Chapter 13
Enhancing Location Privacy in Location-Based Services: The STS Case

Constantinos Delakouridis
Athens University of Economics and Business, Greece

ABSTRACT
Location-based services are receiving signification attention over the last few years due to the increasing use of mobile devices. At the same time, location privacy is important, since position information is considered personal information. Thus, in order to address this issue, several mechanisms have been proposed protecting the mobile user. In this chapter, the authors present an architecture to shield the location of a mobile user and preserve the anonymity on the service delivery. This architecture relies on un-trusted entities to distribute segments of anonymous location information, and authorizes other entities to combine these portions and derive the actual location of a user. The chapter describes how the architecture takes into account the location privacy requirements, and how it is used by the end users’ devices, e.g., mobile phones, for the dissemination of location information to service providers. Furthermore, it notes privacy issues for further discussion and closes with proposed exercises.

INTRODUCTION
As the cost of mobile devices and mobile broadband drops across the globe, the popularity of location based services, shoots up. The convergence of these two trends is influencing the vastly changing world. A number of applications, by using the capabilities of the smartphones (GPS receivers), provide services that affect the way we live, work and interact with each other. Through the aforementioned services, we are able to navigate to destination by avoiding traffic jams, to locate the closest points of interests, to discover the nearby friends, to share location tagged pictures etc. However, this new trend comes at a certain price. The networking technologies (e.g., GSM/
GPRS) offer the infrastructure for advertisement of the location information, and, thus, potential eavesdropping and unauthorized use (or misuse) of it. An adversary can potentially derive location information at different layers of the network stack, from the physical to the network layer (Gruteser & Grunwald, 2003a). Furthermore, data collection and mining techniques might produce historical location data and movement patterns (Gruteser & Grunwald, 2003), which they are subject to unauthorized use, as well. Minch presents and discusses several risks that are associated with the unauthorized disclosure, collection, retention, and usage, of location information (Minch, 2004).

Additionally, the Location Privacy Protection Act, announced on 2001 in the United States, addresses the necessity and identifies several risks related to the privacy of the location information (U.S. Privacy location act, 2001). Location privacy is considered of high importance, since individuals should be able and free to explicitly identify what location information will be disclosed, when this can happen, how this information will be communicated and to whom this information will be revealed. Even through anonymization, as defined in (Pfitzmann & Koehntopp, 2000), personal data collection is bind with privacy, the disclosure of the personal identity might be useful for the delivery of personalized, pervasive or location-aware services, especially when accounting and charging is a requirement.

In this chapter we discuss about an innovative architecture, called STS, originally introduced in (Marias et al., 2006), to address several aspects of the location privacy issue. Firstly, it elaborates on the control of privacy that an individual should have over his/her location. It enables individuals to define different levels or rules of privacy (i.e. secrecy) over different portion of location data, depending on the operation environment (e.g., hostile) and the service that indents or asks to use location data. This is achieved through data and secret sharing techniques, which are discussed in a later section. Additionally, it gives users, or location targets, the capability to explicitly identify services or pervasive applications that might collect, store, and use location information. Finally, it provides anonymity on the distribution of the location information. STS architecture is designed to operate within an un-trusted environment. Portions of a target’s location data are distributed to public available nodes, which act as intermediate and temporal location servers. Targets authorize, on-demand, the pervasive or LBS services to access and combine the distributed location information. This is accomplished implicitly, through the disclosure of the mapping between a pseudonym and user’s or target’s location data. In the last few years, several methods have been proposed which deal with the location privacy issue on the lower layers of the communication stack (e.g., the IP layer). STS address location privacy in the application layer, enabling end-user to disclose location information to authenticated pervasive applications and location-based services. The STS architecture is applicable to environments that consist of user devices with several idiosyncrasies, such as luck of energy autonomy, memory and processing power. To provide secrecy it avoids complex computational tasks, such as producing key pairs, hashing and message authenticated codes. Instead, it deals with the division of location data into pieces and the distribution of these pieces to serving entities. Thus, it is applicable to smart spaces featuring ubiquitous services through the involvement of small gadgets, RF-tags, sensors and actuators that activated to infer the location of a user or target.

The remainder of this chapter is structured as follows. In Section 2 we provide the assumptions that STS considers for its operation. In Section 4 we present the STS architecture and the entities that it consists of. It introduces the secret share mechanism that enables the anonymity and privacy of location information. Subsequently, in Section 5, we discuss the procedures followed by the entities of the architecture. In Section 6, we note some issues for further discussion and finally in Section 7, we close with some proposed exercises.