The Journal of Systems and Software 86 (2013) 2822–2840

Contents lists available at ScienceDirect

The Journal of Systems and Software

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

# A novel approach to evaluate software vulnerability prioritization

Chien-Cheng Huang*, Feng-Yu Lin, Frank Yeong-Sung Lin, Yeali S. Sun

*Department of Information Management, National Taiwan University, No. 1, Sec. 4, Roosevelt Road, Taipei 10617, Taiwan, ROC*

ARTICLE INFO

*Article history:*
Received 22 February 2013
Received in revised form 13 June 2013
Accepted 18 June 2013
Available online 18 July 2013

*Keywords:*
Software vulnerability
Security evaluation
Fuzzy AHP
Fuzzy synthetic
Fuzzy integral

ABSTRACT

The aim of this study is to formulate an analysis model which can express the security grades of software vulnerability and serve as a basis for evaluating danger level of information program or filtering hazardous weaknesses of the system and improve it to counter the threat of different danger factors. Through the utilization of fuzzy analytic hierarchy process (FAHP), we will organize the crossover factors of the software blind spots and build an evaluation framework. First of all, via the fuzzy Delphi method the aspects and relative determinants affecting security will be filtered out. Then we will identify the value equation of each factor and settle down the fuzzy synthetic decision making model of software vulnerability. Thanks to this model we will be able to analyze the various degrees to which the vulnerability is affecting the security and this information will serve as a basis for future ameliorations of the system itself. The higher the security score obtained therefore imply securer system. Beside this, this study also propose an improvement from the traditional fuzzy synthetic decision making model for measuring the fuzziness between enhancement and independence of various aspects and criteria. Furthermore taking into consideration the subjectivity of human in reality and constructing the fuzzy integral decision making model. Through case study, we show that the evaluation model in question is practical and can be applied on the new software vulnerabilities and measure their degree of penetration. The fuzzy integral decision making emphasize through formulation the multiply-add effect between different factors influencing information security.



## 1. Introduction

Thanks to the widespread of internet usage and development of various systems software the users gained a lot of benefits, along with it modern enterprises and corporates also rely more on information technology. However it also leads to the augmentation of virtual attacks, increasing the importance of information security (Anderson and Moore, 2006). The previous empirical research demonstrate that disclosure of software weakness will severely impact the market value of an organization, the stock market for example is constantly under the threat of information security incidents, the internet-based industries are also more than others facing this challenge (Hovav and D'Arcy, 2003; Cavusoglu et al., 2004; Telang and Wattal, 2007; Goel and Shawky, 2009; Gordon et al., 2010; Yayla and Hu, 2011; Ransbotham et al., 2012). As a summary, within the actual business environment, the importance of information security is strongly enhanced (Gordon and Loeb, 2002).

The threat discussed above will not only lead to information security breach or damage to the system itself, to the extreme it would probably paralyze the entire network. Taking as an example the attacks through drive-by-downloads, it is one of the nightmare users are facing today. In general, the offensive actions through internet rely on special programs or target misconfigurations and non-patched vulnerabilities of basic applications (Arora et al., 2010; Wang et al., 2010b). Citing an example here, in April 2011, the Japanese Sony PSN (PlayStation Network) was cracked by hackers, more than 70 million users data such as name, address even credit card information were retrieved from the Sony system (Milian, 2011).

During recent years, the so-called "zero-day attack" frequency increased dramatically, the vulnerability frequency of applications has also surpassed the vulnerability of operating systems (SANS Institute, 2009). In reality, there is usually not enough time to deploy or update a new patch to cover the blind spot of the application or system, exposing the user under the invasion of internet hackers.

This study propose a novel approach to software vulnerability evaluation and prioritization from the point of view of information security healthcare, and help controllers of informative system to fulfill the healthy status of their system. Information security healthcare includes three main domains: (1) health check (verifying the security status of the system), (2) behavior check (the status of information storage and retrieval in the system), (3) user-specific policies check (verifying the policies implied by the user himself). Through these three points, achieve the protection of system

* Corresponding author. Tel.: +886 233661178; fax: +886 233661199.
*E-mail address:* d97725002@ntu.edu.tw (C.-C. Huang).

0164-1212/$ – see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jss.2013.06.040

security configuration and provide security monitoring or strategies or protection from Trojan virus and malware code, therefore maintain a secure usage of the system and its content (Martin, 2008). Nevertheless, this paper focuses on the health check of vulnerability, so we would not emphasize too many other details here.

The main contributions of this paper are to build an analysis model which can reflect the hidden threats of informative system and be used for evaluating the security degree the system in question is actually. Via the fuzzy sets theory and fuzzy analytic hierarchy process (FAHP) we define an evaluation framework, and filter the factors influencing security through the fuzzy Delphi method (Weck et al., 1997). Then according to the relative grades of these factors in reality we set up their relative equation and therefore we are able to make an overall synthetic analysis of the different degrees of influence of each factor on software vulnerability. Improvement can then be made based on the results of above analysis. Moreover, we propose in this study improvement for grading the enhancing effect and independence status between different evaluation factors in fuzzy synthetic decision making model. Taking into account the subjectivity of human in real world and formulating the fuzzy integral decision making model, through which we will be able to evaluate the security degree of software and plan actions to improve.

Within the study, through the process of two stages questionnaire analysis toward experts and via the fuzzy Delphi method we filter out two influential metrics: the "base metric" and the "temporal metric" plus nine evaluating criteria: access vector, attack complexity, authentication instances, confidentiality impact, integrity impact, availability impact, exploitability tools and techniques, remediation level, and report confidence. We also decide at the same time the fuzzy weight of each criterion. Afterward with the application of performance appraisal values and fuzzy statistics methods we are then able to construct the membership function of each criterion and through fuzzy synthetic decision making and fuzzy integral decision making model we then evaluate the security status of the software.

The paper is organized as follows: Section 2 discusses about the related works of information security healthcare, scoring system and the software vulnerability evaluation. Section 3 proposes the evaluation model of software vulnerability. Section 4 is about implementation of the model. Section 5 contains case study. And the conclusion is declared in Section 6.

## 2. Related works

In this section we categorize the related works in three parts, first the historical of information security healthcare studies, then discussion about scoring system and related works, finally the related works of software vulnerability evaluation.

### 2.1. Information security healthcare

In the previous studies and research the general deterrence theory (GDT) has been widely used (Forcht, 1994; Martin, 1973; Parker, 1981; Straub, 1990). In this study we categorize this research in this domain as a defensive point of view of information security, including defense in depth (DiD), intrusion detection/protection, access control, network attack and defense strategy, survivability, resource allocation, and etc. (Liu et al., 2005; Ryu and Rhee, 2008; Wang et al., 2010a; Crampton, 2011). However, this actual study starts from the point of view of the protection motivation theory (Rogers, 1975, 1983) and is toward the domain of information security healthcare, meaning discussing about information security health status. In informative systems, misconfiguration and non-patch of vulnerabilities may occur. Before any data is saved in the computer device, through trusted network connect (TNC) scanning the user can check if it is appropriate or not to download the data in question, this process has already become the de facto standard of information security healthcare (Stiemerling et al., 2008; Trusted Computing Group, 2009). Taking as an example Microsoft network access protection (NAP) and statement of health (SOH), to guarantee the healthy status of the computer device, its antivirus update, operating system update, firewall settings must be conform with the SOH criteria set by the controller (Microsoft, 2010).

In the previous studies of information security healthcare, the starting point was the national vulnerability database (NVD), then moving to the national checklist program (NCP), finally including the realization of the security content automation protocol (SCAP) (The White House, 1998, 2000a, b, 2002; NIST, 2010a, b; Quinn et al., 2011; Waltermire et al., 2011). Taking as an example the control protocols of the information security management system (ISMS), in the special publication 800-53 of the National Institute of Standards and Technology (NIST), regarding its configuration management the office of management and budget (OMB) declared obligatory the federal desktop core configuration (FDCC) since 2007 through the notes M-07-11 (Johnson, 2007; NIST, 2009, 2010c).

NVD and NCP both rely on storing the information into database to provide better information security healthcare, and adding into this knowledge repository the counter-process against attacks on misconfigurations or non-patch of vulnerabilities (Quinn et al., 2011). Provide through SCAP the evaluation of system vulnerability and information security monitoring then supply the involved team with appropriate information security policy at the right timing. All these are to avoid that information security threat sources have the opportunity to illegal access, destroy, divulge or falsify information and affect in a negative way system users or operators. If the above threats are to happen, pernicious events may occur or damage to the informative properties will for sure impact the system and its users. Therefore, the basic process of information security healthcare would be as follow: starting from the vulnerability patch or the information itself, suggesting appropriate actions and policies to assure the security and safety of the information system, so that the organization can provide continuous commercial services (Straub and Welke, 1998).

### 2.2. Scoring systems

CVSS (common vulnerability scoring system) is the industry standard to "evaluate the different security levels of computer information security vulnerability" (Mell et al., 2006, 2007; Scarfone and Mell, 2009) and is also the ranking used in the NVD (NIST, 2010a), it provides a grading system for system vulnerability evaluation, describes the weaknesses of the system through standardization and quantitative qualification. It can help governments or corporates build up a complete policy for computer information security by clarifying the relationship between different vulnerability levels and the appropriate protocol toward each of them so that the team in charge can follow.

Via open architecture, CVSS not only explains its evaluation logic and process but also includes various factors such as: vulnerability bulletin providers, software application vendors, vulnerability scanning and management, security and risk management, and user organizations in the equation, providing in the end a grading system for the system vulnerability. After the information security team apply the grading system of weaknesses and include in the formula the actual environment of the computer information system, they can retrieve the analysis result and allocate their limited resources according to the priority of different system weaknesses.

In particular, Houmb et al. (2010) proposed the quantifying security risk level, in it he proceeds to risk control and measurement based on CVSS evaluation results of frequency and impact. On

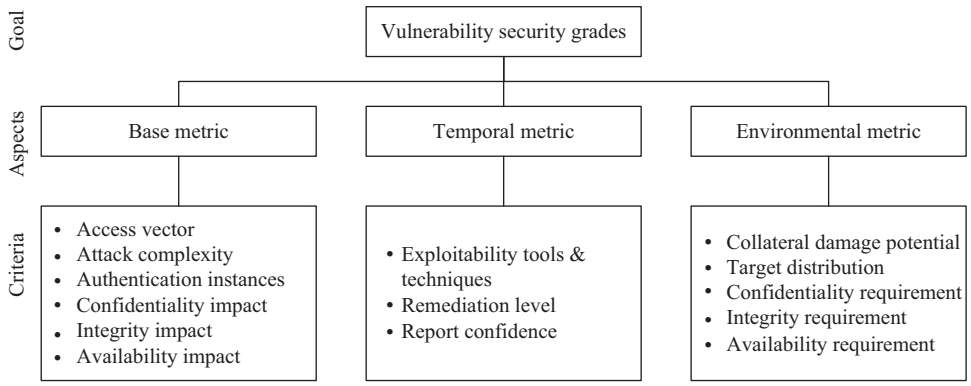


**Fig. 1.** The evaluation framework of software vulnerability security grades.

the other side, Liu and Zhang (2011) also proposed the vulnerability rating and scoring system (VRSS). They both developed afterward AHP to improve the system vulnerability grading of VRSS (Liu et al., 2012).

### 2.3. Security evaluation factor of software vulnerability

In this study we organized the related works from enumerations catalogs regarding software vulnerability evaluation, the main categories would be as follow: common vulnerabilities and exposures (CVE), common weakness enumeration (CWE), common attack pattern enumeration and classification (CAPEC), common configuration enumeration (CCE), common platform enumeration (CPE), SANS top-20, open web application security project's (OWASP) top ten, web application security consortium's (WASC) threat classification, CWE/SANS top 25 most dangerous programming errors and etc. Enumerations catalog the fundamental entities and concepts in information assurance, cyber-security and software assurance that need to be shared across the different disciplines and functions of these practices. CVE enumeration enables all kinds of measurement by providing unique identifiers for publicly known vulnerabilities in software (Martin, 2008).

Through this study, taking the different influencing factors pointed out in the related works of CVSS as reference, we can summarize them into three main categories and fourteen evaluation criteria. The main categories are base, temporal and environmental metric, as shown in Fig. 1. Base metric involves the criteria such as access vector, attack complexity, authentication instances, confidentiality impact, integrity impact, and availability impact. In temporal metric, on the other hand we discuss about exploitability tools and techniques, remediation level, and report confidence. While in environmental metric, collateral damage potential, target distribution, confidentiality requirement, integrity requirement, and availability requirement are the main subjects. The details are explained in Table 1.

## 3. Software vulnerability evaluation methods

Usually when evaluating the software vulnerability, we rely on various fuzziness terms such as "very secure", "securer" or "not secure" this easily leads to an imprecise definition if using only the binary logistic. Therefore, in this study we use the more appropriate "membership function" and "grade of membership" from the fuzzy set theory, and based on their concept we clarify the definition of vulnerability level of various software weaknesses. Beside this, we apply the fuzzy synthetic decision making along with the $\lambda$ fuzzy measures to elaborate the experience model of experts' evaluation toward information security recognition. The details are explained as below.

### 3.1. Model logic and structure

#### 3.1.1. Model logic

When analyzing the vulnerability of software, we usually face two extreme situations to improve its security: the first one is to deny any kind of data storage in the involved system. Obviously this will prevent any kind of attack and from the information security incidents point of view this is named "perfect security" and owns the higher level of security. The second situation being that a break-in program is already implanted in the system, leading to a "totally insecure" status. To be brief, the first situation described above would be ranked level 1 (perfect security) while the second one would be ranked level 0 (totally insecure). While most of the time, the case occurs in between.

Taking into consideration the objectivity of the vulnerability of software, it is possible to describe the real security status with an objective number, located between 0 and 1 and will be directly related to the factors influencing the result of software vulnerability. This number will change along with time, being a function of time.

The information security issue is quite complex and full of uncertainty since it is affected by various vulnerabilities or threats and also the indefinite nature of the influence between factors in the eye of the evaluator, making the alternative nature and relation between all the elements in the equation reflect fuzziness, leading to the fuzzy multiple criteria decision making (FMCDM) issue. This study use a simulation based on fuzzy statistics to handle the fuzziness of semantic factors and build up the quality rules of the equation. To summarize, in this study we rely on the experience of experts to construct a fuzzy synthetic decision making model, providing each grade rule its own analysis model, so that we can understand in a more detailed way the vulnerability of the software in question. Thanks to this model we will be able to run a fuzzy integral decision making analysis for each graded category and evaluate with precision the potential risks of software vulnerability and take action according to its priority level.

#### 3.1.2. Model structure

The main columns in this model are the different points of analysis $Y_1, Y_2, \ldots, Y_k$ (e.g. base, temporal, environmental metric) and the main rules (ex: the rule of point $k$ and point $j$ is $Y_{kj}$). While the filter of all these points and rules uses the fuzzy Delphi method to pick out the appropriate factors. The hierarchy structure of the analysis is shown in Fig. 2.

#### 3.1.3. Formulation procedure

In this study, the evaluation of vulnerability apply the fuzzy multiple criteria decision making (FMCFM) model on software analysis, the obtained model structure resumed by Fig. 3: the formulation

**Table 1**
Explanation of evaluation criteria for software vulnerability.

| Aspects | Criteria | Descriptions |
|---|---|---|
| Base metric | Access vector (AV) | Whether if the storage process is by physical isolation, physical hardware entity, adjacent network, intranet, extranet, Internet, wireless, and etc. it will have different impact on the security level. |
| | Attack complexity (AC) | The higher the attack complexity, the harder it is for hackers to breach the system. The lower the attack complexity the easier it is for hackers to succeed in their action. The vulnerability includes: SQL injection, buffer errors, and etc. influencing the organization security. |
| | Authentication instances (AU) | The authentication instances includes: entity authentication, multiple authentication, single authentication, none authentication, and etc. influencing the organization security. |
| | Confidentiality impact (C) | The impact of a successful attack on the confidentiality: the impact of data leakage on the organization function and security. |
| | Integrity impact (I) | The impact of a successful attack on the integrity: the impact of incomplete data on the organization function and security. |
| | Availability impact (A) | The impact of a successful attack on the availability: the impact of data loss or damage on the organization |
| Temporal metric | Exploitability tools and techniques (E) | The main available tools and techniques are: unproved, proof-of-concept, functional, high. The analysis of technical details of the system vulnerability will influence the organization security. |
| | Remediation level (RL) | Remediation levels include: official fix, temporary fix, workaround, unavailable. The remediation level of the vulnerability will influence the organization security. |
| | Report confidence (RC) | The credibility of the system vulnerability report protocol depends on: unconfirmed, un-corroborative, corroborative, confirmed. The weakness itself can be used to identify technically the attack, influencing the organization security. |
| Environmental metric | Collateral damage potential (CDP) | The influence of collateral or potential damage on the organization function and working security. |
| | Target distribution (TD) | The influence of target distribution caused by the system vulnerability repartition on the organization function and working security. |
| | Confidentiality requirement (CR) | The need of the organization toward data secrecy. The impact of data leakage on the organization function and working security. |
| | Integrity requirement (IR) | The need of the organization toward data completeness. The impact of incomplete data on the organization function and working security. |
| | Availability requirement (AR) | The need of the organization toward data availability. The impact of data loss or damage on the organization function and working security. |

procedure is divided into two parts, in the first one through two stages questionnaire to experts: in the first questionnaire we apply the fuzzy Delphi method and filter the evaluation criteria, these information are the basis for the second questionnaire, by which we will have a more precise picture of how the criteria can affect the level of software vulnerability. After this thanks to the concept of fuzzy statistics we can obtain a simulation of the function membership between criteria and start constructing the fuzzy synthetic decision making model. The first part of formulation procedure is mainly about a whole evaluation of the effect level on various factors on software vulnerability, give a number to each evaluated target, symbolizing its grade, it is the fuzzy synthetic decision making model. However, in this model, we can see that the subjectivity of given grade cannot fulfill the usual additive nature concept, this issue is occurring when we apply the evaluation model from experts subjectivity to grade the vulnerability of software. Therefore in the second part of this study we will refer to the fuzzy grading evaluation concept of Choquet to formulate the fuzzy integral decision making model and improve the traditional evaluation process, the main goal being that we can get even closer to the reality and also its actual software vulnerability. The fuzzy synthetic decision making and the fuzzy integral decision making models formulation are explained in details as follow.

### 3.2. Fuzzy synthetic decision making

The main purpose of this fuzzy synthetic decision making model is to make a complete analysis of the factors affecting the targeted

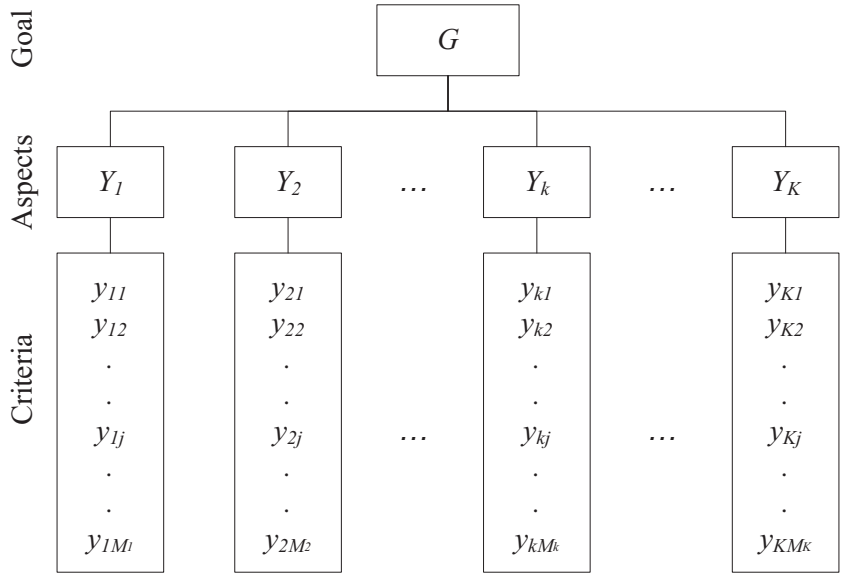


**Fig. 2.** Architecture of the analytic hierarchy.

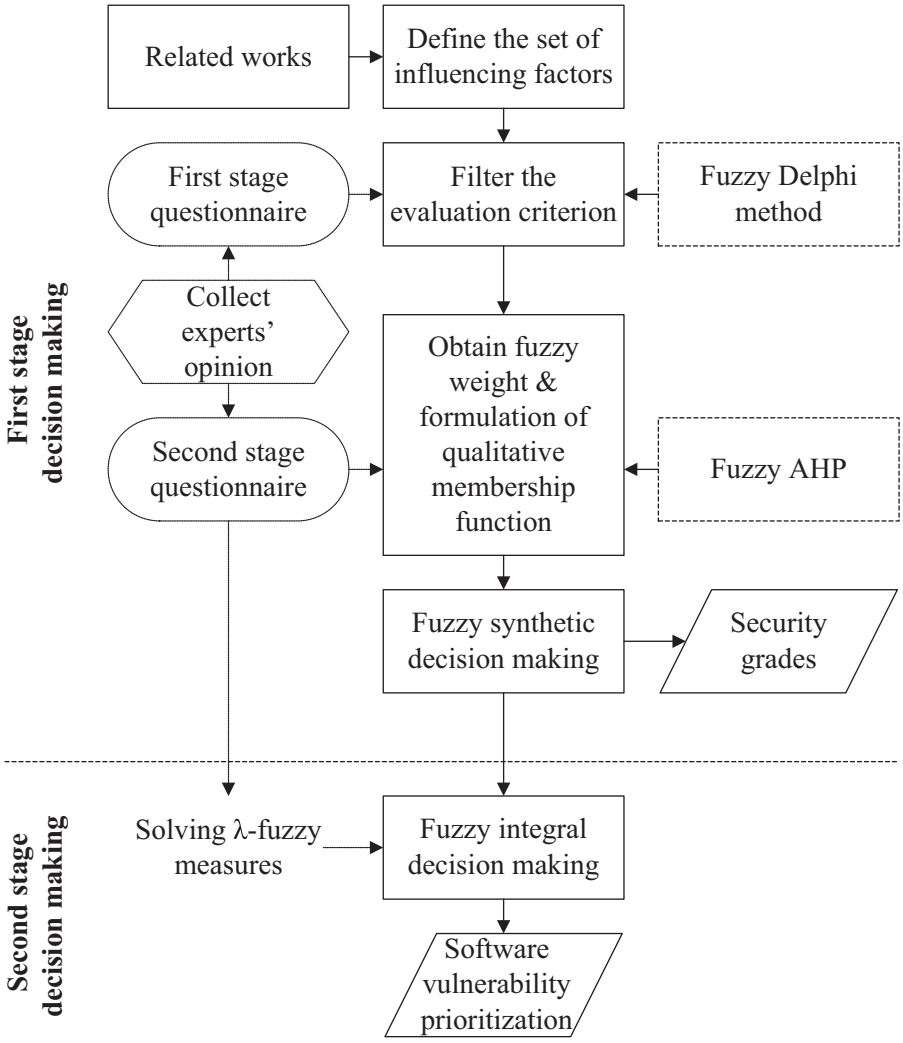


**Fig. 3.** Research methodology.

subject and assign to each of them a real number symbolizing the average result of the evaluation. Regarding the fact that software vulnerability is influenced by various factors and also by different criteria and analysis equation, though the fuzzy synthetic decision making we can obtain a more precise grading of software vulnerability, detailed calculation process and explanation as below.

*3.2.1. Definition of evaluation criteria set and evaluation grade set*

Evaluated vulnerabilities set: $X = \{x_i\}$, $i = 1, \ldots, I$.

First grade evaluation criterion set: $Y = \{y_k\}$, $k = 1, \ldots, K$.

Second grade evaluation criterion set: $Y_k = \{y_{kj}\}$, $k = 1, \ldots, K$; $j = 1, \ldots, M_k$.

Security level set: $Z = \{z_h\}$, $h = 1, 2, 3, 4, 5$, respectively meaning poor security, fair security, moderate security, good security, excellent security.

This study divides software vulnerability into base, temporal, and environmental metric, then uses the fuzzy Delphi method to filter evaluation criteria, as an example: access vector, attack complexity, authentication instances, and etc. Since this study extracts the precious experience of experts toward the influence of vulnerability factors on information security to formulate an expert experience based evaluation model, the main task is to clarify the evaluation criteria. However the factors having an impact on vulnerability are diversified and difficult to analyze, therefore during this study we first gathered the factors mentioned in works related to software vulnerability (Martin, 2008; MITRE, 2010a, b; OWASP, 2010) and collected experts' opinions through a two-step questionnaire.

In the first questionnaire we find out the relation between the evaluation criteria of software vulnerability. Then via the second questionnaire we obtain the grading by importance of these evaluation criteria. The main three steps are explained as below.

**Step 1**: Define the set of influencing factors

The main target: software vulnerability level. Therefore, the set of influencing factors are the one having an impact on software vulnerability, as shown in Table 1.

**Step 2**: Collect experts' opinion

The main target: software vulnerability level. After gathering the factors set, require the experts opinion about their grading, so that we can assign different weight to each individual factor in the set.

**Step 3**: Apply the fuzzy Delphi method and filter the evaluation criterion

**i**. Construct the triangular fuzzy function according to the result of questionnaires.

Organize the result of questionnaires and build up the triangular fuzzy function following the Eqs. (1)–(4).

$$\tilde{N}_A = (L_A, M_A, U_A) \tag{1}$$

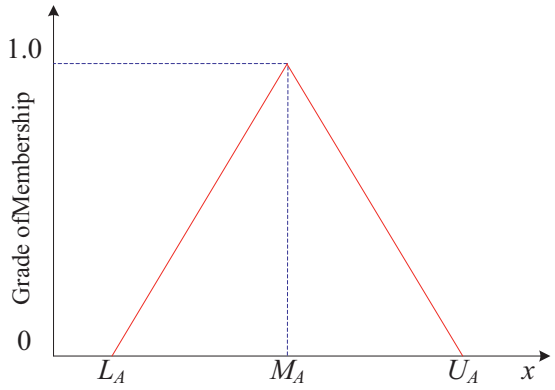


**Fig. 4.** A triangular fuzzy function of criterion.

$$L_A = Min(x_{Ap}), p = 1, \ldots, N \quad (2)$$

$$M_A = (x_{A1}, x_{A2}, \ldots, x_{An})^{1/N} \quad (3)$$

$$U_A = Max(x_{Ap}), i = 1, \ldots, N \quad (4)$$

Here, $x_{Ap}$ is the opinion of the $p$st expert on the factor $A$. $L_A$ is the lowest level the experts graded to factor $A$. $M_A$ is the experts grading average on factor $A$. $U_A$ is the maximum level the experts graded to $A$. $A$ is equal to the factor influencing software vulnerability. $p$ represents the expert. $\tilde{N}_A$ is the fuzzy function of importance. After the above classification we can obtain the triangular function of the influencing factors as shown in Fig. 4.

**ii**. Filter the evaluation criterion

Using the triangular fuzzy function calculated in the previous step to filter the evaluation criterion. In this function, the biggest and smallest grades are extreme examples while the average can represent the opinion of most of the experts. Therefore in this study we take the average of each influencing factor in the triangular fuzzy number $M_A$ as membership level, to represent the common opinion of the experts toward it. In the end, according to the research target quality ($S$) we filter the appropriate evaluation criterion. As $M_A \geqq S$, accepting the influencing factor $A$ as evaluation criterion. In the equation, $M_A$ is the common agreement of experts regarding influencing factor $A$.

### 3.2.2. Define the weight of various evaluation criteria

Calculate one of the fuzzy set from $Y_k = \{y_k | y_k \in Y_k\}$: $\underset{\sim}{A_k} = \{\mu\underset{\sim}{A_k}(y_{k1}), \ldots, \mu\underset{\sim}{A_k}(y_{kM_k})\}$, in it $\mu\underset{\sim}{A_k}(y_{kj})$ is defined as the weight of the second evaluation criterion benchmark $y_{kj}$ ($j = 1, \ldots, M_k$) when doing performance appraisal. The evaluation of system information security can be done by observing how experts evaluate software vulnerability, through collecting their experience via questionnaires and formulating a hierarchy structure in concordance with their opinion.

We can apply analytic hierarchy process (AHP) based on the hierarchy of targeted information vulnerability to obtain the weight of each expert regarding different targeted information vulnerability. Supposing that this decision corpus is composed of $N$ experts, for every single expert we can apply AHP to retrieve his weight of evaluation criteria from $k$ category.

$$\underset{\sim}{A_k} = \{\mu\underset{\sim}{A_k}(y_{k1}), \ldots, \mu\underset{\sim}{A_k}(y_{kj}), \ldots, \mu\underset{\sim}{A_k}(y_{kM_k})\} \text{ for all } p$$

The weight that each expert assigned to the evaluation criterion $y_{kj}$ can only represent one part of its weight. In the past we mostly relied on the average or the geometric mean of the weight, however it would still only reflect one part of the weight. To combine and summarize the opinion of the $N$ experts, in this study we apply the concept of fuzzy number to calculate the fuzzy weight of evaluation criterion. Then we can represent $\mu\underset{\sim}{A_k}(y_{kj})$ by TFN as the Eqs. (5)–(8).

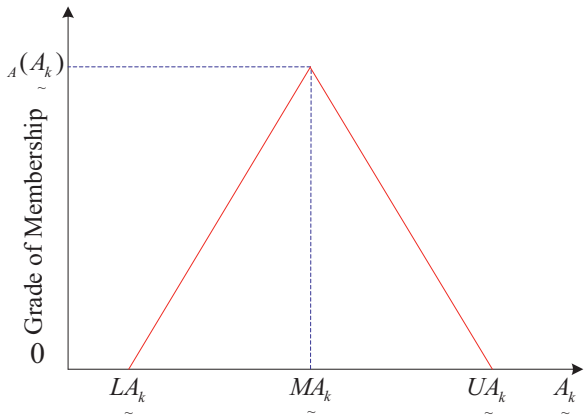


**Fig. 5.** A triangular fuzzy weight of criteria.

$$\underset{\sim}{A_k} = [\underset{\sim}{LA_k}, \underset{\sim}{MA_k}, \underset{\sim}{UA_k}], \; k = 1, \ldots, N \quad (5)$$

$$\underset{\sim}{LA_k} = Minimum\{\mu\underset{\sim}{A_k}(y_{kj})\}, \text{ for all } p \quad (6)$$

$$\underset{\sim}{MA_k} = Average\{\mu\underset{\sim}{A_k}(y_{kj})\}, \text{ for all } p \quad (7)$$

$$\underset{\sim}{UA_k} = Maximum\{\mu\underset{\sim}{A_k}(y_{kj})\}, \text{ for all } p \quad (8)$$

When evaluating the fuzzy weight $\underset{\sim}{A_k}$ of criterion $y_{kj}$, its membership function $\mu_{\tilde{A}}(\underset{\sim}{A_k})$ is as shown in Fig. 5. The reason why applying TFN on $\underset{\sim}{A_k}$ is to simplify the calculation model. When $\underset{\sim}{A_k}$ is under TFN, $\mu_{\tilde{A}}(\underset{\sim}{A_k})$ is continuous, everything out of $[\underset{\sim}{LA_k}, \underset{\sim}{UA_k}]$ would mean $\mu_{\tilde{A}}(\underset{\sim}{A_k}) = 0$, while the one on $\underset{\sim}{MA_k}$ would mean $\mu_{\tilde{A}}(\underset{\sim}{A_k}) = 1$. The one between $[\underset{\sim}{LA_k}, \underset{\sim}{MA_k}]$ would be with strict ascending linear relationship, the one between $[\underset{\sim}{MA_k}, \underset{\sim}{UA_k}]$ would be with strict descending linear relationship.

Since the weight of $\underset{\sim}{A_k}$ is organized by TFN, its membership function $\mu_{\tilde{A}}(\underset{\sim}{A_k})$ can be defined as follow:

$$\mu_{\tilde{A}}(\underset{\sim}{A_k}) = \begin{cases} 0 & , \underset{\sim}{A_k} < \underset{\sim}{LA_k} \\ \dfrac{\underset{\sim}{A_k} - \underset{\sim}{LA_k}}{\underset{\sim}{MA_k} - \underset{\sim}{LA_k}} & , \underset{\sim}{LA_k} \leq \underset{\sim}{A_k} < \underset{\sim}{MA_k} \\ 1 & , \underset{\sim}{A_k} = \underset{\sim}{MA_k} \\ \dfrac{\underset{\sim}{UA_k} - \underset{\sim}{A_k}}{\underset{\sim}{UA_k} - \underset{\sim}{MA_k}} & , \underset{\sim}{MA_k} \leq \underset{\sim}{A_k} < \underset{\sim}{UA_k} \\ 0 & , \underset{\sim}{A_k} > \underset{\sim}{UA_k} \end{cases}.$$

Obviously, $\underset{\sim}{A_k}$ already included the judgment of $N$ experts into consideration, therefore it reflects all the possible situation of weight, not only specific part of it.

### 3.2.3. Define the performance appraisal membership function of each evaluation criterion

One main issue we face before evaluating the evaluation criterion membership function of vulnerability is how to calculate the vulnerability level of the criterion. Due to the fact that the

evaluated vulnerability is facing future uncertainty, we must use fuzzy numbers to describe the possible range. In this study, through questionnaire we filtered experts experience and organized the result with the following concept and turned the result of questionnaire into fuzzy membership function, built the fuzzy membership function of the qualitative criterion as the basis of vulnerability evaluation. Then we inserted in the obtained membership function the real performance appraisal of the criterion waiting to be evaluated so that we finally deduced the vulnerability membership function of each different evaluation criterion.

Calculate from $Y_k \times Z = \{(y_k, z_h) | y_k \in Y_k, z_h \in Z\}$ one of the fuzzy set $\underset{\sim}{B}_{ki} = \begin{bmatrix} \mu\underset{\sim}{B}_{ki}(y_{k1}, z_1), \ldots, \mu\underset{\sim}{B}_{ki}(y_{k1}, z_h) \\ \vdots \\ \mu\underset{\sim}{B}_{ki}(y_{kj}, z_1), \ldots, \mu\underset{\sim}{B}_{ki}(y_{kj}, z_h) \end{bmatrix}$

In it, $\mu\underset{\sim}{B}_{ki}(y_{kj}, z_h)$ is defined as the software vulnerability level in the total grading as $z_h (h = 1, 2, 3, 4, 5)$ of vulnerability $x_i$ in the second level of evaluation criterion $y_{kj} = (k = 1, 2, \ldots, K; j = 1, 2, \ldots, M_k)$.

**i**. Evaluation of criterion

(a) Concept

Taking the access vector as an example, according to the traditional classification, we may find the main security categories: high, physical isolation, medium, Intranet, low, wireless. Obviously we could make it more precise or appropriate, therefore when classifying an access vector security level as high, medium and low we call this membership. The higher the membership the stronger the relationship with that level and it could express correctly the change between levels, as an example: in a random access vector, if it is sure that the security level is high, its membership with "high" security is 1.0, the membership with "medium" or "low" security level is 0. On the other hand, if the security level of the access vector is "medium-high", its membership with "high" security is decreasing from 1.0, while the membership with "medium" security is increasing from 0, and the membership with "low" security is 0.

(b) From verbal data to equation

When formulating the membership function through questionnaires, we turned the results of the survey into membership levels so that we can formulate membership function. The process principle is obtained via the fuzzy statistics concept (Buckley, 1985, 2004) as in Eq. (9). In here, $\mu\underset{\sim}{B}_k(y_{kj}, z_h)$ is defined as the security level of the second evaluation criterion $y_{kj} = (k = 1, 2, \ldots, K; j = 1, 2, \ldots, M_k)$ in different situation level $h$ within the level $z_h$. $y_{kj}$ is the situation level of the second level evaluation criterion in security level $h$. Taking here the formulation of the membership function of the "access vector" as example:

$$\mu_{Access\ vector}(x_p = Expert\ p) = \frac{\sum_{j=1}^{N} \mu_{pj}(Access\ vector\ of\ security\ level : Good)}{N}$$

$$\mu\underset{\sim}{B}_k(y_{kj}, z_h) = \frac{\sum_{j=1}^{N} \mu_{kj}(y_{kj} \in z_h)}{N} \tag{9}$$

Then we use the Eq. (9) to turn the result of questionnaires into the membership frequency table of security grades within the security levels: poor, fair, moderate, good and excellent. The "good" security status is in Table 2, serving as a basis for formulating the membership function of security levels. In $N_1 + N_2 + \ldots + N_R = N$ of Table 2, $N$ is the amount of experts targeted by the questionnaire. $N_r$ $(r = 1, 2, \ldots, R)$ is the amount of experts who choose the "good" security level for level $r$.

**ii**. Formulation of discrete membership function

The discrete membership functions are finite sets. The quality benchmark of security level evaluation criterion must first be obtained via the questionnaires to experts, where they will express their opinion toward various influencing factors and their respective performance appraisal level. Then we change the questionnaires result into numbers. Therefore we can only build the performance appraisal level of quality criterion as independent variable. The dependent variable is the discrete membership function of the dependent variable. To calculate the membership function of each quality benchmark with different security level, in this study we rely on the fuzzy statistics way, applying Eq. (9) and classifying the result of questionnaire into the membership frequency table of security levels such as poor, fair, moderate, good, excellent. "Good" security level shown in Table 2. The security membership level (poor, fair, moderate, good, excellent) of the security $r$ of the status evaluation criterion $y_{kj}$ is as described in Eq. (10).

$$\mu\underset{\sim}{B}_{ki}(y_{kj}, z_h) = \left(\frac{P_r}{N}, \frac{F_r}{N}, \frac{M_r}{N}, \frac{G_r}{N}, \frac{E_r}{N}\right) \tag{10}$$

### 3.2.4. Complete evaluation

After calculating the fuzzy weight and fuzzy performance appraisal values via the previous steps, we must rely on fuzzy numbers to combine the whole equation and obtain the complete performance appraisal number of various categories and criteria. This is the building process of the fuzzy synthetic decision making model.

Obtain the fuzzy set $\underset{\sim}{C}_{ki} = [\mu\underset{\sim}{C}_{ki}(z_1), \ldots, \mu\underset{\sim}{C}_{ki}(z_h)]$ from $Z = \{z | z \in Z\}$. In it, the evaluation benchmark $\mu\underset{\sim}{C}_{ki}(z_h)$ is defined as the status reflected on security level $z_h$ by the vulnerability targeted for evaluation in the first grade $y_k$ security level.

The fuzzy set $\underset{\sim}{A}_k$ represents the fuzzy status of $Y_k$. The fuzzy set $\underset{\sim}{B}_{ki}$ represents the fuzzy relation between $Y_k$ and $Z$. The combination of $\underset{\sim}{A}_k$ and $\underset{\sim}{B}_{ki}$ is the fuzzy set $\underset{\sim}{C}_{ki}$ of the fuzzy status $Z$, noted as: $\underset{\sim}{A}_k \cdot \underset{\sim}{B}_{ki} = \underset{\sim}{C}_{ki}$. The calculation formula of $\mu\underset{\sim}{C}_{ki}(z_h)$ in the fuzzy set $\underset{\sim}{C}_{ki}$ is as explained in Eq. (11).

$$\mu\underset{\sim}{C}_{ki}(z_h) = \mu\underset{\sim}{A}_k \cdot \underset{\sim}{B}_{ki}(z_h) = \sum_{j=1}^{M} \mu\underset{\sim}{A}_k(y_{kj}) \cdot \mu\underset{\sim}{B}_{ki}(y_{kj}, z_h) \tag{11}$$

### 3.2.5. Defuzzification

If we take out the fuzzy nature from the above calculation, we can obtain the information security level of software vulnerability $x_i$ in the first grade evaluation benchmark $Y_k$. The changed numbers are classified by researcher into five levels, in this study we use $[0, 0.25, 0.5, 0.75, 1]^t$, as shown in Eq. (12). After the above evaluation process we can know the complete evaluation result of each information security vulnerability level and classify them according to priority and also clarify the source of a vulnerable point, understand which criterion or factor is responsible. This information would serve as reference for information security improvement.

$$r_{kh} = [\mu\underset{\sim}{C}_{ki}(z_1), \mu\underset{\sim}{C}_{ki}(z_2), \mu\underset{\sim}{C}_{ki}(z_3), \mu\underset{\sim}{C}_{ki}(z_4), \mu\underset{\sim}{C}_{ki}(z_5)] \cdot [0, 0.25, 0.5, 0.75, 1]^t \tag{12}$$

## 3.3. Fuzzy integral decision making

When evaluating the software vulnerability level, we usually add together the individual security levels, but most of the

**Table 2**
The membership frequency of the evaluation criterion $y_{kj}$ under each information security status level with the "good" level of information security.

| Level of evaluation criterion status | Level 1 | Level 2 | ... | Level $r$ | ... | Level $R$ |
|---|---|---|---|---|---|---|
| Membership quantity (times) | $N_1$ | $N_2$ | ... | $N_r$ | ... | $N_R$ |
| Membership frequency | $N_1/N$ | $N_2/N$ | | $N_r/N$ | | $N_R/N$ |

subjective opinion of decision makers does not fulfill the additive concept. To represent in a more accurate way the specificities of real human society, in this study we apply the independent "fuzzy measure" which does not need additive nature to calculate the importance of evaluation criterion. Because fuzzy integral model is independent and do not need supposition attribute, we can apply the non-linear status. Even if from an objective point of view, each attribute is independent from each other, however from the subjective point of view of evaluators this is not always the case, therefore it is more appropriate to apply the fuzzy integral model on the evaluation. As a result we apply the fuzzy integral decision making model to evaluate the software vulnerability of different security levels and formulate the software vulnerability evaluation formula. In this study we use the fuzzy integral of multiply-add model from Choquet (Choquet, 1953; Murofushi and Sugeno, 1989), only via his calculation model can we retrieve the unique possible answer.

In the previous fuzzy synthetic decision making process, we already defined the evaluation criterion and weight. The next step will then be: (1) define if the software vulnerability level of information security has an additive, alternative or multiplicative (complying with monotonicity) nature, by the definition of the λ fuzzy measures. (2) Retrieve the importance level ($g(H_n)$). After obtaining the above data, we can apply the fuzzy integral model of Choquet and calculate the complete evaluation result of information security level. The detailed steps are as below.

### 3.3.1. Deciding the λ measure and obtaining the importance level ($g(H)$)

When calculating the importance level ($g(H_n)$) through the λ fuzzy measure, we must know the inquiry result of fuzzy measure from each secondary set. But when the criterion corpus is big, there are too many corresponding secondary set, making the questionnaire process difficult in reality. Because of this, in this study we simplify the process by the "needed information quantity perspective" (Sugeno and Terano, 1977; Chen and Wang, 2001). The λ fuzzy measure of finite set can be calculated as the Eq. (13).

$$g_\lambda(A \cup B) = g_\lambda(A) + g_\lambda(B) + \lambda g_\lambda(A) g_\lambda(B), \ -1 < \lambda < \infty \tag{13}$$

The casual formula being:

$$g_\lambda(\{x_1, x_2, \ldots, x_l\}) = \sum_{i=1}^{l} g_i + \lambda \sum_{i_1=1}^{l-1} \sum_{i_2=i_1+1}^{l} g_{i_1} g_{i_2} + \cdots + \lambda^{l-1} g_1 g_2 \ldots g_l$$

$$= \frac{1}{\lambda} \prod_{i=1}^{l} (1 + \lambda \cdot g_i) - 1 \tag{14}$$

First, we design the questionnaire by comparing different factors by group of two, to obtain their respective importance proportion and input to Eq. (14). In this study we apply the perception way of characteristic value for λ fuzzy measure (Asai, 1995; Lee and Leekwang, 1995). We compare by pair the entire corpus of secondary set of evaluating factors $x$.

$$\begin{array}{c} \\ \{x_1\} \\ \{x_2\} \\ \vdots \\ \{x_n\} \\ \{x_1, x_2\} \\ \{x_3, x_4\} \\ \vdots \\ \{x_1, x_2, \ldots, x_n\} \end{array} \begin{array}{c} \begin{array}{cccccccc} \{x_1\} & \{x_2\} & \cdots & \{x_n\} & \{x_1, x_2\} & \{x_3, x_4\} & \cdots & \{x_1, x_2, \ldots, x_n\} \end{array} \\ \begin{bmatrix} 1 & a_{12} & \cdots & a_{1n} & & & \cdots & \\ 1/a_{12} & 1 & & & & & & \\ \vdots & & 1 & & & & & \\ 1/a_{1n} & & & 1 & & & & \\ & & & & 1 & & & \\ & & & & & 1 & & \\ \vdots & & & & & & 1 & \\ & & & & & & & 1 \end{bmatrix} \end{array}$$

From this characteristic vector we obtained when calculating the maximum characteristic root the importance level of each factor in different combinations.

$$W = (W_1, W_2, \ldots W_{2^k-1})$$

$$g_\lambda(\{x_1\}) = W_1$$

$$g_\lambda(\{x_2\}) = W_2$$

$$\vdots$$

$$g_\lambda(\{x_1, x_2, \ldots, x_n\}) = 1$$

### 3.3.2. Fuzzy integral decision making

With the importance level ($g(H_n)$) data and the information security represented level ($h(x_n)$) of the evaluated software vulnerability under different criterion from the fuzzy synthetic decision making process, we can calculate an evaluation result number of software vulnerability security level through the fuzzy integral formula of Choquet, as shown in Eq. (15) and Fig. 6:

$$\int h dg = h(x_n) g(H_n) + [h(x_{n-1}) - h(x_n)] g(H_{n-1}) + \cdots + [h(x_1) - h(x_2)] g(H_1) \tag{15}$$

This is called the fuzzy integral of the fuzzy measure $g(\cdot)$ of the dependent function $h(\cdot)$, however:

$H_1 = \{x_1\}, H_2 = \{x_1, x_2\}, \ldots, H_n = \{x_1, x_2, \ldots, x_n\} = X$.

In it, $h(x_i)$ is the performance (information security level) of the being-evaluated software vulnerability on the $i$ level. While $g(H_i)$ represent the importance level when taking into consideration at the same time $H_1 \sim H_i$. The fuzzy measure is represented as $g(\cdot)$, the supposed function $h$ as $h(x_1) \geq h(x_2) \geq \ldots \geq h(x_n)$.

### 3.3.3. Prioritization of software vulnerability security level

By applying the fuzzy synthetic decision making model and the fuzzy integral decision making model on the evaluated software vulnerabilities we obtain the complete picture of information security vulnerability evaluation, and by classifying them according to

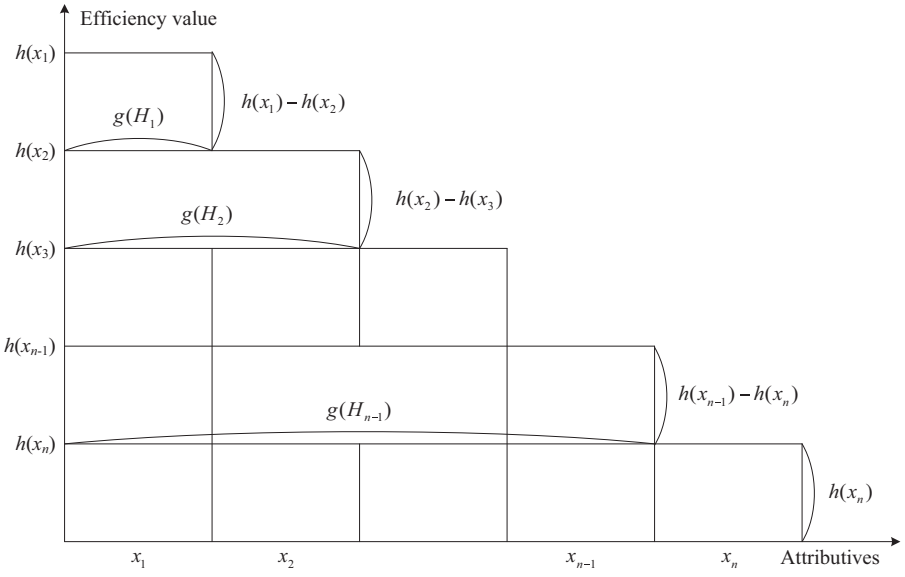


**Fig. 6.** Fuzzy integral.

their respective priority we can obtain a reference for improving policies.

## 4. The implementation of the model

The main goal of this section is to analyze the software vulnerability level relying on the fuzzy integral decision making model formulated and also the common vulnerabilities and exposures (CVE) data (MITRE, 2010a) from the NVD (NIST, 2010a) and vulnerability type according to the common weakness enumeration (CWE) classification system (MITRE, 2010b).

### 4.1. Formulation of analysis structure

#### 4.1.1. Analysis structure and evaluation criterion

The evaluation criterion and software vulnerability security level involved in this study are based on the influencing factors from works related to information security. Fourteen evaluation criteria in total have been chosen. In this study we also categorized the software vulnerability level into three parts. The evaluation criteria and their content are as explained in Table 1, the overall hierarchy structure is as explained in Fig. 1.

#### 4.1.2. Filter of evaluation criterion

In this study we gathered experts' opinion and applied on the result the fuzzy Delphi method, the main target being to filter the evaluation criterion from the common agreement of different experts. The basis is the fourteen evaluation criterion in Fig. 1 and Table 1. We set up ten different level of evaluation benchmark, from 1 to 10 points, the higher the score the greater the importance. We let the experts grade the importance of the fourteen evaluation criterion toward the information security level according to this scale. The subjects targeted for this survey are experts with long years experiences in the field, the total gathered questionnaires reach the amount of thirty, this number being in accordance with the central limit theorem.

In this study we classify the materiality level the experts assigned to different software vulnerability level and the highest score, lowest score, middle number, arithmetic average and geometric mean as a reference for filtering the evaluation criterion, as explained in Table 3. In this study the subjects were from the same population and the experts' opinions mean was calculated, supposing that the evaluation result of evaluation criterion formed a triangular fuzzy function. Therefore, we included the opinion of decision makers in the triangular fuzzy function and used the highest and lowest point of general mean function as the two extremities of the triangular fuzzy function of the experts' opinions, and used the geometric mean to represent the common opinion of the experts toward this influencing factor.

In this study we take the geometric mean of the influencing factors and evaluated level for evaluation criterion to decide the evaluation criterion threshold size and filter out the appropriate evaluation criterion. From Table 3 we can note the geometric mean of the fourteen evaluation criterion. In general, importance level more than 70% means "important". Therefore, in this study we choose 7.2 as the threshold to filter and obtain two influencing metrics: base and temporal, plus nine evaluation criteria.

### 4.2. Define the relative weight of the evaluation criterion

#### 4.2.1. Design of questionnaires and investigation

The hierarchy of the evaluation levels is as shown in Fig. 7, the main target being the software information security level. Taking into consideration two influencing metrics, respectively being the base and temporal plus the nine evaluation criterion and evaluate the effect of different risk levels on the information vulnerability.

AHP applies the comparison by pairs to calculate the weight of different attributes. However to know the relative weight between different attributes we must use the correct regulations. In AHP, to turn the written data into fuzzy numbers, this study relied on the most common by-pair comparison regulation: 1–9 (Chen and Hwang, 1992). Due to the fact that pairwise comparison matrix is reciprocal, only one comparison between two attributes is sufficient when designing the questionnaires in this stage. In other words, if there are $n$ attributes, we need to do $n(n-1)/2$ times comparison.

#### 4.2.2. Evaluating the relative weight of evaluation criterion

During the second stage of questionnaire survey, we can classify the weight of the influencing metrics as in Table 4. Due to the fact that in this study we divided the information security into five security levels, beside the lowest, highest and geometric mean, we added the square root of the multiply geometric mean by minimum and square root of the multiply geometric mean by maximum.

**Table 3**
The importance score of evaluation criterion toward software vulnerability security level.

| Aspects | Criteria | Maximum | Median | Minimum | Geometric mean | Arithmetic average |
|---|---|---|---|---|---|---|
| Base metric | Access vector | 10 | 10 | 8 | 9.68 | 9.7 |
| | Attack complexity | 10 | 9 | 8 | 9.17 | 9.2 |
| | Authentication instances | 10 | 9 | 8 | 8.77 | 8.8 |
| | Confidentiality impact | 10 | 9 | 7 | 8.65 | 8.7 |
| | Integrity impact | 10 | 9 | 7 | 8.75 | 8.8 |
| | Availability impact | 10 | 9 | 7 | 8.64 | 8.7 |
| Temporal metric | Exploitability tools & techniques | 10 | 9 | 7 | 8.66 | 8.7 |
| | Remediation level | 10 | 8 | 5 | 7.42 | 7.6 |
| | Report confidence | 10 | 8 | 5 | 7.98 | 8.1 |
| Environmental metric | Collateral damage potential | 10 | 7 | 5 | 6.87 | 7.1 |
| | Target Distribution | 10 | 7.5 | 3 | 6.05 | 6.6 |
| | Confidentiality requirement | 10 | 7 | 3 | 6.13 | 6.7 |
| | Integrity requirement | 10 | 7.5 | 3 | 6.09 | 6.6 |
| | Availability requirement | 10 | 6.5 | 3 | 5.98 | 6.5 |

*Note*: threshold = 7.2

**Table 4**
The weight of different influencing factors and perspectives.

| Weight | Aspects | |
|---|---|---|
| | Base metric | Temporal metric |
| *Minimum* | 0.6667 | 0.1667 |
| $\sqrt{Minimum \times Average}$ | 0.7130 | 0.1990 |
| *Average* | 0.7625 | 0.2375 |
| $\sqrt{Maximum \times Average}$ | 0.7971 | 0.2814 |
| *Maximum* | 0.8333 | 0.3333 |

The preference repartition of the weight of the evaluation criterion is as in Table 5. We can obtain about each evaluation criterion the mean, the geometric mean, the highest and lowest grade etc.. . . from experts' opinion. Then calculate the coefficient of variation from the individual arithmetic average and standard deviation ratio, helping us to retrieve the preference repartition of the evaluation criterion. In this study, to also assure a correct and logic evaluation process, the grading of evaluation criterion did not fulfill the consistency ratio (CR < 0.1), which we did not include into the equation of analysis.

From the preference repartition of the evaluation criterion (as shown in Table 5), we can realize that taking the arithmetic average into account, the most weighted criterion in Base metric category is access vector (0.2756), while the opposite is the integrity impact (0.0940). In the temporal metric category, the most weighted criterion is exploitability tools and techniques (0.4582), while the opposite is remediation level (0.2071). If we analyze from the geometric mean point of view, the situation is the same. On the other hand, if we cut in from the perspective of the coefficient of variation and range, we can obtain the relative difference and absolute difference. From the coefficient of variation perspective, the biggest difference of opinion appears on availability impact (0.4094) while the lowest difference of opinion is on integrity impact (0.1094). From the range point of view, the criterion on which the experts have the biggest divergence is report confidence (0.3267) and the smallest divergence is on integrity impact (0.0270). Due to the fact that different experts might have different knowledge and perception, the evaluation result of the same subject may of course have different results.

From the above analysis we can realize that the traditional AHP rely on the arithmetic average concept to solve the problem. But this will only reflect one of the possible ranges of the weight, not the entire situation. Therefore, to represent in a better way the subjective judgment and its divergence in the real world, in this study we apply the fuzzy number concept from the fuzzy sets theory, taking the biggest, smallest and average grade of experts on evaluation criterion to obtain the fuzzy weight of these criteria and interpret it through TFN. From the relative weight of different perspectives in Table 4 and the relative weight of different criteria in Table 5, we can calculate the fuzzy weight of the evaluation criteria as in Table 6.

Taking here the evaluation criterion $C_{11}$ (access vector) as an example, the TFN for the overall weight of the criterion (0.1395, 0.1712, 0.2101, 0.2677, 0.2677) and the range of its weight can be resumed in Fig. 8. The formula for calculating the weight as below:

$$f(x) = \begin{cases} 0 & , X \le 0.1395 \\ \dfrac{x - 0.1395}{0.2101 - 0.1395} & , 0.1395 \le X < 0.2101 \\ 1 & , X = 0.2101 \\ \dfrac{0.2677 - x}{0.2677 - 0.2101} & , 0.2101 \le X < 0.2677 \\ 0 & , X > 0.2677 \end{cases}$$

From the relative weight of the evaluation criteria in Table 6, we can know that for the evaluation criterion "attack complexity", its fuzzy weight has the biggest range, therefore implying that

**Table 5**
The preference repartition and weight of different evaluation criterion.

| Criteria | Maximum | Minimum | Arithmetic average | Geometric mean | Coefficient of variation | Range |
|---|---|---|---|---|---|---|
| $C_{11}$: Access vector | 0.3213 | 0.2092 | 0.2756 | 0.2721 | 0.1521 | 0.1121 |
| $C_{12}$: Attack complexity | 0.2733 | 0.0856 | 0.1821 | 0.1678 | 0.3708 | 0.1877 |
| $C_{13}$: Authentication instances | 0.2772 | 0.1537 | 0.2023 | 0.1967 | 0.2432 | 0.1235 |
| $C_{14}$: Confidentiality impact | 0.1808 | 0.0800 | 0.1383 | 0.1325 | 0.2666 | 0.1008 |
| $C_{15}$: Integrity impact | 0.1068 | 0.0798 | 0.0940 | 0.0935 | 0.1094 | 0.0270 |
| $C_{16}$: Availability impact | 0.1615 | 0.0566 | 0.1076 | 0.0982 | 0.4094 | 0.1049 |
| $C_{21}$: Exploitability tools and techniques | 0.5390 | 0.3119 | 0.4582 | 0.4476 | 0.2032 | 0.2271 |
| $C_{22}$: Remediation level | 0.2973 | 0.1638 | 0.2071 | 0.2011 | 0.2587 | 0.1335 |
| $C_{23}$: Report confidence | 0.4905 | 0.1638 | 0.3347 | 0.3101 | 0.3587 | 0.3267 |

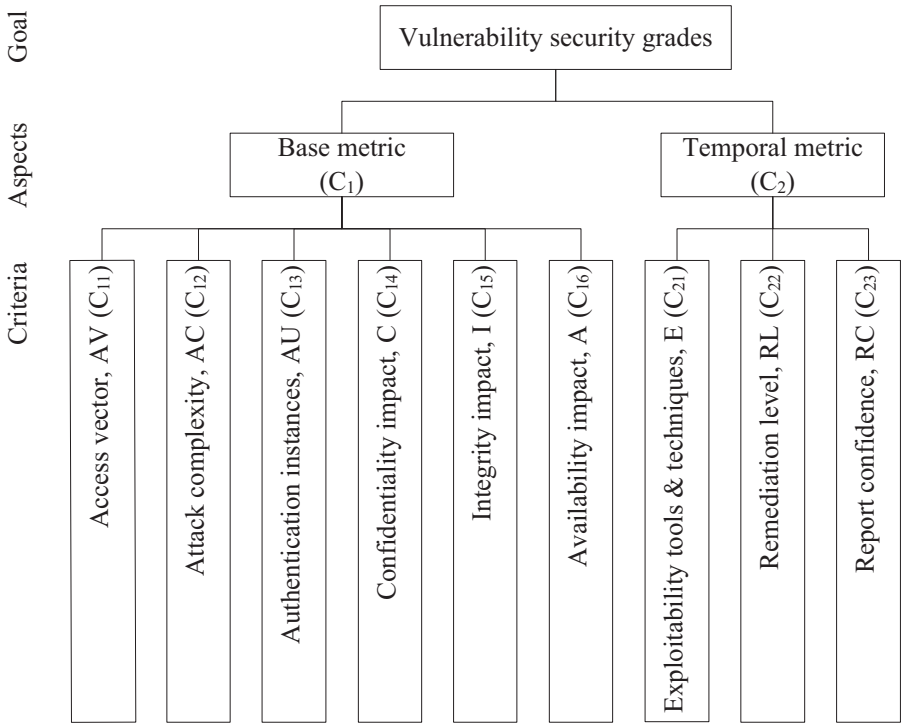


**Fig. 7.** Evaluation structure of software vulnerability security level.

**Table 6**
The fuzzy weight of evaluation criterion for information security level.

| Relative importance level of metrics | Relative importance of criteria | Weight of overall criterion |
|---|---|---|
| Base metric ($C_1$) (0.6667, 0.7130, 0.7625, 0.7971, 0.8333) | $C_{11}$(0.2092, 0.2401, 0.2756, 0.2975, 0.3213) | (0.1395, 0.1712, 0.2101, 0.2372, 0.2677) |
| | $C_{12}$(0.0856, 0.1249, 0.1821, 0.2231, 0.2733) | (0.0571, 0.0890, 0.1389, 0.1778, 0.2277) |
| | $C_{13}$(0.1537, 0.1763, 0.2023, 0.2368, 0.2772) | (0.1025, 0.1257, 0.1543, 0.1888, 0.2310) |
| | $C_{14}$(0.0800, 0.1052, 0.1383, 0.1581, 0.1808) | (0.0533, 0.0750, 0.1055, 0.1260, 0.1507) |
| | $C_{15}$(0.0798, 0.0866, 0.0940, 0.1002, 0.1068) | (0.0532, 0.0617, 0.0717, 0.0799, 0.0890) |
| | $C_{16}$(0.0566, 0.0780, 0.1076, 0.1318, 0.1615) | (0.0378, 0.0556, 0.0820, 0.1051, 0.1346) |
| Temporal metric ($C_2$) (0.1667, 0.1990, 0.2375, 0.2814, 0.3333) | $C_{21}$(0.3119, 0.3780, 0.4582, 0.4969, 0.5390) | (0.0520, 0.0752, 0.1088, 0.1398, 0.1796) |
| | $C_{22}$(0.1638, 0.1842, 0.2071, 0.2481, 0.2973) | (0.0273, 0.0366, 0.0492, 0.0698, 0.0991) |
| | $C_{23}$(0.1638, 0.2341, 0.3347, 0.4052, 0.4905) | (0.0273, 0.0466, 0.0795, 0.1140, 0.1635) |

the experts have very divergent opinion toward it, while for the criterion "integrity impact" they have common agreement most of the time.

### 4.3. Formulation of membership function

In this study we formulate membership function based on qualitative criterion. To build the membership function of the security level evaluation for the qualitative benchmark, we use Eq. (10) and the performance appraisal level of experts toward the qualitative influencing factor to individually obtain the membership frequency of each security level with the information security levels poor, fair, moderate, good and excellent, as in Tables 7–15. After this we also draw out the bar chart of the information security levels poor, fair, moderate, good and excellent to show the growing or decreasing tendency of each membership, as shown in Fig. 9.

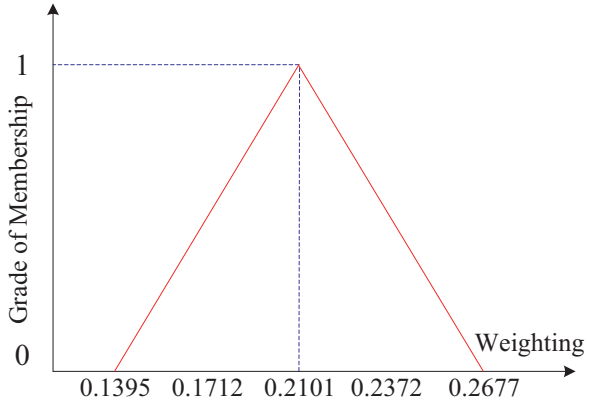


**Fig. 8.** The triangular fuzzy number of the evaluation criterion "access vector" ($C_{11}$).

### 4.4. Defining the λ fuzzy measure

In this study, to define the λ fuzzy measure, we applied the characteristic value method perception and compared all sets by pair. Taking as an example the questionnaire result from one of the experts we surveyed:

$$\begin{array}{c} \\ x_1 \\ x_2 \\ x_1, x_2 \end{array} \begin{array}{c} \begin{array}{ccc} x_1 & x_2 & x_1, x_2 \end{array} \\ \begin{bmatrix} 1 & 3 & 1/3 \\ 1/3 & 1 & 1/4 \\ 3 & 4 & 1 \end{bmatrix} \end{array}$$

After calculation, the characteristic vector is as below:
$\omega = (0.2684, 0.1172, 0.6144)$.
Through normalization making the biggest amount as 1 we obtain:

**Table 7**
Grade of membership for the access vector.

| Access vector ($C_{11}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| 1. Physical isolation | 0.00 | 0.00 | 0.00 | 0.07 | 0.93 |
| 2. Physical | 0.00 | 0.00 | 0.53 | 0.40 | 0.07 |
| 3. Adjacent network | 0.00 | 0.00 | 0.40 | 0.60 | 0.00 |
| 4. Intranet | 0.00 | 0.07 | 0.63 | 0.30 | 0.00 |
| 5. Extranet | 0.00 | 0.67 | 0.33 | 0.00 | 0.00 |
| 6. Internet | 0.37 | 0.33 | 0.30 | 0.00 | 0.00 |
| 7. Wireless | 0.93 | 0.07 | 0.00 | 0.00 | 0.00 |
| 8. Remote access | 0.97 | 0.03 | 0.00 | 0.00 | 0.00 |

Grade of membership:
$\mu_{Physical\ isolation} = (0.00, 0.00, 0.00, 0.07, 0.93)$
$\mu_{Physical} = (0.00, 0.00, 0.53, 0.40, 0.07)$
$\mu_{Adjacent\ network} = (0.00, 0.00, 0.40, 0.60, 0.00)$
$\mu_{Intranet} = (0.00, 0.\ 07, 0.63, 0.\ 30, 0.00)$
$\mu_{Extranet} = (0.00, 0.67, 0.33, 0.00, 0.00)$
$\mu_{Internet} = (0.37, 0.33, 0.30, 0.00, 0.00)$
$\mu_{Wireless} = (0.93, 0.07, 0.00, 0.00, 0.00)$
$\mu_{Remote\ access} = (0.97, 0.03, 0.00, 0.00, 0.00)$

**Table 8**
Grade of membership for the attack complexity.

| Attack complexity ($C_{12}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| 1. Numeric errors | 0.00 | 0.00 | 0.57 | 0.43 | 0.00 |
| 2. Format string vulnerability | 0.00 | 0.00 | 0.27 | 0.73 | 0.00 |
| 3. Link following | 0.00 | 0.00 | 0.40 | 0.60 | 0.00 |
| 4. Path traversal | 0.00 | 0.00 | 0.50 | 0.50 | 0.00 |
| 5. Race conditions | 0.00 | 0.00 | 0.50 | 0.50 | 0.00 |
| 6. Resource management errors | 0.00 | 0.00 | 0.77 | 0.23 | 0.00 |
| 7. Credentials management | 0.00 | 0.27 | 0.50 | 0.23 | 0.00 |
| 8. Cryptographic issues | 0.00 | 0.23 | 0.60 | 0.17 | 0.00 |
| 9. Configuration | 0.00 | 0.30 | 0.70 | 0.00 | 0.00 |
| 10. Security misconfiguration | 0.00 | 0.37 | 0.63 | 0.00 | 0.00 |
| 11. Cross-site request forgery (CSRF) | 0.07 | 0.50 | 0.43 | 0.00 | 0.00 |
| 12. Permissions, privileges, and access control | 0.00 | 0.60 | 0.40 | 0.00 | 0.00 |
| 13. Information leak/disclosure | 0.00 | 0.10 | 0.83 | 0.07 | 0.00 |
| 14. Input validation | 0.00 | 0.23 | 0.73 | 0.04 | 0.00 |
| 15. Authentication issues | 0.00 | 0.47 | 0.53 | 0.00 | 0.00 |
| 16. Cross-site scripting (XSS) | 0.06 | 0.67 | 0.27 | 0.00 | 0.00 |
| 17. Buffer errors | 0.30 | 0.47 | 0.20 | 0.03 | 0.00 |
| 18. Code injections | 0.40 | 0.57 | 0.03 | 0.00 | 0.00 |
| 19. OS command injections | 0.57 | 0.37 | 0.06 | 0.00 | 0.00 |
| 20. SQL injections | 0.27 | 0.70 | 0.03 | 0.00 | 0.00 |

Grade of membership:
$\mu_{Numeric\ errors} = (0.00, 0.00, 0.57, 0.43, 0.00)$
$\mu_{Format\ string\ vulnerability} = (0.00, 0.00, 0.27, 0.73, 0.00)$
$\mu_{Link\ following} = (0.00, 0.00, 0.40, 0.60, 0.00)$
$\mu_{Path\ traversal} = (0.00, 0.00, 0.50, 0.50, 0.00)$
$\mu_{Race\ conditions} = (0.00, 0.00, 0.50, 0.50, 0.00)$
$\mu_{Resource\ management\ errors} = (0.00, 0.00, 0.77, 0.23, 0.00)$
$\mu_{Credentials\ management} = (0.00, 0.27, 0.50, 0.23, 0.00)$
$\mu_{Cryptographic\ issues} = (0.00, 0.23, 0.60, 0.17, 0.00)$
$\mu_{Configuration} = (0.00, 0.30, 0.70, 0.00, 0.00)$
$\mu_{Security\ misconfiguration} = (0.00, 0.37, 0.63, 0.00, 0.00)$
$\mu_{CSRF} = (0.07, 0.50, 0.43, 0.00, 0.00)$
$\mu_{Permissions,\ privileges,\ and\ access\ control} = (0.00, 0.60, 0.40, 0.00, 0.00)$
$\mu_{Information\ leak/disclosure} = (0.00, 0.10, 0.83, 0.07, 0.00)$
$\mu_{Input\ validation} = (0.00, 0.23, 0.73, 0.04, 0.00)$
$\mu_{Authentication\ issues} = (0.00, 0.47, 0.53, 0.00, 0.00)$
$\mu_{XSS} = (0.06, 0.67, 0.27, 0.00, 0.00)$
$\mu_{Buffer\ errors} = (0.30, 0.47, 0.20, 0.03, 0.00)$
$\mu_{Code\ injections} = (0.40, 0.57, 0.03, 0.00, 0.00)$
$\mu_{OS\ command\ injections} = (0.57, 0.37, 0.06, 0.00, 0.00)$
$\mu_{SQL\ injections} = (0.27, 0.70, 0.03, 0.00, 0.00)$

**Table 9**
Grade of membership for the authentication instances.

| Authentication instances ($C_{13}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| Entity | 0.00 | 0.00 | 0.00 | 0.87 | 0.13 |
| Multiple | 0.00 | 0.00 | 0.00 | 0.67 | 0.33 |
| Single | 0.00 | 0.03 | 0.80 | 0.17 | 0.00 |
| None | 0.90 | 0.10 | 0.00 | 0.00 | 0.00 |

Grade of membership:
$\mu_{Entity} = (0.00, 0.00, 0.00, 0.87, 0.13)$
$\mu_{Multiple} = (0.00, 0.00, 0.00, 0.67, 0.33)$
$\mu_{Single} = (0.00, 0.03, 0.80, 0.17, 0.00)$
$\mu_{None} = (0.90, 0.10, 0.00, 0.00, 0.00)$

**Table 10**
Grade of membership for the confidentiality impact.

| Confidentiality impact ($C_{14}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| 1. $C_1$: The divulgation of information content will not add any damage on the organization. | 0.00 | 0.00 | 0.00 | 0.10 | 0.90 |
| 2. $C_2$: The divulgation of information content will damage the organization however the impact will still be bearable. | 0.00 | 0.00 | 0.23 | 0.77 | 0.00 |
| 3. $C_3$: The divulgation of information content will affect the regional reputation of the organization or the rights of people within the range of >100, <1000. | 0.06 | 0.77 | 0.17 | 0.00 | 0.00 |
| 4. $C_4$: The divulgation of information content will affect the national reputation of the organization or more than 1000 people rights. | 0.43 | 0.57 | 0.00 | 0.00 | 0.00 |
| Grade of membership: | | | | | |
| $\mu_{C_1} = (0.00, 0.00, 0.00, 0.10, 0.90)$ | | | $\mu_{C_3} = (0.06, 0.77, 0.17, 0.00, 0.00)$ | | |
| $\mu_{C_2} = (0.00, 0.00, 0.23, 0.77, 0.00)$ | | | $\mu_{C_4} = (0.43, 0.57, 0.00, 0.00, 0.00)$ | | |

**Table 11**
Grade of membership for the integrity impact.

| Integrity impact ($C_{15}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| 1. I1: The incomplete data content will affect small quantity of personnel or individual users | 0.00 | 0.00 | 0.00 | 0.73 | 0.27 |
| 2. I2: The incomplete data content will block the operation of entire department and less than 100 people rights being violated. | 0.00 | 0.00 | 0.80 | 0.20 | 0.00 |
| 3. I3: The incomplete data content will block part of the organization operation and more than 100 people, less than 1000 people rights being violated. | 0.10 | 0.80 | 0.10 | 0.00 | 0.00 |
| 4. I4: The incomplete data content will block the entire organization operation and more than 1000 people rights being violated. | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| Grade of membership: | | | | | |
| $\mu_{I1} = (0.00, 0.00, 0.00, 0.73, 0.27)$ | | | $\mu_{I3} = (0.10, 0.80, 0.10, 0.00, 0.00)$ | | |
| $\mu_{I2} = (0.00, 0.00, 0.80, 0.20, 0.00)$ | | | $\mu_{I4} = (0.83, 0.17, 0.00, 0.00, 0.00)$ | | |

**Table 12**
Grade of membership for the availability impact.

| Availability impact ($C_{16}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| 1. A1: The loss or damage of data will affect the operation of small part of personnel or few users, the acceptable range for service stop > 12 h. | 0.00 | 0.00 | 0.00 | 0.87 | 0.13 |
| 2. A2: The loss or damage of data will affect the operation of entire department, the acceptable range for service stop 1–12 h. | 0.00 | 0.14 | 0.43 | 0.43 | 0.00 |
| 3. A3: The loss or damage of data will affect the operation between departments, the acceptable range for service stop 5 min–1 h. | 0.00 | 0.50 | 0.17 | 0.33 | 0.00 |
| 4. A4: The loss or damage of data will affect the entire organization operation with outsiders, the acceptable range for service stop less than 5 min. | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| Grade of membership: | | | | | |
| $\mu_{A1} = (0.00, 0.00, 0.00, 0.13, 0.87)$ | | | $\mu_{A3} = (0.00, 0.50, 0.17, 0.33, 0.10)$ | | |
| $\mu_{A2} = (0.00, 0.14, 0.43, 0.43, 0.00)$ | | | $\mu_{A4} = (0.83, 0.17, 0.00, 0.00, 0.00)$ | | |

**Table 13**
Grade of membership for the exploitability tools and techniques.

| Exploitability tools and techniques ($C_{21}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| 1. Unproved | 0.00 | 0.00 | 0.87 | 0.13 | 0.00 |
| 2. Proof-of-concept | 0.00 | 0.37 | 0.63 | 0.00 | 0.00 |
| 3. Functional | 0.27 | 0.73 | 0.00 | 0.00 | 0.00 |
| 4. High | 0.93 | 0.07 | 0.00 | 0.00 | 0.00 |
| Grade of membership: | | | | | |
| $\mu_{Unproved} = (0.00, 0.00, 0.87, 0.13, 0.00)$ | | | $\mu_{Functional} = (0.27, 0.73, 0.00, 0.00, 0.00)$ | | |
| $\mu_{Proof\text{-}of\text{-}concept} = (0.00, 0.37, 0.63, 0.00, 0.00)$ | | | $\mu_{High} = (0.93, 0.07, 0.00, 0.00, 0.00)$ | | |

**Table 14**
Grade of membership for the remediation level.

| Remediation level ($C_{22}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| 1. Official fix | 0.00 | 0.00 | 0.00 | 0.07 | 0.93 |
| 2. Temporary fix | 0.00 | 0.00 | 0.87 | 0.07 | 0.06 |
| 3. Workaround | 0.00 | 0.83 | 0.17 | 0.00 | 0.00 |
| 4. Unavailable | 0.87 | 0.13 | 0.00 | 0.00 | 0.00 |

Grade of membership:
$\mu_{Official\ fix} = (0.00, 0.00, 0.00, 0.07, 0.93)$
$\mu_{Temporary\ fix} = (0.00, 0.00, 0.87, 0.07, 0.06)$
$\mu_{Workaround} = (0.00, 0.83, 0.17, 0.00, 0.00)$
$\mu_{Unavailable} = (0.87\ 0.13, 0.00, 0.00, 0.00)$

**Table 15**
Grade of membership for the report confidence.

| Remediation level ($C_{23}$) | Grade of membership | | | | |
|---|---|---|---|---|---|
| | Poor | Fair | Moderate | Good | Excellent |
| 1. Unconfirmed | 0.00 | 0.00 | 0.93 | 0.07 | 0.00 |
| 2. Uncorroborative | 0.00 | 0.10 | 0.87 | 0.03 | 0.00 |
| 3. Corroborative | 0.13 | 0.83 | 0.04 | 0.00 | 0.00 |
| 4. Confirmed | 0.87 | 0.13 | 0.00 | 0.00 | 0.00 |

Grade of membership:
$\mu_{Unconfirmed} = (0.00, 0.00, 0.93, 0.07, 0.00)$
$\mu_{Uncorroborative} = (0.00, 0.10, 0.87, 0.03, 0.00)$
$\mu_{Corroborative} = (0.13, 0.83, 0.04, 0.00, 0.00)$
$\mu_{Confirmed} = (0.87, 0.13, 0.00, 0.00, 0.00)$

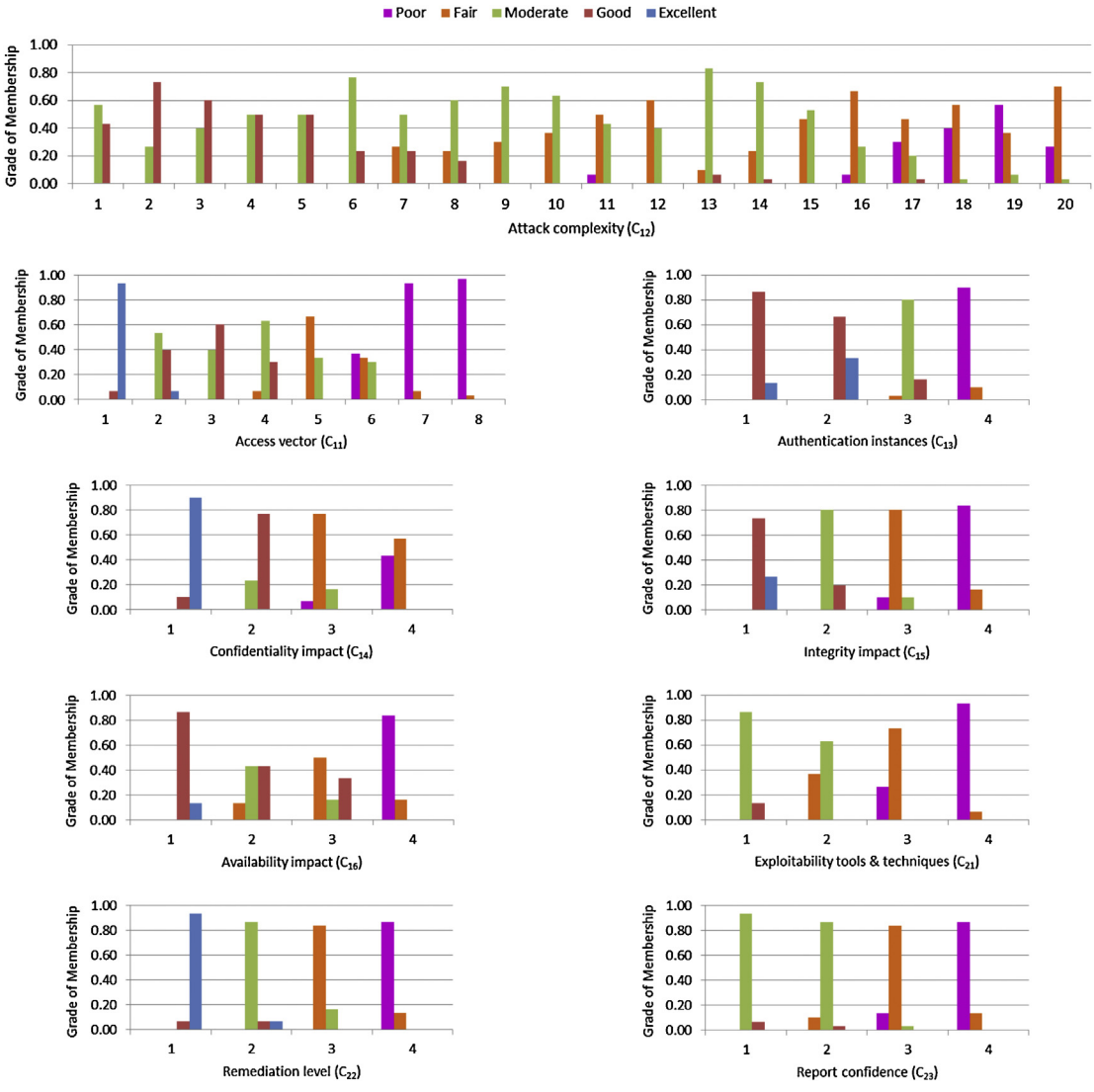


**Fig. 9.** Grade of membership of each criteria.

**Table 16**
The opinion of experts toward importance level of different metrics.

| Weight | Aspects | |
|---|---|---|
| | Base metric $g_\lambda(\{x_1\})$ | Temporal metric $g_\lambda(\{x_2\})$ |
| Minimum | 0.22 | 0.08 |
| Average | 0.40 | 0.18 |
| Maximum | 0.55 | 0.32 |

$\omega = (0.44, 0.19, 1.00)$.

Then we can calculate the importance level of different metrics as below:

$\omega_1 = g_\lambda(\{x_1\}) = 0.44$ (base metric importance level),

$\omega_2 = g_\lambda(\{x_2\}) = 0.19$ (temporal metric importance level),

$\omega_3 = g_\lambda(\{x_1, x_2\}) = 1.00$.

From the opinion of this expert, we know that $g_\lambda(\{x_1,x_2\}) > g_\lambda(\{x_1\}) + g_\lambda(\{x_2\})$, showing that the effect of different metrics toward information security level does not have an additive nature, it rather has the multiplicative effect. The importance assigned by experts on different metrics are in Table 16. We can see that the experts' opinions fulfill the consistency examination and do not have additive nature. The common opinion of the experts (average) being:

$\omega_1 = g_\lambda(\{x_1\}) = 0.40$,

$\omega_2 = g_\lambda(\{x_2\}) = 0.18$,

$\omega_3 = g_\lambda(\{x_1, x_2\}) = 1.00$.

On the basis of the above, when evaluating an information security status from the perspective of base and temporal metric, it does not show an additive nature. Moreover, the subjective opinion did not absolutely have an additive nature either. For example, vulnerability $A$ base metric risk score (weight 0.5) 60 points, temporal metric (weight 0.3) 60 points, the calculation gives $60 \times 0.5 + 60 \times 0.3 = 48$ points. Vulnerability $B$ base metric risk score (weight 0.5) 90 points, temporal metric (weight 0.3) 20 points, the calculation gives $90 \times 0.5 + 20 \times 0.3 = 51$ points. From the additive point of view vulnerability $A$ is securer, however from the fuzzy measure point of view (supposing that $\lambda = 1.333$ fulfill the multiplicative nature), The importance level of $A$, $B$ are respectively $g(A) = 0.5$, $g(B) = 0.5$, $g(A, B) = 1$), as shown in Fig. 10. The risk score of vulnerability $A$ will then be $\int h_A dg = 60 \times 1.0 = 60$, and for vulnerability $B$ it will be $\int h_B dg = 20 \times 1.0 + (90 - 20) \times 0.5 = 55$. As a result, the risk level of vulnerability $A$ is higher.

## 5. Case study

The information source of this study is the national vulnerabilities database (NVD, 2008). We chose four vulnerabilities as evaluation targets: CVE-2008-1611, CVE-2009-1126, CVE-2009-1730, and CVE-2011-2442 as explained in Table 17. We apply therefore the model formulated in this study to evaluate the level of vulnerability. During the process, we first apply the fuzzy synthetic decision making model on the base and temporal metric parts, then we apply the fuzzy integral decision making process.

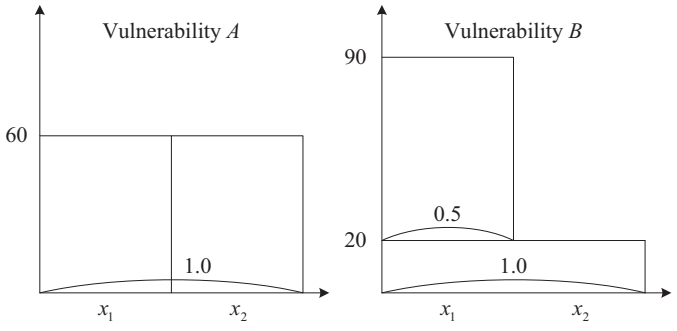


**Fig. 10.** Comparison of vulnerability.

### 5.1. Fuzzy synthetic decision making

The process of fuzzy synthetic decision making is as follow:

**Step 1**: Defining the evaluation criterion and grade level.

Confirm the set for vulnerability evaluation:

$X$ = {CVE-2008-1611, CVE-2009-1126, CVE-2009-1730, CVE-2011-2442}.

First grade for evaluation benchmark set:

$Y$ = {Base metric, Temporal metric}.

Second grade for evaluation benchmark set:

$Y_1$ = {AV, AC, AU, C, I, A}; $Y_2$ = {E, RL, RC}.

Performance appraisal level set:

$Z$ = {Poor, Fair, Moderate, Good, Excellent}.

**Step 2**: Define the weight of each evaluation criterion. Obtain the overall evaluation weight of metric weight and criterion relative weight from Section 4.2.2.

**Step 3**: Define the security membership function of different evaluation criteria. First collect experts' opinions in verbal way then convert the result into membership grade. Obtain the security membership function from Section 4.3.

For example, the calculation of security membership function for CVE-2008-1611 is as shown in Table 18.

**Step 4**: Run the fuzzy synthetic decision making model, following explanation in Section 3.2.4. Multiply the individual security membership grade with the fuzzy weight of information security level evaluation criterion from Table 6. Taking the "access vector" as an example, the result is as shown in Table 19.

$$C_{11} = [0.1395,\ 0.1712,\ 0.2101,\ 0.2372,\ 0.2677] \cdot \tilde{[0.9667,\ 0.0333,\ 0.00,\ 0.00,\ 0.00]} = [0.1348,\ 0.0057,\ 0,\ 0,\ 0]$$

**Step 5**: Defuzzication, following the indications in Section 3.2.5. In this study we apply $[0, 0.25, 0.5, 0.75, 1]^t$. Taking the access vector as an example, the results are as shown in Table 19.

$$r_{11} = [0.1348,\ 0.0057,\ 0,\ 0,\ 0] \cdot [0,\ 0.25,\ 0.5,\ 0.75,\ 1]^t = 0.0014$$

### 5.2. Fuzzy integral decision making

Through the fuzzy synthetic decision making model we obtained the representative data about the vulnerability of base and temporal metrics, which we can use in the fuzzy integral decision making model, the main steps as below:

**Step 1**: Under each evaluation criterion, apply the fuzzy synthetic decision making model and take out the fuzzy nature to obtain the score of the evaluated vulnerability in the two metrics. As shown in Table 20.

**Step 2**: Calculate the importance level $g(H_n)$. From Table 16 we know that: $g(H_{Base}) = 0.40$, $g(H_{Temporal}) = 0.18$

**Step 3**: Fuzzy integral decision making of vulnerability level.

$$\int h_{CVE-2008-1611} dg = 0.0487 \times 1 + (0.1114 - 0.0487) \times 0.18 = 0.059986$$

$$\int h_{CVE-2009-1126} dg = (0.2242 - 0.0989) \times 0.40 + 0.0989 \times 1 = 0.14902$$

**Table 17**
Descriptions of the vulnerabilities.

| CVE-ID | Vulnerability type | CVSS score |
|---|---|---|
| CVE-2008-1611 | Buffer errors | 10.0 |
| Stack-based buffer overflow in TFTP Server SP 1.4 for Windows allows remote attackers to cause a denial of service or execute arbitrary code via a long filename in a read or write request. | | |
| CVE-2009-1126 | Input validation | 7.2 |
| The kernel in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly validate the user-mode input associated with the editing of an unspecified desktop criterion, which allows local users to gain privileges via a crafted application, aka "Windows Desktop Criterion Edit Vulnerability." | | |
| CVE-2009-1730 | Path traversal | 10.0 |
| Multiple directory traversal vulnerabilities in NetMechanica NetDecision TFTP Server 4.2 allow remote attackers to read or modify arbitrary files via directory traversal sequences in the (1) GET or (2) PUT command. | | |
| CVE-2011-2442 | Input validation | 9.3 |
| Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error vulnerability." | | |

$$\int h_{CVE-2009-1730}dg = (0.1214 - 0.1114) \times 0.40 + 0.1114 \times 1 = 0.1154$$

$$\int h_{CVE-2011-2442}dg = (0.1250 - 0.1114) \times 0.40 + 0.1114 \times 1 = 0.11684$$

**Step 4**: Classify the vulnerabilities according to their level, as shown in Table 20.

## 6. Discussion and conclusion

In the related research, CVSS and improved VRSS both apply base metric to calculate the vulnerability scores. However, through this actual study, we realize that even when taking only base metric for fuzzy synthetic decision making, the grading order obtained is similar to the previous research result, as shown in Table 20.

**Table 18**
Membership grade for calculation result of vulnerability.

| Cases | Criteria | Values | Performance appraisal benchmark membership grade for each level | | | | |
|---|---|---|---|---|---|---|---|
| | | | Poor | Fair | Moderate | Good | Excellent |
| CVE-2008-1611 | AV | Remote access | 0.97 | 0.03 | 0.00 | 0.00 | 0.00 |
| | AC | Buffer errors | 0.30 | 0.47 | 0.20 | 0.03 | 0.00 |
| | AU | None | 0.90 | 0.10 | 0.00 | 0.00 | 0.00 |
| | C | C4 | 0.43 | 0.57 | 0.00 | 0.00 | 0.00 |
| | I | I4 | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| | A | A4 | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| | E | Functional | 0.27 | 0.73 | 0.00 | 0.00 | 0.00 |
| | RL | Official fix | 0.00 | 0.00 | 0.00 | 0.07 | 0.93 |
| | RC | Confirmed | 0.87 | 0.13 | 0.00 | 0.00 | 0.00 |
| CVE-2009-1126 | AV | Physical | 0.00 | 0.00 | 0.53 | 0.40 | 0.07 |
| | AC | Input validation | 0.00 | 0.23 | 0.73 | 0.04 | 0.00 |
| | AU | None | 0.90 | 0.10 | 0.00 | 0.00 | 0.00 |
| | C | C4 | 0.43 | 0.57 | 0.00 | 0.00 | 0.00 |
| | I | I4 | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| | A | A4 | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| | E | High | 0.93 | 0.07 | 0.00 | 0.00 | 0.00 |
| | RL | Official fix | 0.00 | 0.00 | 0.00 | 0.07 | 0.93 |
| | RC | Confirmed | 0.87 | 0.13 | 0.00 | 0.00 | 0.00 |
| CVE-2009-1730 | AV | Remote access | 0.97 | 0.03 | 0.00 | 0.00 | 0.00 |
| | AC | Path traversal | 0.00 | 0.00 | 0.50 | 0.50 | 0.00 |
| | AU | None | 0.90 | 0.10 | 0.00 | 0.00 | 0.00 |
| | C | C4 | 0.43 | 0.57 | 0.00 | 0.00 | 0.00 |
| | I | I4 | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| | A | A4 | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| | E | Functional | 0.27 | 0.73 | 0.00 | 0.00 | 0.00 |
| | RL | Official fix | 0.00 | 0.00 | 0.00 | 0.07 | 0.93 |
| | RC | Confirmed | 0.87 | 0.13 | 0.00 | 0.00 | 0.00 |
| CVE-2011-2442 | AV | Internet | 0.37 | 0.33 | 0.30 | 0.00 | 0.00 |
| | AC | Input validation | 0.00 | 0.23 | 0.73 | 0.04 | 0.00 |
| | AU | None | 0.90 | 0.10 | 0.00 | 0.00 | 0.00 |
| | C | C4 | 0.43 | 0.57 | 0.00 | 0.00 | 0.00 |
| | I | I4 | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| | A | A4 | 0.83 | 0.17 | 0.00 | 0.00 | 0.00 |
| | E | Functional | 0.27 | 0.73 | 0.00 | 0.00 | 0.00 |
| | RL | Official fix | 0.00 | 0.00 | 0.00 | 0.07 | 0.93 |
| | RC | Confirmed | 0.87 | 0.13 | 0.00 | 0.00 | 0.00 |

**Table 19**
The fuzzy integral decision making result and taking out fuzzy nature.

| Cases | Criteria | Values of fuzzy synthetic decision | Defuzzification values | Defuzzification values of the aspect |
|---|---|---|---|---|
| CVE-2008-1611 | AV | (0.1348, 0.0057, 0.0000, 0.0000, 0.0000) | 0.0014 | 0.0487 |
| | AC | (0.0171, 0.0416, 0.0278, 0.0059, 0.0000) | 0.0287 | |
| | AU | (0.0922, 0.0126, 0.0000, 0.0000, 0.0000) | 0.0031 | |
| | C | (0.0231, 0.0425, 0.0000, 0.0000, 0.0000) | 0.0106 | |
| | I | (0.0443, 0.0103, 0.0000, 0.0000, 0.0000) | 0.0026 | |
| | A | (0.0314, 0.0093, 0.0000, 0.0000, 0.0000) | 0.0023 | |
| | E | (0.0139, 0.0552, 0.0000, 0.0000, 0.0000) | 0.0138 | 0.1114 |
| | RL | (0.0000, 0.0000, 0.0000, 0.0047, 0.0925) | 0.0960 | |
| | RC | (0.0237, 0.0062, 0.0000, 0.0000, 0.0000) | 0.0016 | |
| | Sum | (0.3805, 0.1833, 0.0278, 0.0106, 0.0925) | 0.1601 | 0.1601 |
| CVE-2009-1126 | AV | (0.0000, 0.0000, 0.1121, 0.0949, 0.0178) | 0.1450 | 0.2242 |
| | AC | (0.0000, 0.0208, 0.1018, 0.0059, 0.0000) | 0.0606 | |
| | AU | (0.0922, 0.0126, 0.0000, 0.0000, 0.0000) | 0.0031 | |
| | C | (0.0231, 0.0425, 0.0000, 0.0000, 0.0000) | 0.0106 | |
| | I | (0.0443, 0.0103, 0.0000, 0.0000, 0.0000) | 0.0026 | |
| | A | (0.0314, 0.0093, 0.0000, 0.0000, 0.0000) | 0.0023 | |
| | E | (0.0485, 0.0050, 0.0000, 0.0000, 0.0000) | 0.0013 | 0.0989 |
| | RL | (0.0000, 0.0000, 0.0000, 0.0047, 0.0925) | 0.0960 | |
| | RC | (0.0237, 0.0062, 0.0000, 0.0000, 0.0000) | 0.0016 | |
| | Sum | (0.2633, 0.1066, 0.2139, 0.1055, 0.1103) | 0.3231 | 0.3231 |
| CVE-2009-1730 | AV | (0.1348, 0.0057, 0.0000, 0.0000, 0.0000) | 0.0014 | 0.1214 |
| | AC | (0.0000, 0.0000, 0.0694, 0.0889, 0.0000) | 0.1014 | |
| | AU | (0.0922, 0.0126, 0.0000, 0.0000, 0.0000) | 0.0031 | |
| | C | (0.0231, 0.0425, 0.0000, 0.0000, 0.0000) | 0.0106 | |
| | I | (0.0443, 0.0103, 0.0000, 0.0000, 0.0000) | 0.0026 | |
| | A | (0.0314, 0.0093, 0.0000, 0.0000, 0.0000) | 0.0023 | |
| | E | (0.0139, 0.0552, 0.0000, 0.0000, 0.0000) | 0.0138 | 0.1114 |
| | RL | (0.0000, 0.0000, 0.0000, 0.0047, 0.0925) | 0.0960 | |
| | RC | (0.0237, 0.0062, 0.0000, 0.0000, 0.0000) | 0.0016 | |
| | Sum | (0.3634, 0.1417, 0.0694, 0.0936, 0.0925) | 0.2328 | 0.2328 |
| CVE-2011-2442 | AV | (0.0511, 0.0571, 0.0630, 0.0000, 0.0000) | 0.0458 | 0.1250 |
| | AC | (0.0000, 0.0208, 0.1018, 0.0059, 0.0000) | 0.0606 | |
| | AU | (0.0922, 0.0126, 0.0000, 0.0000, 0.0000) | 0.0031 | |
| | C | (0.0231, 0.0425, 0.0000, 0.0000, 0.0000) | 0.0106 | |
| | I | (0.0443, 0.0103, 0.0000, 0.0000, 0.0000) | 0.0026 | |
| | A | (0.0314, 0.0093, 0.0000, 0.0000, 0.0000) | 0.0023 | |
| | E | (0.0139, 0.0552, 0.0000, 0.0000, 0.0000) | 0.0138 | 0.1114 |
| | RL | (0.0000, 0.0000, 0.0000, 0.0047, 0.0925) | 0.0960 | |
| | RC | (0.0237, 0.0062, 0.0000, 0.0000, 0.0000) | 0.0016 | |
| | Sum | (0.2797, 0.2139, 0.1649, 0.0106, 0.0925) | 0.2364 | 0.2364 |

Moreover, this actual research included several influential factors and thanks to the common point of view of experts in the field, filter out the adequate evaluating criteria. On the other hand, the numbers obtained in previous risk evaluation symbolize the risks: the bigger the amount the greater the risk, while in this research the numbers obtained are security grades, the higher or the bigger the amount the higher is the security status.

The results show through fuzzy synthetic decision making that evaluation values can be used as basis for security improvement prioritization and that they can also be used to evaluate the security degree of new published software. The evaluation process of fuzzy synthetic decision making can also be applied before the software vulnerability level has been disclosed by official authority, to evaluate security level and serve as reference for improvement procedure. Meaning that relying on different evaluation criteria and their membership function we can realize the extent to which each factor will influence information security. The closer the membership function is to one, the securer it is.

However in this study we apply the fuzzy synthetic decision making model to handle the various influencing factors of software vulnerability and have a complete evaluation. After this through the fuzzy integral decision making model, we take into consideration the issue of multiply-add nature of security level between different influencing metrics. To improve the fuzzy synthetic decision making model we suppose the existence of independence and additive nature between different evaluation metrics and evaluation

**Table 20**
Vulnerability comparison.

| Cases | Vulnerability scoring | | Security grades | | |
|---|---|---|---|---|---|
| | CVSS | Improved VRSS | Base metric of fuzzy synthetic decision | Fuzzy synthetic decision | Fuzzy integral |
| CVE-2008-1611 | 10.0 | 9.86 | 0.0487 | 0.1601 | 0.0600 |
| CVE-2009-1126 | 7.2 | 9.34 | 0.2242 | 0.3231 | 0.1490 |
| CVE-2009-1730 | 10.0 | 9.51 | 0.1214 | 0.2328 | 0.1154 |
| CVE-2011-2442 | 9.3 | 9.46 | 0.1250 | 0.2364 | 0.1168 |

criterion. Then via the fuzzy integral evaluation with non-additive concept, we obtain the overall evaluation result of the software vulnerability in different security levels of each metric. The main goal of this step is to include the subjectivity of human from the real world in the equation. The result of this study shows that from the experts' point of view, the influencing factors of software vulnerability level from different metrics did not fulfill an additive nature. They rather turned out to have a multiplicative effect.

## Acknowledgments

The authors would like to express our appreciation to the anonymous reviewers for their invaluable suggestions. Furthermore, the authors would also like to thank the support from the CyberTrust Technology Institute, Institute for Information Industry, and the Electronic Monitor and Surveillance Center, Criminal Investigation Bureau, for their invaluable help.

## References

Anderson, R., Moore, T., 2006. The economics of information security. Science 314 (5799), 610–613.
Arora, A., Krishnan, R., Telang, R., Yang, Y., 2010. An empirical analysis of software vendors' patch release behavior: impact of vulnerability disclosure. Information System Research 21 (1), 115–132.
Asai, K., 1995. Fuzzy Systems for Management – Fuzzy Evaluation, 1st ed. IOS Press, Amsterdam, The Netherlands, pp. 43–55.
Buckley, J.J., 1985. Fuzzy hierarchical analysis. Fuzzy Sets and Systems 17 (3), 233–247.
Buckley, J.J., 2004. Fuzzy Statistics, 1st ed. Springer, Birmingham, AL, USA.
Cavusoglu, H., Mishra, B., Raghunathan, S., 2004. 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 9 (1), 69–104.
Chen, S.J., Hwang, C.L., 1992. Fuzzy Multiple Attribute Decision Making: Methods and Applications – a State-of-the-art Survey. Springer-Verlag, New York, pp. 465–486.
Chen, T.Y., Wang, J.C., 2001. Identification of λ-fuzzy measures using sampling design and genetic algorithms. Fuzzy Sets and Systems 123 (3), 321–341.
Choquet, G., 1953. Theory of capacities. Annales de l'institut Fourier 5, 131–295.
Crampton, J., 2011. Practical and efficient cryptographic enforcement of interval-based access control policies. ACM Transactions on Information and System Security 14 (1), Article no. 14.
Forcht, K.A., 1994. Computer Security Management. Boyd & Fraser, Danvers, MA, USA.
Goel, S., Shawky, H.A., 2009. Estimating the market impact of security breach announcements on firm values. Information and Management 46 (7), 404–410.
Gordon, L.A., Loeb, M.P., 2002. The economics of information security investment. ACM Transactions on Information and System Security 5 (4), 438–457.
Gordon, L.A., Loeb, M.P., Sohail, T., 2010. Market value of voluntary disclosures concerning information security. MIS Quarterly 34 (3), 567–594.
Houmb, S.H., Franqueira, V.N.L., Engum, E.A., 2010. Quantifying security risk level from CVSS estimates of frequency and impact. Journal of Systems and Software 83 (9), 1622–1634.
Hovav, A., D'Arcy, J., 2003. The impact of denial-of-service attack announcements on the market value of firms. Risk Management and Insurance Review 6 (2), 97–121.
Johnson, C., 2007. Implementation of Commonly Accepted Security Configurations for Windows Operating Systems. OMB (Office of Management and Budget), Memo M-07-11.
Lee, K.M., Leekwang, H., 1995. Identification of λ-fuzzy measure by genetic algorithms. Fuzzy Sets and Systems 75 (3), 301–309.
Liu, P., Zang, W., Yu, M., 2005. Incentive-based modeling and inference of attacker intent, objectives, and strategies. ACM Transactions on Information and System Security 8 (1), 78–118.
Liu, Q., Zhang, Y., 2011. VRSS: a new system for rating and scoring vulnerabilities. Computer Communications 34 (3), 264–273.
Liu, Q., Zhang, Y., Kong, Y., Wu, Q., 2012. Improving VRSS-based vulnerability prioritization using analytic hierarchy process. Journal of Systems and Software 85 (8), 1699–1708.
Martin, J., 1973. Security, Accuracy, and Privacy in Computer Systems. Prentice Hall, Upper Saddle River, NJ, USA.
Martin, R.A., 2008. Making security measurable and manageable. In: Proceedings of the 2008 IEEE Military Communications Conference.
Mell, P., Scarfone, K., Romanosky, S., 2006. Common vulnerability scoring system. IEEE Security and Privacy 4 (6), 85–89.
Mell, P., Scarfone, K., Romanosky, S., 2007. A complete guide to the common vulnerability scoring system (CVSS), Version 2.0. Forum of Incident Response and Security Teams (FIRST).
Microsoft, 2010. Statement of Health for Network Access Protection (NAP) Protocol Specification. Microsoft Corporation.
Milian, M., 2011. Sony: hacker stole PlayStation users' personal info. Cable News Network (CNN), April 26, 2011.
MITRE, 2010a. Common Vulnerabilities and Exposures (CVE).
MITRE, 2010b. Common Weakness Enumeration (CWE).
Murofushi, T., Sugeno, M., 1989. An interpretation of fuzzy measures and the Choquet integral as an integral with respect to a fuzzy measure. Fuzzy Sets and Systems 29 (2), 201–227.
NIST, 2009. Recommended security controls for federal information systems and organizations. NIST Special Publication, 800-53 Revision 3.
NIST, 2010a. National Vulnerability Database (NVD), Version 2.2.
NIST, 2010b. National Checklist Program Repository.
NIST, 2010c. Federal Desktop Core Configuration (FDCC).
OWASP, 2010. OWASP top 10-2010. The ten most critical web application security risk.
Parker, D.B., 1981. Computer Security Management. Prentice Hall, Reston, VA, USA.
Quinn, S.D., Souppaya, M., Cook, M., Scarfone, K., 2011. National checklist program for IT products – guidelines for checklist users and developers. NIST Special Publication, 800-70 Revision 2.
Ransbotham, S., Mitra, S., Ramsey, J., 2012. Are markets for vulnerabilities effective? MIS Quarterly 36 (1), 43–64.
Rogers, R.W., 1975. A protection motivation theory of fear appeals and attitude change. Journal of Psychology 91, 93–114.
Rogers, R.W., 1983. Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. Social Psychophysiology, 153–176.
Ryu, Y.U., Rhee, H., 2008. Evaluation of intrusion detection systems under a resource constraint. ACM Transactions on Information and System Security 11 (4), Article no. 20.
SANS Institute, 2009. Top cyber security risks – vulnerability exploitation trends.
Scarfone, K., Mell, P., 2009. An analysis of CVSS version 2 vulnerability scoring. In: Proceedings of the Third International Symposium on Empirical Software Engineering and Measurement, pp. 516–525.
Stiemerling, M., Quittek, J., Eggert, L., 2008. NAT and firewall traversal issues of host identity protocol (HIP) communication. RFC (Request for Comments) 5207. IETF (The Internet Engineering Task Force).
Straub, D.W., 1990. Effective IS security: an empirical study. Information Systems Research 1 (3), 255–276.
Straub, D.W., Welke, R.J., 1998. Coping with systems risk: security planning models for management decision making. MIS Quarterly 22 (4), 441–469.
Sugeno, M., Terano, T., 1977. A model of learning based on fuzzy information. Kybernetes 6 (3), 157–166.
Trusted Computing Group, 2009. TCG trusted network connect TNC architecture for interoperability. Specification Version 1.4. Revision 4.
Telang, R., Wattal, S., 2007. An empirical analysis of software vulnerability announcements on firm stock price. IEEE Transactions on Software Engineering 33 (8), 544–557.
The White House, 1998. The clinton administration's policy on critical infrastructure protection. Presidential Decision Directive 63, White Paper.
The White House, 2000a. National plan for information systems protection. Version 1.0.
The White House, 2000b. Cyber Security Research and Development Act.
The White House, 2002. E-government act of 2002, title 3 – information security.
Waltermire, D., Quinn, S.D., Scarfone, K., Halbardier, A., 2011. The technical specification for the security content automation protocol (SCAP): SCAP Version 1.2. NIST Special Publication 800-126 Revision 2.
Wang, X., Golle, P., Jakobsson, M., Tsow, A., 2010a. Deterring voluntary trace disclosure in re-encryption mix-networks. ACM Transactions on Information and System Security 13 (2), Article no. 18.
Wang, J., Xiao, N., Rao, H.R., 2010b. Drivers of information security search behavior: an investigation of network attacks and vulnerability disclosures. ACM Transactions on Management Information Systems 1 (1), Article no. 3.
Weck, M., Klocke, F., Schell, H., Rüenauver, E., 1997. Evaluating alternative production cycles using the extended fuzzy AHP method. European Journal of Operational Research 100 (2), 351–366.
Yayla, A.A., Hu, Q., 2011. The impact of information security events on the stock value of firms: the effect of contingency factors. Journal of Information Technology 26, 60–77.

**Chien-Cheng Huang** received his MS degree in information management from the National Chiao Tung University, Taiwan, Republic of China, in 2008. He is currently a Ph.D. student in information management at the National Taiwan University. His research interests include information systems, database systems, data mining, and information security.

**Feng-Yu Lin** received his Ph.D. degree from the National Chiao Tung University, Taiwan, Republic of China, in 2004. Currently, he is working towards the second Ph.D. degree in the Department of Information Management, National Taiwan University. His research interests include communication/network forensics, data mining, and information security.

**Frank Yeong-Sung Lin** received his BS degree in electrical engineering from the National Taiwan University in 1983, and his Ph.D. degree in electrical engineering

from the University of Southern California in 1991. After graduating from the USC, he joined Telcordia Technologies (formerly Bell Communications Research, abbreviated as Bellcore) in New Jersey, U.S.A. Since 1996, he has been with the faculty of the Information Management Department, National Taiwan University. His research interests include network optimization, network planning, network survivability, performance evaluation, high-speed networks, distributed algorithms, content-based information retrieval/filtering, biometrics and network/information security.

**Yeali S. Sun** received her BS from the Computer Science and Information Engineering department of National Taiwan University in 1982, and MS and Ph.D. degrees in Computer Science from the University of California, Los Angeles in 1984 and 1988, respectively. From 1988 to 1993, she was with Bell Communications Research Inc. (Bellcore; now Telcordia). In August 1993, she jointed National Taiwan University and is currently a professor of the Department of Information Management. Her research interests are in the area of wireless networks, Quality of Service and pricing, Internet security and forensics, scalable resource management and business model in cloud services and performance modeling and evaluation.