Privacy through pseudonymity in mobile telephony systems

Privacy through Pseudonymity in Mobile Telephony Systems

***Abstract*—To protect mobile phone from tracking by third parties, mobile telephony systems rely on periodically changing pseudonyms. We experimentally and formally analyse the mechanism adopted to update these pseudonyms and point out design and implementation weaknesses that defeat its purpose by allowing the identification and/or tracking of mobile telephony users. In particular, the experiments show that the pseudonym changing mechanism as implemented by real networks does not achieve the intended privacy goals. Moreover, we found out that the standard is flawed and that it is possible to exploit the procedure used to assign a new pseudonym, the TMSI reallocation procedure, in order to track users. We propose countermeasures to tackle the exposed vulnerabilities and formally prove that the 3GPP standard should require the establishment of a fresh ciphering key before each execution of the TMSI reallocation procedure to provide unlinkability.**

I. Introduction

If a third party that eavesdrops on the radio link was able to identify wireless messages as coming from a particular mobile phone, he would be able to track the location of the mobile phone user in real-time. Mobile phone signalling is used for example by market research companies such as [1], [2] in order to track the movements of people within a shopping centre. Contrary to location based service companies, these companies are tracking bearers of mobile phones in an anonymous way yet without their consent, without offering them a service, and sharing the tracking information with parties which have not previously been agreed with the mobile phone bearers. Similar tracking techniques could lead to stalking and other forms of harassment, as well as more mundane invasions of privacy [3]. In order to prevent this, mobile phone protocols employ temporary identifiers (TMSIs) instead of using long-term unique identities (IMSIs) to identify mobile phones. Temporary identities are periodically updated by the network by means of the *TMSI reallocation procedure*. To ensure confidentiality of a newly assigned TMSI, it is transmitted encrypted using a ciphering key.

Our aim in this paper is to analyse what conditions are required in order for this arrangement to guarantee user privacy as intended. In particular, two aspects appear to be important:

1) TMSI reallocation will protect user privacy only if TMSIs are re-allocated often enough, and at the right times (e.g., when users move between locations). The 3GPP standard does not rigorously define the conditions under which TMSI reallocation takes place. We show that the lack of precise directives permits implementations which violate user privacy.
2) The success of TMSI reallocation requires that an attacker with access to the radio channel cannot link the new TMSI to the old one. Encrypting the TMSI in the allocation message is necessary but not sufficient to ensure that. It turns out that other factors, in particular the use of a fresh encryption key for each TMSI reallocation, are also necessary to guarantee unlinkability of old and new TMSIs. The 3GPP standard does not mandate this, again leaving user privacy subject to choices made by network operators.

We analyse the TMSI reallocation procedure from both a *formal* and an *experimental* point of view. Our experimental analysis exposes the adoption by deployed network implementations of weak policies with respect to privacy and hence are vulnerable to tracking mobile phone users. We show that the TMSI reallocation procedure does not provide unlinkability on most of the analysed mobile networks, because:

1) pseudonyms are not updated frequently;
2) the frequency of updates of pseudonyms does not depend on the amount of activity exposing them to tracking adversaries;
3) the same pseudonyms are maintained across different areas, making users linkable within wide areas;
4) it is possible to mount a replay attack on the TMSI reallocation procedure.

*** All these issues defeat the objective of introducing TMSIs. *** Our formal analysis allows us to prove the condition under which the TMSI reallocation procedure provides unlinkability. In particular, we formally prove that the establishment of a new encryption key before each execution of the procedure should be a mandatory requirement in the standard specification.

Our Contributions. We present a formal and an experimental analysis of the subscriber's privacy in cellular networks and in particular of the TMSI reallocation procedure. We highlight deficiencies in the standard and show how these have led to flawed implementations which do not trigger the reallocation procedure often enough, and when they do they sometimes allow linkability attacks. Our experimental analysis reveals some real and novel network scenarios which allow a third party to violate a user's privacy despite the reallocation protocol being used according to the current standard. In our formal analysis, we prove that the TMSI reallocation procedure provides unlinkability in case a new ciphering key is established before each execution of the TMSI reallocation procedure and we discuss other possible countermeasures. This proof is one of the few examples in the literature [4], [5] of a proof of labelled bisimilarity of a real-sized protocol. Our proof makes use of both manual and automatic proof techniques.

Terminology. In 3GPP specifications, mobile phones together with their SIM card are referred to as *mobile stations*, abbreviated MS. Mobile stations have a permanent identity stored in the SIM card, the *International Mobile Subscriber Identity*, abbreviated IMSI. As stated, the serving network (SN) assigns a temporary identity to an MS, called the *Temporary Mobile Subscriber Identity* (TMSI).

When the network wants to deliver a service to a mobile station (*e.g.* an incoming phone call) it sends a *paging request* message specifying the identity of the MS (TMSI or IMSI if the TMSI is not known). The paging request is sent on a common channel in all the locations most recently visited by the MS. A MS continuously monitors the common channel used for paging of the area it is located in. When the MS receives a paging request, it asks the base station it is attached to to assign a dedicated channel. The MS the sends a paging response containing its own identity (usually TMSI) in clear-text on the dedicated channel.

A. Related Work

Linkability of transactions has been identified and often reported by the media as an important threat to user privacy, in a variety of areas including on-line searches [6], road usage charging [7], electronic passports [8], and mobile telephony [3]. The problem of privacy is a multi-layer/multiprotocol problem [9] which requires all protocols at all layers to satisfy the desired properties. Moreover, privacy properties are often violated because of subtle design/implementation details, hence the need for careful analysis.

Most of the work on security of mobile telephony systems concerns content-secrecy, integrity and authentication properties [10], [11], [12]. There are only few formal and experimental studies concerning the level of usage-privacy provided to the user by mobile telephony systems. Foo Kune et al. [13] presented a study on the use of the paging procedure to locate mobile telephony users. They perform a tracking attack relying on passive sniffing of paging response messages triggered by placing silent phone calls (obtained by hanging up before the receiving phone rings) for the victim phone. This technique allows one to reveal the presence of the victim in an area monitored by the attacker. Munaut and Nohl [11] previously outlined a similar technique. They performed a GSM sniffing attack, which allows one to eavesdrop a GSM phone call by using a modification of the osmocom-BB [14] open source implementation of the GSM protocol stack and an old Motorola mobile phone. Differently from Foo Kune et al., they used a silent SMS to trigger the paging responses needed to locate the victim. Although these works take advantage of the fact that a TMSI is allocated for a long time window, they do not analyse the security and privacy provided by the TMSI reallocation procedure. Moreover, in order to perform the attack, the adversary needs to know the mobile number of the victim. *** Indeed, these attacks consist in establishing the presence of a target MS in a given location by linking the target's telephone number with its TMSI. This attack relies on the fact that TMSI reallocation is not activity-dependent (as confirmed by our experiments). This suggests the adoption of activity dependent reallocation strategies to thwart the attack. However, we show that reallocating a new TMSI after each transaction is not sufficient, because (as we experimentally show) encryption keys are reused in many deployed networks allowing the replay attack we present. This further privacy threat cannot be established from Foo Kune et al's analysis. We formally prove that establishing fresh keys at each TMSI reallocation and adopting an activity-dependent reallocation strategy thwarts Foo Kune et al's attack. Additionally, we show that deployed networks do not follow the standard as they do not all enforce TMSI reallocation at each change of Location Area. This makes a MS traceable across Location Areas by simple sniffing. This further privacy breach is beyond the scope of Foo Kune et al's analysis. So our findings further contribute to help improving future developments of this technology. *** The experiments we carried out show that real networks do not adopt policies for changing TMSI which are dependent on the number of exposure of the TMSI over-the-air by the mobile phone activity and hence they do not tackle these attacks.

Engel showed at the 25C3 conference [15] how network signalling messages, triggered when sending/receiving SMS messages, can be used to locate mobile telephony users. He suggests that network operators should use home routing, i.e. forwarding through the home network, as a countermeasure to this SMS tracking attack. This attack requires access to the intra-network communication infrastructure, which although possible may require subscription to a pay per query service. In this work, we analyse the privacy provided by the more exposed over-the-air communication available to any attacker with a radio enabled device and do not rely on the less easily accessible intra-network communication protocols.

The *gsmmap* project [16], [17] uses a variant of the open source GSM protocol stack developed within the osmocom-BB project to assess and visually render on a map the level of security and privacy provided by network operators across the world. In particular their aim is to check if network operators are protecting the users from well known attacks by adopting countermeasures such as the use of A5/3 encryption, padding randomization, and full authentication for outgoing calls and SMS to prevent impersonation and interception, and the use of regular TMSI updates, and home routing to prevent Engel's SMS tracking attack.

The closest work to ours is the one presented in [18] which also analyses mobile telephony protocols from a privacy point of view. Arapinis et al. [18] uncover some privacy attacks on the 3G authentication protocol and on the paging procedure. These attacks are exposed and exploited through a real implementation. The authors propose and automatically verify privacy-friendly fixes of the attacked procedures. The procedures analysed in [18] are not part of the identity management mechanisms of mobile telephony systems, in particular they do not analyse the TMSI reallocation procedure that is the procedure on which mobile telephony systems rely to provide anonymity and unlinkability from third parties. This procedure is the focus of our work. Moreover, in this work we are concerned with both issues of the standard specifications and issues of the actual implementation by real networks. None of the issues concerning the identity management and the pseudonym changing mechanism that we identify in this paper arise from the analysis presented in [18]. Finally, the proof methods used in [18] are too weak to prove the correctness of the TMSI reallocation. We have to create new proof tech-