Discurs: IMSI-Catchers: Still relevant in the 5G context?

* Intro

Tracking prevention is an important security and privacy goal of mobile networks. In reality, the previous generations suffer from shortcomings that enable the tracking of users. One expectation for the 5th generation of mobile networks was to solve this issue. But a recent study from July 2021 shows that we are still at risk of SUCI Catchers even with the new 5G rolling just around the corner.

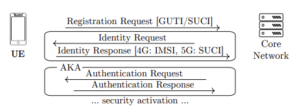
* General background

To better understand what this vulnerability is, let’s take a look at some general information regarding 5G.

1)User Equipment (UE – for examples phones): stores a permanent identifier and permanent key on a Universal Subscriber Identity Module (USIM) card. With these credentials, user and network establish mutual authentication. Three identifiers are important: the permanent identifier SUPI (4G: IMSI), the concealed identifier SUCI (resulted from SUPI using elliptic curves encryption), and the temporary identifier 5G-GUTI.

2) Base Stations (BTS): create the wireless network. Very simply put, the base stations forward all data between the user equipment and the core network.

3) Core Network: performs all management tasks and traffic routing. Most significantly for our disscussion today, it handles authentication and key agreement.



The diagram shows the basic exchange for the user registration and authentication: The user establishes the connection with an initial Registration Request message containing the user’s identity. Usually, the user transmits either a temporary identity (GUTI) or the concealed one (SUCI). The network can request the SUCI if the temporary identity cannot be resolved. Somewhat like websites using cookies to keep you logged in instead of getting you to register all the time. Unfortunately, this early moment of openness can be used to make the user reveal its subscriber identity by malicious actors, for example with fake base stations telling the device that the GUTI is unknown. Subsequently, the Authentication and Key Agreement (AKA) procedure mutually authenticates user and network. All messages of the AKA are unprotected: User Equipment and network can only activate message encryption after agreeing on a session key.

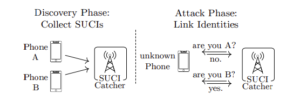
In 5G networks, permanent identifiers are avoided from being sent, using the operator’s public key which is stored in the USIM. The SUPI is encrypted with this public key before transmission, thus becoming SUCI. So, only the operator is able to read the SUPI to reveal the subscriber’s identity. SUCI is regenerated before every usage to prevent linkage (aka perfect forward secrecy), hindering the attacker from identifying if the SUCI refers to the same user ~~(even if the user connects multiple times)~~. Since the SUCI varies, it gives the notion that different users are connecting to the network. THOU, SUPI concealing is an optional feature, configurable by operators. Without SUCI encryption, the permanent identity is directly transmitted with the so-called null scheme, which offers no protection. At the moment, the specification defines two encryption schemes based on the elliptic curves: ~~EC25519 and secp256r1.~~ The USIM stores the public keys of the operator along with a flag for activation.

* IMSI Catchers: SUCI Catchers (5G)

To return to the security issue, let’s talk about SUCI catchers, better known as IMSI catchers. The name is modified because of the new terminology adopted by the 5th generation of mobile networks, but the gist is the same.

In a nutshell, IMSI catchers are fake base stations. On the radio layer, base stations broadcast their identifiers without protection against tampering. That means an attacker can create a fake one just by broadcasting the same identifier as the real network. The fake cell does not have access to any secrets and cannot proceed beyond the security activation after the key agreement procedure, however, that is enough to send the unprotected Identity Request (cf. Figure 1) and other preauthentication messages. Simply put, enough to obtain the user’s permanent identity. The smartphone’s modem continuously monitors the signal strength of nearby cells. If a nearby cell has a stronger or higher-quality signal, the modem selects the cell without interaction from user or operating system. The modem cannot distinguish fake cells from legitimate ones. This type of attack targets everyone within the vicinity of the IMSI catcher and the attacker narrows down to his choice of the target within that list. When the target is connected to the IMSI catcher, the IMSI catcher performs a MITM (Man in the Middle) attack. IMSI catchers are primarily used for spyware delivery, data extraction/interception or location tracking.

So, how does the SUCI-Catcher attack work? The SUCI-Catcher fetches an authentication challenge associated with the SUCI and sends the Authentication Request to all connecting devices. Only the user equipment that accepts the request is the wanted subscriber. The attack is divided into two phases:



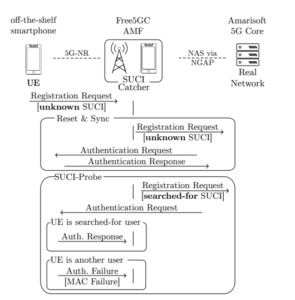
1)Discovery Phase: identifies subscribers of interest and associated SUCIs. Using the AKA linkability, the attack focuses on the UE giving up its own identity in 2 ways:

a) *Obtaining A SUCI via 5G*: The attacker can sniff network traffic for a SUCI or actively request ~~(Identity Request)~~ it once the user connects to the fake 5G base station.

b) *Deriving SUCI from IMSI*: If the IMSI is known, the attacker can perform the encryption from IMSI to SUCI since the operator’s public key is known. The IMSI can be obtained with 4G IMSI catching, which will remain possible as long as the phone supports 4G.

2)Attack Phase: Completing the discovery phase, the attacker now has SUCI of the target. When an unknown UE connects to the catcher, the attacker tries to find out if this unknown UE is identical to the subscriber.

The figure shows the attack in detail.



It consists of two parts: SUCI-Probe and Reset & Sync that are executed repeatedly. The SUCI-Probe resembles the AKA-Linkability, meaning that the attacker tests if the SUCI of the unknown device matches the one that he has. Simply performing the SUCI-Probe has a significant limitation: We observed that after two consecutive authentication failures, the UE cancels the registration attempt. Therefore, we prepend a reset stage that performs a successful AKA between the user equipment and network before the actual SUCI-Probe. This also includes handling a Synch Failure to resynchronize the sequence number at the network to avoid more than one consecutive failure between two SUCI-Probe steps. Consequently, the attacker can repeat the SUCI-Probe step and search for multiple persons.

* Conclusions

To conclude, 5G aims to eliminate the errors from the past generation networks. New functionality brings new vector of attacks, and surely this is the beginning of more and newer attacks. With researchers scrutinising these new stacks, standards need to catch up faster so that issues can be mitigated as soon as possible.