Towards a New Privacy-Aware Location Sharing Platform

Marcello Paolo Scipioni

University of Lugano (USI), Faculty of Informatics, 6904 Lugano, Switzerland

Abstract. Location-based social networking services are becoming very popular among the multitude of mobile applications. The new location sharing functionalities made possible by GPS-based mobile phones, however, also raise two main privacy issues: users often have to share their location data with the service providers; moreover, users are often offered built-in sharing options that just allow for sharing or un-sharing data with friends.
This paper describes two approaches to protect location data from the service provider and to give more privacy options by allowing users to share with different people location data at different granularities. The final goal of automatic group-based sharing is discussed: the resulting platform will be able to automatically share with each friend location data at a different granularity based on the distance from that friend.

1 Introduction

The widespread availability of GPS-enabled smart-phones has pushed the popularity of location-based mobile applications, which offer new location-based social networking features that are very appealing to users, like Google Latitude or Facebook Places[1]. People can share their location with friends thanks to their phone-based applications, which are becoming the killer-apps of the moment.

While most of these services are free, however, there is usually a price to pay: user's location is freely shared with marketers, who develop detailed location profiles to better target online advertising. Moreover, customers are usually only offered very basic privacy settings: typically, users can decide, for each of their friends, whether to share their location with them or not. Recent surveys[2] highlight that, although people feel this kind of services valuable, users are concerned by the lack of control over location data in current LBS. This approach, which forces users to a binary decision, fails in giving effective ways to differentiate the level of detail (e.g. exact location or neighbourhood, city, or country level location) of the shared data among different friends.

This paper describes two approaches for protecting user location data tracks from the service provider and to give richer privacy settings through the offer of different location granularities. Moreover, the envisioned step for merging the

[1] `http://www.google.com/latitude`, `http://www.facebook.com/places`
[2] `http://www.microsoft.com/privacy/dpd`

two solutions in a unified architecture are discussed. The outlook of this work is to create a location sharing tool for supporting automatic friend-grouping and distance-based accuracy determination: friends in the same city will share neighbourhood-level location, friends in different cities will share city-based location, and so on, depending on their relative positions.

2 XMPP-Based Location Sharing: a First Approach

A simple way to solve the issues introduced by the disclosure of location data to the service provider is to build an XMPP-based messenger-like architecture. Such a solution, based on an XMPP[3] client-server structure, allows users to add friends through their client application and share their location by exchanging messages containing their GPS position, which is then displayed by the UI on a map. Given the messaging structure, users can encrypt end-to-end the whole traffic with public key cryptography: the clients can send encrypted location updates, and the server only works as a router to send encrypted messages to the recipients.

This configuration has the advantage of hiding all the location data to the service provider; however, notifications can happen only when both users are simultaneously online. Moreover, each client needs a different key for each friend and has to send a different encrypted message for each friend. It is also possible to employ multiple XMPP servers in a peer-to-peer fashion; bringing it to the extreme, an XMPP server per user could be used [1]. The performance analysis conducted by Mayrhofer et al. showed that this approach is still feasible.

3 Sharing Different Location Granularities

Although the simple XMPP-based messenger protects users from unwanted location disclosure to service providers, it does not provide any way for sharing different location granularities (e.g. exact location or neighbourhood, city, or country level location) for different contacts. This can be accomplished by replacing the end-to-end messenger structure with a publish-subscribe (pubsub) client-server architecture, where the privacy options are enforced on a group basis. The general structure of the conceived architecture is shown in Figure 1.

Each user in the client application can add new contacts, which are combined together in groups. From the server side, each user is associated with a *collection node*, i.e. a set of pubsub nodes. A *component* works as a trusted third party among the client and the server[4]. For each new group of contacts, the component creates a new pubsub node, containing location data having accuracy set by

[3] XMPP is an open-source protocol used for presence notification and instant messaging (see `http://xmpp.org`). XMPP is used e.g. in Google Talk (see `www.google.com/talk`) and Facebook chats (see `www.facebook.com/sitetour/chat.php`).

[4] The communication protocol between the XMPP server and the component is specified at `http://xmpp.org/extensions/xep-0114.html`

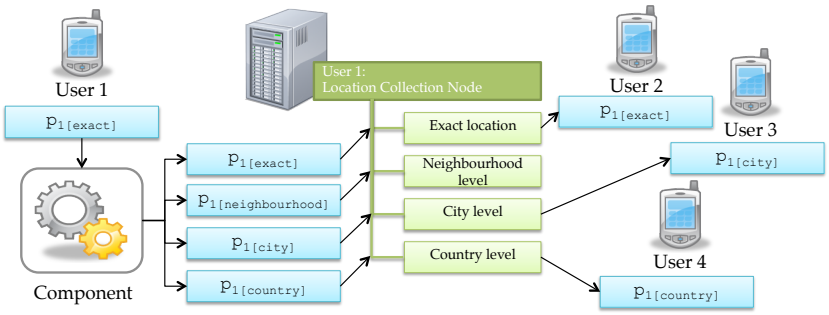

Fig. 1. Architecture of the component-based platform: the client sends a single message to the component, which updates all the nodes according to their accuracy.

the user (street, city, state, country level). Users can thus allow for different location granularity by assigning contacts to different groups. However, the client application never pushes data directly to the pubsub nodes; rather, it sends a geoloc packet to the component which parses it, reverse geocodes it[5] and pushes data onto the different user nodes according to their granularity.

An advantage of this approach is that the client application has to send just one message to the component, and all the friends can see the location update through the pubsub node they have access to. Moreover, when friends are offline, the most recent location update is always available on the server. The modularity of this system has also made simple the implementation of rule-based location disclosure: since only the component can update location on the nodes, it is also possible to configure it in order to limit the location disclosures within user-defined time slots and/or when the subject is within a certain area, similarly to the Loccaccino privacy settings [4].

4 Summary and Outlook

The goal of this work is to deploy the described system and to test it with real users. Until now, both an XMPP-messenger and a component-based prototype systems have been implemented, based on Openfire[6] from the server side and on Android from the client side. A deployment phase of the system is planned in summer 2011, for which the centralized component-based structure will be used. We plan to run a month-long study during which smart-phones will be distributed to around a dozen users with strong social relationships. We would like to involve pilot users belonging to large families, possibly with multiple children – teenagers would work best – to inspect how differently aged people react to the system, and in particular how they use multiple location accuracies at the

[5] The reverse geocoding service available through the Google Maps API is used.

[6] `http://www.igniterealtime.org/projects/openfire`. Openfire is an open source implementation of XMPP server.

same time for sharing with different contacts, since to our knowledge none of the currently available systems offers this option. It would also be interesting to inspect through weekly meetings what kind of family dynamics arise, whether users find the system useful in its privacy-oriented distinctive features and whether the system helps users to increase their awareness of location privacy risks.

At the same time, due to the modular architecture of the system, a number of future architectural extensions are possible. The group-based sharing options available should be extended with group-based cryptography [2] to also protect them from the service provider. Moreover, the data leakage towards the reverse geocoding provider may be avoided by implementing it inside the client using publicly available geographic data; this would allow to look up the appropriate description of the place directly on the phone[7]. For coarse-grained level locations (neighbourhood, city), however, the common location representation with points on a map surrounded by large circles might be confusing for users, which tend to associate the real location with the center of the circle; symbolic description or even user-entered names may be preferable in these cases, and may allow for personalization and more expressive communication.

The resulting architecture will be able to accomplish both the goals of protecting against unwanted disclosure of location data to the service provider and of giving more privacy options. The perspective of this work is to allow for automatic disclosure of location with the appropriate accuracy; the system would need then to compute the distance among two encrypted locations and consequently decide the right accuracy for the current friend. Homomorphic encryption would be helpful in computing the distance blindly – i.e. without the need of decrypting location data [3]. Such automated rules for managing group-based sharing can be of help in applications where the level of detail of shared data depends on the distance among users.

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

References

[1] R. Mayrhofer, C. Holzmann, and R. Koprivec. Friends Radar: Towards a private P2P location sharing platform. Proc. of MCPT - First Int. Workshop on Mobile Computing Platforms and Technologies, Las Palmas, Spain. @ Eurocast 2011.

[2] S. Rafaeli and D. Hutchison. A survey of key management for secure group communication. *ACM Computing Surveys (CSUR)*, 35(3):309–329, 2003.

[3] S. Rane, W. Sun, and A. Vetro. Secure distortion computation among untrusting parties using homomorphic encryption. In *Image Processing (ICIP), 2009 16th IEEE International Conference on*, pages 1485–1488. IEEE, 2009.

[4] 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 *Proc. of Ubicomp*, pages 129–138. ACM, 2010.

[7] Datasets with Swiss boundaries can be found, e.g. at `www.swisstopo.admin.ch/internet/swisstopo/en/home/products/landscape/swissBOUNDARIES3D.html`