Research Article

A Cooperative Model for IS Security Risk Management in Distributed Environment

Nan Feng and Chundong Zheng

College of Management and Economics, Tianjin University, 92 Weijin Road, Nankai District, Tianjin 300072, China

Correspondence should be addressed to Nan Feng; fengnan@tju.edu.cn

Received 24 August 2013; Accepted 21 November 2013; Published 19 January 2014

Academic Editors: J. Shu and F. Yu

Copyright © 2014 N. Feng and C. Zheng. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Given the increasing cooperation between organizations, the flexible exchange of security information across the allied organizations is critical to effectively manage information systems (IS) security in a distributed environment. In this paper, we develop a cooperative model for IS security risk management in a distributed environment. In the proposed model, the exchange of security information among the interconnected IS under distributed environment is supported by Bayesian networks (BNs). In addition, for an organization's IS, a BN is utilized to represent its security environment and dynamically predict its security risk level, by which the security manager can select an optimal action to safeguard the firm's information resources. The actual case studied illustrates the cooperative model presented in this paper and how it can be exploited to manage the distributed IS security risk effectively.

1. Introduction

With the increasing of collaboration between organizations, the management of information systems (IS) security risk is distributed across the allied organizations and the cooperative activities between organizations are imperative [1–4]. Therefore, for more effectively assessing the security risk level of the IS in a distributed environment, it is critical to develop a system for the exchange of security information among the interconnected IS. However, how to achieve the flexible exchange of security information under distributed environment is a significant challenge in the process of modelling [5]. Unfortunately, few previous studies on IS security take the above issue into account.

In this paper, a cooperative model for IS security risk management is proposed to estimate the risk level of each associated organization's IS and support the decision making of security risk treatment in a distributed environment. In the model, the exchange of security information among the interconnected IS is achieved through Bayesian networks (BNs). Moreover, a BN is also exploited to model the security environment of an organization's IS and predict its security risk level. However, it is difficult and critical task for a security

manager to establish an appropriate BN, which is suitable for the environment of organization's information systems [6–8]. To address this issue, in this paper, we develop an algorithm to support the BN initiation. Finally, based on the security risk level for an organization's IS, the security manager selects an optimal action to protect its information resources.

The remaining sections of this paper are organized as follows. We first review the relevant literature in Section 2. Then we discuss the development of the cooperative model in detail in Sections 3 and 4. The proposed model is further demonstrated and validated in Section 5 via a case study. Finally, we summarize our contributions and point out further research directions.

2. Literature Review

There has been increased academic interest in the IS security risk management. From the technical literature, the security protocols [9], fire wall and intrusion detection techniques [10, 11], and authentication technologies [12, 13] have been examined. From an economics perspective, some researchers have investigated the investment on information systems security [14, 15], economics of vulnerability disclosure [16, 17], and

TABLE 1: Information exchange in the interactive process.

Exchange information	Description
Search request	It consists of the requester's id, IP address, and the required input variables. The estimation component has a set of sharing variables. To find components capable of providing required input data, the estimation component sends a search request to the registration component.
Search reply	It consists of the requested variable name, the IP address, and status of the component publishing the variable. Based on receiving a search request, the registration component searches its database to determine which components can provide the requested variables.
Registration message	It consists of component id, IP address, list of published variables, and their possible states. Each estimation component registers with the registration component, which issues an acknowledgment message for entering the new component in its database.
Communication between estimation components	It consists of the request id, the sender's id, and the probability distribution of the requested variable. Upon receiving the list of components capable of providing the required input from the registration component, the request component sends requests directly to these components. Then, the sender sends the probability distribution of the requested variable.

the characteristics of internet security breaches that impact the market value of breached firms [18].

In recent years, a new managerial perspective on IS security has emerged from the literature. This perspective focuses on the managerial processes that control the effective deployment of technical approaches and security resources to create a secure IS environment in an organization. From this perspective, Feng and Li [19] proposed an IS security risk evaluation model based on the improved evidence theory. For the handling of uncertain evidence found in IS security risk analysis, their model provided a novel approach to define the basic belief assignment of evidence theory. In addition, the model also presented a method of testing the evidential consistency, which is capable of resolving the conflicts from uncertain evidence. Then, in order to identify the causal relationships among security risk factors and analyze the complexity of vulnerability propagation, they also developed a security risk analysis model (SRAM) [20], in which the vulnerability propagation analysis is performed to determine the propagation paths with the highest IS security risk level. Yan [21] presented a conceptual model for IS security analysis, which can facilitate to identify potential security risks. Chen et al. [22] focus on controlling the risks in the form of the fault of information networks. They developed an approach to estimate the risk level on the vulnerability of information networks.

Bayesian networks (BNs), also known as probabilistic belief networks, is a knowledge representation tool capable of representing dependence and independence relationships among random variables [23]. A BN, $N = (X, G, P)$, consists of a directed acyclic graph G and a set of conditional probability distributions (beliefs) P for variables X . BN inference means computing the conditional probability for some variables given the evidence, which is defined as a collection of findings. This operation is also called probability updating or belief updating.

In this paper, the developed BN is not only used to facilitate the dynamical prediction of the security risk level of

an organization's IS, but also exploited to model the IS security environment.

3. Model Architecture

In a distributed environment, the proposed model consists of many interconnected network information systems. We call these network information systems as "associated members." Each associated member is installed with three kinds of components: monitor component, estimation component, and treatment component. Besides, the above three kinds of components, the registration component contains the information about each estimation component. It is required that all estimation components in the distributed environment must register with the registration component. The cooperative model architecture is demonstrated in Figure 1.

The interactions among the estimation component and the registration component are shown in Figure 2. In the interactive process, as shown in Table 1, there are four kinds of sharing information: search request, search reply, registration message, and communication between estimation components.

4. Bayesian Network Development

In this section, we present an algorithm based on ant colony optimization (shown in Algorithm 1) to develop the Bayesian network (BN), which is able to model the security environment of an associated member under distributed environment.

The equations appearing in the algorithm are as follows.

(1) Heuristic information:

$$\eta_{ij} = f(x_i, Pa(x_i) \cup \{x_j\}) - f(x_i, Pa(x_i)). \quad (1)$$

(2) Updating rule:

$$\tau_{ij} \leftarrow (1 - \rho) \tau_{ij} + \rho \Delta \tau_{ij} \quad (2)$$

FIGURE 1: Model architecture.

FIGURE 2: Interactions among the components.

in which

$$\Delta\tau_{ij} = \begin{cases} \frac{1}{|f(G^* : D)|} & \text{if } x_j \rightarrow x_i \in G^* \\ \tau_{ij} & \text{if } x_j \rightarrow x_i \notin G^*, \end{cases} \quad (3)$$

in the arc $x_j \rightarrow x_i$, τ_{ij} is the pheromone's degree, and ρ ($0 < \rho \leq 1$) is a variable which can control the pheromone value. Moreover, G^* is the BN structure suitable for the organization's IS best.

(3) Probabilistic transition:

$$r, l = \begin{cases} \arg \max_{i, j \in F_G} \{ [\tau_{ij}]^\alpha [\eta_{ij}]^\beta \} & \text{if } q \leq q_0 \\ I, J & \text{if } q > q_0 \end{cases} \quad (4)$$

in which I and J are two nodes chosen randomly based on the following equation:

$$p_k(i, j) = \begin{cases} \frac{[\tau_{ij}]^\alpha [\eta_{ij}]^\beta}{\sum_{u, v \in F_G} [\tau_{uv}]^\alpha [\eta_{uv}]^\beta} & \text{if } i, j \in F_G \\ 0 & \text{otherwise.} \end{cases} \quad (5)$$

5. Case Study

In this section, the proposed model is applied to a distributed environment, which is composed of four associated members with interconnected IS: two suppliers (S1 and S2), a manufacturer (M1), and a downstream transporter (DT1).

Based on the algorithm presented in Section 4, we develop the BN for each associated member. Taking M1 and

Input: Set of all/candidate edges
Output: Bayesian network

```

(1) repeat
(2)   for  $k = 1$  to  $m$  do
(3)     for  $i = 1$  to  $n$  do  $Pa(x_i) = \phi$ ;
(4)     for  $i = 1$  and  $j = 1$  to  $n$  do
(5)       if  $(i \neq j)$  then  $\eta_{ij} = f(x_i, x_j) - f(x_i, \phi)$ ;
(6)     end
(7)   repeat
(8)     Select two indexes  $i$  and  $j$  by using (4) and (5) and assign edge  $e_{ij}$  to  $G_k$ ;
(9)     if  $(\eta_{ij} > 0)$  then  $Pa(x_i) = Pa(x_i) \cup \{x_j\}$ ;
(10)     $\eta_{ij} = -\infty$ ;
(11)    for all  $x_a \in Ancestors(x_j) \cup \{x_j\}$  and  $x_b \in Descendants(x_i) \cup \{x_i\}$  do  $\eta_{ab} = -\infty$ ;
(12)    for  $k = 1$  to  $n$  do
(13)      if  $(\eta_{ik} > -\infty)$  then  $\eta_{ij} = f(x_i, Pa(x_i) \cup \{x_k\}) - f(x_i, Pa(x_i))$ ;
(14)    end
(15)     $\tau_{ij} = (1 - \rho) \cdot \tau_{ij} + \rho \cdot \tau_0$ ;
(16)  until  $\forall i, j (\eta_{ij} \leq 0 \text{ or } \eta_{ij} = -\infty)$ ;
(17) end
(18)  $G_b = \arg \max_{k: 1 \dots m} f(G_k : D)$ ;
(19) if  $f(G_b : D) \geq f(G^* : D)$  then  $G^* = G_b$ ;
(20) Update pheromone according to (2) using  $f(G^* : D)$ ;
(21)  $N_{iter} ++$ ;
(22) until  $N_{iter} = N_{max}$ ;
(23) return Bayesian network with structure  $G^*$ 

```

ALGORITHM 1: Bayesian network development algorithm.

TABLE 2: BN information of M1.

Node ID	Node name	State space	Parent nodes	Children nodes
M1.1	Network access control	{Effective; average; ineffective}	Φ	{M1.7}
M1.2	Network security audit	{Comprehensive; incomprehensive}	Φ	{M1.7}
M1.3	Change management	{Effective; average; ineffective}	Φ	{M1.9}
M1.4	Supplier threat level	{0; 1; 2; 3; 4; 5}	Φ	{M1.8}
M1.5	Transporter threat level	{0; 1; 2; 3; 4; 5}	Φ	{M1.8}
M1.6	Operational procedures and responsibilities	{Very standard; standard; non-standard}	Φ	{M1.9}
M1.7	Network security	{High; medium; low}	{M1.1, M1.2}	{M1.10}
M1.8	External systems security	{High; medium; low}	{M1.4, M1.5}	{M1.10}
M1.9	Operation security	{High; medium; low}	{M1.3, M1.6}	{M1.10}
M1.10	M1 threat level	{0; 1; 2; 3; 4; 5}	{M1.7, M1.8, M1.9}	Φ

TABLE 3: BN information of S1.

Node ID	Node name	State space	Parent nodes	Children nodes
S1.1	Communication secrecy	{High; medium; low}	Φ	{S1.6}
S1.2	Audit logging	{Secure; average; insecure}	Φ	{S1.6}
S1.3	Network access control	{Effective; average; ineffective}	Φ	{S1.5}
S1.4	Network security audit	{Comprehensive; incomprehensive}	Φ	{S1.5}
S1.5	Network security	{High; medium; low}	{S1.3, S1.4}	{S1.7}
S1.6	Communication security	{High; medium; low}	{S1.1, S1.2}	{S1.7}
S1.7	S1 threat level	{0; 1; 2; 3; 4; 5}	{S1.5, S1.6}	Φ

FIGURE 3: BN structures of M1 and S1.

FIGURE 4: Security manager interface.

S1, for example, their information of BN nodes is given in Tables 2 and 3, and their BN structures are shown in Figure 3.

The manager interface of our proposed model is shown in Figure 4, in which the security manager can specify the BN for each associated organization.

Once the new evidence is obtained through the monitor components, the estimation component is able to make the BN modify its own belief (probability distribution on variable of risk level) in real time and exchange the update of beliefs of the security state with other associated members.

6. Conclusions

In a distributed environment, in order to effectively manage information systems (IS) security, a cooperative model based

on Bayesian networks is presented and illustrated in this paper. We contribute to the IS security literature by supporting the exchange of security information among interconnected IS. Furthermore, for the modelling of IS security environment, an algorithm based on ant colony optimization facilitates to predict IS threat level more objectively. The model proposed in this paper has great potential for future extensions and refinements to provide more utility for the management of IS security.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The research was supported by the National Natural Science Foundation of China (nos. 70901054 and 71271149) and the Program for New Century Excellent Talents in University (NCET). It was also supported by the China Postdoctoral Science Foundation funded Project (no. 2012M520025). The authors are very grateful to all anonymous reviewers whose invaluable comments and suggestions substantially helped improve the quality of this paper.

References

- [1] I. A. Tsoukalas and P. D. Siozos, "Privacy and anonymity in the information society—challenges for the european union," *The-ScientificWorldJournal*, vol. 11, pp. 458–462, 2011.
- [2] Y. Zhang, X. Deng, D. Wei, and Y. Deng, "Assessment of E-Commerce security using AHP and evidential reasoning," *Expert Systems with Applications*, vol. 39, no. 3, pp. 3611–3623, 2012.
- [3] S. Ransbotham and S. Mitra, "Choice and chance: a conceptual model of paths to information security compromise," *Information Systems Research*, vol. 20, no. 1, pp. 121–139, 2009.
- [4] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, pp. 523–548, 2010.
- [5] E. Gal-Or and A. Chose, "The economic incentives for sharing security information," *Information Systems Research*, vol. 16, no. 2, pp. 186–208, 2005.
- [6] C.-F. Fan and Y.-C. Yu, "BBN-based software project risk management," *Journal of Systems and Software*, vol. 73, no. 2, pp. 193–203, 2004.
- [7] L. Sun, R. P. Srivastava, and T. J. Mock, "An information systems security risk assessment model under the Dempster-Shafer theory of belief functions," *Journal of Management Information Systems*, vol. 22, no. 4, pp. 109–142, 2006.
- [8] W. T. Yue, M. Çakanyildirim, Y. U. Ryu, and D. Liu, "Network externalities, layered protection and IT security risk management," *Decision Support Systems*, vol. 44, no. 1, pp. 1–16, 2007.
- [9] R. Di Pietro and L. V. Mancini, "Security and privacy issues of handheld and wearable wireless devices," *Communications of the ACM*, vol. 46, no. 9, pp. 74–79, 2003.
- [10] P. Ning, Y. Cui, D. S. Reeves, and D. Xu, "Techniques and tools for analyzing intrusion alerts," *ACM Transactions on Information and System Security*, vol. 7, no. 2, pp. 274–318, 2004.
- [11] R. Sarathy and K. Muralidhar, "The security of confidential numerical data in databases," *Information Systems Research*, vol. 13, no. 4, pp. 389–403, 2002.
- [12] N. Li and M. V. Tripunitara, "Security analysis in role-based access control," *ACM Transactions on Information and System Security*, vol. 9, no. 4, pp. 391–420, 2006.
- [13] S. Rinderle-Ma and M. Reichert, "Comprehensive life cycle support for access rules in information systems: the CEOSIS project," *Enterprise Information Systems*, vol. 3, no. 3, pp. 219–251, 2009.
- [14] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438–457, 2002.
- [15] H. S. B. Herath and T. C. Herath, "Investments in information security: a real options perspective with Bayesian postaudit," *Journal of Management Information Systems*, vol. 25, no. 3, pp. 337–375, 2009.
- [16] K. Kannan and R. Telang, "Market for software vulnerabilities? Think again," *Management Science*, vol. 51, no. 5, pp. 726–740, 2005.
- [17] M. N. Azaiez and V. M. Bier, "Optimal resource allocation for security in reliability systems," *European Journal of Operational Research*, vol. 181, no. 2, pp. 773–786, 2007.
- [18] H. Cavusoglu, B. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers," *International Journal of Electronic Commerce*, vol. 9, no. 1, pp. 69–104, 2004.
- [19] N. Feng and M. Li, "An information systems security risk assessment model under uncertain environment," *Applied Soft Computing Journal*, vol. 11, no. 7, pp. 4332–4340, 2011.
- [20] N. Feng, H. J. Wang, and M. Li, "A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis," *Information Sciences*, vol. 256, pp. 57–73, 2014.
- [21] Q. Yan, "A security evaluation approach for information systems in telecommunication enterprises," *Enterprise Information Systems*, vol. 2, no. 3, pp. 309–324, 2008.
- [22] P.-Y. Chen, G. Kataria, and R. Krishnan, "Correlated failures, diversification, and information security risk management," *MIS Quarterly*, vol. 35, no. 2, pp. 397–422, 2011.
- [23] J. Pearl, *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan-Kaufmann Publishers, San Mateo, Calif, USA, 1998.