Chapter 79
Addressing Privacy in Traditional and Cloud-Based Systems

Christos Kalloniatis
University of the Aegean, Lesvos, Greece

Evangelia Kavakli
University of the Aegean, Lesvos, Greece

Stefanos Gritzalis
University of the Aegean, Samos, 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. Amid the main criteria that formulate users' trust is the way that that their privacy is protected. Indeed, privacy violation is an issue of great importance for active online users that daily accomplish several transactions that may convey personal data, sensitive personal data, employee data, credit card data and so on. In addition, the appearance of cloud computing has elevated the number of personally identifiable information that users provide in order to gain access to various services, further raising user concerns as to how and to what extend information about them is communicated to others. The aim of this work is to elevate the modern practices for ensuring privacy during software systems design. To this end, 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 modeling privacy requirements during system design are introduced and critically analyzed. The work completes with a discussion of the additional security and privacy concepts that should be considered in the context of cloud-based information systems and how these affect current research.

DOI: 10.4018/978-1-5225-3923-0.ch079

INTRODUCTION

In the online world every person has to hold a number of different data sets in order to have access to 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; Pricehouse Coopers, 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. In addition, the appearance of cloud computing has raised new challenges regarding the security of the information stored, processed and communicated in the cloud environment context. This has further increased user concerns affecting the degree of trust that online users have on the information systems they use.

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), focusing either on methods and techniques for considering security issues (including privacy) during the early stages of system development or on the technological solutions for assuring user privacy during system implementation. However, these works have not been developed for cloud-based systems. On the other hand, industry-led reports (Microsoft, 2012; Version One 2012; Cloud Computing 2012) have been published discussing security and privacy issues within the context of cloud computing. However, most of these reports do not provide a clear linkage with relevant security and privacy threats. Moreover, they do not explicitly define any methodology for incorporating security and privacy analysis in cloud based systems design.

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. Additionally, a number of new security and privacy concepts are presented enhancing the set of identified privacy requirements in order to assist analysts in designing privacy aware information systems in cloud computing environments besides traditional distributed systems.

Specifically, in the second section, the term privacy along with the basic privacy requirements as they are formed from recent research are defined. In the third section, 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. A comparative analysis between these methods is presented in the fourth section. The fifth section focuses on the security and privacy requirements that are specific to cloud based systems. Finally, in the sixth section the paper concludes with a discussion of the challenges and respective features of a methodology to support security and privacy analysis of cloud-based systems.

PRIVACY AND PRIVACY REQUIREMENTS

This section focuses on the meaning of privacy and its characteristics in the context of modern information systems. 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.