Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2007 Proceedings

Americas Conference on Information Systems (AMCIS)

December 2007

Privacy-Friendly LBS: A Prototype-Supported Case Study

Jan Zibuschka
JWG University Frankfurt

Lothar Fritsch

Mike Radmacher
JWG University Frankfurt

Tobias Scherner
University of Frankfurt

Kai Rannenberg

Recommended Citation

Zibuschka, Jan; Fritsch, Lothar; Radmacher, Mike; Scherner, Tobias; and Rannenberg, Kai, "Privacy-Friendly LBS: A Prototype-Supported Case Study" (2007). *AMCIS 2007 Proceedings*. 40.
http://aisel.aisnet.org/amcis2007/40

PRIVACY-FRIENDLY LBS: A PROTOTYPE-SUPPORTED CASE STUDY

Jan Zibuschka, Lothar Fritsch, Mike Radmacher, Tobias Scherner, Kai Rannenberg
University of Frankfurt, Germany
jan.zibuschka, lothar.fritsch, mike.radmacher, tobias.scherner, kai.rannenberg@m-lehrstuhl.de

Abstract

The development of new products in the mobile data services market poses severe challenges for service providers and mobile network operators. Short-lived products, lack of knowledge about acceptance by users, and the requirement to embed new products in existing infrastructures lead to difficulties on several levels. Data protection, potentially ambiguous regulation of telecommunication and the existence of a wide range of communication and localization technologies confront product developers with new challenges. Modeling and balancing business interests, data protection requirements, and user preferences while implementing new products on existing infrastructures are some of them. This paper presents the concept and implementation of a prototype that was developed by an international research project with participation of industry partners

Keywords

Identity Management, Privacy, Infrastructures, Location-Based Services

Introduction

The high market penetration of mobile phones based on the GSM or UMTS standards (Bundesnetzagentur 2006) makes these devices a highly attractive platform for the rendering of location-based services (LBS) reaching a broad user base. Devices including localization technologies such as GPS or Galileo are not yet widely deployed (Bulusu et al 2000). The mobile operator may provide the location data for specialized LBS providers or act as service provider itself.

However, location data is very privacy-sensitive, and as a result there are legal requirements for handling it in various countries and regions. So while mobile network operators are – from a technological point of view – in a very good position to supply user location data, the actual provision of location-based services can pose a legal and commercial risk. Thus, there is an incentive to outsource location-based services to third parties, under clearly defined conditions configurable by the user. With this strategy, the operator can maintain good and trustful customer relations and get rid of potential liabilities that may arise from the specifics of a service. The interface used to make decisions on the transfer of personal data has to be designed properly in order to comply with legal requirements. Therefore, an identity management system is an essential component for enabling such business models.

However, it is a widely held belief that ”people won’t pay for privacy” (Shostack 2003, Acquisti et al. 2003). Alas, the economic relevance of Privacy Enhancing Technologies is believed to be very limited, if existent. We report on a case study in the sense of (Benbasat et al. 1987) performed within the PRIME project (PRIME Project 2005) involving several major partners from industry, exploring the viability of making the deployment of privacy enhancing technologies economically successful. We present a prototype which was designed with a major focus on the interest of the different stakeholders. It has now reached the stage of being transferred into a product and being integrated into the existing infrastructure, demonstrating its economic viability in a real-life environment.

The paper is structured as follows: After presenting a short introductory scenario and state of the art, the parties’ requirements are presented. An architecture and implementation meeting the requirements are introduced, and, finally, experiences from evaluation and deployment are presented.

Usage of Location-Based Services: A Scenarios

Location-based services are employed for a wide range of use cases. For investigation of the problem described by the introduction a typical navigation service prototype implementation is considered in order to evaluate the upcoming solution under realistic conditions.

John, a traveling salesman, arrives in a city he has visited never before. On arrival, he recognizes his daily medicine is missing. By using the pharmacy search service, John opens a connection to the service via his mobile phone, and his position is determined by the mobile network operator. The determined position is passed on to the service provider who compares it to its database. The results – e.g. the 5 nearest pharmacies – are then returned to John's mobile phone where they are displayed. Obviously it is important, that John's location data are only delivered to a service provider John can trust and only after notifying John and getting his approval.

State of the Art

There exist a wide range of technologies for protecting the users' privacy. These technologies are generally referred to as Privacy Enhancing Technologies or PETs (Blarkom et al. 2003). Several protocols and architectures for the privacy-preserving handling of location information have been proposed. This section gives a quick overview of existing solutions and compares them to the implementation presented in this paper.

The Alipes platform (Synnes et al. 2002) offers the possibility to control access to location information using user-configurable privacy policies. Furthermore, location information from different sources may be aggregated. However, Alipes does not offer pseudonymisation, and generally no further identity management functionalities.

The T-Identity Protector (Wagner 2006) concentrates on the pseudonymisation of personal information before transmission. De-pseudonymisation is implemented in order to comply with legislation.

Böhm, Leiber and Reufenheuser (2004) present a concept that offers the possibility to specify explicitly for each service whether localization is allowed or not. However, no deployment architecture or other technical details like the use of pseudonymisation are covered.

In Reynold (2004) a system that limits the accuracy of transmitted location information based on the recipient is proposed. However, neither access control functionalities nor pseudonymisation are considered.

The architecture presented in (Jorns et al. 2004) proposes pseudonymisation and access control functionalities for the location-based services scenario. However, no further analysis of the information flow between the communicating entities is performed.

In Oinonen (2002) procedures for ensuring data security with the contribution of location-based services are proposed. The contribution focuses on the adherence of legal requirements in the context of the mobile telephone systems. Therein a central rule-based decision function is suggested, which is placed between localization source and used application. More details are not specified, in particular any architecture.

In contrast to Oinonen (2002), Myles, Friday and Davies (2003) describes a rule-based mechanism for protecting location data. With the attempt of accessing the data by the service provider, entities named "validators" evaluate the rules and adjudicate the access decision. The paper does not supply any information about the architecture, in particular over the installation of the validators as third party or as part of any other entity.

Further there are beginnings to formalize the modeling of systems which must fulfill data security requirements in order to ensure a consideration of the interests of the different parties, seen in Fritsch, Scherner and Rannenberg (2006). Scientists and industrial partners examine the architecture and the application of these technologies in different research projects in the context of the FP6/IST program of the European Union. Her e.g. the case is examined that location data of a user is placed into the domain of a mobile network operator and passed on to the provider of the respective location-based service (Koelsch et al. 2005, Dumortier).

In parallel the standardization of PETs is being initiated, e.g. in ISO/IEC JTC1/SC27 "IT Security Techniques", that initiated Study Periods on Identity Management and Privacy in 2004/2005 and a working group on "Identity Management and Privacy Technologies" in 2006.

Requirements

The requirements on identity management used for location based services in a mobile telephone network have many facets. This contribution focuses on the business interests of mobile network operators, on regulatory influences in the field of data protection, and on users' privacy requirements. This focus is based on interviews with representatives of all stakeholders, and their respective requirements. Also, requirements were analyzed within the PRIME project (PRIME Project 2004b), leading to a general identity management framework document (PRIME project 2005). Those findings were also used as input.

In line with the current market situation, the basic scenario presented here assumes that communication between service providers and users takes place using network infrastructure supplied by mobile operators. Consequently, a very strong position of the mobile network operators with regard to the localization of the users' mobile devices is assumed. Of course, this strong position leads strong responsibility: A network operator releasing customer data to 3rd parties without legal basis of customer's consent is deemed for trouble.

In the resulting scenario, a service provider offers location-based services based on its own domain knowledge using users' location data acquired via the mobile network operator. Billing is performed by the mobile network operator, who may charge for access to the users, for necessary localizations, and for offered identity management functions. A discussion of this constellation compared to other developments can be found in e.g. Lindner et al. (2004) and Koelsch et al. (2005).

Business Modells

The market structure of mobile value-added services, such as ring tone downloads or mobile phone logos, is built upon cascading retailer structures. Mobile network operators offer interfaces for infrastructure, identity management and accounting services. Therefore, the requirements of the involved parties had to be collected, often from different departments, and compiled into a comprehensive requirements document for the prototype (PRIME Project 2004a). The basic architecture of the system should be similar to the structure used in e.g. the call number or ring tone business, allowing for cascading retailers of location-based services, in order to enable external provision of location based services.

A schematic representation of the architecture resulting from these business requirements is presented in figure 1.

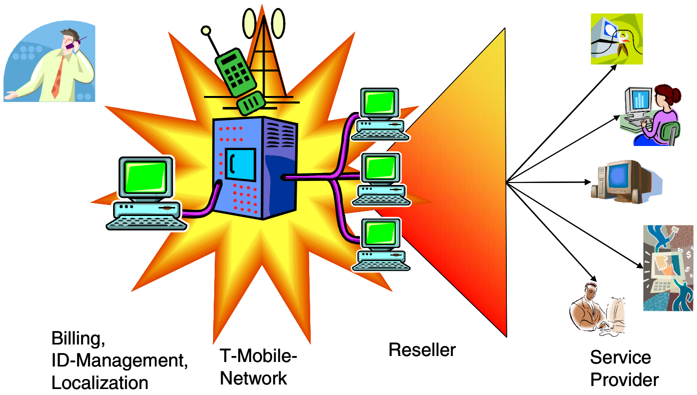


Figure 1. Structure of cascading business model (Radmacher et al. 2007)

Information Intermediars

The pyramid-shaped structure of service bindings at the mobile network operator suggests applying intermediary theory. Efficient organization of selling through service providers, bundled processes, information access and other services can be offered using a unified central interface. The specific advantages of intermediaries concerning e.g. search time and pricing of traded products have been scientifically investigated. A good overview on general information intermediaries can be found in (Rose 1999) as well as in (Schackmann et al. 2002). Value-added services in the context of mobile network services are particularly suitable for intermediation in several fields (Radmacher et al. 2007):

- Identity management and data protection according to telecommunication laws (see (Koelsch, et al. 2005), (Böhm et al. 2004))
- Bundling of account and risk management services.

- Sale of auxiliary services such as geo-information or usage patterns (see (Figge 2004))

Privacy management in the area of conflict between regulation and customer satisfaction is a cost-intensive undertaking, as pointed out by Ponemon (2004). Therefore, implementing widely usable, standardized intermediary architectures for identity management is particularly attractive as part of the value creation chain of the cascading location-based services scenario.

The number of intermediaries does not depend from the number of network operators but from the different ways in which user plays trust in organizations, some users might prefer friend-finders organized by their church while other prefer them organized by their dance-club. It may be helpful if the intermediaries are certified by one or several Trusted Third Parties, especially some that enjoy trust from users and mobile network operators.

Data Protection

On top of the economic requirements presented in sections 2.1 and 2.2, further requirements result from regulation. Telecommunications in Europe is governed by European Union directives, which are then enforced in the particular countries usually after conversion into national legislation. The Directive 2002/58/EC (European Parliament 2002) is relevant for the implementation of location-based services. Legislation on the handling of location data in the context of calls or for use in e.g. value-added services is contained in Article 9. For other uses, e.g. for location-based services, data processing must be explained explicitly and a legally effective consent of the data subject must be collected. Moreover, it must be guaranteed that the user is able to revoke his or her consent at short notice. The homogeneity of the local conversion to national right is unclear in this respect. Besides, so far there are only a few uniform regulations for the collection of consent, particularly in the case of ad-hoc-use of services on mobile devices. There are ideas like the ones presented in Rossnagel (2004), but still no standards. From the point of view of users and mobile network operators it is necessary to verify the consent in a reliable manner. As the mobile network operator may become liable for the initial publication of location data, consent needs to be established before the provider of a location based service receives personal data. Service providers will regard further data protection agreements available in the context of their individual offers for their users (Radmacher et al. 2007).

A detailed analysis of the legal requirements of location-based services can be found in (PRIME Project 2004a) and (PRIME Project 2004b), two requirement analyses for privacy-respecting applications conducted as part of the respective research project.

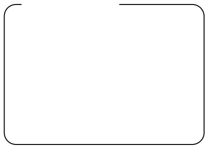
Apart from the fulfillment of the formal data protection requirements for privacy management, another main requirement is the flexibility of the infrastructure component with regard to different national legislations. The users want to employ mobile services regardless of the country they are currently visiting. For voice telephony and data transfer, international roaming already exists. When implementing international infrastructures for location-based services, different local legislations must be considered regarding data protection, data storage, and data monitoring. For the avoidance of new project engineering for each individual country, it is worth to keep uniform intermediate services for privacy management ready and configurable.

Proposed Solution

Based on the requirements presented in Chapter 2, the following solution has been developed for the implementation of a prototype that incorporates both privacy and data security aspects.

We propose the integration of an intermediary as an additional party along with the mobile network operator, the provider of location-based services and the user in the value chain of mobile commerce (Koelsch et al. 2005). The intermediary performs three essential tasks in this scenario. It guarantees the user's anonymity vis-à-vis the other involved parties. To be more precise, this means that (a) the user's identity will not be revealed to the service providers of the location based services and (b) the specific service requested by the user will not be disclosed to the mobile network operator. Any communication between the mobile network operator and service provider is carried out exclusively via the intermediary. The third task of the intermediary is to represent and to act in place of the user throughout the entire communication relationship, to make up for technological limitations of users' terminals, as depicted in figure 2 (PRIME Project 2006a). This representation takes place under the rules which are specified explicitly, but also confine the application of the service aiming at a maximization of data transmission transparency with regard to both privacy and data security.

The prototype, which was developed as part of the work on the project is based on the already existing infrastructure of a mobile network operator and provides a location-based service (LBS) to find nearby pharmacies. Except for the user, all parties involved in the communication process integrate additional identity management components into their existing software infrastructure. The user is granted direct access to the intermediary and thereby enabled to configure identity management and data access policies, as depicted in figure 2 (PRIME Project 2006a). The intermediary may be operated as part of the mobile network operator's infrastructure. An overview of the architecture is given in Figure 2



```
ERROR: invalidaccess
OFFENDING COMMAND: --filter--

STACK:

/LZWDecode
-filestream-
[304 0 0 -90 0 90 ]
true
90
304
-savelevel-
```