Chapter 10
Security and Privacy Requirements Engineering

Nancy R. Mead
Carnegie Mellon University, USA

Saeed Abu-Nimeh
Damballa Inc., USA

ABSTRACT

Security requirements engineering identifies security risks in software in the early stages of the development cycle. In this chapter, the authors present the SQUARE security requirements method. They integrate privacy requirements into SQUARE to identify privacy risks in addition to security risks. They then present a privacy elicitation technique and subsequently combine security risk assessment techniques with privacy risk assessment techniques. The authors discuss prototype tools that have been developed to support SQUARE for security and privacy as well as recent workshops that have focused on additional results in the security and privacy requirements area. Finally, the authors suggest future research and case studies needed to further contribute to early lifecycle activities that will address security and privacy-related issues.

INTRODUCTION

Several initiatives have tried to standardize the processes of the software lifecycle, yet ISO/IEC 12207:2008 is considered the standard of software lifecycle processes (ISO/IEC 12207, 2008) by most. This standard divides software lifecycle processes into five high-level phases:

1. Acquisition,
2. Supply,
3. Development,
4. Operation, and
5. Maintenance.

The acquisition phase concentrates on initiating the project. The supply phase concentrates on developing a project management plan. In the development phase, the software product is designed, created, and tested. In the operation phase, users start utilizing the product. Finally, in the maintenance phase, the product is maintained to stay operational.

DOI: 10.4018/978-1-4666-7381-6.ch010

Software requirements are discussed and addressed at an early stage in the software development phase. Requirements engineering concentrates on the real-world goals for, functions of, and constraints on software systems. In addition, it covers the relationship of these factors to precise specifications of software behavior and to their evolution over time and across software families (Zave, 1997).

Requirements elicitation in software development concentrates on functional and nonfunctional requirements. Functional or end-user requirements are the tasks that the system under development is expected to perform. Nonfunctional requirements are the qualities that the system must adhere to. Functional requirements are not as difficult to tackle, as it is easier to test their implementation in the system under development. Security and privacy requirements are considered nonfunctional requirements, although in many instances they do have functionality (Abu-Nimeh, Miyazaki, & Mead, 2009).

The Security Quality Requirements Engineering (SQUARE) method is used to identify software security issues in the early stages of the development lifecycle. In the following sections, we present the SQUARE method in detail and discuss the integration of privacy requirements into SQUARE.

It is essential to identify the security and privacy issues in a software risk assessment. Conducting a risk assessment is a step in a risk management process that involves the identification, assessment, and prioritization of risks related to a situation. A risk assessment determines, in a quantitative or qualitative way, the value of these risks. A security risk assessment identifies the threats to systems, while a privacy risk assessment identifies data sensitivities in systems. The SQUARE method relies on security risk assessment techniques to assess the levels of security risk in systems. However, these security risk assessment techniques are not adequate to address privacy risks. Therefore, we combine the security risk assessment techniques in the SQUARE method with privacy risk assessment techniques.

Background

While the Security Quality Requirements Engineering (SQUARE) method (Mead, Hough, & Stehney, 2005) aims to identify software security risks in the early stages of the software development process, privacy requirements engineering (Chiasera, Casati, Daniel, & Velegrakis, 2008) serves to identify privacy risks early in the design process. Some research studies (Pfleeger & Pfleeger, 2009) indicate that privacy requirements engineering is a less mature discipline than security engineering and that underlying engineering principles give little attention to privacy requirements. However, more recently, privacy requirements engineering has evolved through work at a number of workshops, notably the RELAW workshops at the IEEE International Requirements Engineering Conference (RE).

Some (Adams & Sasse, 2001) claim that most privacy disclosures happen due to defects in design and are not the result of an intentional attack. Nevertheless, security is necessary but not sufficient to ensure privacy.

Although security and privacy risks overlap, relying merely on protecting the security of users does not imply the protection of their privacy. For instance, health records can be secured from various types of intrusions; however, the security of such assets does not guarantee that the privacy of patients is secure. The security of such records does not protect against improper authorized access or disclosure of records.

The SQUARE method generates categorized and prioritized security requirements following its nine steps (Mead et al., 2005):

1. Technical definitions are agreed upon by the requirements engineering team and project stakeholders.
2. Assets, business, and security goals are identified.
3. In order to facilitate full understanding of the studied system, artifacts and documentation are created.