Editorial

Dear Colleagues,

In the second issue of The SIGSPATIAL Special, we focus on the topic of privacy in Location-based Services (LBSs). Privacy and security in LBSs have become a popular topic of interest in spatial information research during the last few years. Mobile devices, with ever increasing availability, precision, and connectivity, have introduced the feeling of continuous monitoring and being monitored. Thus, in addition to the benefits of LBSs, users have started to consider the disadvantages. In this issue, we visit some of the related definitions, existing research results, as well as future research directions.

The format of the July issue of the newsletter is in the form of letters. We have requested from a few leading researchers in the area to write brief notes on the topic. Authors were kind to respond to our request in a very limited amount of time.

The letters cover a large range of issues related to privacy in LBSs. These include privacy risks and classifications; privacy principles and definitions; privacy metrics; system architectures and privacy; user's context and privacy; continuous query processing and privacy. A common theme that appears to be repeated by the authors is that there is quite a bit of work that needs to be done in the area. We hope that you find the July issue useful in your future research, implementations, teaching, and studies.

Again, we invite you to contact us at `egemen@csse.unimelb.edu.au` for any suggestions regarding the newsletter.

Egemen Tanin, Editor
Department of Computer Science and Software Engineering
University of Melbourne, Victoria 3010, Australia
Tel: +61 3 8344 1350
Fax: +61 3 9348 1184
Email: `egemen@csse.unimelb.edu.au`

Privacy-Preserving Techniques for Location-based Services

Elisa Bertino

CS Department and CERIAS

Purdue University

bertino@cs.purdue.edu

Recent advances in positioning techniques, small devices, GIS-based services, and ubiquitous connectivity, have enabled a large variety of location-based services able to tailor services according to the location of the individual requiring the service. Location information, however, if on one side is critical for providing customized services, on the other hand, if misused, can lead to privacy breaches. By cross-referencing location information about an individual with other information and by exploiting domain knowledge, an attacker may infer sensitive information about the individual, such as healthcare or financial information. To address such problems, different techniques have been proposed that are based on two main approaches: *location cloaking*, under which a suitable large region is returned to the service provider instead of the precise user location [1]; *location k-anonymization*, under which the location of an individual is returned to the service provider only if it is indistinguishable with respect to the location of other k-1 individuals [5, 6]. These techniques have, however, a major drawback in that they do not take into account domain knowledge, and are thus prone to location inference attacks [2]. Given a generalized location of an individual, obtained for example through location cloaking, such an attack exploits the knowledge about the semantics of spatial entities to infer bounds about the location of an individual that are more precise with respect to the generalized location. Another major drawback is that those approaches do not support personalized privacy preferences. We believe that supporting such preferences is crucial in that different individuals have different preferences with respect to which location are considered privacy-sensitive.

A recent system developed by Damiani et al. [2, 3] addresses such shortcomings. The system, referred to as PROBE (Privacy-preserving Obfuscation Environment), is based on a number of key elements. The first element is represented by a classification of spatial entities into two categories: sensitive entities and unreachable entities. An entity is sensitive for an individual if the individual may wish to hide his/her presence in the location represented by the entity; examples of such entities are hospitals. An entity is unreachable if an individual is not able to enter the location represented by the entity; examples of such entities are military bases. The second key element of PROBE is represented by the personal profile; each individual may specify both the types of entity, among a predefined set of spatial entity types, that are sensitive and unreachable for him/her and privacy preference thresholds. Such preferences are recorded in the individual personal profile; different individuals may have different profiles. The third element is represented by a probabilistic privacy model that, based on the personal profile of the individual and on additional spatial semantic knowledge about the reference space, computes the probability that an attacker may be able to obtain a tight bound about the actual location of the individual. Based on such model and on the privacy preference thresholds specified by the

individual, PROBE is able to generate a generalized location so that the probability that an attacker is able to determine the actual individual location is below such threshold. To efficiently generate such location, PROBE adopts a strategy based on Hilbert space-filling curves [7]. Experimental results [2] show that such an approach is efficient and the size of obfuscated maps is very small and thus suitable for storage on small devices. A different approach, based on private information retrieval (PIR) techniques, has been recently proposed by Ghinita et al. [4]. The main innovation of this approach is that it does not require intermediate parties to generate cloaked regions nor the presence of other individuals to achieve anonymity. The main drawback of this approach is that it may be quite expensive.

Despite initial promising solutions like PROBE and the PIR-based approach by Ghinita et al., more work is needed to address the many challenges of LBS privacy. The whole spectrum of possible attacks still need to be identified; even though in the context of PROBE an inference attack has been identified and addressed, other attacks based on information such as the user speed may be possible. More detailed privacy preference models must be devised based on ontological definitions of spatial entities and relationships. Time is also relevant in that whether an individual may wish to hide his/her presence in a given location may depend on time.

References

[1] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar. Preserving user location privacy in mobile data management infrastructures. In *6th Workshop on Privacy Enhancing Technologies*, volume 4258 of LNCS, pages 393–412, 2006.

[2] M.L. Damiani, E. Bertino, and C. Silvestri. PROBE: an obfuscation system for the protection of sensitive location information in LBS. *CERIAS Technical Report*, 2008.

[3] G. Ghinita, M.L. Damiani, E. Bertino, C. Silvestri. Interactive location cloaking with the PROBE obfuscator. In *International Conference on Mobile Data Management (MDM 2009)*, Taipei (Taiwan), May 18-20, 2009.

[4] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K.-L. Tan. Private queries in location based services, anonymizers are not necessary. In *ACM SIGMOD Conference on Management of Data (SIGMOD 2008)*, Vancouver (Canada), June 10-12, 2008.

[5] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias. Preventing location-based identity inference in anonymous spatial queries. *IEEE Transactions on Knowledge and Data Engineering*, 19(12):1719–1733, 2007.

[6] M.F. Mokbel, C.-Y. Chow, and W. Aref. The New Casper: query processing for location services without compromising privacy. In *32nd International Conference on Very Large Databases (VLDB 2006)*, Seoul (Korea), September 12-15, 2006.

[7] H. Samet. Foundations of multidimensional and metric data structures. Morgan Kaufmann Publishers, 2006.

Privacy in Location-aware Systems[1]

Johann-Christoph Freytag
Institut für Informatik
Humboldt-Universität zu Berlin
http://www.dbis.informatik.hu-berlin.de

Abstract

As our world becomes more and more proliferated by sensors and mobile devices - often connected by wireless networks - there is the urging need to develop appropriate abstractions for application development and deployment. Those abstractions should shield applications from the physical properties of the devices thereby allowing applications to focus on information processing based on global conceptual views (of the world) in form of context models.

This paper will briefly elaborate on the concern for privacy in location-aware systems by providing a few examples that should highlight the complexity of such concerns. We show that privacy needs well founded bases for handling user requirements appropriately. Additionally, we argue that privacy aspects in context model based systems should include and embed privacy protection and control mechanism as an integral part on all systems levels therefore increasing the usability of such systems from a user's point of view.

1. Introduction

This recent development of ubiquitous devices and applications that access, combine, and transform context information from different sources has lead to the class of *context-aware systems*. Baldauf et al. [1] trace back the term of context-aware systems to Schilit and Theimer who describe context as "… location, identities of nearby people, objects, and changes to those objects" [2]. Dey et al. give a more general definition; they define context as "… any information that can be used to characterize the situation of entities (i.e. whether a person, place, or object) that are considered relevant to the interaction between a user and an application, including the user and the application themselves." [3].

Using context information as an important source for configuring and driving the system behavior has lead to the class of *context-aware systems*. If these context-aware systems are predominantly location oriented we call them *location-aware systems*. Since location based information reflects and describes properties of real-world scenarios and situations it is important to develop *context models* that provide a general basis to interpret sensor based information in a coherent, consistent and meaningful manner. The NEXUS project is one example project whose goal is to "… to provide an infrastructure to support spatial-aware applications" [4] by developing "… methods and approaches for designing and implementing global and detailed (location-based) context models for mobile context-aware applications. Context models should include stationary

[1] This article is an excerpt from the invited paper "Context Quality and Privacy – Friends or Rivals?" for the QALCON workshop in Stuttgart, Germany, June 25/26, 2009.

as well as mobile objects of the real world. In addition, these objects should be complemented by virtual objects and services." (translated into English from [5]).

When people use location-aware systems to support them in their tasks they usually take those systems around with them. Thus, these systems reveal location information about the user since the location information created by a sensor is identical with the location information about the user of such system. If, for example, the location of a device (and therefore of the user) is transmitted to another system (let it be a mobile or stationary system) this information might be essential to perform a user-requested task such as helping two people to meet or to generate a list of nearby restaurants. However, such information might also be used to the disadvantage of that user, either at the time of transmission – for example, to send unwanted advertisement – or at a later point in time – for example, to determine that the user violated the speed limit while driving a car.

This paper therefore argues that location-aware systems should also be privacy-aware when personal data is involved. The next section, Section 2, investigates the terms private information and privacy in general. Section 3 lists of general privacy principles that - from our point of view - should guide the development of any location-aware system that uses personal data to give the user the freedom and the control over private data that (s)he shares with other systems. As an example of such a system we briefly introduce the EU-funded project PRECIOSA (**PR**ivacy **E**nabled **C**apability **I**n Co-**O**perative **S**ystems and Safety **A**pplications), i.e., a location-aware system, in Section 4 before Section 5 lists future challenges for privacy-location-aware systems.

2. Private Data and Privacy

We first introduce and discuss the term sensitive and private data, and the term privacy, since those are important to understand the technical challenges and threads that today's information technology poses to the individual's right to privacy in various areas and systems, in particular in location-aware systems. For the purpose of personal context-aware systems personal (or private) data "… means any information about a living individual that includes personal data revealing racial or ethnic origin, criminal record information, political opinions, religious or philosophical beliefs, trade-union memberships, and the processing of data concerning health or sex life". This definition resembles the definition of personal data as stated in the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 2, Subsection a [6].

The right for personal privacy was continuously been challenged and continuously endangered even before massive advances in IT technology provided the means for "automated" privacy breaches on a large scale. Already in his book *Privacy and Freedom* published in 1967, Alan Westin was one of the first to define the concept of privacy in the context of modern communication infrastructures. For him privacy is "the claim (right) of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" [7]. The term **privacy** itself was coined much earlier in the American legal system by the article of Warren and Brandeis in 1890 when large scale printing forced a clear standing of the law regarding individual's rights [8].