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
ITB12742

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Analysis of Information Security in Supply Chain Management Systems

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

ABSTRACT

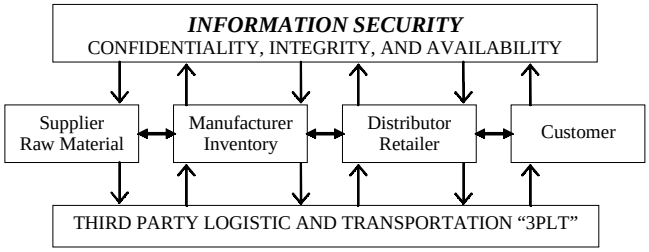
This paper presents a quantitative information security model using measurable values to describe the security of information systems in supply chain management (SCM) systems, [1]. There are four main drivers in a SCM system: 1) suppliers, 2) manufacturers and inventories, 3) distributors and retailers, and 4) the customers [2]. 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 to protect 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: the 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.

Figure 1. Flow of information and the physical parts through the SCM drivers



2. LITERATURE REVIEW

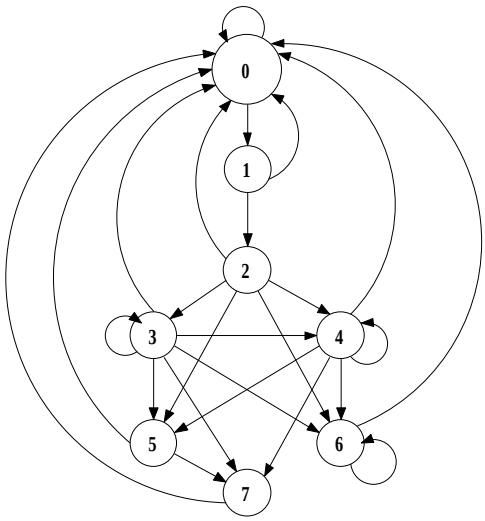
The overall performance of information security of SCM system could be improved drastically by adopting suitable security standards. Security standards could be used to develop measurable values for CIA and to assess these values when collected. These values can de used for building a quantitative model 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

Figure 2. Security state diagram of a Driver under attack



modeling tool to illustrate the behavior of attackers. Markov chains have a special property that, the probability of any event moving to future state depends only on the present state; hence it is independent of past events. Attacker's process fits well this description, so Markov chains provide an important kind of probabilistic model for attackers. The structure of a generic model for the security of any driver in the SCM is shown Figure 2 [6]. The eight states of the security system and their links (probabilities) are indicated in Figure 3. From all the states, the system can return back to state 0, the normal state, with different level of probabilities and with different degrees of losses. Below, is a general transition matrix (GTM) formulation of the relation among the states and their probability.

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_C, p_I, p_A, 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_I, p_A, p_{Acc} from Table 1. The model proposed nine different levels of attacks to present

Figure 3. Generic Transition Matrices (GTM)

$$P = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{array} \begin{array}{c} \begin{array}{cccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \bar{p}_1 & 0 & p_{12} & 0 & 0 & 0 & 0 & 0 \\ \bar{p}_2 & 0 & 0 & p_{23} & p_{24} & p_{25} & p_{26} & 0 \\ \bar{p}_3 & 0 & 0 & p_{33} & p_{34} & p_{35} & p_{36} & p_{37} \\ \bar{p}_4 & 0 & 0 & 0 & p_{44} & p_{45} & p_{46} & p_{47} \\ \bar{p}_5 & 0 & 0 & 0 & 0 & 0 & 0 & p_{57} \\ \bar{p}_6 & 0 & 0 & 0 & 0 & 0 & p_{66} & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

, where,

$$p_{12} + \bar{p}_1 = 1$$
$$p_{23} + p_{24} + p_{25} + p_{26} + \bar{p}_2 = 1$$
$$p_{33} + p_{34} + p_{35} + p_{36} + p_{37} + \bar{p}_3 = 1$$
$$p_{44} + p_{45} + p_{46} + p_{47} + \bar{p}_4 = 1$$
$$p_{57} + \bar{p}_5 = 1$$
$$p_{66} + \bar{p}_6 = 1$$

Table 1. Proposed CIAA for SCM

Multi driver	p_C	p_I	p_A	p_{Acc}	p_{CIAA}
Driver1	0.25	0.25	0.05	0.05	0.60
Driver2	0.10	0.40	0.05	0.05	0.60
Driver3	0.05	0.05	0.40	0.10	0.60
Driver4	0.40	0.05	0.05	0.10	0.60

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:

$$\pi_S = \pi_0 + \pi_1; \text{ and } \pi_C = 1 - \pi_3; \ \pi_I = 1 - \pi_4; \ \pi_A = 1 - (\pi_5 + \pi_7); \ \pi_{Acc} = 1 - \pi_6$$

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.

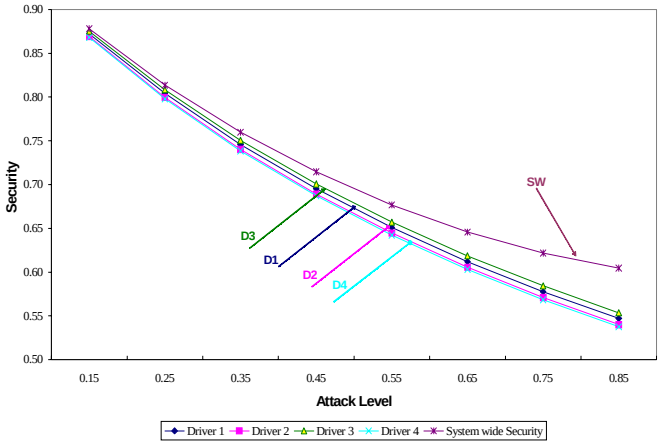
5. CONCLUSIONS AND REMARKS

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

Table 2. System wide security for SCM when it reaches a steady state

Attacker level	Normal π_0	V π_1	Att π_2	C π_3	I π_4	A π_5	Acc π_6	F π_7	Security π_8
0.15	0.5529	0.3302	0.0783	0.0219	0.0031	0.0031	0.0075	0.0032	0.8831
0.25	0.5203	0.3029	0.1172	0.0337	0.0047	0.0047	0.0115	0.0049	0.8232
0.35	0.4946	0.2800	0.1477	0.0439	0.0062	0.0062	0.0151	0.0065	0.7746
0.45	0.4747	0.2610	0.1709	0.0527	0.0074	0.0074	0.0181	0.0079	0.7357
0.50	0.4668	0.2528	0.1800	0.0565	0.0079	0.0079	0.0195	0.0085	0.7196
0.55	0.4602	0.2454	0.1874	0.0601	0.0085	0.0085	0.0208	0.0092	0.7056
0.65	0.4510	0.2332	0.1973	0.0663	0.0094	0.0094	0.0232	0.0104	0.6842
0.75	0.4473	0.2247	0.2003	0.0709	0.0101	0.0101	0.0251	0.0117	0.6720
0.85	0.4498	0.2207	0.1955	0.0733	0.0105	0.0105	0.0266	0.0131	0.6705

Figure 4. Comparing SCM versus individual driver



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

[1] AL Nunu, A. M., "Information Security in Supply Chain Management – A Quantitative Approach", MS Thesis in Engineering Systems Management, American University of Sharjah, UAE, 2005.

[2] Sunil Chopra and Peter Meindl, Supply Chain Management, 2nd ed Prentice Hall, 2004.

[3] E. Jonsson and T. Olovsson, "A Quantitative Model of the security Intrusion process Based on Attacker Behavior," IEEE Transaction on Software Engineering, vol. 23, no. 4, pp. 235-245, 1997.

[4] Konstantin Knorr and Susanne Rohrig, "Security requirements of e-business processes," in Proceedings of the First IFIP Conference on E-Commerce, E-Business, and E-Government (I3E) 2001, pp. 73-86.

[5] Costas Lambrinoudakis, Stefanos Gritzalis, and Petros Hatzopoulos, "A formal model for pricing information systems insurance contracts," Computer Standards & Interfaces, vol. 27, pp. 521-532, 2005.

[6] Baharat B. Madan, Katerina Goseva-Popstojanova, Kalyanaraman Vaidyanathan, and Kishor S.Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems," Performance Evaluation, vol. 56, pp. 167-186, 2004.

[7] R. Ortalo and et al., "Experiments with quantitative evaluation tools for monitoring operational security," IEEE Transaction on Software Engineering, vol. 25, no. 5, pp. 633-650, 1999.

[8] K. S. Trivedi, Probability and Statistics with Reliability, Queuing, and Computer Science Applications, 2nd ed. New York: Wiley, 2001.

[9] Chenxi Wang and William A. Wulf, "Towards A framework for security measurement," Logistics Information Management, vol. 15, no. 5/6, pp. 414-422, 2002.