On Limitations of Existing Methods for Location Privacy

Mads Schaarup Andersen
Department of Computer Science
Aarhus University
Aarhus, Denmark
masa@cs.au.dk

ABSTRACT

This paper argues that there are some limitations when applying location privacy methods developed for point-of-interest services to newer classes of location based services. We support the argument by categorizing methods for location privacy and identifying the issues. It is hypothesized that a more comprehensive analysis of the different ways in which location is used in a system can provide the grounds for choosing a combination of appropriate methods, instead of looking for one overall method.

1. INTRODUCTION

With the number of smart phones based on Android and iOS soon exceeding the number of stationary and laptop computers on the Internet, applications for these devices, usually referred to as *Apps*, are becoming increasingly interesting. One of the interesting aspects of Apps are that they are able to incorporate sensor data from the device and use it to provide services based on these. Currently, many apps are available for these devices and a subset of these use the location of the device (computed in some way using one of more sensors) as an integrated and essential part. These are called location based services (LBSs). In February 2010, there were 6,400 LBSs in Apples AppStore and more than 1,000 LBSs in Androids Marketplace[1]. Using location as an integrated part of an application has enabled a number of new application domains such as navigation, friend finder, route tracking, etc. However, these services require the user to disclose his location. This introduces the concern of preserving the privacy of the user. In 1993, Bellotti and Sellen recognized that ubiquitous computing is particularly prone to attack on privacy [1] and in 2001, Langheinrich proposed six guidelines to system design to include privacy concerns [8]. Partly based on these guidelines, a number of methods have been proposed as more general approaches to solving the privacy problem. Early work in the field was mainly focused at adding privacy to *point-of-interest (POI)* services as these were the dominant LBSs at the time. A POI service is characterized by querying a LBS for the location of an object, either in a reactive or proactive manner. An example is *find nearest gas station*, where POI location privacy is focused on hiding the position of the user from the server and still being able to get the nearest gas station. Location privacy methods for POI services include methods such as *k-anonymity [6], Mixed Zones [2], and CliqueCloak [5].* However, recently new classes of LBSs have emerged. These are: *Crowd-sensing, City-watch, Route Tracking,* and *Social Network Services (SNSs).* This entails that methods such as the aforementioned cannot necessarily be directly applied. This is both due to the fact that rather than following the *request-reply* pattern, these applications might provide the server with data about server without needing an answer e.g. in traffic monitoring systems and in friend finder services where one wants to make the location available to friends, and the fact that the methods might hide the user location making it impossible to share it with others. Some work has been done in the area of location privacy in the newer classes of LBSs. This includes projects such as Loccacino, which explores privacy in Social Network Services [11], and Hitchhiking, which explores privacy in Crowd-sensing applications [10]. However, this work does not fully cover the question of whether the above mentioned methods can be applied to the new classes of LBSs.

[1]http://www.skyhookwireless.com/locationapps/

2. ISSUES WITH EXISTING METHODS

To understand how different privacy methods can be applied to different classes of LBSs an overview of the issues of location privacy methods has to be provided. Privacy methods can be divided into five categories. (Freely adapted from Duckham and Kulik [4] with the addition of the Cryptographic category.)

- *Anonymity/Pseudonymity* - Privacy by hiding identity. In anonymity, this is done by never providing any information which can be used to identify the user. It is still possible to see an exact location, but it cannot be identified who is at that location. In pseudonymity an identifier is applied to a location, but it should be impossible for an adversary to map this identity to an actual user. *Possible issues:* Hiding the identity of the user conflicts with sharing the position with friends.

- *Obscurification* - Privacy by not revealing the exact location. There are two basic forms of obscurification: *temporal* and *spatial*. In the temporal model, it is possible to see that a user has been at a certain location, but not when. In spatial obscurification, the location of the users is hidden in an area larger than a single point. *Possible issues:* Adding temporal obscurification makes it impossible to create a crowd-sensing map. Adding spatial obscurification makes it impossible to share a precise location.

- *Policy Based* - Privacy by allowing/denying subjects permission to the location. Comparable to access con-

Third International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)
June 12, 2011, San Francisco, CA, USA

trol in a file system. *Possible issues:* Might not be expressive enough.

- *Protocol* - Privacy by custom communication protocol. *Possible issues:* Adding privacy to an existing LBS requires changing all communication.

- *Cryptographic* - Privacy by cryptography. This can e.g. be done in social network services where users share locations through a server using public key cryptography. *Possible issues:* Server still knows which parties are communicating.

3. CHALLENGES

As outlined above, a number of location privacy methods have been proposed. The problem is that these are usually quite formally defined, and usually only tested on an example application where the possible issues and limitations of the methods are not usually explored. To have real-world applicability, the methods need to be examined in a wider range of applications. A way to do this, would be to do a survey of the different characteristics of privacy methods, and see how these map to LBSs. The need for such a study is also recognized by Krumm in his 2009 survey of computational location privacy [7]. However, Krumm's survey is limited to computational location privacy methods. To get a full overview of how location privacy methods map to LBSs, it is necessary to include non-computational methods such as *policy based*. In their 2010 paper, Scipioni and Langheinrich propose a categorization based on the multiplicity of data sharing between sender and receiver(s) [9]. This categorization is based on social network services and, therefore, it might add value to broaden this categorization by including POI services as the main part of the methods proposed are of this category.

One of the more unexplored classes of location privacy is *Route Tracking* and hence it seems that more work needs to be done in this area. Within this class, an interesting application domain is the use of location in cars which so far has mostly been limited to navigation. This domain has a number of applications such as enforcing speed limits by automatically issuing speeding-tickets, road-pricing, and usage-based insurance where the insurance premium is calculated based on car usage and driving habits. One overall solution to these three things is addressed by Coroama in the *Smart Tachograph* project [3] which also discusses the privacy considerations. However, the way in which location is used in these three types of applications (within the same system) is not the same. Automatic speeding-tickets requires that a service is queried for the speed limit of the location so it can be determined whether the driver adheres to the speed-limits; road-pricing requires that a service receives the track of the car so that it can be determined how much the driver has been using pay-roads; and usage-based insurance uses location to determine whether the driver drives in high risk areas at high risk times. I.e. rather than using one overall privacy method for such a system, it might make sense to use a different privacy method for each of the applications even though they are part of the same overall system. This approach also makes sense in relation to SNSs where sharing the user location with friends does not necessarily entail the same privacy requirements as making a review of a restaurant.

4. CONCLUSION

This paper outlined a number of interesting challenges in location privacy and a categorization of existing methods stating possible issues. It was pointed out that applying and combining existing location privacy methods to new classes of LBSs would be interesting and it was hypothesized that a more thorough analysis of the use of location in applications could assist in choosing a combination of privacy methods rather than one overall method. Route tracking was identified as being especially interesting due to lack of work in the area. This was exemplified with the use of location in cars.

5. REFERENCES

[1] Victoria Bellotti and Abigail Sellen. Design for privacy in ubiquitous computing environments. In *Proc. of the 3rd European Conf. on Computer-Supported Cooperative Work*, pages 77–92. Kluwer, 1993.

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

[3] Vlad Coroama. The smart tachograph - individual accounting of traffic costs and its implications. In *Proc. of the 4th Int. Conf. on Pervasive Computing*, volume 3968 of *Pervasive*, pages 135–152. Springer Berlin / Heidelberg, 2006.

[4] M. Duckham and L. Kulik. *Drummond J (ed) Dynamic & mobile GIS: investigating change in space and time*. CRC, 2006.

[5] B. Gedik and Ling Liu. Location privacy in mobile systems: A personalized anonymization model. In *Proc. of the 25th IEEE Int. Conf. on Distributed Computing Systems*, pages 620 –629, 2005.

[6] Marco Gruteser and Dirk Grunwald. Anonymous usage of location-based services through spatial and temporal cloaking. In *Proc. of the 1st Int. Conf. on Mobile Systems, applications and services*, MobiSys '03, pages 31–42, New York, NY, USA, 2003. ACM.

[7] John Krumm. A survey of computational location privacy. *Personal Ubiquitous Comput.*, 13:391–399, August 2009.

[8] Marc Langheinrich. Privacy by design - principles of privacy-aware ubiquitous systems. In *Proc. of the 3rd Int. Conf. on Ubiquitous Computing*, UbiComp '01, pages 273–291, London, UK, 2001. Springer-Verlag.

[9] Marcello Paolo Scipioni and Marc Langheinrich. I'm here! privacy challenges in mobile location sharing. *2nd Int. Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use*, 2010.

[10] Karen P. Tang, Pedram Keyani, James Fogarty, and Jason I. Hong. Putting people in their place: an anonymous and privacy-sensitive approach to collecting sensed data in location-based applications. In *Proc. of the SIGCHI conf. on Human Factors in computing systems*, CHI '06, pages 93–102. ACM, 2006.

[11] Eran Toch, Justin Cranshaw, Paul Hankes Drielsma, Janice Y. Tsai, Patrick Gage Kelley, James Springfield, Lorrie Cranor, Jason Hong, and Norman Sadeh. Empirical models of privacy in location sharing. In *Proc. of the 12th ACM Int. Conf. on Ubiquitous computing*, Ubicomp '10, pages 129–138. ACM, 2010.