A Privacy-by-Design Approach to Location Sharing

Marcello Paolo Scipioni
University of Lugano (USI)
Faculty of Informatics
Via G. Buffi, 13
6904 Lugano, Switzerland
marcello.paolo.scipioni@usi.ch

ABSTRACT

Despite the proliferation of location-based services on mobile platforms, privacy concerns still refrain many people from using them regularly. Moreover, current location sharing tools often present over-simplistic privacy settings by which users are forced to the binary alternative of sharing everything or nothing. The goal of this research is to build novel privacy-aware tools through which users can share their location more easily and in the way they consider more appropriate. Starting from the study of the sharing functionalities and how people use them, I aim at building a platform for efficiently sharing location, supported by a usable interface through which users can easily understand how sharing works and feel in control of their data. Furthermore, the security mechanisms employed are conceived such that privacy is considered as an integral part of the sharing mechanisms, in a privacy-by-design approach.

Author Keywords

Location sharing, privacy, location privacy, location based services.

ACM Classification Keywords

H.5.2 Information interfaces and presentation (e.g., HCI): Miscellaneous.; K.4.m Computers and Society: Miscellaneous

General Terms

Algorithms, Design.

INTRODUCTION AND MOTIVATION

Recently, a number of location-based services (LBSs) have been launched serving different purposes, ranging from long-standing location sharing tools where people keep in touch through a persistent stream of automatic updates, such as Google Latitude[1], to the check-in based ones where users notify friends about, e.g., a restaurant, coffee bar or disco where they are currently located, such as Foursquare[2]. While currently available LBSs are perceived as attractive and useful, many people are still concerned of the privacy issues these systems raise. Although much research has been carried out and a number of different approaches for safeguarding location information have already been developed, currently available services still offer only basic privacy settings, which provide limited flexibility for users' needs [25]. As a consequence, users cannot choose to what extent they wish to share, but in practice they are left with the binary decision of sharing all or nothing.

My research has the goal of studying how people share their location, in order to create new tools that can make location sharing easier for people. The aim is to avoid binary choices and build tools that allow people to share just as much as they need for achieving their goals. This is realized by proposing various sharing modes that can be used for specific purposes, through which users can feel on control of their data. At the same time, privacy is considered within the sharing mechanisms, in a privacy-by-design approach [18].

RELATED WORK

The topic of location privacy has been already investigated in detail, and considerable attention has been given to the sensitivity of location data. It has been shown that threats to personal privacy can be generated by the automatic inspection of location traces: Kang et al. highlight how places that are meaningful for users, such as "my place of work", "home", "my favourite lunch spot", etc... can be extracted from location traces [15]; Hoh et al. showed how home locations of people can be extracted after periodically collecting GPS samples [14], while Krumm could identify home location of users and their actual name by comparing their anonymized location traces with publicly available information from white pages [16]. Experiments have demonstrated how location data can be used for inferring also people's modes of transportation [20, 26], to monitor car traffic and to predict and avoid traffic jams (e.g. within the Mobile Millennium project, [1]), or even to predict people's social relationships, by using both location and Bluetooth discovery data [10].

Several approaches have been proposed to address the problem of location privacy, many of which have been summarized by Krumm in a survey [17]. The simple anonymization

[1] `http://www.google.com/latitude`

[2] `https://foursquare.com`

UbiComp '12, Sep 5-Sep 8, 2012, Pittsburgh, USA.
Copyright 2012 ACM 978-1-4503-1224-0/12/09...$15.00

of location tracks has been proven insufficient, as demonstrated by the experiments of many researchers [3, 13, 14]. Another technique degrading the accuracy of location data and enhancing protection against location-related threats is obfuscation, through which the actual coordinates are substituted by street or city level information. Duckam and Kulik [9] suggest a formal model for obfuscating location data, while Krumm [16] shows that a considerable amount of added noise has to be added in order to really protect the subjects from possible attacks. The concept of k-anonymity was introduced in location privacy by Gruteser and Grunwald: it consists of a spatial and temporal cloaking algorithm such that the identity of a subject can be cloaked among those of $k-1$ others by choosing either a large enough area to contain at least k users, or a temporal window such that a specific area is crossed by at least k users, or a combination of the spatial and temporal criteria [12]. A variant of this algorithm is the CliqueCloak algorithm, where each user can define a different k [11]. In another work, Beresford and Stajano propose the so-called "mix-zones", in which the bounding among the identity of a subject, his current place and time is decoupled when different users transit within the same crossing region, called a "mix-zone" [3, 4]. The pseudonyms of users are thus changed with new ones, with the effect of mixing the identity and the history of users.

Despite the richness of approaches proposed in literature, it is still unclear how these methods can be successfully applied to location sharing applications in practice without significantly lowering the quality of service. If we focus on the functionality, applications for locating nearby friends would completely lose their meaning when applying methods such as the mixing of users' identities, in the same way as the check-in into a restaurant would become useless if its exact location would be obfuscated. To overcome this problem, in my thesis the concept of privacy is strictly bound to the functionality provided by the system: the privacy mechanisms are considered as an integral part of the sharing tools, and have to be designed differently depending on the specific task at hand, taking into account all factors involved with the sharing environment [8].

Besides demonstrating the attacks through which people's location privacy can be threatened, research has also investigated the perception of privacy by users. The willingness to disclosure location has in fact been shown to depend on the identity of the subject requesting location data, as well as on the reasons why the request was made and at what level of detail [6]. It is important then to take into account the dynamics among users of the system and the reasons for taking certain actions, in order for people to feel in control of their data. A location-based research application developed with the aim of keeping users in control of what they share is Locaccino [24]. The system offers wide versatility thanks to the rule-based location disclosure that users can set: for different contacts the system can be instructed to disclose location only within certain time slots and/or when a user is located within a certain region. However, the significant effort required by users to come up with rules for all their contacts makes such application hard to manage in a mobile setting, also due to the need of constantly maintaining all the applied rules.

METHODOLOGY

The approach of my thesis to location sharing is based on the analysis of the privacy risks in current applications, and how these risks should be faced in order to build privacy-aware systems. A set of stakeholders which play a significant role in location-based services has been identified: intended recipient (the main goal of the communication), service and infrastructure providers; as well as unintended recipients, such as accidental recipients, illegal recipients and law enforcement [21]. The idea is to study the interactions among all these actors and take them into account for the design of the system. My work is being carried out in parallel on three different but complementary sides, that in the end will be integrated together:

1. building an *efficient architecture* for exchanging data;
2. implementing *security mechanisms* that guarantee the correctness of the intended data flows and prevent unintended disclosures of data;
3. conceiving a *usable interface*, to make the service not only available to users, but also affordable and easy to use.

While the architecture of the system accounts for the linkage among users and the transfer of location data, and the security mechanisms prevent unwanted disclosure of data, it is only with a usable user interface that users can benefit from the application; an interface too cumbersome to use in a mobile context or which is unclear for users, would in fact neutralize the effort spent for building such a system.

Architecture and Security Mechanisms

The design of the architecture for my location sharing system started from the analysis of the stakeholders and on the functionality of the application. As a first step, we considered the long-standing location sharing case in which users share their current GPS location with friends (as for instance in Google Latitude). In this case, the role of the service provider is to route the data traffic towards the right users, based on their friendships; there is in principle no need for the service provider to be aware of users' location data. So far, I have developed two different prototypical architectures for this case [22]. In the first one, users simply exchange with each other location data encrypted with public key cryptography. While this prevents the service provider from learning users' data, this approach encounters scalability problems when it comes to encrypt multiple times the same location update for all friends under different keys. The second architecture supports group-based location sharing, where users can share their location with groups of friends at various levels of precision: GPS location, city level, region level and country level. The introduction of groups and of location granularities goes in the direction of letting people decide at what level of detail they wish to share location, as it probably gets too intrusive to allow all contacts to see location updates with full precision. A client-server architecture with a publish-subscribe pattern has been employed for implementing the system, and the hypothesis was to later apply group-based encryption for ensuring protection from the service provider.

The currently planned approach to solve the scalability issue is instead to apply proxy encryption as a security mechanism, which would allow to encrypt location updates on the client only once [2, 5]. On a server, appropriate cryptographic functions would be applied to transform the encrypted message in order to be decrypted under the keys of the user's contacts with the additional benefit that the server would not be able to decrypt any message [7].

Location sharing functionalities

The architecture described above is the infrastructure on top of which location data will be exchanged; such an infrastructure, however, needs to be surrounded by an interface offering functionalities which make the whole process of location sharing useful for users. For this reason we introduce the concept of location sharing functionalities, i.e., modes for location sharing which involve varying degrees of location disclosure that can be used by users to accomplish specific tasks. The specific aspects of each functionality are then considered in order to apply security mechanisms that block location disclosure towards unintended recipients.

Besides long-lasting location sharing, we considered other sharing functionalities in which the required degree of location disclosure is gradually lowered. One of the sharing modes considered is proximity sharing, in which users share location with their contacts only when they are located in proximity, i.e. within a chosen threshold distance [22, 23]. If with long-standing location sharing people can constantly keep in touch, with proximity sharing they can have "serendipitous encounters", being notified by the application if any contacts happen to be in the neighbourhood. In principle, a client-server architecture can serve the purpose of notifying users when they are in proximity without knowing their positions. Algorithms for privacy aware proximity detection have been developed [19], but no research has yet been carried out to evaluate the usability of such a functionality with real users. Another functionality taken into account allows for ad-hoc meetings: users can define the time and location of a meeting and invite a group of contacts to share their location with each other in occasion of the meeting, similarly to what happens in Glimpse[3]. In this case, the connectivity constraint holds only during the meeting, while no information is disclosed beyond the scheduled event.

EVALUATION AND NEXT STEPS

The above described functionalities (i.e. long-lasting, proximity and ad-hoc meetings) have been evaluated in a preliminary user study, where a set of users have been interviewed to understand their opinions regarding location privacy in general and towards the described functionalities in particular [23]. The results of this study highlight that different sharing modes serve different sharing goals: while long-standing location sharing is perceived as highly intrusive, it is in general considered acceptable for a very limited group of contacts, formed by household members and very close friends with whom users are strongly bound. Proximity sharing was found useful for sharing location in practical cases by users, such as with a set of selected friends in their free time, while ad-hoc meetings obtained the largest approval by participants, who appreciated in particular the possibility to set up a sharing mechanism which is limited in time to the duration of the current event.

In the next steps of my research my goal is to clarify the actual use of location sharing by users, uncovering the goals they wish to reach through sharing. My plan is to integrate the location sharing modes presented above, together with other common sharing mechanisms such as manual check-ins and automatic check-ins, which are already available in several products on market. I then plan to run a field study in which the above-mentioned different sharing functionalities are provided to users and evaluated in a longitudinal study. The role of the user interface will be crucial for making location sharing application simple and usable for users, and to let people feel in control of their data. To understand how people are using these tools and whether they feel satisfied with the on-going location sharing processes, I plan to take advantage of experience sampling methods, through which questions can be asked to users in context, i.e., while users are actually using the application. Finally, I plan to integrate all the above features in a unified privacy-aware system, where the architecture works as an efficient infrastructure for various location sharing modes, and adequate security mechanisms are chosen for every sharing mode.

ACKNOWLEDGEMENTS

This work is being developed within the PALS project funded by the Swiss National Science Foundation under grant n. 200021_129674.

REFERENCES

1. S. Amin, S. Andrews, S. Apte, J. Arnold, J. Ban, M. Benko, R. Bayen, B. Chiou, C. Claudel, C. Claudel, et al. Mobile Century Using GPS Mobile Phones as Traffic Sensors: A Field Experiment.

2. G. Ateniese, K. Fu, M. Green, and S. Hohenberger. Improved proxy re-encryption schemes with applications to secure distributed storage. In *Proceedings of the 12th Annual Network and Distributed System Security Symposium*, pages 29–44, 2005.

3. A. R. Beresford and F. Stajano. Location privacy in pervasive computing. *Pervasive Computing, IEEE*, 2(1):46 – 55, 2003.

4. A. R. Beresford and F. Stajano. Mix Zones: User Privacy in Location-aware Services. In *Proceedings of the Second IEEE Annual Conference on Pervasive Computing and Communications Workshops*, pages 127 – 131, 2004.

5. M. Blaze, G. Bleumer, and M. Strauss. Divertible protocols and atomic proxy cryptography. *Advances in*

[3] http://glympse.com

Cryptology - EUROCRYPT 1998, pages 127–144, 1998.

6. S. Consolvo, I. E. Smith, T. Matthews, A. LaMarca, J. Tabert, and P. Powledge. Location disclosure to social relations: why, when, & what people want to share. In *CHI '05: Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 81–90, USA, 2005. ACM.
7. C. Dong and N. Dulay. Longitude: a privacy-preserving location sharing protocol for mobile applications. *Trust Management V*, pages 133–148, 2011.
8. P. Dourish and K. Anderson. Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-computer interaction*, 21(3):319–342, 2006.
9. M. Duckham and L. Kulik. A formal model of obfuscation and negotiation for location privacy. In *Proceedings of the Third international conference on Pervasive Computing*, pages 152–170. Springer-Verlag, 2005.
10. N. Eagle, A. Pentland, and D. Lazer. Inferring friendship network structure by using mobile phone data. *Proceedings of the National Academy of Sciences*, 106(36):15274–15278, 2009.
11. B. Gedik and L. Liu. A customizable k-anonymity model for protecting location privacy, 2004.
12. M. Gruteser and D. Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proceedings of the 1st International Conference on Mobile Systems, Applications and Services (MobiSys '03)*, pages 31–42, USA, 2003. ACM Press.
13. M. Gruteser and B. Hoh. On the anonymity of periodic location samples. In *In Proceedings of the Second International Conference on Security in Pervasive Computing*, pages 179–192. Springer, 2005.
14. B. Hoh, M. Gruteser, H. Xiong, and A. Alrabady. Enhancing security and privacy in traffic-monitoring systems. *IEEE Pervasive Computing*, 5:38–46, 2006.
15. J. H. Kang, W. Welbourne, B. Stewart, and G. Borriello. Extracting places from traces of locations. *ACM SIGMOBILE Mobile Computing and Communications Review*, 9:58–68, 2005.
16. J. Krumm. Inference attacks on location tracks. In *Proceedings of the 5th international conference on Pervasive Computing*, pages 127–143. Springer-Verlag, 2007.
17. J. Krumm. A survey of computational location privacy. *Personal Ubiquitous Computing*, 13:391–399, 2009.
18. M. Langheinrich. Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems. In *Proceedings of the 3rd international conference on Ubiquitous Computing*, pages 273–291. Springer-Verlag, 2001.
19. S. Mascetti, D. Freni, C. Bettini, X. S. Wang, and S. Jajodia. Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies. *The VLDB Journal - The International Journal on Very Large Data Bases*, 20(4):541–566, 2011.
20. D. Patterson, L. Liao, D. Fox, and H. Kautz. Inferring high-level behavior from low-level sensors. In *Proceedings of the 5th international conference on Ubiquitous computing*, pages 73–89, 2003.
21. M. P. Scipioni and M. Langheinrich. I'm Here! Privacy Challenges in Mobile Location Sharing. Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU), 2010. Co-located with Pervasive 2010.
22. M. P. Scipioni and M. Langheinrich. Towards a new privacy-aware location sharing platform. *Journal of Internet Services and Information Security*, 1, 2011.
23. M. P. Scipioni and M. Langheinrich. To Share or Not To Share? An Activity-centered Approach for Designing Usable Location Sharing Tools. Workshop on Usable Privacy & Security for Mobile Devices (U-PriSM), 2012. Co-located with Soups 2012.
24. E. Toch, J. Cranshaw, P. Drielsma, J. Tsai, P. Kelley, J. Springfield, L. Cranor, J. Hong, and N. Sadeh. Empirical models of privacy in location sharing. In *Proceedings of the 12th ACM international conference on Ubiquitous computing*, pages 129–138. ACM, 2010.
25. J. Tsai, P. Kelley, L. Cranor, and N. Sadeh. Location-sharing technologies: Privacy risks and controls. In *Research Conference on Communication, Information and Internet Policy*, 2009.
26. Y. Zheng, Y. Chen, Q. Li, X. Xie, and W. Ma. Understanding transportation modes based on GPS data for Web applications. *ACM Transactions on the Web (TWEB)*, 4(1):1–36, 2010.