Privacy for Profitable Location Based Services

Tobias Kölsch\(^1\), Lothar Fritsch\(^2\), Markulf Kohlweiss\(^2\), and Dogan Kesdogan\(^1\)

\(^1\) RWTH Aachen University, Ahornstrasse 55, 52074 Aachen, Germany
\{koelsch, kesdogan\}@i4.informatik.rwth-aachen.de

\(^2\) Johann Wolfgang Goethe University Frankfurt am Main, Gräfstrasse 78, 60054 Frankfurt am Main, Germany
\{fritsch, kohlweiss\}@whatismobile.de

Abstract. Location based services (LBS) are distributed multi-party infrastructures with the opportunity to generate profitable m-business applications. Also, LBS pose a great risk for their users' privacy, as they have access to private information about a person's whereabouts in a particular context. As location data is the essential input for LBS, protection of privacy in LBS is not a problem of providing anonymity by suppressing data release, but a problem of identity management and control over information handling. In this paper we show a solution that ensures a LBS user's control over location information with managed identities. At the same time, our solution enables profitable business models, e.g. for mobile telephony operators. Additionally, we provide fine-grained consent management for the LBS user.

1 Introduction

Location based services (LBS) can pose a privacy risk to their users if they collect and use data against a user's intention. Most of the LBS are provided by mobile communications providers that can measure a user's whereabouts by localizing his mobile device while it uses the network infrastructure. Can LBS be deployed in a privacy-respecting way, and still be profitable applications on the commercial market of online-services? How does a privacy-respecting architecture look like? In this paper, we will answer the question by fulfilment of these requirements:

- Enable established business models on a secure, privacy-friendly architecture
- Ensure efficiency & economy of the solution
- No localization violates a user's consent
- Enable users to manage policies & their 'online' identities for each service provider and for each usage cycle
- Hide service usage patterns from observers & infrastructure providers
- Confidentiality of communication content against observers & infrastructure

\* This work was supported by the IST PRIME project; however, it represents the view of the authors only.

© Springer-Verlag Berlin Heidelberg 2005
We use a health-related LBS as an example scenario. An *allergy warning LBS* tracks Mr. John Primeur with his mobile phone. When joining the service, John first registers a profile of his allergies. Then, at the service, data about allergenes is correlated with weather conditions in John’s environment. John’s position is regularly checked by localizing his mobile phone. When the weather and allergene status indicate an allergy risk for John, he receives a warning on his mobile phone. On the other hand, John dislikes the idea that his identity combined with his allergy profile could become known to the LBS, his mobile network operator, or a health insurance company.

Our paper is organized as follows. First, we give an overview over related work in the fields of LBS business models, privacy relevant research, and technological developments that are important for our design. Then, we describe and analyze our privacy-friendly approach, in particular the security protocols that ensure privacy and establish user control. Finally, we summarize our achievements.

2 Related Work

For privacy-respecting LBS architectures, this section presents relevant work and requirements in LBS business models, privacy relevant research, and technological developments of LBS infrastructures.

2.1 Related Work on Business Models

Mobile Commerce applications differ from e-commerce applications in four properties \([1]\). *Ubiquity / Reachability* enable applications to be used from anywhere, any time. *Context Sensitivity* supports applications provided for a particular context. *Identification / Personalization* takes advantage of mobile networks providing identity management technologies that enable personalized, authenticated, and paid-for personal applications. Finally, *Telemetry / ‘Remote Control’* functions enable users to remotely control applications or processes.

Camponovo \([2]\) describes a generic m-commerce business model as a mesh of parties of infrastructure, service, technology, user, communication and regulation domains. As LBS are a special form of m-commerce, Camponovo’s model also applies to them.

**Business Model Overview.** Location data for LBS is either provided by the communication network or by specialized hardware at the user device. The location of a person is highly sensitive data. Thus regulation authorities have an interest in controlling its usage.

The actual LBS are offered by application providers. Due to their infrastructure, mobile operators may act as localization providers, as portal operators or even as application providers themselves.

**Basic LBS Business Scenarios.** LBS business models can be divided into the scenarios shown in figure \([\dagger]\).