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

Le numéro de téléphone est un code d'identité unique d'un abonné mobile, qui joue un rôle plus important dans la vie du réseau social mobile qu'un autre numéro d'identification IMSI. Contrairement à l'IMSI, un appareil mobile ne transmet jamais son propre numéro de téléphone au réseau du côté de radio. Cependant, le réseau mobile peut envoyer le numéro de téléphone d'un utilisateur à un autre terminal mobile lorsque cet utilisateur initie un appel ou un service SMS. Sur la base des faits ci-dessus, avec l'aide d'un IMSI Catcher et d'une attaque 2G homme au milieu, ce papier a mis en œuvre un prototype de capteur de numéros de téléphone pratique et efficace ciblant les téléphones mobiles LTE. Nous avons attrapé le numéro de téléphone de l'utilisateur LTE quelques secondes après que l'appareil a campé sur notre station non autorisée. Ce document vise à vérifier que la vie privée mobile est également très vulnérable, même dans les réseaux LTE, tant que le GSM hérité existe toujours. De plus, nous avons démontré que toute personne possédant des compétences de base en programmation et connaissant les spécifications GSM / LTE peut facilement créer un capteur de numéros de téléphone en utilisant des outils SDR et des dispositifs commerciaux standard. Par conséquent, nous espérons que les opérateurs du monde entier pourront désactiver complètement le réseau mobile GSM dans les zones couvertes par les réseaux 3G et 4G dès que possible afin de réduire la possibilité d'attaques de la génération de réseaux cellulaires. Plusieurs contre-mesures potentielles sont également discutées pour défendre temporairement ou définitivement l'attaque.

1. Introduction

5G / NR (New Radio), qui a conduit de nombreuses nouvelles technologies telles que le edge computing [1], a maintenant été conçu pour remplacer progressivement les réseaux mobiles actuels, tels que la 4G / LTE (Évolution à long terme), 3G / UMTS (Universal Mobile Système de télécommunications) et 2G / GSM (système mondial pour les communications mobiles), mais ces réseaux être largement utilisé pendant une assez longue période en raison de l'existant d'énormes infrastructures de réseaux mobiles et de terminaux 2G / 3G / 4G actuellement, tout comme 2G et 3G ont coexisté avec Réseaux 4G depuis de nombreuses années de loin. Ainsi, c'est toujours un et un travail important pour étudier et réparer la sécurité et la confidentialité des problèmes dans les cellules cellulaires de faible génération (par rapport à la 5G). Le système de communication mobile 2G a de nombreux problèmes de sécurité et de confidentialité en raison de ses défauts inhérents spécifications techniques, par exemple, le manque d'authentification entre les MS (stations mobiles) et les réseaux, difficulté à mettre à niveau les algorithmes cryptographiques faibles,

et le MS campe toujours sur la cellule avec le plus fort puissance du signal radio. Les personnes malveillantes peuvent facilement créer de faux stations de base, appelées IMSI (International Mobile Abonnés), pour usurper les IMSI et les IMEI (International Mobile Equipment Identity) des utilisateurs, suivre leurs emplacements, et même intercepter leurs appels et court messages en utilisant le man-in-the-middle (MITM). La 3G / UMTS et la 4G / LTE ont été conçues pour assurer efficacement la sécurité et la confidentialité, motiver les deux à utiliser un mécanisme de chiffrement beaucoup plus puissant et l'authentification mutuelle. Néanmoins, avec l'aide du des outils logiciels de radio open source accessibles, des les travailleurs de la sécurité ont révélé de plus en plus de sécurité et vulnérabilités de confidentialité dans les réseaux mobiles LTE tels que défauts de protocole et défauts d'implémentation. Un de les failles de protocole potentielles dans LTE est que l'UE (utilisateur Équipement) peut accepter et traiter certains signaux des messages avant l'établissement du contexte de sécurité, selon le 3GPP (Third Generation Partnership Project) la spécification [2], qui peut être exploitée par des personnes malvaillantes pour attaquer à la fois les UE et les réseaux.

Par exemple, le NAS de demande d'identité (Non Access Stratum) message est un catalyseur pour les IMSI Catcher, et l'attachement des messages de rejet de la zone de rejet et de suivi (TAU) sont utilisés pour exécuter des attaques DoS (Denial of Service) sur le terminaux mobiles. Dans cet article, nous avons utilisé RRCConnection- non crypté et sans intégrité qui est un message de libération pour rediriger les téléphones mobiles LTE vers le processus de démarrage pour capturer de numéro de téléphone.

Le numéro de téléphone, alias MSISDN (Mobile Subscriber Numéro RNIS) en terminologie, concerne une importante confidentialité d'un abonné mobile ou d'une personne.Il est conçu pour identifier les utilisateurs dans notre vie réelle, en particulier dans le social mobile la vie du réseau. Selon les spécifications, le mobile l'appareil n'envoie pas son propre numéro de téléphone au réseau du côté à la radio. Ainsi, les IMSI Catchers traditionnels ne peuvent obtenir l'IMSI / IMEI de l'équipement mobile de l'utilisateur en l'envoi du message de signalisation Identity Request et à peine usurper le numéro de téléphone. Il existe une règle de mappage unique que personne ne sait entre l'IMSI et le MSISDN, parce que toutes les informations d'identité de l'abonné ainsi que les relations de mappage ne sont stockées que dans l'USIM (Universal Subscriber Identity Module) les cartes de l'opérateur et la base de données où les deux endroits sont reconnus publiquement fortement sécurisé. Les réseaux de l'opérateur traduiront IMSI au MSISDN dans le réseau principal lors de la fourniture les utilisateurs avec des services d'appel ou SMS (Short Message Service),ce fait a été exploité pour implémenter notre téléphone LTE capteur de numéro.

Dans cet article, nous avons trouvé un modèle de capteur de numéros de téléphone visant à collecter les MSISDN des utilisateurs LTE. Nous avons également démontré que le capteur de numéro de téléphone peut être uneconfiguration facile en utilisant les SDR disponibles (définis par logiciel Radio) et les outils commerciaux disponibles uniquement nécessitant des compétences de base en codage et la connaissance du GSM / Spécifications LTE. Nous sommes le premier récupérateur de numéros de téléphone que le ciblage sur les téléphones mobiles LTE et entièrement mis en œuvre par SDR. Les résultats expérimentaux ont montré que nous pouvions attraper le numéro de téléphone d'un appareil LTE en quelques secondes une fois que

l'appareil victime a campé sur notre fausse station. Le but de notre travail est de confirmer que la sécurité LTE et la vie privée peut également être très vulnérable tant que l'héritage GSM existe toujours. Ainsi, cet article espère que les opérateurs à travers le monde peut éliminer complètement le 2G / GSM réseau mobile dans les zones couvertes par la 3G et la 4G dès que possible pour garantir la sécurité et la confidentialité dans les réseaux mobiles de génération supérieure, ce qui est également considéré comme la solution finale contre ce genre pour le receveur de numéro de téléphone.

2. Arrière plan

2.1. Réseaux de communication mobile.

Les Réseaux de communication mobile jouent un rôle important dans de nombreux scénarios nos vies; par exemple, ils peuvent être très utiles en cas de catastrophe processus de sauvetage lorsqu'il a coopéré avec d'autres avancés technologies [3]. Au cours des dernières décennies, la communication mobile système de réseau a beaucoup varié, et il semble de nombreux systèmes de communication illustres du première génération (1G) à la dernière 5G.

4G / LTE et 2G / GSM sont deux communications sans fil modernes importantes et largement systèmes de communication parmi eux. Dans cet article, notre téléphone LTE modèle de capteur de nombre est également basé sur les deux mobiles systèmes. Alors maintenant, nous décrivons brièvement leurs structures de réseau et les concepts de base qui sont utiles pour comprendre le papier ensuite.

2.1.1. Système Global pour les Communications Mobiles.

Le système de communications mobiles (GSM) est le premier système de communication mobile utilisant la technologie des communications au lieu de l'analogue qui réduit la taille du corps des terminaux mobiles. La structure génèrale du réseau GSM est illustrée à la figure 1. Il existe plusieurs composants différents dans un réseau GSM typique, qui sont MS, BTS (Base Transceiver Station), BSC (Base Contrôleurs de station), MSC (Mobile Switching Center) et les bases de données (HLR / VLR / AuC / EIR) [4]. La MS peut être une cellule téléphone ou autre terminal mobile avec une carte SIM insérée. La carte SIM stocke les IMSI et MSISDN de l'abonné informations que nous visons à saisir. La même identité formation et leur relation de cartographie existent également la base de données de l'éditeur.

2.1.2. Évolution à long terme. Évolution à long terme (LTE)

les systèmes sont la communication mobile la plus populaire à travers le monde pour non seulement l'accès plus élevé taux et latence plus faible, mais aussi la sécurité renforcée et schéma de confidentialité pour les utilisateurs. Le mobile LTE basé sur IP réseau a une structure plate et beaucoup plus simple comparant au GSM. La figure 2 montre les protocoles d'interface entre les unités de réseau ainsi que deux sections principales de LTE structure du réseau: l'EUTRAN (Evolved Universal Terrestrial Radio Access Network) et l'EPC (Evolved Packet Core), et dont chacun comprend plusieurs subdivisions.

Le LTE UE contenant une carte USIM est la cible de notre expérience. L'eNodeB (Evolved Node B) fait référence à la base station qui communique avec les UE en utilisant des liaisons radio et relaie les messages NAS vers le MME (Mobility Manage- entité de gestion) qui est responsable de l'authentification et allocation des ressources aux UE. HSS (Home Subscriber

Server) est la base de données de l'opérateur qui stocke l'authentification informations et autres données d'abonnement importantes des abonnés.

2.1.3. Codes d'identité.

Les codes d'identité sont largement utilisés dans les réseaux mobiles entre l'UE et les côtés réseau, tels que Numéro IMSI, MSISDN, TAC et PLMN qui est apparu dans notre dernière expérience:

(i) IMSI.

L'identité internationale des abonnés mobiles est une identification unique mondiale pour l'USIM de l'abonné carte insérée dans UE. Il a été largement utilisé dans les systèmes de communication cellulaire depuis la naissance de le réseau mobile de première génération. Il est transtransmis au réseau en texte brut lors que la première UE lance une procédure d'attachement après le mobile

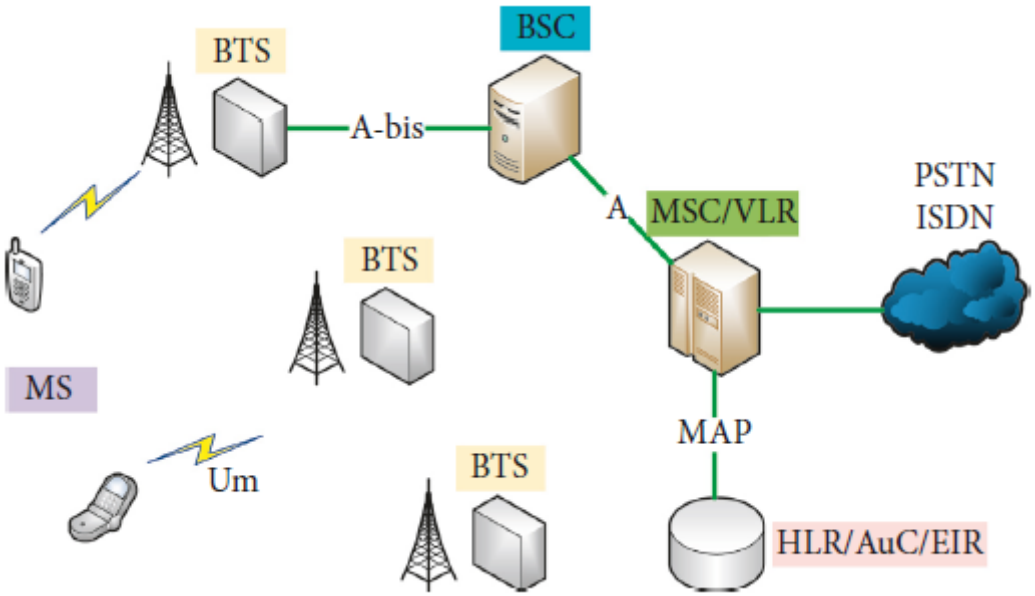

Figure 1: A general structure of GSM network.

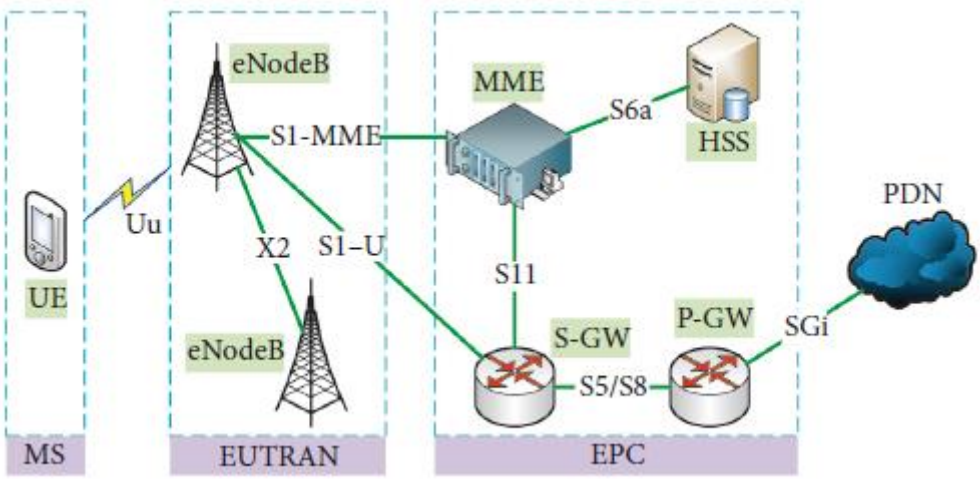

Figure 2: LTE network structure.

l'appareil sous tension, ou lorsque l'UE reçoit un Message NAS de demande d'identité du réseau noyeau.

(ii) MSISDN. Abonné mobile RNIS (intégré Services Digital Network) Numéro,

également appelé le numéro de téléphone, est utilisé pour identifier un utilisateur. Il joue un rôle important dans le social mobile vie du réseau; par exemple, nous l'utilisons pour vous inscrire comptes sociaux sur différentes applications mobiles. Personne connaît la règle de mappage entre les IMSI et MSISDN sauf la carte USIM et le opérateur. L'UE n'envoie jamais son propre MSISDN à le réseau dans la radio, mais le côté réseau peut transmettre le numéro de téléphone de l'UE à un autre appareil mobile pendant le service de lancement UE, parce que les opérateurs de réseaux mobiles traduire l'IMSI de l'UE en MSISDN selon la règle de mappage dans les réseaux centraux pour fournir Service d'identification de l'appelant.

(iii) PLMN. Code de réseau mobile terrestre public membres du MCC (Mobile Country Code) et MNC (Mobile Network Code), qui identifie réseau mobile particulier d'un opérateur dans un pays, par exemple, un numéro PLMN de China Mobile est 46000.

(iv) TAC. L'indicatif régional de suivi est l'identifiant d'une certaine zone géographique et tous les eNodeBs et les cellules situées dans la zone possèdent le même TAC.

2.2. Radio définie par logiciel. Radio définie par logiciel (SDR)

C'est un système de communication sans fil où les composants sont mis en œuvre complètement par logiciel sur un ordinateur personnel général ou système embarqué plutôt que matériel [5].

Le SDR est devenu l'outil d'analyse et de test de types de systèmes de communication mobiles en raison de sa modifiabilité et flexibilité au cours des dernières années. Pendant ce temps, un grand nombre de les projets open source ont été développés. Une telle réussite projets réussis comme srsLTE et OAI (OpenAirInterface) [6] pour LTE, OpenBSC et OpenBTS pour GSM ont mis en œuvre la plupart des fonctions et des piles de protocoles de réseau d'accès radio correspondant. Voici l'ouverture des projets sources utilisés dans notre travail:

(i) srsLTE. Les systèmes radio logiciels LTE sont des bibliothèque open source LTE pour les logiciels d'applications radio définies [7]. Ces applications compris srsUE, srsENB, srsEPC, sont pleinement compatible avec LTE Release 8 qui nous fournit un excellente plateforme d'expérimentation LTE. Nous utilisons ce logiciel pour construire un réseau LTE voyous pour rediriger le téléphone LTE cible vers notre GSM escroc réseau implémenté par OpenBSC.

(ii) OpenBSC. OpenBSC est un projet open source GSM d'Osmocom (Communauté Open Source Mobile Communication) connue sous le nom de collection de projets logiciels open source dans le domaine de communications mobiles. OpenBSC vise à être un environnement stable et système d'implémentation tout-en-un de l'OsmoBSC,OsmoMSC et OsmoHLR pour piles et éléments de protocole du GSM / 3GPP [8].

(iii) OsmocomBB. C'est aussi un GSM open source et gratuit pour l'Implémentation du logiciel de bande de base de communauté Osmocom. Les radio-amateurs peuvent faire et recevoir des appels téléphoniques, envoyer et recevoir des SMS en utilisant

OsmocomBB sur un téléphone GSM compatible tel que MotorolaC118 qui est utilisé comme MS malveillant dans notre expérience [9].

OpenBSC et srsLTE sont tous deux compatibles avec les périphérique USRP (Universal Software Radio Peripheral) de Ettus Research [10]. Nous avons donc choisi deux USRP B210 pour configurer nos eNodeB et BTS. En bref, notre capteur de numéro de téléphone est un système SDR complet en fonctionnant en source ouverte srsLTE et OpenBSC avec USRPs, OsmocomBB avec un téléphone GSM, pour atteindre l'objectif principal de numéros de téléphone dans une zone restreinte.

2.3. Travaux connexes.

Les premières attaques MITM sur GSM mobile système de communication a émergé avec un capteur IMSI [11]. Après cela, la sécurité et la confidentialité du réseau GSM face à une situation plus grave. la communication 4 G / LTE mobile a été jugée beaucoup plus sûre que ses précurseurs, GSM et UMTS. Cependant, avec le large disponibilité d'outils open source pour diverses expériences, un nombre croissant de sécurité et de confidentialité, les vulnérabilités existantes dans LTE [12–17], telles que les attaques DoS et les fuites de la vie privée, ont été découverts par des chercheurs dans dernières années. Shaik et al. a démontré qu'un attaquant actif peut localiser avec précision un appareil LTE en utilisant une station voyou LTE [17].

Jover a exploité le non chiffré et aucun protocoles LTE protégés par l'intégrité, par exemple, Attach Reject et TAU Reject messages, et a découvert les vulnérabilités de refuser le service à un appareil LTE et le rétrograder vers le réseau GSM plus précaire [14]. Shaik et Jover a montré que le capteur IMSI peut également être efficace en construisant un LTE eNodeB escroc dans le réseau mobile LTE en plus en 2G et les réseaux 3G. Mjølsnes et Olimid ont vérifié que le LTE IMSI Catcher peut être mis en œuvre par un logiciel à faible coût radio définie sans aucune programmation [15]. Hussain et al. a proposé une approche systématique pour découvrir 10 nouvelles attaques contre la sécurité, la confidentialité et la disponibilité LTE et validé la plupart [12].

Le premier capteur de numéros de téléphone a été implémenté en réseau GSM pur par Song et al. en utilisant un personnalisé carte matérielle [18], qui ne fonctionnait pas en LTE. Contrairement au ci-dessus, nos expériences ont montré que dans un système LTE, le capteur de numéro de téléphone peut capturer également les systèmes de réseaux mobiles de l'opérateur existant.

3. Modèle de capteur de numéro de téléphone LTE

L'architecture du modèle de capture de numéro de téléphone LTE se compose de deux sous-modules principaux, le redirecteur LTE et le module GSM Middle-Man, comme illustré à la figure 3.

3.1. Redirection LTE. Le redirecteur LTE est en fait un voyou

Réseau LTE (RLN) implémenté en exécutant l'open source codes, srsENB et srsEPC, sur un seul ordinateur portable avec un USRP B210 connecté via USB 3.0. Le plus important but de cette partie est de rediriger la victime UE qui tente de camper sur le RLN à notre réseau GSM

Middle-Man. Aditionellement, nous pouvons également utiliser ce module comme capteur LTE IMSI pour collecter les IMSI dans la zone du redirecteur LTE. Nous en avons fait modifications des codes sources de srsENB et srsEPC pour atteindre les objectifs ci-dessus avec succès.

3.2. GSM Middle-Man.

Le module GSM Middle-Man est un attaque MITM 2G / GSM typique qui est également implémentée par SDR dans notre travail. Il est composé d'un réseau Rogue GSM (RGN), un MS malveillant et un afficheur de numéro de téléphone. Le RGN exécute OpenBSC sur un ordinateur de bureau également avec un USRP B210, et le MS malveillant est exécuté en exécutant les codes OsmocomBB conçus sur le même bureau ordinateur ainsi qu'un MotorolaC118. La communauté RGN s'intègre avec le MS malveillant par socket réseau [19]. Le afficheur de numéro de téléphone est, par essence, un mobile général téléphone pour recevoir un appel ou un SMS du téléphone LTE victime et afficher le numéro de téléphone de la victime.

Une fois qu'un téléphone LTE est redirigé vers le RGN à un ARFCN (Absolute Radio Frequency Channel Number) [20], le RGN attrapera alors l'IMSI / IMEI de l'UE et informera le MS malveillant pour se faire passer pour cet UE victime pour lancer une Demande de mise à jour d'emplacement Location Update Reject (LUR) de type IMSI au Réseau GSM, et après l'authentification et la procédure du programme LUR, le MS malveillant effectue un appel ou envoie un SMS au afficheur de numéro de téléphone pour enfin capturer la victime UE numéro de téléphone.

3.3. Processus de signalisation du modèle. Une signalisation complète

Le processus de capture du numéro de téléphone peut être comme illustré dans la figure 4. Puisque notre modèle de capteur implique des procédures complexes des protocoles du réseau 4G / LTE et 2G / GSM, nous listons simplement la signalisation principale dans chaque procédure. Lorsque le système de capture de numéro de téléphone est activé,

le RLN diffusera en continu les informations du système de la fausse cellule à un EARFCN donné [21]. Une fois un UE LTE est autour de notre fausse station, elle reçoit ces informations importantes, y compris MCC, MNC et TAC, via les messages Master-InformationBlock (MIB) et SystemInformationBlock (SIB), et notre fausse cellule répond aux critères de resélection de la cellule dans LTE [22], puis l'UE lancerait une zone de suivi Mise à jour de notre RLN. Quand le faux EPC reçoit la demande TAU, il peut soit usurper l'IMSI de l'UE victime en envoyant le message de demande d'identité avant de rediriger l'UE vers la fausse station GSM ou rediriger directement l'UE victime vers notre réseau GSM en concevant le redirectedCarrierInfo dans le message RRCConnectionRelease. Le redirectedCarrierInfo indique une fréquence porteuse et est utilisé pour rediriger les UE vers un autre RAN (Radio Access Réseau), par exemple GSM [23]. Après que l'UE victime a accédé à notre réseau GSM et lancé une procédure LUR, nous envoyons la demande d'identité message à l'UE victime et obtenir l'IMSI de la victime dans le Message de réponse d'identité. Ensuite, le MS malveillant sera informé de l'IMSI de l'UE de la victime et lancer une enquête de type IMSI LUR au réseau GSM de l'opérateur à l'aide de l'IMSI de la victime.

On s'attend à ce que le MS malveillant reçoive une authentification, le Message de demande contenant le paramètre d'authentification (Rand) du réseau GSM commercial, et le livrer au

RGN. Le RGN authentifie alors l'UE victime en utilisant le Rand récepteur et obtient le SRES de la victime UE dans le message de réponse d'authentification. Finalement, le MS malveillants utilise ce SRES pour répondre à l'authentification et termine la procédure LUR après la réception du message d'acceptation de la mise à jour de l'emplacement contenant le TMSI (Temporary Mobile Subscriber Identity) que le réseau GSM de l'opérateur qui lui est alloué. En ce moment, Les États membres malveillants peuvent passer un appel ou envoyer un SMS au Afficheur MSISDN utilisant un réseau GSM commercial. l'afficheur reçoit l'appel ou le SMS et obtient le numéro de téléphone de la victime UE.

4. Configuration expérimentale

Dans cette section, nous présentons la configuration expérimentale de notre modèle de capteur de numéro de téléphone comprenant à la fois le matériel pièce et logiciel. Système de communication traditionnel et équipements avaient généralement d'énormes corps et étaient extrêmement coûteux. Cependant, la chose la plus ennuyeuse pour un chercheur en systèmes de radiocommunication ou un amateur est qu'ils pouvaient à peine connaître les codes sources en cours d'exécution sur le dispositifs. Heureusement, la technologie SDR et le low-cost module, de matériel sur étagère, ont illuminé ces personnes.

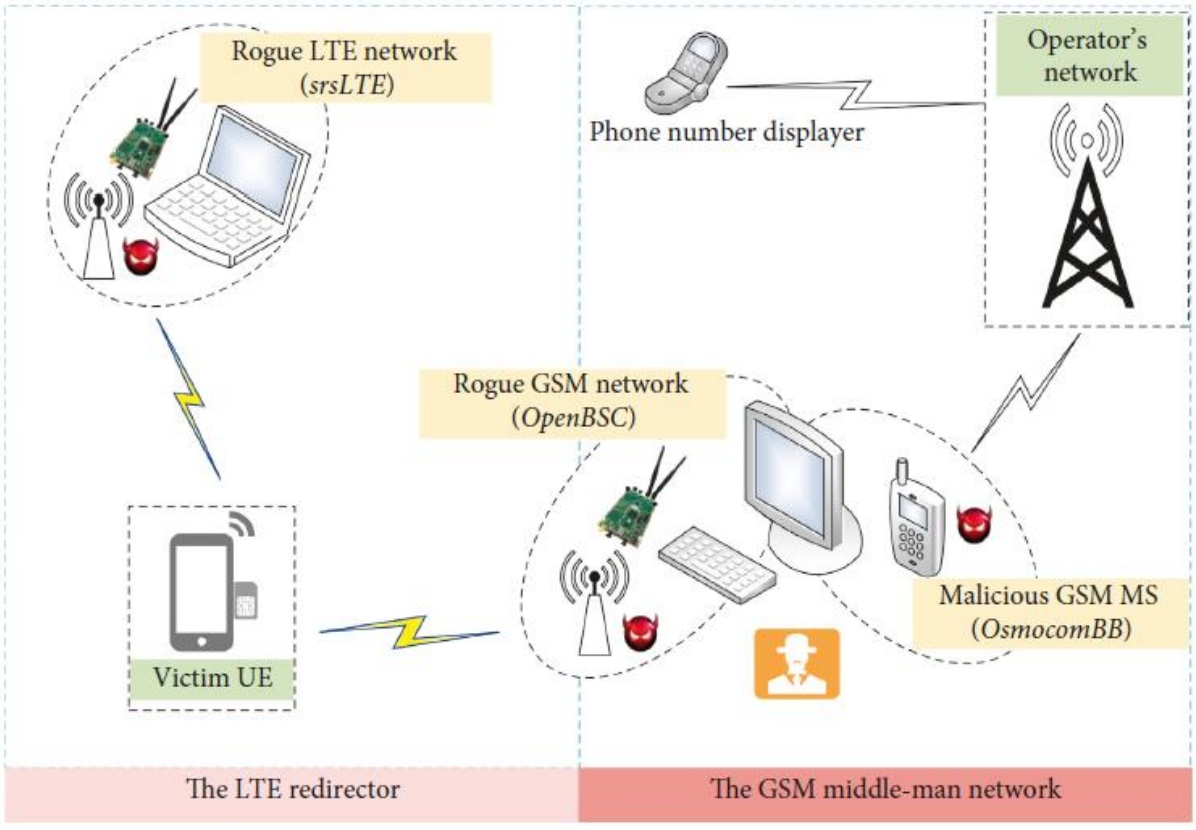

Figure 3: LTE phone number catcher model.

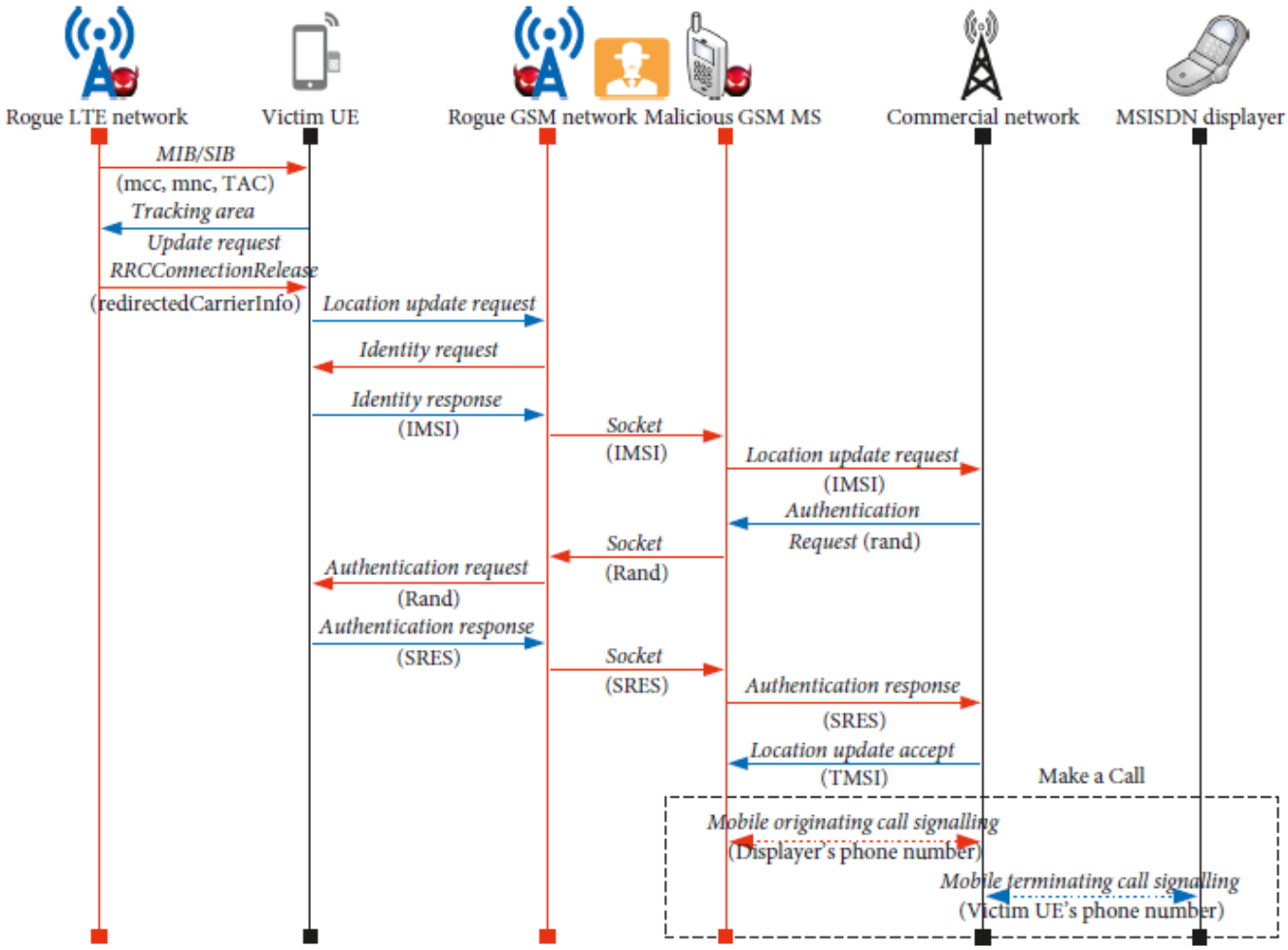

Figure 4: Main signalling of the phone number catcher model.

4.1. Matériel.

Tous les appareils matériels utilisés pour notre experimentation est facilement accessible depuis le marché. La figure 5 illustre la configuration expérimentale du matériel dans notre travail (à l'exclusion des câbles de données USB).

4.1.1. Des ordinateurs.

Un ordinateur de bureau (Gigabyte B85M-D3H i5-4430 CPU@3.00 GHz × 4) et un ordinateur portable ordinateur (Dell Latitude E5470, CPU i7-6600U @ 2,60 GHz × 2) ont été utilisés dans l'expérience.

Le fonctionnement des systèmes des deux ordinateurs sont Ubuntu 16.04 LTS 64 bits [24] avec la version 4.32.0-61-low-kernel du noyau. Tous les deux les ordinateurs étaient connectés aux émetteurs-récepteurs via USB

3.0. L'ordinateur de bureau était également équipé de périphériques standard, y compris moniteur, souris et clavier.

4.1.2. Émetteur-récepteur radio. Deux appareils USRP B210 et un

Le téléphone GSM MotorolaC118 constituait l'émetteur-récepteur radio Matériel. Nous pouvons programmer le B210 pour transmettre et recevoir tout signal radio que nous voulons sur une large gamme de fréquences radio, de 70 MHz à 6 GHz, couvrant toute la fréquence des bandes LTE.

Le C118 peut être utilisé pour exécuter la même fonction à Bande GSM 900/1800 MHz [25].

4.1.3. Téléphones de test.

Deux téléphones mobiles LTE commerciaux ont été utilisés pour accomplir différentes tâches. Un Apple iPhone6s plus (A1699) prenant en charge toutes les fréquences LTE et GSM bandes en Chine, a travaillé comme victime UE; pendant ce temps, le Meizu M5 Note a été utilisé comme afficheur de numéro de téléphone.

Nous avons également utilisé la note M5 pour recueillir le LTE de l'opérateur et Informations sur le réseau GSM telles que (E) ARFCN, le numéro PLMN et le TAC pour configurer notre RLN et RGN. Le 6sp et le M5 Note utilisaient deux cartes USIM différents d'un même opérateur en Chine.

4.2. Logiciel.

Trois ensembles différents de logiciels open source, srsLTE, OpenBSC et OsmocomBB ont été utilisés dans notre mise en place du capteur de numéros de téléphone. Nous avons déjà fait une introduction à eux en section arrière-plan. Nous venons de télécharger, construire et tester la code source de srsLTE sur l'ordinateur portable ainsi que le Code OpenBSC et OsmocomBB sur l'ordinateur de bureau pour la configuration du logiciel expérimental. Plus détaillé et spécifique les étapes se trouvent dans [7–9]. Ensuite, nous pourrions modifier et reconstruit les codes sources pour atteindre les fonctions que nous voulons.

En raison des dispositifs matériels à faible coût disponibles et de l'ouverture du logiciel source, toute personne possédant uniquement des compétences de base en la connaissance des spécifications GSM / LTE pourrait être expérimenté.

5. Mise en œuvre et résultats du DTS

Dans cette section, nous décrivons comment nous avons mis en œuvre le capteur de numéro de téléphone LTE utilisant SDR et présenter les résultats de notre expérience. Nous avons réalisé toutes les expériences dans notre laboratoire de sécurité des réseaux sans fil pour éviter affectant d'autres UE normaux. Nous avons gardé la victime UE près di système de capture de numéro de téléphone dans chaque expérience afin de répondre aux besoins de puissance du signal radio de la cellule resélection.

5.1. Mise en œuvre du SDR

5.1.1. Redirection LTE.

Nous avons exécuté srsENB et srsEPC sur l'ordinateur portable pour construire un RLN. Nous avons d'abord utilisé la note M5 pour collecter les informations du réseau LTE et GSM de l'opérateur à proximité nécessaires à l'expérience.

Nous avons accédé au Mode de test du M5 en composant le ∗ # ∗ # 4636 # ∗ # ∗, qui était de la même manière que décrit dans [15]. Une fois que nous avons réussi EARFCN, MCC, MNC et TAC du réseau LTE commercial et les ARFCN des réseaux GSM (voir Figure 6) autour de notre laboratoire, nous avons configuré notre eNodeB en suivant :

(a) L'eNodeB escroc a utilisé les mêmes MCC, MNC et EARFCN comme commercial

(b) Le TAC de l'eNodeB escroc a été configuré sur un valeur proche de mais non égale à la valeur commercial

c) L'ARFCN vers lequel l'UE victime a été redirigé ét mis à une valeur différente de ces ARFCN que nous avait rassemblé

Nous avons apporté les modifications nécessaires à la source srsENB codes pour permettre à l'eNodeB escroc de renvoyer un rectedCarrierInfo encapsulé dans le message RRCConnectionRedirected après que l'eNodeB a reçu une demande TAU de la victime UE. De plus, nous modifions également Codes source srsEPC pour utiliser l'eNodeB escroc comme IMSI Catcher.

5.1.2. Réseau des intermédiaires.

Nous avons exécuté OpenBSC etOsmocomBB sur le bureau pour construire le middle-man réseau. Le MCC et MNC de la fausse station de base (BS) ont été définies sur les mêmes valeurs que le eNodeB escroc.

Notamment, la définition de la valeur de l'ARFCN pour être exactement celui contenu dans le redirectedCarrierInfo était l'étape le plus importante. Nous avons simplement modifié la source nécessaire des codes d'OpenBSC et d'OsmocomBB à implémenter le processus de signalisation comme le montre la figure 4. Nous avons également mis sous tension M5 Note en attente de l'appel du victime UE.

5.2. Résultats expérimentaux.

Nous avons complètement exécuté l'expérimentation plusieurs fois, et à chaque fois, nous avons toujours eu les résultats expérimentaux que nous attendions après avoir exécuté le système LTE de capture de numéro de téléphone avec succès.

Dans le trafic du voyous eNodeB fonctionnant à la fois comme IMSI Catcher et un redirecteur, nous avons vu la demande TAU de la victime UE, le message RRCConnectionRelease au UE et IMSI de l'UE victime dans la réponse d'identité comme le montre la figure 7.

Nous pourrions probablement déduire de la redirectedCarrierInfo dans la figure 7 que l'UE victime a été redirigée vers notre faux GSM BS, et ce qui s'est passé ensuite dans le BS aussi a confirmé cela. Les figures 8 et 9 ont capturé une partie des Journaux OpenBSC et OsmocomBB, respectivement, dans un périment. Ce qui s'est passé pourrait être décrit comme suit procédures en fonction des résultats:

(i) L'UE victime a initié un LUR au RGN après camper dans notre cellule

(ii) Le RGN a capturé l'IMSI et l'IMEI (SV) du victime UE, et les a envoyés à l'EM malveillants à démarrer un LUR de type IMSI vers le réseau GSM commercial

Figure 5: Experimental hardware setup.

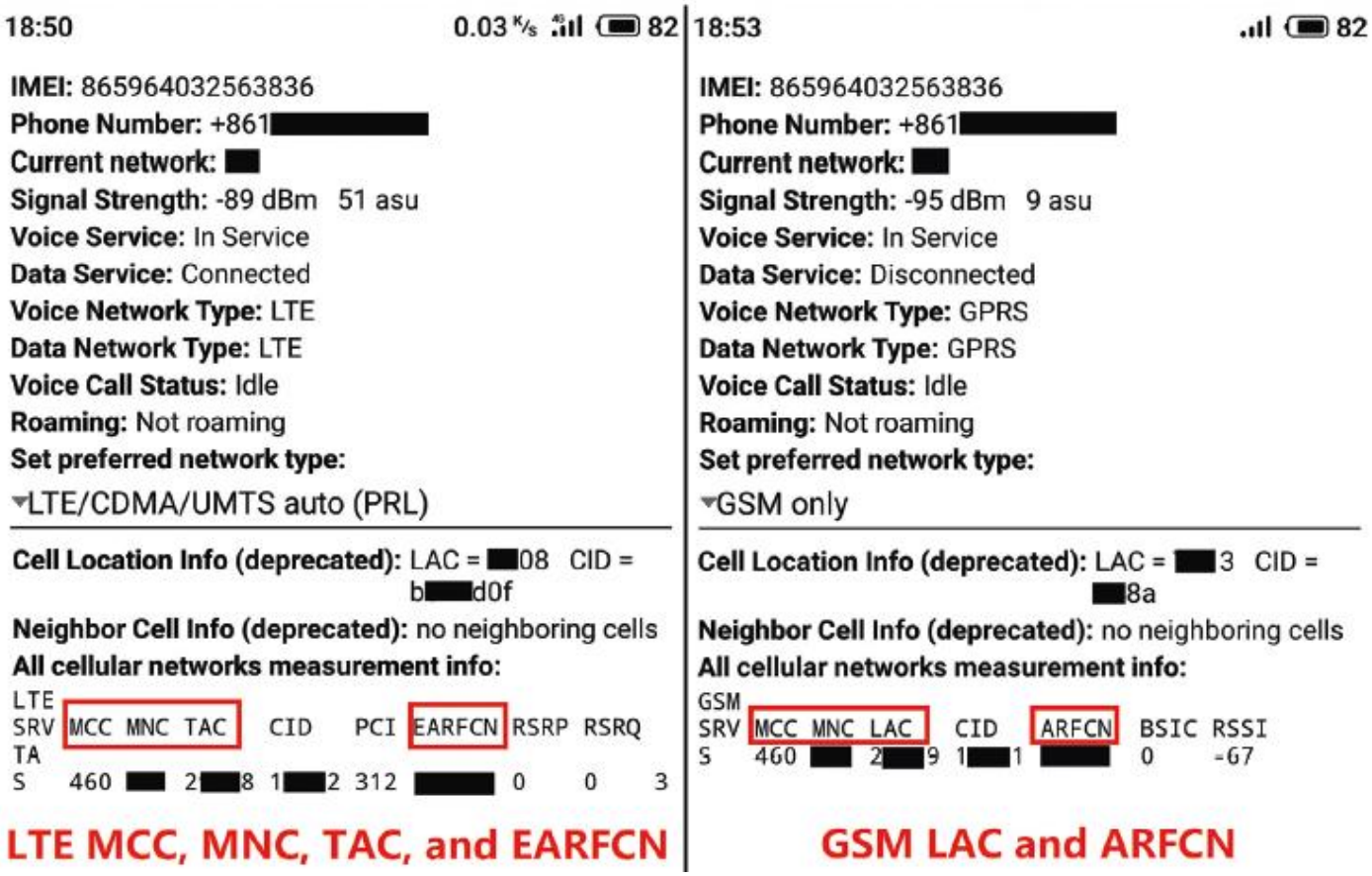

Figure 6: Necessary network information we collected.

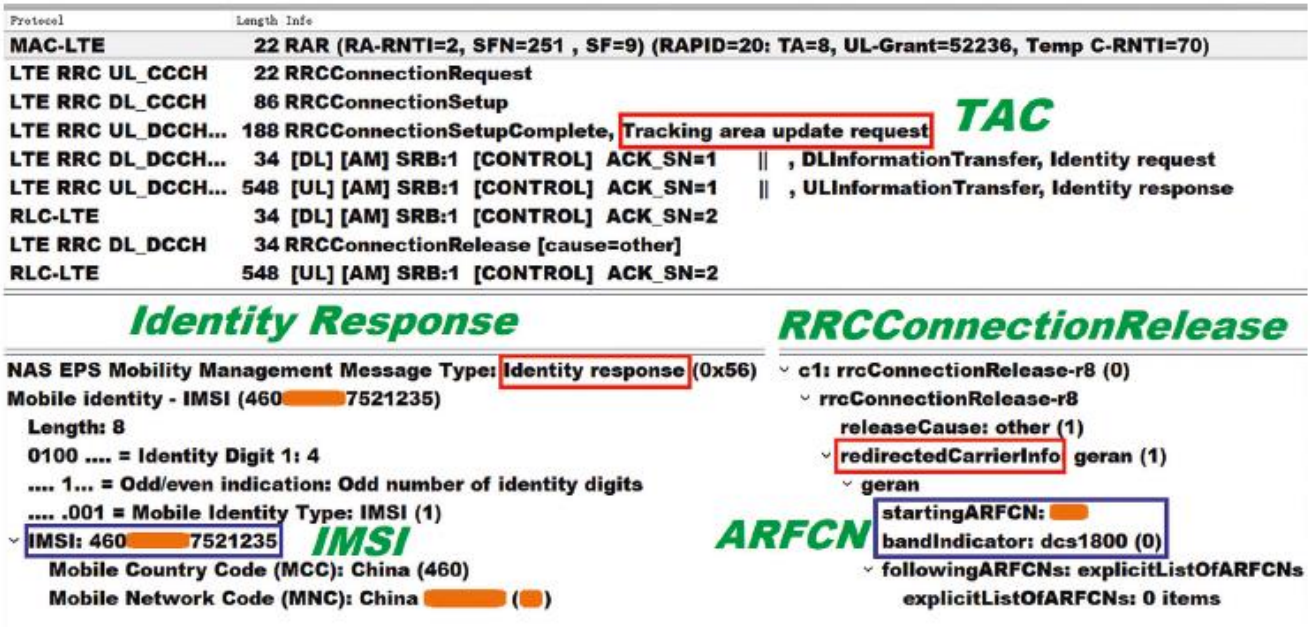

Figure 7: Partial air traffic of the rogue eNodeB.

(iii) Le MS malveillant a relayé le paramètre Rand reçu de l'opérateur au RGN

(iv) Le RGN a utilisé le Rand pour authentifier la victime UE et passé le SRES à la MS malveillante

(v) L'MS malveillant a terminé avec succès l'autorisation procédure d'identification en renvoyant le SRES au réseau GSM de l'opérateur et a également achevé la Procédure LUR en recevant le message de la mise à jour de l'emplacement Accept

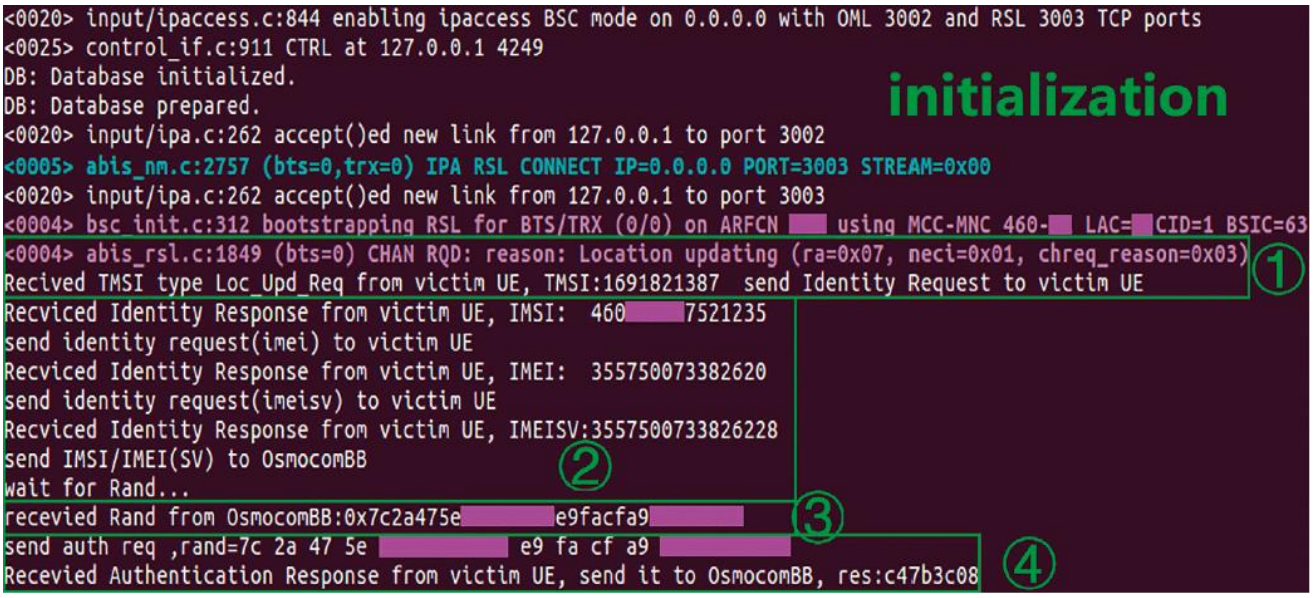

Figure 8: Part of the OpenBSC logs.

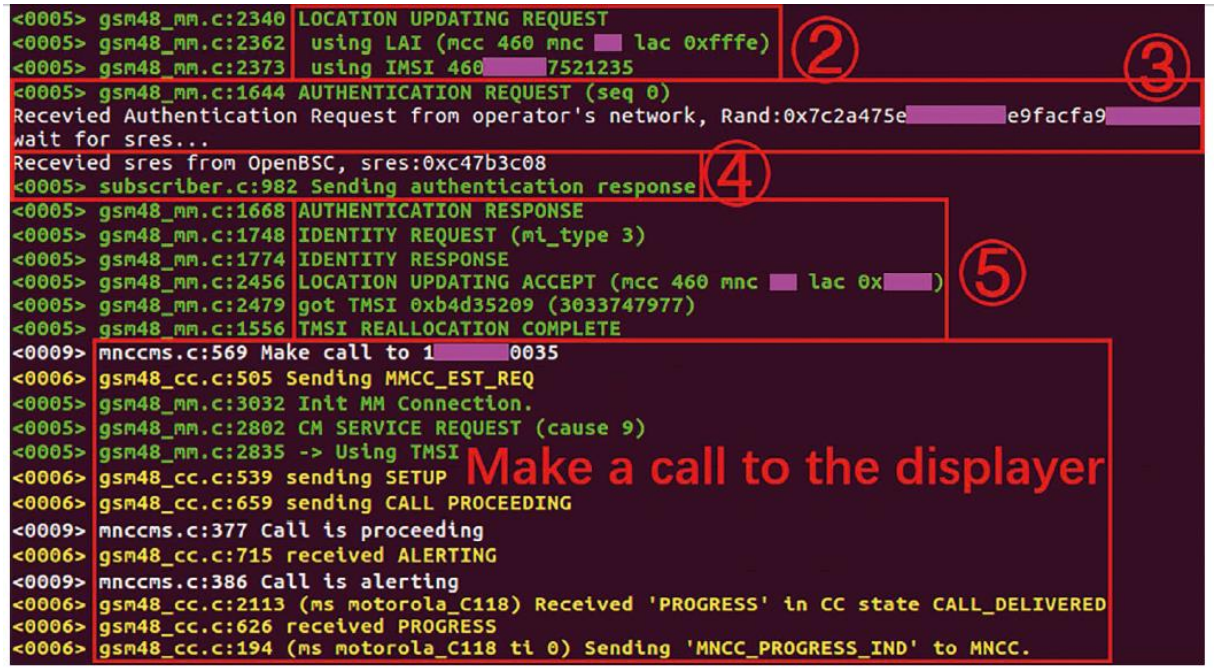

Figure 9: Part of the OsmocomBB logs.

Après cela, nous avons utilisé le logiciel OsmocomBB pour faire un appel à l'afficheur en utilisant l'identité de l'UE victime. Comme attendue, le M5 Note a reçu un appel après la malveillance MS lance un appel d'origine mobile et affiche le numéro de téléphone de l'UE victime sur la figure 10, qui a confirmé la faisabilité de notre numéro de téléphone LTE modèle de receveur.

6. Contre-mesure et discussion

Les résultats expérimentaux ont montré que nous avons pris le test LTE le MSISDN du téléphone portable avec succès lorsque le téléphone de la victime était très proche du système de capture de numéro de téléphone. Dû au problème de puissance du signal radio, le système pourrait être efficace que dans une petite plage lors de l'utilisation des dispositifs et équipements de test. Cependant, lorsque équipé de PA (Power Amplifier), le système de capture de numéro de téléphone LTE est capable d'affecter une zone assez large.

L'attaque est principalement théorique et dans un scénario réel, il serait difficile pour les gens normaux d'en faire bon usage des numéros de téléphone obtenus. Cependant, les agences de renseignement et de force peuvent utiliser ce système comme un outil pour suivre efficacement un criminel en temps réel, quand seulement connaître le numéro de téléphone de ce criminel. Pendant ce temps, les contrevenants pourraient utiliser le système pour écouter confidentialité pour les utilisations illégales, par exemple, les promotions publicitaires, qui brisent sérieusement la sécurité et la confidentialité dans les mobiles réseau.

C’est pourquoi nous proposons maintenant des mesures attaque. La cause première de cette attaque est que les UE acceptent le redirigéCarrierInfo non protégé, donc sous une compromis raisonnable, du point de vue de la spécification LTE, le moyen le plus simple de résoudre ce problème est de transmettre formation qu'après la mise en place du contexte de sécurité. Être-côtés, car il y a un changement perceptible dans le mobile l’icône du réseau sur l’écran du téléphone portable de l'attaque de la victime, l'utilisateur LTE peut activer le mode avion

médiatement en remarquant être attaqué pour éviter la vie privée fuite ou désactiver directement le réseau GSM du téléphone portable.

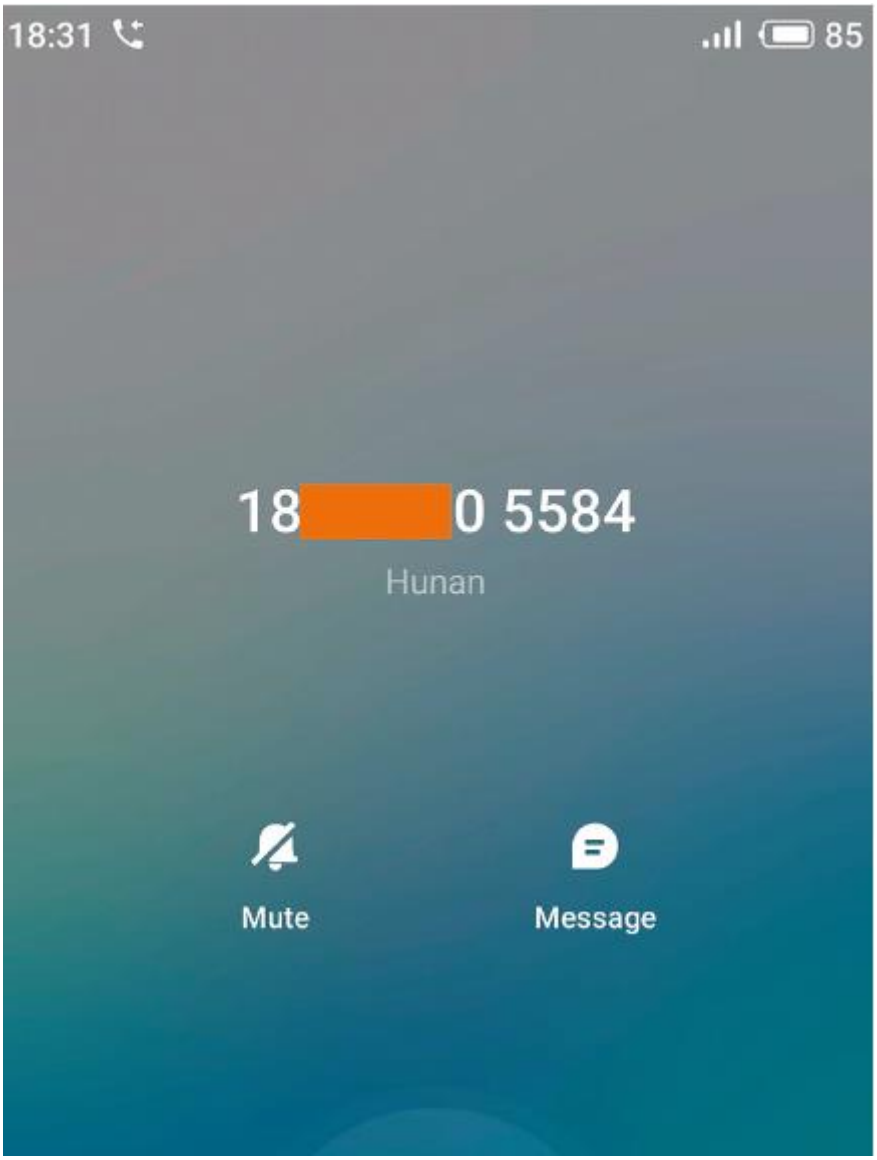

Figure 10: Victim UE's phone number we caught.

Côté opérateur, il n'y a pas de besoin particulier de 2G dans les domaines couverts par la 4G et la 3G; ainsi, la fermeture du réseaux GSM dangereux dans ces domaines est un ultime Solution.

7. Conclusion

En conclusion, ce document a mis en place un numéro de téléphone prototype de capteur destiné aux téléphones mobiles LTE en utilisant des outils SDR facilement disponibles et des

vices. Nous avons décrit le modèle du numéro de téléphone catcher, les implémentations SDR, et a présenté les résultats expérimentaux. Les résultats ont montré que l'existence de GSM a un impact sérieux sur la confidentialité des mobiles dans les réseaux LTE. Ainsi, ce document espère que les opérateurs du monde entier peut totalement désactiver les réseaux 2G / GSM dans les zones couvertes par la 4G et la 3G dès que possible, afin de garantir la

sécurité et confidentialité pour les abonnés de génération supérieure des réseaux mobiles. Enfin, nous avons discuté du potentiel défenses.

Disponibilité des données

Les données de trafic aérien de l'eNodeB escroc utilisé pour les résultats de cette étude n'ont pas été mis à disposition gratuitement en raison de la nécessité de protéger la confidentialité des utilisateurs. Demandes de l'accès aux données doit être fait à Chuan Yu, yuchuan17 @ nudt.edu.cn.

Les conflits d'intérêts Les auteurs déclarent ne pas avoir de conflits d'intérêts.

Remerciements

Le travail est soutenu par le National Key Research and Programme de développement de la Chine dans le cadre de Grant nos. 2018YFB180020, SQ2019ZD090149 et 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 Pro-ceedings 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/.