

On the Efficacy of New Privacy Attacks against 5G AKA

Haibat Khan^a and Keith M. Martin

Information Security Group, Royal Holloway, University of London
Haibat.Khan.2016@live.rhul.ac.uk, Keith.Martin@rhul.ac.uk

Keywords: 5G AKA, mobile telephony, privacy, unlinkability.

Abstract: The AKA protocol is the primary mechanism in mobile telephony for establishment of a secure channel between mobile subscribers and their service providers. In addition to the requisite security guarantees, provisioning subscription privacy is an essential requirement for AKA. A recent paper by Borgaonkar et al. has uncovered a new vulnerability in one of the associated mechanisms of the AKA protocol. Based upon this vulnerability, Borgaonkar et al. have presented two privacy attacks; namely, *activity monitoring attack* and *location confidentiality attack*. In this paper, we analyze these attacks for their effectiveness, practicability and potency against 5G. Our analysis reveal that the *activity monitoring attack* is not as effective against 5G as it is against the previous generations (3G/4G). The analysis also bring to light the fact that the *location confidentiality attack* is a direct extension of an existing privacy vulnerability that affects all generations (including 5G) of mobile telephony in a much severe manner. In this paper we also establish that any countermeasure introduced to fix this existing vulnerability will also render these two new attacks ineffective.


1 INTRODUCTION

More than half of the world's population uses mobile telephony services as an integral part of their daily life. Considering the ubiquity of mobile telephony, it is imperative that appropriate security and privacy guarantees be provisioned to the end-users of these services. The latest generation of mobile telephony services operating on a commercial basis is 4G/LTE. The first phase of the next generation technology (5G Release 15) has already been standardized and is currently undergoing field trials (Geelen, 2019). The international body responsible for standardization of mobile telephony technologies is the *3rd Generation Partnership Project* (3GPP). The 3GPP standard for 3G/4G mobile telephony security (3rd Generation Partnership Project, 2017) provisions an Authenticated Key Agreement (AKA) protocol for establishment of a secure channel between mobile subscribers and their service providers. The AKA protocol for 4G networks is essentially similar to that of 3G with slight differences in identifier and key management. For 5G, an enhanced version of this AKA protocol

called the 5G AKA was introduced by 3GPP (3rd Generation Partnership Project, 2018c). Apart from typical security requirements, an important consideration for AKA (and its associated mechanisms) is end-user privacy. 3GPP has specified the following privacy requirements for mobile telephony users (3rd Generation Partnership Project, 2018a):

- **User Identity Confidentiality.** The permanent identity of a user to whom a service is delivered cannot be eavesdropped on the radio access link.
- **User Location Confidentiality.** The presence or arrival of a user in a certain area cannot be determined by eavesdropping on the radio access link.
- **User Untraceability.** An intruder cannot deduce whether different services are delivered to the same user by eavesdropping on the radio access link.

A recent paper (Borgaonkar et al., 2019) has revealed a new logical vulnerability in one of the associated mechanisms (sequence number re-synchronization) of the AKA protocol. Based upon this vulnerability, this paper presented two privacy attacks; namely, *activity monitoring attack* and *location confidentiality attack*. The *activity monitoring attack* allows an attacker to learn subscribers' mobile service consumption patterns while the *location confidentiality attack* allows tracking of mobile subscribers, thus

^a  <https://orcid.org/0000-0002-2948-4964>

breaking location confidentiality. The paper claimed that these attacks adversely affect all generations of mobile telecommunications, including 5G. More importantly, the authors of (Borgaonkar et al., 2019) stated that these attacks have been acknowledged by the requisite standardization bodies and that remedial actions are underway for the future 5G specifications.

In this paper, we analyze the efficacy of these new privacy attacks against 5G. The reason for confining this analysis to 5G is due to the fact that relatively facile attacks (IMSI-catching (Fox, 2002), linkability via failure messages (Arapinis et al., 2012)¹) provisioning more disastrous breaches of subscriber privacy already exist for the previous generations (2G/3G/4G). Effective countermeasures for these existing attacks were not incorporated in the already deployed standards because of the high upgrade costs involved. It is thus too late to propose any amendments for the 2G/3G/4G specifications. The findings of our analysis contradict some of the claims made in (Borgaonkar et al., 2019). Specifically, we show the following:

- The *activity monitoring attack* is infeasible to execute in 5G networks.
- The *location confidentiality attack* is a direct extension of an existing privacy vulnerability (Arapinis et al., 2012) that exploits linkability of the AKA failure messages. Moreover, we demonstrate that the results obtained with this extension attack are less effective than those achieved via the existing vulnerability.
- Contrary to (Borgaonkar et al., 2019) which claims dedicated fixes are required for their attacks, we establish that in case of effectual countermeasures introduced against the existing vulnerability of (Arapinis et al., 2012), both *activity monitoring attack* and *location confidentiality attack* will be rendered futile.
- The associated security and privacy analysis of the modified 5G AKA, carried out in a symbolic model, is inaccurate and error prone due to omission of important aspects specified within the 3GPP standard.

2 BACKGROUND

Before considering the details of the privacy attacks, we outline the 5G AKA upon which these attacks are based.

¹This linkability attack is also valid for 5G Release 15.

2.1 The 5G AKA

The mobile telephony security architecture consists of three main entities. Subscribers carry *User Equipment (UE)* which is typically a mobile phone (*Mobile Equipment (ME)* in 3GPP terminology) equipped with a *Universal Integrated Circuit Card (UICC)*. While the phones are treated as dumb hosts, the UICC acts as a *Hardware Security Module (HSM)* (Sustek, 2011) which hosts the *Universal Subscriber Identity Module (USIM)* application. USIM securely stores and processes the subscriber’s secret information. The *Home Network (HN)* is a mobile operator with whom the user’s subscription is registered. Home Networks maintain databases about their subscribers and are responsible for their authentication. *UE* and *HN* are trusted entities which share secret data such as a subscriber’s long-term identity *Subscription Permanent Identifier (SUPI)*, long-term symmetric key K , 48-bit monotonically increasing counters called *Sequence Numbers (SQN)* used for replay protection, etc. Sometimes a subscriber is not in the coverage area of its *HN*. In such scenarios, the *UE* is serviced by another semi-trusted mobile operator called *Serving Network (SN)*. The *SN* is semi-trusted in the sense that while the subscription’s *SUPI* gets shared with the *SN* after a successful secure channel establishment (this is essential for billing and Lawful Interception (LI)² purposes), the same is not true for other secret parameters like key K and *SQN*.

In addition to the requirements of mutual authentication and data confidentiality, it is crucial that *SQN* is protected from an eavesdropper during the establishment of a secure channel between the *UE* and *SN* as its exposure may lead to the compromise of the identity and location of a user (3rd Generation Partnership Project, 2018a). In 5G, these requirements are achieved by the 5G AKA. Figure 1 shows details of the 5G AKA and its associated failure mechanisms. In Figure 1 functions f_1, \dots, f_5, f_1^* and f_5^* are unrelated symmetric key algorithms, f_1, f_2 and f_1^* act as message authentication functions, while f_3, f_4, f_5 and f_5^* are used as key derivation functions. Key derivation is performed using the *Key Derivation Function (KDF)* specified in 3GPP TS 33.220 (3rd Generation Partnership Project, 2018b) and SN_{name} is the global identity of the *SN*. A successful 5G AKA culminates in the derivation of the anchor key K_{SEAF} by the *SN* and *UE* from which further keys for securing various layers of communication are derived. The two cases

²Lawful Interception (LI) refers to the facilities in telecommunications and telephone networks that allow law enforcement agencies with court orders or other legal authorization to selectively wiretap individual subscribers.

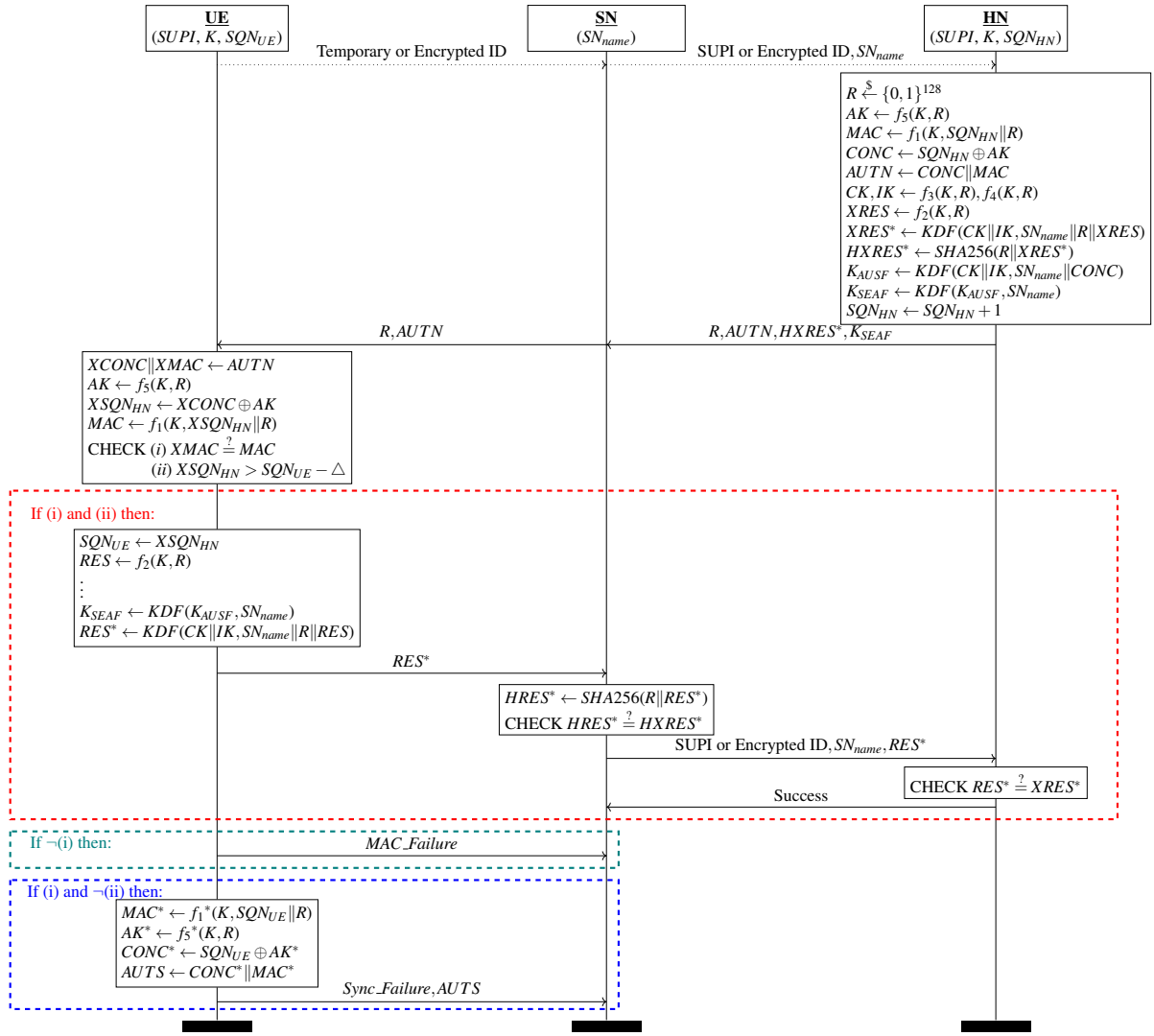


Figure 1: The 5G AKA protocol and its associated failure mechanisms.

of authentication failure for the 5G AKA are as below:

1. **MAC_Failure:** As the first step in authentication confirmation, the *UE* checks whether the received *MAC* value is correct or not. In case of a failure [Case $\neg(i)$ in Figure 1], the *UE* replies with a *MAC_Failure* message back to the *SN*.
2. **Sync_Failure:** After *MAC* verification, the *UE* checks the freshness of the sequence number *SQN* received in the authentication challenge. In case of this failure [Case (i) and $\neg(ii)$ Figure 1], it responds with a *Sync_Failure* message along with a re-sync token *AUTS*. Note that in Figure 1, the sequence number freshness check is denoted by $XSQN_{HN} > SQN_{UE} - \Delta$. What this actually means is that there is some "window" of size Δ , within which sequence numbers smaller than the

current sequence number of *UE* will be accepted given they previously had not been received by the *UE*. This mechanism is there to handle out-of-order delivery of challenge messages from *HN* to *UE*. We discuss this aspect in further detail in Section 3.3.

2.2 The Logical Vulnerability

The logical vulnerability of (Borgaonkar et al., 2019) affecting user privacy stems from the use of XOR within the re-sync token *AUTS*, which is concatenation of two parameters; *CONC** and *MAC**. The parameter *CONC** contains the current sequence number of the *UE* in a masked form as $SQN_{UE} \oplus AK^*$, where $AK^* = f_5^*(K, R)$. Note that during calculation of the masking key AK^* , the value *R* is extracted from

the received authentication challenge. Hence, in case of receiving the same authentication challenge twice at two different times t_1 and t_2 , the masked sequence numbers in their corresponding *AUTS* tokens will be:

$$CONC_1^* = SQN_{UE}^1 \oplus AK_1^* \text{ where } AK_1^* = f_5^*(K, R)$$

$$CONC_2^* = SQN_{UE}^2 \oplus AK_2^* \text{ where } AK_2^* = f_5^*(K, R),$$

where SQN_{UE}^1 is the sequence number of *UE* at time t_1 and SQN_{UE}^2 is the sequence number at time t_2 . Therefore, the adversary can compute:

$$CONC_1^* \oplus CONC_2^* = SQN_{UE}^1 \oplus SQN_{UE}^2.$$

Next we detail the two attacks presented in (Borgaonkar et al., 2019) which, by exploiting this vulnerability, try to compromise user privacy.

2.3 Activity Monitoring Attack

In this attack the adversary tries to learn the n least significant bits of SQN_{UE} at two different time instances, t_1 and t_2 . Thereafter, from the difference between the sequence numbers (corresponding to successful authentication sessions), the attacker infers the volume of ‘‘activity’’ (number of call, SMS, etc) a particular user has performed between these two time instances, hence the name *Activity Monitoring Attack* (AMA). As we will see shortly, to mount this attack the adversary requires malicious interaction with both *UE* and *HN* (via *SN*). Hence, the compromise of both *identity confidentiality* and *location confidentiality* of the target *UE* are prerequisites to launch an AMA. Details of a single instance of the attack at a particular time t are now explained. The online phase of the AMA is depicted in Figure 2. During this phase the attacker first fetches $2^{n-1} + 1$ successive authentication challenges from the *HN* for the targeted *UE*. The attacker then sends a particular $n + 1$ of these challenges to the *UE* each followed by a replay instance of the initially received authentication challenge ($R_0, AUTN_0$) and records the corresponding $n + 1$ resync tokens, i.e. $AUTS_i^*$ and $AUTS_j^*$ (for $j = 0$ to $n - 1$).

In the offline phase, utilizing the logical vulnerability as elaborated earlier in Section 2.2, the attacker retrieves the following values from the recorded resync tokens:

$$\delta_i = SQN_{HN}^0 \oplus (SQN_{HN}^0 + 2^i) \text{ for } 0 \leq i \leq n - 1,$$

where SQN_{HN}^0 is the initial value of the *HN*’s sequence number at the start of the attack. Note that due to receipt of the first authentication challenge ($R_0, AUTN_0$) from the adversary, the *UE* will also sync its sequence number to this value at the start of the attack. Further, by feeding these n values into Algorithm 1, the attacker extracts the n least significant bits of SQN_{HN}^0 .

Algorithm 1: SQN inference algorithm.

Data: δ_i for $0 \leq i \leq n - 1$

Result: $X = n$ least significant bits of SQN_{HN}^0

$X \leftarrow [0, 0, \dots, 0]$ // init an array of size n

for $i \leftarrow 0$ **to** $n - 1$ **do**

 // Analyze δ_i at bit positions $i, i + 1$

$(b_1, b_2) \leftarrow (\delta_i[i], \delta_i[i + 1])$

if $(b_1, b_2) \Leftrightarrow (1, 0)$ **then**

 // No remainder propagates when

$$SQN_{HN}^0 + 2^i$$

$X[i] \leftarrow 0$

else if $(b_1, b_2) \Leftrightarrow (1, 1)$ **then**

 // A remainder propagates when

$$SQN_{HN}^0 + 2^i$$

$X[i] \leftarrow 1$

else

 // Not possible

 Error

end

end

return (X)

2.4 Location Confidentiality Attack

As an other consequence of the logical vulnerability of Section 2.2, (Borgaonkar et al., 2019) presented a *Location Confidentiality Attack* (LCA), i.e. finding out whether some targeted *UE* is present in a certain location. Note that we present LCA as explained in (Borgaonkar et al., 2019). We claim there are several erroneous assumptions upon which this attack is based and we will highlight these when we undertake the corresponding analysis in Section 3.2. The LCA proceeds as follows:

1. The attacker observes a 5G AKA session of some targeted user³ UE_x and extracts the corresponding $CONC_x^*$ value by replaying the observed authentication challenge to UE_x .
2. After some time, if the attacker wishes to check whether another unknown 5G AKA session belongs to UE_x or not, the attacker again replays the earlier observed challenge from Step (1) to this unknown user and obtains $CONC_y^*$.
3. Now based upon the value $CONC_x^* \oplus CONC_y^*$, the attacker can infer (with non-negligible probability) whether this new user is UE_x or not. In case of some other user, this will be a random value, while in case of UE_x , it will equate $SQN_{UE_x}^{old} \oplus SQN_{UE_x}^{current}$ due to canceling out of the common masking key

³Note that it is not necessary for the attacker to know the *SUPI* of the user to launch this attack.

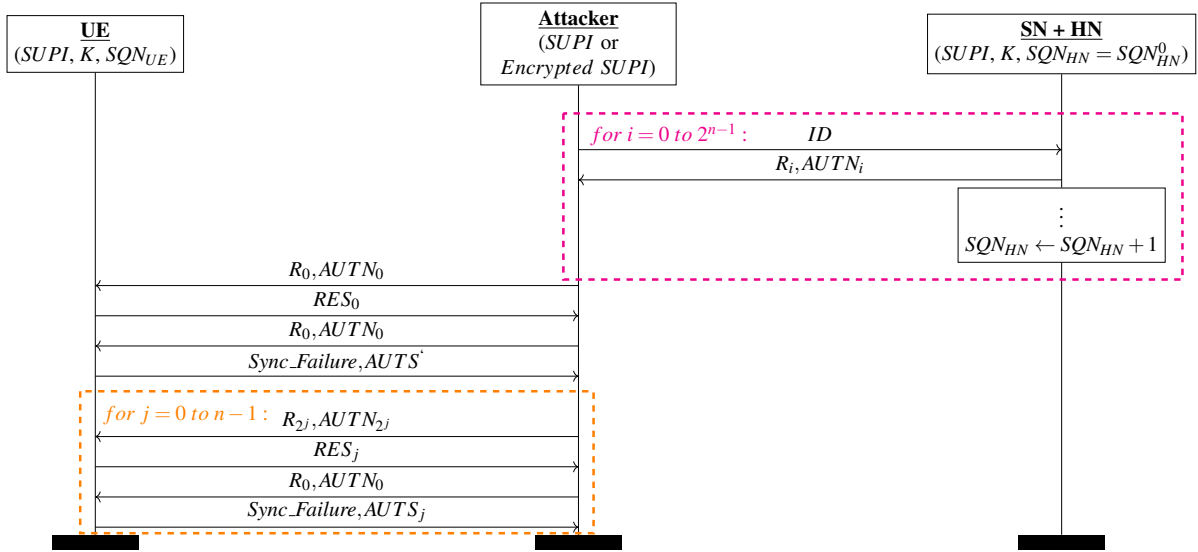


Figure 2: The online phase of the AMA.

AK^* . This value (dependent upon the lapsed time) should be small in the case of user UE_x .

3 ANALYSIS

3.1 AMA

3.1.1 Infeasible Prerequisites

As elaborated earlier in Section 2.3, to launch an AMA, the adversary first needs to compromise the target's identity and location confidentiality. While such a compromise is easy to manage in earlier generations (3G/4G) via *IMSI-catching* attacks (Fox, 2002), how this will be achieved in 5G is not clear. With a randomized public-key encryption mechanism in place to protect direct exposure of the *SUPI* during the *identification phase*, such a compromise is highly unlikely in 5G Release 15. In Section 5.2 of (Borgaonkar et al., 2019), in the case of an unknown *SUPI*, the use of *SUCI* (the randomized encryption of *SUPI*) is suggested for fetching the requisite authentication challenges from the *HN*. This would require correlating the *SUCI* to the appropriate *SUPI*, which in the case of a secure encryption scheme is not possible. The most convincing implementation of AMA in 5G would look something like this: the attacker follows the victim closely⁴ and observes the victim's attach procedure (utilizing *SUCI*) to the network. We stress

⁴In this case the *identity confidentiality* and *location confidentiality* are already compromised as the attacker can already identify the target and is aware of its location.

that all this needs to be undertaken in isolation without the presence of other mobile subscribers in the concerned attack area. Such requirement of physical tracking of the target in AMA render it unattractive for its automated use in 5G.

The prospect of the repeated use of *SUCI* for fetching of successive authentication challenges from the *HN* to launch the AMA is possible because the current identification mechanism in 5G (3rd Generation Partnership Project, 2018c) is susceptible to replay attacks. No dedicated replay prevention mechanism has been built into the 5G randomized encryption scheme used for *SUPI* protection. This was highlighted to 3GPP by the *European Telecommunications Standards Institute Security Algorithms Group of Experts* (ETSI SAGE) during their evaluation of the *SUPI* protection mechanism for 5G (ETSI-SAGE, 2017). Recently, an alternative *SUPI* protection mechanism has been proposed for 5G which prevents such *SUCI* replay attacks (Khan et al., 2018). We stress that adoption of such a mechanism will render attacks such as AMA infeasible.

3.1.2 Requesting Batch of AVs

Unlike the previous generations, Clause 6.1.3.2.0 of (3rd Generation Partnership Project, 2018c) does not support requests for issuing multiple *Authentication Vectors* (AVs) for 5G AKA. Also, after issuance of each 5G AV, the *HN* waits for a response from the *SN* after successful mutual authentication and key agreement between UE and SN as elaborated in Figure 1. Hence, the adversary has to wait for the expiration of the timeout of the currently issued AV before

the next AV issuance request can be entertained by the *HN*. This considerably increases the time complexity of AMA’s online phase in 5G.

3.1.3 The Accuracy of AMA Assumptions

Essentially AMA tries to reveal the n least significant bits of SQN_{UE} at two different time frames for the target user. Thereafter, based upon the assumption that each sequence number increment corresponds to a successful AKA session, it deduces that the difference between the two SQN_{UE} reveals the user’s service consumption during that time interval. The problem with this assumption is that the difference between the sequence numbers does not “fully” correspond to successful AKA sessions. Many times, due to network failure or channel noise (bad weather, etc), legitimate messages may get lost during transmission and may not reach the intended destination. On the other hand, it may be the case that a user is genuinely under attack by some active attacker. In such cases, the end result would be the non-utilization of the affected sequence numbers. Thus, while a difference in sequence numbers may give a rough idea about the user’s service consumption, its efficacy is dependent upon many other factors.

Another assumption that adversely affects AMA’s accuracy is the inference of SQN_{UE} from SQN_{HN} . Note that at the start of the AMA, SQN_{UE} is forced to update to the value SQN_{HN}^0 , the initial value of the SQN_{HN} . The presumption behind this step is that the two values should be equivalent, which may or may not be the case. It is quite possible (due to a variety of circumstances) for SQN_{HN} to be much higher than that of SQN_{UE} at the start of AMA. In such scenarios, AMA’s accuracy about the target’s activity gets negatively impacted.

3.1.4 Severity of AMA

In (Borgaonkar et al., 2019), it is claimed that AMA breaches subscribers’ privacy more severely than either *location confidentiality* or *identity confidentiality* attacks. This seems to be an overstatement as compromise of the permanent identity or location is arguably a more severe breach of privacy than the exposure of a number of voice calls or SMSs sent by a user. Otherwise, such a breach of privacy would have been mentioned in the official 3GPP mobile subscribers’ privacy requirements (3rd Generation Partnership Project, 2018a). In fact, breach of a user’s identity and location does not only violate the user’s privacy but can lead to physical attacks. For (a sensational) example, consider the scenario where a bomb explosion is triggered automatically when a

high value target’s presence is detected in the near vicinity by an *IMSI-catcher* (Goldman et al., 2009; Bock, 2016).

3.2 LCA

3.2.1 No Activity Monitoring

Unlike AMA, LCA does not presume any prerequisite compromises (such as identity and location confidentiality) about the target which makes it a much easier attack to launch in practice. Moreover, LCA targets location confidentiality of a user instead of its service consumption, which is a more severe breach of privacy as discussed in Section 3.1. In a way, LCA can be considered as a more direct application of the logical vulnerability of Section 2.2. Though, (Borgaonkar et al., 2019) have presented LCA as an extension of their primary attack AMA, we argue that LCA is a much more significant attack than AMA as it does not require fetching of authentication vectors from the *HN*, running of the SQN Inference Algorithm and is simple to execute. However, we stress that there is no *activity monitoring* (contrary to the claim made in the Footnote No 2 of (Borgaonkar et al., 2019)). This is because, now, what the attacker gets after a successful LCA is as:

$$CONC_{UE}^* \oplus CONC_{\gamma}^* = SQN_{UE}^{old} \oplus SQN_{UE}^{current}.$$

Note that the presumption for this is that the value $SQN_{UE}^{old} \oplus SQN_{UE}^{current}$ will be small (less than some threshold value). So there are two aspects which hinder the accurate inference of *activity monitoring*:

1. The attacker is already operating the LCA under the presumption of a small increase in SQN_{UE} which renders the aspect of *activity monitoring* ineffective.
2. Unlike AMA, in LCA the attacker is unable to extract the n least significant bits of SQN_{UE} , what the attacker actually gets are the positions of the bits of SQN_{UE} which flipped their value (either 0 to 1 or 1 to 0) hindering an accurate estimate of the difference between the two values. Nevertheless, there is some leakage from a cryptographic viewpoint.

3.2.2 No Requirement of Dedicated Fixes

Having established that LCA is not another version of AMA but rather an attack targeting location confidentiality in its own right, we turn our attention to another important dimension. All generations of mobile telephony (including 5G Release 15) suffer from an existing location attack known in the literature as *Linkability of Failure Messages* (LFM) attack (Arapinis et al.,

2012). The LFM attack exploits the fact that in case of an erroneous authentication challenge, the reason of the authentication failure gets exposed to the attacker, i.e. either *MAC_Failure* or *Sync_Failure*. This allows an attacker to link two failure messages together to identify a target user. LFM is much simpler to execute than LCA. In LFM, the attacker first observes an AKA session of the target user and records the authentication challenge ($R, AUTN$). Later, when the attacker wants to check whether another AKA session belongs to the same user or not, he replays the recorded authentication challenge and observes the type of failure message received. In case of *MAC_Failure* it is some other user, while in case of *Sync_Failure* it is the same user. Note that in LFM, unlike LCA, no further computations are required and the results are precise. Hence, it is a more devastating attack than LCA.

In (Borgaonkar et al., 2019) it is claimed that LCA will work even if LFM attack gets patched. The reason behind this claim seems to be the (erroneous) assumption that a countermeasure for the LFM attack will only hide the reason of authentication failure and not the rest of the failure message contents (including *AUTS* token) leading to the logical vulnerability of Section 2.2. However, the solutions in the literature proposing countermeasures to the LFM attack suggest otherwise. This is essentially because the indistinguishability experiments proving unlinkability in these solutions cover all aspects of unlinkability and not only the reason of the authentication failure. As a concrete example we consider the countermeasure proposed in (Arapinis et al., 2012). In case of an authentication failure (due to any reason), the whole failure message including the resync token is encrypted by the network public key. Hence, the logical vulnerability of Section 2.2 gets resolved before it can be exploited. This leads us to the deduction that in reality, LCA is a more complex version of the LFM attack. Surprisingly, in Release 15 of 5G specification, no countermeasures for this potent LFM attack have been adopted. Though the authors of (Borgaonkar et al., 2019) present LCA as a distinct attack from the LFM attack, suggesting that dedicated countermeasures independent of existing attacks would be required, it is not hard to see that a genuine countermeasure against the LFM attack will also render both AMA and LCA ineffective. This is because now the attacker will not be able to exploit the resync tokens *AUTS* to launch AMA or LCA.

3.3 The Curious Case of Out-of-Order Message Delivery

Although, there has been a number of formal analyses of the 5G AKA (Basin et al., 2018; Cremers and Dehnel-Wild, 2019) in the *symbolic model* using tools such as Tamarin Prover (Meier et al., 2013) and 3GPP has been using this approach for protocol evaluations (3rd Generation Partnership Project, 2001), the problem has always been the necessary abstraction required during the transformation from the real world conditions to the underlying mathematical model of the system being evaluated. As a concrete example, consider the case of the analysis carried out in (3rd Generation Partnership Project, 2001). Even after formal analysis, a number of vulnerabilities were later discovered in the 3G AKA. Another example is that of (Basin et al., 2018), whose analysis of the 5G AKA failed to capture the privacy flaws pointed out in (Borgaonkar et al., 2019). While the formal analysis of 5G AKA undertaken in (Borgaonkar et al., 2019) is based upon enhanced system models which consider the *AUTS* tokens of the *Sync_Failure* messages, there is an important aspect which was missed, i.e. how the 5G AKA (and the earlier AKA protocols) handle out-of-order delivery of the authentication challenges from the *HN* to *UE*.

As per 3GPP specifications (3rd Generation Partnership Project, 2018a), the mechanism in the *UE* for verifying the freshness of sequence numbers should to some extent allow the out-of-order delivery of sequence numbers. This is to ensure that the authentication failure rate due to synchronization failures resulting from such messages is sufficiently low. The standard requires that the *UE* should store in its memory the sequence numbers of a certain number of past successful authentication events. Such a mechanism ensures that a (stale) sequence number can still be accepted if it is among the last 32 sequence numbers generated (i.e. $\Delta = 32$ in Figure 1) and was not previously used. Unfortunately, the formal models of (Basin et al., 2018; Borgaonkar et al., 2019) have ignored this important aspect of sequence number freshness verification which renders their security and privacy analysis of 5G AKA imprecise.

4 CONCLUSION AND RECOMMENDATIONS

In this paper, we analyzed two recent attacks on 5G subscription privacy by (Borgaonkar et al., 2019). We established that the *activity monitoring attack* is in-

feasible in practice to be executed in 5G networks. We have also shown that the *location confidentiality attack* is trying to achieve what previous attacks in the literature have already done with much less effort and greater effectiveness. Moreover, we demonstrated that both these attacks will become void if the existing privacy vulnerability of (Arapinis et al., 2012) is fixed. Additionally, we highlighted how the history of the symbolic modeling of the AKA protocol has been plagued with serious gaps that lead to various vulnerabilities. Looking at the the results of our analysis in hindsight, it seems that the authors of (Borgaonkar et al., 2019) were overoptimistic in interpretation of their results.

Keeping in view the current development status of the 5G AKA the following recommendations are made to 3GPP:

- It is important for user privacy that 3GPP should introduce appropriate countermeasures for the *linkability attack* described in (Arapinis et al., 2012).
- Considering the aspects of protocol analysis discussed in Section 3.3, it is imperative that an all-encompassing comprehensive security and privacy analysis of the 5G AKA in an appropriate *computational model* should be carried out by a group of experts.
- To prevent any further future attacks, it is essential that the existing vulnerability of the 5G AKA *identification phase* to replay attacks be prevented. The proposal of (Khan et al., 2018) is one candidate for such a measure.

REFERENCES

- 3rd Generation Partnership Project (2001). Formal Analysis of the 3G Authentication Protocol 3GPP TR 33.902 Version 4.0.0 (Release 4).
- 3rd Generation Partnership Project (2017). 3GPP System Architecture Evolution (SAE); Security Architecture (3GPP TS 33.401 version 13.5.0 Release 13).
- 3rd Generation Partnership Project (2018a). 3G Security; Security Architecture (3GPP TS 33.102 Version 15.0.0 Release 15).
- 3rd Generation Partnership Project (2018b). Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)(3GPP TS 33.220 Version 15.2.0 Release 15).
- 3rd Generation Partnership Project (2018c). Security Architecture and Procedures for 5G Systems (3GPP TS 33.501 Version 15.0.0 Release 15).
- Arapinis, M., Mancini, L. I., Ritter, E., Ryan, M., Golde, N., Redon, K., and Borgaonkar, R. (2012). New Privacy Issues in Mobile Telephony: Fix and Verification. In Yu, T., Danezis, G., and Gligor, V. D., editors, *the ACM Conference on Computer and Communications Security, CCS'12, Raleigh, NC, USA, October 16-18, 2012*, pages 205–216. ACM.
- Basin, D. A., Dreier, J., Hirschi, L., Radomirovic, S., Sasse, R., and Stettler, V. (2018). A Formal Analysis of 5G Authentication. In Lie, D., Mannan, M., Backes, M., and Wang, X., editors, *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, CCS 2018, Toronto, ON, Canada, October 15-19, 2018*, pages 1383–1396. ACM.
- Bock, M. (2016). Simulation chamber and method for setting off explosive charges contained in freight in a controlled manner. US Patent No. 9335139, Filed September 19th., 2012, Issued May. 10th., 2016.
- Borgaonkar, R., Hirschi, L., Park, S., and Shaik, A. (2019). New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. To appear in Proceedings on Privacy Enhancing Technologies (PoPETs), Issue 3, 2019. <https://eprint.iacr.org/2018/1175>.
- Cremers, C. and Dehnel-Wild, M. (2019). Component-Based Formal Analysis of 5G-AKA: Channel Assumptions and Session Confusion. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society.
- ETSI-SAGE (2017). First response on ECIES for concealing IMSI or SUPI. <https://portal.3gpp.org/ngppapp/CreateTdoc.aspx?mode=view&contributionId=832160>.
- Fox, D. (2002). Der imsi-catcher. *Datenschutz und Datensicherheit*, 26(4).
- Geelen, A. (2019). Port of Hamburg: 5G applications pass field test. <https://www.telekom.com/en/media/media-information/archive/port-of-hamburg-5g-applications-pass-field-test-551178>. [Online; accessed 15-January-2019].
- Goldman, S. O., Krock, R. E., Rauscher, K. F., and Runyon, J. P. (2009). Mobile forced premature detonation of improvised explosive devices via wireless phone signaling. US Patent No. 7552670, Filed September 22nd., 2005, Issued Jun. 30th., 2009.
- Khan, H., Dowling, B., and Martin, K. M. (2018). Identity Confidentiality in 5G Mobile Telephony Systems. In Cremers, C. and Lehmann, A., editors, *Security Standardisation Research - 4th International Conference, SSR 2018, Darmstadt, Germany, November 26-27, 2018, Proceedings*, volume 11322 of *Lecture Notes in Computer Science*, pages 120–142. Springer.
- Meier, S., Schmidt, B., Cremers, C., and Basin, D. A. (2013). The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In Sharygina, N. and Veith, H., editors, *Computer Aided Verification - 25th International Conference, CAV 2013, Saint Petersburg, Russia, July 13-19, 2013. Proceedings*, volume 8044 of *Lecture Notes in Computer Science*, pages 696–701. Springer.
- Sustek, L. (2011). Hardware Security Module. https://link.springer.com/referenceworkentry/10.1007%2F978-1-4419-5906-5_509. [Online; accessed 08-May-2019].