Privacy Protection in Location-Sharing Services

Fei Xu
College of Computer Science and Technology
Beijing University of Technology
Beijing 100124, China
xfei@emails.bjut.edu.cn

Jingsha He
School of Software Engineering
Beijing University of Technology
Beijing 100124, China
jhe@bjut.edu.cn

Matthew Wright
Department of Computer Science and Engineering
The University of Texas at Arlington
Arlington 76019, US
mwright@uta.edu

Jing Xu
School of Software Engineering
Beijing University of Technology
Beijing 100124, China
hxj@emails.bjut.edu.cn

***Abstract*—with the fast development in mobile computing devices, location-sensing technology and wireless communication, new applications for share users' real-time location information are developing at an amazing pace. Location privacy is of utmost concern for location-sharing services. There is already a full agreement that users would like to have the complete control over their location information. Existing privacy protection methods often let users specify their privacy peferences to the service provider and thus not only fail to consider the dynamic nature of privacy preferences but also fail to protect user privacy from service provider. In this paper, we propose an user-centric privacy access control method. By separating sensitive privacy polices apart from standard privacy policies, which are now stored at user side and therefore fully under user's control, we demonstrate that our system can provide users with a flexible way of complete controlling over information about their location without adding too much user burden.**

Keywords-privacy protection; location-sharing services; access control

I. INTRODUCTION

With the fast development in mobile computing devices, location-sensing technology and wireless communication, a new generation of location-based services has come. Today's location-based business offers a broad set of dynamic, feature-rich services that are exciting and desirable to the users, making people's life more convenient. Unlike the first generation LBS, which are reactive, self-referencing, single-target, and content-oriented, today's LBS evolved to proactive, cross-referencing, multitarget, and application-oriented [1]. Location became another context item frequently exchanged between the members of a social network and location sharing became a basic function of many of today's multitarget LBSs.

With the rapid growth of location-sharing services comes the concerns of location privacy, regarding the sharing and use of user's location information. The precise location uniquely identify one person. Most people would not feel comfortable if their current location were known by others without their authorization [2]. It is suggested that a person's location is revealed to other entities, such as a service provider or the person's friends, only if the release is strictly necessary and authorized by that person [3].

However, in location sharing services, users are often forced to share their location information with service providers in order to get the services. Due to many technical and administrative reasons, user's private information is often poorly managed by service providers and sometimes abused, resulting in serious privacy violations: users' sensitive data can be inadvertently leaked, can fall under the control of hackers, and can be abused by service administrators [4]. Besides, there are survey shows that it is rare that systems give users the ability to specify expressive rules to control the sharing of their location information with others.

In this paper, we proposed an user-centric access control method to protect user location privacy in location sharing systems. In the proposed method, we separate sensitive privacy policies from standard privacy policies. The sensitive privacy polices are stored at the user side while standard privacy polices are stored at the service provider side. By doing this, we provide the users a flexible way to control their privacy preferences and to protect their privacy from the service provider without adding too much user burden.

The rest of this paper is organized as follows. In the next section, we review some background information of locating technologies, which is the foundation of location sharing system and analyse location privacy and user privacy preferences, which must be considered to design a good privacy protection method. In section III, we review some related work on location privacy protection in existed location sharing systems. we formally present our privacy access control method in section IV and describe a access control decision procedure to show how our method work in Section in section V. We conclude this paper in section VI which we also present our future works.

II. BACKGROUND INFORMATION

In this section, we briefly introduce and analyse the background information of location privacy protection in location sharing systems. First we introduce the locating technologies and then the location privacy is analysed.

A. Locating technologies

There are several locating technologies to determine a user's location [5]. GPS is the most popular and accurate way to locate a user. It locates a user through a device, such as a mobile phone, that is in communication with a constellation of satellites. It is a kind of user-based positioning systems. In user-based positioning systems,

mobile clients autonomously compute their own location and it is possible for a client not revealing that location to any other entity.

Cell phone positioning using CGI (cell global identity) is another kind of locating method. A cell phone usually is in signal range of upwards of three cell phone towers, allowing a location to be triangulated since the locations of the cell towers are known. It is a kind of network-based positioning systems, in which the network infrastructure is responsible for computing a mobile client's location. In network-based positioning systems, the network infrastructure administrator hold information about the location of mobile clients.

A-GPS is a combination of user-based and network-based positioning system. It combines network-based CGI positioning to increase the speed of GPS positioning. In this kind of network-assisted positioning systems, some but maybe not all the information about a mobile client's location reside in the network infrastructure.

User-based positioning systems can provide users with better location privacy because the location information is lstored on user's device. User can have complete control over location information if user processing location information locally on his/her device and never share location information with a third party. However, processing all the location information on the user device put too much burden to the user and this kind of privacy control can not be used in often-used network- assisted positioning systems.

B. Location privacy

The issues of privacy existed long before the creation of computers and Internet and many different definitions of Privacy has been proposed since then[6]. The most accepted definition of privacy is to regard privacy as the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others[7]. This definition captures the idea that privacy is not simply an absence of information about some users in the minds of others. Rather, it is the control that users should have over the information about themselves.

Location is a special type of private information and location privacy is 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 is communicated to others. The person whose location is being measured should control when and who can know it. Access decisions to user location information should be made exactly based on the user's privacy preferences.

Previous research on user's privacy preferences demonstrated that such privacy preferences vary not only across requesters but also across activities, situations and contexts [8]. The willingness to share one's location and the level of detail shared depends highly on who is requesting this information and the social context of the request. Due to users' varied privacy concerns and preferences depending on the situation or activity in which the user may be engaged, privacy controls need to be flexible [9]. More than often, context is just too complex to be fully considered so that users could hardly have all their privacy preferences predefined. Consequently, real-time user responses to special requests are needed. The goal of location privacy protection is to design mechanism that is flexible enough to provide the users with the capability of defining their privacy preferences and making access decisions at their own discretion.

III. RELATED WORK

To address users' privacy concerns and help LBS provider protect user privacy, CTIA, the International Association for the Wireless Telecommunications Industry, issued Best Practices and Guidelines [10]. These guidelines rely on two of the Fair Information Principles: user notice and consent. Notice: LBS providers must inform users about how their location information will be used, disclosed and protected so that a user can make an informed decision whether or not to use the LBS or authorize disclosure. Consent: once a user has chosen to use an LBS, or authorized the disclosure of location information, he or she should have choices as to when or whether location information will be disclosed to third parties and should have the ability to revoke any such authorization.

Google Latitude [11] and Loopt [12] are popular services that allow users to share their location information with friends. They both provided ways for users to control which participants can track their location by allow users to list which of the user's contacts should or shouldn't be able to see the user's location. They didn't provide users with the ability to specify expressive rules to control the sharing of their location information. Besides, the user's location privacy is not protected from the service providers themselves at all. There are many ways that data confidentiality can be compromised by trusted service providers.

Locaccino[13] is a new 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 the user's location. Users can define the times when they want to share the location, the regions where do and don't want other people to be able to find them, and decide who can see where exactly they are, who gets a blurrier vision, or none at all. It also have the problem that the service provider knows everything about the user's location, and even more, the service provider knows user's privacy preferences, which is also another kind of user privacy.

IV. USER-CENTRIC PRIVACY ACCESS CONTROL

In location sharing systems, a user sets his/her privacy policies and sends the policies to the service provider. The service provider stores the polices as records. When an information requester wants to access user's location information, the requester sends a request to the service provider. Service provider makes the access decision based on the policies that the user set before, and send user

location information to the information requester directly based on the access decision since user real-time location information is also stored on the service provider side.

Because all the location information and access control policies are released to the service provider, all the access decision are made by service provider, user's location privacy and privacy preference can easily compromised by service provider intentionally or unintentionaly. Besides, when user use user-based or network-assisted positioning technology, we believe there is no need for service provider to know the exact user location information, and to let service provider do the access decision process if we provide a good way for the user to do it. Let user do the access decision can not only protect user location privacy but also user location privacy preferences which can also be seen as a kind of user privacy.

In our user-centric access control privacy protection method, we divide the privacy access control policies into two parts. One part consists of the standard privacy access policies and will be stored at the server and the other part consists of the sensitive privacy policies and will be stored at the client side. Standard privacy access policies are generally simple and highly consistent policies that a user may not want to change frequently and doesn't mind to be released to others. Sensitive privacy policies are generally more complex policies that a user can create, change or delete at any time. In our method, we regard user's privacy preferences as a separate kind of privacy that a user should be given the ability to control if desired. Users should have the flexibility to decide which part is standard privacy access policy and which part is sensitive privacy policy since the sensitive privacy policy part is fully at the client side.

When an information requester wants to access the location information about a user, he/she generates an access request and sends the request to the service provider. After successfully authenticating the information requester, the service provider checks the privacy access policy with respect to the information requester. The service provider makes the first access decision based on the standard privacy access polices, which is "approve", "deny" or "ask the user". The service provider will send the result of the decision to the information requester when the decision is "approve" or "deny" but will forward the request to the client if the decision is "ask the user". In the latter case, the user receives the request and makes the second access decision based on sensitive privacy policies. The second access decision result can be "approve", "deny" or "ask user for real-time permission". If the second access decision is"ask user for real-time permission", it will send an message or alert to the user, ask for the user's real-time permission. Based on the access decision, user send his/her location information to the information requester. For further details regarding the user-centric access control and how it can be used to protect information privacy, please refer to[14].

In location sharing systems, If positioning technology is user-based, user can set all the access policies as sensitive privacy policies. So that user can fully control the location information. If positioning technology is network-based or network-assisted, user can set part of the access policies as sensitive privacy policies to protect user privacy preferences from service provider, and let the service provider do part of the access decision procedure to reduce user burden. Our privacy protection mechanism is flexible enough to work under all the situations.

Several advantages of our design can be summarized as follows:

- The new access control method is an new implementation of the existing, widely accepted and used access control model. Therefore, it can be easily integrated into and combined with current access control systems.
- The new method is very general in the sense that it can support privacy requirements in any type of location sharing systems.
- The server can do part of the access control decision. Users can decide the trade off between high privacy and task preformation. Our design provide the way to reduce the tasks that a client has to perform while providing the client with high level of privacy protection.
- Since the access decision may depend on user's context information, our design lets the user side make the second access decision so that the server doesn't get any information about user's context information in the access decision-making. This further improves user privacy.
- The user can establish and easily change his/her sensitive privacy policies and the server has no information about client's privacy policies. Without the release of client's sensitive privacy policies, our design provides a good way to protect user's privacy preferences.

V. EXAMPLE SCENARIO

We now go through an example scenario to illustrate how our method works and we present a step-by-step processing of an access request and the corresponding response. We assume that a location sharing service user, say Alice, is using the location sharing service on her cell phone. She set the standard privacy access control policies to the service provider when she register the location sharing service, and set the sensitive privacy access control policies on her cell phone. We assume there are four information requester who wants to know Alice's location information in this example scenario, namely Bob, Carol, Dave and Eva. Bob is Alice's boyfriend, Carol is Alice's boss, Dave is a stranger to Alice, who knows Alice but Alice doesn't know him at all and Eva is her friend.

The privacy access policies related to these three people that are set by Alice are as follows:

SDP1: when the requester is Bob, immediately approve the access request and send Bob my location information.

SDP2: when the requester is my boss or my friend, forward the request to me.

SDP3: when the requester is a stranger, simply deny the request.

The sensitive privacy policies in Alice's cell phone database are as follows:

SEP1: when my boss issues a request to access my location information, the request should be approved when the request is made at my work time or whenever I am in the office. Otherwise, the request should be simply denied.

SEP2: when my friend request to access my location information, ask me for real-time permission.

Finally, the whole process of making a decision to access Alice's location information are as follows:

1. If Bob wants to know where Alice is now at 8:00pm in the evening, Bpb sends a request to the service provider. The service provider checks the standard privacy access policy database and retrieves the policy related to Bob. Since the policy says that Bob can get Alice's information at any time, Alice's location information is directly sends to Bob.

2. If the requester is Carol, the service provider checks the standard privacy access policy database and retrieves the policy related to Carol. The service provider will send the request to Alice based on the access policy. When Alice receives the request, the sensitive privacy policy related to Carol, i.e., U-P1, and the context information are retrieved. Since it is now 9:00pm in the evening, it's not work time. Then, the access decision would depend on where Alice is at the time. If Alice is in the office, the request is approved and Alice's location can be sent to Carol. If Alice is not in the office, the request is denied according to the policy.

3. If the requester is Dave, the service provider finds out that Dave is a stranger to Alice. So the service provider would simply deny Dave's request.

4. If the requester is Eva, the service provider will send the request to Alice based on the standard privacy access policy. Alice receives the request and retrieves the sensitive privacy policy related to Eva. Since the policy say the access decision should based on Alice's real-time permission. There will be an alert appear on Alice's cell phone ask Alice if Eva can know her current location or not. Alice see the alert and make the access decision in real-time.

VI. CONCLUSION

In this paper, we analyzed the location privacy issues and requirements in location sharing systems. Based on the requirements for providing user location privacy protection, we proposed a new privacy access control method for location sharing services. We separate privacy policies apart from ulta-privacy policies so that the ulta-privacy policies can be made to fully under the user's control. In this way, users can easily make their access decision by themselves and even in real-time. Besides, users don't need to release their location information and privacy preference settings to service provider unless it is extremely necessary. At the same time, we still make the service provider responsible for part of the access control tasks to reduce end user's workload and to improve efficiency.

However, the privacy protection method that we proposed in this paper is still primitive and needs to be further refined . Our future work include the design of an application for the Apple iPhone using the Software Development Kit (SDK) based on this privacy access control method. We also seek to further refine the new model through implementation and application.

REFERENCES

[1] P. Bellavista, A. Kupper and S. Helal, "Location-Based Services: Back to the Future," IEEE Pervasive Computing, Vol. 7, No. 2, April-June 2008, pp. 85-89.

[2] J. Krumm, "A survey of computational location privacy," Journal of Personal and Ubiquitous Computing, Vol. 13, No. 6, Aug 2009, pp.391-399.

[3] 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.

[4] 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.

[5] M. Duckham, L.Kulik, "Location privacy and locationaware computing," In: Drummond J (ed) Dynamic & mobile GIS: investigating change in space and time. Boca Raton, CRC Press, pp 34–51, 2006.

[6] F. Xu, K.P. Chow, J.S. He, X. Wu, "Privacy Reference Monitor –A Computer Model for Law Compliant Privacy Protection," Proc. The 15th International Conference on Parallel and Distributed Systems (ICPADS'09), ShenZhen,China, Dec.8-11, 2009.

[7] A. F. Westin, "Privacy and freedom," Atheneum, New York, 1967.

[8] F. Xu, J. He, X. Wu and J. Xu, "Privacy-Enhanced Access Control Model", Proc. 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC 2009), Wuhan, China, April 25-26, 2009.

[9] F. Xu, J. He, X. Wu and J. Xu, "A Method for Privacy Protection in Location Based Services", Proc. 2009 International Conference on Computer and Information Technology (CIT 2009), Xiamen, China, Oct. 11-14, 2009.

[10] Best practices and guidelines for location-based services. CTIA Wireless Association (April 2 2008). http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.

[11] Google Mobile. Latitude.http://www.google.com/latitude/.

[12] Loopt, Inc. Your social compass | loopt. http://www.loopt.com.

[13] Locaccine. http://locaccino.org/.

[14] F. Xu, J. He, X. Wu and J. Xu, "A User-Centric Privacy Access Control Model", Proc. 2nd International Symposium on Information Engineering and Electronic Commerce(IEEC2010),Ternopil, Ukraine July 23-25, 2010.