Chapter IX
Privacy-Enhancing Technique:
A Survey and Classification

Peter Langendörfer
IHP, Germany

Michael Maaser
IHP, Germany

Krzysztof Piotrowski
IHP, Germany

Steffen Peter
IHP, Germany

ABSTRACT

This chapter provides a survey of privacy-enhancing techniques and discusses their effect using a scenario in which a charged location-based service is used. We introduce four protection levels and discuss an assessment of privacy-enhancing techniques according to these protection levels.

INTRODUCTION

Privacy is a very complex topic that touches legal, social, and technical issues. In this chapter we are focussing on the technical aspect of how to preserve privacy on the Internet. Throughout this chapter we define privacy as users' capability to determine who may know, store, and compute their data.

Privacy is one of the major concerns of Internet users (Cranor, 2000). The combination of wireless technology and Internet provides a means to combine real-world and cyber-world behaviour. Thus, extending Internet use to mobile devices is going to aggravate privacy concerns. But, privacy concerns influence also the revenue of companies which are offering their service via the Internet (Federal Trade Commission [FTC], 1999). So there is an interest in proper preserving of privacy on both sides. Especially big enterprises may suffer a lot from loss of trust in case they cannot protect the privacy-relevant data or do not adhere to their own privacy policies (Anton, He, & Baumer, 2004; Barbaro & Zeller, 2006).

Privacy-enhancing technologies (PETs) have become a hot research topic in the last few years, leading to a plethora of approaches that intend to protect privacy. This chapter provides an overview of PETs and discusses their effect on information disclosed while using a location-based service from a mobile device. In addition, an assessment of the protection level that can be achieved by applying the introduced means is provided. Thus, this chapter helps scientists to understand what is going on in the privacy research area so they can identify new research topics more easily. In addition, it enables practitioners to find approaches that allow them to build a privacy-preserving system.

The rest of this chapter is structured as follows. We first discuss privacy protection goals and provide an example that outlines which information can be gathered while using a charged service. In the third section we explain privacy-enhancing technologies. A discussion of the protection level achieved by individual means is given in the fourth section. The chapter concludes with an investigation of the currently reached deployment of privacy-enhancing techniques and a discussion of new research challenges.

PRIVACY PROTECTION GOALS

While browsing the Web or doing e- or m-commerce every user exposes information about his/her interests, personal data, and so forth to one or several of the following service providers: network service provider, for example, telco company; Internet service provider, for example, online book store; context service provider, for example, location handling system; and payment service provider, for example, his/her bank. Perfect privacy can be achieved if and only if the user reveals no information at all. Since this excludes the user from all benefits online services provide it is not a reasonable choice. The most valuable alternative is to disclose as little information as possible and only to the service provider who essentially needs this information.

In order to achieve a reasonable good separation of information, personal data and communication habits have to be protected at network as well as at application level. The former is an essential prerequisite of the latter, that is, protection at the application level does not make any sense as long as no protection at the network level is used. Protection at application level is much more difficult to achieve than protection at the network level. Here some information has to be revealed in order to get a useful service, that is, data has to be given away and therefore it has to be protected somehow. At the application level two dimensions have to be considered to prevent detailed profiling: time and location (in the sense of data gathering entity). The time dimension hinders service providers to construct a relationship between different service uses executed by the same individual but at different points in time. The location dimension provides separation of information between several service providers so that each one of them knows only data of a specific type.

In the following subsection we discuss a service scenario in which the current position of the user is requested by the service provider, who is also charging for the service. We use this scenario to show which data is known by which party of the whole system. We will also refer to this scenario later on to illustrate the effect of the privacy-enhancing techniques discussed in the following section.

Example

In this section we present a charged location-based service scenario that shows privacy issues in detail. It shows the information flow between the involved parties and the resulting dependencies that may cause privacy flaws.

The service provides its mobile user with information that is dependent on the location of the user. Additionally, the user pays for the information using a payment protocol. As shown in Figure 1 there are five parties, besides the user, involved in this scenario.

1. Positioning system is used to sense the current location of the user. Depending on the kind of the system the location information is sent to the location handling subsystem either direct from the positioning system or is forwarded by the user. In the first case the role of the user in location information forwarding is passive, in the latter active.