IDEA GROUP PUBLISHING
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

ITB12229

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

Chapter VII

Security Management for an E-Enterprise

Ammar Masood, Purdue University, USA

Sahra Sedigh-Ali, University of Missouri-Rolla, USA

Arif Ghafoor, Purdue University, USA

Abstract

Enterprise integration is the key enabler for transforming the collaboration among people, organization, and technology into an enterprise. Its most important objective is the transformation of a legacy operation into an e-enterprise. In an e-enterprise, the tight coupling between business process and the underlying information technology infrastructure amplifies the effect of hardware and software security failures. This accentuates the need for comprehensive security management of the infrastructure. In this chapter, the challenges posed by fulfilling myriad security requirements throughout the various stages of enterprise integration have been outlined. To better categorize these requirements, the set of security domains that comprise the security profile of the e-enterprise have been specified. The set of security metrics used to quantify various aspects of security for an e-enterprise are also identified. The chapter concludes by describing the details of the proposed security management strategy.

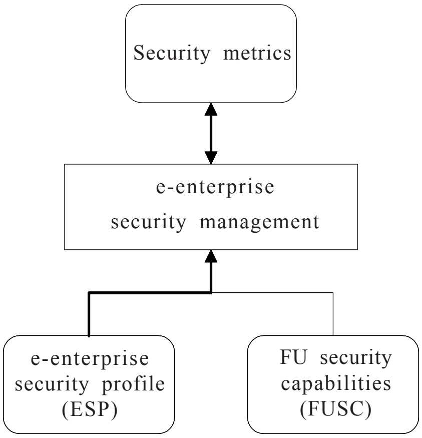
Introduction

Enterprise integration (EI) is the integration of people, organization, and technology in an enterprise (Fox & Gruninger, 1998). One of the objectives of EI is transforming a legacy operation into an e-enterprise, which is defined as an enterprise where business practices are tightly coupled with the underlying *information technology* (IT) infrastructure (Hoque, 2000). This coupling heightens the effect of hardware and software security failures and underscores the need for comprehensive security management of the infrastructure, including configuration management, user activity monitoring, patch management, and integration of security mechanisms (I3p, 2003).

In this chapter, the focus is on the integration problem; namely, how to integrate the diverse security mechanisms and requirements implemented at various levels of the infrastructure into a coherent framework for supporting enterprise security (I3p, 2003). The challenges posed by fulfilling myriad security requirements throughout the various stages of enterprise integration are outlined. To better categorize these requirements, the set of security domains that comprise the security profile of the e-enterprise are specified. The security policy of the e-enterprise is in turn used to determine the requirements for each functional unit.

After determining the security requirements for the identified domains, descriptions are provided for security management techniques used to ensure that these requirements are met. These techniques rely heavily on the use of software metrics, which are used to provide qualitative assessments or quantitative measurements, or both, for the software infrastructure (Fenton, 1991). Metrics provide an integral link from detailed plans at the lowest level of implementation to the highest levels of planning. Security metrics are useful in expressing the cost, benefit, and impact of security controls with respect to economic, technical, and risk perspectives (I3p, 2003). They are useful in guiding both product selection and secure composition (I3p, 2003). In providing security to an e-enterprise, metrics are used to extract information from the operational model of the

Figure 1. E-enterprise security management


Security metrics
e-enterprise security management
e-enterprise security profile (ESP)
FU security capabilities (FUSC)