International Journal of
Electronic Commerce Studies
Vol.2, No.1 , pp.67-76, 2011

STUDY OF A RISK MANAGEMENT MODEL

Marn-Ling Shing
Taipei Municipal University of Education
shing@tmue.edu.tw

Chen-chi Shing
Radford University
cshing@radford.edu

Kuo Lane Chen
University of Southern Mississippi
chenku60@yahoo.com

Huei Lee
Eastern Michigan University
Huei.Lee@emich.edu

ABSTRACT

Risk management has become an important issue in the information security area. This study proposes a Semi-Markov chain model to manage the information security risk. When the state information is not recognized as a normal state, the model can send a warning signal to the manager. A simulated model was used to validate the semi-Markov chain model.

Keywords: Information Security Risk Management, Information Security Assessment, Information Security Modeling and Simulation, Information Security Model Validation

1. INTRODUCTION

Risk management has become an important issue in the information systems area[1]. Risk management in this study refers to the risk in information security or information assurance. Information assurance includes "measures that protect information and information systems by ensuring their availability, integrity, authentication, confidentiality, and

non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" [2].

Over the past decade, the need for information assurance has grown rapidly. This is evidenced by a number of national initiatives spanning the federal government and the private sector. For example, the National Cyber Security Leadership Act of 2003 designated that it is the responsibility of the Chief Information Officer (CIO) within each Federal Agency to:

1. *Identify the significant vulnerabilities of the information technology of such agency, including--(A) vulnerabilities of such classes of information technology of such agency as the Chief Information Officer shall designate for purposes of this section; and (B) vulnerabilities of the information technology of such agency as a whole;*
2. *Establish performance goals for eliminating the significant vulnerabilities of the information technology of such agency identified under paragraph (1), with such performance goals--(A) to be established utilizing the current state of the information technology of such agency as a baseline; (B) to be stated both for particular classes of information technology of such agency (as determined under paragraph (1)(A)) and for the information technology of such agency as a whole; and (C) to be expressed as target ratios of vulnerabilities per information technology;*
3. *Procure or develop tools to identify and eliminate the vulnerabilities identified under paragraph (1) in order to achieve the performance goals established under paragraph (2);*
4. *Train personnel of such agency in the utilization of tools procured or developed under paragraph (3);*
5. *Not less often than once each quarter, test the information technology of such agency to determine the extent of the compliance of the information technology with the performance goals established under paragraph (3); and*

> 6. *To the extent that the information technology of such agency does not comply with the performance goals established under paragraph (3), promptly develop and implement a plan to eliminate significant vulnerabilities in the information technology in order to achieve compliance with such performance goals.*
>
> National Cyber Security Leadership Act of 2003, S 187 IS[3].

In another national initiative (National Strategy to Secure Cyberspace, 2003), the call for increased attention to information assurance was wide reaching – spanning federal government to home Internet users. The plan notes that "our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security".

The objectives of the National Strategy to Secure Cyberspace are to:

1. Prevent cyber attacks against America's critical infrastructures;
2. Reduce national vulnerability to cyber attacks; and
3. Minimize damage and recovery time from cyber attacks that do occur.

On the private side, businesses are becoming increasingly dependent on technology for the liability of security and privacy as required by legislation such as HIPAA, Sarbanes-Oxley, and California's Security Breach Information Act 1986. The job of keeping the company's infrastructure and network safe is growing increasingly complex as the perimeter expands, threats become more sophisticated, and systems become more complex and embedded. Information security is more than just good IDs or firewalls. It involves keeping users educated, creating good policies, getting the right budget, and sometimes monitoring user activity. All of these efforts demand employment of sophisticated technology and well trained personnel in information assurance.

Although information security is very important, it still lacks a quantitative model for security assessment[4]. In the following sections, a semi-Markov model is first proposed, and then simulated and validated.

2. LITERATURE REVIEW ON IT RISK MANAGEMENT

Risk management has attracted considerable research attention in the last 20 years. Risk management in IT can include software project risk[5], outsourcing risk, information security risk[6], and other IT risks. Rainer Snyder, and Carr[1] propose a risk analysis process that employs a combination of qualitative and quantitative methodologies.

A Markov process is a "stochastic process in which the probability of a system state depends only on the previous state, not on the history of how to get to the previous state." [7, 13]

Suppose the probability that the system is in one of the *n* states at time 0 is represented by p(0), and

$$p(0)=\begin{bmatrix} p_1(0) \\ p_2(0) \\ \dots \\ p_n(0) \end{bmatrix}, \quad \sum_{i=1}^{n} p_i(0) = 1 \qquad \text{(Eq. 2.1)}$$

,where $p_i(0)$ is the probability of the system is in state *i* at time 0.

The probability that the system is in one of those n states at time s is represented by p(s), $p(s)=\begin{bmatrix} p_1(s) \\ p_2(s) \\ \dots \\ p_n(s) \end{bmatrix}$, where pi(s) represents the probability of the system is in state i at time s. And p(s)=T'(T'(…(T'p(0))))=T's p(0), where T', the transpose matrix of T. is the transition probability matrix,

$$T'=\begin{bmatrix} p_{11} & p_{21} & \dots & p_{n1} \\ p_{12} & p_{22} & \dots & p_{n2} \\ \dots & \dots & \dots & \dots \\ p_{1n} & p_{2n} & \dots & p_{nn} \end{bmatrix}, \quad \sum_{j=1}^{n} p_{ij} = 1, \text{ for } i=1,2,\dots,n \qquad \text{(Eq. 2.2)}$$

A detailed calculation of the state transitions can be referred in the papers by Shing and Chen et al.[8, 9, 10]. A semi-Markov process is a

stochastic process that can have an arbitrary distribution of time between state changes, and any new state is possible given the current state[11]. Each state is a recurrent non-null and aperiodic. That is, the semi-Markov chain is ergodic[12] and the system has a steady state p(s) when time s is large, where T'p(s) = p(s).

In the next section we show how to simulate the state transitions and how to validate the model.

3. SIMULATION OF THE SEMI-MARKOV CHAIN MODEL

In this study, a simulation program was designed to simulate an e-commerce environment that has potential security attacks. The program was started by randomly generating initial states[7]. After randomly generating the transition probability matrix, the program simulated the state transitions for a large number of times.

In order to generate the transition probability for a semi-Markov chain that satisfies Eq. 2.2, a truncated distribution was generated. If there are eight states initially, the transition probability for the last state on a row of T' is generated by subtracting the sum of transition probabilities of the first three states in the same row from one. The initial state is set to be:

$$p(0)=(p_1(0),p_2(0), \ldots,p_8(0))=(0.349345,0.014499,0.000804,0.020307,0.558151,0.023165,0.001285,0.032445) \text{ and } \sum_{i=1}^{8} p_i(0) = 1.$$

Each simulation runs for one million time units. The simulations are randomly run for ten times. The mean $\mu 0$ of the final states of all 10 runs are created, and the variance-covariance matrix Σ is created for each case. Those eight states are correlated and can be shown by scatter plots as in the Figure 1 below:

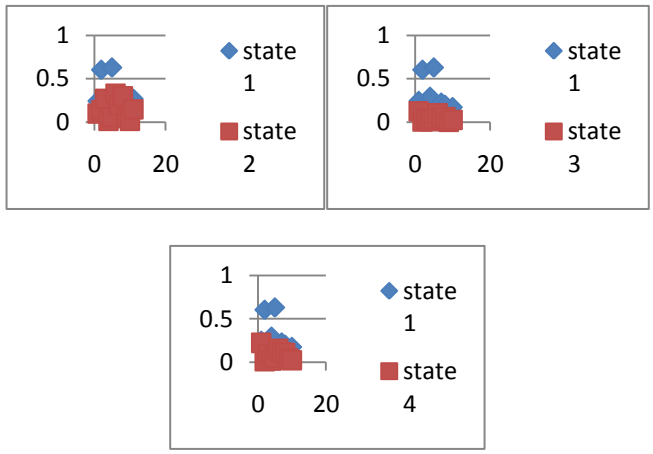

Figure 1. Examples of Scatter Plots of eight states under randomly generated uniform (0,1)

4. VALIDATION OF THE SEMI-MARKOV CHAIN MODEL

Assuming that the variance-covariance matrix between all states Σ is known, we can test the hypothesis H_0: $\mu=\mu_0$ vs H_1: $\mu\neq\mu_0$. We reject H_0 at the α level if $n(\bar{y} - \mu_0)' \Sigma^{-1} (\bar{y} - \mu_0) > \chi^2_{\alpha,p}$, where $\bar{y} = \sum_{i=1}^{10} y_i /10$ is the average of n (n=10) final states of all runs and p (p=8)is the total number of states[10]. That is to reject H_0 at 0.05 level if $10(\bar{y} - \mu_0)' \Sigma^{-1} (\bar{y} - \mu_0) > \chi^2_{0.05,8} = 15.51$. In Table 1 below, it shows mean μ0 and the variance-covariance matrix Σ of 10 runs of a randomly generated exponential distributions with λ =0.5 for the state transition matrix.

Table 1. Average μ_0 and the variance-covariance matrix Σ of 10 runs of a randomly generated exponential distribution with λ =0.5

	state 1	**state 2**	**state 3**	**state 4**	**state 5**	**state 6**	**state 7**	**state 8**
run 1	0.000211	0.000866	0.000625	0.001141	0.07385	0.303895	0.219258	0.400155
run 2	0.022933	0.030593	0.031837	0.059356	0.135532	0.180805	0.188153	0.350791
run 3	0.056049	0.02056	0.056076	0.087025	0.199054	0.073019	0.199152	0.309066
run 4	0.010482	0.015897	0.019021	0.175276	0.037016	0.056141	0.067174	0.618993
run 5	0.30571	0.087617	0.064312	0.206312	0.154731	0.044346	0.032551	0.104422
run 6	0.045532	0.072973	0.167455	0.20848	0.046556	0.074615	0.171221	0.213169
run 7	0.044504	0.048618	0.042462	0.132097	0.121754	0.133008	0.116167	0.361389
run 8	0.163495	0.138899	0.055723	0.172634	0.14455	0.122804	0.049266	0.152629
run 9	0.074417	0.04978	0.058358	0.076203	0.213177	0.142601	0.167172	0.218293
run 10	0.049954	0.043289	0.071834	0.170202	0.099038	0.085826	0.142417	0.337441
Average	0.077329	0.050909	0.05677	0.128873	0.122526	0.121706	0.135253	0.306635
Covariance	0.009703	0.005386	0.005139	0.00601	0.004869	0	0	0
	0.005386	0.004261	0.002982	0.004394	0.002321	0	0	0
	0.005139	0.002982	0.004707	0.004585	0	0	0.000519	0
	0.00601	0.004394	0.004585	0.007353	0	0	0	0
	0.004869	0.002321	0	0	0.006263	0	0.001617	0
	0	0	0	0	0	0.00812	0.00568	0.004526
	0	0	0.000519	0	0.001617	0.00568	0.00696	0.004456
	0	0	0	0	0	0.004526	0.004456	0.015451

However, if Σ is unknown, the sample variance-covariance matrix S is used to estimate Σ . Then we can test the hypothesis H_0: $\mu = \mu_0$ versus H_1: $\mu \neq \mu_0$. We reject H_0 if $10(\bar{y} - \mu_0)' S^{-1} (\bar{y} - \mu_0) > T^2_{\alpha,8,9}$, where $\bar{y} = \sum_{i=1}^{10} y_i /10$ is the average of 10 final states of all runs, and T^2 is the Hotelling's T^2 test. S is the sample variance-covariance matrix, which can be obtained by $\sum_{i=1}^{n} (y_i - \bar{y})(y_i - \bar{y}) \Big/ (n-1)$ [14].

S^{-1} is the inverse matrix of S. In Table 2 below, it shows the mean μ_0 and the sample variance-covariance matrix S for Σ out of ten runs of a

randomly generated Weibull distribution with parameter b=1 for the state transition matrix.

Table 2. Average μ0 and the sample variance-covariance matrix S of Σ of 10 runs of randomly generated Weibull distributions with parameter b=1

	state 1=*y1*	**state 2=*y2***	**state 3=*y3***	**state 4=*y4***	**state 5=*y5***	**state 6=*y6***	**state 7=*y7***	**state 8=*y8***
run 1	0.00286	0.010588	0.019275	0.228209	0.008101	0.029989	0.054595	0.646384
run 2	0.102668	0.029755	0.062048	0.105082	0.24007	0.069575	0.145088	0.245714
run 3	0.046714	0.068358	0.058361	0.244163	0.06515	0.095336	0.081394	0.340525
run 4	0.040084	0.058827	0.051009	0.15216	0.09261	0.135913	0.11785	0.351548
run 5	0.049504	0.05076	0.046313	0.098232	0.152711	0.156585	0.142867	0.30303
run 6	0.074364	0.072936	0.044172	0.201941	0.114659	0.112458	0.068107	0.311365
run 7	0.114699	0.092581	0.054949	0.188128	0.139986	0.112992	0.067063	0.229604
run 8	0.087472	0.027654	0.068372	0.115501	0.205078	0.064835	0.160297	0.270791
run 9	0.061746	0.050827	0.04713	0.346858	0.060147	0.049511	0.045909	0.337873
run 10	0.121126	0.112545	0.032867	0.103201	0.206473	0.191845	0.056025	0.175919
Average	0.070124	0.057483	0.04845	0.178348	0.128499	0.101904	0.09392	0.321275
Covariance	0.003918	0.002738	0.003162	0	0.004984	0.002879	0.001212	0
	0.002738	0.003253	0	0	0.002306	0.003657	0	0
	0.003162	0	0.00151	0	0.002433	0	0.002105	0
	0	0	0	0.008457	0	0	0	0.006978
	0.004984	0.002306	0.002433	0	0.007839	0.004053	0.004584	0
	0.002879	0.003657	0	0	0.004053	0.005311	0.001008	0
	0.001212	0	0.002105	0	0.004584	0.001008	0.004558	0
	0	0	0	0.006978	0	0	0	0.013402

In Table 3 below, an Excel spreadsheet is used to create the S matrix shown in Table 2.

Assuming transition probability distributions are standard normal, and if the system runs normally, the states are distributed as $N(\mu, \Sigma)$. There are ten observations (y_i , i=1,2, …,10) of states in the long run. The value of μ_0 in the testing hypothesis below has been measured before.

Table 3. Using an Excel worksheet to calculate S for Table 2

	*y1*y1*	*y1*y2*	*y1*y3*	*y1*y4*	*y1*y5*	*y1*y6*	*y1*y7*	*y1*y8*
run 1	8.18E-06	3.028E-05	5.513E-05	0.0006527	2.317E-05	8.577E-05	0.0001561	0.0018487
run 2	0.0105407	0.0030549	0.0063703	0.0107886	0.0246475	0.0071431	0.0148959	0.025227
run 3	0.0021822	0.0031933	0.0027263	0.0114058	0.0030434	0.0044535	0.0038022	0.0159073
run 4	0.0016067	0.002358	0.0020446	0.0060992	0.0037122	0.0054479	0.0047239	0.0140915
run 5	0.0024506	0.0025128	0.0022927	0.0048629	0.0075598	0.0077516	0.0070725	0.0150012
run 6	0.00553	0.0054238	0.0032848	0.0150171	0.0085265	0.0083628	0.0050647	0.0231543
run 7	0.0131559	0.0106189	0.0063026	0.0215781	0.0160563	0.0129601	0.0076921	0.0263353
run 8	0.0076514	0.002419	0.0059806	0.0101031	0.0179386	0.0056712	0.0140215	0.0236866
run 9	0.0038126	0.0031384	0.0029101	0.0214171	0.0037138	0.0030571	0.0028347	0.0208623
run 10	0.0146715	0.0136321	0.003981	0.0125003	0.0250092	0.0232374	0.0067861	0.0213084
Average	0.006161	0.0046381	0.0035948	0.0114425	0.0110231	0.0078171	0.006705	0.0187423

To test the hypothesis H_0: $\mu = \mu_0$ versus H_1: $\mu \neq \mu_0$, where μ_0 =

0.006161 0.0046381 0.0035948 0.0114425 0.0110231 0.0078171 0.006705 0.0187423

Using the values in Table 2, the average of ten observations is $\bar{y}$ =

0.070124 0.057483 0.04845 0.178348 0.128499 0.101904 0.09392 0.321275

From Table 2, $10(\bar{y} - \mu_0)' S^{-1} (\bar{y} - \mu_0) = 28 < T^2_{0.05,8,9} = 697.356$.

The null hypothesis is not rejected. Therefore the security has not been breached.

5. CONCLUSIONS

The risk management model we propose is to periodically examine the state transition matrix of the semi-Markov chain model. From the observations of the matrix, we can tell whether the system will reach a steady state. If a state does not belong to one of the possible eight states, it violates the security requirement and poses a possible risk to the information security. Besides, if any state probability p(s) at time s from the simulation run shows an abnormality compared to data collected, then

the system may have a security breach. The proposed risk model can help managers to understand the security status, enabling the manager to implement necessary security strategies.

REFERENCES

[1] R.K.J.R. Rainer, C.A. Snyder, and H.H. Carr, Risk analysis for information technology. *Journal of Management Information Systems*, 8 (1), p129-147, 1991.

[2] The Committee on National Security Systems (CNSS), *CNSS Instruction, No. 4009, 2003*. Retrieved October 21, 2010, from http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[3] Symantec, *U.S. Information Security Law, Part Four*. Retrieved October 21, 2010, from http://www.symantec.com/connect/articles/us-information-security-law-part-four.

[4] M. Bishop, *Computer Security: Art and Science*. Boston, MA: Addison-Wesley, 2003.

[5] M. Keil, A. Tiwana, and A. Bush, Reconciling user and project manager perceptions of IT project risk: a Delphi study. *Information Systems Journal*, 12(2), p103-119, 2002.

[6] L. D. Bodin, L. A. Gordon, and M. P. Loeb, Information Security and Risk Management. *Communications of the ACM*, 51(4), p64-68, 2008.

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

[8] K. L. Chen, H. Lee, and J. Yang, Security considerations on the design of supply chain networks. *Proceedings of the Southwest Division of the Decision Sciences Institute (SWDSI)*. March 1-4, Oklahoma, 2006.

[9] K. L. Chen, M. Shing, H. Lee, and C. Shing, Modeling in confidentiality and integrity for a supply chain network. *Communications of IIMA*, 7(1), p41-48, 2007.

[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), p53-58, 2007.

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

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

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

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