Hindawi Publishing Corporation
The Scientific World Journal
Volume 2014, Article ID 506714, 9 pages
http://dx.doi.org/10.1155/2014/506714

*Research Article*

# Security Threat Assessment of an Internet Security System Using Attack Tree and Vague Sets

**Kuei-Hu Chang**

*Department of Management Sciences, R.O.C. Military Academy, Kaohsiung 830, Taiwan*

Correspondence should be addressed to Kuei-Hu Chang; evenken2002@gmail.com

Received 19 August 2014; Accepted 18 September 2014; Published 21 October 2014

Academic Editor: Ming-Hung Shu



Security threat assessment of the Internet security system has become a greater concern in recent years because of the progress and diversification of information technology. Traditionally, the failure probabilities of bottom events of an Internet security system are treated as exact values when the failure probability of the entire system is estimated. However, security threat assessment when the malfunction data of the system's elementary event are incomplete—the traditional approach for calculating reliability—is no longer applicable. Moreover, it does not consider the failure probability of the bottom events suffered in the attack, which may bias conclusions. In order to effectively solve the problem above, this paper proposes a novel technique, integrating attack tree and vague sets for security threat assessment. For verification of the proposed approach, a numerical example of an Internet security system security threat assessment is adopted in this paper. The result of the proposed method is compared with the listing approaches of security threat assessment methods.

## 1. Introduction

Due to information age's advance, security threat assessment of an Internet security system has become much more important and complicated. To ensure information security, many organizations use firewalls to provide a level of security by controlling access to information systems. A security manager has to make a decision and choose to implement a subset of these policies in order to maximize resource utilization. There has now been extensive research on security threat assessments; for some recent examples, see Tidwell et al. [1], Dhillon and Torkzadeh [2], Satoh et al. [3], Symantec Corporation [4], Opdahl and Sindre [5], Wu and Ye [6], Lee and Chang [7], and Blyth [8]. Helmer et al. [9] proposed the Multi-Agents Intrusion Detection System (MAIDS), which uses mobile agents in a distributed system to obtain audit data, correlate events, and discover intrusions. They used software fault trees to define intrusions and develop the requirement model for intrusion detection systems. Azaiez and Bier [10] used optimal attack strategies by analogy with existing results for the least expected cost failure state diagnosis of reliability systems. In addition, the growing popularity of e-government services on the Internet has also brought with it security threats. Similarly, J. J. Zhao and S. Y. Zhao [11] assessed the security of US state e-government sites to identify opportunities for and threats to the sites and their users. They used a combination of three methods—web content analysis, information security auditing, and computer network security mapping—for data collection and analysis.

The increasing frequency and complexity of Internet attacks have raised the level of sophistication required by systems administrators to effectively cope with script kiddies and more sophisticated hackers, for example, top causes of data breaches of Symantec Corporation in 2012, as shown in Figure 1. Hackers continue to be responsible for the largest number of data breaches, making up 40 percent of all breaches [4]. A secure computer system provides guarantees regarding the confidentiality, integrity, and availability of its data. However, systems generally contain design and implementation flaws that result in security vulnerabilities [9]. In addition, due to uncertainties and imprecision of data, it may be difficult or even impossible to precisely determine the failure probabilities of components. On the other hand, the incomplete failure data of the bottom events suffered in the attack also increase the difficulty of security threat

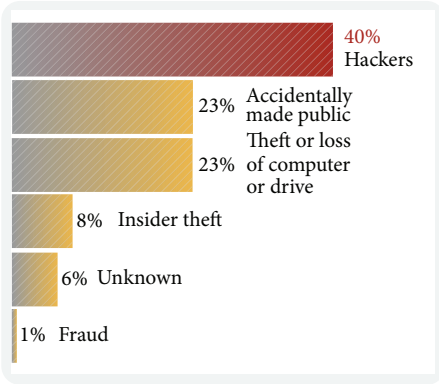



Figure 1: Top causes of data breaches [4].

assessment and calculation. It cannot be fully solved by traditional probability reliability. Therefore, this study used a vague set approach to overcome this problem. The concept of vague set was proposed by Gau and Buehrer [12]. A great deal of literature [13–19] has been carried out in vague set methods.

An attack tree supports design and required decisions. Attack trees are thus a formalized and structured method for analyzing threats. The possible decomposition of an attack tree to divide the goal into subgoals is an interesting alternative to explore. It is also known as a fault tree [20]. In 1999, Schneier was the first to propose attack trees to analyze the security of systems and subsystems [20]. Attacks are represented in a tree structure, with the attacker goal as the root node and the different ways of achieving that goal as leaf nodes. The attack tree includes the "AND" node and the "OR" node. To reach an AND node, all subgoals must be achieved. To reach an OR node, at least one of the subgoals must be achieved. The attack tree is a formal and methodical way of describing the security of the system based on varying attacks.

In reliability assessment, when the malfunction data of the system's elementary event are incomplete, the conventional approach of calculating reliability is no longer applicable [21]. Huang et al. [22] proposed the posbist fault tree analysis method to find a system's reliability by redefining the "AND" and "OR" operators based on the minimal cut of a posbist fault tree. However, their method only selects the maximal failure probability of the bottom event, which can result in biased conclusions. To solve this problem, this paper proposes a novel security threat assessment method that collects experts' knowledge and experience on the problem domain to build the possibility of the failure of leaf nodes through integrating attack tree and vague sets to assess security threats of an Internet security system. A security threat assessment of an Internet security system is presented as a case study to further illustrate the proposed method. It also compares the proposed approaches with several other listed methods in this paper.

The rest of this paper is organized as follows. Section 2 introduces the basic definition and operations of the attack tree. Section 3 introduces the basic definition and operations of the vague sets. Section 4 presents the proposed approach,

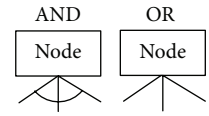



Figure 2: "AND" node and "OR" node.

which integrates the attack tree and the vague sets for safety assessment. A numerical example of an Internet security system is adopted, and some comparisons with the listed approaches are discussed in Section 5. The final section makes conclusions.

## 2. Attack Tree

Schneier [20] proposed attack trees to analyze the security of systems and subsystems. It is a catalog of all possible attacks against a system. The purpose of the attack tree is to define and analyze possible attacks on a system in a structured way. The attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks. An attack tree is initiated by a root node describing a type of attack, and each path is terminated by a leaf node (no children). Nodes can be decomposed by "AND" and "OR" relations.

If we let $x_j$ be a random variable such that $x_j = 1$ corresponds to the accomplishments of subtask $j$ and $x_j = 0$ corresponds to the failure of task $j$, then $P(x_1, x_2, \ldots, x_n)$ is the joint probability distribution. In an "AND" node (see Figure 2), it must have $P(x_1 = 1, x_2 = 1, \ldots, x_n = 1)$. The accomplishment for the parent goal requires the success of all children—that is, $P_{\text{and}} = \prod_{j=1}^{n} p_j$—which is the product of the probability of accomplishments of all children. In an "OR" node (see Figure 2), this is essentially the negation of the probability that all subtasks fail: $1 - P(x_1 = 0, x_2 = 0, \ldots, x_n = 0)$. The accomplishment for the parent goal requires the success of any one of the children—that is, $P_{\text{or}} = 1 - \prod_{j=1}^{n}(1 - p_j)$—which is the product of the probability of an accomplishment of any one of the children. It assumes that the attacker can try all available subtasks until he finds one that succeeds. This is an unrealistic assumption in attack modeling, because if an attacker needs to try more than one subtask, he has manifested at least one failure. This is a situation that may be untenable in an attack. Therefore, Yager [23] assumed that in an "OR" node, where the attacker needs only to succeed at one subtask, he cannot try all possibilities but must try one. Thus, the probability of success at an "OR" node without any failure is $P_{\text{OR}} = \text{Max}_j[P_j]$. It is also clear that $P_{\text{OR}} = \text{Max}_j[P_j] \geq P_{\text{AND}} = \prod_{j=1}^{n} p_j$.

## 3. Vague Sets and Their Operations

This section introduces the definitions and properties of vague sets and four arithmetic operations of the triangle vague set.

*3.1. Definitions and Properties of Vague Sets [24].* Zadeh [25] proposed fuzzy sets to describe fuzzy phenomena under

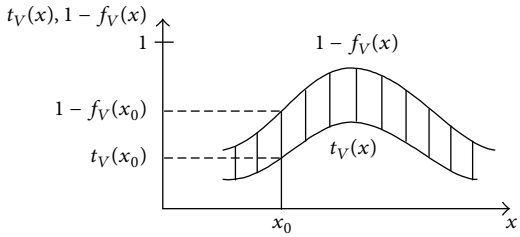



Figure 3: Vague set explanation of a real number $R$.

a specific attribute. A fuzzy set $F$ is a class of objects, along with a grade of membership function. This membership function, $\mu_F(x)$, $x \in X$, assigns a grade membership to each object that ranges between 0 and 1. This single value combines the evidence for $x \in X$ and the evidence against $x \in X$, without indicating how much there is of each value. The notion of an intuitionistic fuzzy set was introduced for the first time by Atanassov [26] in 1983 as a generalization of an ordinary Zadeh fuzzy set. Let a set $X$ be fixed. An intuitionistic fuzzy set $A$ in $X$ is an object that has the form $A = \{\langle x, \mu_A(x), \nu_A(x) \mid x \in X\rangle\}$, where the functions $\mu_A(x) : X \to [0, 1]$ and $\nu_A(x) : X \to [0, 1]$ define the degree of membership and the degree of nonmembership of the element $x \in X$ to the set $A$; moreover, $0 \le \mu_A(x)+\nu_A(x) \le 1$ must hold.

The concept of the vague set was proposed by Gau and Buehrer [12]. In a vague set $V$, for assigning a membership grade to every phenomenon, this membership grade is an interval of $[0, 1]$. This interval presents accepted evidence of $x \in X$ and declined evidence at the same time. In membership grade $\mu_V(x)$, a vague set $V$ uses a truth-membership function $t_V$ and a false-membership function $f_v$ to represent the lower bound ($t_V$) and upper bound ($1 - f_v$). The interval $[t_V(x), 1 - f_V(x)]$ can extend the fuzzy set of the membership function. In 1996, Bustince and Burillo [27] proposed that vague sets are intuitionistic fuzzy sets. The membership grade $\mu_V(x)$ is not clear, but it is located in the subinterval $[t_V(x), 1 - f_V(x)]$ (i.e., $t_V(x) \le \mu_V(x) \le 1 - f_V(x)$) and $0 \le t_V(x) + f_V(x) \le 1$. For example, if $[t_V(x_i), 1 - f_V(x_i)] = [0.6, 0.9]$, then $t_V(x_i) = 0.6$, $1 - f_V(x_i) = 0.9$, $f_V(x_i) = 0.1$. The result can explain that $x_i$ belongs to vague set $V$ and accepts that the evidence is 0.6 and the declined evidence is 0.1. If $x_i$ is the vote result from 10 people, it implies that six people voted in favor, one person voted against, and three persons abstained. Figure 3 shows a vague set explanation of a real number $R$.

The uncertainty of $x$ can be described as the differential value of $(1 - f_V(x)) - t_V(x)$. If the differential value is small, it means that the value of $x$ is more certain. If the differential value is great, it means that the computation is more uncertain about $x$. When $1 - f_V(x) = t_V(x)$, the vague set $V$ regresses to a fuzzy set. Obviously, when $1 - f_V(x) = t_V(x) = 1$ or $1 - f_V(x) = t_V(x) = 0$, the vague set $V$ regresses to a crisp set. From the above result, crisp sets and fuzzy sets can be viewed as special cases of vague sets. Therefore, vague sets can be used to describe vague objects in our daily life in more detail.

*3.2. Arithmetic Operations of Triangle Vague Sets.* Let $A$ and $B$ be two vague sets, as shown in Figure 4. If $t_A \ne t_B$ and $f_A \ne f_B$, then the arithmetic operations are defined as

$$
\begin{aligned}
A &= \left\langle \left[\left(a_1', b_1, c_1'\right); \mu_1\right], \left[(a_1, b_1, c_1); \mu_2\right]\right\rangle,\\
B &= \left\langle \left[\left(a_2', b_2, c_2'\right); \mu_3\right], \left[(a_2, b_2, c_2); \mu_4\right]\right\rangle,\\
A\,(+)\,B &= \left\langle \left[\left(a_1', b_1, c_1'\right); \mu_1\right], \left[(a_1, b_1, c_1); \mu_2\right]\right\rangle\\
&\quad (+) \left\langle \left[\left(a_2', b_2, c_2'\right); \mu_3\right], \left[(a_2, b_2, c_2); \mu_4\right]\right\rangle\\
&= \left\langle \left[\left(a_1' + a_2', b_1 + b_2, c_1' + c_2'\right); \min\left(\mu_1, \mu_3\right)\right],\right.\\
&\qquad \left.\left[(a_1 + a_2, b_1 + b_2, c_1 + c_2); \min\left(\mu_2, \mu_4\right)\right]\right\rangle,\\
A\,(-)\,B &= \left\langle \left[\left(a_1', b_1, c_1'\right); \mu_1\right], \left[(a_1, b_1, c_1); \mu_2\right]\right\rangle\\
&\quad (-) \left\langle \left[\left(a_2', b_2, c_2'\right); \mu_3\right], \left[(a_2, b_2, c_2); \mu_4\right]\right\rangle\\
&= \left\langle \left[\left(a_1' - c_2', b_1 - b_2, c_1' - a_2'\right); \min\left(\mu_1, \mu_3\right)\right],\right.\\
&\qquad \left.\left[(a_1 - c_2, b_1 - b_2, c_1 - a_2); \min\left(\mu_2, \mu_4\right)\right]\right\rangle,\\
A\,(\times)\,B &= \left\langle \left[\left(a_1', b_1, c_1'\right); \mu_1\right], \left[(a_1, b_1, c_1); \mu_2\right]\right\rangle\\
&\quad (\times) \left\langle \left[\left(a_2', b_2, c_2'\right); \mu_3\right], \left[(a_2, b_2, c_2); \mu_4\right]\right\rangle\\
&= \left\langle \left[\left(a_1'a_2', b_1b_2, c_1'c_2'\right); \min\left(\mu_1, \mu_3\right)\right],\right.\\
&\qquad \left.\left[(a_1a_2, b_1b_2, c_1c_2); \min\left(\mu_2, \mu_4\right)\right]\right\rangle,\\
A\,(/)\,B &= \left\langle \left[\left(a_1', b_1, c_1'\right); \mu_1\right], \left[(a_1, b_1, c_1); \mu_2\right]\right\rangle\\
&\quad (/) \left\langle \left[\left(a_2', b_2, c_2'\right); \mu_3\right], \left[(a_2, b_2, c_2); \mu_4\right]\right\rangle\\
&= \left\langle \left[\left(\frac{a_1'}{c_2'}, \frac{b_1}{b_2}, \frac{c_1'}{a_2'}\right) \min\left(\mu_1, \mu_3\right)\right],\right.\\
&\qquad \left.\left[\left(\frac{a_1}{c_2}, \frac{b_1}{b_2}, \frac{c_1}{a_2}\right); \min\left(\mu_2, \mu_4\right)\right]\right\rangle.
\end{aligned}
\tag{1}
$$

When $a_1 = a_1'$, $c_1 = c_1'$ and $a_2 = a_2'$, $c_2 = c_2'$, the vague sets of its four arithmetic operations will be easier.

## 4. Proposed Combination of an Attack Tree and Vague Sets Approach

*4.1. The Reason for Using Attack Tree and Vague Sets.* Security threat assessment of the Internet security system has become a greater concern in recent years, due to progress and diversification of information technology. For an Internet security system, due to uncertainties and imprecision of data, it may be difficult or even impossible to precisely determine the failure probabilities of components. Moreover, we must consider the failure probability of the bottom events suffered in the attack when security threat assessment is executed.

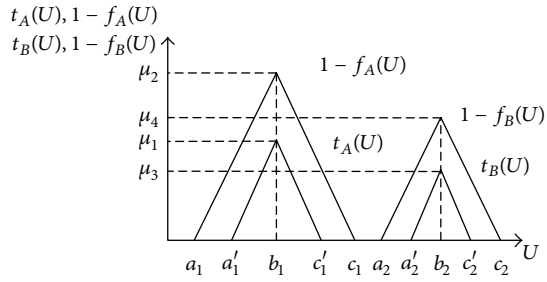



Figure 4: Triangle vague sets $A$ and $B$.

Therefore, it cannot be fully solved by traditional probability reliability. An attack tree provides a way of modeling goals of an attack and alternative ways to achieve that goal. This helps us to study the system from the attackers' points of view, which may lead us to determine possible ways that the system can be compromised. Therefore, using an attack tree and vague sets approach to solve security threat assessment problems is more suitable. The major advantage of the vague set over the fuzzy set is that the vague set separates the positive (the degree of membership) and negative (the degree of nonmembership) evidence of membership of an element in the set. Fuzzy sets are vague sets, but the converse is not necessarily true. For this reason, it is more suitable to use the vague set, not the fuzzy set, in attack tree diagrams.

*4.2. The Procedure of the Proposed Approach.* According to the definitions in Section 3, this paper proposes six steps in order to implement vague attack tree analysis in security threat assessment of an Internet security system. The six steps are described as follows.

*Step 1* (construct the attack tree diagram). Construct the attack tree diagram by the AND node and OR node, tracing back the whole process from the main goal to the physical tasks.

*Step 2* (establish a system of reliability block diagram). A reliability block diagram can explain the units' relationships in parallel and in series.

*Step 3* (define the vague membership degree of leaf nodes). A unit fault can cause the breakdown of the whole system. Define the vague membership degree of leaf nodes according to an expert's knowledge and experience. Possible failure intervals of bottom events are obtained by aggregating group decision-making opinions of the experts' opinions.

*Step 4* (calculate the possible malfunction probability of the main goal). Use the attack tree diagram and vague set arithmetic operations to calculate the possible malfunction probability of the main goal.

*Step 5* (calculate the reliability of the main goal). The reliability of the main goal is equal to one minus the possible malfunction probability of the main goal.

*Step 6* (analyze the results and provide suggestions). From Step 5, the results can be further analyzed to provide the decision maker with feasible solutions.

## 5. An Illustrative Example

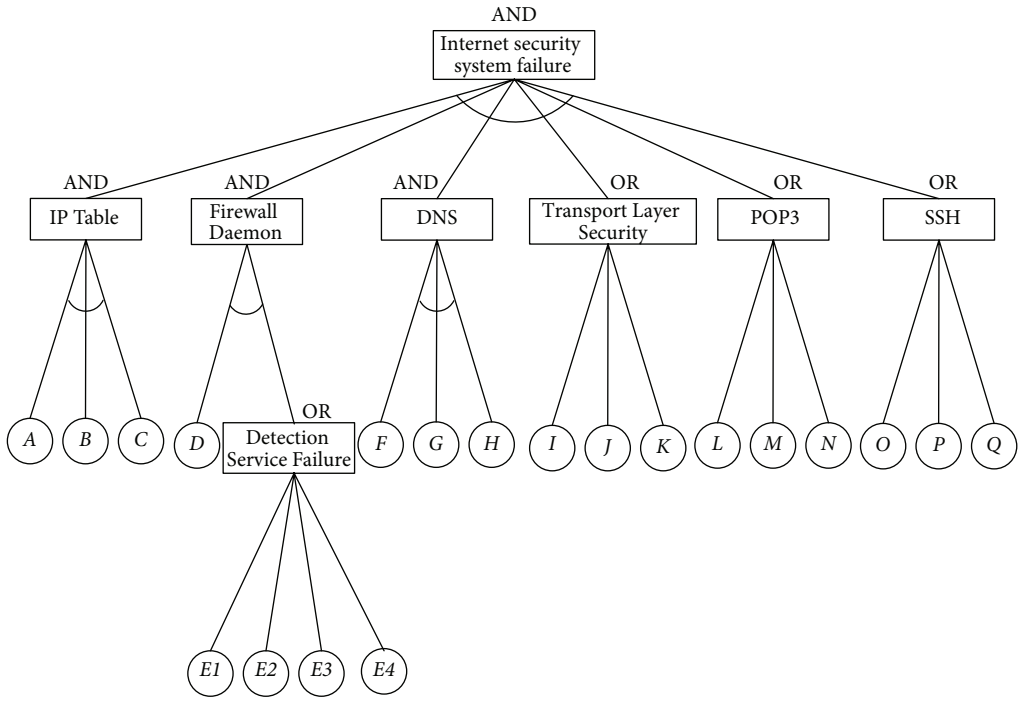
In this section, an illustrative example of Internet security system failure during attack is presented in order to demonstrate the procedure that is proposed in this paper. This research also compares the experimental results with the traditional probability reliability and Huang et al.'s [22] methods. First of all, an attack tree is constructed that includes the main goal (the failure of the Internet security system during attack), the sub-goals (IP table, firewall daemon, domain name system (DNS), transport layer security, post office protocol 3 (POP3), secure shell (SSH)), the subtasks (Detection Service Failure), and the physical tasks (IP Table configuration errors, address translation failure, authentication failure, etc.). An attack tree integrates the main goal, the subgoals, the subtasks, and the physical tasks with "AND" and "OR" nodes (Figure 5). The descriptions of the physical tasks are listed in Table 1. Because of the incomplete failure data of system physical tasks, this paper proposes speculation by experts' opinions according to the incomplete information condition. The reliability block diagram of the Internet security system failure during attack is shown in Figure 6.

*5.1. Traditional Probability Reliability.* This research calculated the failure possibility of an "Internet security system" during attack, based on the data of Table 1 (column $b_i$), by the traditional probability reliability method as follows:

$$\begin{aligned} q_T &= \{1 - (1 - q_A)(1 - q_B)(1 - q_C)(1 - q_D) \\ &\quad \times (1 - q_{E1}q_{E2}q_{E3}q_{E4}) \times (1 - q_F)(1 - q_G)(1 - q_H) \\ &\quad \times (1 - q_I q_J q_K) \times (1 - q_L q_M q_N) \times (1 - q_O q_P q_Q)\} \\ &= \{1 - (1 - 0.35)(1 - 0.15)(1 - 0.10)(1 - 0.05) \\ &\quad \times (1 - 0.13 \times 0.11 \times 0.05 \times 0.04) \\ &\quad \times (1 - 0.10)(1 - 0.05)(1 - 0.40) \\ &\quad \times (1 - 0.14 \times 0.20 \times 0.30) \times (1 - 0.18 \times 0.25 \times 0.40) \\ &\quad \times (1 - 0.09 \times 0.07 \times 0.04)\} \\ &= 1 - 0.2359 = 0.7641. \end{aligned} \tag{2}$$

After the calculation above, it is shown that the failure probability of the "Internet security system" during attack is 0.2359 and the reliability of the "Internet security system" is 0.7641.

*5.2. Huang et al. Method [22].* When the failure probability of a system is extremely small or when essential statistical data are scarce, the posbist fault-tree analysis proposed by Huang et al. [22] could be applied to predict and diagnose a system's failures and evaluate its reliability and safety. Calculations of




*A*: IP Table configuration errors
*B*: address translation failure
*C*: authentication failure
*D*: Firewall Daemon configuration errors
*E1*: scan failure
*E2*: cleanse failure
*E3*: audit failure
*E4*: validation failure
*F*: DNS configuration errors
*G*: monitor service failure
*H*: malicious access detected
*I*: Transport Layer Security configuration errors
*J*: peer entity authentication
*K*: security parameter negotiation
*L*: POP3 configuration errors
*M*: entity authentication
*N*: entry security parameter
*O*: security parameter authentication
*P*: key generation
*Q*: data confidentiality

Figure 5: Attack tree of the Internet security system.

the failure possibility of the "Internet security system," based on the crisp failure possibilities, are listed in Table 1 (column $b_i$), as per the following:

$$\begin{aligned}
P_{\text{oss}}(\text{SSH}) &= \min\left(P_{\text{oss}}(O), P_{\text{oss}}(P), P_{\text{oss}}(Q)\right) \\
&= \min(0.09, 0.07, 0.04) = 0.04, \\
P_{\text{oss}}(\text{POP3}) &= \min\left(P_{\text{oss}}(L), P_{\text{oss}}(M), P_{\text{oss}}(N)\right) \\
&= \min(0.18, 0.25, 0.40) = 0.18, \\
P_{\text{oss}}&(\text{Transport Layer Security}) \\
&= \min\left(P_{\text{oss}}(I), P_{\text{oss}}(J), P_{\text{oss}}(K)\right) \\
&= \min(0.14, 0.20, 0.30) = 0.14, \\
P_{\text{oss}}(\text{DNS}) &= \max\left(P_{\text{oss}}(F), P_{\text{oss}}(G), P_{\text{oss}}(H)\right) \\
&= \max(0.10, 0.05, 0.40) = 0.40, \\
P_{\text{oss}}&(\text{Detection Service Failure}) \\
&= \min\left(P_{\text{oss}}(E1), P_{\text{oss}}(E2), P_{\text{oss}}(E3), P_{\text{oss}}(E4)\right) \\
&= \min(0.13, 0.11, 0.05, 0.04) = 0.04, \\
P_{\text{oss}}&(\text{Firewall Daemon}) \\
&= \max\left(P_{\text{oss}}(D), P_{\text{oss}}(\text{Detection Service Failure})\right) \\
&= \max(0.05, 0.04) = 0.05, \\
P_{\text{oss}}(\text{IP Table}) &= \max\left(P_{\text{oss}}(A), P_{\text{oss}}(B), P_{\text{oss}}(C)\right) \\
&= \max(0.35, 0.15, 0.10) = 0.35.
\end{aligned} \tag{3}$$

Then, the top event possibilities of "Internet security system failure" during attacking can be calculated as

$$\begin{aligned}
P_{\text{oss}}&(\text{Internet Security System Failure}) \\
&= \max\left(P_{\text{oss}}(\text{SSH}), P_{\text{oss}}(\text{POP3}),\right. \\
&\qquad P_{\text{oss}}(\text{Transport Layer Security}), P_{\text{oss}}(\text{DNS}), \\
&\qquad \left. P_{\text{oss}}(\text{Firewall Daemon}), P_{\text{oss}}(\text{IP Table})\right) \\
&= \max(0.04, 0.18, 0.14, 0.40, 0.05, 0.35) = 0.40.
\end{aligned} \tag{4}$$

Table 1: The possible range of leaf node failures.

| Failure possibility | $a_i$ | $a_i'$ | $b_i$ | $c_i'$ | $c_i$ | $\mu_A(U)$ | $1-\nu_A(U)$ |
|---|---|---|---|---|---|---|---|
| *A* (IP Table configuration errors) | 0.30 | 0.33 | 0.35 | 0.37 | 0.40 | 0.8 | 0.9 |
| *B* (address translation failure) | 0.10 | 0.12 | 0.15 | 0.18 | 0.20 | 0.9 | 1.0 |
| *C* (authentication failure) | 0.80 | 0.90 | 0.10 | 0.11 | 0.12 | 0.9 | 0.9 |
| *D* (Firewall Daemon configuration errors) | 0.04 | 0.04 | 0.05 | 0.06 | 0.06 | 0.8 | 0.9 |
| *E*1 (scan failure) | 0.11 | 0.12 | 0.13 | 0.14 | 0.15 | 0.9 | 1.0 |
| *E*2 (cleanse failure) | 0.10 | 0.10 | 0.11 | 0.12 | 0.12 | 0.9 | 1.0 |
| *E*3 (audit failure) | 0.03 | 0.04 | 0.05 | 0.06 | 0.07 | 0.9 | 1.0 |
| *E*4 (validation failure) | 0.03 | 0.03 | 0.04 | 0.05 | 0.05 | 0.9 | 1.0 |
| *F* (DNS configuration errors) | 0.08 | 0.09 | 0.10 | 0.11 | 0.12 | 0.8 | 0.9 |
| *G* (monitor service failure) | 0.04 | 0.04 | 0.05 | 0.06 | 0.06 | 0.9 | 1.0 |
| *H* (malicious access detected) | 0.35 | 0.37 | 0.40 | 0.43 | 0.45 | 0.8 | 1.0 |
| *I* (Transport Layer Security configuration errors) | 0.12 | 0.13 | 0.14 | 0.15 | 0.16 | 0.8 | 0.9 |
| *J* (peer entity authentication) | 0.15 | 0.16 | 0.20 | 0.24 | 0.25 | 0.8 | 1.0 |
| *K* (security parameter negotiation) | 0.27 | 0.28 | 0.30 | 0.32 | 0.33 | 0.8 | 0.9 |
| *L* (POP3 configuration errors) | 0.16 | 0.17 | 0.18 | 0.19 | 0.20 | 0.8 | 0.9 |
| *M* (entity authentication) | 0.22 | 0.24 | 0.25 | 0.26 | 0.28 | 0.8 | 1.0 |
| *N* (entry security parameter) | 0.38 | 0.39 | 0.40 | 0.41 | 0.42 | 0.8 | 0.9 |
| *O* (security parameter authentication) | 0.07 | 0.08 | 0.09 | 0.10 | 0.11 | 0.8 | 1.0 |
| *P* (key generation) | 0.05 | 0.06 | 0.07 | 0.08 | 0.09 | 0.8 | 0.9 |
| *Q* (data confidentiality) | 0.03 | 0.03 | 0.04 | 0.05 | 0.05 | 0.9 | 0.9 |

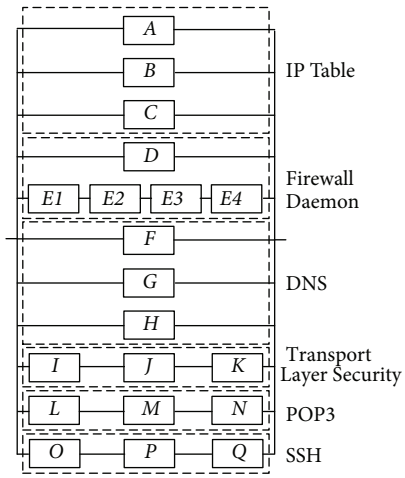



Figure 6: Parallel and series relationship of an attack tree diagram of the Internet security system.

After the calculation above, it is shown that the failure probability of the "Internet security system" during attack is 0.40 and the reliability of the "Internet security system" is 0.60.

*5.3. Proposed Method.* According to (1), the failure range of subgoals (SSH, POP3, Transport Layer Security, DNS, Detection Service Failure, Firewall Daemon, and IP Table) can be calculated as

$$
\begin{aligned}
&P_{\text{and}}\,(\text{SSH})\\
&\quad = P_O \times P_P \times P_Q\\
&\quad = \langle [(0.08, 0.09, 0.10) ; 0.8] , [(0.07, 0.09, 0.11) ; 1.0] \rangle\\
&\qquad (\times) \langle [(0.06, 0.07, 0.08) ; 0.8] , [(0.05, 0.07, 0.09) ; 0.9] \rangle\\
&\qquad (\times) \langle [(0.03, 0.04, 0.05) ; 0.9] , [(0.03, 0.04, 0.05) ; 0.9] \rangle\\
&\quad = \langle [(0.0048, 0.0063, 0.0080) ; 0.8] ,\\
&\qquad\quad [(0.0035, 0.0063, 0.0099) ; 0.9] \rangle\\
&\qquad (\times) \langle [(0.03, 0.04, 0.05) ; 0.9] , [(0.03, 0.04, 0.05) ; 0.9] \rangle\\
&\quad = \langle [(0.000144, 0.000252, 0.000400) ; 0.8] ,\\
&\qquad\quad [(0.000105, 0.000252, 0.000495) ; 0.9] \rangle ,\\
&P_{\text{and}}\,(\text{POP3})\\
&\quad = P_L \times P_M \times P_N\\
&\quad = \langle [(0.17, 0.18, 0.19) ; 0.8] , [(0.16, 0.18, 0.20) ; 0.9] \rangle\\
&\qquad (\times) \langle [(0.24, 0.25, 0.26) ; 0.8] , [(0.22, 0.25, 0.28) ; 1.0] \rangle\\
&\qquad (\times) \langle [(0.39, 0.40, 0.41) ; 0.8] , [(0.38, 0.40, 0.42) ; 0.9] \rangle\\
&\quad = \langle [(0.0408, 0.0450, 0.0494) ; 0.8] ,\\
&\qquad\quad [(0.0352, 0.0450, 0.0560) ; 0.9] \rangle\\
&\qquad (\times) \langle [(0.39, 0.40, 0.41) ; 0.8] , [(0.38, 0.40, 0.42) ; 0.9] \rangle\\
&\quad = \langle [(0.015912, 0.018000, 0.020254) ; 0.8] ,\\
&\qquad\quad [(0.013376, 0.018000, 0.023520) ; 0.9] \rangle ,
\end{aligned}
$$

$$
\begin{aligned}
&P_{\text{and}}\left(\text{Transport Layer Security}\right)\\
&\quad = P_I \times P_J \times P_K\\
&\quad = \langle[(0.13, 0.14, 0.15) ; 0.8] , [(0.12, 0.14, 0.16) ; 0.9]\rangle\\
&\qquad (\times) \langle[(0.16, 0.20, 0.24) ; 0.8] , [(0.15, 0.20, 0.25) ; 1.0]\rangle\\
&\qquad (\times) \langle[(0.28, 0.30, 0.32) ; 0.8] , [(0.27, 0.30, 0.33) ; 0.9]\rangle\\
&\quad = \langle[(0.0208, 0.0280, 0.0360) ; 0.8] ,\\
&\qquad\quad [(0.0180, 0.0280, 0.0400) ; 0.9]\rangle\\
&\qquad (\times) \langle[(0.28, 0.30, 0.32) ; 0.8] , [(0.27, 0.30, 0.33) ; 0.9]\rangle\\
&\quad = \langle[(0.005824, 0.008400, 0.011520) ; 0.8] ,\\
&\qquad\quad [(0.004860, 0.008400, 0.013200) ; 0.9]\rangle ,\\
&P_{\text{or}}\left(\text{DNS}\right)\\
&\quad = \max\left(P_F, P_G, P_H\right)\\
&\quad = \max\{\langle[(0.09, 0.10, 0.11) ; 0.8] , [(0.08, 0.10, 0.12) ; 0.9]\rangle,\\
&\qquad\quad \langle[(0.04, 0.05, 0.06) ; 0.9], [(0.04, 0.05, 0.06) ; 1.0]\rangle,\\
&\qquad\quad \langle[(0.37, 0.40, 0.43) ; 0.8] , [(0.35, 0.40, 0.45) ; 1.0]\rangle\}\\
&\quad = \langle[(0.37, 0.40, 0.43) ; 0.8] , [(0.35, 0.40, 0.45) ; 0.9]\rangle\\
&P_{\text{and}}\left(\text{Detection Service Failure}\right)\\
&\quad = P_{E1} \times P_{E2} \times P_{E3} \times P_{E4}\\
&\quad = \langle[(0.12, 0.13, 0.14) ; 0.9] , [(0.11, 0.13, 0.15) ; 1.0]\rangle\\
&\qquad (\times) \langle[(0.10, 0.11, 0.12) ; 0.9] , [(0.10, 0.11, 0.12) ; 1.0]\rangle\\
&\qquad (\times) \langle[(0.04, 0.05, 0.06) ; 0.9] , [(0.03, 0.05, 0.07) ; 1.0]\rangle\\
&\qquad (\times) \langle[(0.03, 0.04, 0.05) ; 0.9] , [(0.03, 0.04, 0.05) ; 1.0]\rangle\\
&\quad = \langle[(0.0000144, 0.0000286, 0.0000504) ; 0.9] ,\\
&\qquad\quad [(0.0000099, 0.0000286, 0.0000630) ; 1.0]\rangle ,\\
&P_{\text{or}}\left(\text{Firewall Daemon}\right)\\
&\quad = \max\left(P_D, P_{\text{Detection Service Failure}}\right)\\
&\quad = \max\{\langle[(0.04, 0.05, 0.06) ; 0.8] , [(0.04, 0.05, 0.06) ; 0.9]\rangle,\\
&\qquad\quad \langle[(0.0000144, 0.0000286, 0.0000504) ; 0.9] ,\\
&\qquad\quad\quad [(0.0000099, 0.0000286, 0.0000630) ; 1.0]\rangle\}\\
&\quad = \langle[(0.04, 0.05, 0.06) ; 0.8] , [(0.04, 0.05, 0.06) ; 0.9]\rangle ,\\
&P_{\text{or}}\left(\text{IP Table}\right)\\
&\quad = \max\left(P_A, P_B, P_C\right)\\
&\quad = \max\{\langle[(0.33, 0.35, 0.37) ; 0.8] , [(0.30, 0.35, 0.40) ; 0.9]\rangle,\\
&\qquad\quad \langle[(0.12, 0.15, 0.18) ; 0.9] , [(0.10, 0.15, 0.20) ; 1.0]\rangle,\\
&\qquad\quad \langle[(0.09, 0.10, 0.11) ; 0.9], [(0.08, 0.10, 0.12) ; 0.9]\rangle\}\\
&\quad = \langle[(0.33, 0.35, 0.37) ; 0.8] , [(0.30, 0.35, 0.40) ; 0.9]\rangle .
\end{aligned}
\tag{5}
$$

Then, the top event possibilities of "Internet security system failure" during attack can be calculated as

$$
\begin{aligned}
&P_{\text{or}}\left(\text{Internet Security System Failure}\right)\\
&\quad = \max\left(P_{\text{SSH}}, P_{\text{POP3}}, P_{\text{Transport Layer Security}},\right.\\
&\qquad\quad \left. P_{\text{DNS}}, P_{\text{Firewall Daemon}}, P_{\text{IP Table}}\right)\\
&\quad = \max\{\langle[(0.000144, 0.000252, 0.000400) ; 0.8] ,\\
&\qquad\quad [(0.000105, 0.000252, 0.000495) ; 0.9]\rangle ,\\
&\qquad\quad \langle[(0.015912, 0.018000, 0.020254) ; 0.8] ,\\
&\qquad\quad\quad [(0.013376, 0.018000, 0.023520) ; 0.9]\rangle ,\\
&\qquad\quad \langle[(0.005824, 0.008400, 0.011520) ; 0.8] ,\\
&\qquad\quad\quad [(0.004860, 0.008400, 0.013200) ; 0.9]\rangle ,\\
&\qquad\quad \langle[(0.37, 0.40, 0.43) ; 0.8] , [(0.35, 0.40, 0.45) ; 0.9]\rangle,\\
&\qquad\quad \langle[(0.04, 0.05, 0.06) ; 0.8] , [(0.04, 0.05, 0.06) ; 0.9]\rangle,\\
&\qquad\quad \langle[(0.33, 0.35, 0.37) ; 0.8] , [(0.30, 0.35, 0.40) ; 0.9]\rangle\}\\
&\quad = \langle[(0.37, 0.40, 0.43) ; 0.8] , [(0.35, 0.40, 0.45) ; 0.9]\rangle .
\end{aligned}
\tag{6}
$$

*5.4. Comparisons and Discussion.* In order to evaluate the proposed method, a numerical verification is performed in Section 5. This study also compares the experimental results with the traditional probability reliability and Huang et al.'s [22] methods. The input data of these methods are shown in Figure 5 and Table 1. In the comparison of the results of the three methods, the differences between the proposed method and the listing methods can be shown clearly in Figure 7. From Figure 7, there are some findings.

(1) The traditional probability reliability and Huang et al.'s [22] methods do not consider the confidence level of domain experts. Therefore, the proposed method can be more flexible to present the confidence level of experts (highest confidence = 0.9).

(2) In both the traditional probability reliability method and Huang et al.'s [22] methods, the failure possibilities of the top event are all equal to 0.2359 and 0.40. Because these methods are fit, the outcome of the top event is certain and precise as long as the assignment of basic events is decent from reliable information.

(3) In the traditional probability reliability method, the failure possibilities of the top event are all equal at 0.2359. This is because the traditional probability reliability method does not consider the failure probability of the bottom events suffered in an attack and may obtain biased conclusions.

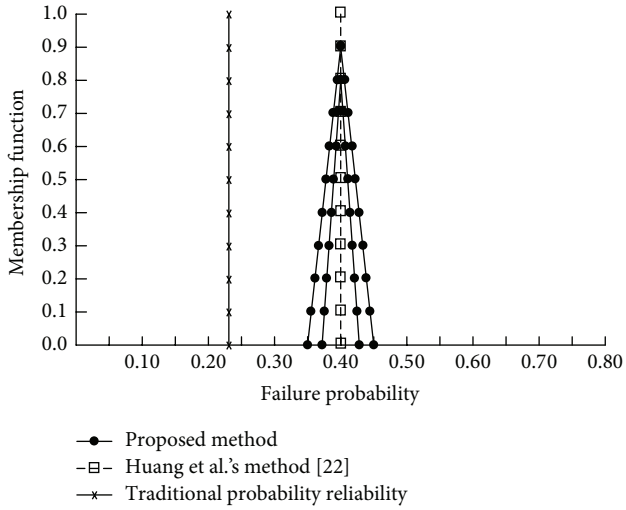



Figure 7: Membership function for top event of Internet security system failure.

(4) The results of the proposed and Huang et al.'s [22] methods under $\alpha$-level 0.9 are the same.

From the comparison, it is clear that the integrated attack tree and vague set technique outlined in this study provides the following advantages. Firstly, the failure information is being described as vague variables; this results in a more realistic and flexible reflection of the real situation. Secondly, the proposed method has considered the failure probability of the bottom events suffered in the attack. Finally, the proposed approach can indeed help to solve security threat assessments of an Internet security system when the available information is incomplete.

## 6. Conclusions

This paper has proposed a novel technique to assess the security threats of an Internet security system while under attack. It is useful when evaluating system reliability using the available information and expert's expertise, which is often uncertain or vague in the Internet security system. In particular, this approach has considered the failure probability of the bottom events of an Internet security system suffered in an attack.

In order to further illustrate the proposed method and compare it with other techniques of traditional reliability methods, the Internet security system example is adopted as a simulation example. This study also compares the simulation results with the traditional probability reliability and Huang et al.'s [22] methods. The results show that the proposed approach could provide a more accurate and reasonable security threat assessment to assist the decision-making process. Furthermore, the presented approach is more realistic and is a flexible reflection of the real situation. Moreover, the proposed methodology can help engineers solve security threat assessment problems under the situation of vague or incomplete information.

The advantages of the proposed approach are summarized as follows.

(1) The proposed method considers the malfunction data of the system elementary event as incomplete.

(2) The proposed method provides more accurate and effective information to assist the decision-making process.

(3) The failure information in a system's elementary event is described as vague variables; this result is more realistic and is a flexible reflection of the real situation.

(4) From a hacker's point of view, finding the weak links in the system for design is to find out a better design of an Internet security system.

## Conflict of Interests

The author declares that there is no conflict of interests regarding the publication of this paper.

## Acknowledgment

The author would like to thank the National Science Council of the Republic of China, for financially supporting this research under Contract nos. NSC 100-2410-H-145-001 and MOST 103-2410-H-145-002.

## References

[1] T. Tidwell, R. Larson, K. Fitch, and J. Hale, "Modeling internet attacks," in *Proceedings of the IEEE Workshop on Information Assurance and Security*, pp. 54–59, United States Military Academy, 2001.

[2] G. Dhillon and G. Torkzadeh, "Value-focused assessment of information system security in organizations," *Information Systems Journal*, vol. 16, no. 3, pp. 293–314, 2006.

[3] N. Satoh, H. Kumamoto, and Y. Kino, "Viewpoint of ISO GMITS and probabilistic risk assessment in information security," *International Journal of Systems Applications, Engineering and Development*, vol. 2, no. 4, pp. 237–244, 2008.

[4] Symantec Corporation, "Full report: internet security threat report," vol. 18, 2013.

[5] A. L. Opdahl and G. Sindre, "Experimental comparison of attack trees and misuse cases for security threat identification," *Information and Software Technology*, vol. 51, no. 5, pp. 916–932, 2009.

[6] K. Wu and S. Ye, "An information security threat assessment model based on Bayesian network and OWA operator," *Applied Mathematics and Information Sciences*, vol. 8, no. 2, pp. 833–838, 2014.

[7] Z. J. Lee and L. Y. Chang, "Apply fuzzy decision tree to information security risk assessment," *International Journal of Fuzzy Systems*, vol. 16, no. 2, pp. 265–269, 2014.

[8] A. Blyth, "An architecture for an XML enabled firewall," *International Journal of Network Security*, vol. 8, no. 1, pp. 31–36, 2009.

[9] G. Helmer, J. Wong, M. Slagell et al., "Software fault tree and coloured Petri net–based specification, design and implementation of agent-based intrusion detection systems," *International Journal of Information and Computer Security*, vol. 1, no. 1-2, pp. 109–142, 2007.

[10] M. N. Azaiez and V. M. Bier, "Optimal resource allocation for security in reliability systems," *European Journal of Operational Research*, vol. 181, no. 2, pp. 773–786, 2007.

[11] J. J. Zhao and S. Y. Zhao, "Opportunities and threats: a security assessment of state e-government websites," *Government Information Quarterly*, vol. 27, no. 1, pp. 49–56, 2010.

[12] W.-L. Gau and D. J. Buehrer, "Vague sets," *IEEE Transactions on Systems, Man and Cybernetics*, vol. 23, no. 2, pp. 610–614, 1993.

[13] Z. Wang, K. W. Li, and W. Wang, "An approach to multiattribute decision making with interval-valued intuitionistic fuzzy assessments and incomplete weights," *Information Sciences*, vol. 179, no. 17, pp. 3026–3040, 2009.

[14] J.-R. Chang, K.-H. Chang, S.-H. Liao, and C.-H. Cheng, "The reliability of general vague fault-tree analysis on weapon systems fault diagnosis," *Soft Computing*, vol. 10, no. 7, pp. 531–542, 2006.

[15] C.-N. Wang, G. K. Yang, K.-C. Hung, K.-H. Chang, and P. Chu, "Evaluating the manufacturing capability of a lithographic area by using a novel vague GERT," *Expert Systems with Applications*, vol. 38, no. 1, pp. 923–932, 2011.

[16] J. Ye, "Fuzzy decision-making method based on the weighted correlation coefficient under intuitionistic fuzzy environment," *European Journal of Operational Research*, vol. 205, no. 1, pp. 202–204, 2010.

[17] K. H. Chang and C. H. Cheng, "A novel general approach to evaluating the PCBA for components with different membership function," *Applied Soft Computing Journal*, vol. 9, no. 3, pp. 1044–1056, 2009.

[18] G.-W. Wei, "GRA method for multiple attribute decision making with incomplete weight information in intuitionistic fuzzy setting," *Knowledge-Based Systems*, vol. 23, no. 3, pp. 243–247, 2010.

[19] K.-H. Chang and C.-H. Cheng, "A risk assessment methodology using intuitionistic fuzzy set in FMEA," *International Journal of Systems Science*, vol. 41, no. 12, pp. 1457–1471, 2010.

[20] B. Schneier, "Attack trees," *Dr. Dobb's Journal*, vol. 24, no. 12, pp. 21–29, 1999.

[21] S. Gupta and J. Bhattacharya, "Reliability analysis of a conveyor system using hybrid data," *Quality and Reliability Engineering International*, vol. 23, no. 7, pp. 867–882, 2007.

[22] H.-Z. Huang, X. Tong, and M. J. Zuo, "Posbist fault tree analysis of coherent systems," *Reliability Engineering and System Safety*, vol. 84, no. 2, pp. 141–148, 2004.

[23] R. R. Yager, "OWA trees and their role in security modeling using attack trees," *Information Sciences*, vol. 176, no. 20, pp. 2933–2959, 2006.

[24] K.-H. Chang, C.-H. Cheng, and Y.-C. Chang, "Reliability assessment of an aircraft propulsion system using IFS and OWA tree," *Engineering Optimization*, vol. 40, no. 10, pp. 907–921, 2008.

[25] L. A. Zadeh, "Fuzzy sets," *Information and Computation*, vol. 8, no. 3, pp. 338–353, 1965.

[26] K. T. Atanassov, "Intuitionistic fuzzy sets," Report 1697/84, Central Tech Library, Bulgarian Academy Science, Sofia, Bulgaria, 1983.

[27] H. Bustince and P. Burillo, "Vague sets are intuitionistic fuzzy sets," *Fuzzy Sets and Systems*, vol. 79, no. 3, pp. 403–405, 1996.