**TELKOMNIKA**, Vol.11, No.1, January 2013, pp. 338~344
e-ISSN: 2087-278X



# E-commerce System Security Assessment based on Bayesian Network Algorithm Research

**Xin Li*, Ting Li**
Computing Center, Liaoning University of Technology
College of Electronics and Information Engieering, Liaoning University of Technology
*Corresponding author, e-mail: lg_lx@163.com

***Abstract***

*Evaluation of e-commerce network security is based on assessment method Bayesian networks, and it first defines the vulnerability status of e-commerce system evaluation index and the vulnerability of the state model of e-commerce systems, and after the principle of the Bayesian network reliability of e-commerce system and the criticality of the vulnerabilities were analyzed, experiments show that the change method is a good evaluation of the security of e-commerce systems.*

***Keywords***: *Bayesian networks, security assessment, vulnerability*



## 1. Introduction

At present, the system safety assessment, especially vulnerability assessment technique has attracted extensive attention of researchers, and it becomes one of the hot research fields of network and system security. The key findings are as follows: Swiler and Phillips proposed analysis model, using the attack graph description of the attacker to the invasion process [1, 2]. The method uses hand-drawn attack graph and analysis results provide a basis for improving the network configuration to achieve the purpose of network defense, but because the shortest path algorithm requires the attacker to know the attack graph structure in advance, and contrary to the actual network attacks, so the accurate needs to be further investigated. Sheyner and Jha generate the automation attack graph [3, 4], using the improved model checker NuSMV to construct the attack graph [5], and Markov decision processes and the steady state distribution to calculate an attacker who successfully completes the maximum attack probability in the minimum security measures. Steven Noel, [6] based on attack graph analysis, proposed minimum cost associated with the costs and security measures, but the lack of the corresponding argument on the applicability of the steady state distribution, especially when a large number of unknown transition probability in the attack graph, Markov decision processes from the analysis results are often large deviation with the correct value. The above methods are taken to attack the idea, to take full account of the lack of other threats to security sources (such as user errors, system failures, etc.), quantitative evaluation method has some limitations. In addition, some studies using fuzzy [7], neural networks [8], the gray theory [9] method to establish an information security assessment model, but mostly focused on the evaluation of the local system, limited to only the technical aspects, and is more common in the theoretical study , but the main drawback is subjective, and too many factors that require human judgment.

To solve the above problem, on the basis of the vulnerability model, this article proposed a system safety assessment method which based on Bayesian networks, and it adopts two indicators of system reliability and weak points as a security quantitative evaluation which based on comprehensive consideration of various security components in the overall system security. It can evaluate the overall system security, optimization theory and data support from the reality, e-commerce system security.

*Received October 2, 2012; Revised November 19, 2012; Accepted December 9, 2012*

## 2. Vulnerability status of an e-commerce systems and evaluation indicators

### 2.1. The vulnerability of the state model of e-commerce systems

Vulnerability modeling is the basis of the vulnerability analysis. Vulnerability - state model of e-commerce system adopts system state as a node, it is much more universal than the attack graph that can be reflected due to system security vulnerabilities, hackers, malicious attacks and network failures caused by security problems and save the state space, so I chose the model as the security of e-commerce systems to assess the quantitative analysis method of the base model.

In this model, the vulnerability of e-commerce systems use a series of transfer steps in the process is broken down into system state, state transition may be due to the hacker to use the vulnerability to attack, the backdoor is triggered operation or network failure. These behaviors to be implemented some of the main conditions, object and environmental conditions. The model also introduces a topology information system used to determine the associated vulnerabilities introduced due to the interconnected and unreasonable trust relationship.

The main consideration of the vulnerability of e-commerce systems modeling: data confidentiality and integrity control mechanism, the signature non-repudiation of control mechanisms, trust models, authentication, key management mechanisms, access control mechanisms, intrusion detection system model, and transaction agreements.

After finishing Vulnerability modeling, you can use the symbolic model to check NuSMV to construct counter-examples, which is contrary to the status of the transfer process of the security attributes, to generate all possible paths to describe the system to reach a state of insecurity vulnerability state diagram (vulnerability status grahpy, VSG).

### 2.2. E-commerce system vulnerability status evaluation indicators

On the basis of the fragile state model, it defines the system reliability and vulnerability of these two vulnerabilities of critical state evaluation index.

(1) System reliability

**Definition 1.** (System reliability) The attack cost of the prescribed conditions and requirements to maintain system security. System reliability index the greater the reliability of the system the higher the better survivability of the systems in complex environments. For the user, means that the use of the e - commerce system security; it means that to achieve the attack purpose is more difficult for the attacker.

(2) Weak point of criticality

**Definition 2.** (Weak point of criticality) The weak point is the existence of the difference of the system reliability can also be understood to enhance the value of the weak point repair, the overall system reliability. A major purpose of the safety assessment of e-commerce system is to optimize the design of e-commerce security features and methods to make recommendations. Meanwhile, the weak point of criticality is also an indicator of the effective assessment of the performance of security methods.

## 3. Bayesian network-based Evaluation Algorithm

### 3.1. Bayesian network

Bayesian network (Bayesian Network) referred to as BN [10], is a directed acyclic graph (Directed Acyclic Graph, the DAG), which consists of nodes representing the variables and to connect these nodes to the edge . One has N nodes, Bayesian networks are available $N = <<V, E> P>$, including two parts:

(1) $< V, E >$ with N nodes represents a directed acyclic graph G. In the node set $V =$ {the $V_1$ and $V_2$ , ... , $V_N$} represents a variable between nodes, directed edges E represents the relationship between the variables Vi parent node collection and a collection of non- descendant nodes, respectively, with pa ($V_i$) and A ($V_i$). $< V, E >$ contains a conditional independence assumption, in a given pa ($V_i$) and $V_i$($V_i$) conditional independence.

(2) P associated with each node the conditional probability distribution (of conditional probabilities distribution, CPD) , to set the top node in the prior probability distribution and conditional probability of non- top node distribution , you can get the joint probability distribution contains all the nodes.

Bayesian networks as a description of the uncertain information of the expert system , expression and analysis of the uncertainty of things , it also has the ability to describe the event

polymorphisms and non-deterministic logical relationship , suitable for the safety of complex systems and reliability , and therefore are increasingly being applied to the system reliability analysis , the field of scientific analysis of the security threat analysis, systems engineering , and achieved fruitful results.

### 3.2. Figure realize the fragility of state based on Bayesian

Vulnerability model of e-commerce systems, reliability is defined as a system to maintain the security of the ability to attack the cost of the prescribed conditions and requirements, the index reflects the degree of vulnerability of e-commerce system. The cost of defining aggressive behavior refers to the time required for the implementation of aggressive behavior, resources, level of knowledge and permission levels, denoted by c. The success rate of attacks recorded is as $\lambda$. The vulnerability of the state diagram consists of three kinds of basic structure, each structure corresponding to the Bayesian network into the reasoning process are given below.

The cost of C exponential distribution function: $F(c) = P\{C \le c\} = 1-e^{-\lambda c}$, where $\lambda$ is the success rate of attacks, $\frac{1}{\lambda} = E(C)$ the average cost of the behavior. The reliability function $R_s(c)$ The aggressive behavior under specified conditions, the provisions of the probability of the cost $C$ for the successful implementation of, $R_s(c) = P\{C>c\}=1-F(c) = e^{-\lambda c}$, where $R_s(c)$ is an e-commerce system reliability function, So $E(c)= \int^{+\infty} R_s(c)dc$ The average attack cost.

Attacker to complete the entire attack process can bear the greatest price for the C, the relationship between the state "and" attacker attained the status of the transfer need to complete the attack, the relationship between the attack cost accumulation; that an attacker completion of the attack for a total consideration is greater than $C$, can be considered in a safe state. Figure 3 shows the structure of the overall reliability function:

$$R_s(c) = 1 - P(C_1 + C_2 + ... + C_n \le c) = \sum_{i=1}^{n} \frac{\prod_{j \ne i} \lambda_j \cdot e^{-\lambda_j c}}{\prod_{j \ne i} (\lambda_j - \lambda_i)} \quad \text{(Assumed } \forall i \ne j \rightarrow \lambda_i \ne \lambda_j \text{)} \quad (1)$$

## 4. Calculation of the E-commerce System Security Assessment

### 4.1. System reliability

General state diagram, the top event probability in the Bayesian network can be equivalent to the dissemination and updating of the probability, given the state of $S_n$ probability distribution can be directly calculated top event T probability:

$$P(T = 1) = \sum_{S_0,...S_{N-1}} P(S_0 = 1, ..., S_{N-1} = 1, T = 1) \quad (2)$$

For the known vulnerability of the state diagram, according to the second formula, the state transition diagram in accordance with the basic structure of the transition probability projections available to the top T- node (final breach of the security attributes of the state node, the corresponding Bayesian network in the top the probability of the event), its integral can be obtained reliability function of the e-commerce system:

$$R_s(c) = \int^{\infty} P(T = 1) dC_i \quad (3)$$

### 4.2. Weak point of criticality

The event probability in the Bayesian network in the bottom refers to wither the end of the event Ei occurs can influence the top event T probability difference between the fragile state diagram, the weak point is the probability of key definition of the weak point was the use of Vi and No violations of security policy events of T (top event) the difference of the probability. That,

$$I_i = R_s(T = 1 \mid V_i = 0) - R_s(T = 1 \mid V_i = 1) \quad (4)$$

Vulnerability status graph nodes correspond to the various states of the e-commerce systems, arcs correspond to the weak point is the use of e - commerce system, in the calculation of $R_S$ ($T = 1 \mid V_i = 0$ ) should be Figure the weak point $V_i$ arc removed , and then the rest of the state diagram to calculate the vulnerability state diagram before and after the change.

In the calculation of the Bayesian network and the fragility of the state diagram, in addition to the top event probability, but also richer information, which is more important is that you can get an vulnerability exploited vulnerabilities to be exploited the posterior probability, namely,

$$P(V_i = 1 \mid V_j = 1) = \frac{\sum_{V_1,...,V_i,V_{i+1},...,V_j,V_{j+1},...V_N} P(V_k = \lambda_k, V_i = 1,...,V_j = 1,\ 1 \le k \le N, k \ne i,\ k \ne j)}{P(V_j = 1)} \quad (5)$$

## 5. Experiments

The e-commerce system security include the physical security, the personnel security, network security and information security, etc, and this paper mainly discussed the methods of information security is, therefore, we use the above vulnerability assessment method for the electronic commerce system of information security evaluation. For this, we constructed as shown in figure 1 shows the experimental environment.

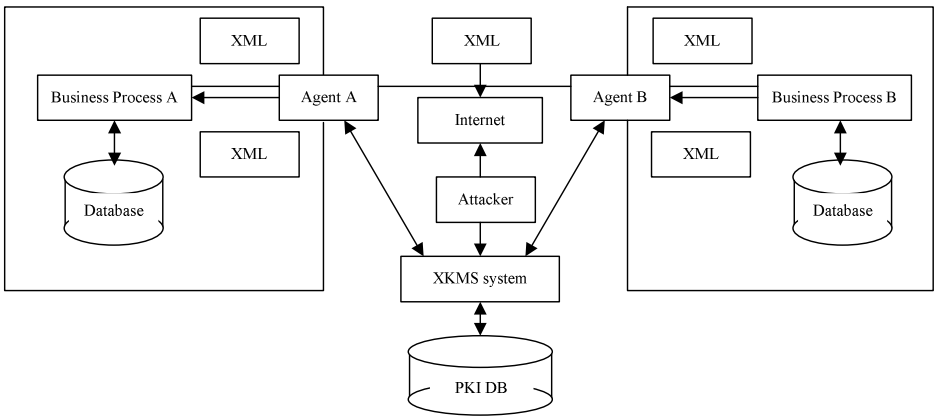


Figure 1. Experimental network environment

In this experiment environment, the attacker purpose is to try to get through all kinds of ways or tamper with the merchants A and B, of the written XML between businesses trading information. Therefore, our security objectives are:

(1) to ensure the confidentiality of the trade information was not stolen and manipulated by the attacker;

(2) to ensure integrity and effectiveness of the digital signature, and non-forge ability.

To ensure that the data of confidentiality in the experiment can make use of the weak points listed in Table 1.

Based on the contrast experiment way, namely for the experimental environment establish three examples model: an example, both parties use of electronic commerce system exists all vulnerable point. Example 2, the use of electronic commerce system contains the weak point V5. Three examples, the use of electronic commerce system contains the weak point V2.

According to the network topology and the figure 1 and table 1 vulnerable point list, by using the model test tools to SPIN [11] three experiment in the configuration of the electronic

commerce system modeling and analyzing respectively. SPIN is a famous analysis verifies the concurrent systems of logical consistency tools to its simplicity and a high degree of automation and much attention. SPIN has been successfully used in the security protocol verification, and control system software verification and validation, optimization planning, etc. Because its process produces the simultaneity, making its distributed network system in the modeling and simulates the concern for more and more researchers.

According to the experimental environment, we can see the path of external attackers : The attacker from the Internet , the radio listening on the Ethernet packets intercepted SOAP message includes the business A and business B transmission between SOAP message XML document there is a confidential vulnerability, an attacker which information may be obtained directly. Otherwise, in order to decrypt or tampering with confidential data in the SOAP message. He needs to get the data encryption key and the signer 's signature private key , or other useful information , this information is available in two ways : one is to use OCSP pre-generated recovery loopholes, through replay attacks by certificate validation , thus posing as parties to the transaction one of them , and then interact with the other party to obtain relevant information , the second is by posing as a third party confirm , in the process of verification of undeniable signature to interact with the verifier , if the agreement does not confirm or deny the undeniable signature scheme with zero knowledge , the attacker could take advantage of access to relevant information . Finally, the key regulatory loop bugs, the encryption key in order to crack the confidential data, or tampering with the data thus pose a threat to the confidentiality of the data.

Table 1. Vulnerability points list

| | Vulnerability names | Vulnerability against categories |
|---|---|---|
| $V_1$ | Access control Bugs | Unauthorized user login/access system |
| $V_2$ | Certificate Validation Vulnerability Bugs | An attacker use the vulnerability OCSP pre- generated reply , resend attack to certificate validation , and then posing as one of the parties to the transaction |
| $V_3$ | Trust vulnerability vulnerability Bugs | Unlimited user access or an attacker posing as members of the trust relationship |
| $V_4$ | Key regulatory loopholes Bugs | Long-term use the same encryption key , allowing the attacker by monitoring the acquisition, and then decrypt confidential data |
| $V_5$ | Data confidentiality and integrity of vulnerability Bugs | Selected encryption mechanism is defective or key compromise , resulting in the attacker from the transaction data of the intercepted forged or tampered with |
| $V_6$ | Undeniable signature verification vulnerability Bugs | Posing as third - party verifier and the authenticator to interact with , the use of non-zero knowledge undeniable signature scheme that may appear in about |

For experiment one, the attacker could take any of these ways to get the tampering expressly transaction information. In the second experiment, the absence of data confidentiality and integrity of the vulnerability, the attacker will try to replay attacks by the certificate validation, thus posing as one of the legitimate parties to the transaction to obtain transaction information or encryption key information in clear text. In Experiment 3, to make up for the OCSP certificate validation vulnerability, an attacker can only be confirmed by posing as the signature third - party agreement to confirm or deny the undeniable signature scheme that may exist in a non-zero knowledge and get some useful information.

For a more comprehensive experimental system vulnerability knowledge, according to SPIN simulation verify the experimental results and the vulnerability of the state model , build fragile state of Figure 2 shows.

### 5.1 Weak point of criticality

According to the vulnerability of state diagrams, network reliability of the three experiments shown in Table 2. By comparing the results for the experimental system the RS1, RS2 to define the success rate of attacks, and its value is less $\lambda$ and $R_{S3}$, which than 1, so

$$\lambda_3' = \lambda_4 \cdot \lambda_5 \cdot \lambda_8, \lambda_4' < \lambda_3'' = \lambda_3''' = \lambda_4 \cdot \lambda_5 < 1$$

and

$$\lambda_2' = \lambda_2'' = \lambda_2 \cdot \lambda_3 < \lambda_2''' = \lambda_3 < 1$$

According to the same upper and lower limits of the integration rules and the integral of the logarithmic function, we can get the rule $R_{S1} < R_{S2} < R_{S3}$.

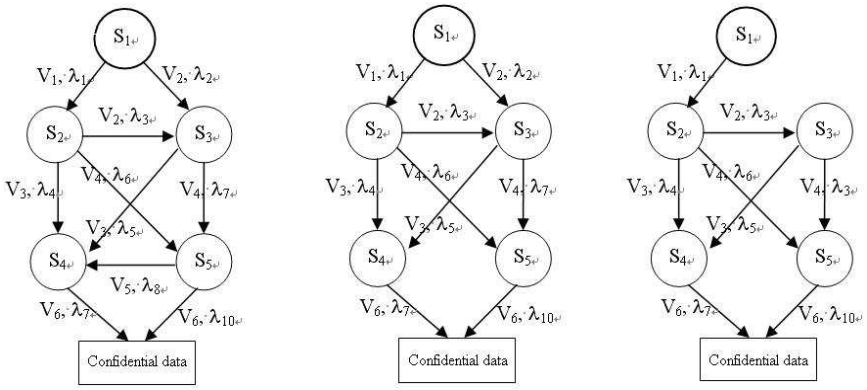


Figure 2. Experimental system vulnerability status graphy

Table 2. Reliability list

| | Reliability function |
|---|---|
| Experiment I | $R_{s_1}(c)=\int_c^{+\infty} e^{-\lambda_1 c_1} e^{-\lambda_2\lambda_3 c_2} e^{-\lambda_4\lambda_5\lambda_8 c_3} e^{-\lambda_6\lambda_7 c_4} e^{-\lambda_9 c_5} e^{-\lambda_{10} c_6} dc_1 dc_2 dc_3 dc_4 dc_5 dc_6$<br>令$\lambda_1'=\lambda_1, \lambda_2'=\lambda_2\cdot\lambda_3, \lambda_3'=\lambda_4\cdot\lambda_5\cdot\lambda_8, \lambda_4'=\lambda_6\cdot\lambda_7, \lambda_5'=\lambda_9, \lambda_6'=\lambda_{10}$<br>$R_{s_1}=\sum_{i=1}^{n}\frac{\prod_{j\neq i}\lambda_j'\cdot e^{-\lambda_j' c}}{\prod_{j\neq i}(\lambda_j'-\lambda_i')}$ |
| Experiment II | $R_{s_2}(c)=\int_c^{+\infty} e^{-\lambda_1 c_1} e^{-\lambda_2\lambda_3 c_2} e^{-\lambda_4\lambda_5 c_3} e^{-\lambda_6\lambda_7 c_4} e^{-\lambda_9 c_5} e^{-\lambda_{10} c_6} dc_1 dc_2 dc_3 dc_4 dc_5 dc_6$, let<br>$\lambda_1''=\lambda_1, \lambda_2''=\lambda_2\cdot\lambda_3, \lambda_3''=\lambda_4\cdot\lambda_5, \lambda_4''=\lambda_6\cdot\lambda_7, \lambda_5''=\lambda_9, \lambda_6''=\lambda_{10}$ $R_{s_2}=\sum_{i=1}^{n}\frac{\prod_{j\neq i}\lambda_j''\cdot e^{-\lambda_j'' c}}{\prod_{j\neq i}(\lambda_j''-\lambda_i'')}$ |
| Experiment III | $R_{s_3}(c)=\int_c^{+\infty} e^{-\lambda_1 c_1} e^{-\lambda_3 c_2} e^{-\lambda_4\lambda_5 c_3} e^{-\lambda_6\lambda_7 c_4} e^{-\lambda_9 c_5} e^{-\lambda_{10} c_6} dc_1 dc_2 dc_3 dc_4 dc_5 dc_6$<br>Let $\lambda_1'''=\lambda_1, \lambda_2'''=\lambda_3, \lambda_3'''=\lambda_4\cdot\lambda_5, \lambda_4'''=\lambda_6\cdot\lambda_7, \lambda_5'''=\lambda_9, \lambda_6'''=\lambda_{10}$ $R_{s_3}=\sum_{i=1}^{n}\frac{\prod_{j\neq i}\lambda_j'''\cdot e^{-\lambda_j''' c}}{\prod_{j\neq i}(\lambda_j'''-\lambda_i''')}$ |

### 5.2 vulnerability criticality analysis

In the critical analysis of vulnerabilities, select the two weak points in the second experiment V2 and V4 to compare:

$$I_4 = R_s(T=1 \mid V_4=0) - R_s(T=1 \mid V_4=1) = 1-R_s(T=1 \mid V_4=1) = 1-R_{s_1}$$

$$I_2 = R_s(T=1 \mid V_2=0) - R_s(T=1 \mid V_2=1) = R_{s_2}-R_{s_1}$$

Visible $I_4 > I_2$ , for the information security of the entire e-commerce system, the weak point V4 than weak point $V_2$, which will lead to greater security threats. Therefore, during the optimization of system security, usually give priority to critical and high vulnerabilities. In addition, we have all the vulnerable points in the Table 7-1 criticality analysis, a weak point of the importance of order of $V_5$, $V_4$ and $V_2$, $V_3$, and $V_6$, the $V_1$.

The above results show that the security measures taken to make information security for e-commerce system to a gradual strengthening trend, quantitative assessment of the vulnerability indicator, combined with the assets, vulnerabilities and repair cost of knowledge in the practical application optimization process for e-commerce systems, the vulnerable point selection, and repair order to provide theoretical and data reference.

## 6. Conclusion

On the basis of analysis and comparison of the vulnerability assessment of existing systems, this paper selected the fragile state of the model to analyze and evaluate the information security of e-commerce systems, Bayesian Networks, and the fragile state of the basic structure of the corresponding relationship, given the method of calculating the quantitative assessment of indicators based on Bayesian network parameters, and with concrete examples to verify the usefulness of the proposed method and characteristics. From the perspective of system vulnerability assessment, vulnerability point critical of two aspects of e-commerce system, a more comprehensive quantitative assessment of reality, e-commerce system optimized to provide the support to the theory and data.

## References

[1] Swiler LP, Phillips C, Gaylor T. A graph-based network vulnerability analysis system. *Technical Report, SANDIA Report No. SAND9723010P1*. 1998.
[2] Swiler LP, Phillips C, Ellis D. Computer attack graph generation tool. *Proceedings of the DARPA Information Survivability Conference and Exposition*. 2001; 2: 307-321.
[3] Sheyner OM. Scenario graphs and attack graphs. Carnegie Mellon University, Ph. D. thesis, 2004.
[4] Sheyner O, Haines J, Jha S. Automated generation and analysis of attack graphs. *Proceedings of IEEE Symposium on Security and Privacy*. 2002; 273-284.
[5] Cimatti A, Clarke E, Giunchiglia F. NuSMV: a new symbolic model verifier. *Proceedings of International Conference on Computer Aided Verification*, 1999. 1633; 495-499.
[6] Noel S, Jajodia S, OpBerry B. Efficient minimum cost network hardening via exploit dependency graphs. *Proceedings of 19th Annual Computer Security Applications Conference*. 2003, 86-95.
[7] Zhu L. B., Dai G. Z. A information security assessment model based on fuzzy comprehensive evaluation. *Journal of Information Security and Communication Secrecy*. 2006; 8(2): 13-15.
[8] Qing Y, Zuo CS, Liu D. A WSNs routing security model based on BP network. *Journal of Software*. 2008; 6(9): 11-13.
[9] Liu P, Liu MH. The application of grey theory in information security assesment model. *Control and Automation*. 2006; 22(12): 95-97.
[10] Murphy KP. A brief introduction to graphical models and bayesian networks. Telkomnika; Indonesian Journal of Electrical Engineering. 2008; 21(2): 164-171.
[11] Bell Labs in the Original Unix Group of the Computing Sciences Research Center. SPIN2formal verification. *Telkomnika; Indonesian Journal of Electrical Engineering*. 2011; 32(11): 101-108.