Advances in Management & Applied Economics, vol.2, no.3, 2012, 1-12
ISSN: 1792-7544 (print version), 1792-7552 (online)
Scienpress Ltd, 2012

An Optimization Approach In Information Security Risk Management

Marn-ling Shing[1], Chen-chi Shing[2], Lee-pin Shing[3] and Lee-hur Shing[4]

Abstract

In order to protect enterprise networks from unauthorized access and malicious attacks, a few risk models were proposed. This paper proposes to use optimization approach for a business to make decision based on certain budget constraint within a certain years.

JEL classification numbers: G32

Keywords: risk assessment; risk management; information security model; risk model

[1] Early Child Education Department and Institute of Child Development, Taipei Municipal University of Education, 1 Ai-Kuo West Road, Taipei, Taiwan, R.O.C., e-mail: shing@tmue.edu.tw

[2] Information Technology Department, Radford University, Box 6933, Radford, VA 24142, e-mail: cshing@radford.edu

[3] Virginia Tech, Blacksburg, VA, e-mail: shingle@vt.edu

[4] Virginia Tech, Blacksburg, VA, e-mail: leehurshing@yahoo.com

Article Info: *Received* : February 5, 2012. *Revised* : April 3, 2012
Published online : August 31, 2012

1 Introduction

Today most enterprise networks are web-based systems or connected to Internet. It makes the enterprise networks more vulnerable to unauthorized access, malicious attacks, or denial of services. One of the shocking cases is the TJX security breach in 2006 [9]. The TJX , the retail giant, eventually has to settle with most banks and banking associations for 40.9 millions. For business owner and enterprise managers, these kinds of events cannot be completely stopped. By looking back the records of last twenty, we can find the enterprise systems of some high-profile companies such as Yahoo and eBay have been compromised. However, the damage to companies operations and finance cannot be ignored. Business today treated security attacks or breaches as an accident similar to a nature disaster. Traditional defense mechanism includes firewalls, intrusion detection system (IDS), and anti-virus programs. Firewalls could be a hardware devise or a software program.

Most firewalls use packet filtering techniques to inspect the incoming packets and decide to accept or reject the incoming packet. The network systems also use authentication and cryptographic techniques to control the access. Anti-virus programs check the potential malicious viruses or worms but they are based on the known virus attacks. Cryptographic techniques include encryption, digital signature, and digital certificates. IDS uses different algorithms to filter possible suspicious attacks but sometimes it may be a false alarm. Similar to the algorithms of IDS, the paper strives to develop an approach to predict the behavior of the systems. If the suspicious behaviors are discovered, the systems will send a warning signal to the network administrators. The administrator will decide the appropriate actions to avoid possible false alarm. On December 2006, TJX company detected a “suspicious software” on its computer system and later it was confirmed an intrusion and data loss. TJX did not discover the suspicious behavior until several months later [9].

Taking risk is an everyday’s action in business. Before making decision, the executive must perform a risk analysis to reach to the optimal decision. In information security area the risk assessment or risk analysis is defined as “analysis of the potential threats against an asset and the likelihood that they will materialize.” [4]

Probabilistic risk assessment (PRA) (or probabilistic safety assessment/ analysis) is a systematic and comprehensive methodology to evaluate risks associated with a complex engineered technological entity. Risk in a PRA is defined as a feasible detrimental outcome of an activity or action. In a PRA, risk is characterized by two quantities:

1. the magnitude (severity) of the possible adverse consequence(s), and
2. the likelihood (probability) of occurrence of each consequence.

Consequences are expressed numerically (e.g., the number of people potentially hurt or killed) and their likelihoods of occurrence are expressed as probabilities or frequencies (i.e., the number of occurrences or the probability of occurrence per unit time). The total risk is the expected loss: the sum of the products of the consequences multiplied by their probabilities.” [10].

Risk analysis starts with understanding what assets are potentially at risk, and indentify what the possible threats are, and find out what are the possible vulnerabilities that could be exploited. The risk assessment can provide a way to protect the assets based on limited resources. Even though a risk assessment has been done and action has been taken to protect the assists, the risk assessment has to be updated due to environment change such as hardware, software or personnel changes. Therefore, risk assessment must be monitored all the time. However, there exists no good tool to monitor those changes for all possible changes. A semi-Markov chain allows any distribution on state changes and it is very powerful to be used to monitor state changes dynamically with time changes. This paper emphasizes on how the likelihood of the risk propagates throughout the time and how to monitor the risk based on semi-Markov chain models.

In the next few sections we will first introduce Markov chain models and their properties. And a simulation was used to study the risk propagation through time. Finally, a statistical hypothesis testing was use to validate the model.

2 Semi-Markov Chain Model

We can use a probability model (such as Markov chain) to predict the possible security condition of the enterprise systems. A Markov chain is a stochastic process in which the probability of a system state depends only on the previous state, not on the previous history of getting to the previous state. If the states and their transitions at discrete points in time are discrete, it is called a Markov chain [3]. In other words, a stochastic process M(t) is a Markov chain if at any n time points $t_1 < t_2 < \ldots < t_n$, there are n corresponding states $m_1, m_2, \ldots, m_n$, the probability that the system is at state m_n at time t_n, given that the system was at state m_{n-1} at time t_{n-1} etc and the system was at state m_1 at time t_1 is equal to the probability that the system is at state m_n at time t_n, given that the system was at state m_{n-1} at time t_{n-1}.

That is, $P(M(t_n)=m_n \mid M(t_{n-1})=m_{n-1}, \ldots, M(t_1)=m_1)= P(M(t_n)=m_n|M(t_{n-1})=m_{n-1})$, where m_i is the state of the process at time t_i $(t_1 \leq t_i \leq t_n)$, i=1, …, n. Thus, the probability that the Markov chain is in state m_n at t_n, depends only on the previous state m_{n-1} at t_{n-1} [1].

Suppose p(0) represents the column vector of the probability that the system is in one of those n states at time 0,

$$\mathrm{p(0)}=\begin{bmatrix} p_1(0) \\ p_2(0) \\ \cdots \\ p_n(0) \end{bmatrix}, \qquad \sum_{i=1}^{n} p_i(0)=1,$$

where $p_i(0)$ represents the probability of the system is in state i at time 0.Then the probability that the system is in one of those n states at time 1 is represented by p(1),

$$\mathrm{p(1)}=\begin{bmatrix} p_1(1) \\ p_2(1) \\ \cdots \\ p_n(1) \end{bmatrix}, \qquad \sum_{i=1}^{n} p_i(1)=1,$$

where $p_i(1)$ represents the probability of the system is in state i at time 1. And p(1)=T' p(0), where T' is the transpose matrix of the transition probability matrix,

$$\mathrm{T'}=\begin{bmatrix} p_{11} & p_{21} & \ldots & p_{n1} \\ p_{12} & p_{22} & \ldots & p_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ p_{1n} & p_{2n} & \ldots & p_{nn} \end{bmatrix}, \quad \sum_{j=1}^{n} p_{ij}=1, \text{ for i =1,2,…,n} \qquad (1)$$

and p_{ij} is the probability of the system in the state j, give it was in the state i. Suppose the probability that the system is in one of those n states at time s is represented by p(s),

$$\mathrm{p(s)}=\begin{bmatrix} p_1(s) \\ p_2(s) \\ \cdots \\ p_n(s) \end{bmatrix}$$

where $p_i(s)$ represents the probability of the system is in state i at time s. Then

$$\mathrm{p(s)=T'(T'(\ldots(T'p(0))))=T'^{s}\ p(0)},$$

where T is the transition probability matrix, That is, $p'(0)= p'(s)\ T^{s}$.

For example, suppose that there are two possible threats to a company's network system. The first one is the intruder through wire network and the second is the intruder through wireless network. If we represent each state as a threat, then there are two states in a state vector. Suppose that in the first year there are 80% of intruders through the wire network and the rest through the wireless network, the security of a company's network system on year 1, the initial state, can be represented by a transpose vector $p^{'}(1)$ of p(1):

$$p'(1) \ =\begin{bmatrix} 0.8 & 0.2 \end{bmatrix}$$

Suppose that if the company was intruded through wire network, there will have 60% of chance that intruder through wire attack in next year even though some patches were done. In the mean time there will have 40% of chance that wireless attack may happen in the next year. On the other hand if the company was intruded through wireless network, there will have 90% of chance that intruder through wire attack in next year even though some patches were done. And there will have 10% of chance that wireless attack may still happen in the next year. That is, the probability transition matrix *T* is

$$T = \begin{bmatrix} 0.6 & 0.4 \\ 0.9 & 0.1 \end{bmatrix} \tag{2}$$

The security on the year 2 can be predicted by:

$$p'(2) = p'(1)T = \begin{bmatrix} 0.8 & 0.2 \end{bmatrix} \begin{bmatrix} 0.6 & 0.4 \\ 0.9 & 0.1 \end{bmatrix} = \begin{bmatrix} 0.66 & 0.34 \end{bmatrix}$$

Thus, there is an 66% chance that intruding through wire in year 2 and 34% chance that intruding through wireless network. The state vector in year 3 can be predicted in the same way:

$$p'(3) = p'(1)\ T^2 = \begin{bmatrix} 0.8 & 0.2 \end{bmatrix} \begin{bmatrix} 0.6 & 0.4 \\ 0.9 & 0.1 \end{bmatrix}^2 = \begin{bmatrix} 0.70 & 0.30 \end{bmatrix}$$

General rules for period n are [1]:

$$p'(n) = p'(n-1)T$$

$$p'(n) = p'(1)T^n$$

In general, p_{ij} in each row of the matrix T' could be from any probability distribution. In fact, a semi-Markov chain can be defined as a stochastic process that can have an arbitrary distribution between state changes [6]. A variety of different distributions will be used in the simulation experiment.

Definition 2.1

A semi-Markov process is a stochastic process that has an arbitrary distribution between state changes given it is in the current state.

In the next section, we will describe how to design pre and post test assessment instruments to collect the necessary data for analysis and show all the pre-test questions used in this study.

3 Properties

In this section we will investigate when a stochastic system will reach to a steady state (or equilibrium state) in the long run. We first introduce the meaning of each state to be a recurrent non-null and aperiodic.

Definition. 3.1 *A state is recurrent if a state will return back to itself with the probability one after state transitions. If the state is not recurrent, then it is a transient. If a recurrent state is called recurrent nonnull if the mean time to return to itself is finite. A recurrent state is a recurrent null if the mean time return to itself is infinite. A recurrent state is aperiodic if for some number k, there is a way to return back in k, k+1, k+2, … transitions. A recurrent state is called periodic if it is not aperiodic.*

Definition 3.2 *A semi-Markov chain is irreducible if all states are reachable from all other states. It is recurrent nonnull if all its states are recurrent nonnull. It is aperiodic if all its states are aperiodic.*

Definition 3.3 *If a semi-Markov chain is called ergodic, then it is irreducible, recurrent nonnull and aperiodic.*

Property 3.1 *If a semi-Markov chain is ergodic, then there exists a unique steady-state or equilibrium probability state.*

Depending on the structure of the transition probability matrix, it may not have any steady state exists. For example, a symmetric random walk process which has p=0.5, is periodic [5].

Property 3.2 *For any semi-Markov chain, if all the entries of its transition probability matrix are non-zero, then it is recurrent nonnull and aperiodic.*
Proof: Since all the entries of its transition probability matrix are non-zero (and also positive), every entry of the n^{th} power of its transition probability matrix are also non-zero. Additionally, any state can go to any other state in any step. Therefore, a state will return back to its state after time n with probability one and it is recurrent. The mean return time is finite and it is recurrent nonnull. If it can return back in k steps, then it can also return back in one more step and it is aperiodic.

Corollary 3.1 *For any semi-Markov chain, if every entry of its transition probability matrix has non-zero in all the entries, then it has an equilibrium state.*
Proof: Since every entry of its transition probability matrix has non-zero, every entry of positive integer power of the transition probability matrix has non-zero in all the entries, and all states are reachable from all other states after n steps and the semi-Markov chain is irreducible. By Eq. 2.1 the semi-Markov chain is also recurrent nonnull and aperiodic. Therefore, it is ergodic and by Eq. 2.1 there exists a unique steady-state.

Corollary 3.2 *The equilibrium state described in Corollary 3.1 is the eigenvector of T', the transpose of the transition probability matrix, of eigenvalues 1.*
Proof: The steady-state p(n) satisfies

p(n)=T’p(n) or (T’-I) p(n)=0, where I is the identity matrix and 0 is a zero-column vector. That is, p(n) is the eigenvector of eigenvalues 1.

Example 3.1 In the matrix T of (2),

$$T' = \begin{bmatrix} 0.6 & 0.9 \\ 0.4 & 0.1 \end{bmatrix}$$

$$T' - I = \begin{bmatrix} -0.4 & 0.9 \\ 0.4 & -0.9 \end{bmatrix}$$

The steady state $\begin{bmatrix} r & s \end{bmatrix}'$, where $r + s = 1$, satisfies

$$\begin{bmatrix} r & s \end{bmatrix} \text{(T-I)} = \begin{bmatrix} 0 & 0 \end{bmatrix}.$$

That is, $0.4r - 0.9s = 0$ and $r + s = 1$ imply $r = 9/13$ and $s = 4/13$. Hence, the steady state is

$$\begin{bmatrix} 9/13 & 4/14 \end{bmatrix}' .$$

In the next section, we will develop a risk model that meets certain criteria.

4 Optimization Model

Suppose that within n years there are s possible threats exist and some chances of damages for a company. The company wants to choose the beast policy that meets its budget. We may model those threats as one of the states in a state vector in a semi-Markov chain model.

That is, the state row vector at time i, q’= [q_{1i}, q_{2i}, …, q_{si}]’ represents those concerned threats combined with different probability. And assuming security installation has total investment value V_{ji} for threat j at time i. Let D_{ji} be the damage cost created by threat j at certain time i. Then the cost at time I, C_i can be represented by

$$\mathrm{C_i} = \sum_{j=1}^{s} (D_{ji} q_{ji} + V_{ji}) \tag{3}$$

Suppose we observe those costs in total time n, the total cost T_n must be within a given budget B, i.e., maximize n such that $T_n < B$, where

$$\mathrm{T_n} = \sum_{i=1}^{n} Ci \tag{4}$$

Note that the steady state vector q satisfies not only (1) but also by Corollary 3.2,

$$\text{(T'-I) q} = 0 \tag{5}$$

If there is no risk knowledge to know which transition probability matrix appears in each year, we may use expected total cost to estimate yearly cost for m years costs and still meet the budget. That is, maximize n such that n* $E(T_n) < B$.

For example, we will consider security policies in three years. Suppose that we choose the policy A in the example that was used in the above section if the total security budget for the company is B= 26k. And assume that in the year 1 the damage for intruder through wire network is \$13K and \$1K if through wireless network. That is, D_{11} =13000 and D_{21} =1000. q_{11} =9/13 and q_{21} = 4/13 Furthermore, suppose that the investment for fixing the damage caused by the wire intruder is \$2K and for the wireless intruder is \$4K, that is, V_{11} =2000 and V_{21} = 4000. Therefore, C_1 = (9+2)+(4/13+4)K= \$15307.

Suppose that in the year 2, we choose a different policy B that have

$$T' = \begin{bmatrix} 0.9 & 0.5 \\ 0.1 & 0.5 \end{bmatrix}$$

Then the steady state in the year 2 is [q_{12} = 5/6 q_{22} = 1/6]. If the damage for intruder through wire network is \$8K and it is \$4K if through wireless network. That is, D_{12} =8000 and D_{22} =4000. Furthermore, suppose that the investment for fixing the damage caused by the wire intruder is \$2K and for the wireless intruder is \$3K, that is, V_{12} =2000 and V_{22} = 3000.
Therefore, C_2 = 8666.67+3666.66= 12333.33.

Suppose that in the year 3, we choose a different policy C that have

$$T' = \begin{bmatrix} 0.8 & 0.7 \\ 0.2 & 0.3 \end{bmatrix}$$

Then the steady state in the year 3 is [q_{12} = 7/9 q_{22} = 2/9]. If the damage for intruder through wire network is \$9K and it is \$2K if through wireless network. That is, D_{13} =9000 and D_{23} =2000. Furthermore, suppose that the investment for fixing the damage caused by the wire intruder is \$1K and for the wireless intruder is \$2K, that is, V_{12} =1000 and V_{22} = 2000.
Therefore, C_3 = 8000+2444.44= 10444.44.

Therefore if we know all risk information in those three years, then we should adopt policy A only in the first year to meet the budget. If we would choose policy B or C, we would have had over the budget. However, if we don’t have those risk information appeared in each year and if each year the risk is randomly appears, then the average cost per year is $E(T_3)$= 12694 and we can cover two years instead of only one year within the budget.

5 Simulation Results

In order to generate the transition probability for a semi-Markov chain that satisfies (2), a truncated distribution is generated. All entries in a transition probability matrix must be non-negative. In addition, the sums of the entries of every row of a transition probability matrix are ones. To simplify the problem, only four states (or four threats) were used and initially the risk in each state is equally possible. There are four different distributions are used for the transition probability matrix from every state to all four possible states in the simulation. They are uniform distribution, exponential distribution of mean 0.5, standard normal distribution and Weibull distribution with ν=0, α=0.5, and β (β=1) [2]. To generate the transition probability matrix for each distribution, three random variates were generated first. Then they are sorted and the probability of the value less than or equal to the random variates were calculated. To guarantee that the generated distribution satisfying (1), the probability for the last state was created by subtracting the sum of those generated probabilities from one. Because every entry of the transition probability matrices is non-zero, the initial state will reach to the steady state. The steady state is obtained by solving a system of linear equations that satisfying (1) and (5) using Gaussian Elimination [7]. It presents a sample of such run of the semi-Markov chain. It reaches a steady state after time one million units. It is assumed that there are three years considered in the simulation. In each year the damage costs for four treats are 1000, 2000, 3000 and 4000. In addition, the investment costs for four threats are 4000, 3000, 2000 and 1000.

A simulation result for the uniform distribution in the probability transition is shown in Table 1 below.

Table 1: A simulation result using uniform distribution

	Year 1	Year 2	Year 3
Run 1	11188	11844	12427
Run 2	11753	12235	11252
Run 3	12119	12334	12017
Run 4	11535	11875	12013
Run 5	12088	12234	12119
Run 6	12111	11496	12378
Run 7	11020	12174	12199
Run 8	12083	11966	11316
Run 9	11744	12175	11631
Run 10	11684	11897	12059
Average	11733	12023	11941

The results in Table 1 will be displayed in Figure 1 below.

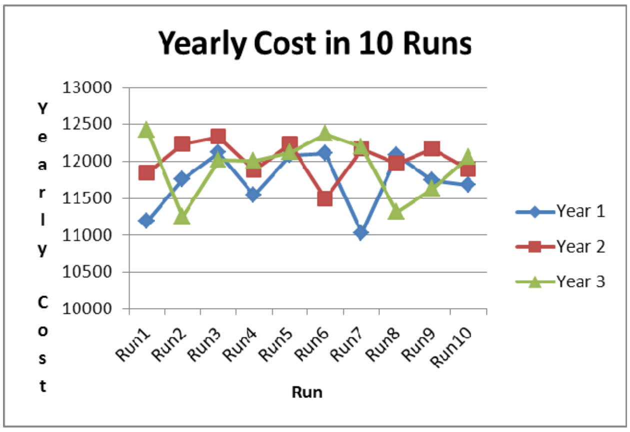

Figure 1: Yearly cost using uniform distribution

The results for all four distributions are shown in Figure 2 below.

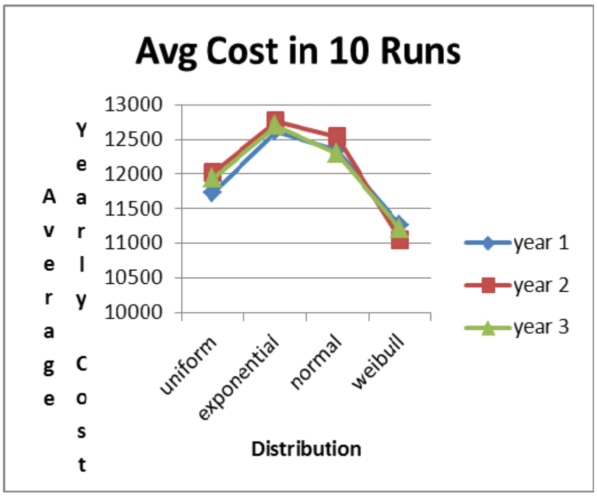

Figure 2: Average cost using four distributions

And the total costs are shown in Figure 3 below.

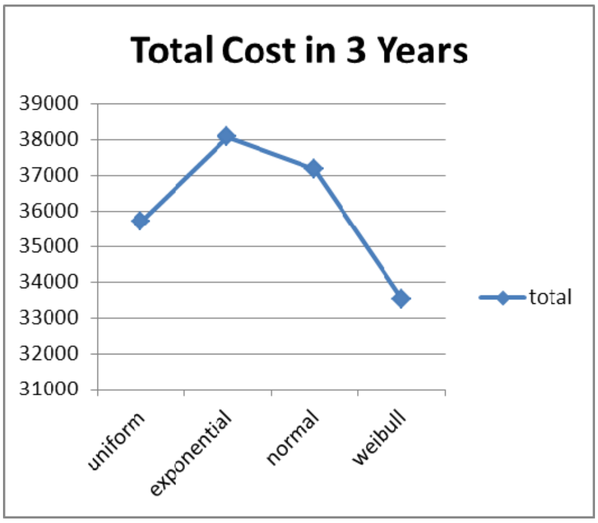

Figure 3: Total cost using four distributions

We can see that using Weibull distribution total cost is optimal.

6 Conclusion

The simple model proposed in this paper can help a company to make its decision under different possible threats with different damages and investments.

ACKNOWLEDGEMENTS. This paper is in memory of my mother for her life time support and encouragement.

References

[1] M. Aburdene, *Computer Simulation of Dynamic Systems***,** Wm. C. Brown Publishing, Dubuque, IA, 1988.

[2] J. Banks, J. Carson and B. Nelson, *Discrete Event System Simulation*, New Jersey, Prentice Hall, 1996.

[3] N. Bhat, *Elements of Applied Stochastic Processes*, John Wiley & Sons, New York, 1972.

[4] M. Bishop, *Computer Security*, Addison-Wesley/Prentice-Hall, Boston, MA, 2003

[5] P. Bremaud, *Markov Chains*. Springer, New York, 1999.

[6] M. Molloy, *Fundamentals of Performance Modeling*, Macmillan Publishing, New York, 1988.

[7] J. Mathews, *Numerical Methods.* Prentice Hall, New Jersey, 1987.

[8] R. Panko, *Corporate Computer and Network Security*, Prentice Hall, 2nd edition, New Jersey, 2009.

[9] A. Rencher, *Methods of Multivariate Analysis,* John Wiley & Sons, New York, 1995.

[10] M. Shing, C. Shing, K. Chen and H. Lee, Security Modeling on the Supply Chain Networks, *Journal of Systemics, Cybernetics and Informatics*, **5**(5), (2008), 53-58.