PLATFORM FOR PRIVACY CONTROL IN LOCATION BASED SERVICES

Kyounghwan An, Kyoungwook Min, and Juwan Kim
Telematics Research Division,
Electronics and Telecommunications Research Institute,
161 Gajeong-dong, Yuseong-gu, Daejeon, 305-350, Republic of Korea
{mobileguru, kwmin92, juwan}@etri.re.kr

ABSTRACT:

Recently, the need for LBS (Location Based Services) is increasing with the rapid growth of the location measurement units, mobile devices, and communication technologies. Especially, wireless carriers are concentrating on LBS since it is regarded as so-called "killer application" among wireless data services. Although LBS give us convenience and useful information, its use also raises privacy issues. There are quite possibilities that the people's locations are tracked by location measurement units while people do not recognize the existence of the units. To protect a person's location information, lawful and technical aspects should be considered. In this paper, we explain issues, regulations, standards, and platforms related to the protection of the location information. Finally, we suggest the architecture of a platform complying with the regulations and standards. It considers various issues not covered in other studies.

KEY WORDS: LBS, Moving Object, Main Memory Database

1. INTRODUCTION

Location Based Services (LBS) are services that provide value added information using locations of things or people. The services are enabled by mobile devices, communication technologies, and positioning technologies based on mobile telephony or GPS. Since the infrastructures previously mentioned are wide spread already, LBS will be more prevalent in the future.

Although LBS give us convenience and useful information, there are quite possibilities that people's privacies are not preserved from infringement. In general, to provide LBS, the user's location needs to be published to one or more service providers, and the location may be provided to third parties. Even more the people's location may be tracked by the location measurement units while people do not recognize the existence of the units. If there do not exist proper methods to protect the user's location, it can be disclosed to unwanted people. Since the location information is closely related to personal privacy, lawful and technical aspects should be considered together.

Currently, the law and regulations governing the use of location information have been or are in the process of being enacted in the United States, the European Union, Japan, and Korea [6]. They are gradually coming into effect in the countries that lead the market of the mobile communications. The current laws and regulations let the wireless carriers collect user's location without user's consent for the public purposes while all the other services should obtain the user's consent.

For LBS, the regulations can not fully protect the people's privacies but need technical mechanisms. The organization for standardization such as 3GPP (3rd Generation Partnership Project) and OMA (Open Mobile Alliance) has been specifying location service procedure in mobile network. In the specification, the privacy control is one of the main concerns. To implement a system for LBS, we need to comply with both the regulations and standard specifications.

The previous study on privacy control in LBS focused on only anonymity of identity and description of policy [1, 2, 3, 4, 5]. They also explained the concept for the personal location privacy. However, they do not consider the law and standard specification simultaneously. Furthermore, they do not fully support (i) preservation of control and (ii) awareness of dissemination of location information that are the most important factors in privacy control in LBS. In this paper, after examining the difference between the location information and personal information, we present issues of privacy control in LBS. Finally, we suggest a platform complying with the regulations and standard specifications.

The remainder of this paper is organized as follows. In section 2, we explain issues of privacies in LBS. In section 3, we present privacy control in all steps of LBS. In section 4, we propose the architecture of a platform for LBS to protect location information. Finally, we conclude with issues and further works.

2. ISSUES OF PRIVACIES IN LBS

In this section, we explain several issues related to LBS. These issues should be considered when designing the platform for LBS.

2.1 Differences between Personal Information and Location Information

In a broad sense, the personal information includes the personal location information. However, the location information has different characteristics from the personal information like name, phone number, medical record and address. The personal information is static but the location information is dynamic since it changes as the time passes. There are more possibilities that the location information is disseminated to unwanted people since LBS are composed of many steps: (i) acquisition, (ii) storage, (iii) management, (iv) service, (v) utilization.

2.2 Protection of Location Information in Public and Commercial Service

If it is seen carefully, the law related to the protection of the location information discriminates between the public and commercial use of the information. For the public purpose, the location information is collected without the consent from the target entity since the emergency situation is more important than the privacy concern. For the commercial purpose, the consent is essential. One thing to consider is whether to allow governmental agencies such as police to track the target entity without the consent.

2.3 Trade-off between Ease of Use and Privacy

To protect the location information, the additional steps to check the privacy are necessary. However, the additional steps are barriers to the deployment of the service. In general, more steps leads to the decrease of the use. Thus, it is necessary to develop a service and system that copes with the reluctance.

2.4 Authorization and Consent

The important thing in the protection of privacies is to obtain consent for the service in advance. When obtaining the consent, the entities involved in the service and the purpose of the service should be specified. In the service, the authorization and checking of the privacy settings should be performed before providing location information.

2.5 Other Issues

There can be confusion in the target to be protected. Recent location based services are mostly provided by wireless carriers. In this case, if the subscriber and actual user of the cellular phone are different, there can be confusion for the target of the protection. In other case, if the owner of things and the carrier are different, there can be still confusion. Which one is outweighs the other? Personality or ownership?

The accuracy of location information is also one of the concerns. The requirements of accuracies are different among the location based services. The more accurate location information does not imply good service. It depends on the user's decision. The policy setting for privacy control can include the QoS (Quality of Service) as a parameter.

3. PRIVACY CONTROL IN ALL STEPS OF LBS

Location based service is composed of several steps. Thus, there are possibilities of intrusion in processing the steps. In this section, we present privacy control in all steps of LBS.

3.1 Entities and Relationships in LBS

We first define entities and their relationships based on the model in the law that is promulgated in Korea. Figure 1 shows the entities and their relationships.

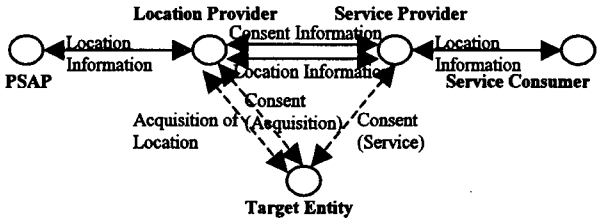

Figure 1. Entities and Relationships in LBS

- **Location Provider**: Entity acquiring location information of the target entity and supplying location information for the service provider. The examples of location provider are wireless carriers and companies that collect location information using GPS (Global Positioning System).

- **Service Provider**: Entity providing location based services to the service consumer using the location information collected by the location provider. For instance, contents providers correspond to this entity. Usually, wireless carriers serve both as the location provider and the service provider.

- **Service Consumer**: Entity using location based.

- **Target Entity**: Entity whose location information will be required to deliver service.

- **PSAP (Public Safety Access Point)**: Entity receiving emergency call and giving an emergency service. This entity uses location information for public purposes.

The following explains sequence of the typical location based service (e.g. buddy finder) and the relationships of the entities.

- The service consumer requests a location based service to service provider with the identity of the target entity.
- The service provider receives an approval (consent information) about the service from the target entity. If

the target entity agrees to the service, the service provider requests location information to the location provider.

- The location provider requests an approval about the acquisition of the location from the target entity (This step can be omitted). The location provider collects the location information from the target entity and provides it to the requesting service provider.
- Finally, the service provider combines the location information and content and then sends them to the service consumer.

The PSAP is different from the service provider. It is operated by government and can collect the location information without the grant of the target entity in case of the emergency call.

The figure 1 is the basic model for LBS. However, it has several problems. First, it is hard to manage consent information. The consent information is needed by both the service provider and the location provider. In this case, the responsibility for the management of the consent is ambiguous. If the location provider does not trust the service provider, the location provider should check the approval again. To the view point of the target entity, it is very bothersome checking approval twice. Second, the target entities are hard to control their privacy settings. It is very hard to remember which companies are using their location information since there can be many location providers and service providers.

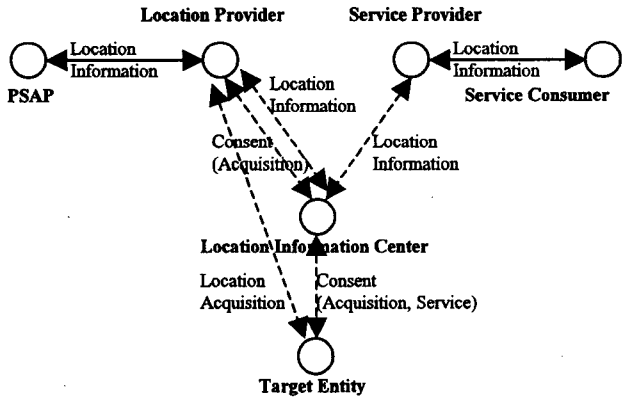

Figure 2 New Entities and Relationships in LBS

The figure 2 shows the new model for LBS. It has additional entities called Location Information Center. The center manages both the consent information and the location information. All consent information and location information is provided though the trusted center (It can be managed by the governmental agency or reliable company). In this case, the all the entities can easily check the consent information and the location information can be transmitted safely to the service consumer. In this paper, our suggesting platform can be installed in the location information center.

3.2 Privacy Control

In this section, we explain privacy control that we have to consider in the steps of LBS. Key factors for privacy control are preservation of control and awareness of dissemination of the location information [4]. If someone believes that he knows his environment well and is in control of his environment, then LBS should be perceived as less of a threat to his privacy. In the following steps, above two principles are considered in the policy. In all steps, the automated operation is necessary to exclude the interception of the location information. Figure 3 shows the steps of the LBS.

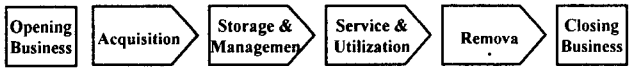

Figure 3 Steps of LBS

- **Opening Business**: To open Business, a company should acquire a license. This prevents the company from a misuse or abuse of the location information.
- **Acquisition**: To acquire the location information, anyone should obtain target entity's consent. If a location measurement unit is attached to something, the fact should be noticed to the person carrying it. The target entity should be able to control one' s own personal information. One should be able to browse or withdraw or suspend the consent. The important thing is the location provider should store the log about the acquisition (the time, requestor, purpose, and the identity of the target entity). This log can be served to the target entity when the target entity wants to know them.
- **Storage & Management**: If the service needs the location to be stored, there should be some technical and administrative methods to protect the stored location information. The location information should be deleted when the service has been completed and the access should be restricted by unauthorized people.
- **Service & Utilization**: The service provider should not use the location information beyond the scope of the contraction with the target entity and the service consumer. To help the awareness of the dissemination of the location information, the message should be sent to the target entity. The method of sending the message can be either by SMS or e-mail, and etc. The service provider also should store the log about the service (the time, requestor, and purpose) to facilitate resolution of security violations. The location information should be provided in a secure and reliable manner that ensures the information is neither lost nor corrupt. The HTTPS protocol can be a solution to the need.
- **Removal**: The location information should be removed when the purpose of the service has been achieved or the target entity withdraws or suspends the consent.
- **Closing Business**: If the location provider or the service provider closes their businesses, the location information and the logs should be deleted.

4. PLATFORM FOR PRIVACY CONTROL

In this section, we suggest the architecture of the open platform for privacy control.

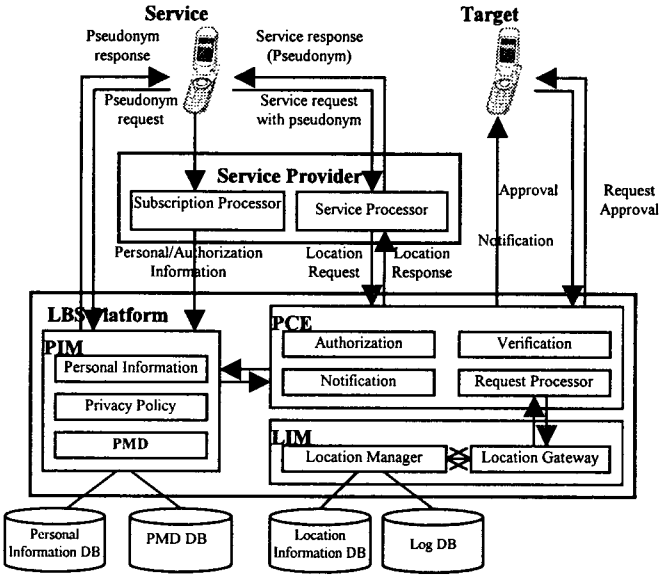

Figure 4 Architecture of the LBS Platform for Privacy Control

The platform for privacy control is composed of PIM (Personal Information Management), PCE (Privacy Control Entity), and LIM (Location Information Management). The functionalities of the modules are explained below.

- **PIM**: When the service consumer subscribes to the service, personal information and polices for controlling the location information are managed by this module. The contents of the policy are explained at the end of this section. PMD (Pseudonym Mediation Device) generate and manage pseudonym. It also translate pseudonym to verinym. The pseudonym is a virtual identity to conceal the user's identity and the verinym is a real identity such MSISDN, SIP URL, and IMSI[7].

- **PCE**: When the location is requested, the verification component examines the privacy policies. If the privacy policy is to allow the positioning, the request processor retrieves the location information from the LIM. If the policy needs a notification, the notification components send the message to the target entity.

- **LIM**: If the location information is requested, the location gateway acquires the location by its own positioning technology. After return the location information, the location manager stores a log. The location information can also be stored in the location information DB to retrieve it later.

The above mentioned policy is stored into subscription profile. The subscription profile is well defined in the standard specification of 3GPP [7]. The profile may include privacy exception list, settings of privacy check related actions, and etc. The target entity may be positioned only if the service consumer is included in the exception list of the target entity. The target entity can select one of the following settings of privacy check related actions: (i) positioning not allowed, (ii) positioning allowed without notifying the target entity, (iii) positioning allowed with notification to the target entity, (iv) positioning requires notification and verification by the target entity; positioning is allowed only if granted by the target entity or if there is no response to the notification.

5. CONCLUSION

In this paper, we presented issues of privacies in LBS and explained privacy control in all steps of LBS. Since the location information is different from the personal information, we suggested several methods to protect location information. To support technical protection of the location information, we proposed a platform for privacy control. The platform reflects lawful aspects and technical aspects, supporting standard specification. The future work is to incorporate policy file written in accordance with P3P format standardized in W3C into the platform.

REFERENCES

[1]C. Hauser, and M. Kabatnik, "Towards Privacy Support in a Global Location Service," Proceedings of the IFIP Workshop on IP and ATM Traffic Management (WATM/EUNICE 2001), pp. 81-89, 2001.

[2]E. Snekkenes, "Concepts for Personal Location Privacy Policies," In Proceedings of the 3rd ACM conference on Electronic Commerce, pp. 48-57, 2001.

[3]B. Schilit, J. Hong, and M. Gruteser, "Wireless Location Privacy Protection," IEEE Computer, pp. 135 - 137, 2003.

[4]T. Rodden, A. Friday, H. Muller, and A.Dix, "A Lightweigth Approach to Managing Privacy in Location-Based Services," Technical Report Equator-02-058, University of Nottingham and Lancaster University and University of Bristol 2002.

[5]C. A. Gunter, M. J. May, and S. G. Stubblebine, "A Formal Privacy System and its Application to Location Based Services," In Privacy Enhancing Technologies (PET), 2004.

[6]L. Ackerman, J. Kempf, and T. Miki, "Wireless Location Privacy: A Report on Law and Policy in the United States, the Europrean Union, and Japan," DoCoMo USA Labs Technical Report DCL-TR2003-001, 2003.

[7] 3rd Generation Partnership Project (3GPP), http://www.3gpp.org/