Chapter 16
Secure Software Education:
A Contextual Model-Based Approach

J. J. Simpson
System Concepts, LLC, USA

B. Endicott-Popovsky
University of Washington,USA

M. J. Simpson
System Concepts, LLC, USA

V. Popovsky
University of Idaho,USA

ABSTRACT

This article establishes a context for secure information systems development as well as a set of models used to develop and apply a secure software production pedagogy. A generic system model is presented to support the system context development, and to provide a framework for discussing security relationships that exist between and among information systems and their applications. An asset protection model is tailored to provide a conceptual ontology for secure information system topics, and a stable logical framework that is independent of specific organizations, technologies, and their associated changes. This asset protection model provides a unique focus for each of the three primary professional communities associated with the development and operation of secure information systems. In this paper, a secure adaptive response model is discussed to provide an analytical tool to assess risk associated with the development and deployment of secure information systems, and to use as a security metric. A pedagogical model for information assurance curriculum development is then established in the context and terms of the developed secure information system models. The relevance of secure coding techniques to the production of secure systems, architectures, and organizational operations is also discussed.

INTRODUCTION

Within the software engineering community, there is an increasing recognition that secure coding practices are only a subset of the activities needed to create secure information systems. Information systems, including the software, hardware, and people that contribute to those systems, continue to change and adapt to new technologies and science. This paper is organized around the fundamental ideas that (1) all system and software security exists in an adaptable system context, and (2) a range of conceptual models are necessary to organize, discuss and understand these adaptable

DOI: 10.4018/978-1-4666-1580-9.ch016

security aspects. The practice of secure information systems design, development, deployment and operation is shared by three professional communities, the systems engineering (including software engineering) community, the information assurance community, and the justice and intelligence communities. A generic system model is introduced and combined with a comprehensive, layered asset protection model to establish an abstract set of security concepts that are independent of any specific technology and/or application approach. The generic system model provides a common basis for the communication within the systems/software engineering communities regarding secure information systems. The asset protection model provides a focus point for each of the professional communities, and supports the clear communication of information associated with secure information systems.

As these two models are interrelated and expanded in a combined system security model, operational connections become evident. System operational effectiveness as well as operational suitability are defined, developed and discussed as they relate to security and security education. Potential information system risks need to be understood and addressed. To this end, a system security metric is introduced that enables an analysis of what risks might be present during the development and deployment of secure information systems. This tool also introduces a method to help determine what topics might need to be addressed within secure information systems or secure coding practices curriculum in order to mitigate those risks. This set of security concepts is then integrated with a pedagogical model for information assurance curriculum development. Common system attack patterns, as well as software weaknesses and vulnerabilities, are used as examples to illustrate the processes necessary to increase software quality by improving software security education and development. Standard secure software approaches are mapped over the combined system security model, and discussed in the proper system context. A rich conceptual topology is developed and used to frame and communicate the many aspects of secure software engineering education. Next the generic system model will be introduced and outlined to support the introduction and discussion of the asset protection model.

GENERIC SYSTEM MODEL

The practice of systems engineering has produced a number of technical, organizational and process-based approaches to the solution of large-scale, socio-technical engineering and process problems. One of the key aspects associated with systems engineering is the development of system context models and system functional models. The Generic System Model (GSM) is based on the fundamental idea of a system boundary that distinguishes a boundary between inside the system and outside the system. The system context exists outside of the system boundary; the system concept is used to organize the internal system content. The system boundary is composed of an outward-looking portion called the boundary context, and an inward-looking portion called the boundary concept that captures the controlling system values, rule sets, and structural view. As depicted in Figure 1, a specific system is composed of system functions, requirements, architecture and tests (Simpson, 2004).

System functions are the actions or activities that the system is designed to perform. System requirements describe how well the system must do its required functions. In combination, the system functions and the system requirements create the system problem statement. This fact further defines the system concept. The system architecture is the mechanism that performs the system functions as well as stated by the system requirements. Successful system tests indicate that the system architecture performs the functions as well as the requirements stipulate. This Ge-