# Online Risk Assessment of Intrusion Scenarios Using D-S Evidence Theory*

C.P. Mu[1], X.J. Li[2,3], H.K. Huang[2], and S.F. Tian[2]

[1]School of Mechatronic Engineering, Beijing Institute of Technology, 100081 Beijing, P.R. China
muchengpo@bit.edu.cn
[2]School of Computer and Information Technology, Beijing Jiaotong University, 100044 Beijing, P.R. China
[3]School of Information Engineering, NanChang University, 330029 NanChang, P.R. China

**Abstract.** In the paper, an online risk assessment model based on D-S evidence theory is presented. The model can quantitate the risk caused by an intrusion scenario in real time and provide an objective evaluation of the target security state. The results of the online risk assessment show a clear and concise picture of both the intrusion progress and the target security state. The model makes full use of available information from both IDS alerts and protected targets. As a result, it can deal with uncertainties and subjectiveness very well in its evaluation process. In IDAM&IRS, the model serves as the foundation for intrusion response decision-making.

**Keywords:** Online Risk Assessment, Intrusion detection, Alert Processing, Intrusion Response, D-S Evidence Theory.

## 1 Introduction

Intrusion detection systems (IDSs) are used to detect traces of malicious activity targeted against networks and their resources. Although IDSs have been studied and developed over 20 years, they are far from perfect and need improvement. The primary weaknesses of present IDSs are as follows.

First, most current IDSs generate a great number of false positive alerts, irrelevant alerts and duplicate alerts. Second, all the current IDSs focus on low-level attacks or anomalies and usually generate isolated alerts; none of them can capture the logical steps or strategies behind these attacks [1]. Finally, Current IDS alerts provide only the information about intrusions, but lack comprehensive parameters that take both attack factors and defence factors into account and indicate the real threat of intrusions to the protected targets. Therefore,it is very hard for an administrator or an automated intrusion response system (AIRS) to make the right intrusion response decision based on these IDS alerts.

* Supported by the Annual Proposed Sci-tech Project of 2008 of Jiangxi Education Bureau (GJJ08036).

S. Jajodia, and J. Lopez (Eds.): ESORICS 2008, LNCS 5283, pp. 35–48, 2008.
© Springer-Verlag Berlin Heidelberg 2008

The proposed online risk assessment model can effectively solve the above mentioned problems while dealing with uncertainties very well. The model presents a concise and real-time picture of the security state of the protected target under an intrusion, while providing much more information about the threat of the intrusion than raw alerts. In addition, It favors further automatic alert processing and forms the foundation for intrusion responses.

## 2 Related Work

Risk assessment is the process of identifying, characterizing, and understanding risk. Most traditional network risk assessment models follow a fairly static procedure and cannot satisfy the requirements of the ubiquitous computing environment. They are usually off-line models and focus on risks caused by the vulnerabilities of targets.

As an updated technique in the network security field, online risk assessment is the real-time evaluation of the threat caused by an ongoing intrusion on a protected target. In other words, it is an online model that focuses on risks caused by intrusions. The result of the risk assessment for an intrusion scenario could represent both the progress of the intrusion and the security states of the corresponding target, which is very important to minimize the impact on network security when the intrusion has been detected. At present,however, very little work has been done to address online risk assessment for technical limitation. Following are a few online assessment models proposed in recent years.

The Stellar real-time system developed by Stephen Boyer et al. [2] consists of a scenario building engine and a security risk assessment engine. Its architecture is similar to our IDAM&IRS. However, security risk is assessed by a set of rules written in Security Assessment Declarative Language similar to SQL, which is different from our risk assessment approach.

The RheoStat system developed by Ashish Gehani,et al is used to manage the real-time risk of a host[3]. Actually, it is an automated intrusion response system. The model takes the attack probability, the vulnerability exposure and the cost of the consequence (related to the asset value) as the risk assessment factors to determine the real-time risk on the protected host caused by an attack scenario. The model calculates the attack probability according to the match extent between the history of occurring events and a known intrusion template. Therefore, the model finds processing new intrusions difficult. In addition, its risk assessment results easily suffer from the impact of false positive alerts.

Andre Arnes et al present a real-time risk assessment approach based on Hidden Markov Models[4]. Although the paper states that one may use either statistical attack data from production or experimental system or the subjective opinion of experts to determine state transition probabilities, it is hard to use the model in practice because the approach lacks the detail calculation model of state transition probability.

In addition,the M-correlator alert processing model proposed by Phillip A. Porras et al ranks security incidents using an adaptation of the Bayes framework

for belief propagation in trees[5]. Dirk Outston et al propose an approach based on the Hidden Markov Models to rank threats caused by intrusions[6]. Although neither of them are online risk assessment models, they enlighten our research work.

Before online risk assessment, most of above the mentioned models don't use multiple approaches to process IDSs alerts. As a result, these models can't make full use of the available information. Therefore, they can not deal with uncertainties well and are prone to high subjectivity in the online risk assessment process.

## 3 The Architecture of IDAM&IRS and Component Functions

The presented online risk assessment model is used in IDAM&IRS (Intrusion Detection Alert Management and Intrusion Response System) developed by our lab. Automated intrusion response is the major function of the system.

To improve the information quality of alerts, different alert processing techniques have their own disadvantages and advantages[7,8]. In IDAM&IRS, alert confidence learning, alert verification, alert correlation and online risk assessment are used. These approaches complement each other and lead to a better result than a single approach in the improvement of IDS alert quality. The alert confidence learning module, the alert verification module and the alert correlation module serve as the foundation of the online risk assessment module because these modules reduce the impact of false positive alerts on the accuracy of risk assessment, form intrusion scenarios and provide objective assessment factors for risk assessment. Further,the proposed online risk assessment provides a strong support for intrusion response decision-making.

Here we briefly introduce the architecture and the component functions related to the proposed approach in IDAM&IRS. The architecture of IDAM&IRS shown in Fig.1 is distributed. The communication module is responsible for receiving alerts from multiple IDSs and sending response instructions to protected targets. In the alert filter, alerts are filtered according to their corresponding confidences. Only alerts with confidence values higher than the confidence threshold can pass through the module. We have proposed a supervised confidence learning approach described in [9], which is effective in filtering out regular and relevant false alerts(concering false alert types refer to[10]). The alert verification module compares the information referred by an alert with the information of its target host. It is used to reduce false alerts and irrelevant alerts, and provide alert relevance scores that represent the likelihood of successful attacks. The details of the module are discussed in [11]. The alert correlation module can aggregate related alerts together and form alert threads that represent corresponding intrusion scenarios, while providing risk assessment factors, including the alert amounts of alert threads and alert type numbers of alert threads. It can reduce random, uncorrelated false-positive alerts and duplicate alerts. The algorithm of the module is introduced in [10]. The online-risk assessment module evaluates

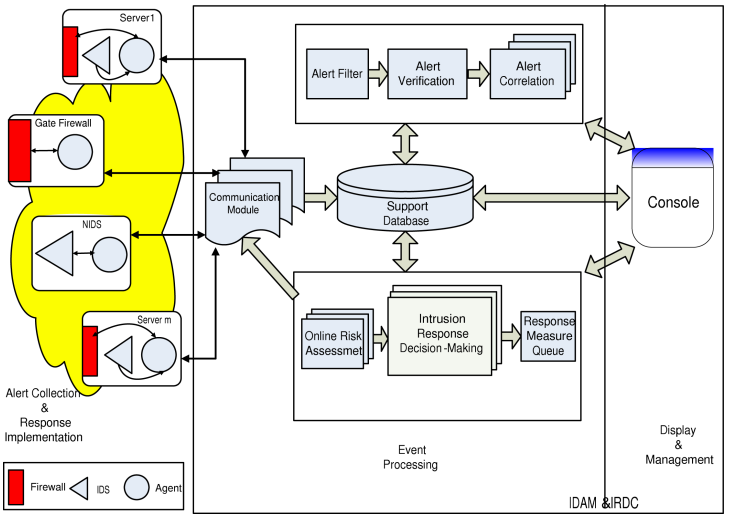


**Fig. 1.** The architecture of IDAM & IRS

the real-time risk caused by each intrusion scenario. According to the result of online risk assessment and other factors, the intrusion response decision-making module can determine response times and response measures, and write response instructions into the response measure queue. Through the console, an administrator can browse and manage alerts, maintain IDAM&IRS, and configure its parameters.

## 4 D-S Evidence Theory

D-S evidence theory (also called D-S theory) was proposed by Dempster and extended by Shafer. It allows the explicit representation of ignorance and combination of evidence, which is the main difference to probability theory that is treated as a special case. Therefore, D-S theory is a frequently used tool in solving complex problems with uncertainties caused by ignorance. Here we introduce the part of D-S theory just related to the online risk assessment model.

The Frame of Discernment $\Theta$ is a finite hypothesis space that consists of mutually exclusive propositions for which the information sources can provide evidence. $2^{\Theta}$ denotes its powerset. A basic probability assignment (bpa) or mass function $m$ is defined such that:

$$m : 2^{\Theta} \rightarrow [0, 1]$$

$$m(\phi) = 0$$

$$\sum_{V \subseteq \Theta} m(V) = 1$$

where $\phi$ is an empty set. $m(V)$ expresses the proportion of all relevant and available evidence that supports the claim that a particular element of $X$ (the universal set) belongs to the subset $V$. If $m(V) > 0$, $V$ is called a focal element of $m$.

Dempster's Rule of Combination gives us a data fusion approach that can combine different pieces of evidence together to get a joint support contribution and at the same time reduce uncertainties. The rule is given by the combined mass function $m = m_1 \bigoplus m_2 \bigoplus ... \bigoplus m_n$, as follows:

$$m(\phi) = 0$$

$$m(V) = \frac{\sum\limits_{\cap V_j = V} \prod\limits_{1 \le q \le n} m_q(V_j)}{\sum\limits_{\cap V_j \neq \phi} \prod\limits_{1 \le q \le n} m_q(V_j)} \tag{1}$$

where the combination operator $\bigoplus$ is called orthogonal summation.

## 5 Online Risk Assessment

### 5.1 Concepts and Idea of the Online Risk Assessment

Online risk assessment could give a comprehensive evaluation of the threat caused by an intrusion and a concise picture of the security state of the protected target. The results of online risk assessment could provide a strong decision support for security administrators or automated intrusion response mechanisms to make response decisions.

No matter off-line risk assessment models or on-line risk assessment models, most models assess risks caused by intrusions from three aspects: asset value, vulnerability and threat. For example, Tim Bass brought forward a risk identification and management model $R(Criticality, Vulnerability, Threat)$ [12]. The Criticality represents the importance of a protected asset(asset value); The vulnerability is a weakness in the system. It results from an error in the design, implementation or configuration of either the operating system or application software. The threat denotes an agent that can cause harm to an asset(the information of alerts indicates such an agent). In order to assess risks in real-time, we propose two notions in the online risk assessment model.

**Definition 1.** The Risk Index $RI$ is the dangerous degree to a protected target caused by an intrusion scenario. The meaning of $RI$ is in three aspects:(1)The probability that an abnormal activity detected by IDS is a true attack.(2)The probability that an attack can successfully compromise its target.(3)The severity caused by an attack.

Only a true and successful attack can cause a true threat to a protected target. Attacks with different severities can result in different threats and damages to a protected target. In addition, $RI$ represents the objective progress of an intrusion scenario.

**Definition 2.** The Risk Distribution is the spectrum of the high risk,the medium risk and the low risk that a target can endure.

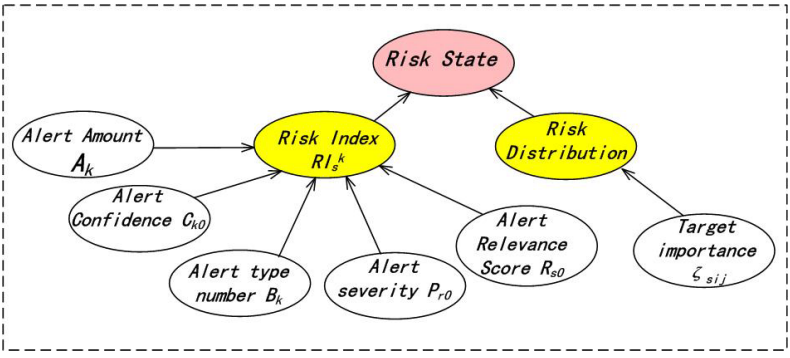


**Fig. 2.** Online risk assessment model

The Risk Distribution of a target is determined by the value or importance of the target. The importance of a target is usually evaluated by a subjective approach that reflects the security preference of an administrator[12].

The proposed online risk assessment model is shown in Fig.2. The model employs D-S evidence theory to fuse five assessment factors to compute $RI$. These factors in the model can be obtained from the alert confidence learning, the alert verification and alert correlation, and respectively represent the three aspects meaning mentioned in the Definition 1. Meanwhile, the target risk distribution can be determined by the importance of the target. Finally,the risk state of the target can be determined by the position of $RI$ in the risk distribution of the target.

### 5.2 Assessment Process

**Step 1 Calculation of $RI$**

In the model, there are three focal elements: $V_1$(No risk),$V_2$(Risk) and, $\theta$ (Uncertain risk $\theta = V_1 \cup V_2$). The membership functions of assessment factors are shown in Fig.3, and as follows:

(1)The alert amount of an alert thread $A_k$ represents not only the attack strength but also the attack confident situation. The more the alerts in an alert thread, the more likely the thread represents a true intrusion process.

$$\mu_{11} = \begin{cases} \frac{\alpha_2 - A_k}{\alpha_2} & A_k \le \alpha_2 \\ 0 & A_k > \alpha_2 \end{cases}, \mu_{12} = \begin{cases} 0 & \alpha_1 \ge A_k \\ \frac{A_k - \alpha_1}{\alpha_3 - \alpha_1} & \alpha_1 < A_k \le \alpha_3 \\ 1 & \alpha_3 < A_k \end{cases} \quad (2)$$

Where $\mu_{ij}$ is the membership degree that the target state belongs to $V_j$ according to $i^{th}$ assessment factor. $\alpha_1 \in [5, 15]$,$\alpha_2 \in [10, 20]$,and $\alpha_3 \in [15, 30]$ are constant and determined by expertise.

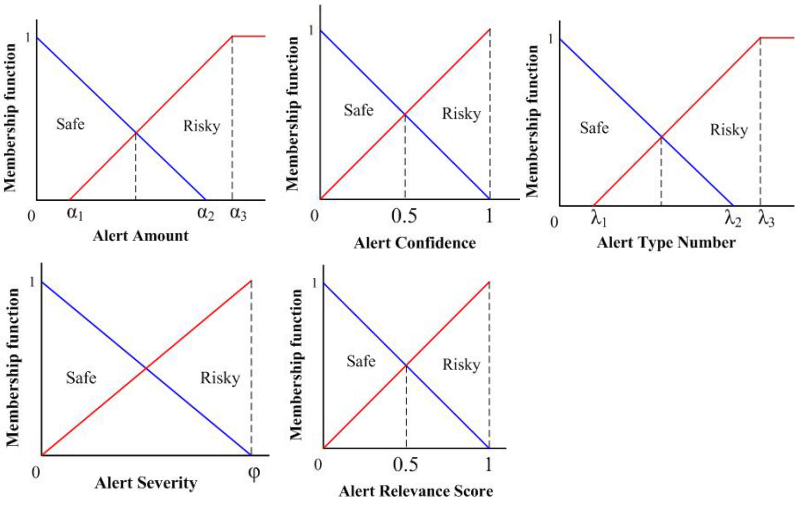


**Fig. 3.** Membership functions of assessment factors

(2)The second assessment factor is the updated alert confidence $C_{k0} \in [0,1]$ in an alert thread, that indicates the probability that an abnormal activity is a true attack. An alert confidence can be got from its corresponding raw alert or from the proposed alert confidence learning approach.

$$\mu_{21} = 1 - C_{k0} \qquad \mu_{22} = C_{k0} \tag{3}$$

(3)With the increase of the alert type in an alert thread, it usually means the corresponding attack scenario is progressing and the attacker is attempting to use different attack techniques. Therefore, the third assessment factor, the alert type number of the alert thread $B_k$, reflects both the attack confident situation and the severity of the corresponding intrusion.

$$\mu_{31} = \begin{cases} \frac{\lambda_2 - B_k}{\lambda_2} & B_k \le \lambda_2 \\ 0 & B_k > \lambda_2 \end{cases}, \mu_{32} = \begin{cases} 0 & \lambda_1 \ge B_k \\ \frac{B_k - \lambda_1}{\lambda_3 - \lambda_1} & \lambda_1 < B_k \le \lambda_3 \\ 1 & \lambda_3 < B_k \end{cases} \tag{4}$$

Where $\lambda_1 \in [1,5]$,$\lambda_2 \in [5,9]$,and $\lambda_3 \in [6,10]$ are constant and determined by expertise.

(4)Most IDSs can provide alerts with alert severity. The higher the alert severity , the riskier the corresponding attack. The updated alert severity in an alert thread $P_{r0}$ can be obtained from its corresponding raw alert.

$$\mu_{41} = \begin{cases} \frac{\varphi - P_{r0}}{\varphi} & P_{r0} \le \varphi \\ 0 & P_{r0} > \varphi \end{cases}, \mu_{42} = \begin{cases} \frac{P_{r0}}{\varphi} & P_{r0} \le \varphi \\ 1 & P_{r0} > \varphi \end{cases} \tag{5}$$

The constant $\varphi$ is determined by the specification of the IDS that generates the alert. For example, the parameter Priority in a Snort alert is used to indicate

the severity of an incident [13]. Priority is divided into three level(Priority=1, the most severe level;Priority=2, severe level; Priority=3, the least severe level). Therefore, set $\varphi = 3$ and $P_{r0} = 4 - Priority$ for Snort alerts.

(5)According to the definition 2 and alert verification process, the relevance score can indicate not only if there is a vulnerability in the protected target but also if the vulnerability is exploited by an attacker. Actually, a relevance score represents the likelihood of a successful intrusion. That is why the relevance score of the updated alert in an alert thread, $R_{s0}$, is introduced in the online risk assessment model.

$$\mu_{51} = 1 - R_{s0} \qquad \mu_{52} = R_{s0} \tag{6}$$

According to the $q^{th}$ assessment factor, a target risk situation resulted by an intrusion thread $k$ could be measured by the value of the bpa $m_q^k(V_j)$. It expresses the proportion of $q^{th}$ assessment factor that supports the claim that the target state belongs to $V_j$. $m_q^k(V_j)$ can be calculated from above membership functions of assessment factors according to the following equations.

$$m_q^k(V_j) = \frac{\mu_{qj}}{\sum_{i=1}^{2} \mu_{qi} + 1 - w_q \times P_{IDS0}} \tag{7}$$

$$m_q^k(\theta) = 1 - \sum_{j=1}^{2} m_q^k(V_j) \tag{8}$$

Where $q = 1, 2, ..., 5; j = 1, 2; P_{IDS0}$ is the general precision of the IDS that generates the updated alert of the intrusion thread $k$. $1 - P_{IDS0}$ is the incorrect classification rate of the IDS which is one of major uncertainty sources.

The function of the coefficient $w_q$ is to make different assessment factors play different roles in the risk assessment process because different assessment factors usually cause different uncertainty in the assessment results. Here set $w_5 \geq w_4 \geq w_3 \geq w_2 \geq w_1$. After the determination of the values of the bpa $m_q^k(V_j)(j = 1, 2, ..., 5)$, these values can be further fused into $m^k(V_1), m^k(V_2), m^k(\theta)$ by Eq.(1). The fusion result $m^k(V_2)$ is the risk index, that is

$$RI^k = m^k(V_2) \tag{9}$$

**Step 2 Determination of Risk Distribution and Risk State**

In the model, the importance value of a target is determined by the services provided by the target. Table 1 shows such an example. Then the risk distribution of a target can be decided according to its corresponding importance value like Fig4 shows.

In Fig4, there is a distribution feature that the more important a target, the lower the position of its high risk rang and the longer its high risk state range. For an ordinary target, its low risk state range,medium risk state range and high risk state range are $[0, 0.5)$, $[0.5, 0.8)$,and $[0.8, 1.0]$ respectively; For an important target, its low risk state range,medium risk state range and high risk state range are $[0, 0.4)$, $[0.4, 0.7)$,and $[0.7, 1.0]$ respectively; For a very important target, its

**Table 1.** Importance values of targets

| Target | Running service | Importance value $\xi_i$ |
|---|---|---|
| Ordinary target | Telnet, Web | 1 |
| Important target | Mail, Ftp | 2 |
| Very important target | DNS, Database | 3 |

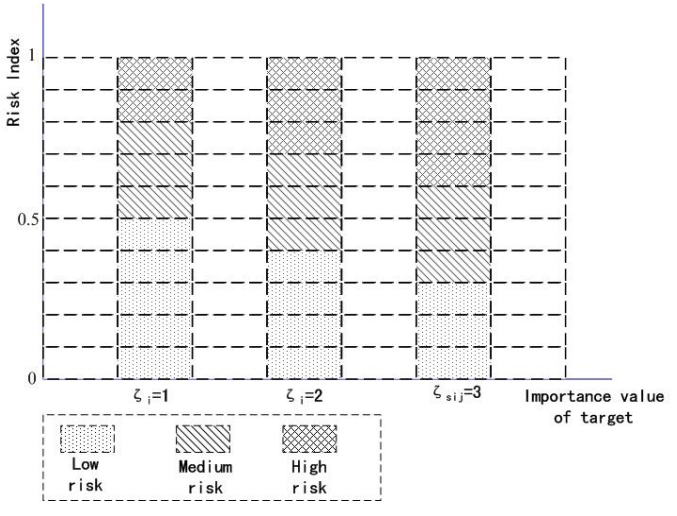


**Fig. 4.** Risk distributions of targets with different importance values

low risk state range,medium risk state range and high risk state range are $[0, 0.3)$, $[0.3, 0.6)$,and $[0.6, 1.0]$ respectively.

Finally the risk state of a target is decided by the position of $RI$ in its corresponding risk distribution. For instance, when $RI$ caused by an intrusion is 0.7, an ordinary target ($\xi = 1$) is at medium risk state. However, a very important target($\xi = 3$) is at high risk state.

## 6 Experiments and Analysis

In the experiments, Snort 2.0 IDS and IDAM&IRS were deployed on the subnet (xxx.71.75.130-xxx.71.75.180) in our laboratory that has a connection to the Internet. BlackICE PC Protection and Norton Internet Security 7.0 IDSs were also installed on some hosts in the subnet. There are four types of network servers, i.e. Http Proxy, Ftp,Web and Database in the subnet. The operating systems include Windows XP, Windows 2000, Windows 2003 server, and Linux. The experiment subnet is shown in Fig5.

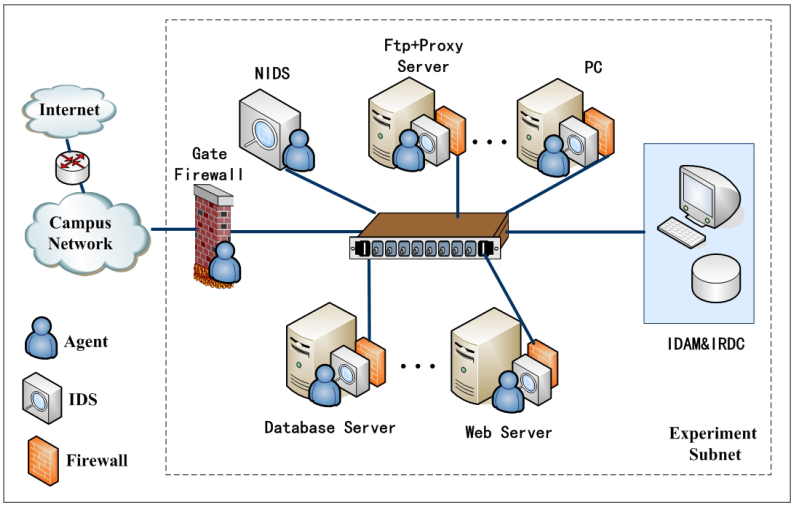


**Fig. 5.** Experiment subnet

At present, there are so many intrusion approaches that it is impossible to test all of them. In the online risk assessment experiments, a few of the typical attacks were carried out.

(1) The Vertical Scan attack[14] is an essential step in most intrusion scenarios. Attackers usually use the approach to collect messages about attacked targets in order to figure out a way to compromise targets. Here we employed a scan tool to probe the database server in which a MS SQL Server database was running. The vertical scan items include:

- opening ports on the server that are usually used to figure out the services provided by the server and the operating system name,etc.;
- NetBios message that can be used to recognize the target's register table, the user names, the work groups, etc.;
- SNMP message that can be used to find the target network connections, the operating system name & version, the user list, etc.

Fig.6 is the online risk assessment result, which shows that as the scan attack progressed, more and more alerts were generated and the risk increased rapidly. The risk curve in Fig.6 accords with the feature of the scan attack. Finally the vertical scan attack can result in the database server ($\xi = 3$ , a very important target) being at the high risk state.

(2)Denial of Service (DoS) is a common attack on the Internet, which dose not need great attack skills but is hardly defended. In the DoS experiment,the SYN flood attack,which is a kind of DoS,lasted 1 min. Fig.7 indicates that the risk caused by DoS attack quickly rises, and soon tends to be a high and constant value (about 0.7963). This risk assessment result answers to the expertise about DoS.

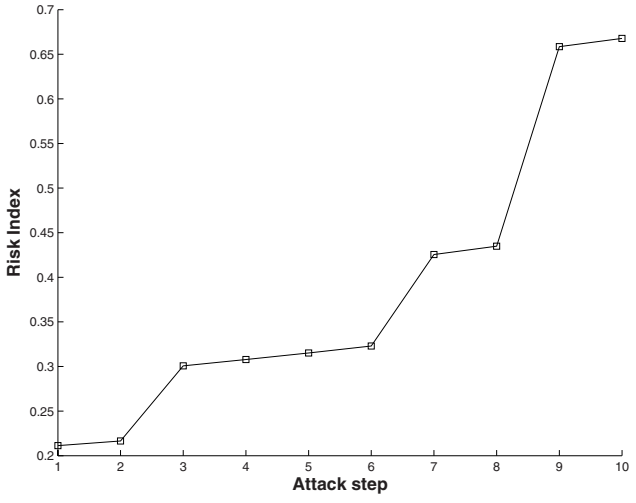


**Fig. 6.** The online risk assessment result for Vertical scan

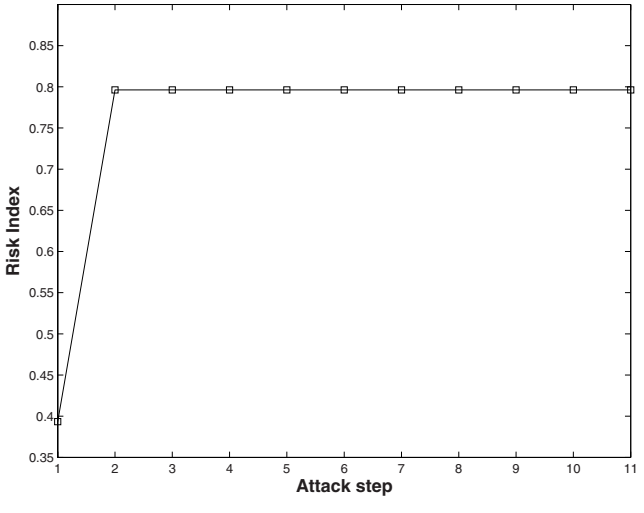


**Fig. 7.** The online risk assessment result for DoS

Under the condition, ordinary targets ($\xi = 1$) are at the medium risk state, both important targets ($\xi = 2$) and very important targets ($\xi = 3$) are at the high risk state.

(3)Most dangerous intrusions usually consist of not a single attack step but multiple attack steps. In the scenario of Ftp MDTM vulnerability intrusion, an attacker can compromise an Ftp server by doing the following steps:

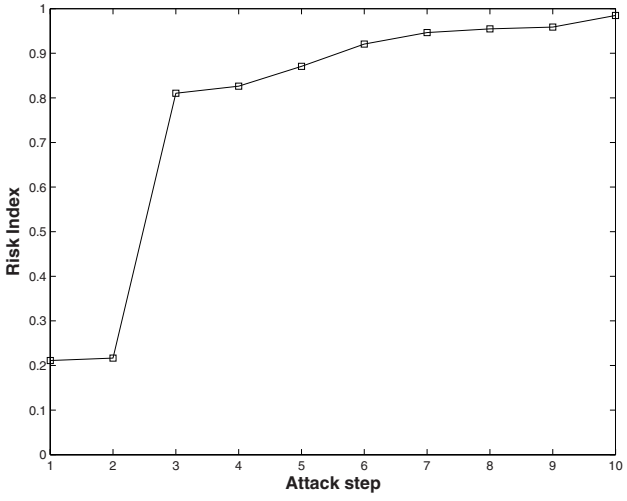


**Fig. 8.** The online risk assessment result for Ftp MDTM overflow attack

- To probe the 21 port of the target in order to decide if the target provides Ftp service and get the messages about the name and version of the Ftp application software. One can make use of these messages to find if there is MDTM vulnerability on the Ftp server.
- To exploit MDTM vulnerability, the attacker has to know a user name and its password of the Ftp application service. Therefore, the second step is to probe a user name and its password through a dictionary attack method. The step could be bypassed if the Ftp service allows anonymous login.
- With the above messages about the Ftp server, the attacker can use an MDTM attack tool (such as Swan) to overflow the Ftp service. If the attack step succeeds, a specific port will be opened. Finally the attacker could get the system operation right of the target by telnetting the opened port.

The risk assessment result shown in Fig.8 clearly indicates the risk variation in the three steps. The risk reaches the highest value (about 0.9936) when the Ftp service is successfully overflowed, which means that the server is totally controlled by the attacker. All kinds of targets ($\xi = 1, 2, 3$) would be at the high risk state in the case.

(4) The online risk assessment model can effectively reduce the impact of false positive alerts because the model can greatly reduce the assessment uncertainties by combining multiple assessment factors. In the experiment, alerts generated by IDSs are processed by the alert correlation model and the online risk assessment model. There are 2 scenarios:one is a true intrusion scenario that consists of only 3 raw alerts; another is a false positive intrusion scenario that consists of 20 raw alerts. The risk assessment result shown in Fig.9 indicates that the online risk assessment approach is able to distinguish a true intrusion scenario from a false positive scenario.

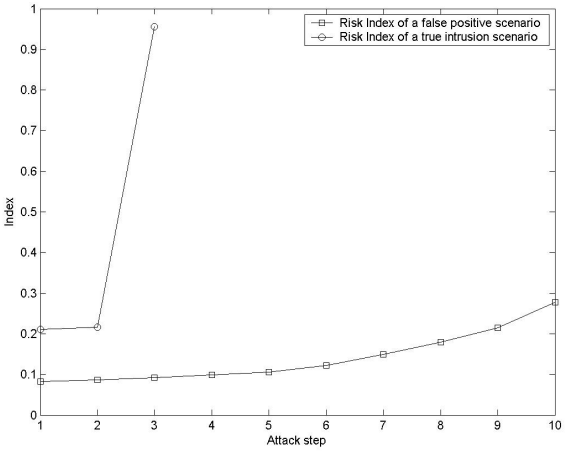


**Fig. 9.** The online risk assessment result for a true intrusion scenario and a false positive intrusion scenario

In addition, many different experiments show that IDSs may generate a great number of false positive alerts. However, the relevance scores of these false positive alerts are low and the alert types of false positive scenarios are monotonous. As a result, risks caused by false positive scenarios are usually low in the model. Therefore, the model is quite helpful to find the most dangerous intrusion,while reducing the impact of false positive alerts.

## 7 Conclusions

The above experiments prove that the real-time risk evaluations of intrusion scenarios accord with the actual features of these intrusions and expertise. The online risk assessment model can deal with uncertainties and subjectiveness well while providing an objective and accurate result for the security state of a protected target. The introduction of the risk assessment model enables IDAM&IRS to tolerate IDS false positive alerts and sets the foundation for intrusion response decision-making.

## References

1. Ning, P., Cui, Y.: An intrusion alert correlator based on prerequisites of intrusion. Technical Report TR-2002-01, Department of Computer Science, North Carolina State University (January 2002)
2. Boyer, S., Dain, O., Cunningham, R.: Stellar: A fusion system for scenario construction and security risk assessment. In: Third IEEE International Workshop on Information Assurance (IWIA 2005), Maryland, USA, pp. 105–116 (2005)

3. Gehani, A., Kedem, G.: RheoStat:Real-Time Risk Management. In: Recent Advances in Intrusion Detection:7th International symposium (Raid 2004), Sophia Antipolis, France, September 15-17, 2004, pp. 196–314 (2004)
4. Arnes, A., Sallhammar, K., Haslum, K., Brekne, T., Moe, M.E.G., Knapskog, S.J.: Real-Time Risk Assessment with Network Sensors and Intrusion Detection Systems. In: Hao, Y., Liu, J., Wang, Y.-P., Cheung, Y.-m., Yin, H., Jiao, L., Ma, J., Jiao, Y.-C. (eds.) CIS 2005. LNCS (LNAI), vol. 3801, Springer, Heidelberg (2005)
5. Porras, P.A., Fong, M.W., Valdes, A.: A mission-impact-based approach to INFOSEC alarm correlation. In: Wespi, A., Vigna, G., Deri, L. (eds.) RAID 2002. LNCS, vol. 2516. Springer, Heidelberg (2002)
6. Ourston, D., Matzner, S., Stump, W., Hopkins, B.: Coordinated internet attacks: Responding to attack complexity. Journal of Computer Security 12(2), 165–190 (2004)
7. Valeur, F., Vigna, G., Kruegel, C., Kemmerer, R.A.: A comprehensive approach to intrusion detection alert correlation. IEEE Trans. Dependable Secure Comput. 1(3), 146–169 (2004)
8. Maines, J., Kewley, D., Tinnel, L., Taylor, S.: Validation of sensor alert correlators. IEEE Security Privacy Mag. 1(1), 46–56 (2003)
9. Mu, C.P., Huang, H.K., Tian, S.F.: Managing Intrusion-Detection Alerts Based on Fuzzy Comprehensive Evaluation. In: 10th International Conference on Fuzzy Theory and Technology (FTT 2005), Salt Lake City, Utah, USA, July 21-26 (2005)
10. Mu, C.P., Huang, H.K., Tian, S.F.: False Positive Alert, Irrelevant Alert and Duplicate Alert Reduction Based on a Comprehensive Approach. Journal of Dynamics of Continuous, Discrete and Impulsive System Series B, Supplementary Issue (2006)
11. Mu, C.P., Huang, H.K., Tian, S.F.: Intrusion Detection Alert Verification based on Multi-level Fuzzy Comprehensive Evaluation. In: Hao, Y., Liu, J., Wang, Y.-P., Cheung, Y.-m., Yin, H., Jiao, L., Ma, J., Jiao, Y.-C. (eds.) CIS 2005. LNCS (LNAI), vol. 3801, pp. 9–16. Springer, Heidelberg (2005)
12. Bass, T., Robichaux, R.: Defence-in-depth: Qualitative risk analysis methodology for complex network centric operation (2004), `http://www.silkroad.com/papers/pdf/archives/defense-in-depth-revisited-origintal.pdf`
13. Caswell, B., Beale, J., Foster, J.C., Posluns, J.: Snort 2.0 Intrusion Detection. Syngress Publishing, Inc., Sebastopol (2003)
14. Staniford, S., Hoagland, J.A., McAlerney, J.M.: Practical automated detection of stealthy portscans. Journal of Computer Security 10(1-2), 105–136 (2002)