User-targeted Denial-of-Service Attacks in LTE Mobile Networks

Rami Ghannam*, Filipo Sharevski† and Anthony Chung‡
College of Computing and Digital Media
DePaul University. Chicago, Illinois 60604
Email: *rghannam@cdm.depaul.edu, †fsharevs@cdm.depaul.edu, ‡achung@cdm.depaul.edu

***Abstract*—Mobile networks are prevalent in today's world, being used in a variety of applications ranging from personal use to the work environment and other. Ensuring security for users in a mobile network is therefore increasingly important. Denial-of-service attacks or DoS proved to be the biggest threat to mobile networks in recent years. A lot of work has been done in DoS targeting the infrastructure of the mobile network. User-targeted DoS attacks have been neglected in comparison. The fourth generation of cellular networks 4G LTE is the fastest growing mobile network in terms of subscriber numbers. The security aspect of mobile networks has improved throughout the generations, however, 4G proved to still have vulnerabilities in the signaling plane that allow a malicious attacker to target a specific user. Deploying a rogue base station and forcing the targeted user to connect to it is possible. The attacker could then deny selected services of the targeted user such as voice and SMS services. In this paper, we survey the work done on user-targeted DoS attacks in LTE networks. We analyze the 3GPP LTE standard specifications that allow such attacks. We also test the response of a LTE mobile device to tweaked Attach Accept messages during an Attach Procedure. We furthermore examine the conditions that affect the attack when we have equal priority cells. We finally present a case study of how a targeted user connected to an LTE network provider could be denied SMS and voice services therefore denying 2-factor authentication. We tested the scenarios using open-source implementations of the LTE network stack and widely available Software Defined Radios.**

I. Introduction

A denial-of-service (DoS) attack is a security threat that prevents legitimate users from accessing specific services by targeting hosting computer systems, network resources or the user devices. DoS Attacks constitute a major threat in communication networks as recent attacks have shown. On October 21st, 2016, a Distributed Denial of Service attack took down Internet services for millions of subscribers on the Eastern seaboard of the United States [1]. Dyn, a company that provides backbone Internet services, sustained a DDoS attack against their DNS infrastructure which denied users access to popular services such as Netflix, Spotify, and Twitter. The attack was launched by the Mirai malware[1] that instructed 100,000 malicious endpoints to forward bogus DNS queries to Dyn and overload their DNS infrastructure.

On the other hand, recent years have witnessed an exponential growth of mobile networks and their user base. By 2020, the global subscriber base is expected to reach 5.6 billion meaning that over 70% of the world's population will be connected to a mobile network [2]. When mobile subscribers use smartphones today to make a call, send an email, check the weather, scroll through social media applications, they expect having good service, good coverage and a fast connection all the time. The spread of security attacks that threaten to disrupt the mobile connection has been narrow thanks to the proprietary interfaces and the adoption of the telephone network-specific Signaling System 7 (SS7) telecommunications standard that made mobile networks less attractive targets than the open and widely-spread IP networks. However, the architecture of the mobile network shifted towards an all IP-based architecture that is inherently more susceptible to security attacks. The transition exposes the cellular networks to traditional DoS IP-based attacks in addition to the signaling/user traffic DoS attacks characteristic of the cellular infrastructure, e.g. [3] and [4]. Hackers have also increased their activity in the mobile network; mobile-specific malware has been on a steep rise as shown in the McAfee mobile threat report [5]. The trend of using mobile devices in the business environment has also contributed to the hackers shift of attention to mobile networks. (BYOD) or Bring Your Own Device is the trend when employee-owned devices are used within a business. Employees use their own device at home, on the road and at work. It is harder to secure devices that the company does not own and control [6]. Mobile security is now a top concern for operators and users alike.

Different mitigation approaches have been proposed to protect against these DoS attack variants, including stateful monitoring, anomaly-based and signature-based detection techniques [7]. However, there is the possibility for DoS vector that can target a single mobile device and not necessarily a server/infrastructure node [8].

A. Problem Statement

This paper focuses on *user-targeted denial-of-service attacks*. Not many works have studied the attacks against a specific user of the mobile network, for example, how to single out a user and block selected services of that user.

Table I categorizes DoS Attacks on Cellular Networks. The *Vector* column indicates whether signaling traffic or valid data traffic is used in the attack. The *Target* indicates whether the infrastructure or the user is the subject of the attack.

[1]Mirai is a malware that takes advantage of vulnerabilities in Internet of Things devices and takes control of them thus creating an army of attacking devices, i.e., a botnet.

TABLE I: DoS Attacks in Cellular Networks.

Reference	Vector		Target		Intensity		Persistence	
	Data traffic	Signaling traffic	Infrastructure	User	High	Low	Yes	No
Dyn DNS [1]		✓	✓		✓			✓
Deutsche Telekom [9]		✓	✓		✓		✓	
KrebsOnSecurity.com [10]	✓		✓		✓			✓
Bassil *et al.* [3]		✓	✓		✓			✓
IMS server attack [4]		✓	✓		✓			✓
SMS client DoS [4]		✓		✓		✓	✓	
Shaik *et al.* [8]		✓		✓		✓	✓	
Huang [11]		✓		✓		✓	✓	

The intensity expresses the impact of the attack; an attack that targets a population of users is considered high intensity, an attack that targets individual users has a low intensity. Finally, an attack is persistent if the affected user/s cannot recover unless they explicitly perform a required action such as rebooting the mobile device.

We list in the table a few of the infrastructure-based DoS attacks for reference and comparison. Deutsche Telekom was attacked in November of 2016 by a variant of the Mirai malware putting more than 900,000 customers offline [9]. Consumer router devices were hacked and the broadband connection therefore disconnected. On September 20th, 2016, the security blog KrebsOnSecurity.com was also attacked using the same Mirai botnet with a traffic magnitude of 650 Gbps [10]. Bassil *et al.* prove that repeatedly triggering Bearer activation and deactivation overloads the signaling plane of the cellular network [3]. Tu *et al.* [4] present the different threats that the IP Multimedia Subsystem[2] faces. Denying SMS services by sending a huge number of SIP/SMS messages to the IMS server is one of the specified attacks. A second attack is SMS client DoS, it exhausts a mobile's resources by sending SIP/SMS messages to the mobile itself; this attack requires malware to be installed on the victim's mobile device. Malware-based attacks put the phone under numerous threats and attacks. More could be found in [12]. Our focus in this paper is on user-targeted DoS attacks that exploit vulnerabilities in the LTE protocol.

The user-targeted DoS attack targets a single subscriber to the cellular network. Various cellular services could be denied. For example, denying 4G services limits the user's phone to use an older/less secure network. Forcing a user to switch from the 4G network to the 2G GSM network makes attacks specific to the 2G network possible. Another attack is to deny all or partial services of the user like voice calling services.

Two distinct adversarial models exist when attacking a mobile network user. Attacks could be passive by only monitoring the network, or active by deploying a rogue base station. Passive attacks goal is to gather data and information flowing in the network without any disruption to the communication. Active attacks entail interruption of the communication between the mobile device and the network, hence directly affecting the normal functioning of the network. Denying the service is considered an active attack.

Radio jamming attacks also lead to DoS. Jamming happens when the attacker generates a radio signal in order to interfere with the legitimate wireless signal between the subscriber and the base station. Zou *et al.* [13] identify the various types of jamming that could occur in a wireless network. Jamming affects all the users that are being serviced by the eNodeB, which makes the attack easy to detect. In this work, the target is one particular user of the network without affecting the rest of the users.

B. Significance of the problem

This research will examine and determine the role of user-targeted DoS attacks in 4G LTE networks. The greater demand and pervasiveness of mobile devices justifies the need for comprehensive security approaches. Therefore, operators will be better prepared to counter such attacks. Standards bodies will be guided on what should be emphasized in future network generations to improve the overall security of mobile communications. For the next generation of mobile networks 5G, the security aspect is of paramount importance especially with the use cases that are being discussed such as controlling critical infrastructure through the 5G network, or controlling self-driving cars. The goal is to achieve an optimal 5G security architecture [14]. Uncovering critical areas in DoS attack scenarios against a targeted user is mandatory.

II. Related Work

Denial-of-service attacks are one of the major threats to network availability. 4G LTE witnessed a major shift in the security paradigm. DIAMETER protocol was adopted as the successor to SS7 protocol. Attacks on SS7 stack included denial of service through excess resource utilization and call spoofing [15]. Mobile operators upgrading to 4G LTE diameter-based security did not resolve all the security issues of previous generations.

The security segment of mobile networks has advanced considerably throughout the mobile generations. However, the increasing sophistication of cyberattacks and the availability of open-source software and cheap hardware to build rogue base stations expose the mobile network to user-targeted DoS

[2]The IP Multimedia Subsystem (IMS) is a 3GPP architecture meant to standardize the delivery of multimedia services over an IP packet-switched network. The 3rd Generation Partnership Project or 3GPP is a collaboration project between telecommunication standard bodies that develops globally applicable specifications for mobile systems.

attacks. An analysis of the 4G wireless standards is therefore needed to uncover the vulnerabilities that allow such attacks.

Barbeau [16] evaluates the impact and application of rogue base station attacks in a WiMax/802.16 network. Jover [17] shows the insecurities of the LTE network using low cost equipment and open source software, thus proving the vulnerability of the LTE network against attacks that could be launched with few resources and a minimal budget. A Software Defined Radio or SDR is a radio communication system in which physical layer functions are implemented in software, allowing reduced cost testing of radio communications. The author experiments with low cost SDR in order to demonstrate the applicability of a series of exploits on the LTE network. The author implements for example the IMSI[3] catcher with a USRP B210 [18] running a modified version of openLTE. Shaik *et al.* [8] realize active rogue eNodeB attacks against an LTE device leading to fine location leaks and DoS. The authors intercept signaling communication of the LTE device. They also send false signaling messages to the device. Huang [11] introduces a new exploit that takes advantage of the vulnerabilities in LTE procedures, particularly the tracking area update procedure, the attach procedure, and the Radio Resource Control redirection procedure. Huang is able to force a targeted LTE device to downgrade into a maliciously controlled GSM network.

III. Background in LTE

The LTE network is divided into three main parts: Evolved Packet Core (EPC), Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) and the User Equipment (UE). The Evolved Packet System (EPS) consists of EPC and E-UTRAN. In this paper, the attack is targeting a specific user of the mobile network by attacking the UE of that user.

The behavior of the User Equipment in a LTE network could be defined using three main states: registered with the EPC, connected and idle. The UE is registered with the network means that the UE has been authenticated and has been allocated an IP address. The UE has to register with the EPC before being able to send or receive any data. A UE is connected when it is active, sending or receiving data. A UE is in idle mode when it has no active connections with the cellular network.

The UE is either in EMM-REGISTERED or EMM-DEREGISTRED [19]. In the deregistered state, the mobile has no service; it is either switched off, in airplane mode, or is out of coverage. In the registered state, the mobile is registered with a serving Mobility Management Entity and a serving gateway, it has an IP address allocated and a default EPS bearer, which provides the device with an always-on connectivity to the default packet data network. The ATTACH procedure takes the UE from the deregistered to the registered state. The DETACH procedure moves the UE back to the deregistered state.

[3]An international mobile subscriber identity (IMSI) is a unique permanent number that identifies a mobile subscriber, it is stored in the SIM card.

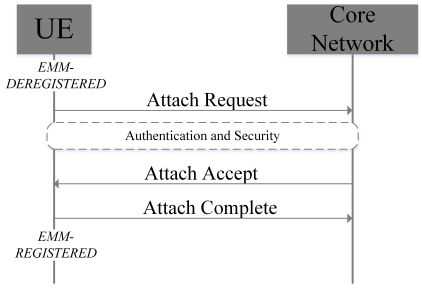


Fig. 1: EPS Mobility Management Attachment Procedure.

Figure 1 illustrates some of the messages involved in the registration process of the UE with the network. The attachment procedure starts with the UE in the EMM-DEREGISTRED state sending an Attach Request to the core network. If the UE is successfully authenticated and secure communication is successfully established between the UE and the core network, the process ends with the exchange of Attach Accept and Attach Complete messages moving the UE to the EMM-REGISTERED state.

Two types are disntiguished when a UE sends an Attach Request to the core network:

- **EPS-only**: The UE is requesting only LTE services.
- **Combined EPS/IMSI attach**: The added IMSI Attach provides access to non-EPS services provided by other Radio Access Technologies (2G, 3G). A successful combined EPS/IMSI attach lets the UE seamlessly handover between RATs.

IV. Building a Rogue Base Station

A. LTE Protocol Vulnerabilities

Specific procedures in the LTE specification need to be exploited to realize the rogue base station [8], [11]. First, the targeted user must connect to the rogue base station. For this purpose, the cell reselection procedure is used. The 3GPP LTE standards provide the "Absolute priority based reselection" method [20] where the user is required to connect to base stations tuned to high priority frequencies. Priorities are broadcast by the legitimate base station in SIB 5[4]. By passively sniffing SIB messages, the higher priority frequencies are divulged. As well, the MCC and the MNC[5] could be detected in SIB 1. The rogue base station could then be configured to broadcast the same MNC and MCC and tuned to the higher priority frequencies, hence luring the user to attach to it instead of the legitimate one.

Once the user is attached to the rogue base station, the attack proceeds to deny services to her/him. The Non-Access Stratum (NAS) is a set of protocols in the LTE architecture. It is used to convey non-radio signaling between the User Equipment (UE)

[4]System information Block is a set of messages that relay system information, each serving a different purpose.

[5]Mobile Country Code is a three digit decimal code that identifies a country. Mobile Network Code is a two or three digit decimal code that identifies a mobile network.

and the Mobility Management Entity (MME). NAS procedures are arranged in two groups: the EPS Mobility Management (EMM) and the EPS Session Management (ESM). EMM is mainly responsible for mobility management, authentication and security. The focal point here is in one of the EMM procedures called the Tracking Area Update (TAU). The TAU procedure updates the location of the UE with the MME. During the update, the MME and the UE also negotiate the network modes whether it is 2G, 3G or LTE services depending on the capabilities of the UE, the capabilities of the operator in that area, and the subscription type of the user. Therefore the operator could deny or allow 2G, 3G or LTE services. In particular, a TAU Reject message is sent to the UE specifying which services are allowed. These messages are not integrity protected hence the user would accept any such message. Shaik *et al.* [8] plant a rogue eNodeB and are then able to send a false TAU Reject message to any LTE subscriber within the range of their rogue base station. Using TAU Reject message with cause number 7 "LTE services not allowed", the services of the device are downgraded to the 2G or 3G network, and using TAU Reject message with cause number 8 "LTE and non-LTE services not allowed", all services to the UE are denied.

Services to the user can be denied also using the network Attach Procedure. During the Attach Procedure, the UE indicates to the network whether it is attaching for EPS services, both EPS and non-EPS services (2G, 3G), SMS-only, or emergency bearer services. For this purpose, the UE sends an Attach Request message to the MME. If the UE does not have a valid EPS security context from a previous authentication procedure, the Attach Request message is not integrity protected [19]. By intercepting the Attach Request message from the device, the attacker is able to modify it to allow only selected services such as SMS only and finally forward it to the network. Since the message is not protected, the network accepts it and the MME registers the UE as SMS-only capable. The user will therefore not receive incoming calls nor will he be able to make outgoing calls.

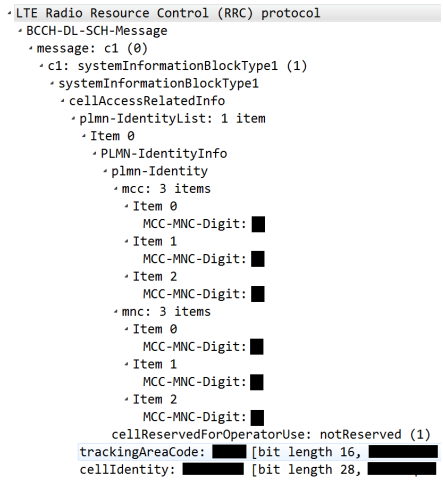
B. Denying Services

The Tracking Area Identity (TAI) identifies a TA and it incorporates the PLMN identity and a Tracking Area Code (TAC) that is unique for each TA. The TAI of a cell is broadcast in SIB 1 that is passively sniffed. By tuning the rogue eNodeB to broadcast a TAC that is different than current TA, the UE is forced into initiating a tracking area update procedure.

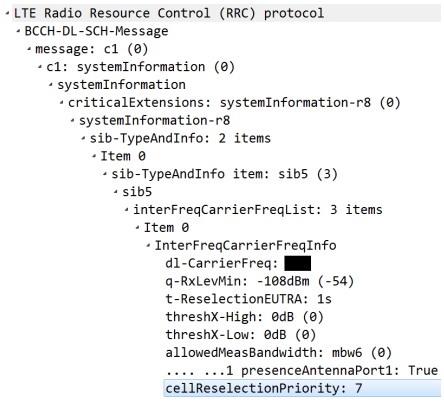
Passively sniffing the unencrypted broadcast information in a cell will provide the required parameters to implement the user-targeted DoS attack, i.e. MNC, MCC, frequency priorities and TAC. Figures 2a and 2b show SIB 1 and SIB 5 respectively of a cell belonging to a USA mobile operator captured in our lab.

Tuning the rogue eNodeB to broadcast the same MNC and MCC will mislead the targeted UE into thinking that the eNodeB is part of the real operator's network. Tuning the frequency of the rogue eNodeB to a higher priority frequency will force the UE to connect to it. Once connected, the attacker could deny selected services to the UE by exploiting NAS signaling procedures as explained in Section IV-A.

Fig. 2: Sniffing eNodeB Configuration.



(a) SIB 1



(b) SIB 5

C. Hardware and Software Requirements

This section elaborates on the hardware and software requirements to build the rogue base station. There is a number of open source projects providing the software that facilitates cellular network research and prototyping. Software defined radio platforms (SDR) allow passive and active experimentation by enabling transmission/reception of data over the air. The SDR combined with an open-source software implementation of LTE would replicate a real LTE eNodeB. Shaik *et al.* [8] use USRP B210 [18] with OpenLTE software [21]. OpenLTE is an open source implementation of the 3GPP LTE specifications; the software architecture is straightforward and code could efficiently be added. Huang [11] use USRP B200 Mini [18] with a laptop running openBTS software [22] to build a fake GSM network, and USRP B210 with a laptop running openLTE software to build a fake LTE network. srsLTE [23] is another open source platform for

LTE experimentation and it includes srsUE, an implementation of the UE stack to emulate a mobile device. srsUE allowed passive sniffing of the broadcast information in an LTE cell. OpenAirInterface (OAI) [24] is also an open source framework for the development of 3GPP cellular networks. OAI is a highly rich tool that we leveraged for our experiments.

The setup in our lab includes a USRP x310 [18]. The USRP SDR was chosen since it is compatible with OpenLTE and OAI and is within budget. The chosen mobile device is a smartphone from Motorola, the Moto G5 Plus [25], and is 4G LTE capable. Finally, a PC is needed to run the open source LTE software.

V. GUTI Discovery

An international mobile subscriber identity (IMSI) is a unique number that identifies a mobile subscriber, it is a permanent number and is stored in the SIM card. Using the IMSI in radio communication makes it vulnerable to sniffing by attackers. In order to maintain user identity confidentiality, the LTE standards define a temporary identifier GUTI that could be used instead of IMSI. GUTI is the Globally Unique Temporary Identity; it is the addition of the PLMN-ID (identifies the mobile operator), the MME Group Identity (identifies a group of MMEs), and the S-TMSI (SAE-Temporary Mobile Subscriber Identity which temporarily identifies a UE). The GUTI is assigned during the Attach procedure.

When a UE receives a call or data and is in IDLE state, the network will page the UE. The network broadcasts paging messages that contain the temporary identifier of that UE. By passively sniffing the broadcast messages in a cell, an attacker could make a list of GUTIs. Mobile operators do not frequently change GUTIs in order to reduce signaling and a GUTI could persist for several days. An attacker could initiate a call or data connection to the targeted user multiple times and sniff the list of GUTIs being broadcast. Applying set intersection analysis proposed in [26] would reveal the mapping between the GUTI and the subscriber phone number. When initiating a call or data connection to the targeted user, the user should not be alerted. Authors in [8] for example use social media applications Facebook and Whatsapp in order to silently initiate a data connection to the UE without the user's awareness.

VI. UE's reaction to different Attach Accept

A. Voice-Centric UE

A UE could be set as Voice-centric or Data-Centric. Voice centric means that the UE always tries to ensure that a voice service is available [27]. If a voice-centric UE discovers that IMS voice and CSFB (Circuit Switch Fallback) are not supported then it disables the LTE capability and searches for other radio access technologies such as GSM radio access network (GERAN) or UMTS terrestrial radio access network (UTRAN). We experimented in our lab with a Motorola Moto G5 Plus. The Moto G5 sends a Combined Attach EPS/IMSI, and has the preference set to Voice centric. Plus it is CS voice only which indicates that voice communication services are allowed to be invoked only over the CS domain. Figure 3a shows a snippet from the Wireshark capture of the Attach Request sent by the Motorola phone to the core network.

TABLE II: UE Mode of Operation.

	Voice centric	**Data centric**
EPS services	PS mode 1	PS mode 2
EPS and non-EPS services	CS/PS mode 1	CS/PS mode 2

Fig. 3: UE Setting.

```
Voice Domain Preference and UE's Usage Setting
    Element ID: 0x5d
    Length: 1
    0000 0... = Spare bit(s): 0
    .... .0.. = UE's usage setting: Voice centric
    .... ..00 = Voice domain preference for E-UTRAN: CS Voice only (0)
```

(a) Moto G5 Plus

```
Voice Domain Preference and UE's Usage Setting
    Element ID: 0x5d
    Length: 1
    0000 0... = Spare bit(s): 0
    .... .1.. = UE's usage setting: Data centric
    .... ..00 = Voice domain preference for E-UTRAN: CS Voice only (0)
```

(b) LTE Dongle

Furthermore, according to TS 24.301 [19], a UE attached for EPS services operates in one of four modes of operation show in Table II. The Moto G5 is therefore in CS/PS mode 1.

Here is how the Moto G5 responds to various Attach Accept messages sent by core network:

(a) EPS-only with no cause: UE sends a TAU Request after 10 seconds with "combined TA/LA updating with IMSI Attach". It waits for T3411 timer to expire which is 10 seconds by default [19]. After 5 attempts, the TAU request is sent again after timer T3402 expires.

(b) EPS-only with cause #17 "Network Failure": Same as point (a).

(c) EPS-only with cause #18 "CS domain not available": UE loses the radio connection. Looking at LTE standards:
- Moto G5 is in CS/PS mode 1 of operation: this mode means the UE registers to both EPS and non-EPS services, and UE's usage setting is *voice centric*.
- A UE in CS/PS mode 1 of operation with "IMS voice not available" shall attempt to select GERAN or UTRAN radio access technology and disable the E-UTRA capability.

(d) EPS-only with SMS-only: Same as point a. EPS-only means that the combined Attach procedure has failed according to TS 24.301 [19]. Therefore same behavior is expected as point a.

(e) Combined EPS/IMSI with SMS-only: UE loses radio connection. Looking at LTE standards:
- The ATTACH ACCEPT message includes the Additional update result "SMS only" or "CS Fallback not preferred", a UE operating in CS/PS mode 1 with "IMS voice not available" attempts to select another radio access technology (RAT) such as GSM RAT and disables the LTE EUTRA capability.

B. Data-Centric UE

We also experimented with a LTE dongle that was in CS/PS mode 2. It was set as data-centric; Figure 3b.

The dongle sends a Combined Attach EPS/IMSI, and has the preference set to Data centric. Plus it is "CS voice only" which indicates as with the Moto G5 that voice communication services are allowed to be invoked only over the CS domain.

Here is how the dongle responds to various Attach Accept messages sent by core network:

(a) EPS-only with no cause: UE loses radio connection. Looking at LTE standards:
   - EPS-only means that the combined Attach procedure has failed.

(b) EPS-only with cause #17 "Network Failure": UE sends a TAU Request after 10 seconds with "combined TA/LA updating with IMSI Attach". It waits for T3411 timer to expire which is 10 seconds.

(c) EPS-only with cause #18 "CS domain not available": UE is connected and can access Internet. Looking at LTE standards cause #18, this behavior is correct for a UE in CS/PS mode 2.

(d) EPS-only with SMS-only: Same as point (a).

(e) Combined EPS/IMSI with SMS-only: UE is connected and can access Internet; matches the standard.

VII. Cell Reselection to an Equal Priority Frequency

When a UE could reselect to a neighboring cell that has the same priority as that of the serving cell, a cell-ranking criterion called the R criterion is used to rank the serving cell and the neighboring cell [28]. The UE measures the signal power from the current serving cell and from neighboring cells in order to choose the best received signal. Furthermore, the UE applies hysteresis and offset values advertised in system information blocks by the network. The hysteresis is added to the serving cell to prevent rapid changes and avoid oscillation of the criterion. The offset is applied to each neighboring cell, giving the operator more precise control over the reselection to specific cells.

When evaluating the cell reselection criteria, the UE abides by the minimum serving cell residence time. The UE should be camped on the serving cell for at least 1 second before reselecting to another cell. This guarantees that cell reselections aren't happening too often. Additionally, the network specifies a $T_{reselection}$ time interval. Before any reselection is triggered, the calculated criterion should be higher for at least $T_{reselection}$ seconds. This avoids any unnecessary ping-pong effect between neighboring cells. We see t-ReselectionEUTRA is 1 second in the capture shown in Figure 2b.

The calculated criterion R values could then be ranked from highest to lowest. A neighboring cell should have a higher criterion for the UE to choose to reselect to it. For the attack to work, the rogue eNodeB should be transmitting a signal power level to have the criterion of the rogue cell higher than the criterion of the current serving cell.

However the LTE standards aim to maximize the battery life of the UE. Therefore, the UE could skip measurements if the received signal quality from the serving cell is above a threshold specified in SIB 3 by the network. In this case, the reselection could not occur even if the criterion of the rogue cell is higher, and the attack will not be successful. In the captures of the SIB information of USA mobile operators, we noticed that many times the cell priority of a neighbor cell is 7 which is the highest priority, and the priority of the current serving cell is 7 as well. The snippet in Figure 2b shows a priority of 7 for the neighbor cell for example. The serving cell in this case had also a priority of 7 as captured in SIB 3 (snippet not shown). Finally, we could conclude that mobile providers that use the highest priority of 7 will be less vulnerable to the the attacks discussed in this paper. However this will affect the operator's ability to use the priorities feature. An operator may concentrate users on a certain cell or distribute them over several cells by associating each cell with a priority from 0 to 7. Therefore, giving each cell a priority of 7 reduces the ability of the operator to divide the users among various cells and maximize network spectral efficiency.

VIII. A case study of blocking two-factor Authentication

Security of Internet applications such as online banking is strengthened by two-factor authentication schemes. Any username-password authentication could be strengthened by deploying a secondary authentication mechanism where a token is sent to a user's mobile device via SMS or voice call.

Two-factor authentication has gained a lot of interest and is widely used today. Breaking this scheme [29] could have disastrous effects on a user and could lead to identity theft.

In our sue case, the attacker has identified a particular user of the mobile network and wants to block two-factor authentication by denying voice calling and/or SMS messaging.

First the attacker catches the GUTI of the user as explained in section V. Second, we suppose that the phone is set to data-centric and it relies on CS voice only. Some smart-phones such as the Samsung Galaxy Note 3 allow the user to choose between voice or data centric. Otherwise, this setting is set by the phone manufacturer.

By tweaking the Attach Accept as seen in VI-B, we could force the UE to react in various ways. Two possible scenarios are listed below:

- Having a rogue employee or installation of user-targeted malware has been proven as a successful attack in the infamous Athens affair [30]. In this case, the lawful interception segment of the Vodafones Greece mobile switching center was reprogrammed (possibly by an insider or an external collaborator) to stealthily create interception streams of all traffic from a small subset of Greek officials and forward it to a designated destination for covert analysis. Similarly, the rogue malware (or a rogue employee with system level access) will tweak the response sent to the UE to be EPS-only with cause #18

"CS domain not available". This will deny both voice and SMS services, therefore stealthily denying two factor authentication to the targeted user.
- If we catch the Attach request and add SMS-only to it, this will deny voice-based two factor authentication.

IX. Discussion

Mobile networks have evolved through different generations. Currently, 4G has the largest percentage of mobile data traffic by connection type carrying 69 percent of total mobile traffic - it is projected to have 79 percent of total mobile data traffic by 2021 [31]. 3GPP specify the standards for mobile communications enhancing the functionality of the network with each generation and incorporating better security features.

The increase in mobile network usage, the trend of BYOD and the pervasiveness of mobile devices made the mobile network an attractive target to hackers. The discussion about network DoS attacks is not a matter of whether it will occur or not, but rather when it will occur, how fast it could be detected, and how to limit the damages. Through the analysis of previous research and the experiments done in our lab, this paper highlights the possibility and feasibility of user-targeted DoS attacks. We studied how we can target a particular user of the LTE network and deny services of that user. We surveyed other works that have targeted individual users of the mobile network. By demonstrating the UE's reaction to different Attach Accept messages, we presented various scenarios that could be used to deny specific services such as voice calling and SMS. We furthermore analyzed the attack feasibility when we have equal priority cells. Finally, we presented a case study of two-factor authentication using SMS or voice call. While two-factor authentication schemes can be effective, blocking these schemes could lead to catastrophic results for the individual user.

A. Implications of User-Targeted DoS

Smart mobile devices are being increasingly used in emergency response systems, specifically in urban settings [32] and in the development of Internet of Things-based disaster response system [33]. Malicious cyber attackers are likely to target key mobile phones to maximize the effect of a widespread attack and compromise the safety of civilians and emergency responders.

When targeting high-value targets, the attacks are advanced and persistent. We have witnessed the number and complexity of cyber-attacks continuously on the rise. The Advanced Persistent Threat or APT is a highly complex and hard to detect attack that requires expert developers and significant financial resources [34]. With APT, we can no longer assume that attackers have limited resources and are remotely located. Furtherrmore, Cyber espionage and insider attacks are currently one of the biggest security threats [35]. States and security companies could both be behind this kind of attacks.

The need for a new security paradigm to govern all the changing trends in the mobile security landscape is critical. Gelenbe *et al.* [36] acknowledge the evolving threat against mobile networks especially with the emergence of large scale botnets and new complimentary access methods to the mobile network via Wi-Fi and femtocells[6]. Authors develop the NEMESYS project that is a mobile security framework with the aim to better understand, analyze and detect security threats against the mobile network. Evolving factors in the mobile network motivated the NEMESYS project: 1- the smart mobile ecosystem where users are always connected and use their phones for personal and corporate purposes, 2- the variety of wireless interfaces and platforms, and 3- the multitude of offered services.

Lastly, we mention here another possible scenario for future investigation where the attacker deploys a connected system of rogue base stations that cover the most visited locations of the targeted user. Knowing the IMSI/GUTI from one location, it would be shared among the rest of the locations, enabling the attacker to single out the user and deny the service of only that user in more than one location.

B. Detection and Prevention

We discuss in this paragraph potential preventive solutions and detection methods both on the network side and on the user side. Several countermeasures could be applied to prevent user-targeted DoS. We discuss these countermeasures here and we leave the evaluation of these measures for future work, especially the impact on the mobile network elements, the amount of modifications needed, and the issues of interoperability and backward compatibility.

The network should have a mechanism where messages received from unauthorized network entities are not accepted by the UEs. Upon receiving a message such as a *TAU reject*, the UE should be able to detect if the message was sent by the legitimate network. The UE could then apply the correct actions and respond only to authentic messages. One proposed solution is to protect these messages using public-private key cryptography where different keys are used for encryption and decryption. The network entities and the UEs will each have their own set of public-private keys. Messages sent by the network or by the UE could therefore be digitally signed and verifiable by the recipient. However, the obstacle when applying such solution is the high computational cost of public key cryptography and the increased signaling overhead [37].

Another solution suggested in [8] is to reallocate the GUTI identifier more frequently so that it cannot be tracked. However, that will require network operators to make the change and comply with the security measure.

In order to regain service, a UE that has been targeted and received an illegitimate TAU Reject message, needs to be rebooted or the SIM card has to be removed and reinserted. Implementing a timer on the UE could mitigate this issue without the involvement of the human user [8]. Once the timer expires, the UE would try to reattach itself to the network. If the user has moved to a place unreachable by the attacker

[6]A femtocell is a mobile phone base station that boosts cellular signal inside a home or office. It is connected to the mobile network via the customer's existing broadband connection.

and the UE is not within the coverage area of the rogue base station anymore, the UE should successfully reattach to the legitimate network and regain service.

Mobile technologies have evolved throughout the years in order to sustain the growth in demand. Four generations have shaped this evolution, the most recently deployed one being 4G. Driven by the growth of mobile data traffic, mostly due to the rising use of smartphones, the industry is now on the path to the fifth generation of mobile networks - 5G. One of the key strategies of 5G design is to alleviate the latency when deploying applications and services. Storing content and processing data closer to the mobile users would reduce the latency. For this purpose, the 5G architecture will include edge-cloud deployments [38]. In this paradigm, real-time insights about the network state become possible, and could be leveraged in security applications to detect attacks in real-time. By monitoring a user's history, the network could detect if a user has been on a downgraded service for a long time, i.e. determine that selected services that were previously available for that user are now unavailable.

One solution on the user side is to warn them when their service is being downgraded, or it is denied due to a TAU Reject message. If the user is being downgraded to a GSM network [11], and a notification pops up on their phone, the user could be given the option to accept the redirection or not. In this case, explicit user confirmation could potentially prevent the redirection attack.

REFERENCES

[1] Dyn analysis summary of friday october 21 attack. [Online]. Available: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack

[2] GSMA: The mobile economy 2016. [Online]. Available: http://www.gsma.com/mobileeconomy

[3] R. Bassil, I. Elhajj, A. Chehab, and A. Kayssi, "Effects of signaling attacks on LTE networks," *27th International Conference on Advanced Information Networking and Applications Workshops*, March 2013.

[4] G.-H. Tu, C.-Y. Li, C. Peng, Y. Li, and S. Lu, "New security threats caused by ims-based sms service in 4g lte networks," *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 1118–1130, October 2016.

[5] B. Snell. (2016) McAfee Mobile Threat Report. [Online]. Available: https://www.mcafee.com/us/resources/reports/rp-mobile-threat-report-2016.pdf

[6] K. W. Miller, J. Voas, and G. F. Hurlburt, " BYOD: Security and Privacy Considerations ," *IEEE IT Professional*, vol. 14, pp. 53–55, 2012.

[7] S. Mavoungou, G. Kaddoum, M. Taha, and G. Matar, "Survey on threats and attacks on mobile networks," *IEEE Access*, vol. 4, pp. 4543–4572, August 2016.

[8] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi, and J.-P. Seifert, "Practical attacks against privacy and availability in 4G/LTE mobile communication systems," *Proceedings of the Network and Distributed System Security Symposium*, February 2016.

[9] Deutsche Telekom hack part of global internet attack. [Online]. Available: http://www.dw.com/en/deutsche-telekom-hack-part-of-global-internet-attack/a-36574934

[10] Krebsonsecurity hit with record ddos. [Online]. Available: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[11] L. Huang, "Forcing a targeted LTE cellphone into an eavesdropping network," *Hack In The Box Security Conference*, May 2016.

[12] G. Suarez-Tangil, J. E. Tapiador, P. Peris-Lopez, and A. Ribagorda, "Evolution, detection and analysis of malware for smart devices," *IEEE Communications Surveys and Tutorials*, vol. 16, pp. 961–987, 2014.

[13] Y. Zou, J. Zhu, X. Wang, and L. Hanzo, "A survey on wireless security: Technical challenges, recent advances, and future trends," *Proceedings of the IEEE*, vol. 104, pp. 1727–1765, May 2016.

[14] G. Horn and P. Schneider, "Towards 5g security," *IEEE Trustcom/BigDataSE/ISPA*, pp. 1165–1170, August 2015.

[15] M. Chen, Y. Qian, S. Mao, W. Tang, and X. Yang, "Signaling system 7 SS7 network security," *45th Midwest Symposium on Circuits and Systems, 2002*, vol. 3, pp. 496–499, 2002.

[16] M. Barbeau, "Wimax/802.16 threat analysis," *Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks*, pp. 8–15, October 2005.

[17] R. P. Jover, "LTE security, protocol exploits and location tracking experimentation with low-cost software radio," *Bloomberg LP Security, Shmoocon 2016*.

[18] USRP Universal Software Radio Peripheral, Ettus Research - A National Instruments Company. [Online]. Available: http://www.ettus.com

[19] "3rd Generation Partnership Project; Technical Specification Group Core Network and Terminals; Non-Access-Stratum protocol for Evolved Packet System; Release 14," *3GPP TS 24.301 V14.2.0 (2016-12)*.

[20] "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Requirements for support of radio resource management (Release 14)," *3GPP TS 36.133 V14.1.0 (2016-09)*.

[21] OpenLTE: an open source implementation of the 3gpp LTE specifications. [Online]. Available: http://openlte.sourceforge.net

[22] OpenBTS: A Platform for Innovation. [Online]. Available: http://openbts.org/

[23] I. Gomez-Miguelez, A. Garcia-Saavedra, P. D. Sutton, P. Serrano, C. Cano, and D. J. Leith, "srslte: an open-source platform for lte evolution and experimentation," in *Proceedings of the Tenth ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation, and Characterization*. ACM, 2016, pp. 25–32.

[24] OpenAirInterface: 5G software alliance for democratising wireless innovation. [Online]. Available: http://www.openairinterface.org/

[25] Motorola Moto G5 Plus. [Online]. Available: https://www.motorola.com/us/products/moto-g-plus

[26] D. F. Kune, J. Koelndorfer, N. Hopper, and Y. Kim, "Location leaks on the GSM Air Interface," *ISOC NDSS*, February 2012.

[27] "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architectural requirements (Release 15)," *3GPP TS 23.221 V15.0 (2017-09)*.

[28] "3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) procedures in idle mode (Release 14)," *3GPP TS 36.304 V14.2.0 (2017-03)*.

[29] A. Dmitrienko, C. Liebchen, C. Rossow, and A.-R. Sadeghi, "Security analysis of mobile two-factor authentication schemes." *Intel Technology Journal*, vol. 18, no. 4, 2014.

[30] V. Prevelakis and D. Spinellis, "The athens affair," *IEEE Spectrum*, vol. 44, pp. 26–33, July 2007.

[31] "Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021," *White Paper, Cisco Public Information*, 2017.

[32] A. Filippoupolitis, G. Gorbil, and E. Gelenbe, "Spatial Computers for Emergency Support," *Comput J*, vol. 56, pp. 1399–1416, 2013.

[33] M. yun Park, Won-yong, K. Wan-soon, Park, E. Park, B.-G. Moon, and S. gon Kwon, "A Study on Development of Interactive Smart Network(IoT)-based Subway Platform Disaster Response System," *Journal of Korean Society of Disaster and Security*, vol. 9, pp. 19–24, 2016.

[34] N. Virvilis and D. Gritzalis, "The big four - what we did wrong in advanced persistent threat detection?" *Eighth International Conference on Availability, Reliability and Security (ARES)*, September 2013.

[35] R. Heickerö, "Cyber espionage and illegitimate information retrieval," *International Journal of Cyber Warfare and Terrorism (IJCWT)*, vol. 6, no. 1, pp. 13–23, September 2016.

[36] E. Gelenb, G. Gorbil, D. Tzovaras, S. Liebergeld, D. Garcia, M. Baltatu, and G. Lyberopoulos, "Security for smart mobile networks: The NEMESYS approach," in *International Conference on Privacy and Security in Mobile Systems (PRISMS)* , June 2013.

[37] M. Ramadan, G. Du, F. Li, and C. Xu, "A survey of public key infrastructure-based security for mobile communication systems," *Symmetry*, vol. 8, no. 9, pp. 85–102, 2016.

[38] Y. C. Hu, M. Patel, D. Sabella, N. Sprecher, and V. Young, "Mobile edge computing: A key technology towards 5g," *ETSI White Paper*, vol. 11, no. 11, pp. 1–16, 2015.