Exposing LTE Security Weaknesses at Protocol Inter-layer, and Inter-radio Interactions

Muhammad Taqi Raza[1(✉)], Fatima Muhammad Anwar[2], and Songwu Lu[1]

[1] Computer Science Department, University of California – Los Angeles, Los Angeles, USA
{taqi,slu}@cs.ucla.edu

[2] Electrical Engineering Department, University of California – Los Angeles, Los Angeles, USA
fatimanwar@ucla.edu

Abstract. Despite security shields to protect user communication with both the radio access network and the core infrastructure, 4G LTE is still susceptible to a number of security threats. The vulnerabilities mainly exist due to its protocol's inter-layer communication, and the access technologies (2G/3G) inter-radio interaction. We categorize the uncovered vulnerabilities in three dimensions, i.e., authentication, security association and service availability, and verify these vulnerabilities in operational LTE networks. In order to assess practical impact from these security threats, we convert these threats into active attacks, where an adversary can (a) kick the victim device out of the network, (b) hijack the victim's location, and (c) silently drain the victim's battery power. Moreover, we have shown that the attacker does not need to communicate with the victim device or reside at the device to launch these attacks (i.e., no Trojan or malware is required). We further propose remedies for the identified attacks.

Keywords: LTE security · LTE protocol interactions
LTE interaction with 2G/3G networks

1 Introduction

The fourth-generation (4G) Long Term Evolution (LTE) technology offers wide-area mobile and wireless access to smart-phone and tablet devices. LTE is a complex network technology consisting of multiple subsystems – designed to provide undisrupted connectivity and backward compatibility to legacy 3G/2G networks. The operations of these subsystems are standardized [1]. These standards ensure interoperability between the device and the network. From the security perspective, LTE employs mechanisms to ensure authentication, authorization, access control, and user data confidentiality between the device and the network.

X. Lin et al. (Eds.): SecureComm 2017, LNICST 238, pp. 312–338, 2018.
https://doi.org/10.1007/978-3-319-78813-5_16

Although both control and data planes in LTE adopt security measures, we have found that security is preserved only for end-to-end user communications. Device operations are carried out by transferring the control-plane packets between different layers of LTE protocols. Similar to the Internet and WiFi designs, LTE protocol layers are functionally independent. Yet these layers communicate with each other to facilitate device operations. Potential loopholes arise when LTE security mechanisms do not guard such inter-layer traffic flows. Certain device control-plane messages may escape authentication and authorization verifications at these layers in the network.

Our study reveals that the LTE network is not secure along the following three dimensions:

1. [**Weak Authentication**] Some messages sent from the LTE network to the device, soon after the device recovers from its idle mode, are executed without any authentication. This gives an adversary a chance to kick the victim out of the network.
2. [**Weak Security Association**] On inter-radio interactions, the target network incorrectly assumes that device has already been authenticated and authorized by the source network. During inter-radio interactions, the adversary can hijack the device location registration procedure and register wrong victim location at the network. The victim device consequently becomes unreachable from the network.
3. [**Lack of Access Control/Non-authorization**] The adversary is authorized to communicate with the victim without having its consent. This vulnerability allows an adversary to drain the victim device's battery by sending periodic control messages.

These security weaknesses arise when (1) different LTE protocol layers communicate with each other, and (2) LTE protocol communicates with its legacy technology, such as WCDMA/3G, and GSM/2G. In the end-to-end protocol interactions, intermediate protocol layers (either at the local device or the remote network) act as forwarding layers. They forward the packets to the layer above or below without inspecting the contents of the forwarded packets. Hence, *packet forwarding blindly facilitates such protocol interactions.*

Furthermore, LTE protocol layers perform atomic network operations to interact with one another. These interactions happen without any integrity check between these layers. This signifies that *the trust among these protocol layers is unconditional.*

We also found that certain control messages are accepted at the network before the device security mechanisms kick in. *LTE network assumes that certain control messages after the device's idle state are legitimate.* These messages specify the device's intent for different types of services, e.g., voice or data service, and set up the network resources accordingly. The device can misuse network resources by generating fake control messages.

Moreover, when the LTE protocol communicates with its legacy technology (such as 3G or 2G), it transfers the user session and security keys to the legacy network. The legacy network does not perform any authentication procedure

Table 1. Summary of findings

Capability	Vulnerabilities	Loophole	Attacks	Root cause	Defense solution
Authentication	Blind execution of messages, non-verification of originator	Authentication bypass	Detach the victim from the network	Network executes message for the device idle mode operation	The device identity should resolve into correct Device-eNodeB-S1AP-ID
Security association	Denial of service, No check on deceptive messages	Network relies on old authentication	Rendering device to be unreachable from the network	Security context mismatch	The device should be re-authenticated after inter-radio switch
Authorization & ACL	Unconditional trust across protocol layers	Strong assumption of secure layers	Draining victims' battery	Device has no authorization process	ACL should be maintained for transitive trust

with the device. Instead, it assumes that the device has already been authenticated at the time of registration with the LTE network. It is possible that the device's native security context gets expired and becomes invalid. This potentially *creates two conflicting security setup views at the device and the legacy network*. Therefore, the device can trick the legacy network by believing that its native security context is valid.

Attacks and Impact. Once we have confirmed the vulnerabilities through analyzing LTE standards, we validate them in operational LTE networks. We thus use the LTE modem diagnostic tool, the non-volatile memory manager, and TeraTerm [2], to capture and analyze traces. After validation, we convert these vulnerabilities into attacks by using our testbed and exploit these weaknesses to compromise the network security. For example, an adversary sends a wireless connection request to the LTE base station and piggybacks the network join request message destined for the LTE core network. Upon receiving the message from the legitimate base station, the core network marks the join request message as being valid and executes it. This procedure can be exploited by an adversary that can make a legitimate wireless connection with the LTE base station but sends unauthorized device messages (e.g., device power-off notification) by impersonating the victim device to the core network. Consequently, the core infrastructure wrongly executes the message (e.g. closes the victim device session).

The potential impacts from such vulnerabilities are quite high. The adversary can kick the victim out of the network, hijack the victim's device location update procedure and register wrong location of the victim at the network, and silently drain the victim's battery. To make things worse, the attacker does not need to interact with the victim device to launch these attacks, (i.e., no Trojan or malware is required). We have summarized our key findings in Table 1.

Prior Studies. Our work differs from existing research efforts that seek to challenge the resilience of LTE security mechanisms under various conditions. Shaik et al. [3] show that a device location can be leaked within 2 km^2. They have also demonstrated the Denial of Service (DoS) attack when the LTE device

accepts the message from rogue LTE base stations and de-registers from the network. They assume LTE device will send non-integrity *Tracking Area Update Request* message, which is replied by the rogue LTE base station.

Jover [4] present LTE DoS attacks through radio signal jamming and amplification, and subscriber database saturation. In a separate work [5], they argue that attacker can use the LTE System Information Blocks, and Management Information Blocks to craft jamming attacks. Patrick [6] shows that compromising physical radio access network can reveal user traffic sent over unencrypted link between the radio access network and the core. Tu et al. [7] and Huang et al. [8] show that LTE protocol interactions are common and can result in performance issues. They have shown how abnormal LTE protocol interactions can degrade quality of service, e.g., the device does not transition from 3G to 4G after making a circuit-switched voice call, the device registration procedure is delayed because of location update, etc. Contrary to previous studies, our work focuses on LTE security weaknesses arising from standardized specifications; especially at LTE protocol inter-layer and inter-radio communications. Moreover, we demonstrate a different set of attacks not revealed by earlier studies. We have challenged the fundamental security principles of the LTE network and expose the vulnerabilities that lead to active attacks.

Scope. We believe, LTE standard body has well thought all LTE operational scenarios and may not have left any obvious mistakes while defining standards. In this paper, we focus on studying corner cases in LTE operations that may not be commonly observed, but could weaken the LTE security. We limit our scope in studying these cases within the relatively less explored area, i.e., LTE protocol inter-layers, and inter-radio interactions.

2 Background

We provide background on LTE protocol inter-layer interaction[1], and access technologies (4G/3G/2G) inter-radio interactions.

2.1 LTE Protocol Inter-layer Interaction

LTE protocol's functionality is divided across different layers, where each layer is designed to carry out a specific function [9]. Figure 1 shows layered LTE protocol at the mobile device (known as User Agent - UE), LTE base-station (known as evolved NodeB - eNodeB), and LTE core-network entity (known as Mobility Management Entity - MME). The design goal of layered LTE protocol is: (a) to simplify communication design by dividing it into functional layers, and (b) assigning independent tasks to each protocol layer. Although, the layers execute their independent tasks, the successful execution of operations lie in frequent interactions among the protocol layers. Such protocol layer interactions take place within the device, and across the device with the network. For

[1] Such interaction can occur within, and across the device and network elements.

example, two procedures known as Hybrid Automatic Repeat Request (HARQ), and Automatic Repeat Request (ARQ) are proposed at Medium Access Control (MAC) layer and Radio Link Control (RLC) layer of LTE protocol stack, respectively [10]. The combination of these two protocol layers (i.e. MAC and RLC) can be viewed as inter-layer protocol interaction. MAC and RLC protocols coordinate back and forth in a feedback channel loop to achieve reliable data transmission, (as shown in Fig. 1).

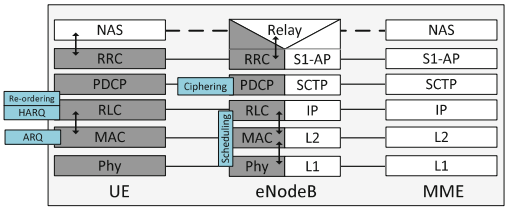

Fig. 1. LTE protocol layering and interaction at device and network side

Another example of LTE protocol inter-layer interaction is shown in Fig. 1, when Radio Resource Control (RRC[2]) layer at UE is communicating with Non-Access Spectrum (NAS[3]) protocol at MME. The RRC layer is responsible for securing radio connection between UE and eNodeB, whereas the NAS ensures secure data connection between UE and MME. Although, RRC and NAS function independently, these two layers coordinate frequently in order to perform certain device/network level operations. One such operation is *device registration procedure (i.e. Attach Request message)* with the network. In this, RRC layer at UE first establishes the radio connection with eNodeB, and then NAS layer at UE registers it with MME. Since NAS operation immediately follows the successful RRC connection, NAS message piggybacks the last successful RRC message [10], to reduce the signaling overhead and, speeds up the device registration procedure [11].

We show that LTE protocol's inter-layer interaction is the culprit of bypassing security setup. For example, LTE core network processes *Attach Request* message, without even authenticating the device. Similarly, *device Power-off*, *Location Update procedure*, *device Idle to Connected Mode operation*, and many other messages can be executed without authentication due to inter-layer communication.

In this paper, we show how seemingly innocuous protocol interaction can cause serious security threats to users' activity in the network. We have found that the vulnerabilities arise when different layers (1) accept the messages from each other without inquiring the true identity of the sender and network functions, (2) execute the message without establishing the authenticity of the message, and (3) do not validate the packets that were sent before the authentication was established.

[2] The communication between UE and eNodeB is performed by RRC.
[3] The communication between UE and MME is performed by NAS.

2.2 Access Technologies Inter-radio Interaction

Cellular technology evolved from GSM (2G) to WCDMA (3G), and then to LTE (4G). Since LTE coverage is not universal, most cell phones incorporate 2G and 3G systems along with 4G support. This solution of combining WCDMA-GSM-LTE (GWL) has indeed many advantages. First, the device can switch to legacy 2G/3G preferred radio access network in the absence of LTE network coverage. Second, in absence of Voice over LTE (VoLTE) feature, LTE can fallback to 3G/2G voice support over circuit switch (CS).

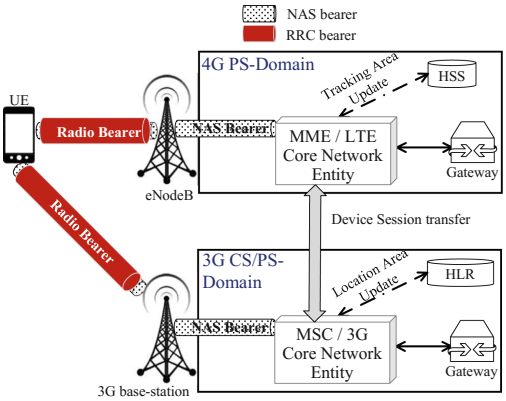

Fig. 2. Inter-radio access technologies (IRAT) interaction

In order to realize preferred network access, GWL radio technologies need to interact with each other via handover procedure, where user session should be seamlessly transferred from one radio technology to the other. Figure 2 depicts an inter-radio communication scenario. At first, the device is connected to LTE network. When handover condition to 3G/2G network arises (such as LTE coverage becomes weaker than 3G signal strength, or LTE system needs to fallback to 3G for CS call), MME transfers user session to 3G core-network function (known as Mobile Switching Center - MSC). This user session also includes the device security vectors on which the device was originally authenticated with the LTE network. The vulnerability arises when target network (3G in this case) skips device authentication procedure, believing that the device native security context is still valid.

When the device successfully completes the handover to 3G, it updates its location at Home Location Register (HLR). This location update procedure is carried out in order to locate the device during its idle period. Since device location update procedure is also part of inter-radio switch, the location update procedure is also exempted from security protection. The attacker tricks the network believing that location update request message is sent by a true originator.

In the next section, we discuss our experimental methodology that discusses vulnerabilities validation in operational LTE network, and converting these vulnerabilities into attack.

3 Experimental Methodology

To validate each vulnerability, we are required to log complete device traces. LTE modem vendors (e.g., Qualcomm or Mediatek) let developers collect LTE protocol traces. Tools such Qualcomm eXtensible Diagnostic Monitor (QXDM) [12] and MobileInsight [13] help to collect LTE protocol traces in operational LTE network. The real challenge is the modification of control message contents for LTE modem. The current modem implementation is hidden and the programmer does not get any interface to inject his commands. Although, AT commands [14] are provided to activate/deactivate the device session with the network, the modem does not allow us to change the contents of these messages (such as security capabilities). We found that LTE modem's functionalities are controlled by non-volatile memory items/NV items. There are around 65535 NV items, holding values from device capabilities to its functioning parameters. In fact, the mobile phone vendors change these NV items to restore phone configurations. Figure 3(left) shows freeware tool that allows us to read/write phone's NV items.

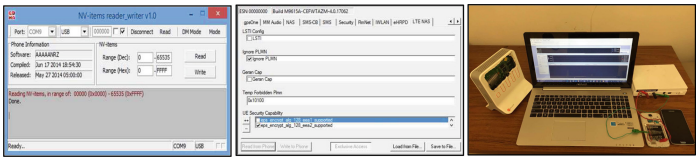

Fig. 3. NV reader/writer tool that modifies non-volatile memory of device (left), service programmer that helps to launch attack from device (center), and our testbed consisting of commodity hardware and open source platform (right) that helps to validate vulnerabilities at the network side

We validated the existence of vulnerabilities by modifying the Non-Volatile Memory of the LTE modem. Then we used Qualcomm's service-programmer tool (QPST Service Programmer) [15], and AT-command tool (TeraTerm) [2] to communicate with the device chipset. For example, we first let the device enter into sleep mode and then issued *"Detach Request (power-off)"* message using AT-command. Section 4 explores this type of attack.

In order to understand how different protocol layers communicate in a feedback loop, we parse the traces and analyse to confirm LTE standard vulnerabilities.

Last, we assess the practical implication of vulnerabilities by converting them into attacks. We launched the attacks either using Qualcomm service programmer [15] or deploying our testbed. The Qualcomm service programmer helps

modify device parameters. By changing these parameters, the adversary can impersonate victim device. Since certain messages are accepted without integrity check, the network believes as if it is talking to the actual device. For some other type of attacks, we are required to provide proof of concept model using a testbed. There are a number of 3GPP compliant open source LTE implementations, such as OpenEPC [16], OpenAirInterface [17], and OpenLTE [18]. Our testbed setup includes gateways (Serving-GW and PDN-GW), LTE core-network entity (MME), subscriber information database (HSS), and external network proxy – all implemented in software, as well as an eNodeB. We have used two Android phones (i.e. Samsung S4 (with Qualcomm's LTE modem MDM-9215 chipset), and S5 (with Qualcomm's LTE modem MDM-9635 chipset)) with USIM cards programmed with the appropriate identification name and secret code to connect with the base-station. Figure 3 (right) gives a snapshot of our testbed that consists of commodity hardware devices including two smartphones, 3G femto-cell, power monitor tool, and a laptop.

The following sections dig deep into the root causes of major exposed vulnerabilities, reveal how these security loopholes arise, and what special attacks can be launched to exploit the LTE protocol's weaknesses.

4 Weak Authentication: Non-authentic Messages Are Accepted

LTE employs power saving mechanisms in which device enters into *RRC Idle state* when it has nothing to send/receive any data (CS or PS). In *RRC Idle state*, the UE releases its radio connection and deactivates the security connection with eNodeB. When UE has some data to send/receive, the UE establishes its radio connection with eNodeB and switches to *RRC Connected state*. After moving to *RRC Connected state*, the device renews its RRC security with eNodeB. However, a threat exists when the UE is able to communicate with the network before activating its radio security procedure. In fact it is allowed by the network to boost device performance by preparing network resources for the UE beforehand.

4.1 Vulnerabilities

When the device enters into connected state, the protocol layers interact to facilitate each other's functions to improve the response time from the network. Issues arise when these protocol functions are used to carry unauthorized traffic.

In the following subsections, we discuss how such protocol interaction can be vulnerable when the security shield is not yet in place.

Blind Forwarding. The logical division of protocols into different layers provide distributed functionality for complex LTE operation. A single protocol cannot perform any functionality without communicating with layers above and

below. Such interaction is divided into two different parts where, (1) one layer communicates with the layer immediately above or below, and (2) a layer communicates with another layer which is either significantly far in the protocol stack or located at remote host. In case of (2), the intermediate layers simply relay anonymous packets. For example, a mobile device establishes RRC layer connection with eNodeB while the device forms NAS layer connection with MME through the eNodeB (refer to Fig. 1). The eNodeB relays NAS messages to MME without looking into the message contents [19]. Such an implementation removes security threats between the device and core-network communication, in case the eNodeB is compromised. Hence, message forwarding without any inspection across different layers of protocols is rooted in the design.

Disjoint Identifications. There are a number of different identities used in LTE, grouped based on their function and usage scenarios. For example, IMSI (International Mobile Subscriber Identity) is a permanent subscriber identity used by mobile operators to identify the mobile subscribers. Leakage of such identity can lead to a number of user privacy issues. Therefore, a Temporary Mobile Subscriber Identity (TMSI) is used instead to ensure the privacy of the mobile subscriber. The network provides mapping between IMSI and TMSI to establish on demand network resources for the device.

LTE network further maintains other identities and group them according to their usage in different network functions. Some of these identities are commissioned upon equipment installation, others are provisioned by the operator before or during service operation, and some are created when user accesses the network for its services. Table 2 sums up all LTE identities as per their classification. We find that some of the identities are not mapped with any other identity in their group. That is, these identities do not hold any identity relation and remain disjoint. This introduces the potential threat where one part of user traffic is communicated with its true identity, whereas the rest of communication is allowed to be carried out by fake identity.

Table 2. Classification of LTE identifications

Group	LTE ID name	Usage
UE ID	IMSI, GUTI, S-TMSI, IP address, C-RNTI, eNodeB UE S1AP ID, MME UE S1AP ID, Old UE X2AP ID, UE X2AP ID	UE, eNodeB and MME
Mobile Hardware ID	IMEI	UE and MME
Location ID	TAI, TAC	UE and MME
Session ID	PDN ID (APN), EPS Bearer ID, E-RAB ID, DRAB ID, TEID, LBI	UE and MME

When the device attaches with the network it receives a number of identities. The MME assigns TMSI to UE based on which the UE can be uniquely identified at MME. Similarly, the eNodeB assigns C-RNTI[4] to distinguish the devices within the radio network. The S1AP[5] layer handles the control messages between an eNodeB and an MME. In order to tell which control message is for which UE, an eNodeB allocates an ID (eNodeB UE S1AP ID) to each UE when it sends the message for a UE to an MME. Similarly, in order to tell which control message is for which UE in which eNodeB, the MME allocates an ID (MME UE S1AP ID) to each UE when it sends the first message for a UE to an eNodeB. Both eNodeB UE S1AP ID and MME UE S1AP ID have one to one mapping that distinguishes a UE across MME and eNodeB.

When the eNodeB receives the message, it maps the UE C-RNTI with eNodeB UE S1AP ID and forwards the packet to MME. The S1AP layer of MME receives the message and forwards it to the MME core function. The MME recognizes UE based on IMSI/TMSI and performs the desired action.

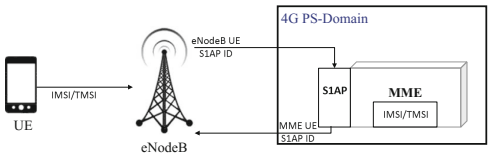

Fig. 4. Different identities are used at various network functions

A potential vulnerability occurs due to the missing mapping between MME UE S1AP ID and IMSI. As shown in Fig. 4, the device generates the NAS message by putting victim's IMSI and sends this to eNodeB. When the eNodeB receives the message from the device, it correctly maps the device C-RNTI and its associated S1AP ID pair, and forwards the message to MME. The MME S1AP layer removes the S1AP header and forwards the actual message to MME core function. The MME core function does not have any mapping between S1AP ID and associated IMSI, therefore, it takes action based on provided IMSI without checking whether the originator of the message is genuine subscriber or not.

Blind Execution of Messages. As stated earlier, when the device switches from idle state to connected state, it is required to establish radio security. Before such security messages exchange take place, certain messages need to be executed first. These messages are (1) type of operation the device has requested (2) the network resources that the device operation may need, etc. Such messages are exchanged between the device and the network, which are executed at both sides in order to establish the type of activity to be performed next.

[4] Cell Radio Network Temporary Identifier (C-RNTI) identifies UE over the air.
[5] S1AP facilitates control-plane traffic between eNodeB and MME.

To take an example, NAS *Service Request* message informs MME about the type of service (such as, PS data or CS call etc.) the UE needs imminently. To prepare the resources that the UE requires, eNodeB forwards such request to MME before initiating RRC security procedure[6]. When MME receives the NAS message, it executes the message even if message authentication code included in the message fails the integrity check or cannot be verified (Sect. 4.4.4.3 *Integrity checking of NAS signalling messages* in LTE NAS specification [19]). Such actions help network to quickly prepare network resources for device but comes at the cost of security risks where an attacker can get unauthenticated messages executed at MME. There exists a vulnerability when the attacker makes MME processes non-integrity protected message. For example, the attacker sends a non-integrity protected *Service Request* message to MME and puts victim's TMSI in the message. MME first receives and then processes the NAS *Service Request* message where it finds the message to be non-integrity protected. The MME generates *Service Reject* message by rejecting the request with cause "*UE identity cannot be derived by the network*" and sends this message to victim UE. On receiving *Service Reject* message, victim device enters into deregistered state and initiates the attach procedure. In short, an attacker can exploit those NAS messages which are processed by MME even if these messages are not integrity protected.

4.2 Attacks and Validation

The three vulnerabilities explained above are rooted in the LTE protocol design and can be exploited even when LTE security shields are well in place. We assume that all components function normally without any misconfiguration, malware, or intrusion. We further assume that all other mechanisms in cellular networks and at other mobile clients work properly. Irrespective of such measures, the attacker can still leverage improper operations at network function to launch attacks against victim.

The attacker connects to radio network as a legitimate user. Once the radio connection has been setup, it announces victim's identity in the NAS message and requests radio layer (RRC) to forward it to MME. The MME receives the message from eNodeB and assumes that the message is part of the chain of steps needed for specific device operation. The MME then executes the message and sends back an acknowledgement to the victim.

This threat becomes more powerful when the attacker is able to execute the message on behalf of victim without asking for an acknowledgement.

[6] Section 5.3.3 *RRC connection establishment* procedure and Sect. 5.3.4 *Initial security activation* in LTE RRC specification [20]. Note that initial NAS message (such as *Service Request*) is sent as a piggybacked message with *RRCConnectionSetupComplete* message that eNodeB forwards to MME. However, *SecurityModeCommand* message is sent thereafter.

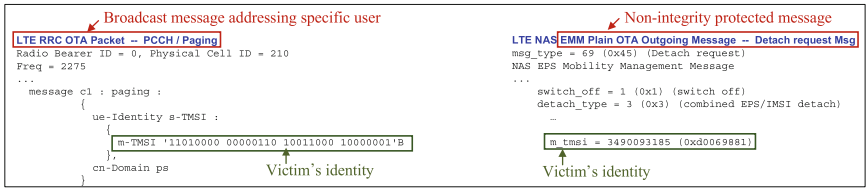

Fig. 5. (a) The victim's identity can be obtained from broadcast paging message (b) Detach message is created by using victim's identity

Detach a Victim from the Network Through Spoofed Message. In this exploit, the attacker can detach any device from the network. This attack is launched when RRC layer at device communicates with the NAS layer at MME. When the device switches from idle state to connected state, it first establishes the RRC connection. The device is allowed to send piggybacked NAS message with the acknowledgement of radio connection setup (i.e. *RRC Setup Complete* message). The attacker takes advantage of this and sends UE *Detach Request* message with an action of *power-off* to MME by putting victim's identity in the message. Once the MME receives the message, it first verifies the integrity of the message by checking message authentication code of the message. Because this message is not originated from legal subscriber, the integrity check fails at MME. However, LTE standard mandates the *Detach Request* message with *power-off* type should be processed by MME even if its integrity check fails or even the message does not include message authentication code (Sects. 4.4.4.3 and 5.5.2.2.2 in [19]). Once the MME receives the message, it takes an action for *power-off* request by releasing victim's network resources. Note that the *device power-off* reason does not trigger acknowledgement from the network to the victim device (Fig. 5.5.2.2.1.1: UE initiated detach procedure in LTE NAS specification [19]) that makes victim device wrongly believe that MME is out of service. The victim device remains out-of-service until victim performs hard-reboot on device or uses airplane mode feature to initiate the device attach procedure.

In order to launch this attack, the adversary needs to expose the victim's identity, which can be obtained from the following procedure.

Exposing Victim's Identity. When the device attaches with the network, it is assigned with TMSI. All the communication between the device and the network is based on TMSI. The TMSI is valid until the UE remains within the reach of serving MME – which typically handles all the devices within a large metropolitan city [21].

The device enters into idle state when it has nothing to send or receive. If a PS data or CS call is destined for the device during idle state, the MME sends *paging-message*[7] to that device. On receiving this *paging message*, the device

[7] Paging message is a control beacon sent from LTE network to a device, when packet switched (PS) data, or circuit switched (CS) call is impending at LTE core network. These paging messages are sent when device is in *RRC Idle state*.

enters into connected state and receives the traffic. Since the device has no active connection with the network during idle period, the *paging-messages* are broadcast in nature. All the neighboring devices receive the paging message and discard it if their identity is not listed in the message. Note that the attacker is a legitimate device connected with LTE network which also receives the paging messages destined for other devices. The attacker can simply get the TMSI of the victim out of the paging message.

The attacker can also originate a *paging message* towards the victim device. It should be recalled that whenever the device receives an incoming voice call during idle state, it is paged by the core-network. Therefore, simply calling victim's phone number and then hanging up even before the phone rings, triggers a *paging message*. The attacker gets hold of this paging message (because paging messages are broadcasted within MME tracking area[8]) and maps the victim's TMSI value with its phone number.

We run device traces and get victims identity through *paging message* (as shown in Fig. 5a). Then the adversary generates *Detach request message* (Fig. 5b) piggybacked over RRC (Fig. 6).

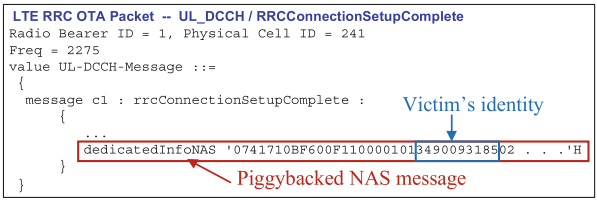

Fig. 6. The RRC layer helps to deliver NAS message when RRC protocol interacts with NAS protocol

To launch this attack, we first register the victim device (Samsung Galaxy S4 smartphone), and the attacker device (Samsung Galaxy S5 smartphone) with our LTE testbed platform. Once both victim device and attacker are registered, the attacker sends *Detach Request message* (i.e. AT + CFUN = 0) in device *RRC idle mode*, as shown in Fig. 7. Note that in this detach request message, attacker can masquerade victim device identity (TMSI). On receiving the detach request message, the MME finds the detach-request type as *Power-off* and immediately releases the associated device connection with Serving GW and PDN GW. We captured wireshark logs (as shown in Fig. 8) that reveal on receiving the detach-request, the UE connection is cleared by MME, serving GW and PDN GW. The associated device is said to be "detached" and "deregistered" from core-network's view.

[8] The tracking area is a logical concept of an area where a user can move around without updating the MME. In operational network, one tracking area spans to a number of eNodeBs.

Fig. 7. The device logs showing that the detach procedure is invoked over unsecured channel

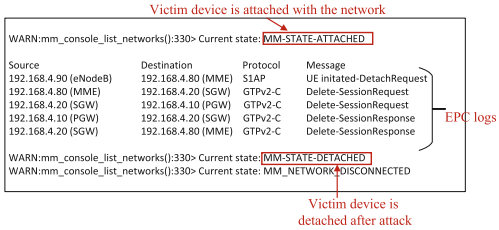

Fig. 8. The victim device is detached from the network on receiving detach request from attacker.

Detach Multiple Victims from the Network Through Broadcast Message. The UE monitors a paging channel during *RRC idle* state to detect its pending notification. The UE can be paged through either of its identities, i.e. TMSI or IMSI. The LTE standard makes distinction between paging messages generated with TMSI and with IMSI. Paging using IMSI is defined as abnormal procedure used for error recovery in the network (Sect. 5.6.2.2.2 *Paging for EPS services through E-UTRAN using IMSI* in LTE NAS specification [19]). The network may initiate paging using IMSI (as shown in Fig. 9) if the TMSI is not available due to a network failure. Upon reception of a paging using IMSI, the UE locally deactivates any bearer context(s), detaches itself locally from LTE network and changes the state to *Network DEREGISTERED*. After performing the local detach, the UE then performs an attach procedure.

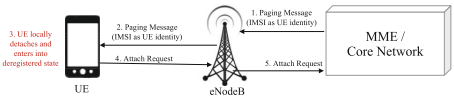

Fig. 9. The device detach procedure is invoked over insecure channel

In our attack model, the attacker uses this abnormal condition to its advantage and kicks victim out of the network. Because the paging messages are in plain text and broadcast in nature, these messages cannot be secured. Furthermore, the device executes such messages while it has not maintained any connection with the network (as it has torn down secure connection with the network before entering into idle mode). This fact brings security vulnerability where an attacker can detach the device by simply generating paging messages using IMSI as device identity. The impact of such vulnerability is enormous where an attacker can take down all of the devices connected to one eNodeB [19].

Exposing Victim's IMSI Identity Through Side Channel. The network operator allocates a unique IMSI to each subscriber, and embeds it to customer USIM card. In order to support the subscriber identity confidentiality, the MME allocates TMSI to mobile subscribers, when the mobile device establishes a new connection with MME. Thereafter, TMSI is used as UE identity for all subsequent messages exchange between UE and MME.

Therefore, finding the IMSI of the victim is a challenging task. Although, previous studies [22,23] have used special hardware [24], to expose the IMSI of a device, we discovered a new method to obtain the device IMSI using commodity hardware, i.e. 3G femto-cell.

We discover whenever the 3G femto-cell is brought within the proximity of a UE, this UE detaches from its LTE eNodeB and camps with 3G femto-cell. This is because the UE finds femto-cell signal strength higher than the serving LTE eNodeB and performs handover to femto-cell. We noticed that during this handover messages exchange, the 3G core-network sends an *identity request* message to the device, where UE responds with its IMSI. We observe this behavior because femto-cell and the eNodeB do not have any direct link with each other. As a consequence, the LTE MME does not send device security keys to 3G core-network, and let the 3G network re-authenticate the user. In order to derive the security keys, the 3G core-network needs to expose IMSI of the device and generate challenge/response messages as part of UE authentication procedure.

Note that *identity request/response* message exchange occurs prior to establishment of device security. This makes these message exchange non-encrypted and can be logged at femto-cell. Since the femto-cell is a closed 3G base-station, *we hacked the femto-cell and defeated its in-place hardware and software security mechanisms*[9].

Once we espied victim (connected to operational LTE network carrier) IMSI through side channel, we now require the victim device to perform cell reselection to our testbed eNodeB. LTE defines priority-based cell reselection in which

[9] Because femtocells are part of operator network, therefore, operators take both hardware and software security measures to secure it. Therefore, as shown in Fig. 3 (right), we only broke small part of femtocell cover, just to access the debugging pins (JP1, JP2, JP5, JP6, PL2, etc.). We used *screen command* to dump femtocell memory image. Then uncompressed it, reversed the kernel image, and looked for user information in */etc/passwd* file. We then applied brute force technique to decode the password string within 7 days.

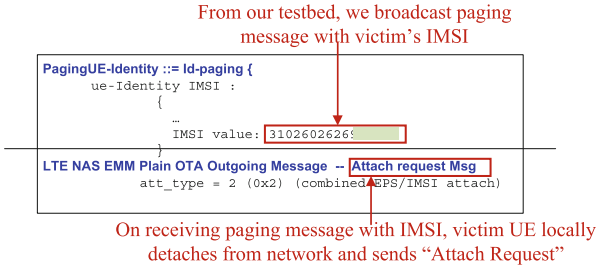

Fig. 10. The network and UE logs show that the paging message with victim's IMSI can detach the victim device from the network

the device in Idle state periodically monitors its neighboring cells. The priority based cell reselection ensures that the device always stay connected with higher priority cell [25]. The operational LTE eNodeB informs its associated devices about cell priorities through broadcast SIB messages. We sniff SIB4 and SIB5 parameters that define Intra-frequency and Inter-frequency LTE neighboring cells priorities [20] and configure our testbed eNodeB accordingly. We configure our eNodeB's cell as of higher cell priorities as compared to operational LTE eNodeB. This tricks victim device to camp over our testbed eNodeB cell. Once the victim device is camped with our eNodeB cell, we generate paging message (where we put UE identity as IMSI) towards the victim device. The victim device treats forged paging message as if it is coming from legitimate eNodeB. Soon after sending paging message, we turn-off our configured eNodeB. This is an important step that makes victim device to camp on operational eNodeB cell that forwards device attach message to operational MME. It is possible that the victim device goes through Radio Link Failure (RLF) as it was disconnected from our testbed eNodeB cell when it initiated the Attach Request message (after detaching locally). On re-establishing the radio connection (RRCConnectionRestablishment procedure), the victim device re-sends the Attach Request message (when it does not receive the reply to its first Attach Request message). We show this in Fig. 10, on receiving the paging message with IMSI, the victim device detaches and sends a new *Attach Request* message to LTE network operator.

Impact and Limitation. In first variant of UE detach attack, the attacker can kick victim device out of the network without raising any alarm at victim device. The victim will observe out-of-network-service symbol until reboot. We believe that the victim will not reboot his device thinking that his mobile device will recover from network outage automatically. We must point out that any implementation that binds the device across all its identities (such as binding of eNodeB UE S1APID, MME UE S1AP ID, and device IMSI/TMSI) can restrain the attack. We discuss this in Suggested Remedies Sect. 7.

In our second variant of the attack, we can generate one paging control message, and can potentially take down all the devices connected within the tracking

area (e.g. a shopping mall or an office space etc.). The paging message allows the network to address multiple recipients by putting their identities (IMSI/TMSI) in one paging message body. Such paging message is sent to all eNodeBs defined within one tracking area. This can potentially cause network outage to all the UEs connected to these eNodeBs. The impact of this attack is limited because the device automatically reconnects with the network after detaching. Nevertheless, an attacker can keep generating paging messages with IMSI as UE identity that will keep UE barred from accessing network services.

5 Weak Security Association: Security Handshake is Skipped on Inter-radio Communication

In this section, we disclose weaknesses of inter-radio interactions. Although, each radio access technology (RAT) (e.g. 4G/3G/2G) is secured when working standalone but breaks security mechanisms when these RATs interact with each other. We find that such weaknesses pose serious threats to user privacy and security.

5.1 Vulnerabilities

The handover procedure is initiated when UE's RAT source coverage starts fading and neighboring RAT coverage starts getting better. The Inter-RAT handover is also triggered when the device initiates or receives a circuit switched call. Once the handover decision is made by the source eNodeB, the handover preparation phase is started at the target base station (3G/2G). During this phase, the target network prepares the resources for an incoming connection. Once the target base station is ready to serve the mobile UE's PS/CS functionality, the source eNodeB transfers the device context to the target network. This also includes the transfer of UE security keys, which basically allows the target network and UE to use old security context and avoid lengthy AKA procedure [26]. This security context is transferred once the network can use mapped security context for follow-up communication.

The use of old security session, potentially leads to serious vulnerability, where the unauthenticated messages are accepted by the network, believing that the source device is secure.

Network Accepts Location Area Update (LAU) Request Before Confirming Device Identity. Once a device is in 2G/3G network, it sends the LAU request message to its network. Its possible that the device's temporary identity (TMSI/GUTI) has expired at the network. In this case, the network initiates the identification procedure by sending an *Identity Request* message to the mobile device. Upon receiving the *Identity Request* message, the mobile device sends back an *Identity Response* message containing device identification parameters. Because the device identity was unknown when the network received the original LAU request message, any security context should be considered void.

But we have found that the network accepts the LAU request message after receiving the *Identity Response* and does not ask the device to authenticate itself. The root cause of this issues lies in the way legacy networks treat two procedures. In this case, Identity Request and LAU procedures are treated independently (Sects. 4.7.8 and 4.4.4 of Core Network Protocols specification [27] define Identity and LAU procedures, respectively). As a result, LAU procedure resumes after getting device identity; and do not authenticate the device that has responded the Identity Request message.

There is a potential for an attacker to send masqueraded LAU request message where the network asks the attacker to verify its identity without authenticating it. Figure 11 shows the logs for a device sending LAU request message, and the network does not ask for any authentication.

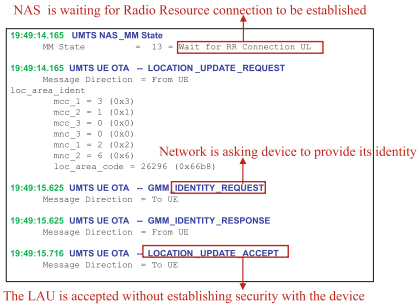

Fig. 11. Location Area Update procedure is accepted without authenticating the sender

Inter-RAT Switch Can Circumvent Location Update Procedure. LTE to WCDMA handover is a frequent phenomena, where device moves from LTE to WCDMA for CS voice call, and comes back to LTE from WCDMA for PS data access after voice call. We find that on successful handover to LTE network, the device does not perform the LAU procedure - known as Tracking Area Update (TAU) in LTE. This is contrary to the switch from LTE to 3G/2G where the LAU is mandatory.

In fact, this is an accepted operation defined in LTE standard. It is stated that when LTE MME has native security context for the UE and does not receive a TAU request within a certain period of time, after the inter-RAT switch, it "shall *assume*" that UE and MME share a native security context (Sect. 9.2.2 From UTRAN to E-UTRAN in [28]). Furthermore, a separate LTE specification mandates the TAU request procedure as optional when the inter-RAT switch does not induce the device location change (such as user makes a voice call within its tracking area) (Sect. 5.3.3 in [29]). These two statements from two different standards are conflicting, where the device although has changed its tracking area but does not send TAU request, making MME wrongly believe that the device's tracking area has not changed.

5.2 Attacks and Validation

We have shown how an attacker can hijack the LAU request message and can render victim device unreachable from the network. This location hijacking does not raise any alarm at the network, and it believes that the device is not reachable because it is either out of coverage or powered off. On the other hand, the victim device does not make any effort to re-establish the connection with the network, believing that it has correct location registered and currently does not have any data pending from the network to be delivered.

Hijacking Location Update. In this attack, the attacker hijacks the victim location by artificially making the victim device do inter-RAT switch. The attacker ensures that the attack remains unnoticed even when the victim moves back to its original RAT (usually LTE network). Figure 12 shows the steps to launch the attack. First the attacker establishes legitimate radio connection with 3G base station (steps 1 and 2) and artificially induces the inter-RAT switch handover (HO) at victim device, registered with LTE network, (step 3). The attacker can simply do it by dialing a phone call towards the victim device and then hanging it up. Upon receiving the voice call, victim device switches to 3G RAT and sends the LAU request to 3G network (step 4). At the same time, the attacker generates LAU request NAS message by putting victim TMSI and wrong location area code in the message body (step 5) and sends it to 3G base station. The 3G base station will forward this message without looking its content to 3G core-network (step 6). Now 3G core-network has received duplicate LAU messages (but with different location identities) for the same victim device, and updates the device location mentioned in the latter message [30]. When the attacker hangs up the call, victim device again performs the switch back to LTE network. Because the victim device has not moved since it has received the phone call, and its location area code has not changed, it does not need to perform TAU procedure with the LTE network [28]. Therefore, the user context including its location will be propagated to LTE network from 3G/2G network. This will result in an unreachable LTE network (because the LTE system will page the UE at wrong location).

We validated the attack through emulation mode [31]. The device is first attached with LTE core network where device initiates handover to 3G MSC. During LAU procedure, we modify the location area code of the device and

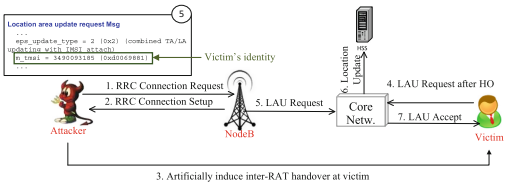

Fig. 12. Location Area Update hijack attack

confirm the device successfully performs handover to 3G (with wrong location area code). On handover from 3G to 4G, the device does not trigger TAU procedure. Afterwards, device initiates the data traffic to confirm 3G to 4G handover was successful.

Impact and Limitation. The attack leaves the victim device in a state in which it can neither receive voice call nor incoming data traffic. The impact of this attack vanishes when both of these conditions are met: (1) the device switches back to LTE from 3G/2G RAT, and (2) the *Periodic TAU* timer has expired at device. The *Periodic TAU* is used to notify the availability of UE to network periodically. The procedure is controlled by UE through *periodic tracking area update* timer, which was sent by the network during device registration procedure. Once *periodic TAU* timer expires, UE establishes the secure network connection and notifies its location, which results in correct UE location to be updated at the network.

However, the timer value is carrier network dependent, which can also be defined as zero (i.e. periodic TAU is deactivated at the device) [26]. In normal operational network, it is defined to be few hours [32].

The second limitation of this attack is related to timing of the attack. The attacker needs to generate a fake LAU request message soon after the victim device has sent out his LAU request message. We believe such timing interval is easy to observe as the attacker can calculate inter-message delay by logging cellular traces prior to launching the attack.

6 Lack of Access Control/Non-authorization

The operators need to deploy servers that keep track of millions of their subscribers, and provide adequate mechanisms for service provisioning, billing, and other services that are available to the subscribers. Once the user is authenticated, the first job of these servers is to identify whether the user is authorized to access certain service or not. In short, the network deploys authorization mechanism even for an authenticated user.

However, LTE standard does not define an authorization procedure at the UE. If the authentication is successful with the network, the device deem all the communication from the network authorized. The authorization measures are also missing for base station (eNodeB). We found that the device subscription and permission control actions are taken only at core-network (MME). When a device fails these checks, it is not allowed to access core-network functions, but this device can still keep its radio connection with eNodeB.

6.1 Vulnerabilities

When the UE is relying on authentication to ensure that the network is authorized to send packets, things change dramatically in the absence of such authentication.

Unconditional Trust Across Protocol Layers. In order to perform an atomic operation, LTE protocol layers need to carry each other messages. There is no defined security mechanism for such inter-layer communication. Thus, the trust model between protocol layers is unconditional.

For example, during *RRC idle state operation*, the UE is *paged* by MME via eNodeB. These *paging messages* contain information which the core-network wants to convey to the device and are used to instruct the device for a particular action. In Fig. 5a, the *paging message* includes the device identity, recognized by MME, and an action to be taken (*cn-domain PS*, i.e. PS data is waiting for the device). Hence, UE blindly authorizes such inter-layer functions to deliver messages. It has been assumed that each link from MME to eNodeB, and from eNodeB to UE is trusted while forwarding the packets to the next link. In this way, the attacker establishes trusted link with eNodeB and injects malicious traffic to the UE and MME.

Permission Control Decisions Are Not Disseminated Across Network. The device authorization procedure is divided into two parts, whether the device is allowed to (1) access particular operator network, and (2) use network services.

When a device powers on, it determines Mobile Network Code (MNC)[10] from USIM and performs cell selection procedure. After appropriate cell selection, the device camps on that cell. Thereafter, UE establishes radio connection with eNodeB. This access control procedure ensures that the device connects to allowed network operator's eNodeB.

If the user is allowed to access network radio resources, it sends NAS control messages to initiate core-network services. On receiving first NAS control message (*Attach Request* message), the HSS authenticates the device and populates device permission control list to MME. In case the device does not have any permission to access the network, the MME refuses the connection request. Since UE and MME communicates over NAS, the eNodeB remains unaware that UE connection has been rejected by MME. As a result, the device radio connection between UE and eNodeB remains alive and the unauthorized device can launch radio attacks. We have found that this vulnerability arises if the MME does not tear down UE connection with eNodeB. In principle, when the UE breaks its connection with MME (such as through *Detach Request* message), the MME propagates UE connection release message to eNodeB (UE Context Release (MME initiated) procedure in S1AP specification [33]). Then the eNodeB releases the device radio connection. But access control verification failure does not trigger UE connection release message from MME to eNodeB. This allows the device to keep only RRC connection even in the absence of NAS connection. It violates the LTE design principle where the device in connected state should keep both connections (RRC and NAS).

[10] MNC uniquely identifies a mobile network operator.

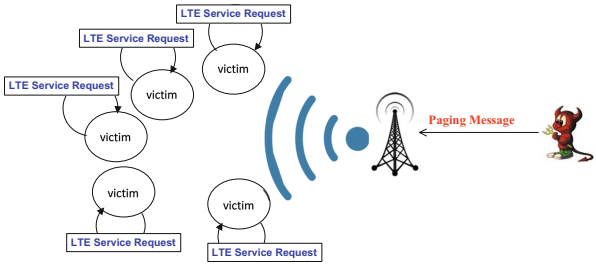

Fig. 13. The paging broadcast message can be used to drain batteries of multiple devices

6.2 Attacks and Validation

This vulnerability is explored through an attacker that can successfully communicate with the device without its consent. Since there is no authorization or access control at UE side, the UE can always be tricked into processing unauthorized packets.

Silently Draining Victims' Battery. In order to save battery power, the mobile device enters *RRC idle state* by switching off its transceiver. In idle state, the device observes Discontinuous Reception (DRX). The DRX duty cycle is divided into DRX active and DRX idle states. On DRX active, the UE listens to the radio channel to receive the control signals from the network. On pending CS call/PS data, the device is instructed (through broadcast *paging messages*) to secure its connection with the network. When the device finds its TMSI in the paging message, it sends the *Service Request*[11] message in plaintext to the network. Thereafter, the security setup procedure starts and device delivers/receives its data.

As shown in Fig. 13, the attacker gets benefit of the fact that device takes action on its paging message. The adversary generates a paging message by addressing multiple victims about their pending CS/PS data. On receiving this message, all addressed victim devices will send *Service Request* message to the network. These devices will stay awake for a configurable amount of period (usually 10 s) [20]. By sending this paging message to these victim periodically, the attacker can never let these victim devices enter into *RRC idle state*. This single *paging message* can drain battery power of multiple mobile devices.

For our validation, we logged LTE packets and ensured the victim UE enters in RRC idle state. The victim UE which is also connected with Monsoon power monitor [34] is placed under good radio coverage (i.e. around −90 dBm). This ensures the device remains in idle state and does not perform any radio measurements for handover procedure.

Once the phone is in idle state, the attacker generates the paging message for the victim. To do so, the attacker dials a voice call to the victim phone, but

[11] Service Request establishes UE connection with MME, when uplink/downlink data is to be sent/received at device idle state.

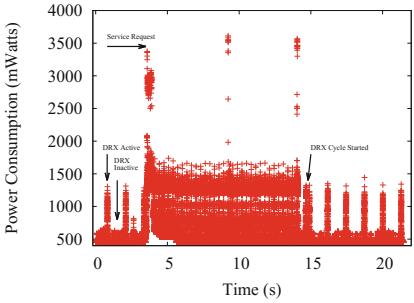

Fig. 14. The energy consumption from idle to connected state transition and then staying in connected state

hangs-up before the phone even rings. We noticed that dialing a call for a couple of seconds, triggers a paging message with *cn-domain CS* (i.e. the device should wake-up to receive CS call).

On receiving the paging message, the victim device enters into *RRC connected mode* and generates *Service Request message* to MME. The MME first authenticates the UE and then establishes the requested core network resources. After few seconds, when MME does not receive any data activity from the victim device, it requests eNodeB to release radio resources for the connected UE. The device enters into idle mode after receiving the *radio connection release* message from eNodeB.

Figure 14 shows power trace for the victim UE under attack. We can see when the device is in idle state, it observes *DRX idle* and *DRX active* states by consuming 500 mW and 1300 mW power values, respectively. But as soon as the phone receives a paging message, it ramps up its radio and sends *Service Request message* that brings the power consumption to as high as 3500 mW. After sending the *Service Request message*, the UE exchanges authentication messages with MME (which is marked by two other high power consumption peaks in Fig. 14) and keeps connected to the radio network. In Fig. 14, we can also see that the overall power consumption in *RRC Connected* state is 3X-4X higher compared to *RRC Idle* state. Therefore, by generating paging broadcast messages, the attacker can silently drain the victim battery power.

We drained victim's device battery by generating paging request messages in an interval of 10 s. Note that, on the expiration of *device inactivity timer* at MME (which is 10 s), the MME releases the device bearers and device switches back to idle state. In this attack, we aim to bypass the victim device's *inactivity timer* by generating paging messages every 10 s.

7 Suggested Remedies

In this section, we suggest some remedies to address the discussed vulnerabilities. Our proposal seeks to mitigate the impact from the attacks, within current LTE standard (i.e. 3GPP standard). We should point out that the device, eNodeB,

and core-network entities are 3GPP compliant and any vendor specific implementation, conflicting with the LTE standard, may fail inter-operability between devices and the network functions. Therefore, these vulnerabilities need to be discussed in the 3GPP standard for a permanent solution. Below, we propose some quick fixes for the discussed attacks.

Detach Attack Prevention. Once the operator receives the non-integrity protected "power-off" request message from the device, it should consult its database to resolve device identity (IMSI or TMSI) to eNodeB-S1AP-ID. If the received and look-up eNodeB-S1AP-IDs do not match, the network should discard the "power-off" message.

In order to address device detach using paging message, the device vendor should keep the counter value for "paging using IMSI" request messages. If the counter value exceeds a threshold defined by the vendor, the device should discard any follow-up *paging request messages*. Note that, in this attack, the adversary needs to periodically send "paging using IMSI" request messages to refrain UE from gaining network resources.

Location Update Hijack Attack Prevention. TAU procedure must always be executed whenever the device changes its RAT. We believe this security solution should not impact device performance, because the TAU procedure only generates 2 signaling messages (*TAU Request and TAU Reply* messages). Since the TAU request message is always sent as integrity protected, the attacker cannot generate TAU request message on behalf of victim device.

Moreover, the network must not accept LAU request message for a device whose identity is unknown. In case the network needs to resolve the device identity (by sending *identity request message*), the security setup procedure must be executed before the LAU request message is accepted at the network.

Battery Drain Attack Prevention. The device should keep a mapping between paging request and gaining network resource. That way, no resources are reserved by the network when the adversary is sending fake paging request messages. Therefore, the device can easily count how many fake paging messages it has received. Once the number of fake paging request messages exceed vendor specific counter value, the device should drop subsequent messages.

8 Related Work

Closest to our work are [3,7]. [7] disclose performance issues on inter-protocol communication in operational LTE network. However, we discover security vulnerabilities that are rooted in LTE standard and do not discuss any performance bottlenecks. [3] discusses privacy attacks in which signalling information is leveraged to infer user privacy information. Moreover, such attacks are only possible if network operator disables integrity and ciphering protection. For LTE DoS attacks, [3] assumes the attacker can change the message contents (such as device capabilities in *Attach Request*) for non-integrity protected *Attach Request* message. In contrast, this paper discloses security weaknesses of common device

operations even if all LTE security mechanisms are well in place. [35] studies how to block the CS service caused by the unwanted traffic in the PS domain. [36] shows that current cellular infrastructures exhibit security loopholes (off-path TCP hijacking) due to their NAT/firewall settings. These contributions exploit operational network configuration issues, which can only be local to a specific operator. [37] proposes a denial-of-service attack on cellular networks by consuming the radio resources of control channels via significant spamming SMSs. However, the attack may not be applied to 4G LTE networks, since SMSs can be delivered to 4G LTE users by PS traffic as Whatsapp without 3G↔4G switches. [38] discloses a attack model to drain the battery of mobile phones via low-rate of retrieval of malicious MMS. However, this attack is not valid when the victim device black list the attacker device phone number. Security on mobile devices and their applications focus on permission control [39], inter-application communication [40,41], plagiarizing applications [42] and leaking privacy information [43] by smartphones. Our attack models do not depend on any given mobile data application.

9 Conclusion

In this work, we have uncovered new vulnerabilities in the current LTE security measures. We learn several lessons from our study. The unsecured messages should not be executed unless the device message integrity procedures are in place. The broadcast messages must also be integrity protected. Since all devices are connected to the same core infrastructure, the core-network messages can also be integrity protected using the public-private key pair.

Acknowledgement. We thank anonymous reviewers for their excellent feedback that has helped to improve the paper. This work is also supported in part by NSF grants (CNS-1422835 and 1528122).

References

1. 3GPP Specification series. http://www.3gpp.org/dynareport/36-series.htm/
2. Tera-Term-A Terminal Emulator. http://ttssh2.sourceforge.jp/index.html.en
3. Shaik, A., Borgaonkar, R., Asokan, N., Niemi, V., Seifert, J.-P.: Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In: NDSS (2016)
4. Jover, R.P.: Security attacks against the availability of LTE mobility networks: overview and research directions. In: IEEE WPMC (2013)
5. Jover, R.P.: LTE security, protocol exploits and location tracking experimentation with low-cost software radio. arXiv preprint arXiv:1607.05171 (2016)
6. The Security Vulnerabilities of LTE: Opportunity and Risks for Operators. http://forums.juniper.net/t5/Industry-Solutions-and-Trends/The-Security-Vulnerabilities-of-LTE-Opportunity-and-Risks-for/ba-p/214477/
7. Tu, G.-H., Li, Y., Peng, C., Li, C.-Y., Wang, H., Lu, S.: Control-plane protocol interactions in cellular networks. In: ACM SIGCOMM (2014)

8. Huang, J., Qian, F., Guo, Y., Zhou, Y., Xu, Q., Mao, Z.M., Sen, S., Spatscheck, O.: An in-depth study of LTE: effect of network protocol and application behavior on performance. In: ACM SIGCOMM Computer Communication Review (2013)
9. LTE protocol layer stack. http://www.tutorialspoint.com/lte/lte_protocol_stack_layers.htm/
10. Ahmadi, S.: LTE-Advanced: A Practical Systems Approach to Understanding 3GPP LTE Releases 10 and 11 Radio Access Technologies, 1st edn. Academic Press, Waltham (2013)
11. Stefania Sesia, M.B., Toufik, I.: LTE - The UMTS Long Term Evolution: From Theory to Practice, 2nd edn. Wiley, Hoboken (2011)
12. Qualcomm: QxDM Professional - QUALCOMM eXtensible Diagnostic Monitor. http://www.qualcomm.com/media/documents/tags/qxdm
13. Mobile Insight. http://mobileinsight.net/
14. AT Commands List. http://www.lte.com.tr/uploads/pdfe/1.pdf
15. QPST Service Programming. http://forum.xda-developers.com/showthread.php?t=1180211
16. Open EPC - open source LTE implementation. http://www.openepc.net/
17. OpenAirInterface. http://www.openairinterface.org/
18. Open LTE. http://openlte.sourceforge.net/
19. 3GPP. TS24.301: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3, June 2013
20. 3GPP. TS36.331: Radio Resource Control (RRC) (2012)
21. MME Pool Overlap. http://lteuniversity.com/get_trained/expert_opinion1/b/johnmckeague/archive/2012/03/06/mme-pool-overlap.aspx
22. Borgaonkar, R., Udar, S.: Understanding IMSI privacy. In: Vortrag auf der Konferenz Black Hat (2014)
23. Ginzboorg, P., Niemi, V.: Privacy of the long-term identities in cellular networks. In: Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications, pp. 167–175. ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering) (2016)
24. Strobel, D.: IMSI catcher. Chair for Communication Security, Ruhr-Universität Bochum, p. 14 (2007)
25. 3GPP. TS36.304: User Equipment procedures in idle mode (2013)
26. Securing the Mobile Network. http://www.us.aviatnetworks.com/media/files/Securing_the_Mobile_Network.pdf/
27. 3GPP. TS24.008: Core Network Protocols (2012)
28. 3GPP. TS33.401: 3GPP SAE; Security architecture, September 2013
29. 3GPP. TS23.401: GPRS Enhancements for E-UTRAN Access (2011)
30. 3GPP. TS23.012: Location management procedures (2011)
31. UE Emulation Mode. https://wiki.phantomnet.org/wiki/phantomnet/oepc-protected/openepc-tutorial/
32. LTE Cat-0 Power Saving Mode: What it Could Mean for Cellular IoT. http://www.eleven-x.com/2015/04/29/lte-cat-0s-power-saving-mode-what-it-could-mean-for-cellular-iot/
33. 3GPP. TS36.413:E-UTRAN S1 Application Protocol (S1AP) (2014)
34. MonSoon Power Monitor Tool. https://www.msoon.com/LabEquipment/PowerMonitor/
35. Traynor, P., McDaniel, P., La Porta, T.: On attack causality in internet-connected cellular networks. In: USENIX Security (2007)
36. Qian, Z., Mao, Z.: Off-path TCP sequence number inference attack-how firewall middleboxes reduce security. In: IEEE Security & Privacy (2012)

37. Enck, W., Traynor, P., McDaniel, P., La Porta, T.: Exploiting open functionality in SMS-capable cellular networks. In: ACM CCS (2005)
38. Racic, R., Ma, D., Chen, H.: Exploiting MMS vulnerabilities to stealthily exhaust mobile phone's battery. In: SecureComm 2006 (2006)
39. Barrera, D., Kayacik, H.G., van Oorschot, P.C., Somayaji, A.: A methodology for empirical analysis of permission-based security models and its application to android. In: ACM CCS (2010)
40. Chin, E., Felt, A.P., Greenwood, K., Wagner, D.: Analyzing inter-application communication in android. In: ACM MobiSys (2011)
41. Marforio, C., Ritzdorf, H., Francillon, A., Capkun, S.: Analysis of the communication between colluding applications on modern smartphones. In: ACM ACSAC (2012)
42. Potharaju, R., Newell, A., Nita-Rotaru, C., Zhang, X.: Plagiarizing smartphone applications: attack strategies and defense techniques. In: ACM ESSoS (2012)
43. Schlegel, R., Zhang, K., Zhou, X., Intwala, M., Kapadia, A., Wang, X.: Soundcomber: a stealthy and context-aware sound trojan for smartphones. In: NDSS (2011)