Chapter 3
Towards Designing E-Services that Protect Privacy

George O. M. Yee
Carleton University, Canada

ABSTRACT

The growth of electronic services (e-services) has resulted in large amounts of personal information in the hands of service organizations like banks, insurance companies, and online retailers. This has led to the realization that such information must be protected, not only to comply with privacy regulations but also and more importantly, to attract clients. One important dimension of this goal is to design e-services that protect privacy. In this paper, the author proposes a design approach that incorporates privacy risk analysis of UML diagrams to minimize privacy risks in the final design. The approach iterates between the risk analysis and design modifications to eliminate the risks until a design is obtained that is close to being risk free.

INTRODUCTION

Numerous electronic services (e-services) targeting consumers have accompanied the rapid growth of computerization. For example, e-services are available for banking, shopping, learning, healthcare, and Government Online. E-services include "web services" that are based on the service oriented architecture (SOA) (O'Neill et al., 2003). However, most of these services require a consumer's personal information in one form or another, leading to concerns over privacy.

Researchers have proposed various approaches to protect personal information, including data anonymization (Iyengar, 2002; Kobsa & Schreck, 2003) and pseudonym technology (Song et al., 2006). Other such proposals include treating privacy protection as an access problem and then bringing the tools of access control to bear for privacy control (Adams & Barbieri, 2006), treating privacy protection as a privacy rights management problem using the techniques of digital rights management (Kenny & Korba, 2002), and considering privacy protection as a privacy policy compliance

DOI: 10.4018/978-1-4666-1580-9.ch003

problem, verifying compliance with secure logs (Yee & Korba, 2004). However, most e-services today do not use the above approaches, preferring to rely instead on stating a privacy policy and then trying to follow that policy manually, without any of the above techniques or tools or any automated checks in place. As a result, the public is often the victim, as privacy leaks (e.g., credit card files stolen) are discovered and reported in the media. Thus, today's e-services do a poor job of protecting consumer privacy and new effective approaches for such protection are always needed. This is the motivation for this work.

The area of e-services has been chosen for this work because it probably holds the highest risk for the loss of privacy today, in terms of the amount of private information held and the growth of that information. Consider the following. E-services probably require the most consumer private information in order to function than any other type of application. This can be seen once one realizes that if an application requires consumer private information, it can probably be categorized as an e-service. E-services include e-health services where privacy is critical. E-services are growing very rapidly, along with the Internet.

The various approaches for protecting privacy described above all presume to know where and what protection is needed. They presume that some sort of analysis has been done that answers the question of "where" and "what" with respect to privacy risks. Without such answers, the effectiveness of the protection comes into question. For example, protection against house break-ins is totally ineffective if the owner only secures the front door without securing other vulnerable spots such as windows (the "where"). Of course, how the owner secures these spots is critical too ("what" protection). A more effective break-in risk analysis would have identified the windows as being vulnerable to break-ins as well, resulting in better protection against break-ins if the owner additionally secures the windows. In the same way, privacy risk analysis of service systems, considering "where" and "what", is essential to effective privacy protection.

The objective of this paper is to propose an e-services design approach that incorporates privacy risk analysis to obtain designs that are more likely to preserve privacy than designs that did not use privacy risk analysis. The final design is obtained as the culmination of a series of alternative designs where each alternative design is obtained by re-design to avoid or lessen privacy risks identified through a privacy risk analysis on the last design. Each design is comprised of UML diagrams and the privacy risk analysis is done on a Personal Information Map (PIM, explained below) that is derived from UML diagrams. UML has been chosen for its widespread use among software developers. Basing this approach on UML will make it easier to adopt this approach in practice. Note that the approach does not guarantee that the system implemented from the final design is totally free of privacy risks. Such risks can arise due to implementation errors or the final design itself was not totally risk free (a totally risk free design may not have been feasible due to other constraints, e.g., tight financial budget).

This design approach is based on the principal that it is more effective to design privacy protection into a software system from the beginning, rather than to add it later after the system has been implemented. This is the same principal that it is more effective to design in security from the beginning rather than adding it after implementation, as described in McGraw (2002).

This paper is organized into the following sections: "Privacy and E-Services" defines privacy, privacy policies, privacy risks, and what they mean for e-services. "Approach for Designing E-Services that Protect Privacy" presents the proposed design approach. "Related Work", "Evaluation of Approach" and "Conclusions and Future Research" are as suggested by their names.