4G to 5G: New Attacks

Altaf Shaik[*], Ravishankar Borgaonkar[#]

[*]Technische Universität Berlin and Kaitiaki Labs
Email: altaf329@sect.tu-berlin.de

[#]SINTEF Digital and Kaitiaki Labs
Email: rbbo@kth.se

Abstract

5G raises the security bar a level above 4G. Although IMSI exposure is prevented in 5G, we found new vulnerabilities to attack devices and subscribers. In this talk we expose a set of vulnerabilities in the 5G/4G protocols that are found in network operators equipment and also consumer devices such as phones, routers, latest IoT sensors, and even car modems. Our vulnerabilities affect several commercial applications and use cases that are active in 4G networks and are expected to take off in 5G networks. We developed automated tools to exploit the exposed cellular information and share some of our research traces and data sets to the community. We demonstrate a new class of hijacking, bidding down and battery draining attacks using low cost hardware and software tools. We did a rigorous testing worldwide to estimate the number of affected base stations and are surprised by the results. Finally our interactions with various vendors and standard bodies and easy fixes to prevent our attacks are discussed.

1. Introduction

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 standardization context, these technical features and network services termed as device capabilities and exchanged with the network during the device registration phase. In this talk, 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, 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 (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 standardization 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.

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.

• First, both core network and radio access capabilities can be acquired from a UE without establishing authentication. 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.

• Second, mobile network operators are requesting the radio access capabilities from the UE prior to the RRC security setup. As a result, UE capabilities are transferred in plain-text and an adversary can hijack these capabilities. We study the threats resulting from this vulnerable operation and demonstrate device bidding down attacks.

• Third, Attach Request message is always sent unencrypted by the UE to the network, 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.

3. Experimental Setup

We build an experimental setup as shown in Figure 1 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. 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 that acts as a MITM between a victim UE and the legitimate network.

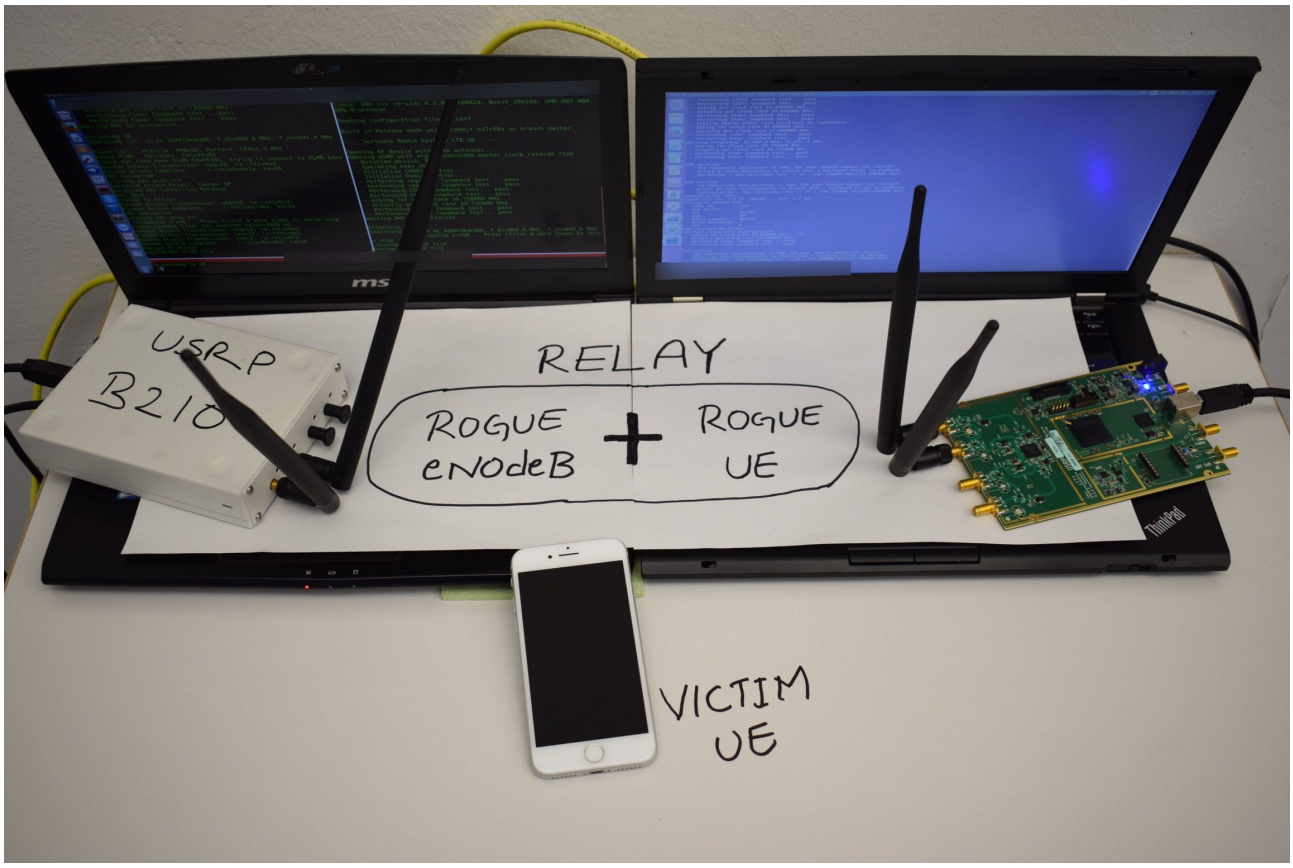

Figure 1: Experimental Setup (MITM Relay)

4. Attacks

a. Device Fingerprinting

To identify the type of devices on a mobile network and intellectually estimate the underlying applications. We start by analyzing the UE's capabilities and build a reference model using a set of known devices and techniques to distinguish various devices and applications. Next we use our reference model to perform Mobile Network Mapping (MNmap) attack. We present various identification levels in figure 2 below. Either being an active or passive attacker, we acquire UE core and radio capabilities and perform the identification.

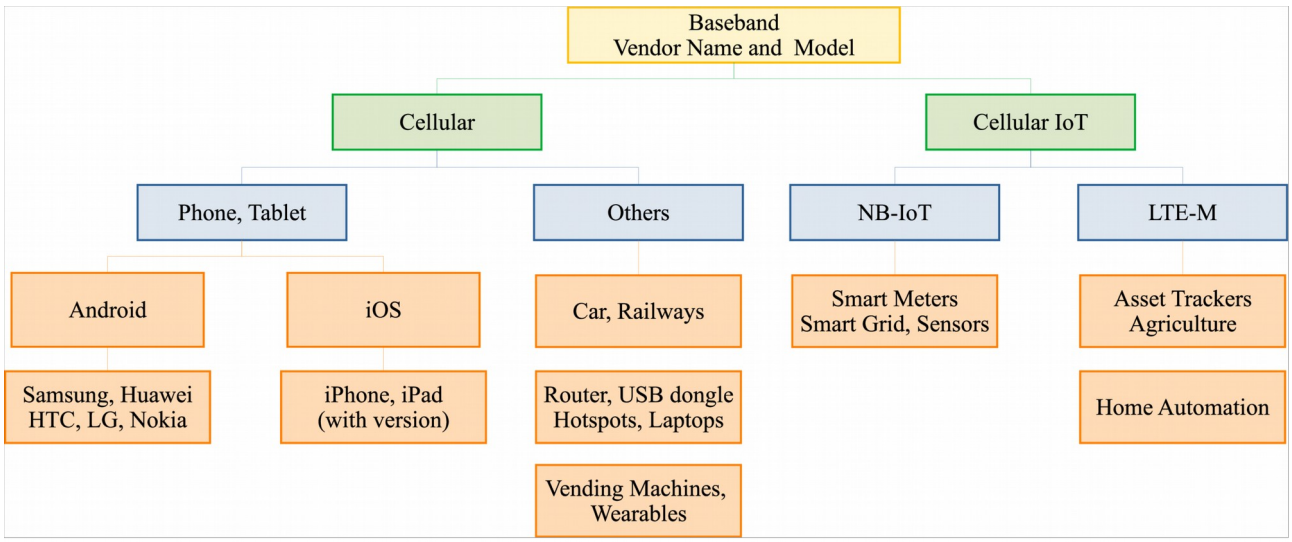

Figure2: Device Identification Levels

b. Device Bidding Down

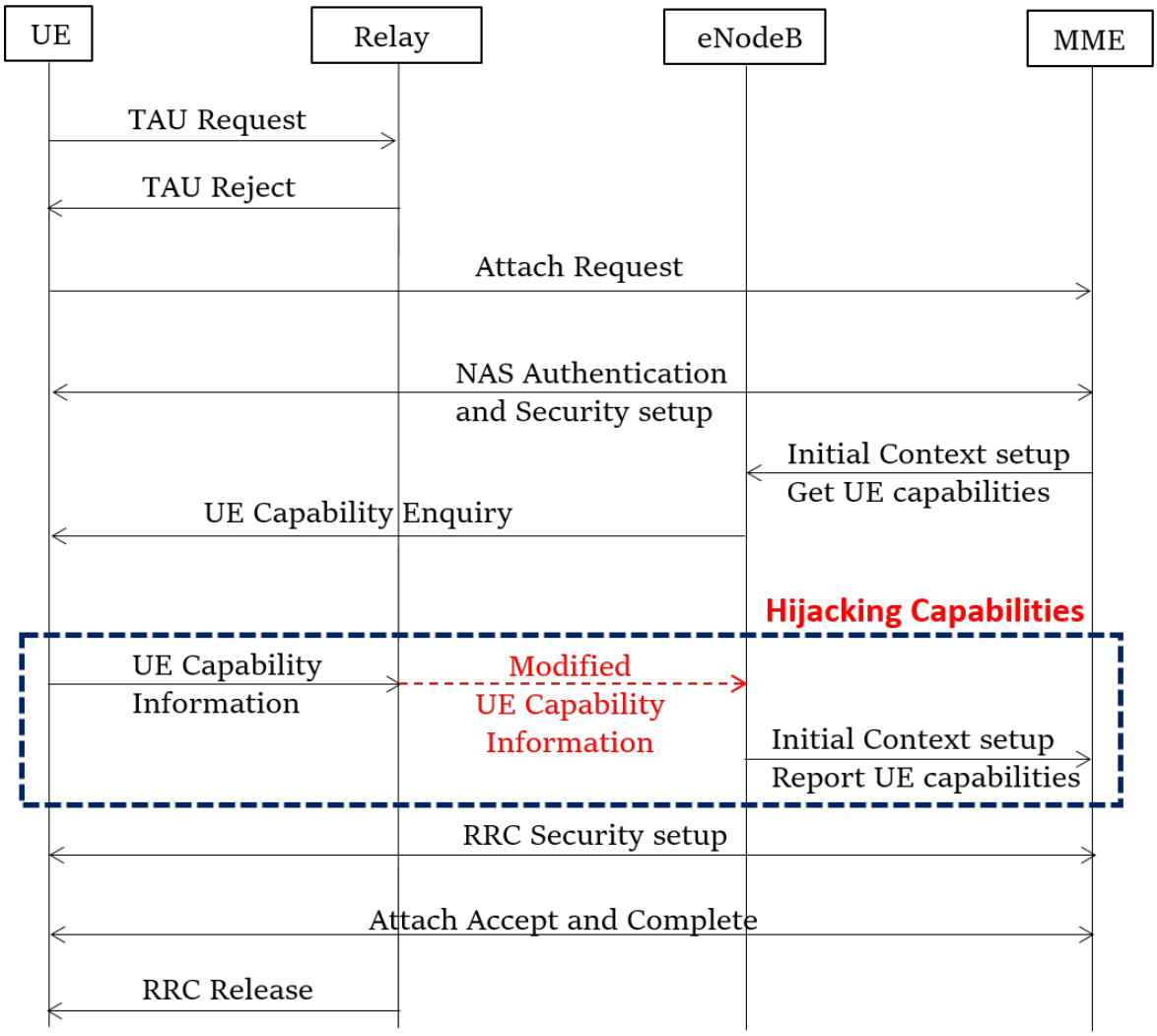

Figure 3: Device Bidding down attack

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 as seen in figure 3 above. Experiments with iphone 8 and Nighthawk M1 mobile router. Speeds crashed down from 27 Mbps to 3 Mbps. Attack is persistent since capabilities are store at MME and reused by the eNodeB for every UE's transaction. Tested on 30 mobile networks worldwide and 21 being affected.

c. Device 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 (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 signaling messages and internal activity logs. In the attack, our relay modifies the contents of the Attach Request message as shown in Figure 4 below. Attacker disable the Power saving mode from the attach request and thus BC68 cannot receive PSM ON message from the network. Hence BC68 battery is continuously drained due to its usage for signal measurements and other internal activities by the modem since it is not OFF. The battery life is reduced by 5 times.

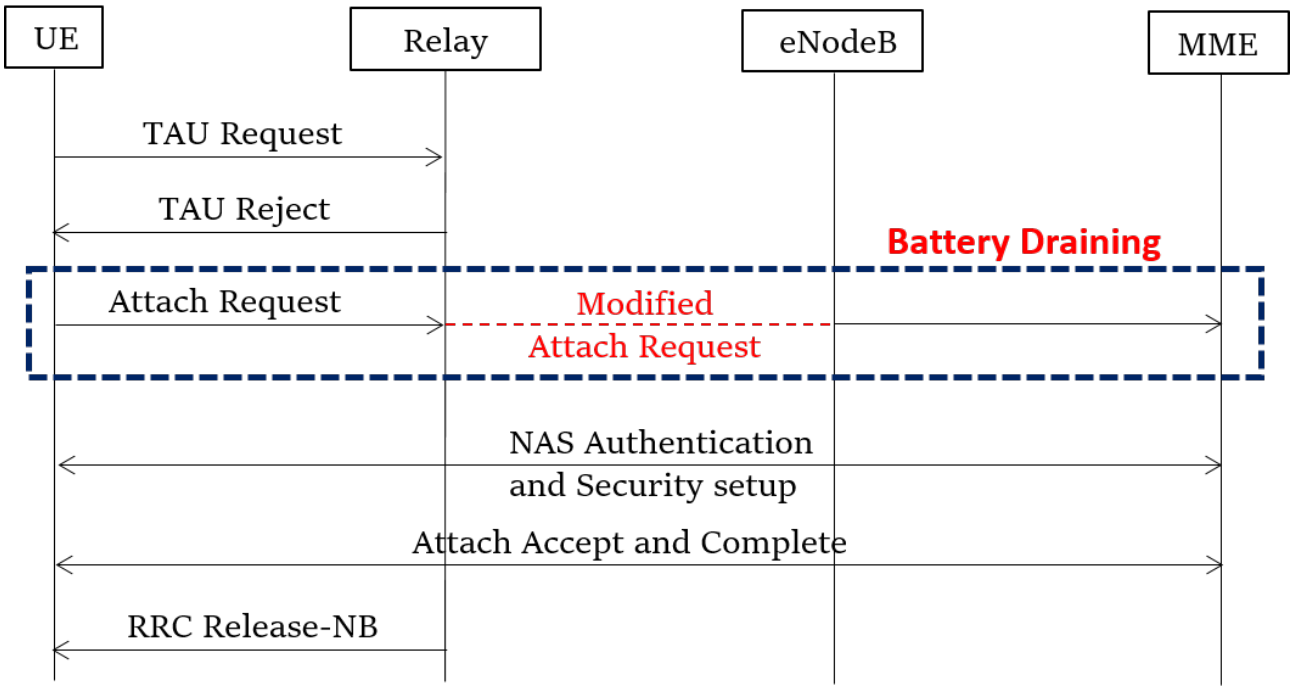

Figure 4: Battery Draining

5. Mitigations

- Device Radio capabilities should be accessed only after establishing security.
- All the Core Network capabilities sent in Attach request messages should be verified upon establishing NAS Security.

6. More Resources

For Detailed Paper:

[1]. https://dl.acm.org/citation.cfm?id=3319728

Follow up on 3GPP mitigations

[2]. https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_95Bis_Sapporo/Docs/S3-192271.zip