Chapter 22
Designing Secure and Privacy-Aware Information Systems

Christos Kalloniatis
University of the Aegean, Lesvos, Greece

Argyri Pattakou
University of the Aegean, Lesvos, Greece

Evangelia Kavakli
University of the Aegean, Lesvos, Greece

Stefanos Gritzalis
University of the Aegean, Samos, Greece

ABSTRACT

Pervasiveness of information systems is well underway, redefining our social and economic relationships. This technological revolution has generated enormous capabilities, but also enabled the creation of new vulnerabilities and threats. A major challenge in the field of information systems is therefore, to ensure the trustworthiness of the underlying technologies that make possible the generation, collection, storage, processing and transmission of user data at rates more intensive than ever before. Trust in information systems depends on different aspects, one of which is the security of user's data. Data security is referred as the protection of user's data from corruption and unauthorized access. Another important aspect of trust is the protection of user's privacy. Protecting privacy is about complying with user's desires when it comes to handling personal information. Without security to guarantee data protection, appropriate uses of that data cannot be realized. This implies that security and privacy issues are inherently intertwined and should be viewed synergistically. The aim of this paper is to elevate modern practices for ensuring security and privacy during software systems analysis and design. To this end, the basic security and privacy requirements that should be considered are introduced. Additionally, a number of well known methods in the research area of requirements engineering which focus on eliciting and modeling security and privacy requirements are described. Finally, a comparative analysis between these methods is presented.

DOI: 10.4018/978-1-5225-7113-1.ch022

1. INTRODUCTION

Recent years have witnessed an increasing integration of information and communication technology (ICT) into everyday activities. As a result, the social and economic processes of our society are becoming increasingly dependent on the functioning of the information and communication infrastructure. At the same time, interconnectivity and dependencies between information systems and the increased complexity of new computing paradigms, such as cloud computing, big data and the Internet of Things create vulnerabilities, signifying that there is a correspondingly greater chance of suffering security breaches with consequences ranging from extensive financial losses to dangers to human life (Mellado et al. 2010; Nemati, 2011).

Another aspect of this increase in ICT-mediated activities in various societal spheres is that individuals, organizations and companies need to manage private or confidential data sets. Such data sets require special consideration since they may convey personal data, sensitive personal data, employee data, credit card data etc. Recent surveys (Chip 2007; PricewaterhouseCoopers, 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 becoming an issue of great importance especially for the active online users that daily accomplish transactions in the new digital world. As a result, concerns are raised regarding the lack of trust regarding the use of information systems and the extent to which information security and user privacy can be ensured.

Information systems development approaches dealing with security and privacy issues fall in two main categories: security-oriented requirement engineering methodologies and security enforcement techniques (including privacy enhancing techniques). 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 security and 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 technologies is of critical importance. Security enforcement techniques, on the other hand, focus on system architecture and implementation issues, irrespective of the organizational context in which the system will be incorporated. This lack of knowledge makes it difficult to determine which solution best fits the organizational needs (Salini & Kanmani, 2013).

The aim of this paper is to elevate the modern practices for ensuring security and privacy during information systems design. It provides a unifying view of security and privacy requirements engineering through the explicit definition of the basic requirements in each category, and the comparative analysis of existing approaches using a multidimensional framework.

Specifically, section 2 discusses the relation of data security and privacy and describes a set of basic security and privacy requirements as they have been defined in relevant literature. 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 described. In section 4, a comparative analysis between these methods is presented along with the analysis of the comparison results. Finally, section 5 concludes by discussing related work and future directions.