Analysis of Information Security in Supply Chain Management Systems

Ibrahim Al Kattan, Ahmed Al Nunu, & Kassem Saleh
Engineering Systems Management, American University of Sharjah, ilkattan@aus.edu

ABSTRACT
This paper presents a quantitative information security model using measurable values to describe the security of information systems in supply chain management (SCM) systems. There are four main drivers in a SCM system: 1) suppliers, 2) manufacturers and inventories, 3) distributors and retailers, and 4) the customers. The security of supply chain management concerns the security of various interactions among these drivers. Each driver requires a different security level relevant to the services it contributes to the overall SCM system. A transition matrix representing the semi-Markov chain model of each driver is developed. Then, a system-wide security for SCM is produced using the transition matrices of each driver to reach a steady state of SCM information security. The model includes nine different levels of attacks presenting several scenarios for an intruder. Comparison of the steady-state security for multi driver model with different levels of attacks is presented. An analysis of the results is then presented and discussed.

1. INTRODUCTION
Information security management has become an integral part of supply chain management. The importance of security is more evident as the value of system assets is protected increases. The supply chain management drivers often face the challenge of integrating security into their systems development from suppliers to customers. The main goals of security are: Confidentiality; Integrity; Availability and Accountability (CIAA). The security involves three system elements: software; hardware; and information. The main focus of this research is on the performance analysis of information security (PAIS) through supply chain management (SCM) drivers. The security functions should be integrated and well communicated through all supply chain drivers with regular test warnings and feedback for recovery from any attack. This research will focus on the development of a quantitative model to provide a measurable description of security. In addition, we will analyze and compare the security among the supply chain drivers for different levels of attacks. A semi-Markov chain model will be developed to present several scenarios with different levels of attacks [1].

Improving the performance of information among the supply chain drivers has a valuable effect on customer satisfaction. But due to the existence of competitors, hackers, and intruders information should be secured at the supply chain parties while being shared. The process starts with an order of raw materials and/or semi finished parts from the supplier. Then they are used for the manufacturing or assembling processes, transported to the distributor, then to the retailer, and to the final users-the customers. Usually, the supply chain parties could come from different countries, or regions, with different levels of technologies and levels of securities. In fact, most supply chain management systems are global in nature. For these reasons, sharing information among them will be truly vulnerable to the individual party and to the supply chain security [3, 4]. One example is e-commerce: customer has to insert a credit card number, address, and other information which should be secured during transaction processing. Figure 1 shows the flow of information, the goal of security, and the physical flow of parts through the SCM drivers.

2. LITERATURE REVIEW
The overall performance of information security of SCM system could be improved drastically by adopting suitable security standards. Security standards could be used to develop measurable values for CIA and to assess these values when collected. These values can be used for building a quantitative model for security. Jonsson et al [3] are the pioneers in using a quantitative analysis approach of attacker behavior based on empirical data collected from intrusion experiments. They divided the attacker’s behavior into three different phases: the learning phase, the standard attack phase, and the innovation phase. The probability for successful attacks is shown to be considerably higher in the standard attack phase. Lambrinoudakis et al [5] presented a probabilistic structure, in the form of a Markov model. The model provides detailed information about all possible transitions of the system in the course of time. Lambrinoudakis, stated that the probabilistic structure enables both the estimation of the insurance premium and the evaluation of the security investment. Madan et al [6] initiated security attributes for intrusion by applying a quantitative model. The model is run for steady-state behavior leading to measures like mean time to security failure (MTSF). Madan, used the steady-state to find the probabilities for confidentiality, integrity, availability and the value of absorbing states representing the MTSF. Ortalo et al [7] introduced a stochastic model by using Markov chain to obtain a steady state. The model allows obtaining the mean time to security failure by evaluating the proposed measure of operating security. Trivedi [8] considers that the attacker could arrive at a random time, just as a failure may occur randomly. Also, he used a Markov process to estimate the amount of time or effort that an attacker has to spend in injecting an attack. This could be modeled as a random variable that can be described by choosing Poisson distribution functions. Wang, C. et al [9] developed a quantitative security model by using a semi-Markov model for an intrusion tolerant system.

3. SECURITY MODEL
An attacker’s behavior is unpredictable and random in nature which represents a stochastic process. The security model developed in this research is based on stochastic processes. A stochastic process is an evolution model where the systems are either exhibiting inherent randomness, or operating in an unpredictable environment. This unpredictable behavior of attackers might be in more than one form. The semi-Markov chain process is considered to be an appropriate...
emerging trends and challenges in IT management

4. PERFORMANCE ANALYSIS

The security of supply chain management is a state-wide application which concerns a variety of decisions about the interactions and security of several drivers. The steady state probabilities of supply chain management could be developed by generating an individual Markov chain for each driver. The proposed values of \( p_r, p_f, p_s, p_{acc} \) for each driver (depending on its mission) is shown in Table 1. However, the reader can use this model for many drivers and use corresponding CIAA data. Next step to develop a generic transition matrix GTM for each driver (i) created by substituting the parameters of \( p_c, p_r, p_f, p_{acc} \) from Table 1. The model proposed nine different levels of attacks to present these scenarios of attacks. These levels of attacks are (15%, very low; 25% low, 35% - 45% more or less low, 50%, medium, 55% - 65%, more or less medium, 75%, high 85% very high ) are tested to present different security responses. So, repeating the same process on the GTM for each attack level, we obtain nine steady state matrices.

The following steps are used to develop the study state security for SCM drivers:

1. Develop 4 matrices of GTM for each driver.
2. Use GTM for each driver at nine attack levels (36 GTM).
3. Solve for the steady state matrix (SSM) for individual drivers.
4. Find the system wide SW security by multiply each driver GTM to get the SW transition Matrix.
5. Run the SW transition matrix to get the study state for the SCM system as a security unit.

The steady states of SCM for system wide can be achieved by multiplying the matrices of all drivers as presented in Table 2. The steady states probability for system wide and CIAA could be found using the following relationships:

\[
\pi_x = \pi_0 + \pi_s; \quad \text{and} \quad \pi_{-x} = 1 - \pi_x; \quad \pi_x = 1 - \pi_x; \quad \pi_{acc} = 1 - \pi_s
\]

The state wide system security for SCM has less vulnerability leading to better security due to the sharing of information about attacks. Once an attack on a Driver occurs, the information about this attack could be shared among the remaining drivers.

Therefore, an individual driver is more vulnerable than a SCM. Figure 4 illustrates 5 curves one represents SW for a SCM as an integral system and the other 4 curves represent 4 drivers as individual security unit. In Figure 4, the curve for system wide (SW) security shows improvements for all levels of attack (15% - 85%). Curves D1, D2, D3 and D4 are representing the security for Driver1, Driver2, Driver3, and Driver4, respectively. These curves show a much lower security level than the overall SCM security. On the other hand, when each driver represents individual business where their security information are not shared, each of them will be more vulnerable to an attack as shown in Figure 4.

5. CONCLUSIONS AND REMARKS

This research developed a quantitative model using measurable values to describe the information system security of four drivers in statewide application of SCM. A semi-Markov chain model was used to describe different security levels. This model is used to present several scenarios with different levels of attacks. The model has been tested for SCM with

four drivers where each driver provides different services within SCM. The model runs for steady-state using MATLAB for all combinations. The analysis of the model and graphical representation show that the SCM sharing security and information has been improved at all level of attacks. Individual driver exposed to higher risk of attack which could lead to a higher vulnerability of the SCM, if the information about its own vulnerability and risk level are not shared with other drivers. In the future, we would like to generalize our quantitative model to analyze the security of multi-agent based systems and then apply it to electronic commerce systems. Moreover, we would like to carefully study the problem of assigning probabilities for different security goals and drivers, and the correlation between the elements of the CIAA security model.

6. REFERENCES


Related Content

Assessing Computational Thinking
[www.irma-international.org/chapter/assessing-computational-thinking/112561](www.irma-international.org/chapter/assessing-computational-thinking/112561)

The Use of Smart Card Technology in Health Care
[www.irma-international.org/chapter/the-use-of-smart-card-technology-in-health-care/112776](www.irma-international.org/chapter/the-use-of-smart-card-technology-in-health-care/112776)

Multimodality Medical Image Fusion using M-Band Wavelet and Daubechies Complex Wavelet Transform for Radiation Therapy

I-Rough Topological Spaces
[www.irma-international.org/article/i-rough-topological-spaces/144708](www.irma-international.org/article/i-rough-topological-spaces/144708)

Metadata Crosswalks as a Way Towards Interoperability
[www.irma-international.org/chapter/metadata-crosswalks-as-a-way-towards-interoperability/112589](www.irma-international.org/chapter/metadata-crosswalks-as-a-way-towards-interoperability/112589)