# 5G SUCI-Catchers: Still catching them all?

Merlin Chlosta
merlin.chlosta@rub.de
Ruhr University Bochum
Germany

David Rupprecht
david.rupprecht@rub.de
Ruhr University Bochum
Germany

Christina Pöpper
christina.poepper@nyu.edu
NYU Abu Dhabi
United Arab Emirates

Thorsten Holz
thorsten.holz@rub.de
Ruhr University Bochum
Germany

## ABSTRACT

In mobile networks, IMSI-Catchers identify and track users simply by requesting all users' permanent identities (IMSI) in range. The 5G standard attempts to fix this issue by encrypting the permanent identifier (now *SUPI*) and transmitting the *SUCI*. Since the encrypted SUCI is re-generated with an ephemeral key for each use, an attacker can no longer derive the user's identity. However, this scheme does not prevent all tracking and linking: if the identity of a user is already known, an attacker can *probe* users for that identity.

We demonstrate a proof-of-concept 5G SUCI-Catcher attack in a 5G standalone network. Based on prior work on linkability through the Authentication and Key Agreement (AKA) procedure, we introduce an attack variant that enables practical, repeatable attacks. We capture encrypted SUCIs and use the AKA-procedure to link the encrypted identities between sessions. This answers *Is user X present now?* — a typical scenario for IMSI-Catchers. We analyze the attack's scalability, discuss real-world applicability, and possible countermeasures by network operators.

## CCS CONCEPTS

• **Networks → Mobile and wireless security**.

## KEYWORDS

5G Security, IMSI-Catcher, SUCI-Catcher, Fake Base Station, AKA, SUPI, SUCI, IMSI, Subscription Concealed Identifier

**ACM Reference Format:**
Merlin Chlosta, David Rupprecht, Christina Pöpper, and Thorsten Holz. 2021. 5G SUCI-Catchers: Still catching them all?. In *Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '21), June 28–July 2, 2021, Abu Dhabi, United Arab Emirates.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3448300.3467826

## 1 INTRODUCTION

Tracking prevention is an important security and privacy goal of mobile networks: only the operator should know the identity and location of users [1, 5.1.1]. In reality, however, the previous mobile network generations (2G, 3G, 4G) suffer from shortcomings in the standard that enable the tracking of users. One expectation for the 5th generation (5G) of mobile networks was to solve this issue.

The most popular and widespread radio-layer tracking technique involves *IMSI-Catchers* (sometimes called *Stingrays*), used by law enforcement agencies and others for surveillance [9, 20]. Commercial IMSI-Catchers work as a Fake Base Station, i. e., they copy the identity of the real network and actively *request* the user's permanent identity [18]. Any user within range eventually connects to the IMSI-Catcher and thus unwillingly exposes his or her identity. There are two main use cases: *i) Who is currently nearby?* The attacker records the identity of all nearby users. *ii) Is a particular individual present?* Here, the attacker checks if a known Person of Interest (PoI) is within reach of the IMSI-Catcher.

5G standalone (SA) deployments promise a countermeasure against IMSI-Catchers: the Subscription Permanent Identifier (SUPI) (equivalent to the International Mobile Subscriber Identity (IMSI)) can be *concealed* (i. e., encrypted) with the network operator's public key, yielding the so-called Subscription Concealed Identifier (SUCI) [2]. Only the operator can decrypt the identifier and thus attackers cannot derive the permanent identity anymore. Furthermore, the user's device generates a fresh SUCI for every transmission. Thereby, users should be untraceable.

This paper investigates to which extent the SUCI encryption scheme keeps its privacy promises in practice. We build upon weaknesses in the AKA procedure that enable user linkability [6–8]. We extend the existing weakness to the 5G SUCI scheme and conceptualize a SUCI-Catcher attack. As a result, the SUCI-Catcher can verify if a specific, known subscriber is present in proximity of the SUCI-Catcher, despite the encryption of the permanent identity in 5G-SA networks. Further, we scale the attack to confirm the presence of *multiple* subscribers, implement the first over-the-air SUCI-Catcher attack, and provide real-world evaluations.

In summary, our main contributions are as follows:

- We evaluate the SUPI-SUCI concealment and find that an *active* Machine-in-the-Middle (MitM) can verify the presence of an individual. We enhance the SUCI-Catcher attack to track *multiple* users, in particular, we can check for the presence of more than 500 Persons of Interest (PoI) within 60 seconds in a lab setting.
- We demonstrate the feasibility of the SUCI-Catcher in a 5G standalone network against a commercial phone. We explore the practical limits of the attack's scalability, imposed by the phone and network. Our results show that SUCI-Catchers are applicable in practice and scale well *if operators take no countermeasures like rate-limiting*. We test three networks and found they already throttle the AKA-procedure.
- We discuss the attack implication for users and possible mitigation on top of the current standard. We hope this enables operators to deploy SUCI encryption effectively and drives further security efforts within the 3GPP.

*WiSec '21, June 28–July 2, 2021, Abu Dhabi, United Arab Emirates*

ACM ISBN 978-1-4503-8349-3/21/06.
https://doi.org/10.1145/3448300.3467826

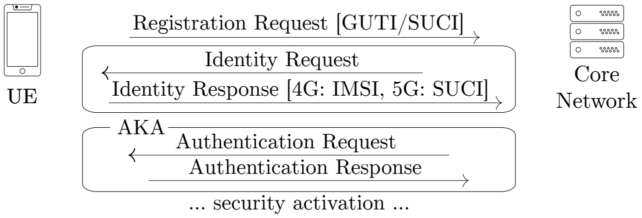
UE
Core Network
Registration Request [GUTI/SUCI]
Identity Request
Identity Response [4G: IMSI, 5G: SUCI]
AKA
Authentication Request
Authentication Response
... security activation ...

**Figure 1: The Authentication and Key Agreement (AKA) Procedure as part of the user registration.**

*Disclosure Process.* We have reported our findings via the GSMA CVD program [14] and discuss the response in Section 5. Our findings do not expose immediate security risks in any networks, instead, we examine the SUCI feature in a practical lab setting to understand the level of protection it offers once deployed.

## 2 BACKGROUND

We briefly introduce the basics of mobile networks, with a focus on IMSI-Catcher attacks and the 5G security measures to mitigate these attacks. We assume that networks and phones transitioned to 5G-only so that these security measures are effective and cannot be circumvented by 2G/3G/4G issues.

### 2.1 5G Networks

*User Equipment (UE).* The UE (essentially the modem) stores a permanent identifier and permanent key on a Universal Subscriber Identity Module (USIM) card. With these credentials, user and network establish mutual authentication (see Section 2.2). Three identifiers are important: the *permanent* identifier SUPI (4G: IMSI), the *concealed* identifier SUCI, and the *temporary* identifier 5G-GUTI.

*Base Stations.* Base Stations create the wireless network. Within this paper, we assume that base stations simply forward all messages between the user equipment and the core network.

*Core Network.* The back-end core network performs all management tasks and traffic routing. Most significantly for this work, it handles authentication and key agreement.

### 2.2 Registration & Authentication Procedures

Figure 1 shows the basic message exchange for user registration and authentication: The user establishes the connection with an initial *Registration Request* message containing the user's identity. Usually, the user transmits a temporary identity or the SUCI. The network can request the permanent identity if the temporary identity cannot be resolved. For simplicity, we assume that the 5G Registration Request always contains the SUCI. 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.

### 2.3 IMSI-Catchers

IMSI-Catchers are known to attack devices to identify and track users. In this section, we focus on the question: *How can IMSI-Catchers find out the identity of surrounding users?*

*Attacker Capabilities.* Commercially available IMSI-Catchers operate as active Fake Base Station [18]. We assume that the attacker can *relay* messages to the real network as a MitM; several studies found this possible with freely available open-source projects [10, 15, 21, 23].

*Fake Base Station.* On the radio layer, base stations broadcast their identifiers without protection against tampering. That means an attacker can create a fake base station 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 pre-authentication messages [22]. Technically, attacks that confirm the presence of *prior known* subscribers are called IMSI-*probing* rather than IMSI-catching. However, we think this technicality hinders the general discussion on practical, effective surveillance, where the term IMSI-Catcher refers to Fake Base Stations that carry out all sorts of attacks.

*Cell Selection.* The smartphone's baseband 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, thereby, eventually connects to in-range IMSI-Catchers.

*Use Cases.* Park et al. cover detailed modes of operation for 20 models of IMSI-Catchers [18]. By logging the identity of nearby users, IMSI-Catchers usually serve two goals:

(1) *Mass Surveillance*: The device operates with high power or in very frequented places to record as many people as possible. For example, this could act as a snapshot of all individuals who participate in a political demonstration. Law enforcement agencies could subsequently request personal data from the mobile operator using the IMSI.
(2) *Targeted Attacks and Location Monitoring*: Another scenario is surveillance of geographically small areas, e. g., a single house with only a few people going in and out. IMSI-Catchers may help to check if an individual is at home or to trace the contacts of an individual. Figure 2 visualizes this situation: First, the attacker observes interesting subscribers (both physically, and via the attack); later, the attacker checks for presence of these Persons of Interest (PoI).

### 2.4 SUPI Concealing: SUCI

5G avoids sending the permanent identifier using an operator's public key that is stored in the USIM. The permanent SUPI is encrypted with this public key before transmission (SUCI). Thus, only the operator—but no attacker—can read the user's identity. The SUCI is re-generated before every usage to prevent linking of SUCIs such that an observer cannot distinguish if the same user connects twice,

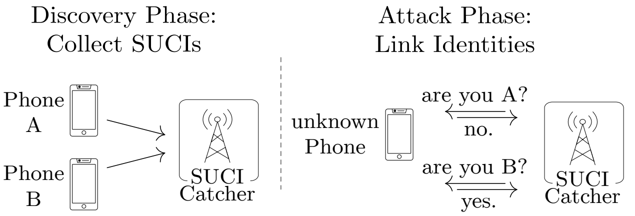

**Figure 2: Two phases of the SUCI-catcher attack.**

or if this represents two distinct users. SUPI concealing is an *optional* feature, configurable by operators [2, Sec 6.12.2]. 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 [2]. The USIM stores the public keys of the operator along with a flag for activation.

## 3 SUCI-CATCHER ATTACK

We apply Authentication and Key Agreement (AKA) linkability [6–8] to the 5G SUCI encryption scheme. In this SUCI catcher attack, the victim *indirectly* discloses their identity. The UE's initial Registration Request to the network is associated with the subscriber's identity. The network proceeds with an Authentication Request and the UE can accept or reject that request. The SUCI-Catcher attack exploits this: it fetches an authentication challenge *associated with the searched-for subscriber's identity* and sends the Authentication Request to all connecting UEs. Only the UE that accepts the request is the wanted subscriber. The attack is divided into two phases (cf. Figure 2): First, a discovery phase identifies subscribers of interest and associated SUCIs. Second, when an unknown UE connects, the SUCI-Catcher can confirm whether the unknown UE belongs to the searched-for subscriber.

### 3.1 Discovery Phase

The attacker must learn *any* SUCI that contains the victim's permanent identity. That is, either (*i*) a SUCI the victim has previously used, or (*ii*) a SUCI derived from the 4G IMSI.

*(i) Obtaining A SUCI via 5G*: The attacker can sniff network traffic for a SUCI or actively request (Identity Request) the SUCI once the user connects to his/her 5G fake base station. Connecting observed SUCIs to the Person of Interest could happen by monitoring a location e.g. by surveillance cameras or with fine-grained location information.

*(ii) 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. Further, the IMSI can leak via SS7 attacks or smartphone apps.

### 3.2 Attack Phase: Linking SUCIs

The attacker is in possession of the searched-for SUCI from the discovery phase. Now, whenever a new user $\text{UE}_{\text{unknown}}$ connects to the fake cell, the attacker tries to find out if $\text{UE}_{\text{unknown}}$ is identical to that searched-for subscriber. Figure 3 shows the attack in detail. It consists of two parts: *SUCI-Probe* and *Reset & Sync* that are executed in repeatedly.

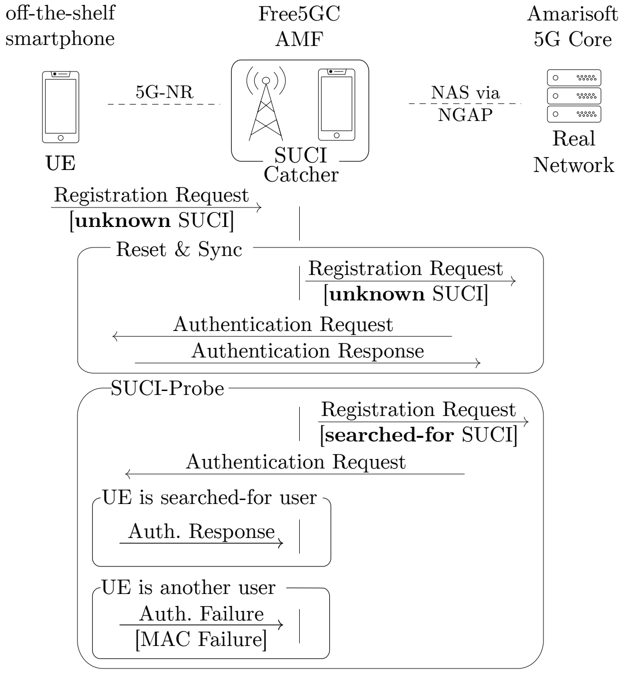

**Figure 3: *Attack Phase:* Modified AKA-Linkability attack with an additional reset-step that enables repetition.**

#### 3.2.1 *SUCI-Probe.*

The *SUCI-Probe* resembles the AKA-Linkability and consists of two components:

- *Requesting Authentication Vectors*: The Registration Request itself is unauthenticated, and the attacker can insert the searched-for SUCI into the identity field. The network looks up the identity and responds to it with an Authentication Request that only the user associated with $\text{SUCI}_{\text{searched-for}}$ can answer.
- *UE confirms its identity*: When the UE receives the Authentication Request, one of two cases may occur:
  - *(i)* the unknown UE is actually $\text{UE}_{\text{searched-for}}$: The UE successfully authenticates the network and responds with Authentication Response, or Authentication Failure with cause *Synch Failure* (which is used to synchronize the sequence number SQN).
  - *(ii)* the UE is not $\text{UE}_{\text{searched-for}}$: The UE sends an Authentication Failure with cause *MAC Failure* to the SUCI-Catcher.

#### 3.2.2 *Reset & Sync.*

Simply performing the SUCI-Probe has a significant limitation: We observed that after two *consecutive* authentication failures, the UE cancels the registration attempt (see Section 4.2) This limitation allows an attacker to search for a maximum of two persons of interest. Therefore, we prepend a *reset* stage that performs a successful AKA between UE 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.

### 3.3 Scalability: Searching multiple subscribers

*IMSI*-Catchers scale well: Each connecting UE only requires a single message to determine the identity, which becomes impossible with SUCI encryption. The basic SUCI-Probe supports testing for a *single* identity. We extended the scheme with an additional reset stage that ensures that no two consecutive authentication failures occur. This allows scaling the SUCI-Catcher attack and *search for multiple subscribers* among connecting UEs: each smartphone entering the cell is tested for a series of subscriber identities.

Suppose the attacker is interested in $N$ subscribers and collected SUCIs for those during the Discovery Phase. The attacker needs to send $2N$ Authentication Requests to each connecting phone. Similarly, the attacker needs to request $2N$ authentication vectors from the real network, which can be lowered to $N$ if old authentication vectors are re-used during the SUCI-Probe stage.

Conveniently, the reset stage allows performing multiple Authentication procedures in a row *without* forcing the unknown user to re-connect on the radio layer. Still, the procedure assumes that *i*) the real network provides fresh authentication challenges without limit, and *ii*) the smartphone answers them. Therefore, we perform dedicated experiments to explore the practical limitations.

## 4 ATTACK EVALUATION

We perform an over-the-air evaluation of the SUCI-Catcher in a 5G-Standalone (SA) lab network, targeting an off-the-shelf smartphone. We successfully run the attack and show the effectiveness *i*) of the AKA-linkability attack in a functional 5G setup with SUCI encryption enabled, and *ii*) of the enhanced SUCI-Catcher that allows searching for multiple subscribers. Further, we *iii*) examine the speed of commercial 4G USIM cards and 4G networks to find out if networks commonly throttle the authentication procedure. For artifacts (PCAPs and logs), see https://github.com/RUB-SysSec/SUCI-artifacts

First smartphones with 5G-Standalone support (including SUCI encryption) are on the market. We perform all tests with a Quectel RM500Q board and an off-the-shelf OnePlus 8 containing the Qualcomm X55 5G chipset. The MitM attacker is based on the open-source core network Free5GC [26] and the Amarisoft gNodeB [5]. The victim's UE and the attacker's gNodeB use a 5G NR radio link in standalone mode. The real network consists of the Amarisoft core network. We directly relay messages between attacker and real network through NGAP interface due to the lack of an open-source standalone 5G UE component. Placing the MitM-attacker on NGAP does not affect the experiment, since it only concerns pre-authentication NAS-layer messaging where both NGAP and radio-layer are merely the transport. We perform additional experiments to show that commercial 4G/5G-Non-Standalone networks respond as expected to our registration requests.

### 4.1 Proof-of-Concept: 5G SUCI-Catcher

We provision sysmocom USIM cards that include the network's public key and enable the USIM-service 124 'subscription identifier privacy support' that instructs the mobile phone to perform SUCI encryption [25]. The NULL-mode is explicitly disabled to ensure that the permanent identity SUPI is never exposed. Both devices can successfully register to the Amarisoft network. Once the attacker's cell becomes available and stronger than the original network, the smartphone joins the cell and the attack from Section 3 begins.

| | | | Commercial Network | | |
|---|---|---|---|---|---|
| | | Lab | A | B | C |
| USIM Auth. | Valid | 12.5/s | 0.9/s | 4.8/s | 18.1/s |
| Responses | Invalid | 16.6/s | 1.1/s | 6.3/s | 35.1/s |
| Network | First 5s | 282/s | 2.0/s | 1.4/s | 2.0/s |
| Auth. | ... 30s | 282/s | 0.8/s | 0.8/s | 0.9/s |
| Requests | ... 60s | 282/s | 0.6/s | 0.7/s | 0.8/s |
| | ... 240s | 282/s | 0.5/s | 0.5/s | 1.1/s |
| UE | RM500Q | 8.3/s | - | - | - |
| | OnePlus 8 | 8.3/s | - | - | - |
| 10 PoIs | [worst case] | 1.2 s | 20 s | 20 s | 9,1 s |
| 500 PoIs | [worst case] | 60 s | 16 min | 16 min | 7.5 min |

**Table 1: Limiting factors for the attack's scalability; commercial networks already rate-limit authentication.**

We could reliably test the attack with both the Quectel RM500Q and the OnePlus 8. The highest speed reliably achieved is 500 tested identities within 60 seconds. Further, we could hold the UE in the cell for more than 2 hours by regularly enforcing a new Authentication. We did not observe divergent behavior from the UE that would require interaction. Our lab setup reflects a realistic 5G standalone setup. However, we test with powerful lab SIM cards and a core network without much load or throttling. Therefore, we further assess commercial networks and USIM cards for their authentication performance. Since 5G and SUCI protection is not yet rolled out, we test the equivalent 4G network authentication.

### 4.2 Practical Attack Scalability

Testing for multiple subscribers requires three components to play along: 1) the UE must not cancel the registration procedure, 2) the real network needs to provide fresh Authentication Requests, and 3) the USIM has to answer them. All components should respond as quickly as possible to minimize the attack runtime and enable practical scenarios. In reality, USIMs are optimized for low cost rather than speed, and networks may apply throttling on messaging. Hence, we test commercial USIM-cards and networks to observe practical boundaries. We test over 4G and expect the same results for 5G, as it depends on the operator's policy rather than technology.

*UE.* The delay between any message must not exceed the 30-second NAS timer T3516 that interrupts unsuccessful authentication procedures. Further, the attacker's gNodeB configures a very high RRC inactivity timer to keep the UE connected, at least until the next message. We found that the UE cancels the connection in practice if no message was received within 15 seconds or after two failed authentication attempts; hence, the regular reset & sync step.

*USIM Speed.* For SIM cards, we test how fast they respond to *i*) valid and *ii*) invalid Authentication Requests. We tested SIM cards from three commercial operators and one from sysmocom as the baseline. Authentication challenges for commercial SIMs were requested from the mobile network, stored, and fed to the SIM cards in one batch. Table 1 shows our results. We did not observe throttling depending on the number of requests. Still, the speeds vary greatly from just 0.9 valid authentications per second to 18.1/s, and from 1.1 invalid authentications per second to 35.1/s. Our attack requires a valid authentication as for the reset & sync step, followed most likely by a failing authentication. Thereby, the attack would be limited to 0.5 identity tests per second for the slowest SIM card and 12 tests per second for the fastest card.

*Network Authentication Throttling.* Fresh authentication vectors coming from the real network are key to the repeated SUCI-Catcher attack; the network needs to supply them constantly and quickly. We used a modified srsUE [13] that constantly maintains physical and MAC-layer connections to the network to rapidly establish RRC connections and send NAS Attach Requests. Table 1 shows the results for three tested networks: We found that all networks throttle after the first few requests, dropping from up to 2.0 messages per second within the first 5 seconds to only 0.5 authentication challenges sent over a 4-minute interval. Our lab setup is unthrottled and supplies 282 challenges per second.

*Attack Scalability.* The attacker can parallelize all attack steps: Fetching the authentication token for the reset & sync step can be done while waiting for the response to the Authentication Request of the SUCI-Probe step. Additionally, fetching authentication tokens during SUCI-probe is not throttled by the network because it is requested for an alternating identity. This step can also be run in parallel while waiting to respond to the Authentication Request of the reset & sync step. Consequently, the scalability and runtime are limited by the slowest step involved.

In our lab experiment, we can test 500 identities within 60 seconds, which is limited by the number of attempts at the UE. We use this insight to estimate the SUCI-Catcher attack's scalability in commercial networks using the most limiting factor. For all operators, network throttling is the most limiting factor (0.5/s, 0.5/s, 1.1/s). We assume that the attacker looks for 10 or 500 Persons of Interest (PoI) for our estimation. We only consider the worst-case scenario and see that the attack scales well for small groups. In networks A and B, it would take 20 seconds to verify if or if not the unknown person is among the 10 PoIs. If the attacker searches 500 PoIs, it already takes 16 minutes (networks A, B) or 7.5 min (C).

## 5 DISCUSSION

**Real-World Applicability and Scalability**: We demonstrate linking users in a 5G standalone network against a COTS 5G phone. Our experiment is limited by using a direct NGAP interface between the attacker and the real network, due to the lack of a modifiable 5G-SA UE component. Prior work shows MitM attackers in 4G [15], and protocols have not fundamentally changed. Likewise, it is a question of time until commercial platforms upgrade to 5G features.

Based on our experiments, we estimate that the attack scales very well for few Persons of Interest (N smaller 10), but takes much longer for large groups. Under the assumption that SUCI catchers try to operate quietly, large-scale attacks could catch the phones' or operator's attention. We conclude the SUCI-Catcher attack is particularly suitable for targeted identification and tracking purposes, e. g., to check if someone is at home.

**Responsible Disclosure**: Similar to our targeted and untargeted scenarios, the 3GPP distinguishes between IMSI-catching and IMSI-probing. With IMSI-probing, an attacker already knows the identity and wants to determine whether the subscriber is present in a given area. Hence, introducing the SUCI was understood as a countermeasure against IMSI-catching but not against *probing*. Further, the 3GPP is aware of session linkability based on the authentication, as they discuss the shortcomings of the AKA procedure and potential mitigation in 5G systems [4]. Despite the 3GPP's knowledge of the attack vector, we followed the responsible disclosure guidelines to raise awareness under the GSMA members and trigger a discussion with 3GPP groups. In particular, the 3GPP considers the attacks less powerful compared to IMSI-Catching. We hope that our efforts help to understand the effectiveness and scalability of the SUCI-Catcher attack. We think the attack could have a relevant impact in certain, targeted scenarios.

## 6 COUNTERMEASURES

The SUCI-Catcher works as a fake base station and exploits linkability in the AKA — two starting points for an attack prevention.

**Fake Base Station Prevention**: The SUCI-Catcher attack exploits pre-authentication traffic and unprotected broadcasts with the real network's identity. The 3GPP discusses different approaches to secure broadcast information in TR 33.809 [3]. Hussain et al. [19] evaluate a similar approach. Securing the pre-authentication traffic would ultimately mitigate SUCI-Catchers. This however needs to be standardised first and offers no immediate mitigation for 5G.

**Prevention of Linkability**: Another option is to mitigate the linkability of authentication responses. The 3GPP study TR33.846 proposes to hide the failure cause in the authentication reject [4]. However, our here-discussed approach does not rely on the failure cause: it detects the UE's presence based on the message *type* (reject or accept). A solution that only hides the failure cause does not protect against a SUCI-Catcher attack. Even if failure cause and message type could be hidden, the attacker would observe whether the connection establishment proceeds or not. Hence, the linkability would not be circumvented.

**Network-based Prevention and Detection**: The attacker uses the legitimate network as an oracle to generate fresh authentication vectors. *A throttling mechanism reduces the attack's scalability effectively and requires little efforts for adoption.* Operators can also detect large scale SUCI-Catcher attacks by keeping track of already-used SUCIs (e.g., storing them in a database). Reappearing likely originate from an attack. However, this detection does not work if the attacker generates SUCIs from a known IMSI. Further, the operator could deploy a custom SUCI encryption scheme to detect such attacker-originating requests. This scheme must guarantee the freshness *and* the SUCI's authenticity, e.g., with a counter and UE's private-public key pair.

**UE-based Detection**: The UE can detect a SUCI-Catcher attack by detecting anomalous protocol behavior. For example, the UE can detect a SUCI-Catcher by observing multiple, repeated authentication request. The UE or USIM can limit or delay the responses, which degrades the attack scalability: if the number of responses is limited to small numbers, the attack has only a few attempts to guess the correct authentication token. Such solutions can be integrated into an App with baseband access, e. g., SnoopSnitch [24].

**Conclusion** The attack remains feasible as long as both the linkability and the generation of a fresh authentication token remain feasible. Sustainable protocol mitigation against the SUCI-Catcher needs to eliminate both attack causes. Networks and UEs can detect the SUCI-Catcher's abnormal behavior. Throttling at both sides limits large-scale attack attempts.

## 7 RELATED WORK

Basin et al. [7] performed a formal analysis of the 5G-AKA protocol and found the SUCI linkability issue, which represents the theoretical foundation of the SUCI-Catcher attack. Multiple linkability attacks are known in mobile networks. One of the first attacks was discovered by Arapinis et al. [6]. The authors describe identification through different failure types in authentication reject messages. We describe one variant of the SUCI-Catcher that uses this mechanism. Other side-channel attacks disclose information beyond the victim's identity. Borgaonkar et al. [8] identify the number of connections the victim had through the sequence number SQN that verifies the freshness of the authentication token. The SUCI-Catcher could be combined with this attack variant.

IMSI-Catchers are one of the most prominent attacks in mobile networks. Park et al. analyze the capabilities of 20 different commercial IMSI-Catchers [18]. Several studies analyze fake base station detection, e.g., by looking for suspicious traffic such as frequent identity requests [11, 12, 16, 17, 24]. The repeating pattern of the SUCI-Catcher would make the attack detectable for those approaches. User-side detection apps were found insufficient for sound detection [17].

## 8 CONCLUSION

5G networks are a key technology for future society and it is crucial to protect the privacy of users. In previous generations, IMSI-Catchers are an *easy* way of user identification and tracking at scale. 5G standalone networks come with an optional protection scheme, SUCI-encryption, that will stop transmitting the user's permanent identifier in plain text and hence make user identification and tracking much harder. However, the protection does not fully prevent linking identifiers, the starting point for our attack. We implement a proof-of-concept SUCI-Catcher in a 5G network. Our experiments show that the technique scales worse than traditional IMSI-Catchers especially when operators rate-limit the user authentication, but enables *targeted* tracking of *specific users*.

## 9 ACKNOWLEDGEMENTS

This work was supported by the German Research Foundation (DFG) within the framework of the Excellence Strategy of the Federal Government and the States – EXC 2092 CaSa – 39078197. It was also supported by the Center for Cyber Security at New York University Abu Dhabi (NYUAD) and the Abu Dhabi Award for Research Excellence (AARE-2019) under grant AARE19-236.

## REFERENCES

[1] 3GPP. 2010. *3G security; Security architecture.* TS 33.102. http://www.3gpp.org/ftp/Specs/html-info/33102.htm

[2] 3GPP. 2018. *Security architecture and procedures for 5G System.* TS 33.501. http://www.3gpp.org/ftp/Specs/html-info/33501.htm

[3] 3GPP. 2018. *Study on 5G Security Enhancement against False Base Stations.* TR 33.809. http://www.3gpp.org/ftp/Specs/html-info/33809.htm

[4] 3GPP. 2018. *Study on authentication enhancements in 5G System;.* TR 33.846. http://www.3gpp.org/ftp/Specs/html-info/33846.htm

[5] Amarisoft. [n.d.]. AMARI Callbox Series. https://www.amarisoft.com/products/test-measurements/amari-lte-callbox/. [Online; accessed May 28, 2021].

[6] Myrto Arapinis, Loretta Mancini, Eike Ritter, Mark Ryan, Nico Golde, Kévin Redon, and Ravishankar Borgaonkar. 2012. New Privacy Issues in Mobile Telephony: Fix and Verification. In *Conference on Computer and Communications Security (CCS)* (Raleigh, NC, USA). ACM, 205–216.

[7] David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler. 2018. A Formal Analysis of 5G Authentication. In *Conference on Computer and Communications Security (CCS).* ACM, 1383–1396.

[8] Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik. 2019. New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. *Proceedings on Privacy Enhancing Technologies* 2019, 3 (2019), 108–127.

[9] Bundesregierung. [n.d.]. Einsätze von sogenannten Stillen SMS, WLAN-Catchern, IMSI-Catchern, Funkzellenabfragen im ersten Halbjahr 2019, BT-Drucksache 19/11706. https://kleineanfragen.de/bundestag/19/12465.

[10] Merlin Chlosta, David Rupprecht, Thorsten Holz, and Christina Pöpper. 2019. LTE Security Disabled — Misconfiguration in Commercial Networks. In *Conference on Security & Privacy in Wireless and Mobile Networks (WiSec).* ACM.

[11] Adrian Dabrowski, Georg Petzl, and Edgar R Weippl. 2016. The Messenger Shoots Back: Network Operator Based IMSI Catcher Detection. In *Recent Advances in Intrusion Detection (RAID)* (Paris, France). Springer.

[12] Adrian Dabrowski, Nicola Pianta, Thomas Klepp, Martin Mulazzani, and Edgar Weippl. 2014. IMSI-Catch Me If You Can: IMSI-Catcher-Catchers. In *ACM Annual Computer Security Applications Conference (ACSAC).* ACM.

[13] Ismael Gomez-Miguelez, Andres Garcia-Saavedra, Paul D Sutton, Pablo Serrano, Cristina Cano, and Doug J Leith. 2016. srsLTE: an open-source platform for LTE evolution and experimentation. In *ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization (WiNTECH)* (New York City, NY, USA). ACM, 25–32.

[14] GSMA. [n.d.]. GSMA Coordinated Vulnerability Disclosure Programme). https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/. [Online; accessed 25-May-2021].

[15] Syed Rafiul Hussain, Omar Chowdhury, Shagufta Mehnaz, and Elisa Bertino. 2018. LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE. In *Symposium on Network and Distributed System Security (NDSS).* ISOC.

[16] Peter Ney, Ian Smith, Gabriel Cadamuro, and Tadayoshi Kohno. 2017. SeaGlass: Enabling City-wide IMSI-Catcher Detection. *Privacy Enhancing Technologies (PETS)* 2017, 3 (2017).

[17] Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, Andrew Martin, and Jean-Pierre Seifert. 2017. White-Stingray: Evaluating IMSI Catchers Detection Applications. In *Workshop on Offensive Technologies (WOOT).* USENIX Association.

[18] Shinjo Park, Altaf Shaik, Ravishankar Borgaonkar, and Jean-Pierre Seifert. 2019. Anatomy of Commercial IMSI Catchers and Detectors. In *Workshop on Privacy in the Electronic Society* (London, United Kingdom) *(WPES'19).* 74–86.

[19] Syed Rafiul Hussain, Mitziu Echeverria, Ankush Singla, Omar Chowdhury, and Elisa Bertino. 2019. Insecure Connection Bootstrapping in Cellular Networks: The Root of All Evil. In *Conference on Security & Privacy in Wireless and Mobile Networks (WiSec).* ACM.

[20] Alexia Ramirez. 2020. ICE Records Confirm that Immigration Enforcement Agencies are Using Invasive Cell Phone Surveillance Devices. https://www.aclu.org/news/immigrants-rights/ice-records-confirm-that-immigration-enforcement-agencies-are-using-invasive-cell-phone-surveillance-devices/. [Online; accessed May 28, 2021].

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

[22] 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 *Symposium on Network and Distributed System Security (NDSS).* ISOC.

[23] 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 *Conference on Security & Privacy in Wireless and Mobile Networks (WiSec).* ACM.

[24] SR Labs. [n.d.]. SnoopSnitch. https://opensource.srlabs.de/projects/snoopsnitch.

[25] sysmocom. [n.d.]. sysmoISIM-SJA2 SIM. http://shop.sysmocom.de/products/sysmoISIM-SJA2. [Online; accessed May 28, 2021].

[26] National Chiao Tung University. [n.d.]. free5GC. https://www.free5gc.org. [Online; accessed May 28, 2021].