmoBSC, OsmoMSC, and OsmoHLR for the GSM/3GPP protocol stacks and elements [8].

(iii) *OsmocomBB*. It is also an open source and free GSM Baseband software implementation of Osmocom community. Radio amateurs can make and receive phone calls, send, and receive SMS by using OsmocomBB on a compatible GSM phone such as MotorolaC118 which is used as a malicious MS in our experiment [9].

OpenBSC and srsLTE are both compatible with the off-the-shelf device USRP (Universal Software Radio Peripheral) from Ettus Research [10]. So we chose two USRP B210 to set up our eNodeB and BTS. In short, our LTE phone number catcher is an entire SDR system by running open source srsLTE and OpenBSC with USRPs, OsmocomBB with a GSM phone, to achieve the main goal of collecting phone numbers in a restrict area.

2.3. Related Work. The first MITM attacks in GSM mobile communication system emerged along with an IMSI catcher [11]. After that, the security and privacy of the GSM network has been in face of a more severe situation. 4G/LTE mobile communication was considered to be notably more secure than its precursors, GSM and UMTS. However, with the wide availability of open source tools for various experimentations, an increasing number of security and privacy vulnerabilities existing in LTE [12–17], such as DoS attacks and privacy leaks, have been uncovered by researchers in recent years. Shaik et al. demonstrated that an active attacker

can precisely locate an LTE device by using an LTE rogue station [17]. Jover exploited the unencrypted and none-integrity protected LTE protocols, e.g., Attach Reject and *TAU* Reject messages, and uncovered the vulnerabilities of denying service to an LTE device and downgrading it to the more insecure GSM network [14]. Both Shaik and Jover showed that IMSI catcher can also be effective by building an LTE rogue eNodeB in LTE mobile network besides in 2G and 3G networks. Mjølsnes and Olimid verified that LTE IMSI catcher can be implemented by low-cost software-defined radio without any programming [15]. Hussain et al. proposed a systematic approach to uncover 10 new attacks against LTE security, privacy, and availability and validated most of them [12].

The first phone number catcher was implemented in pure GSM network by Song et al. using a customized hardware board [18], which did not work in LTE. Unlike the attacks above, our experiments showed that the LTE subscriber's phone number can also be caught based on the existing operator's mobile network systems.

3. LTE Phone Number Catcher Model

The architecture of the LTE phone number catcher model consists of two main submodules, the LTE Redirector, and the GSM Middle-Man module, as illustrated in Figure 3.

3.1. LTE Redirector. The LTE Redirector is actually a Rogue LTE Network (RLN) implemented by running open source codes, srsENB and srsEPC, on a single laptop computer with a USRP B210 connected via USB 3.0. The most important goal of this part is to redirect the victim UE that tries to camp on the RLN to our GSM Middle-Man network. Additionally, we can also use this module as a LTE IMSI catcher to collect IMSIs in the area of the LTE Redirector. We made some changes to the source codes of srsENB and srsEPC to achieve the above goals successfully.

3.2. GSM Middle-Man. The GSM Middle-Man module is a typical 2G/GSM MITM attack which is also implemented by SDR in our work. It is composed of a Rogue GSM Network (RGN), a malicious MS, and a phone number displayer. The RGN runs OpenBSC on a desktop computer also with a USRP B210, and the malicious MS is carried out by running the designed OsmocomBB codes on the same desktop computer as well as a MotorolaC118. The RGN communicates with the malicious MS by network socket [19]. The phone number displayer is, in essence, a general mobile phone for receiving a call or SMS from the victim LTE phone and displaying the victim's phone number.

Once an LTE phone is redirected to the RGN at a specific ARFCN (Absolute Radio Frequency Channel Number) [20], the RGN then will catch the UE's IMSI/IMEI and inform the malicious MS to masquerade as this victim UE to initiate an IMSI-type Location Update Request (*LUR*) to the operator's GSM network, and after the authentication and *LUR* procedure, the malicious MS makes a call or sends an SMS to the phone number displayer to finally catch the victim UE's phone number.

3.3. Signalling Process of the Model. An entire signalling process of the phone number catcher model can be simplified in Figure 4. Since our catcher model involves many complex procedures of the 4G/LTE and 2G/GSM network protocols, we just list the main signalling in each procedure.

When the phone number catcher system is turned on, the RLN will continuously broadcast the fake cell's system information at a given EARFCN [21]. Once a LTE UE around our fake station receives these important information, including MCC, MNC, and TAC, via *MasterInformationBlock* (*MIB*) and *SystemInformationBlock* (*SIB*) messages, and our fake cell meets the cell reselection criteria in LTE [22], then, the UE would initiate a *Tracking Area Update* to our RLN. When the fake EPC receives TAU request, it can either spoof the victim UE's IMSI by sending it the *Identity Request* message before redirecting the UE to the GSM fake station or directly redirect the victim UE to our GSM network by designing the *redirectedCarrierInfo* component in the *RRCConnectionRelease* message. The *redirectedCarrierInfo* indicates a carrier frequency and is used to redirect the UEs to another RAN (Radio Access Network), e.g., GSM [23].

After the victim UE accessed to our GSM network and initiated a *LUR* procedure, we send the *Identity Request* message to the victim UE, and get the victim's IMSI in the *Identity Response* message. Then, the malicious MS will be informed of the victim UE's IMSI and initiate an IMSI-type *LUR* to the operator's GSM network using the victim's IMSI. The malicious MS will expectedly receive an *Authentication Request* message containing the authentication parameter (*Rand*) from the commercial GSM network, and delivery it to the RGN. The RGN then authenticates the victim UE using the receiving *Rand* and gets the *SRES* from the victim UE in the Authentication Response message. Finally, the malicious MS uses this *SRES* to respond to the operator's authentication and completes the *LUR* procedure after receiving the *Location Update Accept* message containing the TMSI (Temporary Mobile Subscriber Identity) that the operator's GSM network allocated to it. At this moment, the malicious MS can either make a call or send an SMS to the MSISDN displayer using commercial GSM network. The displayer receives the call or SMS and gets the phone number of the victim UE.

4. Experimental Setup

In this section, we present the experimental setup of our phone number catcher model including both the hardware part and software. Traditional communication system devices and equipment usually had huge bodies and were also extremely expensive. However, the more annoying thing for a radio communication system researcher or an amateur is that they could hardly know the source codes running on the devices. Fortunately, the SDR technology and the low-cost off-the-shelf hardware module have lighted up these people.

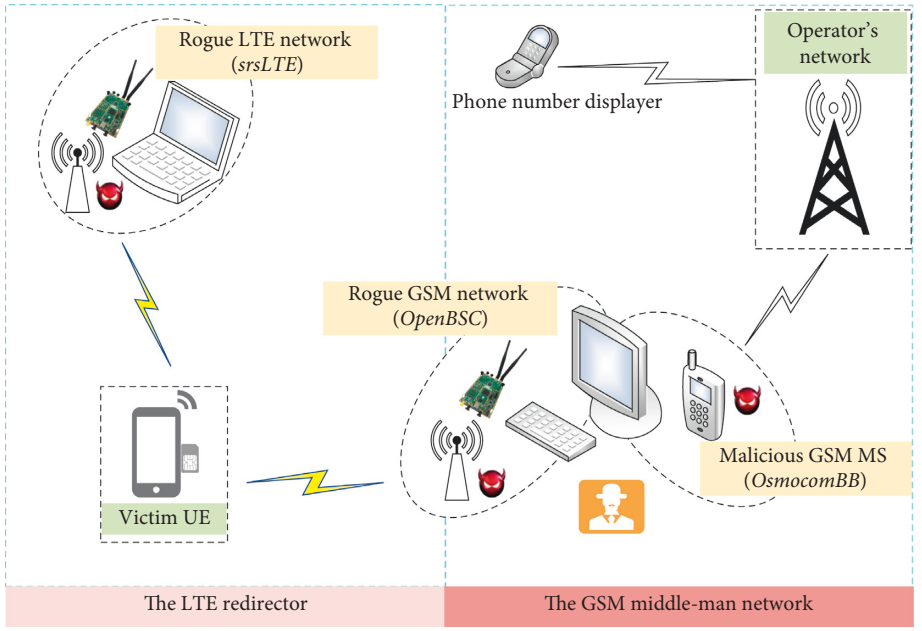

Figure 3: LTE phone number catcher model.

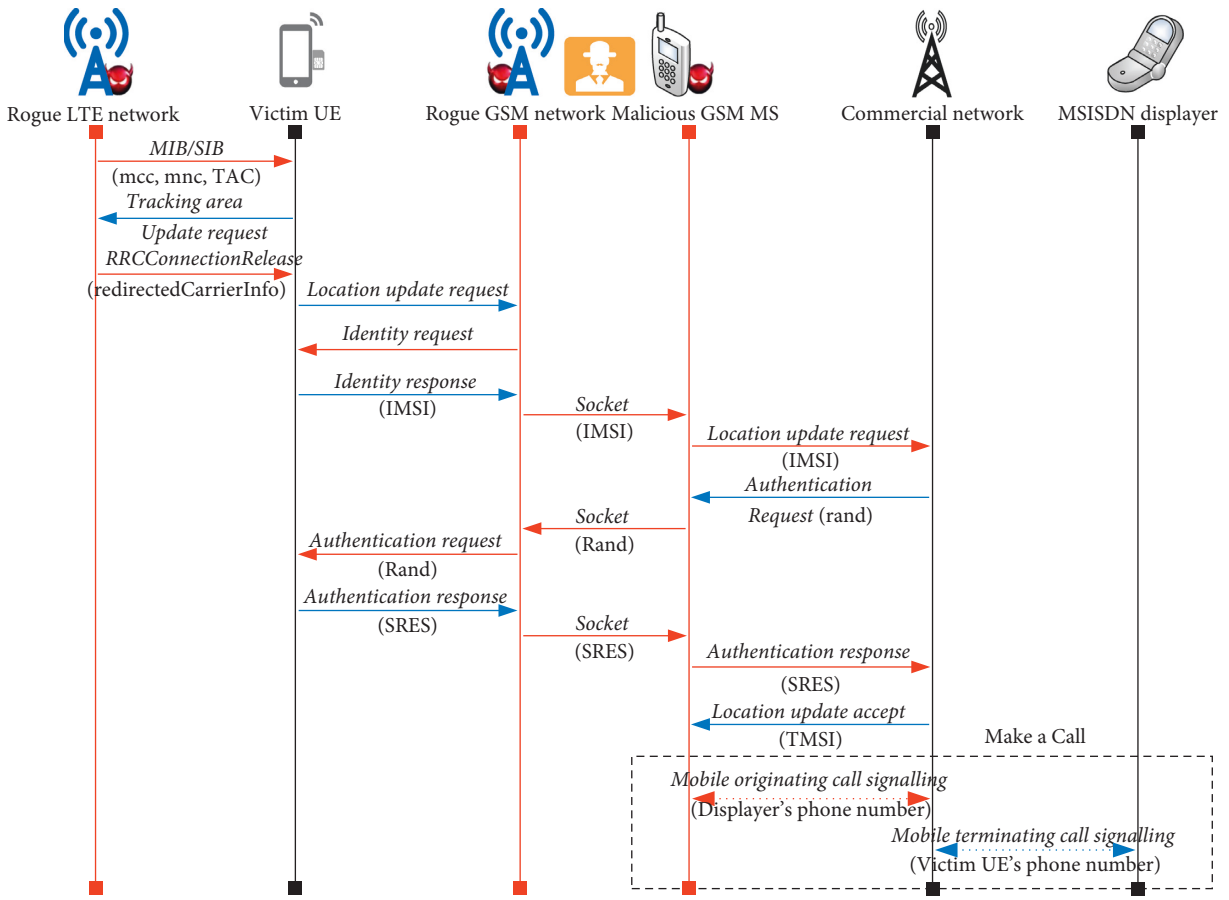

Figure 4: Main signalling of the phone number catcher model.

4.1. Hardware. All the hardware devices used for our experiment can be easily accessed from the commercial market. Figure 5 depicts the hardware experimental setup in our work (excluding USB data cables).

4.1.1. Computers. One desktop computer (Gigabyte B85M-D3H i5-4430 CPU@3.00 GHz × 4) and one laptop computer (Dell Latitude E5470, i7-6600U CPU@ 2.60 GHz × 2) were used in the experiment. The operating

systems of both computers are 64-bit Ubuntu 16.04 LTS [24] with kernel version 4.32.0-61-low latency. Both computers were connected to the transceivers via USB 3.0. The desktop computer was also equipped with standard peripherals including monitor, mouse, and keyboard.

4.1.2. Radio Transceiver. Two USRP B210 devices and a MotorolaC118 GSM phone constituted the radio transceiver hardware. We can program the B210 to transmit and receive any radio signal we want over a wide radio frequency range, from 70 MHz to 6 GHz, covering all the LTE frequency bands. The C118 can be used to perform the same function at GSM Band 900/1800 MHz [25].

4.1.3. Test Phones. Two commercial LTE mobile phones were used to accomplish different tasks. One Apple iPhone6s plus (A1699) supporting all the LTE and GSM frequency bands in China, worked as the victim UE; meanwhile, the Meizu M5 Note was used as the phone number displayer. We also used the M5 Note to gather the operator's LTE and GSM network information such as the (E)ARFCN, the PLMN number, and the TAC to configure our RLN and RGN. The 6sp and the M5 Note used two different USIM cards from a same operator in China.

4.2. Software. Three different sets of open source software, srsLTE, OpenBSC, and OsmocomBB, were used in our implementation of the phone number catcher. We have already made an introduction to them in the background section. We just downloaded, built, and tested the source codes of srsLTE on the laptop computer as well as the OpenBSC and OsmocomBB codes on the desktop computer for experimental software setup. More detailed and specific steps can be found in [7–9]. Then, we could modify and rebuilt the source codes to achieve the functions we want. Due to the available low-cost hardware devices and the open source software, anyone with only basic coding skills and the knowledge of GSM/LTE specifications could carry out the experiment.

5. SDR Implementation and Results

In this section, we describe how we implemented the LTE phone number catcher using SDR and present the results of our experiment. We carried out all the experiments in our wireless network security laboratory to avoid affecting other normal UEs. We kept the victim UE close to the phone number catcher system in each experiment so as to meet the radio signal power requirement of cell reselection.

5.1. SDR Implementation

5.1.1. LTE Redirector. We ran srsENB and srsEPC on the laptop to build a RLN. We first used the M5 Note to collect the operator's LTE and GSM network information nearby which were necessary for the experiment. We accessed the M5's Testing Mode by dialing ∗#∗#4636#∗#∗, which was the same way as described in [15]. Once we successfully got the EARFCN, MCC, MNC, and TAC of the commercial LTE network and the ARFCNs of the GSM networks (see Figure 6) around our lab, we configured our rogue eNodeB as follow:

(a) The rogue eNodeB used the same MCC, MNC, and EARFCN as the commercial one

(b) The TAC of the rogue eNodeB was configured to a value that closed to but not equalled to the commercial one

(c) The ARFCN that the victim UE was redirected to was set to a value different from those ARFCNs that we had collected

We made some required changes in the srsENB source codes to let the rogue eNodeB send back a *redirectedCarrierInfo* encapsulated in the *RRCConnectionRelease* message after the eNodeB received a TAU request from the victim UE. Furthermore, we also modify the srsEPC source codes to use the rogue eNodeB as an IMSI catcher.

5.1.2. Middle-Man Network. We ran OpenBSC and OsmocomBB on the desktop to build the middle-man network. The MCC and MNC of the fake Base Station (BS) were set to the same values as the rogue eNodeB. Notably, setting the value of the ARFCN to be the exactly one contained in the *redirectedCarrierInfo* was the most important step. We merely modified necessary source codes of both OpenBSC and OsmocomBB to implement the signalling process as shown in Figure 4. We also powered on the M5 Note waiting for the call from the victim UE.

5.2. Experimental Results. We completely executed the experiment several times, and at each time, we always got the experimental results that we expected after we ran the LTE phone number catcher system successfully.

In the traffic of the rogue eNodeB running as both an IMSI catcher and a redirector, we saw the TAU request from the victim UE, the *RRCConnectionRelease* message to the UE, and the IMSI of the victim UE in the *Identity Response* message as shown in Figure 7.

We could probably infer from the *redirectedCarrierInfo* in Figure 7 that the victim UE had been redirected to our fake GSM BS, and what happened next in the BS also confirmed that. Figures 8 and 9 captured part of the OpenBSC and OsmocomBB logs, respectively, in one experiment. What happened could be described as follow procedures according to the results:

(i) The victim UE initiated a *LUR* to the RGN after camping in our cell

(ii) The RGN caught the IMSI and IMEI(SV) of the victim UE, and sent them to the malicious MS to

Figure 5: Experimental hardware setup.

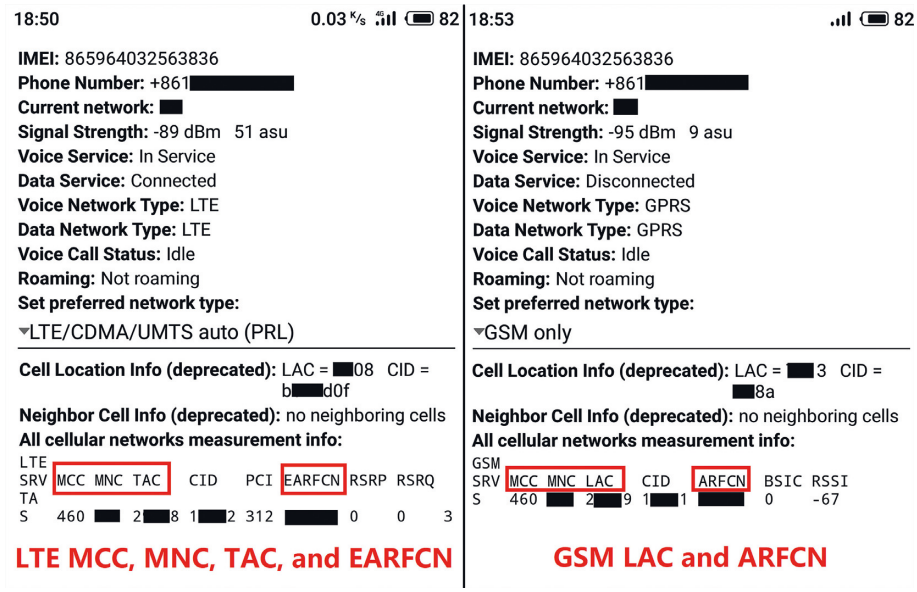

Figure 6: Necessary network information we collected.

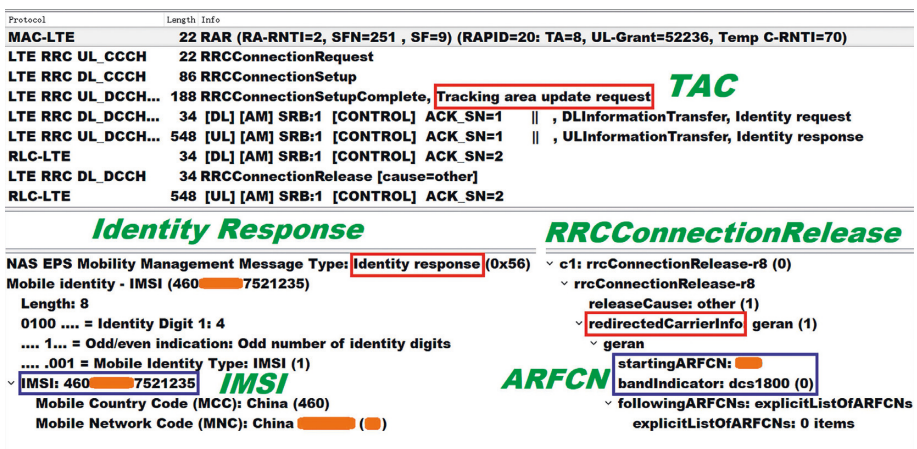

Figure 7: Partial air traffic of the rogue eNodeB.

start an IMSI-type *LUR* to the commercial GSM network

(iii) The malicious MS relayed the authentication parameter *Rand* received from the operator to the RGN

(iv) The RGN used the *Rand* to authenticate the victim UE and passed the *SRES* to the malicious MS

(v) The malicious MS successfully completed the authentication procedure by sending back the *SRES* to the operator's GSM network and also completed the

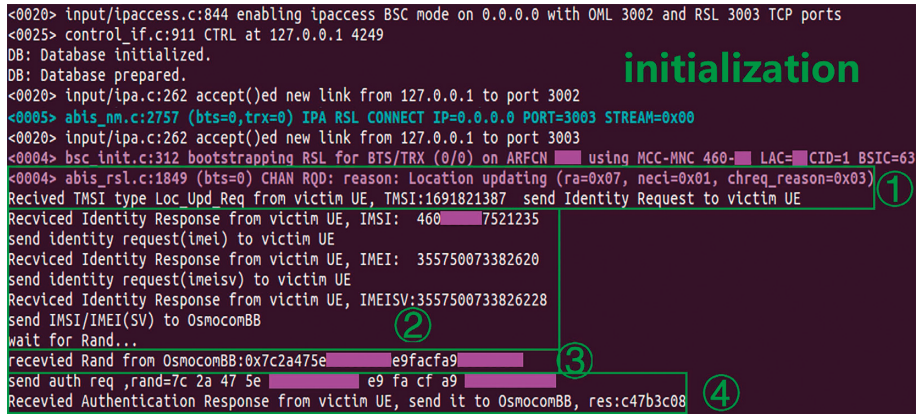

Figure 8: Part of the OpenBSC logs.

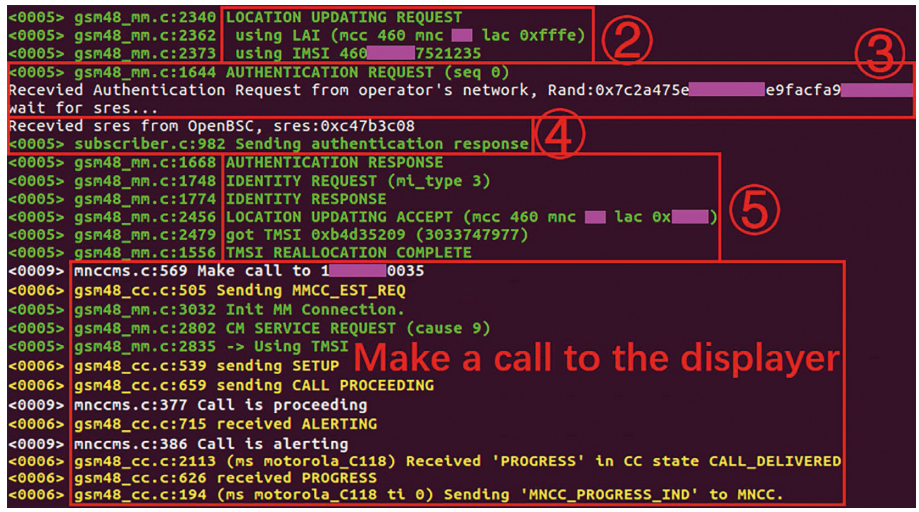

Figure 9: Part of the OsmocomBB logs.

LUR procedure by receiving the *Location Update Accept* message

After that, we used the OsmocomBB software to make a call to the displayer using the victim UE's identity. As expected, the M5 Note received a call after the malicious MS initiating a mobile originating call and displayed the phone number of the victim UE in Figure 10, which confirmed the practicability of our LTE phone number catcher model.

6. Countermeasure and Discussion

Experimental results showed that we caught the LTE test cell phone's MSISDN successfully when the victim phone was very close to the phone number catcher system. Due to the radio signal power issue, the system could be effective only in a small range when utilizing existing experiment devices and equipment. However, when equipped with PAs (Power Amplifier), the LTE phone number catcher system is able to affect a quite large area. The attack is mostly theoretical and in an actual scenario, it would be hard for normal people to make any good use of the phone numbers obtained. However, the law enforcement and intelligence agencies can use this system as a tool to track a criminal efficiently in real time, when only knowing that criminal's phone number. Meanwhile, lawbreakers might utilize the system to eavesdrop user's privacy for illegal usages, e.g., advertising promotions, which seriously break the security and privacy in mobile network.

Hence, we now propose possible measures against the attack. The root cause of this attack is that the UEs accept the unprotected *redirectedCarrierInfo*, so under a reasonable trade-off, from the LTE specification aspect, the simplest way to fix this is to transmit the redirect information only after setting up the security context. Besides, since there is a perceptible change in the mobile network icon at the victim's cell phone screen during the attack, the LTE user can turn on the airplane mode immediately when noticing being attacked to avoid privacy leak, or directly disable the GSM network of the cell phone.

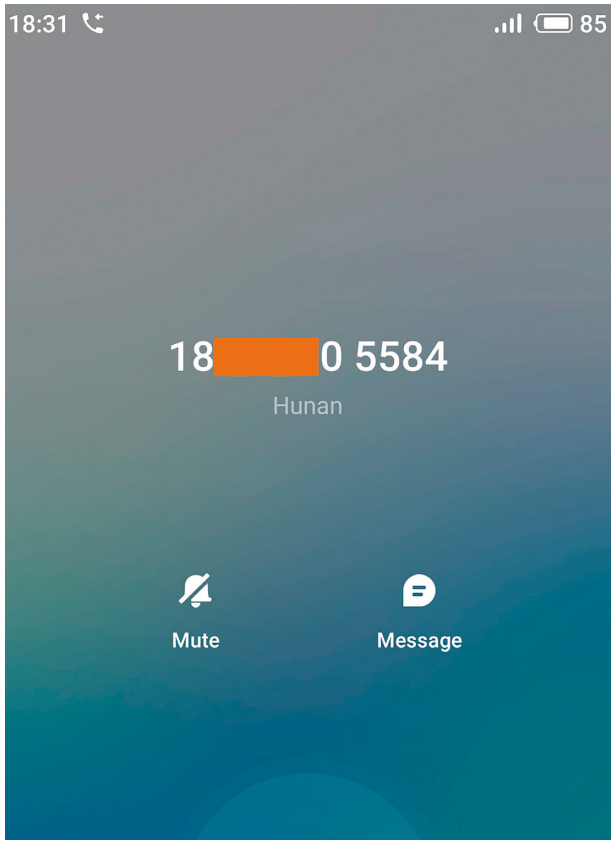

Figure 10: Victim UE's phone number we caught.

From the operator side, there is no particular need for 2G in the areas covered by both 4G and 3G; thus, closing the unsafe GSM networks in these areas is an ultimate solution.

7. Conclusion

In conclusion, this paper implemented a phone number catcher prototype aiming at LTE mobile phones by using easily available SDR tools and affordable commercial devices. We described the model of the phone number catcher, the SDR implementations, and presented the experimental results. The results showed that the existence of GSM seriously impacts the mobile privacy in LTE networks. Thus, this paper hopes that the operators worldwide can totally disable the 2G/GSM networks in the areas covered by 4G and 3G as soon as possible, to guarantee the security and privacy for subscribers in higher generation mobile networks. Finally, we discussed the potential defenses.

Data Availability

The air traffic data of the rogue eNodeB used to support the findings of this study have not been made freely available because of the need to protect user privacy. Requests for access to the data should be made to Chuan Yu, yuchuan17@nudt.edu.cn.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The work is supported by the National Key Research and Development Program of China under Grant nos. 2018YFB180020, SQ2019ZD090149, and 2017YFB0802300.

References

[1] F. Liu, G. Tang, Y. Li, Z. Cai, X. Zhang, and T. Zhou, "A survey on edge computing systems and tools," *Proceedings of the IEEE*, vol. 107, no. 8, pp. 1537–1562, 2019.

[2] 3GPP, Technical Specification Group Core Network and Terminals; Non-Access-Stratum (NAS) Protocol for Evolved Packet System (EPS); Stage 3 (TS 24.301 v15.4.0 Release 15), 2018-09, http://www.3gpp.org/ftp/Specs/archive/24_series/24.301/.

[3] L. Fang, G. Yeting, C. Zhiping, X. Nong, and Z. Zhiming, "Edge-enabled disaster rescue: a case study of searching for missing people," *ACM Transactions on Intelligent Systems and Technology*, vol. 10, no. 11, pp. 1–26, 2019.

[4] GSM Network Structure, https://en.wikipedia.org/wiki/GSM/.

[5] M. Dillinger, K. Madani, and N. Alonistioti, *Software Defined Radio: Architectures, Systems and Functions*, Wiley & Sons, Hoboken, NJ, USA, 2003.

[6] N. Nikaein, R. Knopp, F. Kaltenberger et al., "Demo: OpenAirInterface: an open LTE network in a PC," in *Proceedings of the 20th Annual International Conference on Mobile Computing and Networking (MobiCom'14)*, pp. 305–308, Maui, HI, USA, September 2014.

[7] srsLTE, http://www.softwareradiosystems.com/products/#srslte/.

[8] OpenBSC, http://osmocom.org/projects/openbsc/.

[9] OsmocomBB, http://osmocom.org/projects/baseband/wiki/.

[10] Ettus research, "USRP", https://www.ettus.com/.

[11] D. Strobel, "IMSI catcher," Tech. Rep. 14, Ruhr-Universität Bochum, Bochum, German, 2007.

[12] S. R. Hussain, O. Chowdhury, S. Mehnaz, and E. Bertino, "Lteinspector: A systematic approach for adversarial testing of 4G LTE," in *Proceedings of the 25th Annual Network and Distributed System Security Symposium (NDSS 2018)*, San Diego, CA, USA, February 2018.

[13] R. P. Jover, "Security attacks against the availability of LTE mobility networks: overview and research directions," in *Proceedings of the 16th International Symposium on Wireless Personal Multimedia Communications (WPMC 2013)*, pp. 1–9, Atlantic City, NJ, USA, June 2013.

[14] R. P. Jover, "LTE security, protocol exploits and location tracking experimentation with low-cost software radio," 2016, http://arxiv.org/abs/1607.05171.

[15] S. F. Mjølsnes and R. F. Olimid, "Easy 4G/LTE IMSI catchers for non-programmers," in *Proceedings of the 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS 2017)*, pp. 235–246, Warsaw, Poland, August 2017.

[16] M. T. Raza, F. M. Anwar, and S. Lu, "Exposing LTE security weaknesses at protocol inter-layer, and inter-radio interactions," in *Proceedings of the Security and Privacy in Communication Networks—13th International Conference (SecureComm 2017)*, pp. 312–338, Niagara Falls, ON, Canada, October 2017.

[17] A. Shaik, J. Seifert, R. Borgaonkar, N. Asokan, and V. Niemi, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," in *Proceedings of the 23rd Annual Network and Distributed System Security Symposium (NDSS 2016)*, San Diego, CA, USA, February 2016.

[18] 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, Shanghai, China, November 2011.

[19] Network Socket, https://en.wikipedia.org/wiki/Network_socket/.

[20] Absolute Radio-Frequency Channel Number, ARFCN, https://en.wikipedia.org/wiki/Absolute_radio-frequency_channel_number/.

[21] 3GPP, Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Radio Transmission and reception; Carrier Frequency and EARFCN (3GPP TS 36.101 v15.4.0 Release 15), 2018-09, http://www.3gpp.org/ftp/Specs/archive/36_series/36.101/.

[22] 3GPP, Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Procedures in Idle Mode (3GPP TS 36.304 v15.1.0 Release 15), 2018-09, http://www.3gpp.org/ftp/Specs/archive/36_series/36.304/.

[23] 3GPP, Evolved Universal Terrestrial Radio Access (E-UTRA), Radio Resource Control (RRC), Protocol Specification (3GPP TS 36.331 v15.3.0 Release 15), 2018-09, http://www.3gpp.org/ftp/Specs/archive/36_series/36.331/.

[24] Ubuntu 16.04.5 LTS (Xenial Xerus), http://releases.ubuntu.com/16.04/ubuntu-16.04.5-desktop-amd64.iso.

[25] GSM Frequency Bands, https://en.wikipedia.org/wiki/GSM_frequency_bands/.