Information Sciences 256 (2014) 57–73

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis

Nan Feng [a], Harry Jiannan Wang [b], Minqiang Li [a,*]

[a] College of Management and Economics, Tianjin University, 92 Weijin Road, Nankai District, Tianjin 300072, PR China
[b] Department of Accounting and MIS, University of Delaware, Newark, DE, United States

ARTICLE INFO

Article history:
Available online 4 March 2013

Keywords:
Information systems
Security risk
Bayesian networks
Ant colony optimization
Vulnerability propagation

ABSTRACT

With the increasing organizational dependence on information systems, information systems security has become a very critical issue in enterprise risk management. In information systems, security risks are caused by various interrelated internal and external factors. A security vulnerability could also propagate and escalate through the causal chains of risk factors via multiple paths, leading to different system security risks. In order to identify the causal relationships among risk factors and analyze the complexity and uncertainty of vulnerability propagation, a security risk analysis model (SRAM) is proposed in this paper. In SRAM, a Bayesian network (BN) is developed to simultaneously define the risk factors and their causal relationships based on the knowledge from observed cases and domain experts. Then, the security vulnerability propagation analysis is performed to determine the propagation paths with the highest probability and the largest estimated risk value. SRAM enables organizations to establish proactive security risk management plans for information systems, which is validated via a case study.

1. Introduction

As information systems have become more prevalent in business, the consequences of information system security violations have become more and more costly [43]. For example, the 2010 Computer Crime and Security Survey on 738 organizations by the Computer Security Institute reported a total estimated annual loss of $190 million caused by information systems security incidents [20]. Recent literature [3,6,7,34] has also documented significant costs related to information systems security breaches.

As an important part of enterprise risk management (ERM), security risk analysis mainly focuses on analyzing vulnerabilities and threats to the information resources and deciding what countermeasures to take for reducing risk to an acceptable level. However, security risk analysis for information systems is a very challenging task due to the complex and dynamic environment. For example, there often exist complex interactions among the components of information systems. Therefore, any single vulnerability may have multiple propagation paths, leading to different security risks in information systems.

In recent years, the security risk analysis for information systems has attracted much attention of researchers in the field [8,35,28]. The existing approaches for risk analysis can be grouped into three major categories: the quantitative approaches, the qualitative approaches, and the combination of quantitative and qualitative approaches.

* Corresponding author. Tel./fax: +86 22 27404796.
E-mail address: tjufengnan@gmail.com (M. Li).

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.02.036

The quantitative approaches utilize mathematical and statistical models to represent risk [28]. Security risk exposure is represented as a function of the probability of the threats and the expected loss due to the vulnerability to those threats [6]. Gordon and Loeb [19] presented a mathematical model to determine the optimal security investment level for information systems. Their work and subsequent literatures on security risk analysis focused on a single system or a single type of protection technology. Yue et al. [47] extended those studies by formulating and solving the problem according to the risk management paradigm, and therefore provided manager with additional insights into making optimal decisions. Wu et al. [46] analyzed various risks and challenges in the product development of the concurrent engineering environment and proposed a quantitative approach to systematically identifying the most important risks for accomplishing concurrent engineering projects. Grunske and Joyce [21] proposed a risk-based approach that created modular attack trees for each component in information systems. These modular attack trees were specified as parametric constraints, which allowed quantifying the probability of security breaches that occurred due to the internal component vulnerabilities as well as vulnerabilities in the component's deployment environment.

There are also many qualitative security risk analysis methods and techniques. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) approach [1] defines a set of impact evaluation criteria to establish a common basis for determining the impact values due to threats to the critical assets. Peltier [35] presented a qualitative risk analysis process using techniques such as Practical Application of Risk Analysis (PARA) and Facilitated Risk Analysis Process (FRAP) to evaluate tangible and intangible risks. This process allowed for the systematic evaluation on risk, threats, hazards, and concerns, and provided cost-effective measures for lowering risk to an acceptable level. Some other popular qualitative methods are CCTA Risk Analysis and Management Method (CRAMM) developed by the UK Government's Central Computer and Telecommunications Agency (CCTA) and INFOSEC Assessment Methodology (IAM) [15].

Some comprehensive approaches combining both quantitative and qualitative methods have also been proposed [2,38]. Chen et al. [9] applied the similarity measures of generalized fuzzy numbers to deal with fuzzy risk analysis problems. Although this approach is good at processing the ambiguous information by simulating the characteristic of human in making judgments, it is unable to provide the graphical relationships among various security risk factors using flow charts or diagrams. For representing the relationships among risk factors, Fan and Yu [16] developed a Bayesian networks (BNs) based procedure to provide risk analysis support. In their approach, the BN is structured solely based on domain experts' experience. Sun et al. [43] proposed an evidential reasoning approach under the Dempster–Shafer theory for the risk analysis of information systems security, which provides a rigorous, structured means to incorporate relevant security risk factors, related countermeasures, and their interrelationships when estimating security risk in information systems. In addition, sensitivity analyses were performed to evaluate the impact of important parameters on the model's results in this approach. Models that are implemented incorrectly or developed based on questionable assumptions are vulnerable to model risks [45]. Wu and Olson [45] summarized a series of model risks in financial services industry and demonstrated an effective means to mitigate such risks through predictive scorecards.

The approaches aforementioned have contributed a great deal to the development of security risk analysis. However two issues need to be further investigated in the field of information systems security risk management. First, in the process of security risk analysis for information systems, models are built in order to analyze and better understand the security risk factors and their causal relationships in real-world information systems. Establishing an appropriate model suitable for the target security risk problem is a crucial task that ultimately influences the effectiveness of risk analysis results. Existing literature [9,16] either assumes that the structure of the model was provided by domain experts or was chosen from some general well-known class of model structures. Therefore, how to leveraging both the database of observed cases and domain experts' experience to construct a representative model for observed information systems is a critical issue in security risk analysis.

Second, one security vulnerability could propagate and escalate through the causal chains of security risk factors via multiple paths, leading to different security risks in information systems. Existing approaches largely focuses on risk probability and severity without considering vulnerability propagation. Therefore, there is an imperative need for advanced vulnerability propagation analysis tools that can help establish proactive security risk management plans for information systems.

To address challenges aforementioned, we propose a security risk analysis model (SRAM) in this paper based on Bayesian networks and ant colony optimization. SRAM extends existing work by constructing the BNs using both the database of observed cases and domain experts' experience. Then, security risk assessment is performed to deduce the occurrence probabilities and the consequence severities of security risks. After that, the vulnerability propagation paths are calculated using ant colony optimization to provide guidance for developing security risk treatment plans.

The rest of this paper is organized as follows: Section 2 reviews theoretical backgrounds in this study. After that, we discuss the process for developing the SRAM in detail. The model is further demonstrated and validated in Section 4 via a case study. We compare our model with other related approaches and discuss its limitations in Section 5. Finally, we summarize our contributions and point out further research.

2. Theoretical backgrounds

The SRAM is based on Bayesian networks and ant colony optimization, which are introduced in this section.