Anonymization in Proactive Location Based Community Services

Georg Treu, Axel Küpper and Peter Ruppel*

Abstract. *Location information of mobile users is very sensitive with regard to privacy. This is especially true for proactive location based services (LBSs) where users are continuously tracked. Effective privacy enhancing technologies for these services are still an open field of research. In this paper, we focus on proactive location based community services (PLBCSs), such as mobile gaming or buddy tracking. Instead of relating the spatial position of users to fixed real-world entities, like e.g. tourist sights in a navigation service, in PBLCSs, the focus is on a user's spatial relation to other users or virtual entities. In the paper, we discuss why existing privacy mechanism for LBSs are not well suited for PLBCSs. We also present initial ideas for a novel anonymization technique, where location coordinates are obfuscated by a key shared among community members before they are emitted to a PLBCS. Like this, statistical attacks on pseudonym-associated can be avoided while calculations of spatial relations between the entities can be done with unchanged accuracy.*

1. Proactive Location Based Community Services (PLBCSs) and Privacy

In ubiquitous computing environments the need for privacy amplifies, as ubiquity of computing leads to reduced user control over collected data [Lang01]. For proactive LBSs this is especially true. Although users agree to be tracked in general, location information is collected continuously and therefore without explicit user knowledge so that events relevant for the LBS, such as e.g. a target reaching a point of interest (PoI) can be recognized.

In the following, we would like to focus on proactive Location Based Community Services (PLBCS) like buddy tracking [AEM+04], where community members are notified when their mutual distance falls below a pre-defined threshold, or mobile gaming, where, in contrast to e.g. navigation services that relate user positions with real-world entities, the positions of users are only related with the one of other players or virtual entities.

Generally, we identify the following requirements for the PLBCSs considered:

- The precision of collected position information must be relatively high, service latency low.
- Application areas can include the living-area or workplace of a user.

*Mobile and Distributed Systems Group
Institute for Informatics
Ludwig-Maximilian University Munich, Germany
email: [georg.treu|axel.kuepper]@ifi.lmu.de, peter.ruppel@cip.ifi.lmu.de

- Community membership (resp. game participation) of a user must be traceable for the LBS. That means, user identifiers (which can be pseudonyms) must not change at least for the duration of an application session (which can last for a relatively long time).
- Instead of relating location data of users with real world entities, like e.g. in the case of a navigation system or similar, in PLBCSs the spatial position of users is observed with relation either to other users or virtual entities, such as computer animated players.

We believe that PLBCSs are likely to be realized on a large scale basis of users. This is due to (economical) network effects, which means that service popularity increases with the number of users (because possibilities of forming communities increase). This trend can already be observed for non-location based community services like MSN Messenger or ICQ. For their possibly large scale, PLBCSs are likely to accumulate a huge amount of (pseudonym-associated) location data and thus constitute a major threat to the privacy of their users. For these reasons, we believe the amount of privacy-sensitive user information emitted to a PLBCS should be reduced to a minimum for the service to work.

While in [CCR03] and [KuTr05] architectures for efficient tracking of a target are proposed, privacy aspects have not been discussed sufficiently yet. An overview of privacy attacks on LBS and possible solutions is given in [GHT04] and [Kuep05].

One way for users to specify how location data about them should be processed are privacy policies [MFD03]. The problem associated here is that after location data has been handed out to an LBS in the first place, it depends on the trustworthiness of the LBS if policies are respected.

In contrast to the policy-based approach, anonymization mechanisms aim to technically hide a user's true identity behind emitted location information. It can be distinguished between techniques of data or identifier abstraction.

In the data abstraction approach, anonymization is achieved by cloaking location data, e.g. by reducing temporal and/or spatial accuracy, so that location information of different individuals cannot be distinguished. In [GrGr03] this is done based on the formal model of k-anonymity [Swee02]. k-anonymity protection is given if the location data of a person cannot be distinguished from at least *k-1* individuals. The problem with this approach is that data accuracy is reduced, especially in sparsely populated areas, and for the temporal version, service response time may significantly rise due to the introduced delay. This stands in conflict with the high quality of service requirements of many LBSs, like mobile gaming.

In identifier abstraction, pseudonyms are associated with the location information. The problem here is that pseudonyms can be uncovered by statistical attacks. Locations known to be highly frequented by a given person, like living- or workplace, can be related with sampled, pseudonym-associated position data so that the mapping to a user's true identity can be done. For this reason, in [BeSt03] the usage of LBS is restricted to so called "application zones", which exclude these critical whereabouts of a user. Unfortunately, with this restriction, users are just not able to use an LBS most of their time, which may be unacceptable. To improve the protection from statistical attacks, pseudonyms can be dynamically changed in so called "mix zones". But this conflicts with LBSs that require a consistent user identifier for the time of an application session. Changing pseudonyms makes it also hard to maintain user profiles over different application sessions, since traceable links (which would be the case for user profiles migrated from one pseudonym to another) between pseudonyms of a user make the mechanism ineffective.

Although the presented anonymization techniques are certainly useful for some LBSs, we see from the list of requirements above that neither cloaking of location data, nor the mix/application-zone approach is adequate for anonymization of location data in PLBCSs like buddy tracking.

2. Idea: Abstracting Location Data by Coordinate Transformations

In this section, an anonymization technique suitable for PLBCSs is presented. It uses pseudonyms in conjunction with coordinate transformations and is based on the idea that for PLBCSs the real-world position of a user is not relevant. Knowledge about the relative spatial position of a community member or player w.r.t. other members, resp. his position within a virtual playground is enough.

We propose that members of a community, like users of a buddy tracking service or participants in a mobile game, transform their location coordinates (origin displacement, rotations, ...) with a shared key hidden from the PLBCS and specific to the community and application session they are in. The key is exchanged over a channel hidden from the PLBCS. The coordinate transformation happens in a way so that relative distances are preserved or at least uniformly scaled, but that the real location is obfuscated[1]. This way, proximity between buddies as well as events in a mobile game with respect to other members or virtual entities can still be triggered by the PLBCS. We distinguish two types of attacks on the mechanism.

First, during execution of the service, one possibility would be to introduce a “snitcher” into a community who leaks out the shared key, another would be to deduce the key by relating real-world position data of a community member with the obfuscated data. We believe this type of “online”-attacks is hard to avoid (but also hard to conduct) and is also not covered by existing approaches. It is not subject of this work.

Second, there are attacks that happen posterior to service execution targeting a database or similar of collected location data. Here, the collected data is searched after locations associated with a given person (living place, ...). By observing cumulations of pseudonyms the used pseudonym and with that a full trace of the person may be discovered. It is this attack we try to avoid.

Above, we discussed how in [BeSt03] mix/application-zones counteract on it and also why the mechanism is not suitable for PLBCSs. We believe that coordinate transformations in conjunction with pseudonyms are a better way for anonymization in PLBCSs. Since coordinates are transformed before sending them to a PLBCS, it is impossible to search the database of the PLBCS provider for specific locations of a person.

So called privacy homomorphisms (PHs) were originally introduced in [RAD78]. PHs are encryption transformations that map addition and multiplication on plaintext to the addition and multiplication on ciphertext. Cryptanalysis like by [Bao03] showed that PHs are relatively insecure [2]. However, this aspect of security relates to the first type of attack from above.

In our work, PHs (distance preserving coordinate transformations can be seen as PHs) are used to

[1] For terminal-based positioning like GPS, this can be done on a user’s mobile device

[2] PHs are provably insecure against known-plaintext attacks

obfuscate location data to withstand statistical attacks (the second type) only, and for the mentioned reasons we believe it is appropriate for it. The approach is thus better classified as *data obfuscation* than security. [BPB+04] can be used as an overview in this field.

3. Conclusion and Outlook

To our knowledge, using coordinate transformations to provide anonymity for LBS users has not been considered so far. The main benefit of the approach in the context of PLBCSs is that, in contrast to mix-zones, pseudonyms need to be changed less often. Instead, the key used for obfuscation can be regularly exchanged among the (trusted) community members. Like this, user profiles can be maintained more coherently, while an increased level of anonymization is provided. Furthermore, PLBCSs are not restricted to application areas, which substantially promotes their usage. Finally, contrarily to cloaking, the precision of location data is not reduced. Although the proposed idea is promising to us, there are issues that are still under heavy discussion and are thus subject to future work. Among them are:

- Is the mechanism applicable to more general LBSs than PLBCSs?
- What kinds of coordinate transformations should be realized (rotations, origin displacements, scaling, ...) ?
- In the paper, we assume communities that share a secret key used for transformation. Because of this, communities are assumed to be rather closed. Is it possible to apply the mechanism also to open PLBCSs, such as e.g. a profile-based dating service that triggers upon proximity between so far unknown members? Can a PKI help here?
- Although the described statistical attacks based on known whereabouts of a user should be avoided by the mechanism: How secure is it against attacks that match mobility patterns of users?

References

[Lang01] Langheinrich, M. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems,*Proceedings of Ubicomp 2001*, Springer, Lecture Notes in Computer Science, Vol. 2201, 2001, 273–291

[CCR03] Chen, X., Y. Chen, F. Rao. An efficient spatial publish/subscribe system for intelligent location-based services, *Proceedings of the 2nd international workshop on Distributed event-based systems*, San Diego, USA, ACM Press, ISBN 1-58113-843-1, 2003, 1–6

[GHT04] Görlach, A., A. Heinemann, W. Terpstra. Survey on Location Privacy in Pervasive Computing, *SPPC: Workshop on Security and Privacy in Pervasive Computing*, Vienna, Austria, April 2004.

[Swee02] Sweeney, L. k-anonymity: a model for protecting privacy, *International Journal on Uncertainty, Fuzziness and Knowledge-based Systems*, World Scientific Publishing Co., Inc., 10 (5), 2002, 557–570

[BeSt03] Beresford, A., F. Stajano. Location Privacy in Pervasive Computing, *IEEE Pervasive Computing*,IEEE Educational Activities Department, 2 (1), 2003, 46–55

[MFD03] Myles G., A. Friday, N. Davies. Preserving Privacy in Environments with Location-Based Applications, *IEEE Pervasive Computing*, IEEE Educational Activities Department, 2 (1), 2003, 56–64

[GrGr03] Gruteser M., D. Grunwald. Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking, *Proceedings of the First International Conference on Mobile Systems, Applications, and Services*, USA, San Francisco, May 2003

[AEM+04] Amir, A., A. Efrat, J. Myllymaki, L. Palaniappan, K. Wampler. Buddy Tracking — Efficient Proximity Detection among Mobile Friends. *Proceedings of IEEE Infocom 2004*, Hongkong, March 2004.

[KuTr05] Küpper, A.,G. Treu. From Location to Position Management: User Tracking for Location–based Services. *Proceedings of the 14. Fachtagung Kommunikation in Verteilten Systemen KIVS05*, Kaiserslautern Germany, February 2005, Springer–Verlag.

[Kuep05] Küpper, A. *LBS — Fundamentals and Operation.* To be published. John Wiley & Sons, 2005.

[Bao03] Fen Bao. Cryptanalysis of a Provable Secure Additive and Multiplicative Privacy Homomorphism. *Proceedings of International Workshop on Coding and Cryptography*, March 24-28, 2003, Versailles (France), pp. 43–50,

[RAD78] Rivest, R. L., L. Adleman, M. L. Dertouzos. On data banks and privacy homomorphisms. in *Foundations of Secure Computation*, eds. R. A. DeMillo et al., Academic Press, 1978, 169–179.

[BPB+04] Bakken, D.E., R. Parameswaran, D.M. Blough, A.A. Franz, T.J. Palmer. Data Obfuscation: Anonymity and Desensitization of Usable Data Sets. In *IEEE Security & Privacy Magazine*, 2 (6), 2004, 34–41