New vulnerabilities in 4G and 5G cellular access network protocols : exposing device capabilities

Altaf Shaik
Technische Universität Berlin
altaf329@sect.tu-berlin.de

Ravishankar Borgaonkar
SINTEF Digital
ravi.borgaonkar@sintef.no

Shinjo Park
Technische Universität Berlin
pshinjo@sect.tu-berlin.de

Jean-Pierre Seifert
Technische Universität Berlin
jpseifert@sect.tu-berlin.de

ABSTRACT

Cellular devices support various technical features and services for 2G, 3G, 4G and upcoming 5G networks. For example, these technical features contain physical layer throughput categories, radio protocol information, security algorithm, carrier aggregation bands and type of services such as GSM-R, Voice over LTE etc. In the cellular security standardisation context, these technical features and network services termed as *device capabilities* and exchanged with the network during the device registration phase. In this paper, we study *device capabilities* information specified for 4G and 5G devices and their role in establishing security association between the device and network. Our research results reveal that *device capabilities* are exchanged with the network before the authentication stage without any protection and not verified by the network. Consequently, we present three novel classes of attacks exploiting unprotected *device capabilities* information in 4G and upcoming 5G networks – identification attacks, bidding down attacks, and battery drain attacks against cellular devices. We implement proof-of-concept attacks using low-cost hardware and software setup to evaluate their impact against commercially available 4G devices and networks. We reported identified vulnerabilities to the relevant standardisation bodies and provide countermeasure to mitigate *device capabilities* attacks in 4G and upcoming 5G networks.

ACM Reference Format:
Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2019. New vulnerabilities in 4G and 5G cellular access network protocols : exposing device capabilities. In *12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '19), May 15–17, 2019, Miami, FL, USA.* ACM, New York, NY, USA, 12 pages. https://doi.org/10.1145/3317549.3319728

1 INTRODUCTION

As mobile network generations advance, new technologies and innovative applications come into existence. From tiny low-powered sensors to vehicular networks everything can be now controlled and managed via mobile networks. Current fourth generation and fifth generation networks in short 4G (also called Long Term Evolution (LTE)) and 5G respectively, are built to support a wide range of applications including smart homes, critical infrastructure, industry processes, HD media delivery, automated cars, and etc. Besides, low-cost and low-energy mobile devices referred as Narrow Band - Internet of Things (NB-IoT) and and LTE - Machine type communications (LTE-M)[1] are redefining the IoT market with a brand new LTE protocol suite tailored for IoT applications.

The standard body 3rd Generation Partnership project (3GPP) has designed several capabilities in 4G and 5G specifications to address these applications and control them via mobile networks. These capabilities are communicated to the network by mobile devices during the registration process. The device capabilities play an essential role in defining the communication model between the device and the network. For instance, they define the speed, frequency bands, security parameters, application specific parameters such as telephony capabilities of the device. This allows the network to recognise the application type and accordingly offer the appropriate service. For example, a automated car indicates its Vehicle-2-Vehicle (V2V) support to the network and receives the required parameters to establish communication with surrounding vehicles. Similarly, high end smartphones indicate their support for carrier aggregation and Multiple-Input and Multiple-Output (MIMO) techniques to receive high data rates from the network. Also, low-powered and light weight IoT devices indicate their support for power consumption techniques and accordingly activate them after negotiating with the network. Hence, capability information of device plays an essential role for the right operation of the device with respect to its application.

In this paper, we analyse device capabilities specified in 4G and 5G network standards with respect to security aspects. Our research study reveals that device capability information is exchanged with the network without any protection during the device registration phase. Consequently, the device capability information can be misused by an adversary to perform several attacks against the mobile subscriber. We present three classes of attacks – **a) Identification attacks** allow an adversary to discover devices on the mobile network and reveal their hardware and software characteristics (such as model, manufacturer, version) and applications running on them; **b) Bidding down attacks** that hijack the device capabilities exposed on the LTE air-interface and degrade the data-rate of a device from 27 Mbps to 3.7 Mbps and further deny Voice Over LTE

[1] LTE-M is the term for the LTE-MTC low power wide area (LPWA) technology standard published by 3GPP in the Release 13 specification.

WiSec '19, May 15–17, 2019, Miami, FL, USA

ACM ISBN 978-1-4503-6726-4/19/05…$15.00
https://doi.org/10.1145/3317549.3319728

(VoLTE) services to LTE subscribers and downgrade them to 3G/2G networks; **c) Battery draining attacks** that target NB-IoT and LTE-M devices to breakdown their power saving abilities and drain their battery life 5 times faster than the expected lifetime.

We have implemented all our attacks and tested them using commercial LTE devices and also on real LTE networks. As the vulnerabilities we identified are present in the 3GPP standards, all the devices supporting LTE (and upcoming 5G as well) standards are affected. Moreover our attacks are silent and persistent for several days and fortunately require minor fixes to mitigate them.

Our research results are reported to the cellular standardisation bodies (SA3), network operators and remedial actions are underway. We hope to see changes to the 3GPP 5G specifications to address the shortcomings we outlined in this paper. Our contributions in this paper are the following:

- A new vulnerability in the LTE and 5G specifications that enables device identification attacks. As a consequence of this specification vulnerability, an implementation vulnerability is found in network operator equipment that is exploited during LTE device registration procedure. Further, a protocol vulnerability in the first release of LTE NB-IoT protocols that compromises the battery life of low-powered devices.
- A low cost experimental setup built using off-the-shelf hardware and openly available software. Implementation of various proof-of-concept attacks and their evaluation using commercial devices and cellular networks.
- Countermeasures to mitigate the attacks that can be included into 4G protocols and also as recommendations to the ongoing second phase 5G security standard design.

2 BACKGROUND

We first present different type of capabilities defined for mobile devices and then discuss the standardized registration procedure as defined by the 3GPP. Next, we introduce cellular IoT devices and their operate in LTE networks. In 3GPP terminology a mobile device, a base station and a core network are referred to as User Equipment (UE), evolved NodeB (eNodeB) and Mobility Management Entity (MME) respectively. A UE (phone, router, or IoT gateway, etc) with a valid SIM card can register to a mobile network and receive access to call/data services. A eNodeB is responsible for the radio transmission and reception with the UEs and a MME handles administrative tasks such as the authentication, security and management of the subscribers. Hereafter we refer to a device as a UE.

2.1 UE Capabilities

A UE supports several capabilities for various LTE services and operations. They are classified into core network capabilities [9, 15] and radio access capabilities [6, 8] and are exercised by the MME and the eNodeB respectively. The core network capabilities contain non-radio related capabilities, e.g. security algorithms, telephony features and etc whereas radio access capabilities provide radio aspects of the UE, such as supported frequency bands, receive and transmit capabilities and etc. Further, a UE can support various radio access technologies such as LTE, 3G, 2G, and CDMA and reports its capabilities to the network during the registration procedure.

2.2 LTE Registration

A typical registration procedure in LTE network is performed using control plane messages as shown in Figure 1. To begin, upon turning ON, a UE sends an *attach request* message to the MME indicating its request for voice/data services or both. It primarily consists of subscriber identities such as *International Mobile Subscriber Identity* (IMSI) or *Temporary Mobile Subscriber Identity* (TMSI) and UE's core network capabilities. Since *Attach Request* is a first message to the network it is sent in plaintext. Upon identifying the subscriber, both UE and network perform mutual authentication and establish the first level of security. In particular, Non-Access Stratum (NAS) security is established between the UE and the MME to enable encryption and integrity protection of the messages hereafter exchanged between them.

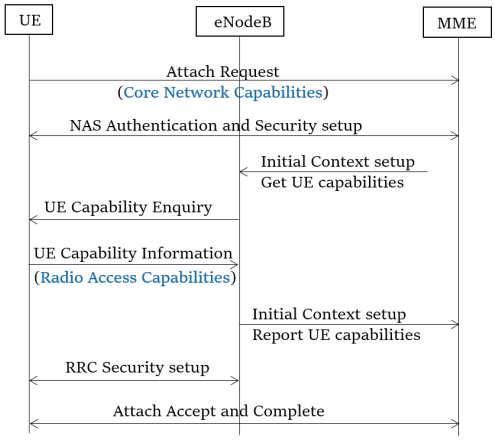

Figure 1: LTE Registration Procedure

Next, the MME instructs the eNodeB to fetch UE's radio access capabilities. Thus upon receiving a *UE Capability Enquiry* message from eNodeB, UE transfers the requested radio access capabilities using *UE Capability Information* message. eNodeB forwards these capabilities to MME and are stored there until the UE de-registers from the network. Further, eNodeB and UE establish a second level of security called Radio Resource Control (RRC) security. Hereafter the messages exchange between UE and eNodeB are encrypted and integrity-protected. In the coming sections we highlight that the sequence of radio access capability transaction and the RRC security setup varies among operators. Following this, the registration is successfully completed when the UE receives an *Attach Accept* message. Now the UE can utilize voice and data services offered by the network.

LTE network deployments divide a geographical location into Tracking Areas (TAs) and each TA is assigned with an identifier called TA Code (TAC). While moving from one TA to other, a registered UE should perform a Tracking Area Update (TAU) procedure in order to update its current location to the network. UE initiates this procedure by sending a *TAU Request* message to MME and its contents are similar to *Attach request* message. Next, UE, eNodeB and MME follow a similar procedure like in Figure 1 and complete the update procedure with a *TAU Accept* message. Note that UE reports its core network capabilities during the TAU procedure. A

similar update procedure known as periodic TAU is also performed (even though UE did not change its location) by the UE upon the expiry of a timer *T3412*. *T3412* is sent to the UE in *Attach Accept* and *TAU Accept* messages.

2.3 Cellular IoT UEs

Two new categories of UEs known as NB-IoT and LTE-M are defined by the 3GPP in LTE Release 13 specifications to support low-powered, battery constrained IoT devices in mobile networks. An optimized registration procedure is defined for these categories in which these UEs are required to establish only the NAS level of security and eliminate RRC security setup. Moreover, data transmission is facilitated using secure NAS control plane messages [15].

3 VULNERABILITIES AND THREAT MODEL

This section uncovers the vulnerabilities we discovered LTE protocols and implementations. First, we present a threat model and discuss the vulnerabilities. Next, we build an experimental setup to exploit the vulnerabilities using commercial devices and networks.

3.1 Threat Model

We define a threat model and characterize two type of adversaries: passive and active. Both have the knowledge of LTE protocols, and access to software and hardware elements required to listen and decode LTE control channel messages over the air-interface. Additionally the active one has the capability to mount a rogue LTE network in two ways. The first type of active adversary can operate a rogue eNodeB and exchange LTE control plane messages with the victim UE(s). The second type of active adversary can act as a Man in the Middle (MitM) and relay the traffic between a victim UE and a legitimate network, and can further modify/inject information into the unencrypted LTE control plane messages.

3.2 Vulnerabilities

We identified three vulnerabilities in the LTE registration procedure. They exploit the UE capabilities sent to the network during registration or TAU procedures and are described as follows.

- (V1) First, both core network and radio access capabilities can be acquired from a UE without establishing authentication [6, 15]. This allows an active or passive adversary to obtain all the capabilities of a UE. We exploit this vulnerability and demonstrate device type identification attacks in section 4.

- (V2) Second, mobile network operators are requesting the radio access capabilities from the UE prior to the RRC security setup as shown in Figure 1. As a result, UE capabilities are transferred in plaintext and an adversary can hijack these capabilities. We study the threats resulting from this vulnerable operation and demonstrate device bidding down attacks in section 5.

- (V3) Third, *Attach Request* message is always sent unencrypted by the UE to the network [15], but it can be integrity protected in case of an existing NAS security context in the UE. However, the registration process is not interrupted even if the integrity verification fails at the MME. In such a case the content of the *Attach Request* message is vulnerable to injection or modification attacks. In particular, the core network capabilities inside this message can be hijacked by an adversary. We discovered that modifying certain core network capabilities can cause power drain attacks on NB-IoT devices and are demonstrated in section 6.

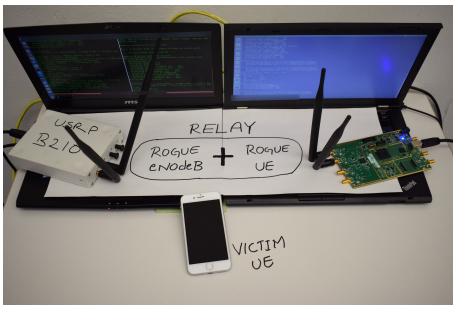

Figure 2: Experimental setup

3.3 Experimental Setup

We build an experimental setup as shown in Figure 2 to demonstrate and validate our attacks. Our hardware elements consist of two host i7 PCs using Linux OS and two radio modules made of Universal Software Radio Peripheral B210 [18]. B210 is a software defined radio that is controlled by a host-based software via a USB3 port to perform transmit and receive operations. Next, our software elements are created using the open source project srsLTE [38]. Precisely, we leverage srsUE software and srseNB to operate as a UE and eNodeB respectively. Further, we used a testbed offered by a vendor to perform NB-IoT experiments. On this testbed, we have access to configure, modify and visualize LTE control plane messages. For confidentiality reasons we do not exhibit this testbed in this paper. As highlighted in Figure 2 the software is executed on the host PC which controls the B210 to transmit and receive LTE signals. To perform our attacks we design and operate a rogue eNodeB and a relay which are detailed below.

Rogue eNodeB Operation. A rogue eNodeB impersonates a real eNodeB by spoofing the frequency and network codes of a real network operator. Further, to attract UEs in the operating region, we use a TAC that is different from the current TA. Most importantly, we surpass a legitimate eNodeB by transmitting relatively higher power to automatically receive a *TAU Request* message from the UEs. To achieve this we modified the srseNB software and present a rogue network to the UE. Our rogue eNodeB in Figure 2 exchanges LTE control plane messages with the UE and naively redirects them to a legitimate network after the attack.

Relay Operation. A relay consists of a rogue UE and a rogue NodeB. The configuration of the rogue eNodeB is similar to the eNodeB discussed above and further it is directly connected to the rogue UE (on a different host) that relays the traffic between the victim UE and the legitimate network. We followed a similar approach like in [32] to maintain a stable connection between legitimate UE and the network. However, we used a frequency number for the

operation of rouge eNodeB different from the legitimate operator and hence avoiding our rogue UE connecting to our own rogue eNodeB. For the setup in Figure 2, we use the modified srseNB (like above) and a modified srsUE to receive and relay the control plane messages (RRC and NAS) between legitimate network and victim UE. Our major modifications involve the integration of srsUE and srseNB segments. Moreover, we used directional antennas and power amplifiers to improve the signal conditions between rogue UE and legitimate network. Similar to this relay setup we have a UE segment and eNodeB segment in our NB-IoT testbed and also refer to them as a relay in our experiments.

Note: We performed all the experiments using our test phones and extreme care is taken not to interfere with nearby communications. Further, we have legitimate permissions from an operator to transmit in one of their commercial LTE frequencies.

4 DEVICE-TYPE IDENTIFICATION

This section presents techniques to identify the type of devices on a mobile network and intellectually estimate the underlying applications. We start by understanding UE capabilities and their usage in commercial devices and applications. Next, we discuss our reference model using a set of known devices and techniques to distinguish various devices and applications. Lastly, we use our reference model to perform Mobile Network Mapping (MNmap) attack and discuss the impacts of such an attack.

4.1 Understanding UE Capabilities

The term device-type in our work represents device specifics such as the combination of the maker, model, software and the application(s) on the device. The manufacturing of cellular-enabled devices involves multiple entities: a baseband vendor producing the modem, a device manufacturer integrating the modem with other components such as sensors or displays, and an application developer providing lightweight firmware or full-stack operating system. Baseband vendors define UE capabilities according to the 3GPP standards [6] and make them adjustable for device manufacturers and application providers according to their specifications and requirements. Due to a large number of optional capabilities (several hundred), each baseband manufacturer may implement a subset of the whole capabilities in a distinct way. Similarly, device and application providers can also adjust the UE capabilities. Based on these distinct implementations, we discovered that it is possible to identify a device-type and its corresponding application.

Each target application requires different UE capabilities. For example, a mobile phone requires telephony capability. A tracking device requires persistent GPS access, while telephony is not always required. Cars require multiple capabilities: GPS for navigation, V2X for self-driving car [13]. All these capabilities are defined in the modem and are enabled/disabled according to the target application. Thus, there is a direct correlation between a UE capability and a target application. We now continue to analyze the UE capabilities (both core and radio) and create a reference model that enables us to identify the device-type details of any cellular-enabled device.

4.2 Reference Model

Device identification is based on the differential analysis of the capabilities that are obtained from a UE. Initially we perform dedicated experiments to learn the ground truth information about device-types and create a reference model from it. This reference model is a huge database of capabilities and techniques to identify device-types. We used 40 devices for our experiment including mobile phones, cars, tablets, routers, USB data sticks, e-bikes, cellular IoT devices like trackers, and coffee machine (detailed list in Table 3). Device-types are then systematically identified based on a tree-based model shown in Figure 3 consisting of four levels (marked in different colors). The first level identifies the baseband vendor and the model of the device and the second level differentiates cellular and cellular IoT devices. The third level determines the device's application and the fourth level identifies the device manufacturer and application provider.

By using our eNodeB setup, we acquire both the core network and radio access capabilities from the test devices and analyze them. In particular, UE initiate a registration process with our eNodeB and we extract the capabilities from the *Attach Request* and *UE Capability Information* messages. We then compare the implementation differences of specific capabilities listed in Appendix B to identify the right baseband vendor and model. Further, we investigate the presence/absence of one or more capabilities listed in table Appendix C, Appendix D and Appendix E to determine the right device level and further deduce the device-type details. We define each of the levels and corresponding identification techniques as follows:

Baseband Vendor Name and Model. We primarily identify the baseband vendor and model of the UE. As the number of active baseband vendors are limited, we can distinguish them using a few implementation differences in the capabilities. We consider the following popular baseband vendors with a significant market share: Qualcomm, Samsung, MediaTek, Intel and Huawei. We discovered a set of capabilities as shown in table Appendix B that are (de)activated in each of these basebands and allow us to identify the vendor. For instance, Qualcomm based UEs by default do not support the NULL integrity algorithm EIA0 [11]. EIA0 is particularly used for emergency calling and Qualcomm baseband dynamically activates it, unlike other vendors. Hence any UE lacking the support for EIA0 can be considered as a Qualcomm baseband. Similarly, Huawei basebands support all the listed capabilities. Further, Samsung, Intel, and MediaTek can be differentiated based on the combination of other capabilities.

Next, every baseband model is designed to support a particular LTE specification release and a corresponding set of capabilities. By referring and comparing a baseband model to our reference model, the model name (or number) of the baseband can be determined. For e.g., release 9 specifications support only LTE technology whereas 10 specifications support LTE-advanced features. Hence in the case of Qualcomm the former is found in MDM9615 baseband model and the latter in MDM9625 (or higher) models. Upon revealing the model, the corresponding list of devices using this baseband model can be obtained from various sources on the internet such as GSMArena [2] and WikiDevi [3]. This information is later used in other levels as assistance to identify the device manufacturer and

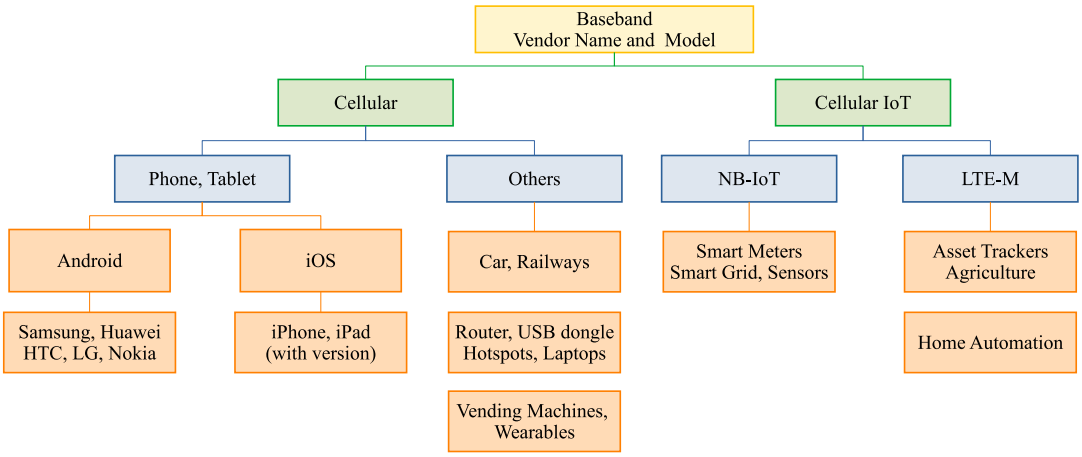

Figure 3: Device type identification levels

also the application.

Cellular vs Cellular IoT. 3GPP defines various UE Categories (Cat) depending on their LTE specifications and the supporting technical capabilities [8], between 0 and 19. Further, NB-IoT and LTE-M are different categories and features defined especially for IoT applications. These categories do not support voice calling features and instead support power saving features. As shown in table Appendix C, timers *T3324* and *T3412 ext* are included in *Attach Request* message to indicate power saving features [15]. Hence when these timers are active we can accurately make a decision at level two that they are a certain type of cellular IoT devices.

Phone vs Others. The primary use of a mobile phone is to make voice calls, therefore voice capability is activated by default. In contrast, there are cellular modems dedicated to data-only purposes without voice calls, hence we categorize them as "others". These include data sticks, cars, hotspots, wearables like watches, and etc. The device capabilities in table Appendix D clearly distinguish UEs that are phones from all other UEs that are not phones. Unlike "others", a phone indicates its *UE Usage Setting*, *Voice Domain Preferences* and *voice codec* support to the network and activates voice calling capabilities. iPhone models can be distinguished based on the specification release and also UE category whereas we have a different approach to distinguish various android manufacturers.

A UE fixed in a car requires GPS features to be constantly turned ON. Further, in LTE and 5G networks, UE capabilities indicate V2X or V2V support. When such a capability is detected it can be referred to as a vehicle. A railway specific modem has special features that support frequencies dedicated to railways such as GSM-R [20]. Differently, USB dongles and routers (also hotspots) are purely data-oriented and lacks any voice codec facilities. These distinct capabilities can distinguish different devices at level 3.

NB-IoT vs LTE-M. While both NB-IoT and LTE-M are targeting low-powered IoT applications with 10 years of battery life [7, 22], they have different operational aspects. NB-IoT uses different radio channels compared to LTE-M and hence easily distinguishable from each other. The separation of these two categories assists in identifying the underlying IoT application.

Android vs iOS. iPhones have constantly been using basebands from either Qualcomm or Intel. Thus, devices using other basebands are not considered as an iOS device. Although an Android devices can use Qualcomm or Intel baseband, we noticed multiple differences between Android and iOS devices with the same baseband as shown in tableAppendix E. *MS assisted GPS* is a capability that we found disabled in all tested iPhone models but whereas it is always enable across android models using Qualcomm and Intel baseband. Note that we did not consider phones with other operating systems such as Windows and Firefox due to their low market share.

Android Device Manufacturers. Based on our analysis Android device manufacturers have certain preferences in choosing their basebands. Huawei and Samsung basebands are exclusively used in-house. Other manufacturers such as LG, Nokia, HTC use basebands from multiple vendors such as MediaTek, Qualcomm and Intel. Hence, by referring to the device list [2, 3] it is possible to narrow down the possible options and determine the right phone manufacturer.

Application. Cellular types devices are multi-purpose devices with moderate to high computing capabilities and can be identified based on above techniques. For example, upon detecting a router its operating system can be inferred from various internet sources. In contrast, cellular IoT type devices have less computing power and are dedicated to single application usage. LTE-M provides better latency than NB-IoT, making it suitable for mission-critical applications such as those involving emergency data and precision tracking data. A wide range of applications and the appropriate category is defined in [22] as a recommendation to the device manufacturers. Similarly, the application can be inferred based on the requested

timer values. A UE can request lower *T3412* values such as 15 seconds or less to save more power. This could be translated to a device or a sensor like smart-meter that only pushes data to a server and do not expect any responses. Differently, a vending machine or an asset trackers require up to 1 minute active state depending on the requirements. However, this heavily depends on the settings of the application. Some device may use the default value supplied by the baseband manufacturer, which may not be optimal for their specific use case.

4.3 Mobile Network Mapping (MNmap)

The primary goal of this attack is to identify devices on a mobile network by analyzing their capabilities. Since a UE transfers its capabilities to the network without performing authentication [6], an active adversary can acquire these capabilities (both core and radio) by operating a rogue eNodeB as described in our setup. Besides, a passive adversary can also acquire UE's core network capabilities but not the radio capabilities (provided they are exchanged after RRC security setup). In this section we perform the attack being an active adversary as we require both core and radio capabilities to perform a granular identification. We perform an experiment with an unknown UE and apply our reference model to determine its device-type. Upon receiving a *TAU Request* message from the UE, we extract the core network capabilities and send a *UE Capability Enquiry* message. The UE responds with a *UE Capability Information* message and we extract the radio capabilities from it and release the UE to a legitimate network using a *RRC Release* message.

In our experiment, an unknown device was identified to use Intel XMM7480 baseband based on our model, due to its Cat 6 support. It is determined as a phone/tablet since the device has voice support (ref table) and reports itself as a voice centric device. By searching the smartphones and tablets with Intel XMM7480 baseband, we could identify that this is an iPhone 8.

The secondary goal of this attack is to determine potential vulnerabilities applicable to the identified device. Precisely, MNmap can be supplemented with vulnerability information from the external sources such as vulnerability databases from baseband vendors (Huawei [25], Qualcomm [29]), OS developers (Google [19], Apple [16]) and device manufacturers (Samsung [33]) and perform targeted attacks. Further, these device fingerprints can be combined with the permanent identifier IMSI to track subscribers. While 5G prohibited the plaintext transmission of IMSI in any situation [12, 14], fingerprinting of a device and user is still possible when the device-type information is unique among the nearby devices.

4.4 Evaluation and Challenges

While we only consider 5 major baseband manufacturers, our reference model is also expandable to other baseband manufacturers. Identifying the baseband vendor and chipset model is a biggest achievement and can be easily accomplished with the set of parameters we mentioned in the appendix. We evaluate our fingerprinting techniques with 10 other unknown UEs and could successfully determine their type up to the fourth level. These 10 devices are similar to the devices registered in our reference model. The MNmap depends on the reference model and publicly available databases to infer the device-type information. Hence a bigger and diverse reference model is required for an accurate device-type identification.

Phones, tablets, routers and automotive devices are easily identified using our reference model whereas determining the application of cellular IoT device is challenging due to its limited set of capabilities and similarities among several applications. Another challenge is to determine the application OS version since the baseband model and mobile OS versions are not linked and not synchronously updated. Besides, in certain UEs (especially phones) a USIM card can activate/deactivate certain capabilities. For e.g., frequency bands are enabled and disabled according to certain settings by the network operator. Hence, identification is affected by the USIM card setting and should be considered during MNmap attack.

5 DEVICE BIDDING DOWN

This section presents a bidding down attack performed on a UE by hijacking its capabilities. We first discuss the capabilities that are exploited and followed by an experimental attack and its evaluation on commercial networks. We finally present the feasibility and impact related issues of this attack.

5.1 LTE Radio Access Capabilities

A UE communicates its radio access capabilities [6] with the eNodeB and indicate its support for specific radio operations. A eNodeB needs to respect the received UE radio access capabilities when configuring and scheduling data/signaling for the UE [8, 26]. We now explain these capabilities that are exploited in our attacks along with their usage in LTE network.

UE Category. It is used to set the number of bits allocated by the eNodeB over the radio channels for a UE in both downlink and uplink transmissions [8]. The higher the category the higher the number of bits allocated. This directly translates to the data rate of the UE over the air-interface. For instance, theoretically, a Cat 6 UE is entitled to receive a maximum of 300 Mbps speed on the downlink whereas a Cat 1 UE has a peak of 10 Mbps.

Carrier Aggregation (CA) and Multi Input and Multi Output (MIMO). To boost the capacity of the network and offer higher bit rates, 3GPP introduced CA and MIMO technologies. Both CA and MIMO increases the bitrate, but CA increases the bandwidth while MIMO uses multi-antenna techniques. A UE supporting these technologies is entitled to receive higher bit rate provided that the network also supports it.

Bands. Bands refer to a set of radio frequencies supported by the UE. Support of multiple bands are required for inter-frequency handovers and facilitates international roaming across multiple regions. Most commercial UEs will normally support multiple frequency bands depending on the region they are sold. For instance, band 3, 7 and 20 are operated in Europe whereas band 2, 4 and 12 are widely used in the North America.

Voice Over LTE (VoLTE). As LTE is an all-IP network, the standard procedure for making voice calls is using Voice over LTE

(VoLTE) technology. The mandatory radio access capabilities required [21] to support VoLTE are Robust Header Compression (RoHC), Unacknowledge Mode (UM), Semi-Persistent Scheduling (SPS), and Transmission Time Interval (TTI) bundling. A UE that is not supporting these capabilities is not entitled to receive VoLTE operations but instead use the traditional circuit switched (2G/3G) approach to making voice calls.

5.2 Capability Hijacking

We perform a MitM attack using our experimental setup to hijack the radio access capabilities of a UE during its registration procedure. Due to the mobile network operators configuration or vendor implementations the eNodeB requests UE's radio access capabilities prior to RRC security setup. This allows a MitM adversary to alter the *UE Capability Information* sent by the UE. To exploit this vulnerability on a commercial network we use an iPhone 8 as a victim UE in our experiment. It is a Cat 12 device and houses an Intel XMM7480 baseband and can boost speeds upto 600 Mbps and further also support CA, MIMO and several LTE bands. The flow of the attack is pictured in Figure 4. To trigger the attack, our relay is configured with a TAC that is different from the iPhone 8's current registration area. This will lure it to initiate a TAU procedure, which is rejected by the relay with a *TAU Reject* message. As a result, this will delete the current security context and other temporary identities in the iPhone 8 and initiate a new registration procedure by sending an *Attach Request* message to our relay.

We simply forward this message to the legitimate network using our rogue UE segment and allow the iPhone 8 to successfully finish the NAS security setup. Since this is a new registration and not a TAU procedure, MME requests the eNodeB to acquire UE capabilities. Our relay forwards the *UE Capability Enquiry* message received from legitimate eNodeB to iPhone 8 and retrieves the capabilities in the *UE capability Information* message in a plain-text format. Upon receiving them we alter these capabilities in the following way: UE Category is changed from Cat 12 to Cat 1, CA and MIMO are disabled, VoLTE required capabilities are disabled and all the supported bands are disabled except the current operational band. Next, we forward the modified *UE Capability Information* message to the legitimate network and allow the iPhone 8 to successfully establish RRC security and complete the registration procedure with *Attach Accept* being delivered to iPhone 8. Subsequently, we release the UE to the legitimate network using a *RRC release* message. Note that eNodeB forwards these (modified) capabilities to MME which are then stored for future transactions i.e., when UE reconnects to the eNodeB to send/receive data, the capabilities are transferred from MME to eNodeB without repeating the UE capability transaction procedure.

Hereafter when the iPhone 8 connects to any legitimate eNodeB, it is treated as a Cat 1 device and receives downlink data rate according to what a Cat 1 device is entitled to receive [8]. Thus the e iPhone 8's speed and quality of service are downgraded after this attack. Further, during a voice call operation, due to lack of 4G band support iPhone 8 is handed over to a 3G base station for call continuity. As a result, the UE will lose access to certain services and also cannot receive the elite QoS and data rate as originally allocated to the subscriber (based on USIM data plan). We discuss more on our experiments and evaluation with different UEs in the next subsection.

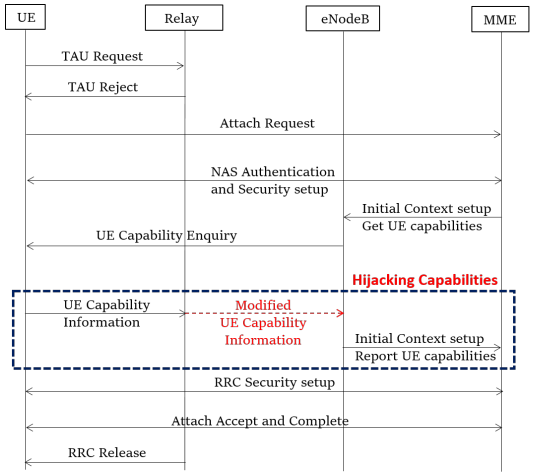

Figure 4: MITM Capability Hijacking attack

5.3 Experiments and Evaluation

In normal conditions, the iPhone 8 offers a data rate (with an elite USIM plan) of 27 Mbps on the downlink Under the attack, the data rate of the iPhone 8 as measured using Speedtest [1] reduced to 3.7 Mbps. We tested this on two commercial networks and discovered that maximum speed we received is 5 Mbps. We repeated the experiments with other Gigabyte LTE Cat 16 devices that can boost up to 1 Gbps speeds: a Nighthawk M1 Mobile router [4] and Samsung Galaxy S8 phone. During our tests, although a Cat 16 device supports a theoretical downlink speed of 1 Gbps, we observe 35 to 38 Mbps in practice during low-traffic hours (after 21:00). However, after the attack the downlink speed is reduced to 2.9 Mbps. Differently, in peak hours (10:00) the speed is further reduced to 1 Mbps. Although our test SIM is entitled to receive high quality of service and data rate, the bottleneck persists at the radio layer. Hence, when a UE's radio cannot support higher speed, having an elite subscriber profile is useless.

5.4 Feasibility and Impact

The attack is practically feasible due to the following reasons. As per the standard [6] UE's radio access capabilities can be requested without establishing security and is reflected in the operator's network configurations. Furthermore, we recorded registration procedure traces of 30 network operators from 20 countries worldwide. We discovered that 20 out of 30 operators are affected with the vulnerability V2, i.e., UE's radio access capabilities are requested prior to RRC security. Hence, an adversary can perform a MitM attack on these networks and downgrade subscriber's services. However, the remaining 10 networks perform RRC security prior to the UE capability transaction procedure i.e., the radio access capabilities are transferred in a encrypted and integrity protected message. As a result, any MitM operation will be detected on the eNodeB and aborted.

The attack is silent since neither the UE nor the eNodeB can detect the modification of the radio access capabilities. It is also persistent because these capabilities received during the registration procedure are stored at the MME for a configured period of time (until UE is turned off as observed). During this period, the altered radio access capabilities are used to configure the data rate and services for the UE. We also observed that the majority of the networks do not request UE's radio access capabilities during periodic TAU or normal TAU procedures in order to preserve radio resources because the size of these capabilities accounts to 8188 octets [10] and is the longest radio message. Further, our experiments with a UE that is registered and roaming inside a city, the network did not request radio access capabilities for a week which means that the MME retained UE capabilities for several days. Besides, we also observed that the some networks repeatedly ask only for UE's 3G radio access capabilities when UE performs data transmission [5]. Hence, the UE's LTE capabilities are retained at the network for a longer period and also the UE remains affected even if the attacker deactivates the relay.

- Data rate of the UE is adversely affected and depends on the UE category chosen by the MitM adversary. UE's speed cannot be upscaled by the attack since there is a maximum data rate supported by each category but not a minimum.
- By removing VoLTE capabilities, if UE or network does not support 2G/3G technologies, calls will be denied to UE.
- UE will be handed over to 3G/2G base station in case UE is moving and does not support operated bands in that region. A downgrade to lower generations of network will make UE vulnerable to more attacks.
- UE should to be restarted and/or re-registered to recover from the attack. A subscriber affected with the attack would potentially launch a complaint with the customer service or switch to another operator.
- Future technologies such as V2V and other industrial vehicles that require low latencies are severely affected with poor speeds and low quality of service. Further, by disabling V2V capabilities UE is completely denied of those services.

6 DEVICE POWER DRAIN

We first understand the power saving features defined for IoT devices and then exploit the vulnerability V3 in the registration procedure of NB-IoT and LTE-M UEs. Next, we perform a power drain attack on them and study the related feasibility and impact issues.

6.1 Power Saving Feature in LTE

Certain IoT devices are deployed only to send/receive small amounts of data intermittently and are basically battery-operated. Hence, to significantly lower power consumption in such devices the 3GPP introduced Power Saving Mode (PSM) into LTE specifications in 2015 [15]. PSM is a state where UE is powered-OFF, but still remains registered with the network. Precisely, the 3GPP indicates to turn off the baseband and thus the radio operations but however, applications (or sensors) can still operate depending on the device settings. A UE can request the use of PSM by including a timer *T3324* in the *Attach* or *TAU Request* messages. *T3324* defines the time period that the UE stays active before entering into PSM. During this active state UE monitors the eNodeB channels for incoming messages from the network.

As per 3GPP and certain vendor documents [15, 17], network activates PSM only when the UE requests *T3324* in *Attach Request* or *TAU Request* messages and further if the network has PSM support. Similarly, a UE can activate PSM only if the network has provided the *T3324* value IE during the last registration procedure with a value different from "deactivated" [15]. Hence UE and network are equally responsible for the activation/deactivation of the PSM. Upon the expiry of *T3412* UE leaves PSM and initiates a periodic TAU procedure. Additionally an extended version of *T3412* called *T3412 ext* is defined to further lower power consumption, and can optionally be used with *T3324*. When *T3412 ext* is included, UE chooses it over *T3412* since the former can specify longer sleep durations. In this way a device that transmits once per day in PSM could last well over 10 years on 2 AA batteries [7].

6.2 Battery Draining

We drain the battery of low-powered NB-IoT devices by being a MitM on the LTE air-interface. To demonstrate this attack we mount our NB-IoT testbed as a MitM (relay) and Quectel BC68 Evaluation Kit [30] (referred as BC68 hereafter) as a victim UE. As BC68 is a development board we have access to its diagnostic ports and can monitor its LTE signalling messages and internal activity logs. In the attack, our relay modifies the contents of the *Attach Request* message as shown in Figure 5. In specific, the relay is configured in such a way that it lures the BC68 to trigger a TAU procedure. Upon receiving a *TAU Request* message, our relay acknowledges it with *TAU reject* message which causes the BC68 to delete its previously stored context and temporary identifiers and start a new registration by sending *Attach Request* message to our relay. Subsequently, our relay removes the *T3324* from the message and forwards it to the legitimate network without modifying any other contents. Further, as overseen by the relay both legitimate MME and BC68 perform authentication and establish NAS security. Finally, an *Attach Accept* message is delivered to BC68 and is released to the legitimate network. Note that the *Attach Accept* message does not contain *T3324* since, the MME did not receive it in the *Attach Request* message. Thus, BC68 cannot activate PSM and does not power OFF. Instead, it decodes broadcast messages from the eNodeB and perform cell measurement activities leading to power consumption. Besides, the network assigns *T3412 ext* to BC68 with a value of 310 hours which indicates that it should perform the next TAU procedure after approximately 13 days.

6.3 Feasibility and Impact

The vulnerability is present in the 3GPP LTE registration procedure defined especially to benefit the low-powered IoT devices. Hence all manufacturers implementing the LTE release 12 standards are affected with this vulnerability. The attack persists even when the attacker turns off the relay and holds until the *T3412* or (*T3412 ext*) expires in the UE. In our experiments we observed that certain networks implement 10 to 15 days as a periodic TAU timer. It can heavily vary depending on the subscription of the SIM, IoT application and configuration of the operator. To recover from

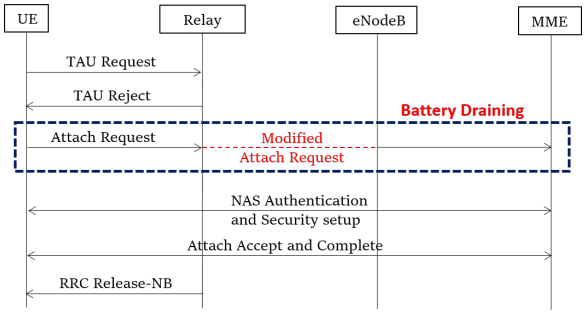

Figure 5: MitM Power drain attack on NB-IoT devices

the attack the UE should reconnect to the network and perform a registration procedure (or TAU) in the adversary's absence.

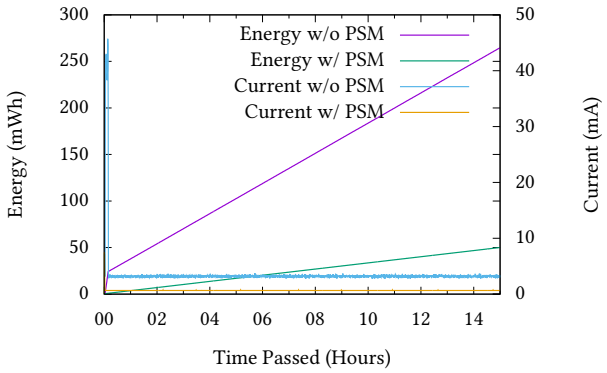

Figure 6: Current and power consumption of BC68 with and without PSM

During our experiments, in a scenario without the attacker, T3324 is configured to 30 seconds and T3412 ext to 13 days. Thus BC68 enters into PSM 30 seconds after it completes registration and performs a periodic TAU after 13 days. But, under the influence of the attack, UE is constantly ON for 13 days and performs periodic TAU after 13 days. We measured the current and power consumption of BC68 for several days with and without the attacker and plotted in the Figure 6. The initial peak of current drawn in both cases is caused by the initial registration with the network. Without PSM, BC68 performs power measurements of neighbouring cells which consumes power. This is reflected as constant fluctuations in the current consumption. In contrast, when PSM is active, the baseband is OFF and consumes almost negligible current.

3GPP [7] promises 10+ years of battery life for NB-IoT devices when powered with 5Wh battery. When we extrapolate our results for 5 Wh battery (assuming no losses), with PSM, BC68 consumed 0.65 mA of average current, making 1538 hours (64 days) to draw the whole power. In contrast, under the attack, BC68 consumed 3 mA of average current with 5 V input, making 333 hours (13 days) to draw the whole power. Hence, a power drain attack reduces the battery life by a factor of 5. Note that the total battery life decrease depends on other factors, such as sensors attached to it and how often the communication is performed. In our experiments with BC68, no sensors are attached and no messages were exchanged and all the current is explicitly used by the baseband.

7 DISCUSSION AND COUNTERMEASURES

An overview of the vulnerabilities, attacks and countermeasures is presented in Table 1. In this section we propose two countermeasures to prevent these attacks in LTE and 5G networks. Our solutions can be easily integrated into current LTE ecosystem and can be considered for future 5G networks.

Device Capability Protection. 3GPP should consider to mandate security protection for UE capabilities. In particular, *UE Capability Enquiry* message carrying radio access capabilities should be accessible/requested by the eNodeB only after establishing RRC security. This will prevent a MitM from hijacking those capabilities. Although changing current LTE standards is considered challenging and unappealing to the 3GPP body this mitigation can be considered in the ongoing second phase of 5G development. Even though if our fix is implemented into LTE standards, baseband vendors need longer periods to update their basebands and hence attackers can still exploit this vulnerability.

On the network operator side eNodeB configuration or implementation should be changed such that a eNodeB should request *UE Capability Information* only after establishing RRC security. This is a very easy fix and can be implemented by the operators either as a software update or a configurational change on their eNodeBs. Nevertheless, in practice only a minor number of operators are acquiring capabilities after security setup. The difference among various operators we tested clearly indicates that this could be either an implementation or configuration problem.

Besides, core network capabilities are accessible by both active and passive adversaries as they are sent in plain-text *Attach Request* message. Even if the radio access capabilities are protected as discussed above, an attacker could still perform MNmap attack. However, currently no specific protection exists for core network capabilities and hence their protection can be considered for future work.

Verification of Device Capabilities. We propose to provide protection for UE capabilities in addition to the UE security algorithms. Although a similar approach is mentioned in [35], we propose a customized approach that can be implemented with less effort. Along with the security algorithms, the capabilities such as timers and UE requested services should be sent back to the UE in an integrity protected *NAS Security Mode Command* message to confirm if they are the same capabilities that are originally sent by the UE. This will prevent any type of bidding down attacks and service downgrade. When a mismatch is found UE can renegotiate with the network with right services (assuming attacker is disabled). Recently, 3GPP has introduced a hash based mechanism into LTE release 14 specifications [11] that protects LTE core network capabilities but all the older release versions including NB-IoT are still vulnerable to our attacks. However, the radio capabilities are still at risk and we hope they will addressed in the upcoming 5G release.

Responsible Disclosure. We have reported our research to GSMA organization through their CVD programme. We also disclosed our vulnerabilities to 3GPP SA3 body and several affected operators worldwide. All the informed parties have successfully

acknowledged our findings and have initiated measures to prevent these attacks. We are currently in discussion with network operators to propose modifications to the upcoming 5G releases.

8 RELATED WORK

We study and discuss a set of wireless security research papers related to our work. We focus on three categories primarily – MitM, identification, and service availability.

A. MitM threats: Recent literature has witnessed several attacks targeting LTE subscribers privacy using rogue base stations. In [32] authors perform DNS hijacking attack on HTTP based DNS traffic. The cause for such an attack is due to lack of integrity protection for data traffic on LTE air-interface. Although our experimental setup is similar, our attacks do not involve any cryptanalysis and are easier to perform. Also, this problem is addressed and fixed in 5G networks hence they are not applicable to 5G networks. Whereas, the vulnerabilities we raised prevail in 5G phase 1 release and require immediate correction. MitM capability modification attacks are proposed in low-powered wireless networks. Capability exchange during Bluetooth pairing procedure is presented in [23, 24, 39] and LoRa has *spreading factor* which changes bit rate and power consumption [34], but unlike LTE it is static configuration. Besides, Sigfox [37] has a different security model where MitM is not feasible, and are not affected by this attack unless a cellular network is used as a backhaul link.

B. Identification threats: IMSI transmission in plaintext over-the-air is possible in LTE networks and can reveal subscriber identity to active and passive adversaries. However, the transmission of International Mobile Equipment Identity (IMEI) in plaintext is restricted over LTE networks by the 3GPP to enable device privacy. But certain baseband implementations reveal [31] the device IMEI to rogue base stations. In our work, the problem persists in the 3GPP standard rather than the implementation and hence all LTE devices all vulnerable to our attack. Differently, in [27, 28] authors present device type identification techniques using MAC layer information and network interactions for IP-enabled IoT devices or cellular devices connected over wired ethernet or WLAN interfaces. Further, they also pinpoint vulnerable devices based on the information from vulnerability databases. They perform numerous experiments with real-world off-the-shelf IoT devices. Unlike theirs our research focuses on devices with cellular capabilities and hence applies to latest cellular IoT technologies introduced in last couple of years. Moreover we do not use private identifiers such as IMEI or MAC addresses for identification but determine the device type using its features. Most importantly our identification technique also detects wide range of devices on 5G networks. Next, in [35] authors identify LTE subscribers and their location using temporary identifiers. However, sufficient randomization of these temporary identifiers eliminate the tracking issue and is already implemented by several operators worldwide. Besides, our methods fingerprint devices based on their capabilities that are mostly remain static. Further, we can also link these fingerprints to IMSI and track users on LTE networks.

C. Service availability threats: Attacks targeting LTE service availability fall into DoS and downgrade of service categories. Recently, rogue base station attacks on LTE self organizing networks is presented in [36]. Majorly, the paper uncovers vulnerabilities existing in the measurement reporting procedure, where the network internal data can be poisoned with malicious information causing call drops and service downgrades. Unlike ours the attacks are not persistent and UEs can recover once the attacker shuts down the rogue eNodeB. Moreover, our work targets UEs rather than eNodeBs and hence we require less effort and cost to cause a heavy damage. Next, in [35] perform denial of service attacks by using dedicated LTE control plane messages. Further, we learn that authors have discussed a vulnerability like V3 but lack any experiments to justify their attack in real networks. In contrast, we exploit the latest NB-IoT protocols to cause power drain attacks and have tested and evaluated them on commercial UEs.

9 CONCLUSION

We presented three vulnerabilities that exploit UE capabilities exposed on an LTE network and evaluated them using an experimental setup. We demonstrated that hardware and software characteristics of any device with cellular capabilities can be determined using our reference model. Next, we highlighted an LTE network misconfiguration among 20 operators that causes several service downgrades and affects subscriber experience. Further, we also discussed the battery draining attacks on cellular IoT device. Lastly, we presented mitigations to prevent our attacks and also recommendations to consider for the 5G phase 2 development.

Impact. Several operators are reported on implementation vulnerabilities and remedial actions are underway. Further, the 3GPP SA3 body is considering to add protection for UE capabilities.

Acknowledgements. This research was partly performed within the SerIOT project (seriot-project.eu) the EU Framework Programme for Research and Innovation Horizon 2020 under grant agreement no. 780139. We would like to thank anonymous reviewers for their valuable inputs and suggestions.

REFERENCES

[1] [n. d.]. SPEEDTEST. http://speedtest.net/. ([n. d.]).
[2] [n. d.]. GSMArena.com. https://www.gsmarena.com/team.php3. ([n. d.]).
[3] [n. d.]. WikiDevi. https://wikidevi.com/wiki/Main_Page. ([n. d.]).
[4] 2018. NighthawkÂő M1 Mobile Router . http://www.za.netgear.com/landings/nighthawk-mr1100-mobile-router/. (2018).
[5] 3GPP. 2013. *Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description; Stage 2.* TS 36.300. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/36300.htm
[6] 3GPP. 2013. *Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification.* TS 36.331. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/36331.htm
[7] 3GPP. 2015. *Technical Specification Group GSM/EDGE Radio Access Network; Cellular system support for ultra-low complexity and low throughput Internet of Things (CIoT) (Release 13).* TS 45.820. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/45820.htm
[8] 3GPP. 2016. *3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) radio access capabilities (Release 13).* TS 36.306. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/36306.htm
[9] 3GPP. 2017. *Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; Mobile radio interface Layer 3 specification; Core network protocols; Stage 3 (3GPP TS 24.008 version 14.4.0 Release 14).* TS 24.008. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/24008.htm

Vulnerability	Problem in	Attack	Attack Mode	Impact	Mitigation
UE capabilities accessible without authentication (V1)	3GPP LTE protocols [6]	Mobile Network Mapping (MNmap)	Rogue eNodeB	Identification of devices (Model, OS)	Mandatory security protection for UE capabilities
UE radio capabilities accessed before security setup (V2)	operator's eNodeB Configuration or implementation	Bidding Down	MitM Relay	Decline of data rate, downgrade to 3G/2G for voice calls	
UE (NB-IoT) core capabilities not protected (V2)	3GPP LTE protocols [15]	Battery Draining		Excess power consumption on device	Core network capabilities mutually verified after NAS security setup

Table 1: Overview of the attacks and vulnerabilities

[10] 3GPP. 2017. *LTE;Evolved Universal Terrestrial Radio Access (E-UTRA); Packet Data Convergence Protocol (PDCP) specification (3GPP TS 36.323 version 14.3.0 Release 14).* TS 36.323. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/36323.htm

[11] 3GPP. 2018. *3GPP System Architecture Evolution (SAE); Security architecture.* Technical Specification (TS) 33.401. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/33401.htm

[12] 3GPP. 2018. *Security architecture and procedures for 5G System.* Technical Specification (TS) 33.501. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/33501.htm

[13] 3GPP. 2018. *Service requirements for V2X services.* Technical Specification (TS) 22.185. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/22185.htm

[14] 3GPP. 2018. *System architecture for the 5G System (5GS).* Technical Specification (TS) 23.501. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/23501.htm

[15] 3GPP. 2018. *Universal Mobile Telecommunications System (UMTS);LTE; 5G; Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS); Stage 3 Release 15* . TS 24.301. 3rd Generation Partnership Project (3GPP). http://www.3gpp.org/DynaReport/24301.htm

[16] Apple Inc. [n. d.]. Apple security updates. https://support.apple.com/en-us/HT201222. ([n. d.]).

[17] Cisco. 2018. *Power Saving Mode (PSM) in UEs, MME Administration Guide, StarOS Release 21.* Technical Report. Cisco. https://www.cisco.com/c/en/us/td/docs/wireless/asr_5000/21/MME/b_21_MME_Admin/b_21_MME_Admin_chapter_0111010.pdf

[18] Ettus. [n. d.]. USRP B210. ([n. d.]). http://www.ettus.com/product/details/UB210-KIT

[19] Google Inc. [n. d.]. Android Security Bulletin. https://source.android.com/security/bulletin. ([n. d.]).

[20] GSM-R. [n. d.]. ([n. d.]). https://en.wikipedia.org/wiki/GSM-R

[21] GSMA. 2015. *IMS Profile for Voice and SMS Version 9.008.* Technical Report. GSMA. https://www.gsma.com/newsroom/wp-content/uploads/IR.92-v9.0.pdf

[22] GSMA. 2016. *3GPP Low Power Wide Area Technologies, GSMA white paper.* Technical Report. GSMA. https://www.gsma.com/iot/wp-content/uploads/2016/10/3GPP-Low-Power-Wide-Area-Technologies-GSMA-White-Paper.pdf

[23] K. Haataja and P. Toivanen. 2010. Two practical man-in-the-middle attacks on Bluetooth secure simple pairing and countermeasures. *IEEE Transactions on Wireless Communications* 9, 1 (January 2010), 384–392. https://doi.org/10.1109/TWC.2010.01.090935

[24] K. M. J. Haataja and K. Hypponen. 2008. Man-In-The-Middle attacks on bluetooth: a comparative analysis, a novel attack, and countermeasures. In *2008 3rd International Symposium on Communications, Control and Signal Processing*. 1096–1102. https://doi.org/10.1109/ISCCSP.2008.4537388

[25] Huawei Technologies Co., Ltd. [n. d.]. All Bulletins - PSIRT. https://www.huawei.com/en/psirt/all-bulletins. ([n. d.]).

[26] HUAWEI TECHNOLOGIES CO., LTD. 2010. eRAN2.0 Feature Description. https://www.scribd.com/document/132066434/Huawei-LTE-eRAN2-1-Feature-Description-doc. (Sept. 2010).

[27] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A. Sadeghi, and S. Tarkoma. 2017. IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. In *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*, Vol. 00. 2177–2184. https://doi.org/10.1109/ICDCS.2017.283

[28] P. OâĂŹHanlon, R. Borgaonkar, and L. Hirschi. 2017. Mobile Subscriber WiFi Privacy. In *2017 IEEE Security and Privacy Workshops (SPW)*. 169–178. https://doi.org/10.1109/SPW.2017.14

[29] Qualcomm Technologies, Inc. [n. d.]. Qualcomm Technologies, Inc. Security Bulletin. https://www.qualcomm.com/company/product-security/bulletins. ([n. d.]).

[30] Quectel. [n. d.]. LTE BC68 NB-IoT Module. https://www.quectel.com/product/bc68.htm. ([n. d.]).

[31] R.Borgaonkar, A.Shaik, N.Asokan ,V.Niemi, J.P.Seifert . 2015. LTE and IMSI catcher myths; Blackhat EU. https://www.blackhat.com/docs/eu-15/materials/eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths.pdf. (Nov. 2015).

[32] David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper. 2019. Breaking LTE on Layer Two. In *IEEE Symposium on Security & Privacy (SP)*. IEEE.

[33] Samsung Electronics. [n. d.]. Android Security Updates - Samsung Mobile Security. https://security.samsungmobile.com/securityUpdate.smsb. ([n. d.]).

[34] Semtech Corporation. 2015. LoRa Modulation Basics - AN1200.22. (2015).

[35] Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert. 2016. Practical attacks against privacy and availability in 4G/LTE mobile communication systems. In *23rd Annual Network and Distributed System Security Symposium*. The Internet Society, Reston, VA, USA.

[36] Altaf Shaik, Ravishankar Borgaonkar, Shinjo Park, and Jean-Pierre Seifert. 2018. On the Impact of Rogue Base Stations in 4G/LTE Self Organizing Networks. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '18)*. ACM, New York, NY, USA, 75–86. https://doi.org/10.1145/3212480.3212497

[37] Sigfox S.A. 2017. Sigfox Technical Overview. (2017).

[38] srsLTE. [n. d.]. ([n. d.]). https://github.com/srsLTE/srsLTE

[39] Da-Zhi Sun, Yi Mu, and Willy Susilo. 2018. Man-in-the-middle Attacks on Secure Simple Pairing in Bluetooth Standard V5.0 and Its Countermeasure. *Personal Ubiquitous Computing*. 22, 1 (Feb. 2018), 55–67. https://doi.org/10.1007/s00779-017-1081-6

A LIST OF ACRONYMS

Acronyms	
3GPP	Third Generation Partnership Project
CA	Carrier Aggregation
DoS	Denial-of-Service
E-UTRAN	Evolved Universal Terrestrial Radio Access Network
eNodeB	evolved NodeB
GSMA	GSM Association
LTE	Long Term Evolution
IMSI	International Mobile Subscriber Identity
IMEI	International Mobile Equipment Identity
MitM	Man in the Middle
MIMO	Multi Input Multi Output
MME	Mobility Management Entity
MNmap	Mobile Network mapping
NAS	Non Access Stratum
NB-IoT	Narrow Band - Internet of Things
PSM	Power Saving Mode
RRC	Radio Resource Control
TAU	Tracking Area Update
TAC	Tracking Area Code
UE	User Equipment
USIM	Universal Subscriber Identity Module
VoLTE	Voice over LTE
V2V	Vehicle to Vehicle

Table 2: Summary of Acronyms

B DIFFERENCES AMONG BASEBAND VENDORS

Capability	Huawei	Sam	Intel	MTK	QC
CM Service Prompt	1	0	0	0	1
EIA0	1	1	1	1	0
Access class control for CSFB	0	1	0	1	1
Extended Measurement Capability	0	0	0	1	0

- **Sam**: Samsung, **MTK**: MediaTek, **QC**: Qualcomm
- **1:** enabled, **0:** disabled
- **CM Service Prompt**: Call waiting
- **CSFB**: Circuit Switch Fallback (voice call in 2G/3G).
- **Extended Measurements**: Radio Measurements that can be performed for frequency planning purposes.

C CELLULAR VS CELLULAR IOT

Capability	Cellular	Cellular IoT
PSM timer: T3324	0	1
Extended timer for periodic TAU: T3412 ext	0	1

D PHONE VS OTHERS

Capability	Phone	Other
UE's usage setting	Voice Centric or Data Centric	Not present
Voice domain preference for E-UTRAN	CS Voice or IMS PS Voice	Not present
UMTS AMR codec	Present	Not present

E ANDROID VS IOS

Capability	Android	iOS
MS assisted GPS	1	0
voiceOverPS-HS-UTRA-FDD-r9	1	0

- **MS-Assisted GPS**: The phone can use "assistance data" from the network to improve the accuracy of satellite-based positioning.
- **voiceOverPS-HS-UTRA-FDD**: Indicates whether UE supports IMS voice profile in 3G

F LIST OF TEST DEVICES

We used the following devices to build the reference model.

Manufacturer	Model	Baseband Type
Samsung	Galaxy Alpha	Intel XMM7260
Samsung	Galaxy S6	Samsung Exynos Modem 333
Samsung	Galaxy S7	Samsung Exynos 8890
Samsung	Galaxy S8	Samsung Exynos 8895
Huawei	Honor 7	Kirin 935
Huawei	P20	Kirin 970
HTC	One E9	MediaTek X10
LG	G Flex 2	Qualcomm MSM8994
Sony	Xperia Z5	Qualcomm MSM8994
Sony	Xperia X	Qualcomm MSM8956
Planet Computer	Gemini	MediaTek X27
Apple	iPhone 6	Qualcomm MDM9625
Apple	iPhone 8	Intel XMM7480
Apple	iPhone 8 (US)	Qualcomm MDM9655
Apple	iPhone X (US)	Qualcomm MDM9655
Google	Nexus 5X	Qualcomm MSM8992
Nokia	8110 4G	Qualcomm MSM8905
Asus	ZenFone 2E	Intel XMM7160
Huawei	E3372	Huawei
Samsung	GT-B3740	Samsung CMC220
Sierra Wireless	EM7455	Qualcomm MDM9635
Fibocom	L850-GL	Intel XMM7360
Telit	LN930	Intel XMM7160
AVM	FritzBox LTE	Intel XMM7160
Huawei	B310s	Huawei
Netgear	Nighthawk	Qualcomm MDM9250
GlocalMe	G2	Qualcomm MSM8926
Quectel	BC68	Huawei NB-IoT
Quectel	BC66	MediaTek NB-IoT
Quectel	BG69	Qualcomm MDM9206
Audi	A6	Qualcomm MDM9635
Samsung	SM-V110K	Qualcomm MDM9206
Mobile Eco	ME-K60KL	Qualcomm MDM9206
Apple	Watch Series 3	Qualcomm MDM9635M
Huawei	MediaPad M5	Kirin 960
Apple	iPad 5th gen	Qualcomm MDM9625M

Table 3: List of Test Devices