LTE and IMSI catcher myths

Ravishankar Borgaonkar*, Altaf Shaik¶, N. Asokan#, Valtteri Niemi§, Jean-Pierre Seifert¶

* Aalto University
Email- rbbo@kth.se

¶ Technische Universita¨t Berlin and Telekom Innovation Laboratories
Email- (altaf329, jpseifert) @sec.t-labs.tu-berlin.de

# Aalto University and University of Helsinki
Email: asokan@acm.org

§ University of Helsinki
Email - valtteri.niemi@helsinki.fi

Abstract

Mobile devices have become a necessity in human life, thanks to availability and bandwidth of LTE network services everywhere. LTE (4G) communication protocols promise several appropriate levels of subscriber location privacy and availability of network services all the time. In this work, we analyze access network security protocols of LTE networks. We discovered several issues in LTE security standards and baseband chipsets. We demonstrate feasibility of attacks exploiting these issues against LTE devices using an experimental fake base station.

Introduction

Promise of LTE high-speed data connections with the growth of smartphones and new mobile applications and services are playing a vital role in providing vital societal benefits and enriching consumer experience. However these developments and reliance on mobile networks for emergency services are also leading to the emergence of new privacy and availability challenges across the mobile ecosystem.

Security in mobile communications networks has been improving in every generation. 3G introduced mutual authentication that made it a lot harder to mount fake base station attacks (such as those used in IMSI catchers). LTE tightened up many signaling protocols by requiring authentication and integrity protection for them. The generally held belief has been that LTE security is robust and in particular, fake base station attacks mostly difficult to mount.

In this work, we discovered different issues in LTE 3GPP specification and baseband chipsets. These issues allow an attacker to mount fake base station attacks to track LTE subscribers and deny selected network services. We evaluated attacks on commercially available LTE phones at low cost and in a real operator network. In addition, we discuss LTE network configuration issues responsible for assisting passive tracking of subscribers.

The paper is structured as follows. Chapter 1 presents attacks leaking information about subscriber locations. Denial of services attacks against subscribers attached to LTE networks are discussed in Chapter 2. Ethical considerations and experimental setup are presented in Chapter 3. We conclude in Chapter 4.

Note that, we describe our attacks briefly in this paper. More detailed and technical information about our research can be found in [1].

1. Location Leak Attacks

Already when 2G (GSM) networks were being designed, location privacy was considered important. When a mobile device attaches to a network, it is given a temporary identifier (known as TMSI - Temporary Mobile Subscriber Identity). All the signaling messages between the mobile device and the network will thereafter refer only to the TMSI, rather than the user's permanent identifiers (such as phone numbers or IMSIs - International Mobile Subscriber Identity). TMSIs are random and updated frequently (e.g., whenever the mobile device moves to a new location area). The idea is that an attacker passively monitoring radio communication would not be able to link TMSIs to permanent identifiers or track movements of a given user (since his TMSIs would change over time). A couple of years ago, Dennis Foo Kune et al showed that an attacker in a 2G (GSM) network can trigger a paging request (by sending a silent text message or initiating and quickly terminating a call) to be sent to a target user with a given phone number [2]. Paging requests contain TMSIs. The attacker can thereby link TMSIs to phone numbers.

We discovered that paging requests can be triggered in a new and surprising manner -- via social network messaging apps. For example, if someone who is not your Facebook friend sends you an instant message, Facebook will silently put it in the "Other" folder as a spam protection mechanism (unless the spammer pays Facebook 1€!). If you have Facebook Messenger installed on your LTE smartphone, incoming messages, including those destined to the Other folder, will trigger a paging requests, allowing a passive attacker to link your TMSI to your Facebook identity and track your movements. To make matters worse, we noticed that TMSIs are not changed sufficiently frequently -- in one urban area TMSIs assigned by multiple mobile carriers persisted up to three days! In other words, once the attacker knows your TMSI, he can passively track your movements for up to three days.

An active attacker using a fake base station can do even better. LTE access network protocols incorporate various reporting mechanisms that allow the network to troubleshoot faults, recover from failures and assist mobiles in handovers. For example, after a failed connection, a base station can ask an LTE device to provide a failure report with all sorts of measurements including which base stations are seen by the device and with what signal strength. Once an attacker grabs such a report, he can use the information to triangulate the device's location. In fact, at least one device we tested even reported its exact GPS location. Failure recovery mechanisms are essential to the reliable operation of large mobile networks -- LTE designers had a difficult design trade-off between potential loss of user privacy and ensuring network reliability.

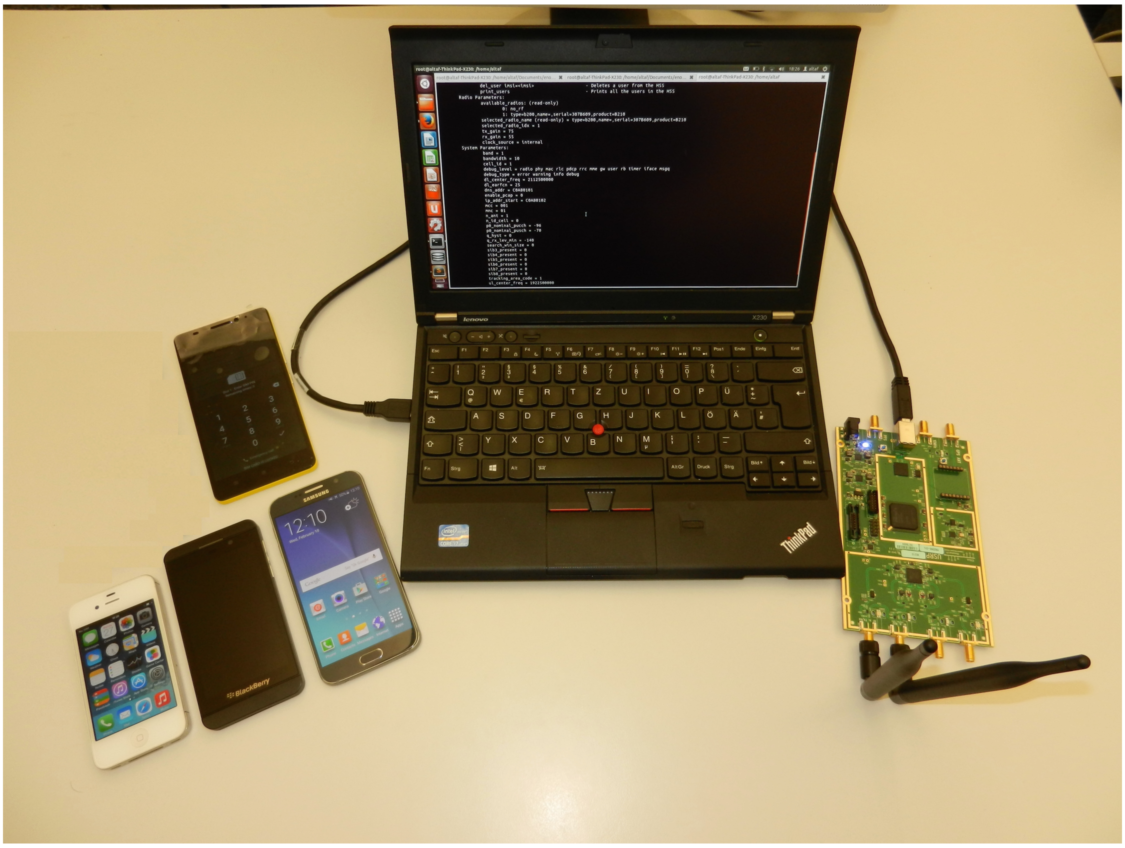
2. Denial of Service Attacks

Imagine that you travel to a different country but your mobile subscription does not include roaming. When your phone tries to connect to the network at your destination, it will be rejected with an appropriate "cause number" (such as "ROAMING NOT ALLOWED"). Your phone will dutifully accept this directive and *will not* attempt to connect again until you re-initialize the device (e.g., by rebooting it). This is so that your device does not waste its battery in vain by repeatedly trying to connect to a network only to be rejected. It is also a way to minimize unnecessary signaling over the air. In other words, this design decision was also motivated by a desire to trade-off in favor of reliability and performance. You can guess the rest: we show, for example, that an attacker can deny 4G and 3G services to a 4G device, thereby effectively downgrading it to 2G. Once downgraded, the device is open to all the legacy 2G vulnerabilities. The parameter negotiation during the LTE connection set up process is vulnerable to bidding down attacks by a man-in-the-middle who can fool an LTE device and an LTE network into concluding that they can only communicate using 2G.

3. Experimental Setup and Ethical Considerations

To evaluate feasibility of the attacks, we built a fake base station using open source software and readily available hardware tools.

To build an LTE test network, we used a USRP B210 device [3], which acts as a base station. On the software side, we modified OpenLTE [4] and srsLTE [5] packages in order to be able to communicate with commercial LTE devices. Following figure depicts the setup.



```
        del_user imsi=<imsi>                  - Deletes a user from the HSS
        print_users                           - Prints all the users in the HSS
  Radio Parameters:
        available_radios: (read-only)
              0: no_rf
              1: type=b200,name=,serial=307B609,product=B210
        selected_radio_name (read-only) = type=b200,name=,serial=307B609,product=B210
        selected_radio_idx = 1
        tx_gain = 75
        rx_gain = 55
        clock_source = internal
  System Parameters:
        band = 1
        bandwidth = 10
        cell_id = 1
        debug_level = radio phy mac rlc pdcp rrc mme gw user rb timer iface msgq
        debug_type = error warning info debug
        dl_center_freq = 2112500000
        dl_earfcn = 25
        dns_addr = C0A80101
        enable_pcap = 0
        ip_addr_start = C0A80102
        mcc = 001
        mnc = 01
        n_ant = 1
        n_id_cell = 0
        p0_nominal_pucch = -96
        p0_nominal_pusch = -70
        q_hyst = 0
        q_rx_lev_min = -140
        search_win_size = 0
        sib3_present = 0
        sib4_present = 0
        sib5_present = 0
        sib6_present = 0
        sib7_present = 0
        sib8_present = 0
        tracking_area_code = 1
        ul_center_freq = 1922500000
```

Fig. Experimental Setup

We took precautions to prevent our experiments from interfering with other phone users in the vicinity. Active attacks were carried out in a Faraday cage [6] whereas for passive attacks we made sure not to cause service interruption to normal users. Only our designated test devices were subject to any attack. Further description of techniques we used can be found in [1]. We notified relevant vulnerabilities to baseband chipset vendors and standardization bodies.

4. Conclusions

We have shown new vulnerabilities in LTE standards and baseband chipsets, which allow tracking of subscribers and denial of services using a fake base station. We tested several LTE devices to evaluate our attacks. Further we showed how privacy attacks can be exploited using popular social application such as Facebook in our test experimental setup. Our research report [1] provides more technical details. For up–to–date information about our work, check out the project website (https://se–sy.org/

References

1. http://arxiv.org/abs/1510.07563

2. http://www.internetsociety.org/location-leaks-over-gsm-air-interface

3. http://www.ettus.com/product/details/UB210-KIT

4. http://openlte.sourceforge.net/

5. https://github.com/srsLTE/srsLTE

6. http://www.gamry.com/application-notes/instrumentation/faraday-cage