Chapter 11
Combining Security and Privacy in Requirements Engineering

Saeed Abu-Nimeh
Damballa Inc., USA

Nancy R. Mead
Carnegie Mellon University, USA

ABSTRACT

Security requirements engineering identifies security risks in software in the early stages of the development cycle. In this chapter, the authors present a security requirements approach dubbed SQUARE. They integrate privacy requirements into SQUARE to identify privacy risks in addition to security risks. They present a privacy elicitation technique and then combine security risk assessment techniques with privacy risk assessment techniques.

INTRODUCTION

There have been several initiatives to standardize the processes of software lifecycle. Yet, ISO 12207 is considered the standard of software lifecycle processes (Singh, 1998). The standard divides software lifecycle processes into 5 high level phases: acquisition, supply, development, operation, and 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, and in the maintenance phase the product is maintained to stay operational.

Software requirements are addressed and discussed 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 is concerned with the relationship of these factors to precise specifications of software behavior, and to their evolution over time and across software families (Zave, 1997).

DOI: 10.4018/978-1-61350-507-6.ch011

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. However, nonfunctional requirements are the qualities that the system is to 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. Next, we present SQUARE in detail. Then, the integration of privacy requirements into SQUARE is discussed in the following section.

To identify the security and privacy issues in software a risk assessment is needed. Risk assessment is a step in a risk management process. A risk management process involves the identification, assessment, and prioritization of risks related to a situation. Risk assessment is determining in a quantitative or qualitative way the value of these risks. Security risk assessment identifies the threats to systems, while privacy risk assessment identifies data sensitivities in systems. SQUARE 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 addressing privacy risks. Therefore, we combine the security risk assessment techniques in SQUARE with privacy risk assessment techniques.

BACKGROUND

Security requirements engineering (Mead, Hough, & Stehney, 2005) aims to identify software security risks in early stages of the design process. Privacy requirements engineering (Chiasera, Casati, Daniel, & Velegrakis, 2008) serves to identify privacy risks early in the design process. Recent research studies (Peeger & Peeger, 2009) have shown that privacy requirements engineering is less mature than security engineering and that underlying engineering principles give little attention to privacy requirements. In addition, (Adams & Sasse, 2001) claim that most of the privacy disclosures happen due to defects in the design, and are not the result of an intentional attack. Therefore, although security and privacy risks overlap, relying merely on protecting the security of users does not necessarily 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. SQUARE generates categorized and prioritized security requirements following these 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.
4. A security risk assessment is applied to determine the likelihood and impact of possible threats to the system.
5. The best method for eliciting security requirements is determined by the requirements engineering team and the stakeholders.
6. Security requirements are elicited.
7. Security requirements are categorized.
8. Security requirements are prioritized.
9. The security requirements are inspected to ensure consistency and accuracy.