Chapter 15
Usable Privacy-Enhancing Identity Management: Challenges and Approaches

Simone Fischer-Hübner
Karlstad University, Sweden

John Sören Pettersson
Karlstad University, Sweden

ABSTRACT

A critical success factor for Privacy-Enhancing Technologies (PETs), and for Privacy-Enhancing Identity Management in particular, will be user-friendly and intelligible user interfaces that are legally compliant and convey trust. Such user interfaces have to meet challenges such as the user-friendly representation of complex PET concepts (such as “pseudonyms”, “unlinkability” or “anonymous credentials”) that are unfamiliar to many users, the provision of security, the enforcement of legal privacy principles, such as informed consent or transparency, as well as the mediation of reliable trust to the end users. In this paper, we will discuss such challenges for usable privacy-enhancing identity management and will provide some HCI guidelines for addressing those challenges.

INTRODUCTION

In today’s network society, users have lost effective control over their personal spheres. When communicating via the Internet, users are leaving many personal data traces at various sites, which can be easily compiled to extensive personal profiles. These processes of personal data collection and processing are often not transparent for the individuals concerned. It is however critical to our society and to democracy to retain and maintain the individual’s autonomy and thus to protect privacy and particularly the individual’s right to informational self-determination. Powerful tools for technically enforcing user control and informational self-determination as well as the privacy principle of data minimisation can be provided by privacy-enhancing Identity Management systems, as those which have been developed within the EU FP6 integrated project PRIME (“Privacy and Identity Management for Europe”) and its follow-up EU FP7 integrated project PrimeLife (“Privacy and Identity Management for Life”).

DOI: 10.4018/978-1-60960-057-0.ch015
Identity Management (IDM) can be defined to subsume all functionality that supports the use of multiple identities, by the identity owners (user-side IDM) and by those parties with whom the owners interact (services-side IDM). According to Pfitzmann and Hansen (2008), identity management means managing various partial identities (i.e. set of attributes, usually denoted by pseudonyms) of a person, i.e. the administration of identity attributes including the development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role. Privacy-enhancing IDM is also sufficiently preserving unlinkability (as seen by an attacker) between the partial identities of an individual person required by the applications.

With privacy-enhancing identity management such as with PRIME, all interactions are a priori anonymous, and individuals can choose to act under different pseudonyms with respect to communication partners or activities, and furthermore have control over whether or not interactions and pseudonyms can be linked with each other or not. Moreover, PRIME provides tools that help individuals to define who has the right to do what under which conditions with their personal data, as well as tools providing transparency about who has received what personal data related to them and possibilities to trace personal data being passed on.

Privacy-enhancing identity management implies that users can make informed choices about the releases of personal data, the selections of credentials for proving personal properties, and about their privacy and trust policy settings. For enabling users to make well-informed decisions, user interfaces (UIs) are needed that inform them about the trustworthiness and the privacy policies of their communication partners as well as the implications of personal data releases. These user interfaces should be informative while not being perceived as intrusive, intuitive, legally compliant and trustworthy. Privacy-enhancing identity management technologies will only be successful if they are accepted and applied by the end users.

Therefore, several challenges have to be addressed regarding the user interfaces such as how to represent complex Privacy-Enhancing Technology (PET) concepts that are unfamiliar to most users in a user-friendly way, how to provide security against phishing and spoofing attacks, how to enforce legal privacy principles and how to mediate reliable trust.

In this chapter, we will discuss these challenges and problems for meeting them in more detail. Then, we will propose a list of recommendations for designers of privacy and identity management systems to address these challenges. These recommendations also include concrete suggestions of possible approaches to meet those challenges that we have elaborated within the PRIME and PrimeLife projects or that have been suggested by others.

**RELATED WORK**

This chapter is based on results from the HCI activities of the PRIME and PrimeLife projects. Earlier results from the HCI work within the PRIME project have also been reported, e.g. in (Fischer-Hübner et al. 2008) and (Pettersson 2008). However, this paper contains substantial updates of PRIME project results and includes also some first results from the PrimeLife project’s HCI work.

There has been some previous related work discussing HCI challenges and HCI Guidance for secure system (e.g., Herzog 2007, Johnston et al. 2004, Yee 2002, Garfinkel 2005) and for privacy-enhancing technologies (e.g., Patrick et al. 2003, Patrick and Kenny 2003). Also very recently Dhamija and Dusseault discuss flaws of identity management posing HCI and security challenges and provide some recommendations how to address them (Dhamija and Dusseault 2008). However, in contrast to our work presented