Cryptographic Approaches for Privacy Preservation in Location-Based Services: A Survey

Emmanouil Magkos, Ionian University, Greece

ABSTRACT

Current research in location-based services (LBSs) highlights the importance of cryptographic primitives in privacy preservation for LBSs, and presents solutions that attempt to support the (apparently) mutually exclusive requirements for access control and context privacy (i.e., identity and/or location), while at the same time adopting more conservative assumptions in order to reduce or completely remove the need for trust on system entities (e.g., the LBS provider, the network operator, or other peer nodes). This paper surveys the current state of knowledge concerning the use of cryptographic primitives for privacy-preservation in LBS applications.

Keywords: *Cryptographic Primitives, Cryptography, Information Systems, Location-Based Services, Privacy and Security*

INTRODUCTION

In the era of mobile and wireless communication technologies, recent advances in remote sensing and positioning technologies have altered the ways in which people communicate and interact with their environment. In the not-so-far future, *Location-Based Services* (LBS) that take into account the location information of a user, are expected to be available anywhere and anytime. Such services will be highly personalized and accessible even by resource-constrained mobile devices. A classification of the most popular services includes: a) *point-of-interest* or "pull" services where a user sporadically queries an LBS provider to receive a nearby point of interest (Konidala et al., 2005; Candebat et al., 2005; Hengartner, 2006; Solanas & Balleste, 2007; Kohlweiss et al., 2007;Ghinita et al., 2008; Solanas & Balleste, 2008; Hengartner, 2008; Olumofin et al., 2009; Ardagna et al., 2009; Ghinita et al., 2009); b) *people-locator* services, where a watcher asks the LBS provider for the location of a target (Hauser & Kabatnik, 2001; Rodden et al., 2002; Bessler & Jorns, 2005; Jorns et al., 2005, 2007; Zhong et al., 2007; Sun et al., 2009); c) *notification-based* or "push"' services, where location-based alerts or notifications are sent to a user (Zhu et al., 2003; Kolsch et al., 2005).

A typical scenario involves a user with a handheld device connecting through a mobile

DOI: 10.4018/jitsa.2011070104

communication network to an external third party that provides an LBS service over the Internet. As with many aspects of ubiquitous computing, there is an inherent *trade-off* between access control and user privacy in LBS applications (Hauser & Kabatnik, 2001; Langheinrich, 2001; Rodden et al., 2002; Duckham & Kulik, 2006; Ardagna et al., 2007). On one hand the system typically needs to be protected from unauthorized access and misuse. On the other hand mobile users require the protection of their context information (e.g., location and/or identity information) against privacy adversaries (e.g., big-brother type threats, user profiling, unsolicited advertising) (Hauser & Kabatnik, 2001; Gruteser & Grunwald, 2003; Duckham & Kulik, 2006; Ardagna & Cremonini, 2009). The privacy issue is amplified by the requirement in modern telematics and location-aware applications for real-time, continuous location updates and accurate location information (e.g., traffic monitoring, asset tracking, location-based advertising, location-based payments, routing directions) (Gruteser & Liu, 2004; Kulik, 2009; Ghinita, 2009).

Recent research highlights the importance of *cryptography* in privacy preservation for LBSs, and presents solutions that attempt to support the (apparently) mutually exclusive requirements for access control and context privacy, while at the same time adopting conservative assumptions in order to reduce or completely remove the need for trust on system entities (e.g., the LBS provider, the network operator, or even the peer nodes). While a number of recent survey papers (Ardagna et al., 2007; Solanas et al., 2008; Ardagna & Cremonini, 2009; Kulik, 2009) cover aspects of access control and privacy, to the best of our knowledge there has been no thorough survey of the use of cryptographic techniques for privacy-preservation in LBS services.

Our Contribution

This paper surveys the current state of knowledge concerning the use of cryptographic primitives for achieving privacy-preservation in LBS services. Specifically, we categorize current research into three groups, based on the trust assumptions between parties involved in LBS schemes: TTP-based approaches, semi-distributed schemes, and TTP-free approaches. For each category, we review and evaluate the current literature in terms of privacy, security and efficiency.

DESIGN CONSIDERATIONS

Privacy Requirements

In general, privacy-preserving systems for LBS services are expected to satisfy some or all of the basic properties below (Pfitzmann & Kohntopp, 2000; Hauser & Kabatnik, 2001; Beresford & Stajano, 2003; Gajparia et al., 2004; Ardagna et al., 2007; Jorns et al., 2007; Kohlweiss et al., 2007; Solanas & Balleste, 2008; Hengartner, 2008; Ardagna & Cremonini, 2009):

- **Location privacy**: The protocol does not reveal the (exact) user's location information to the LBS provider. More generally, no unauthorized entity (or a coalition of unauthorized entities) should have access to the location data of the user, past or current.
- **Identity privacy (untraceability)**: The LBS provider is not able to find the identity of the user, based on the location information received during the user access. More generally, no unauthorized entity (or a coalition of unauthorized entities) should be able to trace the real identity of the user.
- **Tracking protection (unlinkability)**: The LBS provider is not able to link two or more successive user positions. More generally, no unauthorized entity (or a coalition of unauthorized entities) should be able to link different sessions of the user.

Security Requirements

Access control in LBS involves satisfying some or all of the following security properties (Hauser & Kabatnik, 2001; Konidala et al.,