Chapter 3.22
Privacy Enforcement in E-Service Environments

Carlisle Adams
University of Ottowa, Canada

Katerine Barbieri
University of Ottowa, Canada

ABSTRACT

This chapter presents technological measures for privacy enforcement (techniques that can be used to ensure that an organization's privacy promises will be kept). It gives an introduction to the current state of technological privacy enforcement measures for e-services environments, proposes a comprehensive privacy enforcement architecture, and discusses some remaining issues and challenges related to privacy enforcement solutions. The goal of the proposed architecture, aside from integrating many of the current isolated technologies, is to ensure consistency between advertised privacy promises and actual privacy practices at the e-service provider Web site so that users can have greater confidence that their personal data will be safeguarded.

INTRODUCTION

Privacy has become a growing concern for users on the Internet. It is widely believed that privacy concerns have affected the success of e-commerce initiatives, since users are reluctant to use online services for fear that their private data will be violated in some way. Privacy violations can be categorized according to many different schemes, but perhaps the simplest categorization divides violations into two major types. The first is the dissemination of private data to unintended recipients; for example, an entity collects a user's private data (such as address, phone number, and credit card number) and sells it to another entity without user consent. The second is the illegitimate use of a user's private data by an entity that legitimately received that data during a transaction; for example, private data provided for one purpose (a shipping address submitted for delivery of a book purchased online) is used by the legitimate receiver for another purpose (the

address is used for sending unwanted advertising pamphlets). Privacy enhancing technologies (PETs) can be helpful in protecting users against both types of privacy violation. The ultimate goal of PETs is to allow users to control how and with whom their private data is shared.

A number of organizations have begun efforts—including the implementation and use of PETs—to alleviate users' concerns regarding privacy. For example, many organizations now publish textual privacy policies on their Web sites. Some instead (or in addition) use the Platform for Privacy Preferences (P3P 1.0, 2002) policy definition language to formulate their privacy policies in a standard, machine-readable format. Other initiatives include performing privacy impact assessments (Hope-Tindall, 2002) and audits to ensure that defined privacy policies are adhered to. However, publishing privacy promises and performing assessments are only first steps to what may be referred to as *privacy enforcement*. Privacy promises and audits do not guarantee a user that the organization is always protecting his or her private data and using it only for its intended purpose.

Privacy enforcement takes privacy promises one step further: enforcement is the collection of techniques used to ensure (and, correspondingly, to give users the assurance) that an organization's privacy promises will be kept. That is, enforcement has to do with guaranteeing that organizations do what they say they will do with personal data ("practice what they preach"). This pertains to the entire lifespan of the data (collection, storage, use, dissemination, destruction) and should ideally take into account a user's own personal preferences regarding his or her personal data.

The techniques used in privacy enforcement today are typically procedural, organizational, or legal in nature. However, there is growing interest in the use of technological measures for privacy enforcement, primarily for the greater assurance that such measures can offer with respect to accuracy and effectiveness of the enforcement.

Research initiatives in privacy enforcement technology focus on such things as privacy policy definition languages that are machine-readable and machine-processable, storage technologies that are privacy-aware, data transformation or encapsulation methods that explicitly or implicitly incorporate privacy policies, and tools that assist users in creating appropriate privacy preferences. However, a critical lacking element is an overall architecture that ties these various initiatives together and provides a consistent privacy enforcement strategy across the enterprise. Such an architecture should readily accommodate industry standards wherever possible and would also be beneficial in helping to clarify missing components or research gaps in the privacy enforcement picture.

The primary objectives of this chapter are to introduce the reader to the state of technological privacy enforcement measures for e-services, to propose a comprehensive privacy enforcement architecture, and to discuss some remaining issues and challenges related to privacy enforcement solutions.

BACKGROUND

This section provides definitions and detailed descriptions of technological measures for privacy enforcement, as well as systems and major architectural components that have been researched and implemented.

Privacy Policy Definition and Exchange Languages

A significant amount of work has been done in the area of privacy policy definition languages. Some examples follow.

Platform for Privacy Preferences (P3P)

Platform for Privacy Preferences (P3P) is an XML-based W3C standard (P3P 1.0, 2002) for