Privacy of the long-term identities in cellular networks

Philip Ginzboorg
Huawei Technologies and
Aalto University, Finland
e-mail: philip.ginzboorg@iki.fi

Valtteri Niemi
University of Helsinki and
University of Turku, Finland
e-mail: valtteri.niemi@helsinki.fi

ABSTRACT

Identity and location privacy are of particular interest for mobile devices because people typically carry their mobile phone all the time and they also use the same device for a long time. Attacks by IMSI catchers have been reported in many countries. Cellular systems have had protection against passive attackers since GSM: identity confidentiality is provided by use of temporary identities that are delivered from the network to the mobile device over encrypted signalling channel. We discuss the reasons why protection against active attackers, e.g. IMSI catchers, is not provided in 3G or 4G networks. In 5G networks, the number of different kinds of heterogeneous network operators could increase, and we explain that some of these may become active or passive attackers against identity and location privacy. We show that typical protection mechanisms that have been proposed against active attackers who are outsiders would not work against these insider attackers. Then, we discuss further protection mechanisms against insider attackers and conclude that these would become too heavy for large-scale consumer networks like 5G.

Keywords

Communication system security; data privacy; encryption; identity management systems; public key.

1. INTRODUCTION

The possibility of tracking users by listening to the common control channels was well understood in the design phase of GSM (during 1980s). Therefore, a mechanism was created where a temporary pseudonym (TMSI: temporary mobile subscriber identity) is used instead of the permanent identity – IMSI: international mobile subscriber identity – for the purposes of identifying and addressing the mobile user. Once an encrypted dedicated channel is established between a particular user and the network, it is possible for the network to update the pseudonym TMSI in a secure manner.

If no temporary identity exists, identification of the mobile user has to be based on the permanent identity IMSI. This happens, for instance, in situations where a user is roaming to another country and switches the mobile device on after a long flight. Another example is an error situation where the temporary identity is somehow lost either on the user side or on the network side, or the two temporary identities are not equal anymore.

An active attacker could utilize this possibility and masquerade as the genuine network, pretending to have lost the temporary identity and asking for the permanent one from the user. This kind of attacker is called an "IMSI catcher" and actual attacks of this type have been observed in several countries recently [1].

Please note that the term "IMSI catcher" is also used in a wider meaning, referring to extended attacks, including "man-in-the-middle" type of attacks [2]. However, in this paper we consider "IMSI catchers" in the original, narrower meaning where the purpose of the attack is to "catch the IMSI," that is to obtain the long-term identifier of the mobile user.

The same mechanism that protects against passive attackers who try to break identity and location privacy in GSM has been included also in the major upgrades to the cellular networks technology: the third generation (3G) and the fourth generation (4G, or LTE) networks. However, none of these technologies provides protection against active attackers. At first sight this seems surprising because IMSI catchers were known to exist already at the time of creation of 3G technology. (The first 3G specifications were published by 3GPP: 3rd Generation Partnership Project, in the year 2000.) Actually, the concept of this kind of attacker was considered already at the design phase of GSM but it was concluded that building such a fake network element would be too complex task compared to the expected benefit for the attacker, and therefore protection against fake network elements was not included in the GSM security architecture.

One of the cornerstones in the 3G security architecture is mutual authentication that is provided by the 3GPP AKA (Authentication and Key Agreement) procedure [3]. Because of AKA, the mobile device is able to verify that it is not trying to connect to a fake network element. This procedure does not, however, protect against an IMSI catcher because the network needs to identify the mobile device be-

MOBIMEDIA 2016, June 18-19, Xi'an, People's Republic of China

DOI 10.4108/eai.18-6-2016.2264410

fore it can trigger the AKA procedure. Therefore, mobile device has to provide its identity to the network before it can verify that the network is a genuine one.

A key feature of AKA is that it tries to minimize the long distance signalling to the home network, where the mobile user has a subscription, and to reduce the number of sent messages to and from the home network. The network to

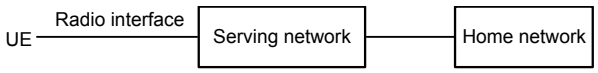

Figure 1: Schematic illustration of some cellular network concepts.

which the mobile device connects is called the "serving network." The serving network is called "visited network" when the user roams outside the coverage of his home network; otherwise the serving network is the same as the home network. Figure 1 schematically illustrates these cellular network's concepts. The UE is the "user equipment," that is the user's mobile device in 3GPP parlance.

The UE has two parts: a mobile phone or other terminal device, called "mobile equipment" (ME), and the universal subscriber identity module (USIM), which is an application that tyically runs inside a smart card. That card is called universal integrated circuit card (UICC). The operator dependent data about the subscriber is stored in the USIM. This data includes IMSI and the subscriber's master key K, which is shared with the home network.

The rest of this paper consists of six sections. In section 2 we discuss the reasons why protection against active attackers, e.g., IMSI catchers, is not provided in 3G or 4G networks. In section 3 we explain why we are concerned about attackers inside a genuine visited network in 5G. In section 4 we show how the approaches for enhancing user identity privacy outlined by 3GPP could be extended to hide user's IMSI from visited network. Section 5 describes a new attack by an active attacker in visited network. In section 6 we analyse the protection of end-user's identity privacy against passive and active attackers in the existing cellular networks and also include speculations and/or predictions for 5G. The paper concludes with a summary of our main contributions in section 7.

2. COUNTERMEASURES DESIGN IN 3GPP

Although identification has to precede authentication, this does not necessarily imply that the door for IMSI catchers is opened: the mobile device could give its permanent identity in encrypted form. Public key cryptography is an excellent tool for this kind of scenario: the mobile device could encrypt its permanent identity IMSI with the public key of the network and the network would decrypt with its private key and thus find out the IMSI.

But now we find another pitfall: the mobile device would need to obtain the public key of the network from a reliable source. It cannot just take a key given by the network because this key could be generated by the IMSI catcher itself.

This is a crucial problem in public key cryptography, and it is usually solved by introducing certificates and some sort of public key infrastructure to the system. During the time of 3G design, solution of this type was seen as too heavyweight, especially because public key technology was not needed for the AKA procedure.

Instead, a solution based on symmetric cryptography was considered. The idea was to use group keys where a group of users would use the same shared key to encrypt their IMSIs when sending them to the network. In the roaming case, the mobile device would only need to reveal the identity of its home operator and the identity of the group to the visited network. By this information, the visited network would be able to forward the encrypted IMSI to the correct home operator and the home operator would be able to decrypt it with the correct key. After this, the IMSI would be sent to the visited network, together with authentication data that is needed for running the AKA procedure.

We have a trade-off situation for the size of the group. On the one hand, if the group is too small, the group identity could be revealing too much about the user identity. For instance, it could easily be the case that at most one member of the group is roaming in a certain country at a certain time point. On the other hand, if the group is too large, then too many people would have access to the group key and the active attacker could be an insider from the group. Remember here that any mobile phone user (including the attackers) would belong to one of the groups.

This feature was called as Enhanced User Identity Confidentiality in 3GPP and it was developed into detailed stage, involving six different 3GPP working groups [4]. However, it was finally decided that the feature is not included in the first release of 3G specifications [5], [6]. One reason affecting the decision was that the possibility for other, non-IMSI related active attacks was identified during the discussions of this feature. It seemed also possible that some of these other attacks could be as easy to carry out as an attack with an IMSI catcher. One such attack that was mentioned in the discussions involved calling the victim's phone number (potentially several times) and checking whether correlated activity appears on the paging channel. (This is a broadcast channel. It carries signalling messages that include an IMSI of a specific user whose mobile device is in a power-saving mode, in order to alert that user, e.g., about incoming call.)

Introducing the feature of Enhanced User Identity Confidentiality in later releases of 3G was not seen as a tempting option either, because the IMSI catcher would of course masquerade as a network element that conforms to the first release of 3G only, and the natural requirement of backward compatibility would then guarantee that the mobile device would provide its IMSI to the active attacker.

Another aspect worth noting is that mobile devices typically support also other radio technologies in addition to cellular ones. Attacks similar to IMSI catching could also be carried out againt identities used for non-cellular radio interfaces, such as WiFi or Bluetooth addresses. Discussion about how to protect against these attacks is left out of the scope of this paper. One simple solution is to turn off these radios when

not needed but this may not be convenient for the user.

The next natural point for re-consideration of the situation appeared at the design phase of 4G (LTE) technology. (The first LTE specifications were published by 3GPP in 2008.) After considering threats, risks and costs involved with identity and location privacy it was decided that similar mechanism that was in use for GSM and 3G was sufficient for 4G also [7].

At that time 3GPP had also started standardization of machine type communications [8]. No special arrangements for identity privacy were done for that type of communication.

3. IDENTITY PRIVACY IN 5G

It is likely that the privacy of long-term user identities will be considered once again during the standardization of the next, fifth generation (5G) of cellular networks [9, 10]. Two features of 5G networks could influence these future considerations of identity privacy.

First, 5G networks are expected to be more heterogeneous than previous generations and so the trust relationships between different operators cannot simply be assumed to follow the same principles as in 3G or 4G. For example, parts of the dense 5G network coverage could be provided by city districts, or shopping malls. As another example, some physical network elements of the current cellular networks, like the LTE Mobility Management Entity (MME) that is responsible for, e.g., initial registration, authentication and paging of mobile devices, may in 5G be replaced by virtual nodes in data centers, where the same general-purpose physical equipment hosts virtual nodes of several network operators and other service providers. What makes the situation different from 3G or 4G is that we are also concerned about the genuine visited network as an attacker, which may attempt to track people, profile them, learn their secrets, and conduct billing fraud. Even a passive attacker inside the genuine visited network may obtain the long term identifier of the user from application-level data.

Second, communications with and between machines, e.g., sensors or vehicles, are expected to have a big role in 5G. The requirement for identity privacy for machines may be different than the same requirement for humans. Please note here that the identity of a gadget that is used by a person can sometimes indirectly reveal the identity or location of the owner. In this paper we do not go deeper into this direction.

Also the mobile equipment has its own identity, called International Mobile Equipment Identity (IMEI). In LTE the sending of IMEI from mobile equipment to the serving network happens after encryption in the radio interface has been turned on. (If encryption in the radio interface is not used, then identity privacy is compromised anyway.) Thus, in LTE the radio interface encryption also provides confidentiality of IMEI. In 3G the situation is different: IMEI may be transmitted in cleartext in the beginning of the radio connection. One reason for this is the fact that knowing the IMEI would help the network in handling of the particular device.

In the rest of this paper we will take a closer look at the potential issues with enhancing user identity privacy for 5G.

4. TWO EXAMPLES OF ENHANCING USER IDENTITY CONFIDENTIALITY

The 3GPP report TR 33.821 [7], created during the design of 4G security, outlines two main solution types for enhanced user identity confidentiality: pseudonym-based approach and public key-based approach. We will now give one example of each approach. In contrast to [7], our examples have been devised in order to provide protection also against attackers inside the genuine visited network. Many details have been simplified in the examples but they should still help us in understanding issues that may typically appear with the two approaches.

The design goals in both examples are:

1. First, IMSI is never sent as cleartext on radio interface between the UE and the serving network. This is because we want to protect user identity privacy from outsider attackers.
2. Second, the principles of the cellular authentication and key agreement procedure (AKA) are still followed. The reason for this goal is that the AKA has been well tested by time and it would provide backwards compatibility.
3. Third, the serving network never gets the cleartext IMSI. This is because we would like to protect user identity privacy also against attackers inside the serving network.

It is clear that all designs to enhance user identity confidentiality should have (1) as a goal. Using public-key cryptography instead of adhering to AKA principles (goal 2) was discussed in 3GPP already during 3G design phase. This question should be re-considered for 5G but, anyway, approaches to enhance user identity privacy in both of our examples would still be valid in modified form even if AKA would be abandoned in favor of public-key based authentication.

Designs that intend to protect the long-term user identity on the radio interface (goal 1), while also concealing the long-term identity of the user from serving network (goal 3) have been proposed in the literature. For example, in the scheme of G. Yang et al. [11] the UE first authenticates directly with the home network in a manner that is opaque to the serving network. If that authentication succeeds, then the home network sends a pseudonym both to the UE and to the serving network. However, the design of [11] breaks the principle of cellular AKA, where the UE does not talk directly to the home network authentication servers: UE talking directly with the home network authentication servers would increase the potential of Denial of Service (DoS) attacks and the amount of long-distance signalling.

There was already a substantial amount of work in the academic community in 1990s about providing location privacy in mobile networks in such manner that not even the serving

network is able to track users [12]–[16]. However, all these proposed mechanisms would imply significant architectural changes in how mobile networks work.

One reason why it is useful to maintain AKA is the following. Due to mobility of the UE, the radio interface between the UE and the serving network's base station is unstable, compared to the communication link between the serving network and the home network. When UE authenticates directly to the home network servers, this instability may result in frequent authentication failures that must be handled somehow by the remote servers in the home network. On the other hand, by adhering to cellular AKA principles, the local authentication failures due to problems of the radio interface can be resolved locally in the serving network.

Before going into the examples, we illustrate the steps leading to the cellular AKA procedure in Figure 2, and provide detailed descriptions of the steps (similarly as we do later in the examples). This hopefully helps the reader to compare our example designs with current state-of-the-art.

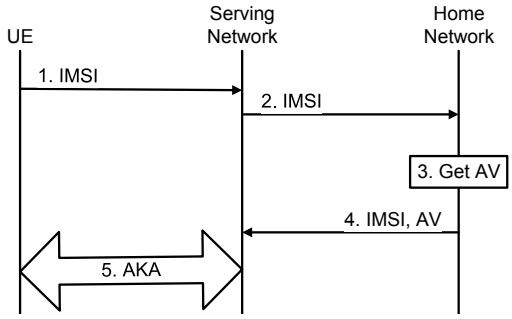

Figure 2: Illustration of the steps leading to the cellular Authentication and Key Agreement (AKA) procedure.

1. The unauthenticated UE sends its long-term identity IMSI to the serving network. The first three to five digits of IMSI point to the country and the home network of the subscriber.

2. The serving network forwards IMSI to the home network.

3. The home network finds, based on IMSI the master key K of the subscriber and computes the authentication vector AV for that subscriber.

4. The home network sends IMSI and the authentication vector AV to the serving network.

5. The serving network runs the cellular AKA procedure with the UE using the received AV. After the procedure the serving network allocates a local temporary identity for the UE. In all subsequent communications with the UE temporary identity would be used instead of IMSI.

In the non-roaming case the serving network is the same as the home network, hence in steps (2) and (4) we have communication between network elements belonging to the same network.

The serving network would use the long-term identity IMSI in subsequent communications towards home network, e.g., for the purpose of charging and updating the location of the UE. The home network would similarly use IMSI in communication towards serving network, e.g., for the purpose of directing incoming calls.

4.1 Example of pseudonym-based approach

In this example it is required that: (i) the UE has initially received a pseudonym (temporary identity) from the home network; (ii) given a pseudonym, the home network can efficiently find the corresponding permanent identity (IMSI) of the subscriber; and (iii) the UE pseudonym is periodically refreshed by the home network. When the UE joins the serving network the current UE pseudonym will be used in the following manner, that is schematically illustrated in Figure 3.

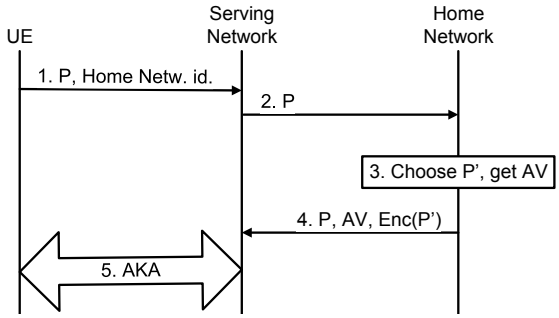

Figure 3: Illustration of the pseudonym-based approach for enhancing user's privacy.

1. The unauthenticated UE sends its temporary identity (pseudonym) P and the identity of the home network to the serving network.

2. The serving network forwards P to the home network.

3. The home network first finds, based on the pseudonym P, the permanent identity (IMSI) and the master key K of the subscriber. Then it computes the authentication vector AV, chooses the next pseudonym P' for that UE and encrypts the new pseudonym with the key K (or some key derived from K). The next pseudonym is intended to be used when the UE joins another serving network.

4. The home network sends P, the authentication vector AV and the encrypted next pseudonym P' to the serving network.

5. The serving network runs the cellular AKA procedure with the UE using the received AV. During the procedure it also forwards the encrypted next pseudonym P' to the UE and allocates a local temporary identity for the UE. The temporary identity would be used in all subsequent communications with the UE. If allocation of the temporary identity somehow fails then the pseudonym P would be used with UE. Also, if AKA fails, then P would be used in error messages. If there is a need to page for the UE and the temporary identity is not available, then P would be used.

Similarly as above, in the non-roaming case steps (2) and

(4) consist of intra-network communications.

After a successful authentication the old pseudonym P will still be used in place of permanent identity IMSI by the current serving network, for example, in paging messages, and in subsequent communications between home network and serving network. The identity P' comes into play in the next serving network. Therefore, the UE is identifiable by P as long as it stays in the same serving network.

The pseudonym could be in form similar to IMSI, where the first three to five digits point to the country and the home network of the subscriber. In this option, in place of the long-term Mobile Subscriber Identity Number (MSIN) there is a randomly chosen number.

Summarizing, in this example design we have added the concept of state in order to protect privacy. The main issue with this approach is the need to have the same value of the pseudonym P in both the UE and the home network. Keeping synchronized state (with time stamps, dynamic data, etc.) in a large distributed system can be costly in terms of memory and communication resources. Also, it needs to be specified how to recover from error situations, where the synchronization is lost. Of course, the whole feature would be next to useless if the recovery mechanism could be exploited by an active attacker.

Another type of issue is caused by the natural requirement of backward compatibility: a mobile device, or network that supports new generation technology should also interwork with the technology of the older generation. Therefore, it is important that the pseudonym mechanism could work even when the serving network is not aware of existence of such mechanism. Otherwise, the mobile device would be forced to use plain IMSI in that network, and an active attacker would have a chance to catch the IMSI by pretending to be such serving network.

For these reasons it is desirable that the pseudonym looks exactly like a legitimate IMSI to the serving network. This in turn creates pressure inside the number space of IMSIs, because the number of pseudonyms must be many times bigger than the number of real IMSIs.

Detailed proposals have been presented about how to use IMSI format for pseudonyms [17, 18]. These proposals have the big advantage that it would be possible to introduce them also for legacy networks, since changes would only be needed in the USIM and in the home network. (The affected part in the home network is the home subscriber system, HSS). Since changes on the user side are restricted to the USIM, it would even be possible to introduce protection to legacy terminal devices.

One caveat for 3G networks is the fact that the identity of the device itself, i.e. IMEI, may be sent in cleartext. Introduction of pseudonyms for IMEIs is also possible in theory, but this would bring in complications because of the following reasons: (i) IMEI number space is allocated to device manufacturers, not to operators; (ii) sometimes operators adjust the network's behavior based on parts of IMEI (like the identity of mobile device manufacturer); and (iii) IMEI may be used to track stolen devices.

But another, and perhaps more likely scenario is, that users would upgrade their terminal devices while the pseudonym-based identity protection mechanims is developed and deployed. Then it would also be possible to manage pseudonyms (with IMSI format) completely in the ME; and legacy UICCs would be sufficient to support the mechanism. If this solution is introduced, there is a need to somehow inform the ME about using pseodonym IMSIs. This could be done by the Authentication Management Field (AMF) in the AKA procedure. A precedence of this approach was established during LTE standardization, when one bit of AMF field was chosen to indicate whether authentication vector AV was created for LTE or not.

It is also possible to support both USIM-based and ME-based solutions at the same time. This would imply that is is sufficient to upgrade either UICC or ME.

4.2 Example of public-key based approach

During the radio connection establishment, UE encrypts its long-term identity with the public key of the home network (which we assume the UE knows), and sends the resulting ciphertext to the serving network, together with the identity of the home network. The steps are listed below and illustrated in Figure 4.

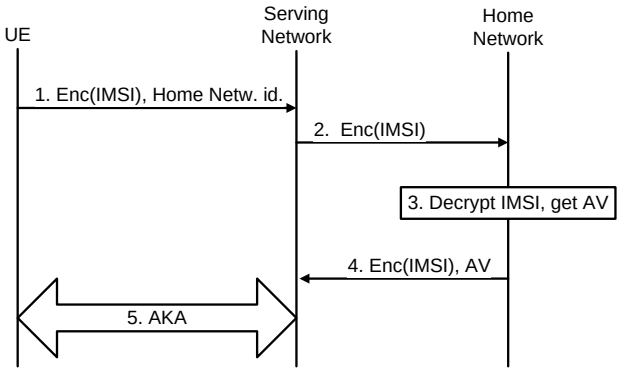

Figure 4: Illustration of the public-key based approach for enhancing user's privacy.

1. UE sends to the serving network the public identity of the home network, and the ciphertext Enc(IMSI), which is the long-term identity IMSI of UE encrypted with the public key of home network. We assume here that the public key of home network is stored in the UE. We also assume that encryption is randomized, i.e. IMSI would be encrypted differently each time.

2. Serving network looks at the home network identity and forwards ciphertext Enc(IMSI) to the home network.

3. Home network decrypts the ciphertext in the message with its private key, finds the long term subscriber identity IMSI; and gets the authentication vector for this IMSI from the home subscriber system (HSS).

4. Next the home network sends back to the serving network the authentication vector AV together with Enc(IMSI).

5. The serving network and UE run the cellular AKA procedure between them. During this procedure the serving network also allocates a local temporary identity for the UE. The temporary identity would be used in all subsequent communications with the UE. If there is a need to communicate with the UE when temporary identity is not yet available, e.g., for AKA error message or paging, then Enc(IMSI) is used. The identity Enc(IMSI) would be used also in subsequent communications between home network and serving network.

Similarly to the previous example, in the non-roaming case, the serving network is the same as the home network, hence in steps (2) and (4) we have intra-network communication.

On the one hand, and in contrast to the pseudonym-based approach, this design does not require the home network to maintain synchronized state information between UE and the home network about short-term identity with the UE.

On the other hand, the issue of backward compatibility is even more severe than in the pseudonym-based approach, because a ciphertext encrypted by any of the established public key methods is longer than the length of IMSI. Therefore, an encrypted IMSI cannot look like a cleartext IMSI. There are also other potential issues.

One issue is the need for supporting infrastructure to distribute securely the public key of home network to the UE. A straight-forward solution is to pre-install the public key into all smart cards that are distributed to the subscribers. However, this solution does not enable refreshing of the key. For this purpose, the home network could distribute the public key to his subscribers over-the-air using an application in the card.

Another issue is the computational load and need for additional crypto-elements in the home network servers. The load created on the home network servers by the decryptions in step (3) depends on several factors: the choice of the public key cryptosystem together with its configuration (like the key size), and the amount of traffic towards home network servers.

In our scenario the public key operation happens when UE is encrypting its IMSI, and the private key operation happens when the home network server decrypts the encrypted IMSI. In the RSA cryptosystem, the public key operation is significantly faster than the private key operation, while in the elliptic curve cryptography (ECC) there is no significant difference between the two. Partially because of this reason, the load on the home network server will be less when ECC is used to hide the IMSI, instead of RSA. Therefore, it seems sensible to use ECC in our scenario. Still, computational load with ECC decryption is much higher than computational load of decryption with symmetric encryption schemes, at a given level of security.

Summarizing both examples, user identity privacy can be enhanced with a few simple modifications to the steps that lead to cellular AKA in Figure 2. Still, our above example solutions in Figures 3 and 4 are not light-weight. The pseudonym-based approach requires keeping synchronized state in a large distributed system. The public key-based approach needs support infrastructure for public key distribution and additional crypto-elements in the home network servers.

5. IDENTITY-PROBING ATTACK FOR A CHOSEN TARGET

The result of enhancing user identity confidentiality based on one of the approaches that were outlined in the previous section, is that IMSI is never visible in the signalling messages that are exchanged over the radio interface. But, as mentioned earlier in the section about 3GPP countermeasures, there are also attacks against identity confidentiality of mobile users that are not related to IMSI. Let us take a closer look and start by assuming that the attacker can (i) contact a target user based on the public identity of the latter (like the public phone number), and (ii) observe all radio interface signaling in the target area. The combination of (i) and (ii) enables the following chosen-target attack.

The attacker who suspects that the user Bob is in the target area, looks up Bob's public phone number and calls (as another user) to that number (or tries to create a connection to Bob's phone by some other means, e.g. messaging). If at that time Bob's mobile phone is connected to the serving network in the target area then the signaling messages will point to Bob's mobile phone.

Please note that there may be several mobile devices that are receiving a suitable signaling simultaneously with attacker's call. But the attacker can wait a bit and call Bob again. Note also that the attacker should stop each of its calling attempts as early as possible, preferably so that no "missed call" is visible in Bob's phone. After this operation is repeated sufficiently many times, the attacker gains confidence on either that Bob is in the area or that he is not there. If each of the calling attempts causes paging with some common element, e.g., Bob's temporary pseudonym, then confidence can be gained with fairly small number of attempts. Indeed, if Bob is not in the target area then it is highly likely that the set of pseudonyms that appear immediately after the first call attempt is disjoint from the set of pseudonyms appearing immediately after the second call attempt; and as long as Bob is in the target area, each set of pseudonyms that appear after a calling attempt contains at least one common element: Bob's pseudonym.

If paging is arranged so that repeated attempts to call to the same number do not cause paging with a common element, e.g., user follows many different pseudonyms simultaneously, then the increase of signaling after each calling attempt has to be observed statistically. Even in this case, a reasonable amount of calling attempts would reveal whether Bob's phone is in the target area or not.

The identity-probing attack against LTE mobile phones by an active outsider attacker (which is not part of a legitimate LTE network), has been implemented by Borgaonkar et al. [12]. Facebook and WhatsApp identities were used for sending messages to the target user. By monitoring the

implied signalling it was possible to locate the target user with the accuracy of two square kilometers.

Combating these attacks may be tried by somehow removing the premise (i) and/or (ii). For instance, the paging signaling may be somehow hidden in the radio traffic, hence removing (ii). This may be tried with mixing, random delays and adding fake signaling messages. But it is hard to do this effectively and efficiently in large consumer networks.

Removing premise (i) is also difficult because an adversary who wants to attack against a chosen target, typically has quite a lot of information about the target already. But, it may be possible to avoid (i) in some niche areas, e.g., in military communications. Still, even if (i) or (ii) could be removed in the case of an outsider attacker, an insider who has access to the serving network from inside can carry out an attack similar to that described above.

Let us next take a closer look at a scenario where the attacker is inside a genuine serving network.

The insider attacker's main advantage over outsider attackers is that he can both observe and control the signalling messages in the serving network. We also assume that the attacker knows Bob's identity in a form that is recognizable by Bob's home network so that he can call Bob.

We will now illustrate how these could help the attacker. Let us initially assume that like in today's cellular networks, the identifier of the caller is visible in the signalling messages that enter into the serving network.

Similarly to an outsider attack described above, an active attacker inside the serving network who suspects that a target user Bob is in his serving network could make a call towards Bob.

After placing the call to Bob the insider attacker would match the caller's identifiers in all signalling messages related to incoming calls in the serving network with his own identity as a calling party. If there there is a match, then the attacker would know the called party (i.e. Bob's) identity in the serving network, and he would also be able to track Bob's movements while Bob stays in the serving network. Moreover, after recognizing himself as a calling party, the attacker can also prevent all signalling messages that are related to his call from reaching Bob's UE. As a result, Bob would remain completely unaware of the identification attempt.

We could try to mitigate this attack by hiding the calling party (including the identity of the network where the call originates) from the serving network. This could be done, e.g., by adding a new layer of encryption (for identity of the calling party) between the home network and the end user. Consequently, a significant amount of complexity would need to be added to the identity privacy solution. Note that the calling party identity would need to be hidden from the serving network both when the roaming user is the called party and when the roaming user is the calling party.

But even with calling party hidden, the insider attacker can still use the times of arrival of signalling messages to carry out this sort of attack. Repeating the same procedure for a few times would reveal whether the signalling is indeed related to Bob and not to some other user.

In order to mitigate timing analysis by the serving network, we could, for example, introduce time jitter into signalling traffic between different networks (in addition to hiding calling parties from the serving network). But if we do so, then the increased randomness in the times of arrival of signalling messages means that the response time of the network becomes less predictable. This, in turn, would degrade the performance of interactive applications, like voice calls, video calls and text chat. All in all, artificial time jitter is likely to impact negatively on the end users' experience with those applications.

Summarizing, these countermeasures against insider attackers seem to make the privacy solution far too heavy for applying in large-scale consumer networks.

It should be noted that our example solutions for enhancing user identity privacy, described in the previous section and illustrated in Figures 2 and 3, will still protect from passive insider attacker. This sort of attacker would look at the logs of signalling and data traffic in his network, but he would not make fake call attempts to the target.

The conclusion from our analysis of the active insider attack is that complete hiding of the IMSI from insider attacker in the serving network should not be required from enhanced user identity confidentiality solutions in 5G.

6. ANALYSIS

The protection of end-user's identity privacy in the existing 2G, 3G and 4G systems is summarized in Table I. The table also includes predictions and/or recommendations for 5G.

Table 1: Existence in cellular networks of protection measures against different types of attacker.

Attacker type		2G	3G	4G	5G
Outside the serving network	Passive	Yes	Yes	Yes	Yes?
	IMSI catcher	No	No	No	?
	MitM	No	Yes	Yes	Yes?
Serving network is attacker	Passive	No	No	No	?
	Active	No	No	No	No?

It is sensible that identity privacy for human subscribers in 5G will be at least as good as in 4G. This implies that we should have "Yes" in 5G column of Table I in all rows where there is "Yes" already for 4G. It should be noted, however, that the identity privacy protection for machine communication, e.g., between very simple devices, like sensors, may be different than for human subscribers.

Another observation is that there may be pressure on the industry from the public to enhance user's privacy in future mobile networks. It is likely that this issue will be raised during 5G standardization. This may imply that protection against active IMSI catcher is needed in 5G, and so there is a question mark "?" the second row of the 5G column.

We have shown that the enhancements to the identity confidentiality based on cryptographic techniques could be made effective against passive attackers. This is true for both outsider and insider (inside the visited network) attackers. However, a significant complexity is introduced by these solutions. Thus, "?" is in the fourth row of 5G column. In other words, we leave it open whether some of the solutions are light-weight enough to justify their inclusion in 5G.

But, even with these enhancements implemented, an active attacker inside the visited network may still find a long-term identity of a person by identity probing. For that reason there is "No?" in the last row of the 5G column of Table I. In other words, none of the solutions planned against IMSI catchers can stop visited network as an active attacker.

7. CONCLUSION

We conclude the paper with a list of its three main points.

1. First, we have shown how the approaches for enahcing user identity privacy in 3GPP TR 33.821 [7] could be extended to hide user's IMSI from visited network.

   Actually, the scope of this protection is broader, because the same protection could be used in situation where the serving network is same as the home network, and the passive attacker is inside the radio access network or in the core network, but not in the home subscriber system (HSS).

   Moreover, we discuss how pseudonym-based mechanisms can be arranged with legacy UICC and legacy serving network.

2. Second, we have outlined a new simple attack by an active-insider attacker in the visited network. It seems that the known solutions and extensions mentioned above in (1) would not protect against this attack. Even though further countermeasures to this attack could be devised, they would be too heavy to apply in large-scale consumer networks. This means that while hiding user's IMSI from visited network may help to protect user's privacy from passive insders in that network, it cannot fully protect user's privacy against active insider attackers in visited network.

3. Third, the finding of (2) impacts on 5G security requirements: complete hiding of the IMSI from active-insider attacker in the visited network should not be required from enhanced user privacy solutions.

8. ACKNOWLEDGMENTS

This work was supported by TEKES as part of the 5th Evolution Take of Wireless Communication Networks (TAKE-5) project, and the Internet of Things program of DIGILE (Finnish Strategic Center for Science, Technology, and Innovation in Digital Business).

9. REFERENCES

[1] A. Soltani and C. Timberg, "Tech firm tries to pull back curtain on surveillance efforts in Washington," *The Washington Post*, Sept. 17, 2014.

[2] A. Dabrowski., N. Pianta, T. Klepp, M. Mulazzani, E. Weippl, "IMSI-Catch Me If You Can: IMSI-Catcher-Catchers," Proceedings of Annual Computer Security Applications Conference (ACSAC 2014), New Orleans, LA, USA, December 2014, pp. 246-255.

[3] 3GPP TS 33.102, 3G security; Security architecture, v. 12.2.0.

[4] 3GPP TS 33.102, 3G security; Security architecture, v. 3.4.0.6.

[5] 3GPP, Liaison Statement concerning Enhanced User Identity Confidentiality (EUIC) status (24 February 2000), SP-000006.zip. `http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_07/Docs/PDF/SP-000006.pdf`

[6] 3GPP, Report of TSG SA Plenary Meeting #7 - version 1.0.0, `http://www.3gpp.org/ftp/tsg_sa/TSG_SA/TSGS_07/Report/SP_07_Approved_Rep_v100.pdf`

[7] 3GPP TR 33.821, Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE), v. 9.0.0.

[8] 3GPP TS 33.187, Security aspects of Machine-Type Communications (MTC) and other mobile data applications communications enhancements, v. 12.2.0.

[9] D. Warren, H. Yang, J. Albares, E. Balestra, S. Burcher, M. Bloxham and W. Bocquet, "Understanding 5G: Perspectives on future technological advancements in mobile," GSMA Intelligence Report, Dec. 2014.

[10] NGMN Alliance, "NGMN 5G White paper," editors J. Erfanian and B. Daly, February 2015.

[11] G. Yang, D.S. Wong, X. Deng, "Anonymous and Authenticated Key Exchange for Roaming Networks," IEEE Tran. Wireless Comm., vol. 6, No. 9, Sep. 2007, pp. 3461-3472.

[12] H. Federrath, A. Jerichow, D. Kesdogan, A. Pfitzmann, "Security in Public Mobile Communication Networks," Proceedings of the IFIP TC 6 International Workshop on Personal Wireless Communications, 1995, pp. 105-116.

[13] D. Kesdogan, X. Fouletier, "Secure Location Information Management in Cellular Radio Systems," Proceedings of IEEE Wireless Communication System Symposium 95, Long Island, 1995, pp. 35-46;

[14] H. Federrath, A. Jerichow, A. Pfitzmann, "Mixes in mobile communication systems: Location management with privacy," in R. Anderson (Ed.): Information Hiding, LNCS 1174, Springer, Berlin 1996, pp. 121-135.

[15] D. Kesdogan, H. Federrath, A. Jerichow, A. Pfitzmann, "Location management strategies increasing privacy in mobile communication," in S. K. Katsikas, D. Gritzalis (Ed.): Informations Systems Security, IFIP SEC '96 Conference Committees, Chapman & Hall, London, 1996, pp. 39-48.

[16] D. Kesdogan, P. Reichl, K. Junghärtchen, "Distributed Temporary Pseudonyms: A New Approach for Protecting Location Information in Mobile Communication Networks," in Proceedings of European Symposium on Research in Computer Security (ESORICS 1998), LNCS 1485, Springer Berlin 1998.

[17] F. van den Broek, R. Verdult, and J. de Ruiter, "Defeating IMSI Catchers," in Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS 2015). ACM, New

York, NY, USA, pp. 340-351.

[18] M. S. A. Khan and C. Mitchell, "Improving Air Interface User Privacy in Mobile Telephony," in Proceedings of second Security Standardisation Research conference (SSR 2015), Tokyo, Japan, December 15-16, 2015, pp. 165-184.

[19] R. Borgaonkar, A. Shaik, N. Asokan, V. Niemi and J. P. Seifert, "LTE and IMSI catcher myths," Blackhat Europe 2015, Amsterdam, The Netherlands, Nov. 2015.