Cluster Comput (2007) 10: 47–55
DOI 10.1007/s10586-007-0002-2

A fuzzy outranking approach in risk analysis of web service security

Ping Wang · Kuo-Ming Chao · Chi-Chun Lo · Chun-Lung Huang · Muhammad Younas

Published online: 24 March 2007

Abstract Risk analysis is considered as an important process to identify the known and potential vulnerabilities and threats in the web services security. It is quite difficult for users to collect adequate events to estimate the full vulnerabilities and probability of threats in the Web, due to the rapid change of the malicious attacks and the new computer's vulnerabilities. In this paper, a fuzzy risk assessment model is developed in order to evaluate the risk of web services in a situation where complete information is not available. The proposed model extends Pseudo-Order Preference Model (POPM) to estimate the imprecise risk based on richness of information and to determine their ranking using a weighted additive rule. A case study of a number of web services is presented in order to test the proposed approach.

P. Wang (✉)
Department of MIS, Kun Shan University of Technology, Tainan, Taiwan
e-mail: pingwang@mail.ksu.edu.tw

K.-M. Chao
Software School, Fudan University, Shanghai, China
Faculty of Engineering and Computing, Coventry University, Coventry, UK
e-mail: k.chao@coventry.ac.uk

C.-C. Lo · C.-L. Huang
Institute of Information Management, National Chiao Tung University, Hsinchu, Taiwan

C.-C. Lo
e-mail: cclo@faculty.nctu.edu.tw

C.-L. Huang
e-mail: clhuang@iim.nctu.edu.tw

M. Younas
Department of Computing, Oxford Brookes University, Oxford, UK
e-mail: m.younas@brookes.ac.uk

Keywords Fuzzy outranking · Risk analysis · Web services security · Pseudo-order · POPM

1 Introduction

Web services, based on software technologies such as WSDL, SOAP, XML, UDDI, provide an environment for dynamic discovery and integration of new and pre-existing software components which are distributed across the Web [24]. Web services are increasingly used to automatically perform a variety of business tasks including business-to-client and business-to-business transactions. Though web services provide novel means for conducting online business they create new research challenges such as dynamic discovery and integration of component services, performance, reliability, trust, security and risk analysis. This paper investigates into the risk analysis of web services security. Our literature survey identifies that a limited work has been done on the risk assessment of the web services security. Risk assessment assists experts to identify the existing and potential threats and measure the risk level (i.e., high, medium and low risk) in order to prevent losses pertaining to monetary, resources reputation and business opportunities.

According to a recent survey [1] there was a total flip with 95 percent of responding organizations experiencing more than 10 web site incidents. Another survey of 2004 found that 89 percent of those organizations experienced more than 10 such incidents [1]. Consequently, 61% enterprises lead to financial losses, with a total loss of $130,104,542. In addition, it shows that the top three categories of losses—i.e., viruses, unauthorized access and theft of proprietary information—swamped the losses from all other categories. Web security tools must ensure that corporate data remains confidential, integrated, available, and accountable from

Table 1 A summary of security threats on the webs (modified version of [2])

	Threats	Consequences	Countermeasures
Integrity	·Modification of user data ·Malicious code attack ·Modification of memory or message traffic in transit	·Loss of information ·Compromise of machine ·Vulnerability to all other threats	·Cryptographic checksums
Confidentiality	·Eavesdropping on the Net ·Theft of info from server ·Theft of data from client ·Info about network configuration ·Info about which client talks to server	·Loss of information ·Loss of privacy	·Encryption, Web proxies
Denial of service	·Killing of user threads ·Flooding machine with bogus threats ·Filling up disk or memory ·Isolating machine by DNS attacks	·Disruptive ·Annoying ·Prevent user from getting work done	·Difficult to prevent
Authentication	·Impersonation of legitimate users ·Data forgery	·Misrepresentation of user ·Belief that false information is valid	·Cryptographic techniques
Access control	·Data replication or modification	·Loss of information	·Users access management
Availability	·Storage damage or system crash ·Nature disasters	·Disruptive ·System damage	·System backup ·Physical improvement

unauthorized access. Web services security can be threatened from different directions such as integrity, confidentiality, denial of service, authentication, and access control. Table 1 summarises related threats and their consequences [2].

A number of security technologies and tools have been developed to prevent web security threats. The available security techniques [2, 3] including firework, Intrusion Detection System (IDS) security tokens, digital signature, key management, Secure Sockets Layer (SSL), Secure Electronic Transaction (SET), and XML encryption techniques have been already employed to authenticate and protect business transaction from unauthorized access. However, most of the new techniques for web security such as two-factor authentication, encrypted XML data exchange [4, 5] distributed access control [6], and Secure SOAP traffic [7], are based on the known threats. They neglect the risk arising from potential attack, which leads to lose the war of defense.

Obviously, the risk analysis for web service security is not only limited to calculate the recognized web threats, but should also estimate potential risks. In fact, it is difficult for decision makers to identify the entire network threats and to collect precise and adequate events to estimate all probable vulnerabilities of threats. Risk analysis is a complex process which links to substantial ambiguous and uncertain information. The traditional risk analysis approaches are not readily applicable to web services, due to the assumptions of known threats and vulnerabilities. This paper extends Pseudo-Order Preference Model (POPM) to estimate the imprecise risk on alternatives depending on richness of incomplete information. Accordingly, it presents a new scheme to measure the potential risk of web services. The aim is to make valuable recommendations for web services providers so that they can improve the security of their services.

The paper is structured as follows. Sect. 2 reviews related work. Section 3 presents the proposed model. A case study, based on a number of web services and security measures, is given in Sect. 4. Section 5 discusses the experimental results which are based on the case study. Section 6 concludes the paper and identifies future work.

2 Related work

Various approaches have been made to address web (services) security issues. Damiani et al. [4] discuss various approaches in relation to web services security such as W3C XML-signature syntax and processing, Security Assertion Markup Language (SAML), and eXtensible Access Control Markup Language (XACML). The aim is to identify ways in which these approaches can be utilized in providing web services with secure infrastructure. Similarly, Naedele [5] reviews various security standards for XML and web services such as SAML, XACML, XML DSig (digital signature), XML Enc (encryption) and so on. The author illustrates the dependencies between these standards and the issues (such as confidentiality, integrity, access control) they address. Bhargavan et al. [7] develop mechanisms to refine WS-Trust and WS-Secure Conversation using a formal scripting language for security protocols. The contribution of this work is claimed to provide a formal approach which can be used during standardization process in order to verify security properties of a particular security approach.

In addition to above, many researchers and organizations have studied information security and network risk assessment to assist information security managers in decision making. Carroll (1983) [8] proposed a familiar approach that uses the 'Annual Loss Expectancy (ALE)' to calculate the security level of an information asset by simply multiplying the Annual Rate of Occurrence (ARO) with the Single Loss Expectancy (SLE), Exposure Factor (EF) and the monetary value of assets. It could be extended to evaluate the security of distributed network by aggregating all components' ALE. Furthermore, ISO13355 ISO/IEC TR13355-1 [9] provides qualitative models for risk assessment of organizations. Lee (1996) [10] and Chen (2001) [11] introduced a qualitative risk assessment method with fuzzy multi-criteria decision-making theory.

Koller (2000) [12] analyzed classical mathematical methods and comprehensively classified the existing methods into five types: (1) Discriminant Function Analysis (DFA), (2) Bayesian analysis, (3) Decision tree technique, (4) Factor analysis, and (5) Neural nets. Moreover, other well-known techniques for modeling risk assessment include the Hazard operable process, fault tree analysis, the Consultative Objective Risk Analysis System (CORAS), Consultative Objective and Bi-functional Risk Analysis (COBRA), etc.

However, the above quantitative and classical mathematical methods suit the situations wherein security data is precise and the data form is crisp. The risk analysis of web services security often holds under uncertainty situations with incomplete data due to the rapid change of the emerging malicious attacks and the new computer's vulnerabilities in the Web. For example, it is difficult to numerically quantify the estimation of data being modified due to the lack of encryption protection. We believe that such estimation can be more appropriately modeled and evaluated using fuzzy variables. In this paper we therefore employ fuzzy logic to construct a parameter-driven risk analysis model for measuring web services security.

3 The proposed model

Our proposed method is based a new resolution process of risk assessment which consists of the POPM (Pseudo-Order Preference Model) [13] and RMGDP (Resolution Method for Group Decision Problems) [14–17]. The POPM is an outranking approach which allows decision makers to represent their imprecise preference in strict preference, weak preference, or indifference based on richness of information and then prioritizes the ranking of alternatives in partial order or complete order relation using non-dominant set and dominant set.

The RMGDP is incorporated with POPM to resolve the group difference and obtain a collective preference relation as group preferences. It can be divided into the following three steps: (1) transformation process, i.e., to transform the individuals' opinions into preference values, (2) aggregation process, i.e., to aggregate the individual preference values to obtain the group preference for all decision makers, and (3) exploitation process, i.e., to compute the ranking of the alternatives by group preference. These steps are explained as follows:

Assume that a group of decision makers, $d_k (k = 1, \dots, m)$, is formed as an evaluation committee. Each decision maker (DM) has to evaluate a set of alternatives a_i and a_j $(i, j = 1, \dots, n)$, based on a set of criteria c_l $(l = 1, \dots, q)$ with their relative importance and then assign rating $\tilde{x}_i^k, \tilde{x}_j^k$ to the alternatives a_i and a_j. $P(\tilde{x}_i^k, \tilde{x}_j^k)$ denotes that the d_k allocates preference degree of alternative a_i over alternative a_j. The proposed method allows the decision makers to express their imprecise risk in linguistic quantifiers considering potential threats and explicitly represent them with fuzzy numbers.

3.1 Transformation process

A transfer function, f, is applied to convert individual rating of alternatives to a preference relation as follows [18]:

$$p_{ij}^k = f\left(\tilde{x}_i^k, \tilde{x}_j^k\right) = \frac{1}{2}\left(1 + \left(\tilde{x}_i^k \Theta \tilde{x}_j^k\right)\right), \tag{1}$$

where p_{ij}^k characterizes the preference degree between alternative a_i and a_j expressed by d_k and Θ is the subtraction operation on two fuzzy numbers.

According to Pseudo-order preference model [13], there are three fundamental preference relations in the classical preference structure. These relations are: (1) Strict preference (**P**), (2) Weak preference (**Q**) and (3) Indifference (**I**) which can be applied to determine an imprecise preference relation based on the richness of risk information. **P**, **Q**, and **I** reveal the imprecise preference degree between alternative a_i and a_j expressed (by d_k) as follows:

Strict preference relation $(a_i P a_j)$:

$$P_{ij}^k - p_{ji}^k > p. \tag{2}$$

Weak preference relation $(a_i Q a_j)$:

$$q < P_{ij}^k - p_{ji}^k \leq p. \tag{3}$$

Indifference relation ($a_i I a_j$):

$$|P_{ij}^k - p_{ji}^k| \leq q, \tag{4}$$

where the preference threshold p and indifference threshold q are defined to distinguish between strict preference, weak preference, and indifference relations. When the difference between $\tilde{x}_i^k$ and $\tilde{x}_j^k$ exceeds p, it indicates that $\tilde{x}_i^k$ is strictly preferred to $\tilde{x}_j^k$. Similarly, if the difference between $\tilde{x}_i^k$ and $\tilde{x}_j^k$ is smaller than q, it means that $\tilde{x}_i^k$ and $\tilde{x}_j^k$ are not regarded as significantly different.

The POPM can flexibly characterize decision maker's imprecise preference, but it decides the preference structure without considering the weighting (relative importance) of alternative. Hence two useful modified models are proposed in this paper—Semi-Order Preference Model (SOPM) and Complete-Preorder Preference Model (CPPM). These are derived from [19] in order to develop an appropriate method for risk assessment.

SOPM is a special case when $p = 0, q \neq 0$. It is applied to obtain the outranking relation between alternatives when the relative importance of each alternative is predictable. Weak preference relation is neglected, and only the indifference threshold is employed to discriminate the preference or indifference relation. The relations between two alternatives (a_i, a_j) for a specific decision maker d_k are shown as follows:

$\forall a_i \quad \text{and} \quad a_j \in A.$

Preference relation:

$$P_{ij}^k - p_{ji}^k > q. \tag{5}$$

Indifference relation:

$$|P_{ij}^k - p_{ji}^k| \leq q, \tag{6}$$

where indifference threshold q is defined in order to distinguish the preference degree between a_i and a_j.

CPPM is used for obtaining a complete order for alternatives when a decision maker can express his/her explicit preference on alternatives in a precise matter. It is also a special case of POPM, when $p = 0$, $q = 0$, where no threshold is used. In general, the decision maker is likely to obtain a complete order relation on alternatives when precise and sufficient information is gathered.

3.2 Aggregation process

Assume that the relative importance of each decision maker is given, the collective preference (P_{ij}^c), an aggregation of the individual preferences $\{p_{ij}^1, \ldots, p_{ij}^m\}$($m$ is the number of decision makers), for the set of $d_k (k = 1, \ldots, m)$ can be aggregated by the weighted sum of P_{ij}^k as,

$$P_{ij}^c = \sum_{k=1}^m w_k \cdot P_{ij}^k, \sum_{k=1}^m w_k = 1. \tag{7}$$

Once P_{ij}^c is obtained, decision makers could prioritise the ranking of alternatives based on group preference using the exploitation process detailed in the following section.

3.3 The exploitation process

The exploitation process is a consequence of identifying the priority of alternatives of group preference. Three preference models are introduced to discriminate the ranking of alternatives as follows:

3.3.1 Pseudo-order preference model

When the relative importance of decision maker is absent, the outranking relation is defined as follows [13]:

Outranking relation ($a_i S a_j$):

$$a_j P a_i \text{ is false, and } |A| + |B| > |C|, \tag{8}$$

where $A = \{a_i P a_j\}$, $B = \{a_i Q a_j\}$, $C = \{a_j Q a_i\}$.

Incomparability relation ($a_i R a_j$):

$$\textit{otherwise} \tag{9}$$

$|x|$ represents the cardinality of the finite set $x = \{A, B, C \ldots\}$. From Eq. (8), we see that a_i outranks a_j if no criterion supports that a_j is strictly preferred to a_i, and the number of assessments which support that a_i is strictly preferred to a_j, is more than the number of assessments, which consider that a_j is weakly preferred to a_i. Otherwise, a_i is incomparable to a_j [19].

3.3.2 Semi-order preference model

When the relative importance of decision maker is given, the outranking relation is defined as:

Outranking relation ($a_i S a_j$):

$$P_{ij}^c - P_{ji}^c > q. \tag{10}$$

Incomparability relation ($a_i R a_j$):

$$|P_{ij}^c - P_{ji}^c| \leq q. \tag{11}$$

From Eq. (10), we see that a_i outranks a_j, if the difference between weighted sum of P_{ij}^k and P_{ji}^k is greater than q. Otherwise, a_i is incomparable to a_j. According to [13], this model is extended to identify the partial-order ranking of alternatives which might be more rational than the original approach. The outranking relation of the original approach $(a_i S a_j)$, is that $a_j P a_i$ is false and $\sum_{j \in X} w_j > \sum_{k \in y} w_k$. It considers outrank relation as two conditions (i.e., preference relation P and sum of weighting) must hold true at same time. However, this rule may be excessively strict for two consecutive alternatives and it may lead to having too many incomparability relations and lowering the discrimination capability. Hence we use Eq. (10) as the outrank function.

3.3.3 *Complete-preorder preference model*

When precise and sufficient information is gathered, the outranking relation can be judged using two well-known fuzzy ranking indexes—Non-Dominance Degree and Dominance Degree.

Dominance Degree The Dominance Degree (DD) can quantify the dominance that a_i has preference degree over all others where a_j $(j = 1, \dots, n)$. As a result, it is used for prioritizing the ranking order with collective preference defined in Eq. (12)

$$u_{DD}(a_i) = \frac{1}{n-1} \sum_{\substack{j=1 \\ j \neq i}}^{n} p_{ij}^{c}. \tag{12}$$

Non-Dominance Degree Orlovsky (1978) [20] developed a method for fuzzy ranking by means of fuzzy preference relations. The method determines the best alternative by group preferences. The Non-Dominance Degree (NDD) of fuzzy ranking can be calculated by individual preference relation, which is formulated as follows:

$$u_{NDD}(a_i) = \frac{1}{n-1} \sum_{\substack{j=1 \\ j \neq i}}^{n} (1 - d_{ji})$$

$$d_{ji} = \max\left\{p_{ji}^{c} - p_{ij}^{c}, 0\right\}. \tag{13}$$

By applying Non-Dominance Degree and Dominance Degree, the outranking relation is defined as:

Outranking relation $(a_i S a_j)$:

$$u_{DD}(a_i) > u_{DD}(a_j). \tag{14}$$

Indifference relation $(a_i I a_j)$:

$$u_{DD}(a_i) = u_{DD}(a_j), \tag{15}$$

where $u_{NDD}(a_i)$ is used for identifying the best alternative that can validate the ranking results of $u_{DD}(a_i)$.

Table 2 Linguistic scale for weight of security criteria

Linguistic scale	Quantitative scale
Very Important (VI)	5
Rather Important (RI)	4
Important (I)	3
Less Important (LI)	2
Unimportant (U)	1

Table 3 Weightings of 11 security criteria

Criterion	Quantitative scale	Normalized weight
c_1	5	0.114
c_2	4	0.091
c_3	5	0.114
c_4	3	0.068
c_5	4	0.091
c_6	4	0.091
c_7	3	0.068
c_8	4	0.091
c_9	4	0.091
c_{10}	3	0.068
c_{11}	5	0.114

4 Risk assessment: a case study

In this section a case study of risk analysis for web services is given in order to test the validity of the proposed approach. The case study comprises five web services which are evaluated by a group of decision makers d_k $(k = 1, \dots, 6)$ according to six security factors including integrity, confidentiality, authenticity denial of service, access control and availability [2]—which are evaluated using the following eleven subcriteria C_l $(l = 1, \dots, 11)$.

The five web services used in this case study include: a ticket selling web service (a_1), two travel agent web services (a_2 and a_3), a civil lodge web service (a_4), and hotel booking web service (a_5). These are evaluated through the eleven security criteria including: web security policy (c_1), information security framework (c_2), digital signature (c_3), XML encryption (c_4), system fault-tolerance (c_5), user access management (c_6), disaster recovery (c_7), key management (c_8), privacy preferences management (c_9), system log audit (c_{10}), user authentication (c_{11}). These criteria, derived from major security techniques [2, 21, 22], are employed to evaluate the risk analysis method.

The relative weightings of the above security criteria w_l $(l = 1, \dots, 11)$ are evaluated with linguistic scale [23] listed in Table 2, and the normalized weightings for all criteria are calculated and given in Table 3.

Table 4 Linguistic scales for the risk rating

	Items										
Assets	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}
a_1	M	M	H	H	M	H	M	M	M	H	H
a_2	M	H	VH	M	M	H	M	M	H	M	H
a_3	M	H	H	M	M	H	M	M	H	H	M
a_4	L	H	H	VH	M	M	M	H	VH	M	M
a_5	M	H	M	H	H	VH	M	M	H	M	M

Table 5 Linguistic scale for the risk rating

Linguistic scale	Membership function
Very Low (VL)	(0.0,0.1,0.3,0.5)
Low (L)	(0.1,0.3,0.5,0.7)
Medium (M)	(0.3,0.5,0.7,0.9)
High (H)	(0.5,0.7,0.9,1.0)
Very High (VH)	(0.7,0.9,1.0,1.0)

The risk rating of alternative a_i with respect to risk criterion c_l is given by the $n \times q$ fuzzy risk evaluation matrix $\widetilde{V} = \{\tilde{v}_{il} | i = 1, \ldots, n; l = 1, \ldots, q\}$. The decision makers assign the linguistic scale to fuzzy evaluation matrix $\widetilde{V}$ (shown in Table 4), using five-level linguistic scales. These scales can be transformed into numeric form through the fuzzy membership function, as depicted in Table 5.

According to [10, 11], the aggregative rating of risk of an information asset a_i assessed by d_k is given by

$$\tilde{x}_i^k = \left(\left(\tilde{v}_{i1}^k \otimes w_1^k\right) \oplus \ldots \oplus \left(\tilde{v}_{iq}^k \otimes w_q^k\right)\right), \tag{16}$$

where $\oplus$, $\otimes$ are the addition and multiplication operations for fuzzy numbers. By applying Eq. (16), the aggregative ratings of risk for each alternative are calculated.

After obtaining the aggregative ratings of risk for each decision maker, we apply group decision theory to aggregate group ratings by three steps [14] and prioritize the ranking as follows.

4.1 Step 1: transformation process

For each of the six decision makers, his/her preference rating on five alternatives is converted to fuzzy preference relation using Eq. (1):

$$p_{ij}^1 = \begin{bmatrix} 0.50 & 0.280 & 0.500 & 0.580 & 0.710 \\ 0.720 & 0.50 & 0.72 & 0.800 & 0.930 \\ 0.500 & 0.280 & 0.50 & 0.580 & 0.710 \\ 0.420 & 0.200 & 0.420 & 0.50 & 0.630 \\ 0.420 & 0.070 & 0.290 & 0.370 & 0.50 \end{bmatrix}$$

$$p_{ij}^2 = \begin{bmatrix} 0.50 & 0.175 & 0.230 & 0.395 & 0.455 \\ 0.825 & 0.50 & 0.555 & 0.720 & 0.780 \\ 0.770 & 0.445 & 0.50 & 0.665 & 0.725 \\ 0.605 & 0.280 & 0.335 & 0.50 & 0.560 \\ 0.605 & 0.220 & 0.275 & 0.440 & 0.50 \end{bmatrix}$$

$$p_{ij}^3 = \begin{bmatrix} 0.50 & 0.250 & 0.335 & 0.345 & 0.545 \\ 0.750 & 0.50 & 0.585 & 0.595 & 0.795 \\ 0.665 & 0.415 & 0.50 & 0.510 & 0.710 \\ 0.655 & 0.405 & 0.495 & 0.50 & 0.700 \\ 0.655 & 0.205 & 0.290 & 0.300 & 0.50 \end{bmatrix},$$

$$p_{ij}^4 = \begin{bmatrix} 0.50 & 0.310 & 0.485 & 0.545 & 0.625 \\ 0.690 & 0.50 & 0.685 & 0.735 & 0.815 \\ 0.505 & 0.315 & 0.50 & 0.550 & 0.630 \\ 0.455 & 0.265 & 0.450 & 0.50 & 0.580 \\ 0.455 & 0.185 & 0.370 & 0.420 & 0.50 \end{bmatrix}$$

$$p_{ij}^5 = \begin{bmatrix} 0.50 & 0.320 & 0.550 & 0.510 & 0.380 \\ 0.680 & 0.50 & 0.730 & 0.690 & 0.560 \\ 0.450 & 0.270 & 0.50 & 0.650 & 0.330 \\ 0.490 & 0.310 & 0.540 & 0.50 & 0.370 \\ 0.490 & 0.440 & 0.670 & 0.630 & 0.50 \end{bmatrix}$$

$$p_{ij}^6 = \begin{bmatrix} 0.50 & 0.075 & 0.310 & 0.340 & 0.465 \\ 0.925 & 0.50 & 0.735 & 0.765 & 0.890 \\ 0.690 & 0.265 & 0.50 & 0.530 & 0.6550 \\ 0.660 & 0.235 & 0.470 & 0.50 & 0.625 \\ 0.660 & 0.110 & 0.345 & 0.375 & 0.50 \end{bmatrix}$$

4.2 Step 2: aggregation process

It is assumed that the relative importance of six decision makers is determined by his/her job experiences and roles of jobs, and the normalized weights are given as $w_k = [0.1, 0.15, 0.20, 0.15, 0.20, 0.10]$. All preference relations can be aggregated to calculate the collective preference relation (p_{ij}^c) using Eq. (7).

$$p_{ij}^c = \begin{bmatrix} 0.50 & 0.210 & 0.329 & 0.341 & 0.395 \\ 0.600 & 0.50 & 0.524 & 0.547 & 0.604 \\ 0.488 & 0.288 & 0.50 & 0.421 & 0.489 \\ 0.468 & 0.261 & 0.385 & 0.50 & 0.459 \\ 0.468 & 0.207 & 0.322 & 0.345 & 0.50 \end{bmatrix}$$

4.3 Step 3: exploitation process

4.3.1 Pseudo-order preference model

When the preference threshold $p = 0.85$ and indifference threshold $q = 0.25$ are adopted [19], the non-dominance set and dominance set are obtained according to Eqs. (8), (9): $S_{NDD} = \{a_2\}, \{a_3\}$, and $S_{DD} = \{a_4, a_5, a_1\}$. It is obvious that alternatives 2 and 3 outrank alternatives 4, 5, and 1.

4.3.2 Semi-order preference model

Assume that indifference threshold $q = 0.10$, decided by sensitivity analysis, the non-dominance set and dominance set are obtained according to Eqs. (10), (11): $S_{NDD}(a_i) = \{a_2\}, \{a_3, a_4\}$ and $S_{DD}(a_i) = \{a_1, a_5\}$. Clearly, the risk ranking of alternatives 2, 3, and 4 outranks alternatives 1 and 5. Sensitivity analysis of *p, q* for pseudo-order and preference model semi-order preference model will be discussed in Sect. 5.

4.3.3 Complete-preorder preference model

In order to obtain the "best" alternative and the complete order of each alternative, the dominance degree (DD) and the non-dominance degree (NDD) are calculated as follows:

Dominance Degree (DD) The dominance degree of alternatives is calculated using Eq. (12) as:

	a_1	a_2	a_3	a_4	a_5
$u_{DD}(a_i)$	0.318	0.569	0.421	0.393	0.336

Obviously, the risk ranking of alternatives is $a_2 \succ a_3 \succ a_4 \succ a_1 \succ a_5$.

Non-dominance Degree (NDD) By applying Eq. (13), the non-dominance degree of alternatives is shown as follows:

	a_1	a_2	a_3	a_4	a_5
$u_{NDD}(a_i)$	0.812	1.000	0.941	0.919	0.831

Clearly, the corresponding maximal set of *NDD* is $S_{NDD}(a_i) = \{a_2\}$. From the computational results of Eqs. (12), (13), we conclude that the complete order of alternatives is:

$a_2 \succ a_3 \succ a_4 \succ a_1 \succ a_5$

5 Discussion of the results

In Pseudo-Order Preference Model, the preference threshold, p, is set to 0.85 and the indifference threshold q is set to 0.25, respectively. Alternatives 2 and 3 outranks alternatives 4, 5, and 1. The selection of two thresholds may be changed by the different confidence-level of decision makers. If decision makers have precise and sufficient information, they might increase the value of the preference threshold and discrimination capability, and vice versa. The higher preference threshold implies that the decision makers have higher confidence levels.

Table 6 Sensitivity analysis for semi-order preference structure

q	Preference structure
0.40	$S_{NDD} = \{a_2, a_3, a_4, a_5, a_1\}$, $S_{DD} = \{\}$
0.35	$S_{NDD} = \{a_2, a_3, a_4\}$, $S_{DD} = \{a_5, a_1\}$
0.30	$S_{NDD} = \{a_2, a_3\}$, $S_{DD} = \{a_4, a_5, a_1\}$
0.20	$S_{NDD} = \{a_2\}$, $S_{DD} = \{a_4, a_3, a_5, a_1\}$
0.10	$S_{NDD}(a_i) = \{a_2\}, \{a_3, a_4\}$, $S_{DD}(a_i) = \{a_5, a_1\}$

In semi-order preference model, the selection of indifference threshold q is an important issue. From Table 6, we know that the choice of value for q will affect the preference structure of SOPM. If the indifference threshold is decreased, then the discrimination capability is increased and the non-dominant set becomes smaller. For example, only alternative 2 locates in non-dominance set when q resides in [0.1,0.2], otherwise, alternatives 2, 3, and 4 could be selected when $q = 0.35$.

It is observed that the discrimination capability of pseudo-order preference model is decided by two thresholds, which might be affected by the preciseness and completeness of data collection. Consequently it will influence the confidence levels of the decision makers.

6 Conclusions

Web service security is an important issue for e-Commerce. How to assess risk in web service security breaches and their potential damage is a challenging task, due to insufficient information available. The problem is compounded by the existence of vague information in the decision making process. In order to overcome the inadequacy of the existing approaches, the proposed method incorporates a pseudo–order preference model and fuzzy logic to measure the risk of web service security problem under imprecise and incomplete information situation. Consequently, our approach explores imprecise preference structure of risk evaluation and objectively outranks the security of web services. In this paper, an example of an e-Commerce application was used to illustrate that the importance of potential risks can be classified according to a group of experts' opinions with various confidence levels. Future work will focus on the rational selection of the preference threshold and indifference threshold, and will address the relationship between two thresholds and confidence levels of decision makers.

Acknowledgement This research is partially supported by grant No. NSC 95-2416-H-168-007 from the National Science Council of the Republic of China.

References

1. 2005 CSI/FBI Computer crime and security survey. www.usdoj.gov/criminal/cybercrime/FBI2005.pdf, May 2006
2. William, S.: In: Cryptography and Network Security: Principles and Practice, 2nd edn., pp. 441–473. Prentice Hall, London (1999)
3. Maiwald, E.: Network Security: a Beginner's Guide. McGraw-Hill, New York (2001)
4. Damiani, E., Vimercati, S.D.C., Samarati, P.: Towards securing XML web services. In: Proceedings of the 2002 ACM Workshop on XML security, November, 2002
5. Naedele, M.: Standards for XML and web services security. Comput. **36**(4), 96–98 (2003)
6. Kraft, R.: Designing a distributed access control processor for network services on the Web. In: Proceedings of the 2002 ACM Workshop on XML security, November, 2002
7. Bhargavan, K., Corin, R., Fournet, C., Gordon, A.D.: Secure sessions for web services. In: Proceedings of the 2004 Workshop on Secure Web Service (SWS '04), October, 2004
8. Carroll, J.M.: Decision support for risk analysis. Comput. Secur. **2**(3), 230–236 (1983)
9. ISO/IEC 13335-1:2004: Management of information and communications technology security—Part 1: Concepts and models for information and communications technology security management
10. Lee, H.M.: Group decision making using fuzzy sets theory for evaluating the rate of aggregative risk in software development. Fuzzy Sets Syst. **80**(3), 261–271 (1996)
11. Chen, S.-M.: Fuzzy group decision making for evaluating the rate of aggregative risk in software development. Fuzzy Sets Syst. **18**, 75–88 (2001)
12. Koller, G.R.: Risk Assessment and Decision Making in Business and Industry: a Practical Guide. CRC, London (2000)
13. Roy, B., Vincke, P.H.: Relational system of preference with one or more pseudo-criteria: some new concepts and results. Manag. Sci. **30**(11), 1323–1335 (1984)
14. Chiclana, F., Herrera, F., Herrera-Viedma, E.: Integrating three representation models in fuzzy multipurpose decision making based on fuzzy preference relations. Fuzzy Sets Syst. **97**, 33–48 (1998)
15. Chiclana, F., Herrera, F., Herrera-Viedma, E.: A classification method of alternatives for multiple preference ordering criteria based on fuzzy majority. J. Fuzzy Math. **34**, 224–229 (1996)
16. Herrera, F., Herrera-Viedma, E., Verdegay, J.L.: A rational consensus model in group decision making using linguistic assessments. Fuzzy Sets Syst. **88**, 31–49 (1997)
17. Kacprzyk, J., Fedrizzi, M.: A human-consistent degree of consensus based on fuzzy logic with linguistic quantifiers. Math. Soc. Sci. **18**, 275–290 (1989)
18. Tanino, T.: Fuzzy preference ordering in group decision making. Fuzzy Sets Syst. **12**, 117–131 (1984)
19. Wang, J.: A fuzzy outranking approach for design evaluation in conceptual design. Int. J. Pro. RES **35**(4), 995–1010 (1997)
20. Orlovski, S.A.: Decision-making with a fuzzy preference relation. Fuzzy Sets Syst. **1**, 155–167 (1978)
21. Holgersson, J., Soderstrom, E.: Web service security—vulnerabilities and threats within the context of WS-security. In: The 4th Conference on Standardization and Innovation in Information Technology, September 2005, pp. 138–146
22. BS 7799-1:2000: Information security management—Part 1: Code of practice for information security management. British Standards Institution, London
23. Zadeh, L.A.: A computational approach to fuzzy quantifiers in natural languages. Comput. Math. Appl. **9**, 149–184 (1983)
24. Web services activity, http://www.w3.org/2002/ws/

Ping Wang is an Assistant Professor in the Dept. & Grad Program of Information Management at Kun Shan University (KSU), Taiwan R.O.C. He received his Ph.D. degree from IIM at NCTU in 2005. His research interests include risk management, group decision making, and fuzzy decision analysis.

Kuo-Ming Chao is a Senior Lecturer at Department of Computer and Network Systems, Coventry University, UK and he leads the Distributed Systems and Modeling Research Group in the department. He is also Adjunct Professor at Software School, Fudan University, China.

Chi-Chun Lo is a Professor in the Institute of Information Management at National Chiao Tung University, Taiwan R.O.C. He received his Ph.D. degree in Computer Science from Brooklyn Polytechnic University, USA in 1987. His research interests include network management, network security, network architecture, and wireless communications.

Chun-Lung Huang is a Ph.D. student in the Institute of Information Management (IIM) at National Chiao Tung University (NCTU), Taiwan R.O.C. He received his M.B.A. degree from IIM at NCTU in 2001. His research interests include service-oriented computing, consensus reaching and mobile payment.

Muhammad Younas is a Senior Lecturer in Computer Science at the Department of Computing, Oxford Brookes University, UK. He has Ph.D. in Computer Science from the University of Sheffield, UK. His research expertise is in web-based technologies including web-database systems, web services, web searching and mobile web.