Chapter 8
Designing Privacy Aware Information Systems

Christos Kalloniatis
University of the Aegean, Greece

Evangelia Kavakli
University of the Aegean, Greece

Stefanos Gritzalis
University of the Aegean, Greece

ABSTRACT

A major challenge in the field of software engineering is to make users trust the software that they use in their everyday activities for professional or recreational reasons. Trusting software depends on various elements, one of which is the protection of user privacy. Protecting privacy is about complying with user’s desires when it comes to handling personal information. Users’ privacy can also be defined as the right to determine when, how and to what extend information about them is communicated to others. Current research stresses the need for addressing privacy issues during the system design rather than during the system implementation phase. The aim of this chapter is to elevate the modern practices for ensuring privacy during the software systems’ design phase. Through the presentation of the modern methods, the basic privacy requirements that should be considered during system analysis are introduced. Additionally, a number of well known methods that have been introduced in the research area of requirements engineering which aim on eliciting and analyzing privacy requirements during system design are introduced and analyzed. Finally, a comparative analysis between these methods is presented.

INTRODUCTION

In the online world every person has to hold a number of different data sets so as to be able to have access to various e-services and take part in specific economical and social transactions. Such data sets require special consideration since they may convey personal data, sensitive personal data, employee data, credit card data etc. Recent surveys (Business, 1998; PricehouseCoopers, 2001) have shown that people feel that their privacy is at risk from identity theft and erosion of individual rights. Therefore, it is obvious that privacy violation is an issue of great importance.
these days especially for the active online users that daily accomplish transactions in the new digital world. Another issue of great importance is the degree of trust that online users have on the information systems they use.

One of the main criteria that formulate users’ trust regarding the use of an information system is the way that that their privacy is protected. The aforementioned issues along with the issue of handling privacy as a design criterion during the design and not the implementation phase of an information system consist the basic concerns of recent researches (Anton, 1996; Kalloniatis et al., 2009; Mouratidis et al., 2003a).

Research efforts aiming to the protection of user privacy fall in two main categories: security-oriented requirement engineering methodologies and privacy enhancing technologies. The former focus on methods and techniques for considering security issues (including privacy) during the early stages of system development and the latter describe technological solutions for assuring user privacy during system implementation. The main limitation of security requirement engineering methodologies is that they do not link the identified requirements with implementation solutions. Understanding the relationship between user needs and the capabilities of the supporting software systems is of critical importance. Privacy enhancing technologies, on the other hand, focus on the software implementation alone, irrespective of the organizational context in which the system will be incorporated. This lack of knowledge makes it difficult to determine which software solution best fits the organizational needs.

The aim of this chapter is to elevate the modern practices for ensuring privacy during the software systems’ design phase. Through the presentation of the modern methods, the basic privacy requirements that should be considered during system analysis are introduced. Additionally, a number of techniques are mentioned for incorporating these requirements on the processes of the developing systems.

Specifically, in section 2, the term privacy along with the basic privacy requirements as they are formed from recent research are defined. In section 3, a number of well-known methods and techniques, proposed in the fields of requirements engineering and security engineering, which support the elicitation and management of security and privacy requirements during the early stages of system development, are mentioned. In section 4, a comparative analysis between these methods is presented along with the analysis of the comparison results. Finally, in section 5, the chapter concludes by addressing issues regarding the incorporation of privacy during system development.

**PRIVACY AND PRIVACY REQUIREMENTS**

In this section the basic concepts of privacy are presented. Additionally, the need for protecting privacy during the system design phase is stressed out and the basic privacy requirements during the analysis and design of information systems are presented.

**Privacy**

When a user types a text using a typical text editor he/she usually does not think if someone is close enough to observe and see the text being written. When the same user surfs the Internet it is like walking in the middle of a Rolling Stone’s Concert while hundreds of people can see what he/she is doing or listen what he/she says (Cannon, 2004).

Most people use the Internet for its services either for personal or for recreational reasons. Internet and email services are offered from the Internet Service Providers (ISPs). These providers use servers that keep logs of Internet traffic, typically for tuning, performance monitoring etc. Also personal data are stored for various reasons...