IDEA GROUP PUBLISHING **ITB12233**

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

This paper appears in the publication, Enterprise Information Systems Assurance and Systems Security
edited by Merril Warkentin © 2006, Idea Group Inc.

Chapter XI

Security Engineering: It Is All About Control and Assurance Objectives

Ronda R. Henning, Harris Corporation, USA

Abstract

Information security engineering is the specialized branch of systems engineering that addresses the derivation and fulfillment of a system's security requirements. For years, security engineering practitioners have claimed that security is easier to build into a system when it is integrated with the system analysis and design. This paper presents some basic tenets of security analysis that can be applied by any systems engineer to ensure early integration of security constraints into the system definition and development process. It sheds light on security requirements interpretation to facilitate the fulfillment of security requirements throughout the system lifecycle.

Introduction

The systems engineering process manages the overall requirements fulfillment and derivation process for a given information system development effort. The specialized branch of systems engineering that supports the fulfillment of information security

requirements is the discipline of security engineering. Ideally, information assurance requirements are engineered into a system from the concept definition phase forward. Too often, security is considered an afterthought or a "should" requirement that is optional to the system function and is discarded during early system analysis. Security engineering must support a methodical, repeatable process with measurable, quantifiable results to be considered a scientific pursuit.

Sommerville (2001) characterizes system properties as being functional and non-functional in nature. Functional properties contribute to the achievement of the system objectives. Non-functional properties relate to the behavior of the system in operation and are most often related to the user's perception of the system's value. For example, security is often considered a non-functional property of a system, but if the data is corrupted due to the failure of security mechanisms, it impacts the ability of the system to meet its functional objective.

Koch and Parisi-Presicce (2003) states, "Security requirements are difficult to analyze and model. Security policies are generally specified in terms of highly specialized security models that are not integrated with general software engineering models" (p. 67). Haley, Laney, and Nuseibeh (2004) states, "Expressing specific security requirements is difficult. They tend to be stated as crosscutting concerns that impact many functional requirements" (p. 112). Security requirements are often discarded during early analysis and addressed through the use of separate appliances, such as firewalls, later in the design process.

This chapter presents an approach to security requirement analysis that can be applied during systems analysis. For the broadest application, the chapter does not tie itself to any given development methodology or design technique, nor does it endorse any single standard. Each enterprise tailors its system development artifacts to reflect their unique environments, so this chapter focuses on the content of these artifacts rather than artifacts themselves.

The remainder of this chapter is organized as follows: the security objectives associated with system requirements development are presented. Then, the distinction between security requirements and assurance requirements is described. Sources of security requirements are discussed next. Creation techniques for good security requirements are presented, as are some techniques for tying security requirements into subsequent design phases. Finally, the major cost/benefit analysis factors associated with selecting among alternative security implementations are presented.

Control Objectives

As with other requirement families, information security requirements are normally expressed in terms of their control objectives. For both the *information system* and the *information* it contains, the control objectives provide the foundation for all derivative security requirements. The control objectives are based on three sources (ISO/IEC, 1998):