Device-Centric Detection and Mitigation of Diameter Signaling Attacks against Mobile Core

Zhaowei Tan, Boyan Ding, Zhehui Zhang, Qianru Li, Yunqi Guo, Songwu Lu
University of California, Los Angeles
{tan,dboyan,zhehui,qianruli,luckiday,slu}@cs.ucla.edu

2021 IEEE Conference on Communications and Network Security (CNS) | 978-1-6654-4496-5/21/$31.00 ©2021 IEEE | DOI: 10.1109/CNS53000.2021.9705031

***Abstract*—Mobile networks exchange signaling messages to manage their users' state. A spoofed signaling message can be leveraged by an attacker to change a victim user's state and disable his/her service. Despite the mobile operators' continuous efforts, such attacks can still be launched in the current 4G LTE Networks. We prototype and analyze 6 practical user DoS attacks that leverage Diameter, the protocol used in LTE to carry signaling messages. We demonstrate their damages and draw insights on how to defend against them.**

We propose D3, a device-centric software solution to detect and mitigate LTE Diameter attacks. Different from any previous solution, D3 operates at the device side only, without expensive infrastructure upgrade. With deep domain knowledge, D3 monitors and analyzes the control message exchange between the device and network when a certain service is disabled. By comparing with the normal state, D3 can infer if a Diameter attack is underway. It also supports device-only mitigation that can quickly help the device regain the service. We implement D3 on Android devices and show that it achieves a perfect success rate in combating all 6 Diameter attacks.

I. Introduction

To date, mobile networks are the only large-scale infrastructure that provides ubiquitous data, voice, and texting services. To facilitate the services, signaling messages are frequently exchanged within and among the mobile core networks. These messages query or update the users' states, so that the mobile networks can serve the users properly. It is thus crucial for a core network to authenticate the signaling messages, especially in roaming scenarios. Otherwise, an attacker can pretend to be another legitimate operator and spoof signaling messages. A major consequential damage is user Denial-of-Service (DoS), where the victim is disabled from accessing certain services.

In the current 4G Long-Term Evolution (LTE) network, Diameter is the de facto protocol used to carry the signaling messages. Despite its proclaimed superior security features, Diameter is reported by multiple sources to be vulnerable to spoofing attacks [1, 2, 3] (§II). We set up a standard-compliant LTE testbed with a USRP board (as base station) and a Linux server (as core network). We implement 6 reported Diameter user DoS attacks on our testbed (§III). In each attack, a spoofed Diameter message forces a victim user to lose certain services. We demonstrate and quantify the damages of those attacks: The victim user will lose certain services for minutes or until a reboot is initiated. However, the attacks either appear as a normal service loss due to bad signal, or cannot be observed by the victim at all. It is thus challenging to identify the attacks.

We further propose D3 (**D**evice-centric **D**efense for **D**iameter attacks) that can detect such attacks and attempt mitigation in the victim device only (§IV). Mobile users can install the software solution without expensive hardware or infrastructure upgrade. The main idea for device-centric detection is to analyze the message exchange between the device and network. D3 also actively interacts with the network to further confirm the attack. On the other hand, device-centric mitigation aims at re-synchronizing the state in core network components, where the state inconsistency empowers the Diameter attacks to cause severe DoS damages.

D3 can detect and mitigate the 6 attacks we introduce (§V). For two of the three attack categories, we study how each one results in consequential messages that cause DoS. D3 compares the message contents with those under normal cases. It then accurately detects whether a Diameter attack is underway. For the other category, an active approach is used to check whether an incoming text/call is blocked. Afterwards, D3 takes a device-centric method to mitigate the damage by toggling airplane mode, which will force the device to re-establish connection with the network. When a re-attach is not sufficient, D3 further asks the device to connect to another base station by frequency band locking.

We note that the design of D3 could benefit the security of future 5G core signaling messages. The first phase of 5G plans to reuse the current 4G core, where D3 can directly apply. Although 5G will eventually replace the Diameter with HTTP/2, the trust model is similar to 4G. So an attacker can still forge signaling messages from a lesser operator and launch attacks. Meanwhile, 5G inherits 4G's message exchange between the network and the device. We can adapt D3 to 5G attack detection without much modification.

We implement D3 in Android devices and develop a prototype on a Google Pixel XL phone (§VI). We evaluate how D3 combats the Diameter attacks (§VII). D3 can successfully detect all 6 attacks and mitigate the DoS effects completely in seconds with low overhead. We also show that D3 achieves perfect precision and recall when we mix Diameter attacks with other normal loss of services.

II. Background

A. LTE Mobile Core Network

Figure 1 depicts a simplified architecture for LTE mobile core network control plane, which includes two critical components: Mobility Management Entity (MME) and Home

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.

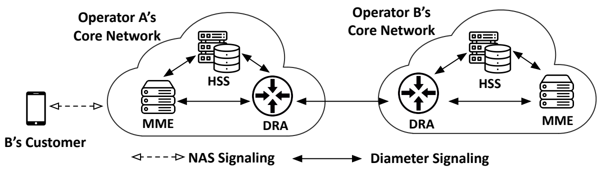


Fig. 1: An overview of LTE network architecture.

Subscriber Server (HSS). MME manages user mobility and sessions while HSS serves as a database that stores users' identification and subscription data. An LTE device exchanges NAS (Non-access stratum, as detailed in [4]) messages with core network for data and texting/voice service.

HSS and MME exchange signaling messages for session management, mobility support, and security. The signaling messages among them are carried by Diameter [5]. For example, when a user device attempts to connect to the network, the serving MME queries the HSS for identification verification. These signaling messages are crucial in supporting data delivery, voice calls, and texting services.

Signaling messages are also exchanged among different operators' core networks in roaming cases. Networks exchange the Diameter messages through Diameter Routing Agent (DRA). The DRA on the receiving side examines the incoming messages and forwards them to the destined component (MME, HSS, etc.). For instance, when an AT&T user roams to Telcel in Mexico, Telcel's MME will send an identity request to AT&T's HSS through DRAs.

B. Vulnerabilities in Core Network Messaging

Researchers have found Diameter signaling vulnerable to multiple threats, including Denial-of-Service, information leakage, location tracking [2, 3, 6]. These attacks rely on gaining access to the Diameter channel. Although major operators with billions of subscribers are difficult to attack, it is likely to tamper with a lesser and vulnerable operator [7, 8].

Access to a single operator can cause serious damage due to the improper trust model within LTE core network signaling. It is assumed that LTE components running Diameter are from a trustworthy "closed community". Hence, a single vulnerable operator renders all (usually hundreds of) roaming partners susceptible to Diameter attacks. Although the GSMA recommends adopting filtering [9], there is still a large part of operators that do not adopt such techniques [1]. Moreover, it is difficult to differentiate malicious signaling messages from legitimate ones. Even with the adoption of filtering techniques, existing researches [2, 3] show that most Diameter attacks succeed with high probability (38%-100%).

C. Threat Model

We are concerned with an adversary who seeks to disrupt a victim's access to mobile network services (e.g., Operator A in Figure 1). The attacker gains access to another vulnerable operator (Operator B in Figure 1), which has a roaming contract with the target network. The adversary intercepts and sends Diameter messages from/to the vulnerable operator. It spoofs fake signaling messages to the target network's DRA, pretending to be a legitimate message during roaming. The messages subsequently prompt the target network to stop providing the target user with certain services.

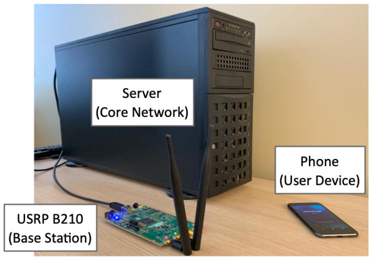


Fig. 2: Our testbed for Diameter attacks.

III. Prototyping Diameter Attacks Against LTE Signaling Messages

In this section, we implement and study the reported attacks on LTE core networks signaling messages using Diameter attacks. Specifically, we *do not* introduce any new or unreported attacks. Instead, this section focuses on the following:

- Prototype and validate typical Diameter attacks on LTE mobile core on our testbed.
- Quantify the attack impact and understand the severity.
- Gain insights that can lead to detection and mitigation.

A. Testbed

Our testbed is shown in Figure 2. We deploy our own LTE mobile core network on our server with a 12-core Intel Xeon Silver 4214 CPU and 32GB RAM, without affecting the real operator networks. Facebook Magma [10], which has been deployed in real-world networks, is adopted as our core network software. The base station is implemented on USRP B210 software-defined radio, running the open-source, standard-compliant LTE stack OpenAirInterface [11]. We use a Pixel XL phone with a standard-compliant GSM SIM card sysmoUSIM [12] as the victim device. The SIM is programmed and registered in the testbed core network.

To launch the Diameter attacks, we implement the attacker by launching another process which sends spoofed Diameter messages to the HSS or MME based on the attack type.

Ethical Considerations In our testbed, the wireless communication is operated in LTE Band 7, which is not used by any commercial device in the area of the experiments. The spoofed Diameter signaling messages only circulate within our testbed and do not harm real networks or LTE users.

B. Overview of Diameter Attacks

In this paper, we focus on Diameter attacks against LTE core signaling messages that cause user DoS. The general procedure of launching such attacks is shown in Figure 3. The attacker sends a spoofed Diameter message that leverages the vulnerability in §II-B (step 1). Based on the attack type, either HSS or MME updates the state for the victim user (step 2).

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.

Signaling Functionality	Involved Msg	Receiver	Description of Damage	Detection
Subscription Update	IDR (ARD) IDR (APN) IDR (ODB)	MME MME MME	The victim device detaches from the LTE network and loses data, voice, and texting services (§III-C1)	Device investigates the detach message and re-initiates an attach (§V-A1)
Device Purging	PUR	HSS	The victim device loses voice call and texting services (§III-C2)	Device exchanges the text messages and checks the reply (§V-A2)
Location Update	ULR CLR	HSS MME	The victim device detaches from the LTE network and loses data, voice, and texting services (§III-C3)	Device re-attaches to the network and checks the returned messages (§V-A3)

TABLE I: Overview of attacks using LTE core network signaling messages. We list the Diameter messages involved in each attack and introduce their caused damages. The detection will be detailed in §V.

The new state indicates that the victim user will be disabled from certain services. The network subsequently initiates some signaling exchanges with the victim device (step 3). As a result, the user device under DoS can no longer access data and/or voice services (step 4).

Table I summarizes three different types of Diameter attacks we study, targeting subscription update, device purging, and location update. The attacks leverage four Diameter messages: IDR (Insert Subscriber Data Request), PUR (Purge Request), ULR (Update Location Request), and CLR (Clear Location Request). They are common Diameter messages in real roaming scenarios [13] and can thus pass the DRA checking in the victim network. The mentioned attacks are practical based on real-world studies [2, 3] and evaluation in our testbed. The attacks all cause user DoS, ranging from loss of specific service to complete detach from the network.

Other Diameter Attacks The attacks we study in Table I cover the most known device DoS Diameter attacks, as shown in [3]. Although we do not cover other types such as Operator information leakage and Device information leakage, our testbed supports prototyping any attack that involves standard-compliant Diameter messages. They can be launched by the same procedure in Figure 3, by changing the message content.

C. Prototype Diameter Attacks in LTE Core Network

We now describe in detail how each Diameter attack is realized and analyze its severity. For each attack, we introduce how to launch it with a specific Diameter message. We show our realization of each attack in the prototype testbed. The consequences of attacks are also presented.

1) Attacking Subscription Update: IDR (Insert Subscriber Data Request) is a Diameter message from HSS to MME for updating user subscription data. When user subscription changes in HSS, it notifies the MME with an IDR message. IDR includes fields that specify what parts of subscription are changed. In this paper, we focus on three of them: ARD (Access-Restriction-Data) specifies which network types (4G LTE, 3G, etc.) are restricted by the network. APN (Access-Point-Names) specifies which sub-network within LTE a user can connect to for data transfer. ODB (Operator-Determined-Barring) specifies if a user's certain service (Data, voice, etc.) is barred.

Attack Details The attack message is shown in Figure 3(a). For ARD attack, the ARD header present in the IDR message is set to 0x3F to disabled 4G service of the user. For APN attack, IDR message includes an APN header with "All-APN-Configurations-Included-Indicator" set to 0. This forces MME to delete all available networks for the user. It then adds APN-Profile of a non-existent network to serve the victim user. For ODB attack, the ODB header is present with the value set as 0x1FF, which indicates that both data and voice services are barred. After the subscription update, MME determines that the user should no longer be served by it. Consequently, the network sends a detach message to notify the user.

Prototype and Attack Damage We realize the IDR attack and successfully force the victim device to disconnect from the network. Diameter IDR attack can be launched whenever a user is connected to the LTE network. Upon receiving the detach request, the user device disconnects from the network. It thus loses the network connection and cannot use any data, voice, or texting service, as shown in Figure 4(a)

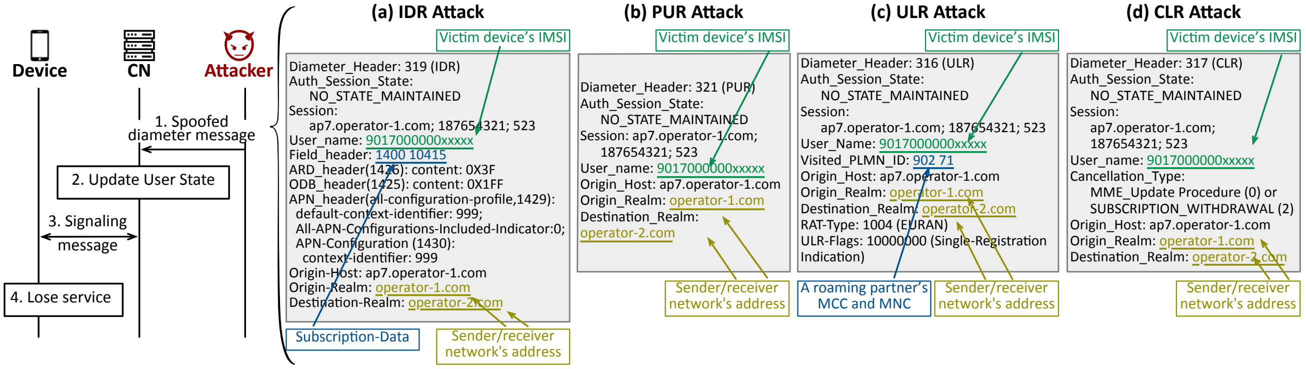
To evaluate the attack impact, we record the throughput of file downloading. Figure 4(b) shows that the download speed drops to 0 after the launch of the attack. The damage cannot be automatically mitigated; in our illustrative attack, the device loses any service for more than 60 seconds. After that, we let the victim device launch a full reboot. However, the attack can be re-launched any time afterwards. We replay the attack 20 times and reach a 100% attack success rate for all ARD, APN, and ODB attacks.

Insight We verify that the IDR attacks can be launched with a *single* attack Diameter message. Its damage is persistent for minutes without further action. The attack can be re-launched even after user reboots the device. Meanwhile, its damage cannot be easily distinguished from other valid reasons such as bad signal. It is necessary to analyze the message exchange with the network to detect the attack. Moreover, fast mitigation is required as the attacks can be repeatedly launched.

2) Attacking Device Purging: PUR (Purge Request) is a Diameter message sent from MME to HSS to notify that it no longer serves a user (due to detach, etc.). Upon receiving this message, HSS sets the purge flag to true in the database. When an incoming call or text message is intended for this user, HSS decides the user status by checking the purge flag [14, 15]. If the flag is true, HSS thinks the user is offline and rejects the call or delays the text messages.

Attack Details An attacker sends a PUR Diameter message to block a user's voice and texting services. It spoofs a standard-compliant PUR message with the content shown in

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.



(a) IDR Attack

```
Diameter_Header: 319 (IDR)
Auth_Session_State:
    NO_STATE_MAINTAINED
Session:
    ap7.operator-1.com; 187654321; 523
User_name: 9017000000xxxxx
Field_header: 1400 10415
ARD_header(1426): content: 0X3F
ODB_header(1425): content: 0X1FF
APN_header(all-configuration-profile,1429):
  default-context-identifier: 999;
  All-APN-Configurations-Included-Indicator:0;
  APN-Configuration (1430):
    context-identifier: 999
Origin-Host: ap7.operator-1.com
Origin-Realm: operator-1.com
Destination-Realm: operator-2.com
```

(b) PUR Attack

```
Diameter_Header: 321 (PUR)
Auth_Session_State:
    NO_STATE_MAINTAINED
Session: ap7.operator-1.com;
    187654321; 523
User_name: 9017000000xxxxx
Origin_Host: ap7.operator-1.com
Origin_Realm: operator-1.com
Destination_Realm:
operator-2.com
```

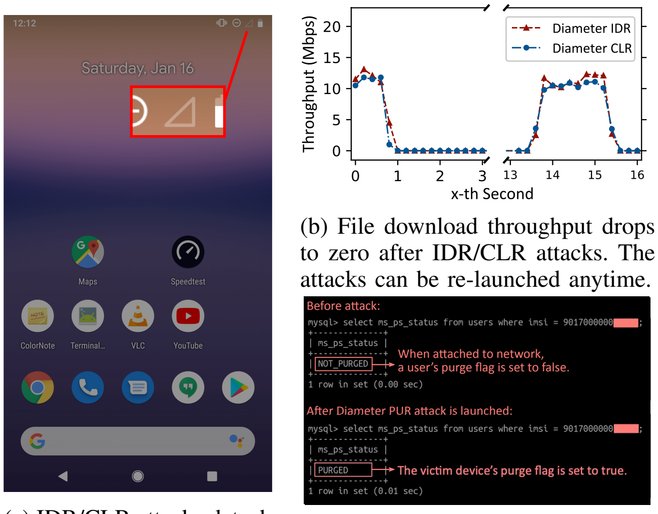
(c) ULR Attack

```
Diameter_Header: 316 (ULR)
Auth_Session_State:
    NO_STATE_MAINTAINED
Session:
    ap7.operator-1.com; 187654321; 523
User_Name: 9017000000xxxxx
Visited_PLMN_ID: 902 71
Origin_Host: ap7.operator-1.com
Origin_Realm: operator-1.com
Destination_Realm: operator-2.com
RAT-Type: 1004 (EURAN)
ULR-Flags: 10000000 (Single-Registration
Indication)
```

(d) CLR Attack

```
Diameter_Header: 317 (CLR)
Auth_Session_State:
    NO_STATE_MAINTAINED
Session:
    ap7.operator-1.com;
    187654321; 523
User_name: 9017000000xxxxx
Cancellation_Type:
    MME_Update Procedure (0) or
    SUBSCRIPTION_WITHDRAWAL (2)
Origin_Host: ap7.operator-1.com
Origin_Realm: operator-1.com
Destination_Realm: operator-2.com
```

Fig. 3: Overview of Diameter attacks. A general procedure is shown on the left and the concrete attack message details are listed in (a)-(d) for each Diameter attack.



(a) IDR/CLR attacks detach the victim device from the network.

(b) File download throughput drops to zero after IDR/CLR attacks. The attacks can be re-launched anytime.

```
Before attack:
mysql> select ms_ps_status from users where imsi = 9017000000[redacted];
+--------------+
| ms_ps_status |
+--------------+
| NOT_PURGED   |→ When attached to network,
+--------------+  a user's purge flag is set to false.
1 row in set (0.00 sec)

After Diameter PUR attack is launched:
mysql> select ms_ps_status from users where imsi = 9017000000[redacted];
+--------------+
| ms_ps_status |
+--------------+
| PURGED       |→ The victim device's purge flag is set to true.
+--------------+
1 row in set (0.01 sec)
```

(c) The PUR attack flips the purge flag to true.

Fig. 4: Damages of Diameter attacks in our testbed.

Figure 3(b), where the attacker specifies the victim's IMSI. Since the message is legitimate in roaming scenarios, HSS accepts the message and sets the purge flag in database [13].

Prototype and Attack Damage We implement the PUR attack in the attacker process. Diameter PUR attack can be launched any time when a user is connected to the network. We verify that the purge flag is modified for the victim user in HSS database, as in Figure 4(c). The attack is robust in that the success rate is 100% in Magma after repeating 20 times.

Consequently, any incoming voice call or text message cannot reach the user as the purge flag indicates that the user is currently offline. Unfortunately, we cannot directly show this as none of the open-source LTE core network supports voice or texting service to the best of our knowledge. These services rely on circuit-switch Telecom infrastructure from older generations (2G and 3G).

Insight The PUR attack is stealthy and cannot be directly observed by the victim device. Any data service and outgoing call/texting will be processed normally, while the victim cannot receive any incoming message without *any* notification. Therefore, a device needs to actively trigger incoming texting or voice call to learn whether they are blocked.

3) Attacking Location Update (ULR/CLR): CLR (Clear Location Request) is a Diameter message sent from HSS to MME to detach a user and delete its subscription. A CLR message can be triggered when the user moves to a new tracking area. CLR includes a field that specifies the reason for this message and a flag that allows the user to immediately re-attach. ULR (Update Location Request) is a message from MME to HSS when the MME starts to serve a newly attached user. The receiving HSS sends a CLR message to the MME which previously served the user.

Attack Details An attacker can either spoof a ULR message to the victim's HSS that triggers CLR. It can also directly spoofs a CLR message to the victim's serving MME. In the former ULR attack, the attacker sends a ULR message with the victim's IMSI to the victim's home HSS, as shown in Figure 3(c). This message falsely announces that the victim is attached to another network. The victim HSS starts update location procedure by sending a CLR to the MME. In the latter method, the attacker directly sends a CLR message (Figure 3(d)) to the victim's serving MME, informing that the victim has moved to another area. The following steps and results are similar to the ULR attack above.

Prototype and Attack Damage We implement the ULR and CLR attacks by creating those messages in the attacker process. Since ULR attack consequently triggers a CLR, we only show the results from CLR attack for simplicity. After receiving the CLR message, the serving MME deletes the victim's subscription profile and detaches the victim, as shown in Figure 4(a). This causes the victim to lose any service. We replay the attack 20 times and reach a 100% success rate.

The download speed drops to 0 after the attack, as shown in Figure 4(b). Similar to IDR, the effect can last seconds or even minutes, until a reboot is initiated by the victim. The device might reconnect to the network; however, the Diameter attack can be relaunched any time afterwards.

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.

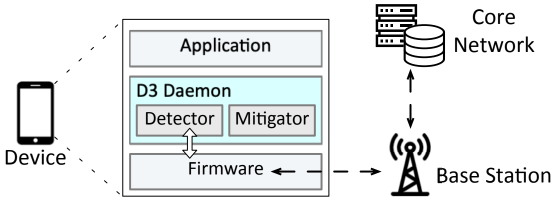


Fig. 5: D3 system components.

Insight Similar to IDR, CLR/ULR attack messages target the core network, but trigger notable effects on mobile devices. This leads us to two clues to potentially detect and mitigate such attacks on the device side. First, the actual message that causes the DoS on device may bear certain characteristics that distinguish it from normal service loss. Also, the attack effect is caused by incorrect removal of subscription data on MME. Meanwhile, the authentic copy on MME is still intact. Discovering and resolving the discrepancy is the crucial step.

IV. D3 Overview

A. D3 System Components

We design D3, a **D**evice-centric **D**efense for **D**iameter attacks, that runs on phone-side as an application-layer software for detecting and mitigating Diameter attacks. D3 can detect all 6 attacks that we introduce in §III and mitigate their negative effects with pure in-device softwares. Its ideas can be extended to other Diameter attacks. D3 consists of two major components, Detector and Mitigator, shown in Figure 5. Detector interacts with device LTE chipset. It captures, decodes, and analyzes the NAS message exchanges between the device and the network. Whenever a Diameter attack happens, Detector can detect it by analyzing the abnormal message exchanges. It then notifies such an event to Mitigator. Mitigator operates purely in-device as well. By changing device-side configurations or manipulating the communication with the LTE network, Mitigator can offset the negative effect caused by the Diameter attacks. D3 is robust, as it works even if the attacker is aware. It leverages NAS messages, which are generated by the authentic MME or device. They cannot be modified or controlled by the attacker.

Relationship with Infrastructure-centric Solutions Our device-centric solutions are complementary to infrastructure-centric ones. A device can report the situation to the network after detecting the attacks, to further prevent the attacks. In addition, infrastructure-centric solutions are good at detecting any unauthorized Diameter message *before* the damage. D3 offers a solution that detects and mitigates the attacks *after* they have impacted the victims.

In addition, detecting some Diameter attacks is only possible on the device side. If the attacker is an operator shown in §II, the attack messages will be considered legitimate by the victim's network, thus passing all infrastructure security checks. For instance, a ULR attack message has the exact same content as one in a legitimate roaming scenario. However, a device-centric solution can detect such attacks by checking whether the victim's service is abnormally blocked. The software solution does not need expensive infrastructure update, and can be realized by software patches.

B. Device-Centric Detector

Although Diameter messages are exchanged within the core network, a device can observe the resulting NAS message exchange between the core network and itself. The key is to establish the relationship between the attack Diameter messages and the resulting NAS. We have seen hints from §III that Diameter attacks need to communicate with the device in a certain pattern. Our device-centric solutions also check the difference between the NAS messages under Diameter attacks and under normal conditions that could also trigger a loss of service, such as bad signal.

To find evidence for Diameter attacks, a device needs access to its NAS message exchange with the network. Mobile networks have long been considered a closed community and mobile devices have limited access to runtime operational logs. Fortunately, device-centric solutions are no longer impossible with the development of software tools that can extract mobile chipsets information (such as [16]),

C. Device-Centric Mitigator

Since the Diameter attacks can be relaunched to be persistent, the victim cannot completely eliminate the damage. One immediate action is to notify the operator for attack prevention (the operator can add filters on Diameter messages). However, the user can also initiate device-side mitigation. It is run after every time a Diameter attack is detected by Detector.

To design Mitigator, we first need to understand why the Diameter attacks cause DoS damages. LTE stores a user's subscription (service access control, data rate, etc.) in HSS. However, it creates a copy in MME to serve the user locally. The Diameter attacks falsely notify MME or HSS that the subscription (copy) is changed in the other component. The distributed state design has made the DoS attacks possible, yet it is challenging to roll out a new core network architecture.

Our mitigation solution provides a quick attempt to make the state consistent without infrastructure update. The device initiates several actions, which can force HSS and MME to re-synchronize. We will elaborate on them in the next section.

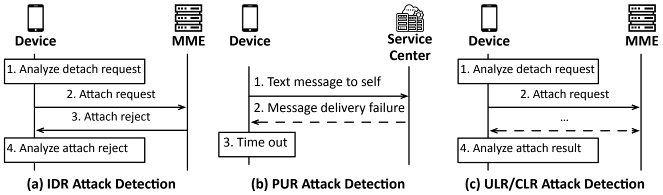
V. D3 Design Details

We have shown the logistics to launch device-centric detection and mitigation. In this section, we demonstrate how each attack is detected and mitigated by D3.

A. Detecting Diameter Attacks

1) Detecting IDR Attack: As we described in §III, regardless of the field used in IDR message, MME will detach the device immediately. Ideally, a device-centric detection can directly find out the detach is caused by the Diameter message in the detach message from the network. Unfortunately, the detach message only contains a flag of re-attach without any specific reason. In all discussed IDR attacks, attach type is set to no re-attach [4].

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.



(a) IDR Attack Detection (b) PUR Attack Detection (c) ULR/CLR Attack Detection

Fig. 6: D3 detection procedure for each attack.

However, a detach request of type "no re-attach" itself is a hint for a Diameter attack. In normal cases, e.g. bad signal or network internal error, the user will not receive detach request but instead either directly lose wireless connection with the base station or implicitly released by the core network [4].

To further confirm the Diameter IDR attack, D3 actively queries the network. D3 does so by forcing the device to re-attach. Although the detach request suggests that the chipset firmware should stay idle, we can still initiate it at the OS level by toggling the airplane mode. The network will respond with an attach reject message with an embedded PDN connectivity reject, which specifies the exact cause [4]. The cause value will be 0001000 for the ODB attack, 1110000 for the ARD attack, and 0110110 for the APN attack. Unless a user requests a subscription update, it is impossible that these three parts are certainly changed in the MME. We can thus use this indicator to confirm that the previous detach is caused by a Diameter attack. The above detection procedure is shown in Figure 6(a).

This detection can be done in a very timely fashion: D3 only needs to check the message exchange between network and device to get the hint, which can be acquired from chipsets within a negligible time. The overhead of observing the NAS messages is minor, as LTE control message exchange is low-frequency and low-volume.

2) Detecting PUR Attack: The first idea for device-centric detection of PUR is to check the NAS messages received by device side. However, the PUR attack only affects HSS without explicitly notifying the user. To detect such PUR attack, D3 adopts an active approach.

The key to detecting this attack is to check if a user's incoming texting service is disabled. One possible way is to set up a texting server which periodically sends messages to users. D3 uses a yet simpler device-only way, where the device periodically sends a text message to itself. According to the standard, the messages still go through the identical procedure of normal texts [15]. The outgoing texting is not affected, while the incoming message can be used to indicate the PUR flag status. If the user fails to receive the echoed message while other services (e.g., data) are normal, D3 detects a PUR attack. The procedure is shown in Figure 6(b).

The only overhead of detecting PUR attack is the periodic text messages. The sending and receiving of texts are usually freely provided by LTE operators. Meanwhile, detecting such attack can be done within a periodicity of sending text messages, which can be configured by the user's preference.

3) Detecting ULR/CLR Attacks: Both CLR and ULR attacks will cause the victim's detach from the network [13], as confirmed in our implementation. The solution of D3 is illustrated in Figure 6(c). It starts with detecting the detach request and service loss, similar to IDR attacks. It is necessary to distinguish the attacks from normal detach, such as change of serving MME or subscription expiration.

D3 first checks the detach type in the NAS detach request from the network. If it is "re-attach required", the detach is triggered by a valid reason and the chipset will handle it according to standard. Otherwise, after receiving the detach request, D3 immediately retries attaching to the network, regardless of the "re-attach not required" detach request type. If the user is under ULR/CLR attack, the attack message only affects subscription at MME side, where the master copy at HSS is intact. A re-attach can help the user regain the service. Whereas in a normal case, the user will still fail to get service in the attempt to re-attach.

B. Mitigating Diameter Attacks

Although a device can notify the core network for defending the attacker, D3 proposes complimentary device-centric fixes to mitigate the damage. Depending on the core network implementation, the device itself can regain the denied service without the infrastructure support. The goal of the mitigation, as briefed in §IV-C, is to force the network to re-synchronize the state among the core network components.

The main approach used by D3 to synchronize the state is to toggle the airplane mode. This will force the user device to disconnect from the network (if connected) and then resend an attach request. This approach is guaranteed to work for ULR/CLR attack, as MME after ULR/CLR completely deletes user subscription. Therefore, when a user re-attaches to the network, MME will send a new (and legitimate) ULR to the HSS which will retrieve the correct subscription. With the same procedure, PUR attack is also guaranteed to be fixed: HSS will be notified who is the current MME that serves the user. As a result, the purge flag is set to false.

D3 further considers scenarios where simple airplane mode does not work: According to standard, MME implementation can choose to cache the user subscription even after the user detaches from the network [13]. In this case, the user subscription at the MME side after Diameter attack could persist for a predefined period. If the user re-attaches to the network in this period, MME will not query the HSS for user subscription synchronization.

Consequently, we devise optional mitigation for IDR attacks. The first measure is to handover to another LTE cell. This can be done by searching available cell list and then locking the phone to another one by internal or 3rd party tools, such as Network Signal Guru [17]. A new serving base station might notify the MME to update the subscription. The second available measure is to keep the device in airplane mode for an extended period of time (e.g. a few minutes), during which the MME subscription cache will expire.

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.

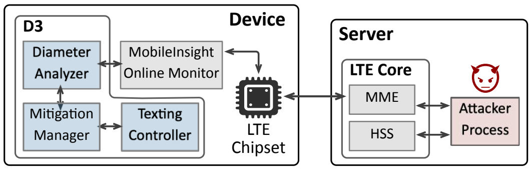


Fig. 7: Implementation of D3.

C. D3 Applicability to 5G and Other Diameter Attacks

We study whether D3 works for 5G. Operators are deploying the first phase of 5G, known as 5G Non-Standalone (NSA). 5G NSA reuses the 4G core network, which means that the same Diameter attacks described in this paper will still threaten 5G NSA. Consequently, D3 is still applicable.

The next stage 5G Standalone (SA) will adopt a new core design [18]. 5G SA employs network functions (NF) for different functionalities. New security measures are introduced to protect communications among NFs, including OAuth2.0, Security Edge Protection Proxy [19], to name a few. It also replaces Diameter with more secure HTTP/2 to carry signaling [19]. However, NFs from the same community can still bypass the security measures without checking content [20], similar to 4G. Therefore, a trusted but compromised NF from another operator can still launch DoS attacks.

We can adapt D3 to detect similar threats in 5G. Even with its new architecture and security techniques, 5G mostly inherits NAS from LTE [21]. Moreover, D3 can mitigate the attacks with minor changes, e.g. handover to another 5G small cell instead of a 4G cell for state re-synchronization.

VI. D3 Implementation

Figure 7 outlines our implementation of device-centric solution D3. We implement it as an Android application on mobile devices. Diameter Analyzer runs in the background and collects mobile network logs from MobileInsight online monitor [16]. MobileInsight is an open-source software that can expose real-time cellular information from chipset. When the device loses service, Diameter Analyzer extracts the collected NAS messages and analyzes them. Meanwhile, Texting Controller regularly sends text messages with Android's SmsManager API for detecting PUR attack.

When an attack is detected, Diameter Analyzer or Texting Controller calls the Mitigation Manager, which uses the Android Settings Module and broadcast services to toggle the airplane mode. If it is not sufficient, D3 sends a toast notification and prompts the user to lock band with internal system tools.

VII. Evaluation

A. Effectiveness of D3 Detection and Mitigation

In this section, we verify the D3's ability to detect the launched attacks and mitigate them. The implementation is mainly tested on a Google Pixel XL phone device. In our experiments, Diameter attacks can be perfectly detected and D3 can fully eliminate the damage caused by the attack.

Attack Name	IDR	PUR	ULR/CLR
Precision (%)	100	N/A	100
Recall (%)	100	N/A	100
Detection + Mitigation (s)	1.0	6.1	1.1
CPU Usage (%)	42.0→46.9 (+4.9)		
Memory Usage (%)	47.0→48.0 (+1.0)		

TABLE II: Precision, recall, and overhead of D3.

For Diameter IDR and ULR/CLR, D3 will first get notified that the device loses the network connection. For detecting IDR, D3 checks the detach NAS message, as shown in Figure 8(a). It can quickly send another attach request message to the network, which is rejected, shown in Figure 8(b). A PDN connectivity reject is embedded in the attach reject message and its cause code helps us determine the Diameter attack type (Figure 8(c)). Meanwhile for ULR/CLR attacks, the device's attach request is accepted and consequently mitigates the attack. We show that D3 can detect the attack and recover the download speed to its initial level in a run of fixing IDR attack in Figure 9. The mitigation works similarly for recovering Diameter ULR/CLR. D3 is effective in all 20 attempts of Diameter IDR and ULR/CLR attacks in our experiments.

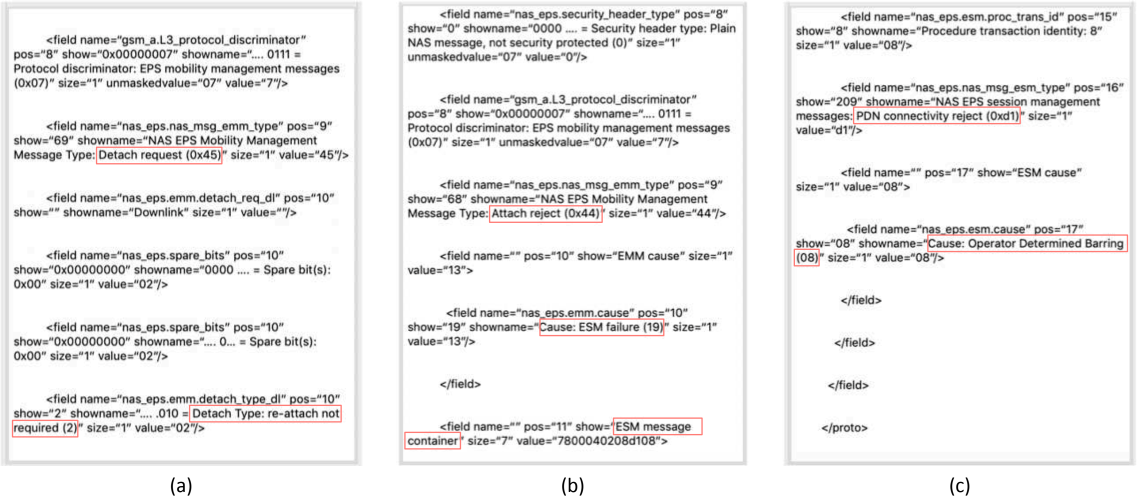
For PUR attacks, since no open-source core network supports circuit-switched Telecom services including call and text messaging, we emulate the detection as follows: Instead of exchanging text messages with the core network, the phone sets up a TCP connection with the server and periodically sends packets to it. The server plays the role of service center for text messages. If the user's purge flag is set off, the server will respond with a TCP packet. Otherwise, it ignores the packet, which emulates the behavior where the core network delays the delivery of an incoming text message when the purge flag is set on. The detection also achieves a 100% success rate for all 20 attempts. By initiating a re-attach, device can quickly mitigate the problem.

We provide some further insights on why D3 can fully negate the impact caused by Diameter attacks in our testbed. We discussed in §V-B that the effectiveness of D3 mitigation depends on the period that MME keeps the copy of the user subscription. In our testbed, Magma deletes the user subscription immediately after a user detaches. Therefore, the designed re-attach will force the MME to retrieve a correct copy for this user, which results in a full recovery from the Diameter attacks. In an operational implementation, D3 might need to switch to another base station for full mitigation.

B. Accuracy, Promptness, and Overhead

We evaluate the accuracy and efficiency of D3. We mix the Diameter attacks with other operations that can cause the same damages and check if they can be distinguished by D3. Recall that the results of both the Diameter IDR and ULR/CLR attacks are complete loss of service. Therefore, we manually create three other scenarios where the device is completely disconnected from the network: bad signal, network internal error, and device error. Bad signal is performed by moving device out of the testbed coverage. Network internal error

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.



```
        <field name="gsm_a.L3_protocol_discriminator"
pos="8" show="0x00000007" showname=".... 0111 =
Protocol discriminator: EPS mobility management messages
(0x07)" size="1" unmaskedvalue="07" value="7"/>

        <field name="nas_eps.nas_msg_emm_type" pos="9"
show="69" showname="NAS EPS Mobility Management
Message Type: Detach request (0x45)" size="1" value="45"/>

        <field name="nas_eps.emm.detach_req_dl" pos="10"
show="" showname="Downlink" size="1" value=""/>

        <field name="nas_eps.spare_bits" pos="10"
show="0x00000000" showname="0000 .... = Spare bit(s):
0x00" size="1" value="02"/>

        <field name="nas_eps.spare_bits" pos="10"
show="0x00000000" showname=".... 0... = Spare bit(s):
0x00" size="1" value="02"/>

        <field name="nas_eps.emm.detach_type_dl" pos="10"
show="2" showname=".... .010 = Detach Type: re-attach not
required (2)" size="1" value="02"/>
```

(a)

```
        <field name="nas_eps.security_header_type" pos="8"
show="0" showname="0000 .... = Security header type: Plain
NAS message, not security protected (0)" size="1"
unmaskedvalue="07" value="0"/>

        <field name="gsm_a.L3_protocol_discriminator"
pos="8" show="0x00000007" showname=".... 0111 =
Protocol discriminator: EPS mobility management messages
(0x07)" size="1" unmaskedvalue="07" value="7"/>

        <field name="nas_eps.nas_msg_emm_type" pos="9"
show="68" showname="NAS EPS Mobility Management
Message Type: Attach reject (0x44)" size="1" value="44"/>

        <field name="" pos="10" show="EMM cause" size="1"
value="13">

          <field name="nas_eps.emm.cause" pos="10"
show="19" showname="Cause: ESM failure (19)" size="1"
value="13"/>

        </field>

        <field name="" pos="11" show="ESM message
container" size="7" value="7800040208d108">
```

(b)

```
          <field name="nas_eps.esm.proc_trans_id" pos="15"
show="8" showname="Procedure transaction identity: 8"
size="1" value="08"/>

          <field name="nas_eps.nas_msg_esm_type" pos="16"
show="209" showname="NAS EPS session management
messages: PDN connectivity reject (0xd1)" size="1"
value="d1"/>

          <field name="" pos="17" show="ESM cause"
size="1" value="08">

            <field name="nas_eps.esm.cause" pos="17"
show="08" showname="Cause: Operator Determined Barring
(08)" size="1" value="08"/>

          </field>

        </field>

      </field>

    </proto>
```

(c)

Fig. 8: NAS message exchange captured at the device for attack detection and mitigation. Decoded by MobileInsight and opened by its GUI tool. (a): Detach request message; (b) & (c) Attach reject message with PDN connectivity reject.

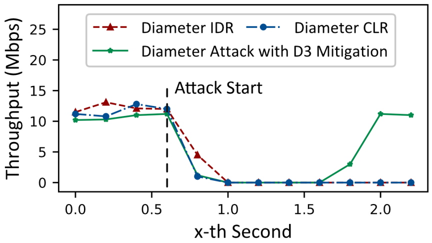


Fig. 9: Download throughput drops to 0 after Diameter attacks but recovers after `D3` mitigation.

is raised by inserting segfault to Magma at runtime. Device error is realized by sending signals to change APN setting that disables LTE services at the device side. Our experiment randomly injects Diameter IDR attack, Diameter ULR/CLR attack, or one of the three scenarios and repeats 100 times.

Our experiment shows that, `D3` can detect the attacks with perfect precision (Table II). No false positive is found as different scenarios yield different message exchange results (discussed in §V). Nevertheless, it is possible that rare cases exist that can cause false positives. However, `D3` does not incur much extra cost even it mis-classifies another scenario as Diameter attack. We also measure recall, which represents the fraction of the detected attacks among the launched attacks. `D3` detects all attack attempts and achieves a recall of 1.

Since there is no other known case where voice and texting are disabled while data is still available, we did not evaluate PUR's precision and recall. However, similar to IDR and ULR/CLR, `D3` will not cause any negative impact even if the normal operation is mis-classified as Diameter PUR attack.

`D3` can detect and mitigate Diameter attacks promptly. Table II records the latency of detecting and mitigating such attacks. Since part of the mitigation is already done during detection, we record their total latency. It takes 1.0s, 6.1s, and 1.1s on average to detect and mitigate Diameter IDR, PUR, and ULR/CLR attacks. The major latency sources come from message analysis, airplane toggling, and network re-attach. Detecting and mitigating PUR attacks take longer time because the device relies on periodic messages to confirm the attack, which can be reduced if the periodicity is configured to a small value (10s in our testbed).

`D3` incurs marginal overhead. We measure its overhead using Android CPU and Memory monitors [22, 23]. The results are concluded in Table II. `D3` consumes <5% extra CPU usage, while the memory usage is barely increased. This is because `D3` only monitors the LTE NAS messages, which is lightweight for modern Android phone devices.

VIII. Related Work

Studies on Diameter attacks highlight vulnerabilities and attack practice [2, 3, 24, 25]. Various other security vulnerabilities in cellular core network are exposed to cause DoS [26, 27], service downgrade [28], and privacy leakage [27, 29]. They only propose costly infrastructure-side countermeasures by adding new functions, such as IP filtering or firewalls [30, 31]. These solutions cannot defend against our threat model where the attacker forges a message from another operator, and they suffer from high overhead [2, 3]. Meanwhile, [32] proposes detection of SS7 attack at device side but still requires network assistance. `D3` provides a lightweight device-centric solution which can detect and mitigate the attacks. [33, 34] propose device-centric security solutions, but focus on control-plane and caller-ID spoofing, respectively. `D3` instead leverages the messages to detect the attacks targeting mobile core network signaling and propose countermeasures.

IX. Conclusion

We present the design, implementation, and evaluation of `D3`, a device-centric solution to defend against Diameter attacks in mobile networks. Instead of traditional operator-led

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.

solutions, D3 takes a fresh view. It infers and mitigates the user DoS caused by spoofed Diameter messages by in-device analysis of message exchange, without any additional infrastructure support. We prove the effectiveness and efficiency of this approach in an LTE standard-compliant testbed.

The solution idea of D3 can be applied to a broader context. Since the industry is under transition to the 5G, many new attacks that target user service will surface. While D3 only offers a showcase example that covers 6 attacks, the device-centric approach can be further leveraged. By exploiting in-depth analysis and domain knowledge, we can potentially adapt D3 to defend against new Diameter attacks or other threats. More community efforts are thus needed to work on this promising yet essential direction.

Acknowledgment

We greatly thank the reviewers for their insightful comments and constructive feedback. This work is partly supported by NSF CNS-1910150 and NSF CNS-2008026.

References

[1] European Union Agency For Network and Information Security, "Signalling Security in Telecom SS7/Diameter/5G: EU level assessment of the current situation," March 2018.

[2] Positive Technologies, "Diameter Vulnerabilities Exposure Report," 2018.

[3] ——, "Security assessment of Diameter networks," 2020.

[4] 3GPP, "TS24.301: Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)," Sep. 2019. [Online]. Available: https://www.3gpp.org/dynareport/24301.htm

[5] V. Fajardo, J. Arkko, J. Loughney, and G. Zorn, "Rfc 6733-diameter base protocol," 2012.

[6] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking attacks for lte networks using the interworking functionality," in *IFIP Networking*. IEEE, 2016, pp. 315–322.

[7] Ars Technica, "Hackers are exploiting a platform-agnostic flaw to track mobile phone locations," Sept. 2019. [Online]. Available: https://arstechnica.com/information-technology/2019/09/hackers-are-exploiting-a-platform-agnostic-flaw-to-track-mobile-phone-locations/

[8] The Verge, "For $500, this site promises the power to track a phone and intercept its texts," June 2017. [Online]. Available: https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime

[9] GSMA, "FS.21 Interconnect Signalling Security Recommendations," Dec. 2019.

[10] Facebook, "Facebook Magma," Mar. 2020, https://github.com/facebookincubator/magma.

[11] OpenAirInterface, "OpenAirInterface Official Website," April 2018, http://www.openairinterface.org.

[12] sysmocom, "sysmoUSIM-SJS1 SIM + USIM Card," 2016. [Online]. Available: http://shop.sysmocom.de/products/sysmousim-sjs1

[13] 3GPP, "TS29.272: Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol," Sep. 2019. [Online]. Available: https://www.3gpp.org/dynareport/29272.htm

[14] ——, "Basic call handling; Technical realization," Jun. 2018. [Online]. Available: https://www.3gpp.org/dynareport/23018.htm

[15] ——, "Circuit Switched (CS) fallback in Evolved Packet System (EPS)," Dec. 2017. [Online]. Available: https://www.3gpp.org/dynareport/23272.htm

[16] Y. Li, C. Peng, Z. Yuan, J. Li, H. Deng, and T. Wang, "Mobileinsight: Extracting and analyzing cellular network information on smartphones," in *Mobicom*, 2016, pp. 202–215.

[17] Q. Technologies, "Network Signal Guru," 2020. [Online]. Available: https://play.google.com/store/apps/details?id=com.qtrun.QuickTest&hl=en_US

[18] T-Mobile, "T-Mobile Achieves Significant 5G Firsts with Cisco, Ericsson, MediaTek, Nokia, OnePlus and Qualcomm," May 2020. [Online]. Available: https://www.t-mobile.com/news/tmobile-achieves-significant-5g-firsts

[19] 3GPP, "TS123.500: 5G; 5G System; Technical Realization of Service Based Architecture; Stage 3," Mar. 2020. [Online]. Available: https://www.3gpp.org/DynaReport/29500.htm

[20] ——, "TS123.502: 5G; Security architecture and procedures for 5G System," Mar. 2020. [Online]. Available: https://www.3gpp.org/DynaReport/33501.htm

[21] ——, "TS124.501: Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3," Apr. 2020. [Online]. Available: https://www.3gpp.org/DynaReport/24501.htm

[22] S. monitor tools lab Cpu Ram Battery, "CPU Monitor - temperature, usage, performance," 2020. [Online]. Available: https://play.google.com/store/apps/details?id=com.glgjing.stark&hl=en_US

[23] ——, "RAM Booster (Memory Cleaner)," 2020. [Online]. Available: https://play.google.com/store/apps/details?id=com.glgjing.captain&hl=en_US

[24] S. Holtmanns, S. P. Rao, and I. Oliver, "User location tracking attacks for lte networks using the interworking functionality," in *2016 IFIP Networking Conference (IFIP Networking) and Workshops*, 2016, pp. 315–322.

[25] S. P. Rao, B. T. Kotte, and S. Holtmanns, "Privacy in lte networks," in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, 2016, p. 176183.

[26] M. T. Raza, F. M. Anwar, and S. Lu, "Exposing lte security weaknesses at protocol inter-layer, and inter-radio interactions," in *International Conference on Security and Privacy in Communication Systems*. Springer, 2017, pp. 312–338.

[27] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4g/lte mobile communication systems," *NDSS*, 2015.

[28] A. Shaik, R. Borgaonkar, S. Park, and J.-P. Seifert, "New vulnerabilities in 4g and 5g cellular access network protocols: exposing device capabilities," in *ACM WiSec*, 2019, pp. 221–231.

[29] B. Hong, S. Bae, and Y. Kim, "Guti reallocation demystified: Cellular location tracking with changing temporary identifier." in *NDSS*, 2018.

[30] Huawei, "LTE International Roaming Whitepaper." [Online]. Available: https://carrier.huawei.com/en/technical-topics/core-network/lte-roaming-whitepaper

[31] Oracle Communications, "Oracle Communications Diameter Signaling Router." [Online]. Available: http://www.oracle.com/us/industries/communications/diameter-signaling-router-ds-2100660.pdf

[32] C. Peeters, H. Abdullah, N. Scaife, J. Bowers, P. Traynor, B. Reaves, and K. Butler, "Sonar: Detecting ss7 redirection attacks with audio-based distance bounding," in *S&P*. IEEE, 2018, pp. 567–582.

[33] M. Echeverria, Z. Ahmed, B. Wang, M. F. Arif, S. R. Hussain, and O. Chowdhury, "Phoenix: Device-centric cellular network protocol monitoring using runtime verification," in *NDSS*, 2021.

[34] H. Deng, W. Wang, and C. Peng, "Ceive: Combating caller id spoofing on 4g mobile phones via callee-only inference and verification," in *Proceedings of the 24th Annual International Conference on Mobile Computing and Networking*, 2018, pp. 369–384.

Authorized licensed use limited to: UCLA Library. Downloaded on January 10,2023 at 01:29:44 UTC from IEEE Xplore. Restrictions apply.