Chapter VI

Pseudonym Technology for E-Services

Ronggong Song, National Research Council Canada, Canada
Larry Korba, National Research Council Canada, Canada
George Yee, National Research Council Canada, Canada

Abstract

Pseudonym technology is attracting more and more attention and, together with privacy violations, is becoming a major issue in various e-services. Current e-service systems make personal data collection very easy and efficient through integration, interconnection, and data mining technologies since they use the user’s real identity. Pseudonym technology with unlinkability, anonymity, and accountability can give the user the ability to control the collection, retention, and distribution of his or her personal information. This chapter explores the challenges, issues, and solutions associated with pseudonym technology for privacy protection in e-services. To have a better understanding of how the pseudonym technology provides privacy protection in e-services, we describe a general pseudonym system architecture, discuss its relationships with other privacy technologies, and summarize its requirements. Based on the requirements, we review, analyze, and compare a number of existing pseudonym technologies. We then give an example of a pseudonym practice — e-wallet for e-services and discuss current issues.
Introduction

Background and Context

E-services such as e-commerce, e-government, e-health, and e-learning are becoming part of everyday life and, together with the Internet, have come to be seen as an information infrastructure for every subject and many application domains. The tremendous growth of the varied e-services has catapulted them from their original realm of academic research toward new mainstream acceptance and increasing social relevance. However, this dramatic increase has created the potential for eroding personal privacy. The fact is that cyberspace has invaded private space. Currently, almost all of the online e-services can be monitored by some unseen parties on the Internet. Controversies about cookies, click streams, traffic analysis, packet sniffing, and spam form merely the tip of an iceberg. It is a small wonder that privacy is such a critical issue for e-services. Users feel that one of the most important barriers to using e-services is the fear of having their privacy violated. Governments around the world have introduced legislation placing requirements upon the way in which personal information is handled.

According to the definition given by Goldberg in 1997, privacy refers to the ability of individuals to control the collection, retention, and distribution of information about themselves (Goldberg, Wagner, & Brewer, 1997). This does not mean that their personal information never gets revealed to any others. However, a system that respects their privacy should allow them to select what information about them is revealed and to whom. This personal information may be any of a large number of items, including their shopping habits, nationality, work history, living habits, personal communications, e-mail address, IP address, physical address, identity, and others.

Recently, many new techniques have been developed for providing privacy protection. Privacy protection is a process of finding an appropriate balance between privacy and multiple competing interests. Generally, they can be summarized into several kinds of techniques. One technique is the use of pseudonym technology for providing both anonymity and accountability. Another is the use of an anonymous communication network for providing anonymity and unobservability. A third is the use of personal privacy policies along with secure mechanisms to guarantee that e-service providers conform to these policies (Yee & Korba, 2005).

A pseudonym is a fake name or alias, for instance, a user’s digital account in a bank or an access account for a Web service. However, these pseudonyms are not protected with any special technologies so they can be easily linked to the real identity of the user. We name the special technologies as pseudonym technologies that can prevent service providers from linking a pseudonym to the real identity of the user. With pseudonym technology, users can access the e-services by their pseudonyms instead of their real identities while still allowing the system to authenticate them as valid users. Furthermore, the system not only cannot link the pseudonyms with the real identities but also cannot link the pseudonyms used for different applications. This gives the users certain privacy protection and the service provider essential security protection. For instance, the users can protect their personal information and shopping habits if they use pseudonym-credentials (e.g., e-cash) to access some e-services or order some products. At the same