

Techniques for countering privacy threats of Location-based services

Lauri Suomalainen

Seminar
UNIVERSITY OF HELSINKI
Department of Computer Science

Helsinki, February 22, 2016

Tiedekunta — Fakultet — Faculty		Laitos — Institution — Department	
Faculty of Science		Department of Computer Science	
Tekijä — Författare — Author			
Lauri Suomalainen			
Työn nimi — Arbetets titel — Title			
Techniques for countering privacy threats of Location-based services			
Oppiaine — Läroämne — Subject			
Computer Science			
Työn laji — Arbetets art — Level		Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Seminar		February 22, 2016	2
Tiivistelmä — Referat — Abstract			
Abstract			
Avainsanat — Nyckelord — Keywords			
Geo-location, Privacy, Social Networks			
Säilytyspaikka — Förvaringsställe — Where deposited			
Muita tietoja — Övriga uppgifter — Additional information			

Contents

1	Introduction	1
2	Threats in Location-based Services	1
3	Techniques for countering the privacy threats	1
4	Evaluation of the techniques	1
	Sources	1

Most of the social networking services today exploit location-based data in one way or another. Services like Facebook allow users to GeoTag their current location and tag themselves and their friends. In exchange the service can use the data to offer recommendations, news and so on. While the users of the services are often aware that they are providing personal locational data, its pervasiveness and accuracy may come as a surprise and have serious repercussions when it comes to users' real-life privacy. A malicious actor such as a burglar could exploit the data a user provides to for example find out their street address and times when they are not home. This seminar paper reviews and evaluates several techniques used to preserve and protect users' privacy when using Location-based services. The goal for the techniques is to counter several threats Location-based Services face in such manner that users can still use said services without compromising their security.

1 Introduction

Location-Based Services (LBS) are applications that operate on geographical or other location based data. Original LBSs can be traced back to mid-20th century, but what is understood by LBS today is tied to the mid-21st century emergence of G3 networks and hand-held devices with GPS capability [1]. Many contemporary LBSs take a form as a part of a social networking applications such as Facebook, Foursquare and Instagram. There are several ways LBSs work. They can make use of users' mobile device's GPS and provide services based on users' whereabouts when requested or continually monitor users' location [3]. Some services allow users to *check-in* to pre-determined venues or points of interest (POI) whereas other allow more exact location with the GPS data. This practice is commonly known as *GeoTagging*.

LBSs do not come without security risks. By publishing their location on the internet exposes users to threats in the real world. A malicious agent, for example a burglar, could monitor one user's LBS usage and e.g. determine when the user is not at their residence. Using that information the attacker could orchestrate a break-in without the risk of being caught red-handed [2]. While many applications require user to explicitly publish their locational data, users also often do it unknowingly. For example many contemporary smart phones as well as digital cameras automatically embed metadata to photographs and it can contain privacy sensitive information such as coordinates and the time the photograph was taken [2]. In some cases the user themselves does not expose their location data explicitly, but with certain LBSs supporting *User Tagging*, a user's acquaintance can expose the user without them having a say for it. Thus a user can be associated with places, people and other information they would rather keep private.

The obvious privacy issues have been researched a lot and many techniques have been presented which address one or more possible privacy threats LBSs face [3]. These range from offering users options to rule how, where and when can their locational and identity data used to more technical solutions such as query enlargements and encryption-based techniques. Each of them have their uses and shortcomings: They can only address a certain set of privacy threats and may come with pre-assumptions and computational costs.

In this paper we first review threats LBSs face in section 2. Then in section 3 we take a look at the techniques designed to address different kinds of privacy threats in LBSs. Section 4 compares and evaluates the techniques in respect of their intended use as well as other techniques. Section 5 will be the concluding part summarizing the state of privacy in Location-Based Services and also shortly addressing the future trends of the field.

2 Threats in Location-based Services

3 Techniques for countering the privacy threats

4 Evaluation of the techniques

Sources

- [1] Bellavista, P., Kupper, A., and Helal, S.: *Location-based services: Back to the future*. Pervasive Computing, IEEE, 7(2):85–89, April 2008, ISSN 1536-1268.
- [2] Friedland, Gerald and Sommer, Robin: *Cybercasing the joint: On the privacy implications of geo-tagging*. In *Proceedings of the 5th USENIX Conference on Hot Topics in Security*, HotSec’10, pages 1–8, Berkeley, CA, USA, 2010. USENIX Association. <http://dl.acm.org/citation.cfm?id=1924931.1924933>.
- [3] Vicente, C.R., Freni, D., Bettini, C., and Jensen, Christian S.: *Location-related privacy in geo-social networks*. Internet Computing, IEEE, 15(3):20–27, May 2011, ISSN 1089-7801.