Location Privacy Protection Mechanisms in Location-Sharing Service

Fei Xu[1], Jingsha He[2], Jinqiao Shi[3], Jing Xu[1] and Yuqiang Zhang[1]

[1]*Computer Science and Technology*
[2]*School of Software Engineering*
Beijing University of Technology, Beijing 100124, China
[3]*Institute of Information Engineering*
Chinese Academy of Sciences, Beijing 100195, China
[1]*{xfei, hxj, yqzh}@emails.bjut.edu.cn,* [2]*jhe@bjut.edu.cn,*[3]*shijinqiao@iie.ac.cn*

Abstract

The blooming of location-sharing services has led to serious privacy concerns, particularly location privacy concerns. In this paper, we first discuss the definition of location privacy and then review several location privacy protection mechanisms. After that, we classify location privacy protection mechanisms into four categories: legislation & regulatory, anonymity & obfuscation, protocol and policy-based protection. We explain each privacy protection mechanism category in detail and discuss if it can be used in particular kind of location-sharing services along with their advantages and disadvantages.

Keywords: *location-sharing services; location privacy; privacy protection mechanisms.*

1. Introduction

Location-based services, notably the location-sharing services, are becoming ubiquitous and represent a growing market with the proliferation of mobile devices and the maturing of location-based service applications. There exist numerous applications that allow users to share their location information with each other. Meanwhile, as the list of applications that use users' location information grows, concern about privacy risks is increasing along with it. Location information is considered to be privacy-sensitive by the overwhelming majority of users since location information is personal and can be used to infer other personal information such as identity and social activities. There are concerns that location information can be used to cause undesirable consequences, such as location-based spam, compromising personal safety and intrusive inferences, i.e., inferring personal information or embarrassing proclivities.

Location privacy was defined by Duckham and Kulik as a special type of information privacy which concerns the claim of individuals to determine for themselves when, how, and to what extent location information about them can be communicated to others [1]. Privacy is regarded as a fundamental human right. Therefore, everyone should have the right to location privacy and access to user's location information should be protected since any leakage of such information would lead to serious privacy violation.

There is already a rich collection of literature that aims at protecting the privacy of users using location based services. However, there has been little discussion about location privacy protection mechanisms in location-sharing services. In some papers, location-sharing services and location-based services are not well distinguished. In this paper, we consider location-sharing services as a special kind of location based services. Location-sharing services refer

only to the services that specifically allow one user to share his or her location information with another user. We mainly discuss location privacy in location-sharing services.

The rest of this paper is organized as follows. In the next section, we review related work. In Section 3, we present the types of location protection mechanisms in location-sharing services and discuss their characteristics as well as the differences between then. Finally, we conclude this paper in Section 4.

2. Related Work

There are already several survey papers about location privacy, most of which are focused on location privacy in location-based services. Although there are differences between location-sharing services and location-based services, some of the privacy protection mechanisms can be used in both services.

In paper [1], Kulik gave a general introduction to location privacy. The paper first discussed the background information like definition of location privacy and positioning systems. It then classified existing privacy protection strategies into four types: regulatory, privacy policies, anonymity and obfuscation. After explicit discussion, the paper concludes that no single strategy currently available is capable of providing a complete solution to location privacy protection since each strategy has its own advantages and disadvantages.

In paper [2], Krumm discussed computational approaches in location privacy protection. Main approaches include anonymity and obfuscation. The paper first talked about the definition of location privacy and then discussed the need for location share after analyzing location privacy threats and stressing the need for location privacy protection. The paper focused on computational privacy protection measures in which popular anonymity approaches include pseudonym, K-anonymity, L-diversity and false locations. Special and temporal obfuscation approaches to protect location privacy include obfuscation. However, all the mechanisms sacrifice user location accuracy. The paper also discussed privacy protection in certain applications such as querying for weather or being alerted when a friend is near.

In Paper [3], Tsai et al. first discussed the main privacy issues in real time location based services and then gave an overview of existing approaches for location privacy protection. The paper provided a survey of open problems and possible future research directions in real-time location-based services. Important problems include the quantification of location privacy, the need for decentralized structure of location privacy protection, etc.

In paper [4], Burghardt et al. thoroughly evaluated privacy risks and privacy controls in existing commercial location sharing applications by conducting an online survey. The survey reached the conclusion that people's privacy concerns had not been comprehensively addressed by industry guidelines or existing applications and suggested that more expressive and individualized privacy controls should be made available to the users. Meanwhile, ways of reducing user burden should also be considered.

3. Privacy Protection Mechanisms

In this section, we classify different mechanisms existed for privacy protection in location sharing services into four categories: legislation & regulatory, anonymity & obfuscation, protocol and policy-based protection. We discuss each category in detail and analyze their advantages and disadvantages.

3.1. Legislation & Regulatory

Legislation and regulatory privacy protection methods involve the development of rules and regulations to govern fair use of location information. It contains government rules on the use of location information and self-regulation. For example, Internet Safety Task Force is a type of self-regulation, which was originally formed by MySpace and 49 State Attorney Generals and is now managed by the Berkman Center at Harvard University, to set the rules on the use of privacy information.

Legislation and regulatory can be easily used in location sharing services and most location sharing services are using this method. However, this method alone cannot fulfill user privacy requirements. Firstly, it only ensures as accountability when unauthorized access to information happens. It cannot provide ways of preventing information from leakage. Secondly, since each user may have different privacy requirement, legislation and regulatory approach may not be flexible enough to fit the needs of all the users. Therefore, other technical solutions to privacy protection must be provided.

3.2. Anonymity & Obfuscation

Anonymity and obfuscation are two of the most popular methods in location privacy protection. Anonymity is to use a pseudonym and create ambiguity by grouping an individual with other people. Many location privacy protection mechanisms based on k-anonymity and l-diversity have been proposed to provide anonymized use of location information.

K-anonymity methods cause the accuracy of the disclosed location to be reduced since a user is made indistinguishable from at least other 'K-1' users in the same area. L-diversity based location privacy protection mechanisms extend the shared clocking area until 'L-1' different locations are included. Obfuscation is to reduce the quality of the location data to protect user location privacy. Anonymity and obfuscation can all result in sacrificing the quality of information about user's location to protect user's identity and location privacy.

There are many studies on these two types of methods. For example, in paper [5], the authors proposed a middleware system which delays and reorders messages from users within a mix zone to confuse an observer. In paper [6], a cloaking mechanism is described which can conceal a user within a group of k people. In paper [7], the mechanism for achieving k-anonymity is through an ad-hoc network formed by users and surrounding neighbors meanwhile in paper [8], the authors proposed a method to achieve k-anonymity in a distributed environment where there are multiple non-colluding servers.

However, since the main propose of location sharing services is to share location between two qualified users, if one user is sharing location information with another user, they should already be willing to share their information and, therefore, should not hide their true identity or obfuscation their location information. Therefore, anonymity & obfuscation may not directly applicable in many location-sharing services.

3.3. Protocol

This kind of privacy protection method involves protecting user privacy by using some kind of protocols. The protocols often use some encryption schemes to prevent information from being leaked to unauthorized parties. Since there are many types of location sharing services, service providers can develop different protocols to meet different requirements. Encryption protocol always plays an important role in information protection as well as privacy protection.

The design of Longitude [9] is based on proxy re-encryption. In Longitude, the actual data is encrypted by using an efficient hybrid encryption scheme, in which a secure symmetric

stream cipher is chosen to encrypt the location data using a random key and the random key is then encrypted using the proxy re-encryption scheme. Longitude can ease privacy concerns by making it possible to share a user's location data blindly and allowing the user to control who can access his/her location information as well as when and to what degree of precision.

3.4. Policy-based Protection

Privacy policies are most often used in privacy protection mechanisms in location sharing services. By defining privacy policies, a user can specify who can access his/her location data, over what period of time, and to what degree of precision. In paper [3], Tsai et al. examined 89 location-sharing services and showed that the most widely adopted privacy controls include white list, being invisible, blacklist, group-based permission and those providing less detailed location. White lists appear to be particularly ineffective at capturing user's preferences. Several research projects in this area have tried to provide more expressive and effective policy settings to enhance policy-based privacy controls.

For example, pawS system [10] allows users to use P3P policies to define their location privacy settings and to negotiate with location service providers. Locaccino [11] is a location-based friend-finding service for Facebook developed by Carnegie Mellon University. It is a location-sharing system that allows users to have more precise control over who can see user's locations. Users can define the times when they want to share the location information and the regions where they do and don't want other people to find them, and can also decide who can see where exactly they are, who gets a blurrier vision or none at all. Locaccino exhibits the problem that service providers know everything about user's locations and, even more, service providers know user's privacy preferences settings, which is considered to be another kind of user privacy for many users.

Policy-based protection through service providers, middleware and third parties remains a source of concern. Also, privacy policies provided by existing location sharing services are often too simple and hence can hardly fully meet the needs of user's privacy preferences.

4. Conclusion

In this paper, we discussed the definition of location privacy in which we differentiated location-sharing services from location-based services. We revealed several papers about location privacy and also classified existing privacy protection mechanisms in location-sharing services into four categories: legislation & regulatory, anonymity & obfuscation, protocol and policy-based protection. We introduced each type of location privacy mechanism in detail and discussed their advantages and disadvantages. As location sharing services grow at an amazing speed, we believe that in order to better protect user location privacy in location sharing services, more work should be done in both research and practices.

References

[1] L. Kulik, "Privacy for Real-time Location-based Services", In: SIGSPATIAL Special **(2009)**.

[2] J. Krumm, "A Survey of Computational Location Privacy", Journal of Personal and Ubiquitous Computing, 13, 6 **(2009)**.

[3] 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 (TPRC), **(2009)**.

[4] T. Burghardt, E. Buchmann, J. M¨uller and K. B¨ohm, "Understanding User Preferences and Awareness: Privacy Mechanisms in Location-based Services", In OnTheMove Conferences (OTM), **(2009)**.

[5] A. Beresford and F.Stajano, "Location Privacy in Pervasive Computing", IEEE Pervasive Computing, 2(1), 46-55 **(2003)**.

[6] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-based Services through Spatial and Temporal Cloaking", In: MobiSys **(2003)**.

[7] T. Hashem and L. Kulik, "Safeguarding Location Privacy in Wireless Ad-hoc Networks", In: Krumm, J., Abowd, G.D., Seneviratne, A., Strang, T. (eds.) UbiComp 2007. LNCS, vol. 4717, pp. 372-390. Springer, Heidelberg **(2007)**.

[8] G. Zhong and U. Hengartner, "A Distributed k-Anonymity Protocol for Location Privacy", In: IEEE International Conference on Pervasive Computing and Communications PerCom 2009, pp. 1-10 **(2009)**.

[9] C. Dong and N. Dulay, "Longitude: A Privacy-Preserving Location Sharing Protocol for Mobile Applications", In: Proc. of IFIPTM 2011, IFIP AICT 358 **(2011)**.

[10] M. Langheinrich, "A Privacy Awareness System for Ubiquitous Computing Environments", In: Borriello, G., Holmquist, L.E. (eds.) UbiComp 2002. LNCS, Vol. 2498, pp. 237-245. Springer, Heidelberg **(2002)**.

[11] Locaccine: A User-Controllable Location-Sharing Tool. http://locaccino.org/

Authors

Fei Xu is currently a Ph.D. candidate in the College of Computer Science and Technology at Beijing University of Technology. Her research interests include network and information security, especially privacy protection.

Jingsha He is currently a professor of the School of Software Engineering at Beijing University of Technology. His research interests include network security and wireless communication technologies.

Jinqiao Shi is an Associate Professor of Institute of Information Engineering, Chinese Academy of Sciences. Between 2007 and 2011, he has been with Institute of Computing Technology, Chinese Academy of Sciences. His research interest is network and information security, especially privacy enhancing techniques, data leakage detection and protection, and anomaly detection in massive dataset.

Jing Xu is currently a Ph.D. candidate in the College of Computer Science and Technology at Beijing University of Technology. Her research interests include network and information security and privacy protection.

Yuqiang Zhang is currently a Ph.D. candidate in the College of Computer Science and Technology at Beijing University of Technology. His research interests include network and information security and privacy protection.