Chapter 23

Software Security Engineering – Part II: Security Policy, Analysis, and Design

Issa Traore
University of Victoria, Canada

Isaac Woungang
Ryerson University, Canada

ABSTRACT

This chapter explains the major objectives of a security policy, with focus on how applications that can protect data at all access points can be developed. Access control models and their known issues are discussed. From a security policy prospective, the security design principles and modeling using the UML are also discussed. In addition, an informal discussion on potential software security metrics that can be used for security measurement, and that are currently the purpose of active research, is conducted. Finally, a discussion on security testing involving the use of these metrics, are discussed. Several examples are used to illustrate the studied concepts.

INTRODUCTION

More often, security is compromised not only by breaking the mechanisms such as encryption or security protocols that have been put in place in organizations, but by actually identifying and making use of the weaknesses by following the way that they are being utilized. Integrating the security requirements analysis into the standard requirements process has been proved to be the right direction to pursue. In our Chapter entitled "Software Security Engineering – Part I: Security Requirements and Risk Analysis," a novel model-driven perspective on secure software engineering was proposed, which integrates seamlessly software security analysis with traditional software development activities, resulting to a systematic security engineering process. A discussion on the security risk analysis was also presented as related to the notions of threat, vulnerability, and attacks. These steps are not a one-time deal in the sense that they should be complemented with the development of a security policy for the organization (as well as its updates) in order to realize a complete

DOI: 10.4018/978-1-4666-8111-8.ch023

and effective security protection framework. A security policy can be characterized as driven by the different methods used for performing the risk analysis in conjunction with the support of the organization's management in developing a plan to deal with security, in addition to the actual security protocols in place in the organization.

There is a common consensus among computer security actors and professionals that ensuring the security of the software for an organization is a continuous process that relies on the improvements made on the formulation of the security policy, with the goal to efficiently asses the security risks. Typically, this process involves formulating a statement that spells out the types of defenses that are needed to be configured so that unauthorized access to the system is blocked (access control), the methods to be used by the organization to respond to attacks (attack models and countermeasures), the manner in which the organization's resources should be safely handled so as to avoid or reduce the loss/damage of data and resources.

Different types of risk analysis can be used to design a security policy as well as to update and improve it. Two benchmark approaches that are often used.

The first one is the Survivable Network Analysis (SNA) developed by the CERT (US-CERT, 2012). The SNA approach comprises four steps: (1) *System definition* – where the system's organizational requirements are defined, and the system architecture is analyzed; (2) *Essential capability definition* – where the essential assets and services of the system are identified and marked as critical to the organization; (3) *Compromise capability definition* – where scenarios of intrusion to the system are defined and the types of damage resulting from these intrusions can be identified and traced within the targeted system architecture; (4) *Survivability analysis* – where potential point of failure in the system are identified and methods for addressing them are presented, along with recommendations on improving the system's capability to survive the above intrusions and related attacks.

The second benchmark approach is Threat and Risk Assessment (TRA) approach discussed in (ACSI, 2012). The TRA approach is composed of four steps as well: (1) Asset definition – where the information/data need to be defended (such as software, hardware, etc) are identified; (2) Threat assessment – where the types of threats affecting the asset are identified; (3) Risk assessment – where each asset is evaluated for existing safeguards and risks to other assets; (4) Recommendations – where recommendations on methods each risk identified in Step 3 are provided (as part of a security policy).

Any of the above risk analysis frameworks can be used as a starting point towards designing and developing a security policy process. To this purpose, several systematic approaches (so-called security policy roadmaps) have been proposed in the literature (ITSEC,1991), (ISO17799, 2012), (ISS, 2001), (Sun, 2001), (SANS, 2007), (Security Classification: PUBLIC, 2011). each of which reflects in its own fashion the way that safeguards and controls that protect information from security threats can be identified, the issues and factors that should be considered when setting up the policies, and how these policies can been developed and their compliancy can be measured (Krishni, 2001). The goal of these guidelines and controls is to ensure that the developed security policy reflects the organization's security needs as much as possible.

Typically, the approach used in designing a security policy roadmap consists of: (1) identifying the assets to be protected; (2) identifying the vulnerabilities and threats and their likeliness to occur; (3) Determine a cost effective measures to be used to protect the asset; (5) Release the findings to the appropriate parties; (6) Monitor and update the process in a continuous manner in order to improve it.

In this Chapter, our attention is on introducing the major objectives of a security policy, with focus on access control models and their known issues are discussed. From a security policy