Protecting IMSI and User Privacy in 5G Networks

Karl Norrman
Ericsson Research
Ericsson AB
Stockholm, Sweden
karl.norrman@ericsson.com

Mats Näslund
Ericsson Research
Ericsson AB
Stockholm, Sweden
mats.naslund@ericsson.com

Elena Dubrova
School of ICT
Royal Institute of Technology
Stockholm, Sweden
dubrova@kth.se

ABSTRACT

In recent years, many cases of compromising users' privacy in telecom networks have been reported. Stories of "fake" base stations capable of tracking users and collecting their personal data without users' knowledge have emerged. The current way of protecting privacy does not provide any protection against an active attacker on the air-interface, claiming to be a legitimate network that has lost the temporary identity. Moreover, there is also no protection against passive eavesdroppers who are present when requests for International Mobile Subscriber Identity (IMSI) are made. This paper presents a new method for protecting the IMSI by means of establishing a pseudonym between the user equipment and the home network. The pseudonym is derived locally at the user equipment and the home network without affecting existing Universal Subscriber Identity Modules (USIMs). We analyse the solution from a technical perspective, as well as from a regulatory and operational perspective. The presented method protects the IMSI from passive and active IMSI-catchers as well as honest but curious serving networks. Moreover, it can recover from lock-out situations where one party has lost the pseudonym.

CCS Concepts

•Security and privacy → Pseudonymity, anonymity and untraceability; Privacy-preserving protocols; Security protocols; Mobile and wireless security; Privacy protections; •Networks → Network protocol design;

Keywords

Privacy; user identifiers; IMSI catching; fake base station; 5G

1. INTRODUCTION

In recent years, many cases of privacy-related attacks on networks supporting the operation of mobile communications systems have been reported. For example, attackers have obtained an access to *Signaling System 7* (SS7) networks and, by using that access, obtained subscribers' precise geographical location [26]. Other cases of actively compromising nodes in the mobile network core and using fake base stations have also been reported, including [29, 17, 27].

In this paper, we focus on *IMSI-catching* attacks that aim at obtaining the *International Mobile Subscriber Identity* (IMSI) of a mobile subscriber, e.g., for tracking purposes. The IMSI-catcher, in the simplest form, requests the long-term subscriber identity from a mobile device. Since this is a valid request in normal operations, the mobile device replies with its IMSI according to standard protocols. The IMSI-catchers can be used, for example, to monitor who is moving in a certain area [14], or to track which locations a given subscriber is visiting [33, 28, 34]. In addition, more advanced IMSI-catchers can eavesdrop on the traffic to and from the mobile device [18, 25]. Current mobile broadband standards do not address threats from IMSI-catchers. This problem is non-trivial since the IMSI requests may occur when there is no security context available to cryptographically protect the request.

A current solution for protecting subscribers' identity is based on a serving network assigning a randomly generated *Temporary Mobile Subscriber Identity* (TMSI) to the mobile device at regular intervals. The long-term IMSI is used only as a fault recovery mechanism and when a TMSI has not yet been assigned. The recovery mechanism is needed to avoid lock-out of a mobile device when errors occur, e.g., when the serving network or the mobile device has lost the TMSI. The mobile device falls back to using the IMSI whenever the serving network requests. This recovery mechanism is what IMSI-catchers exploit to obtain the IMSI from the mobile devices. Hence, the current way of protecting privacy does not provide any protection against an active attacker on the air-interface, claiming to be a legitimate network that has lost the temporary identity. Neither is there any protection against passive eavesdroppers who are present when IMSI requests are made.

During the initial phases of *Universal Mobile Telecommunications System* (UMTS) and *Long Term Evolution* (LTE) standardization, some enhanced long-term identity protection mechanisms were discussed. Three options were considered: (1) encrypting IMSI using a public key of the serving network, (2) encrypting IMSI using a shared group key, and (3) authenticating IMSI requests by the network.

The first option of encrypting IMSI using a public key of the serving network was eventually dismissed due to the

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

DOI 10.4108/eai.18-6-2016.2264114

complexity of managing the *Public Key Infrastructure* (PKI) and the limited processing power for of mobile devices that existed at the time. Further, this option may not protect against malicious insiders, e.g., from a roaming partner who could see a business case in extracting and selling information related to the location of mobile devices.

The second option of encrypting IMSI using a shared group key does not prevent other mobile devices, who also know the group key, from obtaining the IMSI.

The third option, the authenticating IMSI requests by the serving network, does not protect against passive (eavesdropping) attackers and shares the complexity issues related to PKI with the first option.

The traditional trust model for 3GPP mobile networks assumes that anyone with access to the roaming interconnect network is trusted to behave well. Consequently, nodes in one network can request sensitive information from nodes in other networks, which is necessary for normal operations. This trust model was designed in a time when the operators were few, large, and depended heavily on each other. Breaching the trust of others in such a setting could lead to severe consequences. Therefore, this walled-garden trust-model worked well. However, as time passed, the number of operators rapidly grew, adding new smaller operators as well as other actors to the interconnect networks. This led to that trust in other actors remained the same, but the basis for that trust in some cases had eroded. As is evident from various attacks [15], this trust model no longer match reality. Further extrapolating from the current situation, and taking into account that with 5G even coffee shops and galleries might act as serving network operators, the number of operators will continue to grow and new, unconventional actors may need to be part of the walled-garden. This motivates a need for subscriber privacy enhancements for mobile broadband systems that reduce or eliminate the necessity to trust other agents connected to the interconnect networks.

The rest of the paper is organized as follows. Section 2 provides background information. Section 3 describes the presented enhancements. Section 4 reviews the previous work. Section 5 concludes the paper.

2. BACKGROUND

We now describe the 3GPP architecture and trust model as well as how mobile devices are identified and authenticated in this context. We then explain how this setting has made it possible for IMSI-catchers to breach user privacy.

2.1 Communication network

The architecture and trust model is the same for all 3GPP networks for the aspect we consider, albeit with slightly differently named network elements (see Fig. 1). For simplicity, we will use terminology from the LTE standard [2]. The LTE network provides wireless access and mobility services to mobile devices, which are called *User Equipment* (UE). To this end, the LTE network is divided into multiple domains. On the highest level there is a *home network* and a *serving network*. The home network is controlled by the operator with which the user has a subscription, and the serving network, which may be controlled by a different operator, provides the actual connectivity and mobility services. The home network contains a *Home Subscription Server* (HSS), which holds a database of all the operator's subscribers, and interfaces through which the serving network can obtain authentication and other subscriber related information. The serving network authenticates the UE before granting it service. More specifically, the serving network authenticates a *Universal Subscriber Identity Module* (USIM), hosted on a smart-card inserted in the mobile device. The authentication is executed by the *Mobility Management Entity* (MME), which resides in the *Core Network* (CN) of the serving network. The wireless access service is provided via a base station (called eNB) in the *Radio Access Network* (RAN) that is connected to the CN.

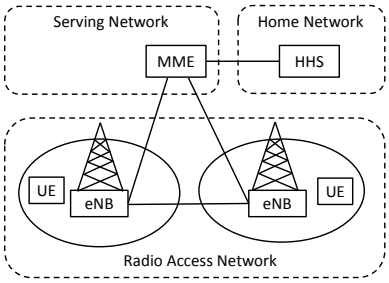

Figure 1: General architecture of a basic LTE network; UE is a User Equipment; eNB is a base station; MME is a Mobility Management Entity; HSS is a Home Subscriber Server

From a business perspective, the serving network needs assurance that the UE accessing the service can be fairly charged. The subscription authentication procedure meets this need by ensuring that the UE requesting access can be securely associated with the authentication information that the serving network obtained from the home network of the UE.

The home network operator trusts the serving network operator to authenticate the UE using authentication information that the home network provides. Note that the home network operator does not trust the serving network operator with the actual long-term credential for authentication. Instead it trusts the serving network operator with one-time authentication information usable for authentication and session key generation. The home network operator also trusts the serving network operator to provide correct charging information related to the services used by the UE according to the roaming agreements between the two operators. The serving network operator trusts that the HSS in the home network provides authentication information that can authenticate a unique UE associated with that HSS.

2.2 Identification and Authentication

Authentication credentials and other subscriber data is identified in the HSS by the subscriber's *International Mobile Subscriber Identity* (IMSI). IMSI is a unique, usually 15-digit, number provisioned in a USIM [1]. It consists of the *Mobile Country Code* (MCC), *Mobile Network Code* (MNC), and *Mobile Subscription Number* (MSIN). Together, the MCC and MNC identifies the home network and the MSIN identifies the actual subscriber in that home network.

Once the MME has authenticated the UE, the MME assigns a temporary identifier TMSI to it, for the purpose of user privacy. This TMSI is then used by the MME and UE when they need to transmit an identifier for the UE in further communication. The TMSI can be updated at regular

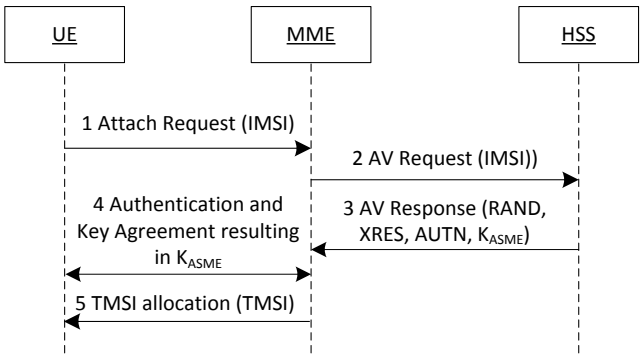

Figure 2: A simplified message sequence chart of AKA preceded by the UE identifying itself to the MME, and followed by the MME assigning a new TMSI to the UE.

intervals.

LTE uses a three-party protocol for subscription authentication and session key establishment called *Authentication and Key Agreement* (AKA) (see Fig 2). The basis for AKA is the symmetric key K and the corresponding IMSI shared by the USIM and the HSS. While 3GPP systems use two different versions of AKA, one originated with GSM and the other was introduced with UMTS, we will, without loss of generality, consider only the latter. It provides mutual authentication and it is the only allowed version for LTE, whereas GSM and UMTS allow both versions of AKA. The three parties involved in AKA are the HSS, the MME and the USIM card inserted in the UE. Upon successful completion of AKA, the MME considers the USIM authenticated. Implicitly, the MME then also considers the entire UE and the subscriber authenticated.

Before AKA is initiated, the UE provides the IMSI to the MME. Alternatively, if the UE has been assigned a TMSI, this identifier is used instead of the IMSI. In this case, the MME resolves the TMSI into the corresponding IMSI. Once the MME has the IMSI, the MME requests authentication information from the HSS in the home network. This authentication information is returned by the HSS in the form of a tuple ($RAND$, $XRES$, $AUTN$, K_{ASME}), where $RAND$ is a challenge for the UE, $XRES$ is the expected response to the challenge, $AUTN$ is a network authentication token, and K_{ASME} is the session key corresponding to the challenge. The tuple is referred to as an *Authentication Vector* (AV). MME forwards the $RAND$ and $AUTN$ to the UE, who in turn forwards these to elements to the USIM. The USIM verifies that the $AUTN$ is correct and fresh. If the verification fails, the USIM rejects the authentication. Otherwise, the USIM calculates the session key K_{ASME} and makes it available to the UE together with the response RES to the $RAND$. The UE sends the RES back to the MME, which can compare it to the expected response $XRES$ from the authentication information received from the HSS. We will omit the details of the authentication protocol that are not related to the privacy aspects of the IMSI.

2.3 IMSI Catching

IMSI catching is an attack aiming to reveal the identity of a user by catching the IMSI of the users UE [30]. The attack is based on the fact that the UE will fall back to using the IMSI as its identifier when there is no TMSI available. This may happen because of, e.g., MME or UE deleted the TMSI due to timeout.

The IMSI catching attack can be done passively or actively. A *passive* IMSI-catcher eavesdrops on the wireless traffic in its neighborhood and collects all IMSIs captured. The coverage area of the IMSI-catcher is dependent on receiver/antenna technical properties. If it is possible to erect an antenna of similar gain and at similar height as an authentic base station, e.g., on building roof-top, the coverage area could be of roughly the same area as that of a normal cell in the network. Listening over a large area can be done using a mobile setup or a network of receiving antennas. The presence of receiving antennas is difficult to detect. However, the passive approach is slow since an attacker has to wait for a mobile device to transmit its IMSI spontaneously, which is an uncommon event in most locations (exceptions are, e.g., airports). A faster, *active* way to catch IMSIs is to set up a "fake" base station which acts as a preferred base station in terms of signal strength. Mobile devices typically prefer base stations emitting the strongest signal. This fake base station can then be used to send an Identity Request message to all mobile devices in the area, which will respond with their IMSIs since they assume that they are connected to a real network which has lost access to the TMSI. In this way, IMSIs of all mobile device in the area can typically be captured rapidly.

The area covered varies depending on the type of IMSI-catcher and targeted network standard. For example, a semi-passive attack presented in [10] can locate an LTE-compliant UE within a $2\,\mathrm{km}^2$ area in an urban setting.

Catching IMSIs is often a first step in more elaborate eavesdropping attacks in GSM, such as when a fake base station places itself as a man-in-the-middle between the UE and the real base station, requesting the victim to use no encryption [6]. Such attacks do not work against UMTS or LTE since they rely on the lack of integrity protection in GSM.

In the past, active IMSI-catchers such as StingRay were expensive (in the range $68,000-$134,000) and sold only to law enforcement and government officials [18]. However, advances in low-cost software defined radio made active IMSI-catchers relatively cheap and accessible. In 2010, Chris Paget demonstrated that it is possible to build a home-made active IMSI-catcher for about $1,500 using a software-defined radio, two directional antennas, and a laptop running OpenBTS and Asterisk [25]. The price of active IMSI-catchers dropped even further with the introduction of commercially available cheap home base stations called *femtocells* [19, 12].

Recent news uncovered widespread use of unregulated active IMSI-catchers in the areas of airfields and embassies [29, 17, 27, 5]. The Federal Communications Commission of the United States has started an investigation of the use of IMSI-catchers by criminal organizations and foreign intelligence agencies [31], showing that these attacks are considered to be a serious threat. IMSI-catchers can also potentially be used for physical attacks since methods to trigger bombs when a target comes into vicinity of an IMSI-catcher are known [20, 9].

3. ENHANCED IMSI PROTECTION

We propose an enhancement to subscriber privacy in 5G, allowing the home network operator to put less trust in the serving network and protecting against IMSI-catchers. The main approach is to enhance protocols and identifier handling so that only the home network and the UE see the IMSI in clear-text. This is based on the observation that the MME does not need to be aware of the whole IMSI; knowing MNC and MCC is sufficient for requesting authentication information. Therefore, the identifier of the actual subscriber can be hidden from the MME, even though the MME knows to which home network the subscriber belongs. In contrast to the approach proposed in [32], we do not require transmitting a new pseudonym from the HSS. Rather, we *derive* the pseudonym in the HSS and UE separately, which reduces the complexity greatly compared to the approach in [32].

We assume that 3GPP will use the same basic structure for subscriber identification and authentication for 5G as has been used in all prior 3GPP systems since GSM.

3.1 Pseudonym Assignment Procedure

We describe the main steps in two phases. First we describe an initial attach by the UE when it does not share any pseudonym with the home network nor with the serving network. The result of this phase is that the UE is assigned a pseudonym P by the home network and a TMSI by the serving network. This is illustrated in the top half of Fig. 3. Next we describe the second phase where the UE no longer shares a TMSI with the serving network, and it is forced to identify itself using P. This is illustrated in the bottom half of Fig. 3. Once P has been used, it is replaced by a new pseudonym to ensure unlinkability.

At step 1, the UE performs an attach procedure with the MME in order to register to the serving network. This is an attach where the UE has not yet been assigned a TMSI. Neither has the UE been assigned a pseudonym P by the HSS. This may occur, for instance on the UE's very first attach. As suggested by others, the UE resort to sending the IMSI encrypted by the public key of the home network K_{HSS}. Doing so hides the IMSI from any passive or active attacker anywhere on the path between the UE and the HSS. Note that the UE only need to store one public key,K_{HSS} associated with the home network. This is in stark contrast to requiring the UE to store the public key of all potential serving networks it may roam into, or having to distribute those keys when needed. The approach is, however, connected with some problems discussed below, and should thus only be applied as a recovery mechanism in the rare event when the pseudonymity mechanism has malfunctioned. The encryption needs to be randomized, but that does not constitute a serious problem, since most or all existing public key encryption schemes are randomized. Because the MME needs to identify the HSS, the Attach Request message contains the MNC and MCC parts of the IMSI in clear text. In the rest of the paper, we use the term "encrypted IMSI " to refer to the IMSI with the MSIN part encrypted using the public key of the home network K_{HSS}.

Once the MME receives a message from a UE identified by an encrypted IMSI, the MME requests an authentication information from the HSS in form of an AV. The HSS decrypts the encrypted IMSI and generates an AV as usual. In addition, the HSS generates a fresh pseudonym P as a function of the K_{ASME} associated with the AV. The HSS also creates a mapping between P and the IMSI to enable future lookup. Finally, the HSS returns the AV to the MME.

Next, at step 5, the MME authenticates the UE based on the obtained AV. As a result, the MME and UE share the key K_{ASME}. When the UE has established the K_{ASME}, it can compute the P using the same function as the HSS as illustrated in step 6. To provide any privacy protection, the function needs to be one-way and it can be instantiated using, for example, HMAC-SHA256 or another hash function. At this point, the UE and the HSS share a pseudonym P which can be used in their next communication. Further, after completion of the authentication procedure, the MME can deduce that the UE has derived the associated P. As an additional robustness measure, the MME can inform the HSS about the successful authentication, and thusly that the UE has access to P. This information can be piggy-backed on the Update Location Request message the MME sends to the HSS after a UE has successfully registered.

Step 7 illustrates that the MME applies the existing TMSI mechanism. The mechanism is still valuable, since it protects the privacy of the UE for protocol procedures run between the UE and the MME. This is in contrast to the pseudonym P, which protects the privacy of the UE for protocol procedures run between the UE and the HSS.

Assuming a pseudonym P has been established as above, we now describe its use, starting from step 8. The MME may delete the TMSI, e.g., due to a timeout. When this happens and the UE attempts to use the TMSI as its identifier (step 9), the MME is forced to initiate an identity request procedure. Under normal circumstances, the UE would respond with its IMSI and thus reveal itself. Using an encrypted IMSI as in the first phase above solves the privacy issue, but wastes bandwidth. Instead, the UE replies with the pseudonym P together with the MNC and MCC of the home network. The latter is necessary for routing the subsequent authentication information request from the MME to the correct HSS. Upon receipt of the authentication information request, the HSS looks up the IMSI corresponding to the P, and generates a new AV. The HSS also generates a new pseudonym P' from the K_{ASME} associated with the generated AV, creates a mapping between P' and the IMSI, and returns the AV and P to the MME as depicted in steps 13 and 14. From this point on, the operations performed by the MME and the UE are analogous to steps 5, 6 and 7 in the previous phase.

3.2 Recovery From a Lost Pseudonym

If the HSS or the UE lose the pseudonym, e.g., due to a time-out based cleanup of memory in the HSS or a malfunction in the UE, then the UE can identify itself to the MME by sending the encrypted IMSI and get a new pseudonym from the HSS according to the procedure in the top half of Fig. 3. This recovery mechanism is crucial, since the UE would otherwise be locked out of the system. Diagnosing such a lock-out may be difficult for an operator, and even impossible for some subscribers. Even if the reason for the lock-out is detected, it is a relatively costly procedure to provide a subscriber with a new USIM.

Clearly, encrypting the IMSI using public key cryptography expands message size. There are, however, encryption schemes space efficient enough that may make the recovery mechanism practical. For example, elliptic curve ElGamal encryption based on a 256-bit elliptic curve with point-

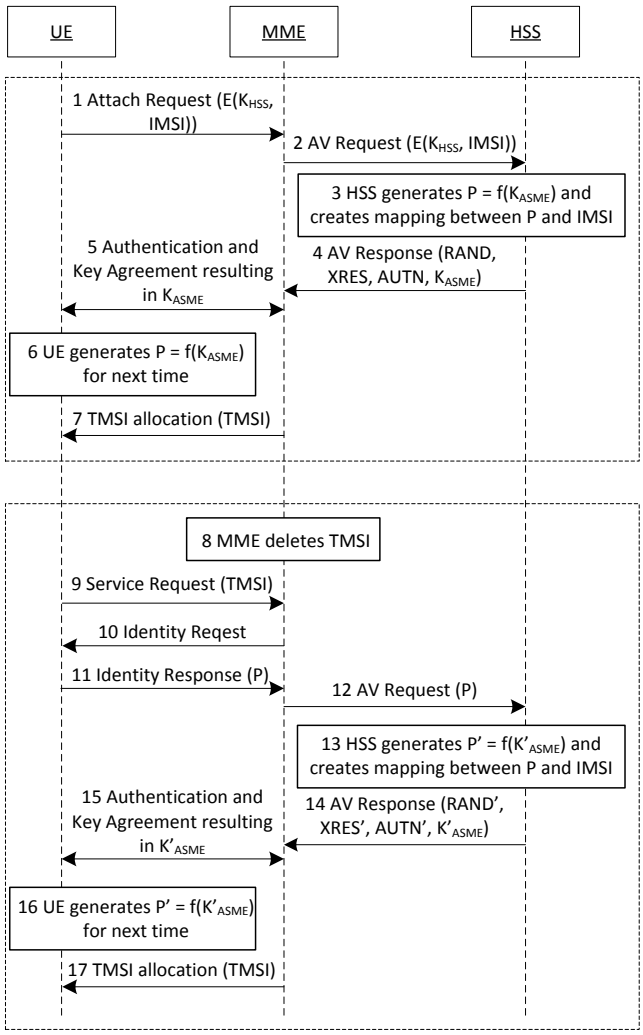

Figure 3: Sequence diagram of the presented method.

compression may be used. It results in that instead of transmitting a typical 40-bit MSIN the UE have to transmit a 256-bit encrypted MSIN

3.3 Backwards Compatibility Issues

If implemented in a legacy networks, a vast amount of legacy nodes would have to be simultaneously updated. To allow legacy UEs to get service, fall-back mechanisms will be required. This may lead to possibilities for downgrade attacks where the network or the UEs are fooled into believing they must refrain from using the presented enhanced privacy mechanism due to the (incorrect) assumption that the other party does not support it. If, on the other hand, the presented method is implemented in 5G, all entities supporting the 5G radio interface will also support the presented method and no backwards compatibility problems would arise. For instance, the UEs would not respond to requests from visited serving networks for their IMSIs, but would instead use only the pseudonym or the encrypted IMSI.

The end-to-end principle prescribes that modifications should not affect nodes between the end-points. Based on this principle, a solution modifying only the USIM and the HSS would be preferable. However, this takes neither telecom history nor economics into account. Rolling out new USIMs to subscribers is a rather expensive operation. Should it be required for all subscribers, it can sum up to a substantial amount. Further, when UMTS was designed, even though a new type of SIM was added, the USIM, backwards compatibility with the SIM was kept. When LTE was later designed, USIMs were still supported and deprecating the SIM was only done after a long and careful consideration. Therefore, it is plausible that 5G will also require that mechanisms are backwards compatible with SIM and USIM, which our proposed mechanism supports.

3.4 Regulatory and Lawful Intercept Issues

It is important to realize that telecommunication systems are heavily regulated and need to take national laws into account. A concrete example is an emergency call, which is required to be authenticated in some countries, whereas other countries require emergency calls to be possible even without subscription or credentials. Consequently, 3GPP systems are designed so that operators can configure them to enforce either policy.

When it comes to Lawful Intercept (LI), 3GPP systems abide by requirements collected in technical specifications; the ones relevant for this paper are TS 33.106 [3] and TS 33.107 [4]. These requirements prescribe how law enforcement agencies shall be able to obtain the traffic of identified targets, and are derived from national and regional laws.

For the mechanisms discussed in this paper, the following requirements and aspects are of prime importance.

- A lawful intercept target can be a roaming user with a subscription belonging to another 3GPP network.
- A target shall be identifiable through its IMSI.

An option to ensure that LI targets can be identified through the IMSI in the serving network is to allow the HSS to include the IMSI for identified targets. The presented method would then prevent mass-tracking of users based on IMSI; individual targets need to be registered as such in their home network's HSS. However, TS 33.106 requires that *"The visited network shall be able to support the interception of all services without home network assistance or visibility"* [3]. Therefore, it is, according to LI requirements, not a permissible option to let the HSS include the IMSI for identified targets only.

The target needs to be identifiable through the IMSI, and the serving network must be able to perform interception without this being noticeable to the home network. It seems impossible to fulfill these requirements and at the same time hide the IMSI from the serving network. Even though implementing mechanisms for hiding the IMSI from the serving network is technically possible, operating such a system would be illegal in some countries.

When the mechanism is implemented transparently to the MME, an interesting aspect appear when the MME is located in a country A and the HSS is located in a different country B. If country A has regulatory requirement for IMSI identification of LI targets, the operator of the MME cannot control whether the operator of the HSS uses the mechanism or not. A possible result is that operators in country A are forbidden by law to form incoming roaming agreements with operators of country B.

3.5 Advantages and Limitations

The presented enhancement has several advantages. First, IMSI-catchers become virtually useless since they are only able to catch a pseudonym, which is frequently changed, or an IMSI with the MSIN part, identifying the subscriber, encrypted. Second, nodes of the serving network, such as MME, *Mobile Switching Center* (MSC), and *Serving GPRS support node* (SGSPLMN), can no longer identify the subscriber from the identification and authentication protocols. Third, the enhancement prevents entities with access to an interconnecting network to request the precise location of a given subscriber. In general, the enhancement supports a more relaxed trust model with honest but curious serving networks.

While our proposed enhancement solves the user privacy problem in this particular set of procedures, it must be realized that protocols are not run in isolation. Particularly, the identity of the user may be deduced by other means than attacking the identification and authentication protocols. For example, the MME can obtain subscription data, which may contain the telephone number of the subscriber from the HSS during, e.g., location area updates and the attach procedure. With this in mind, protecting the IMSI from the serving network in the identification and authentication procedures may seem insufficient. However, one option to tackle this issue is to partition subscription information into a private and a public part. The former can then be provided only to trusted serving networks. It is for further study to investigate whether such an approach can be made effective.

4. RELATED WORK

Already in 1994, Herzberg et. al. [22] described privacy issues in GSM and derived general principles for protecting the IMSI and some example protocols. Specifically, they classified solutions based on which parties are involved in establishing a pseudonym for the UE. Moreover, they made a clear distinction between the home network and the visited network, an important aspect of the 3GPP systems design which we also adhere to in this paper.

A number of methods for detecting IMSI-catchers have been presented. Dabrowski et al. [13] formulated several indicators of potential presence of an IMSI-catcher. They have shown how IMSI-catchers can be detected with the help of a network of stationary measurement devices. They also presented an Android application capable of detecting IMSI-catchers.

Other applications for IMSI-catchers detection have been reported [24, 11, 13, 5]. Detecting IMSI-catchers and warning users is a valuable measure. However the detection does not prevent IMSI-catching attacks.

Federrath et. al. [16] and Kesdogan et. al. [23] presented privacy enhancing schemes for mobile communication networks based on a hierarchy of pseudonyms. Specifically, some of the schemes used a pseudonym for the IMSI, similarly to our approach. They do, however, in some versions, require addition of new entities to the architecture. Further, there is no clear treatment of the initial establishment of the first pseudonym in all cases, unless a global clock exists.

Arapinis et al. [7] used ProVerif to formally verify the 3G specifications. Their work revealed two new privacy-related problems: (1) linkability of the IMSI to the TMSI using paging of mobile phones and (2) traceability. As solution to both problems, they proposed to encrypt the IMSI in a paging command with a shared session key and encrypt the response of a failed authentication request with a public key of the network. It is not clear whether they intended the public key to belong to the serving network or the home network. Because they claimed that the public key can be used to solve the problem of lack of explicit serving network authentication towards the UE, we assume they intended the public key to belong to the serving network. Such a solution is likely to have scalability issues or require cross-signing certificates of all potential roaming partners. Note that encryption does not prevent the problem of misbehaving serving network nodes, e.g., MMEs.

Hahn et al. [21] presented a different solution for the traceability problem which uses the new symmetric session key instead of the public key of the provider to encrypt the response of a failed authentication. This solution might be more efficient, but consequences of switching to the session key provided by a re-played challenge need to be better explored.

In [8], the TMSI reallocation protocol was investigated formally and experimentally. Both the specifications and common implementations were found to have issues with linkability between different TMSIs and recovering the link between an IMSI and a TMSI, opening possibilities for privacy attacks.

Van den Broek et al. [32] proposed a solution which replaces the IMSI with changing pseudonyms. These pseudonyms are only identifiable by the home network of the USIM's own network operator. Consequently, they are unlinkable by serving network providers and malicious adversaries, and therefore mitigate both passive and active IMSI-catcher attacks. This method requires some changes to the USIM. This differs it from the presented method, which requires no changes to the USIM. As explained in Section 3.3, it is preferable not to modify the USIM. Further, since the presented method derives the pseudonyms from the K_{ASME} instead of transmitting them as part of the $RAND$ as in [32], the agreement on the pseudonym becomes simpler in our case. For example, there is no need for including a sequence number in the $RAND$ parameter (which is undesirable because it reduces randomness of the $RAND$). Neither is there a size restriction on the pseudonym imposed by the size of the $RAND$. Moreover, the method [32] provides no recovery mechanism for lock-out situations. As discussed in Section 3.2, ability to recover from a lock-out is important. Finally, the method [32] requires different solutions for SIM and USIM.

5. CONCLUSION

In this paper we presented a new method for protecting users' privacy in telecom networks by means of establishing a pseudonym between the UE and the HSS. The pseudonym is derived locally at the UE and the HSS without affecting existing USIMs. The presented method protects the long-term identifier IMSI from passive and active IMSI-catchers as well as honest but curious serving networks. Moreover, the presented method can recover from lock-out situations where one party has lost the pseudonym.

We have examined the method from a lawful intercept perspective and concluded that confidentiality protection of the IMSI from attackers in the serving network may render the system illegal to operate in some jurisdictions.

We also analyzed the method as a stand alone protocol from a technical security and privacy perspective and found it adequate. Further, we have discussed what level of privacy can be expected from the method when it is used as a component in a larger system. The method protects against IMSI-catchers, but does not, by itself, protect against honest but curious attackers in the serving network. These attackers can obtain the identity of a subscriber by other means; we propose a countermeasure for this.

6. ACKNOWLEDGEMENTS

The authors would like to thank Yi Chen for her help with this work while at Ericsson Research, and John Mattsson from Ericsson Research for his help with the work.

The third author was supported by the research grant No SM14-0016 from the Swedish Foundation for Strategic Research.

7. REFERENCES

[1] 3GPP TS 23.003. Numbering, addressing and identification. Retrieved 2016-04-07. http://www.3gpp.org/DynaReport/23003.htm.

[2] 3GPP TS 23.401. General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network; (E-UTRAN) access. Retrieved 2016-04-07. http://www.3gpp.org/DynaReport/23401.htm.

[3] 3GPP TS 33.106. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful Interception requirements. Retrieved 2016-04-07. http://www.3gpp.org/DynaReport/33106.htm.

[4] 3GPP TS 33.107. 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Lawful interception architecture and functions. Retrieved 2016-04-07. http://www.3gpp.org/DynaReport/33107.htm.

[5] D. Abodunrin, Y. Miche, and S. Holtmanns. Some dangers from 2G networks legacy support and a possible mitigation. In *2015 IEEE Conference on Communications and Network Security (CNS)*, pages 585–593, Sept. 2015.

[6] I. Androulidakis. Using a GSM tester to intercept calls and SMS. TwelveSec, 4 Jaunary 2015. Retrieved 2016-04-07. http://www.twelvesec.com/using-gsm-tester-intercept-calls-sms-pt1/.

[7] M. Arapinis, L. Mancini, E. Ritter, M. Ryan, N. Golde, K. Redon, and R. Borgaonkar. New privacy issues in mobile telephony: Fix and verification. In *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, CCS '12, pages 205–216, New York, NY, USA, 2012. ACM.

[8] M. Arapinis, L. I. Mancini, E. Ritter, and M. Ryan. Privacy through pseudonymity inmobile telephony systems. In *NDSS'2014*, 2014.

[9] M. Böck. Simulation chamber and method for setting off explosive charges contained in freight in a controlled manner, September 4 2014. US Patent App. 14/345,697.

[10] R. Borgaonkar, A. Shaik, N. Asokan, V. Niemi, and J.-P. Seifert. LTE & IMSI Catcher Myths. In *BlackHat Europe'2015*, 2015. Retrieved 2016-04-07. https://www.blackhat.com/docs/eu-15/materials/eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths.pdf.

[11] R. Borgaonkar and S. Udar. Understanding IMSI privacy. In *BlackHat'2014*, 2014. Retrieved 2016-04-07. https://www.isti.tu-berlin.de/fileadmin/fg214/ravi/Darshak-bh14.pdf.

[12] F. Broek and R. Wichers Schreur. *Proceedings of 18th Nordic Conference on Secure IT Systems (NordSec'2013)*, chapter Femtocell Security in Theory and Practice, pages 183–198. Springer Berlin Heidelberg, Berlin, Heidelberg, 2013.

[13] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl. IMSI-catch me if you can: IMSI-catcher-catchers. In *Proceedings of the 30th Annual Computer Security Applications Conference*, ACSAC '14, pages 246–255, New York, NY, USA, 2014. ACM.

[14] S. Datoo. How tracking customers in-store will soon be the norm. The Guardian, 10 Jaunary 2014. Retrieved 2016-04-07. http://gu.com/p/3ym4v/sbl.

[15] T. Engel. Ss7: Locate. track. manipulate, 2014. Retrieved 2016-04-07. http://berlin.ccc.de/ tobias/31c3-ss7-locate-track-manipulate.pdf.

[16] H. Federrath, A. Jerichow, and A. Pfitzmann. Mixes in mobile communication systems: Location management with privacy. In *Information Hiding, First International Workshop, Cambridge, U.K., May 30 - June 1, 1996, Proceedings*, pages 121–135, 1996.

[17] A. B. Foss, P. A. Johansen, and F. Hager-Thoresen. Secret surveillance of Norways leaders detected. Aftenposten, 16 December 2014. Retrieved 2016-04-07. http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html.

[18] R. Gallagher. Meet the machines that steal your phone's data. Arstechnica, 25 September 2013. Retrieved 2016-04-07. http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data.

[19] N. Golde, K. Redon, and R. Borgaonkar. Weaponizing femtocells: the effect of rogue devices on mobile telecommunication. In *NDSS'2012*. The Internet Society, 2012.

[20] S. Goldman, R. Krock, K. Rauscher, and J. Runyon. Mobile forced premature detonation of improvised explosive devices via wireless phone signaling, June 30 2009. US Patent 7,552,670.

[21] C. Hahn, H. Kwon, D. Kim, K. Kang, and J. Hur. A privacy threat in 4th generation mobile telephony and its countermeasure. In *Proceedings of the 9th International Conference on Wireless Algorithms, Systems, and Applications - Volume 8491*, WASA 2014, pages 624–635, New York, NY, USA, 2014. Springer-Verlag New York, Inc.

[22] A. Herzberg, H. Krawczyk, and G. Tsudik. On travelling incognito. In *First Workshop on Mobile Computing Systems and Applications, WMCSA 1994, Santa Cruz, CA, USA, December 8-9, 1994*, pages 205–211, 1994.

[23] D. Kesdogan, P. Reichl, and K. JunghÃd'rtchen.

Distributed temporary pseudonyms: A new approach for protecting location information in mobile communication networks. In *Proceedings of ESORICS'98. Louvain*. Springer, 1998.

[24] K. Nohl. Mobile self-defense (SnoopSnitch). In *Proceedings of Chaos Computer Security Conference*, 2014. Retrieved 2016-04-07. https://events.ccc.de/congress/2014/Fahrplan/system/attachments/2493/original/Mobile_Self_Defense-Karsten_Nohl-31C3-v1.pdf.

[25] C. Paget. Practical cellphone spying. In *Proceedings of DEFCON*, 2010. Retrieved 2016-04-06. https://media.defcon.org/DEF CON 18/DEF CON 18 video and slides/DEF CON 18 Hacking Conference Presentation By Chris Paget - Practical Cellphone Spying - Video and Slides.m4v.

[26] Positive Technologies. Signaling system7 (SS7) security report, 2014. http:.

[27] M. A. Russon. 19 fake mobile base stations found across US are they for spying or crime? IBTimes, 4 September 2014. Retrieved 2016-04-07. http://www.ibtimes.co.uk/19-fake-mobile-base-stations-found-across-us-are-they-spying-crime-1464008.

[28] K. Shubber. Tracking devices hidden in London's recycling bins are stalking your smartphone. Wired magazine, 9 August 2013. Retrieved 2016-04-07. http://www.wired.co.uk/news/archive/2013-08/09/recycling-bins-are-watching-you.

[29] A. Soltani and C. Timberg. Tech firm tries to pull back curtain on surveillance efforts in Washington. The Washington Post, 17 September 2014. Retrieved 2016-04-07. http://wapo.st/1qgzImt.

[30] D. Strobel. IMSI catcher. Ruhr University Bochum report, 13 July 2007. Retrieved 2016-04-07. https://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf.

[31] C. Timberg. Feds to study illegal use of spy gear. The Washington Post, 11 August 2014. Retrieved 2016-04-07. http://www.washingtonpost.com/blogs/the-switch/wp/2014/08/11/feds-to-study-illegal-use-of-spy-gear/.

[32] 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 '15, pages 340–351, New York, NY, USA, 2015. ACM.

[33] B. Woods. 3g flaw makes any device vulnerable to tracking. Zdnet, 9 October 2012. Retrieved 2016-04-07. http://www.zdnet.com/article/3g-flaw-makes-any-device-vulnerable-to-tracking/.

[34] K. Zetter. Florida cops' secret weapon: Warrantless cellphone tracking. Wired, 3 March 2014. Retrieved 2016-04-07. http://www.wired.com/2014/03/stingray.