Chapter 3.6
A Stochastic Model for Improving Information Security in Supply Chain Systems

Ibrahim Al Kattan
American University of Sharjah, UAE

Ahmed Al Nunu
American University of Sharjah, UAE

Kassem Saleh
Kuwait University, Kuwait

ABSTRACT

This article presents a probabilistic security model for supply chain management systems (SCM) in which the basic goals of security (including confidentiality, integrity, availability and accountability, CIAA) are modeled and analyzed. Consequently, the weak points in system security are identified. A stochastic model using measurable values to describe the information system security of a SCM is introduced. Information security is a crucial and integral part of the network of supply chains. Each chain or driver requires a different security level according to the services it contributes to the overall SCM system. Different probabilistic weights are assigned to the four goals CIAA of security depending on the SCM driver's mission. A Semi-Markov chain model is used to describe the probabilistic nature of different security levels for each driver in the system. A comparison of the steady-state security for a multi-driver model with different levels of attack is performed, and the results analyzed. Enhanced supply chain security could be achieved by identifying the effects of attacks on the security goals of an organization. The use of this model helps to identify weak points in supply chain system security, and offers hints on how to strengthen them. The model is tested by considering intrusion scenarios representing different levels of attack on the SCM system. An analysis of the results is performed using an interactive application.

INTRODUCTION

At the present time, leaders of business and industry frequently use the acronyms of globalization, security of information technology, and supply chain management (SCM). These terms have together grown to become powerful tools for business and industry expansion. Toyota, Dell, and Wal-Mart were among the first companies to succeed in the implementation of SCM tools in their specialized industries. These tools have developed over the last two decades as a result of competitor growth and mutual international interests; which has led to the development of a variety of products. Product variety (enhanced by IT) has pressured international business to reduce the restrictions placed on global trade. Consequently, accurate information technology is a crucial part of proper integration to all parties involved in globalization and has enhanced the success of international business. Growing competition has forced companies to generate high quality, lower cost products, and maintain quick responsiveness in the delivery of products and services (Chopra & Meindl, 2004). Figure 1 shows the integration process of supply chain and globalization, as developed by the authors.

The supply chain is a complex network of facilities dispersed over a large geographical area may be across the globe. The supply chain system is a dynamic system that evolves over time due to changes in customer demand. The key issues in SCM system are a wide spectrum of corporate activities from strategic to tactical and operational levels. IT and its security are essential for the integration of the chain of SCM and securing the success. Today, business growth is enhanced by rapid development of information concerning internet-based technologies and services. Information available on the internet has provided organizations with new and creative ways to improve business processes, drive revenue growth, reduce costs and improve customer satisfaction; and consequently, facilitates the implementation of SCM systems. The evolving information systems require that the information resources need to be shared securely among customers, employees, business partners and financial institutions. With this, however, come serious security threats (Al Nunu, 2006).

Undoubtedly, as globalization increases, competing in today's international marketplace has become challenging. In order to survive, organizations must tighten the supervision placed on information security in supply chain system. While many realize the vulnerability of supply chain visibility, many companies are still unaware of the right approach in information security implementation. However, information security of complex systems, such as supply chain management, is essential and covers a wide range of an organization's function. The main challenges in securing of an integrated system such as supply chain management are information integration and the lack of standardization (Chopra & Meindl, 2004). The IT security problem becomes crucial due to attacker accessibility of more than one chain or driver of a supply chain system. The main objective of security in any SCM system is based on the following premises: accountability, security assurance and continuity. Accountability within a system ensures that security violations can be traced back to the violators. Security assurance provides a desirable level of confidence that the confidentiality, integrity and availability requirements of a system are met. The last point, continuity assures that a life cycle approach to security engineering presents a level of confidence that accountability and assurance is continuously maintained throughout the system lifetime (Pfleeger & Pfleeger, 2004).

The flow of information and the transportation of goods are the main bridges to link and integrate all chains or drivers. The performance of information security could also be achieved through interaction and facilitation of information between suppliers and customers (Chopra & Meindl, 2004). Various types of information are needed – information on customer wants the

Related Content

An Associative Classification-Based Recommendation System for Personalization in B2C E-Commerce Applications

Y. Zhang (2007). *Mass Customization Information Systems in Business (pp. 107-121).*

www.irma-international.org/chapter/associative-classification-based-recommendation-system/26121

Technology Institutionalisation through Technological, Organisational, and Environmental Isomorphism

Azadeh Pishdadand Abrar Haider (2015). *Business Technologies in Contemporary Organizations: Adoption, Assimilation, and Institutionalization (pp. 54-74).*

www.irma-international.org/chapter/technology-institutionalisation-through-technological-organisational-and-environmental-isomorphism/120751

The e-ERP Transformation Matrix

Colin G. Ashand Janice M. Burn (2005). *Managing Business with SAP: Planning Implementation and Evaluation (pp. 158-178).*

www.irma-international.org/chapter/erp-transformation-matrix/25723

Software Maintenance of Process Modeling Line Model

Zeljka Car (2005). *Managing Corporate Information Systems Evolution and Maintenance (pp. 272-294).*

www.irma-international.org/chapter/software-maintenance-process-modeling-line/25753

The Interplay between Practitioners and Technological Experts in the Design Process of an Archaeology Information System

Tommaso Federiciand Alessio Maria Braccini (2013). *Cases on Performance Measurement and Productivity Improvement: Technology Integration and Maturity (pp. 449-473).*

www.irma-international.org/chapter/interplay-between-practitioners-technological-experts/69123