International Journal of Security and Its Applications
Vol.8, No.1 (2014), pp.363-372
http://dx.doi.org/10.14257/ijsia.2014.8.1.34

Network Security Situation Assessment Ecurity Based on the Associated Diffusion Analysis

Xiangdong Cai[1],Yuran Wang[1],Fushuai Zhang[1] and Yangjing yi[2]

[1]*School of Automation, Harbin University of Science and Technology*
150080 Harbin, PR China
[2]*Harbin Engineering University*
150001 Harbin, PR China
Harbin University Of Science And Technology, Harbin150080, China
E-mail:82380102@163.com

Abstract

The abstract is to be aiming at the complex security situation, situation assessment through a comprehensive analysis of the conclusions drawn generalization to ease management staff awareness and response pressure. Analysis of a number of typical characteristics and lack of assessment methods, we propose a conversion to right harm, dangerous and spread overlay analysis assessment model as the core of the vector, Aims correlation within the network point of view, more thorough, more accurately reveal the security situation. Describes the data, services due authorization, depending on the association occurs, discussed attacking position, risk measure, as well as the superposition of effects coordinated attack. From the point of view of the invasion, the attacker through security breaches or theft of fake login authorization, illegal operation of various resources, directly against the data, services, confidentiality, integrity, availability, and then pass along the dependencies harm, causing wider ramifications indirect losses. From the potential risks, dynamic threats, permanent loss of three levels starting assessed value of each component of the momentum, using the overlay method and clustering method to speculate attacks intended, identify coordinated attack and guiding automatic defense. At last, using with experiments to validate and assess. This model adaptable well, and it's able to draw more precise conclusions credible assessment.

Keywords: *network security; situation evaluation; correlation analysis; spread analysis; attack intention*

1. Introduction

As the increasingly large, complex and heterogeneous network, security threats, tend to be diversified, in the face of a large number of different format, form the log and alarm of each different, the traditional safety assessment have been overwhelmed, and derive the situation assessment and prediction. From regulatory facilities of multi-source information filtering, integration and abstract, enable managers to the security situation and have a general understanding of the change trend, make quick response to the complex security threats. Different Angle and focus on research has begun.

In terms of situation assessment, BASS [2] is based on intrusion detection system, with the aid of multi-sensor data fusion evaluation, and it is an early attempt, and limited to the proof-of-concept.

ISSN: 1738-9976 IJSIA

In terms of trend prediction, Overall, foreign started earlier, domestic research more, the following points shall be referred.

In the security elements, evaluation indicators and quantitative methods such as basic research, not yet widely recognized system formed from the systematic, standardized, practical use is still far away, despite the plethora of active exploration [1], but little progress. Network is an organic whole thing, and which is not a simple pile of several hosts. These methods more or less ignored the topology separates the link between nodes, Tianping Chen et al [8] of graph theory and Yongzheng Zhang *et al.*, [9] the risk of propagation models recognize this, but the emphasis on traditional security assessments.

By time series analysis as the main line, accurate prediction is extremely difficult to achieve, excessive fitting is the result of coincidence, more related to the selected data. Learn from existing models [10], such as GM (1,1), ARMA, Holt-Winter, etc., the poor accuracy of the forecasts. From the law identification, description means, uncertainty, the angle of the sample size analysis of the causes of forecast bias: If attacks have occurred are difficult to identify, describe its rule, it gets harder the presentation of future trends. Individual sudden attack very strong, great uncertainty, the forecast for this random perturbations near-guessing. Only when the sample size is large enough, the individual random variation can largely offset each other, thereby limiting the growth of macroeconomic uncertainty, easy forecast reflects a smooth trend. Difficult to predict if the independent variable lines of attack, it is difficult to predict the trend of the dependent variable lines. If through the filter to remove high frequency disturbances, leaving only the low-frequency trends, forecasts would be better.

In the situation assessment, there are still many problems to be solved, common: Apply even tend to cater to a variety of models, which distorts the nature of the security situation. Floating on the macroscopic evaluation, ignoring microscopic analysis, resulting in accurate conclusions beneath. Neglect or fragmented the nodes, the correlation between services. Based indicators is difficult to determine, quantitative methods are not natural. Detained in mutual restraint type weighting scheme, larger scale, the artificial setting is very difficult. Single scalar value type situation too general. Assessment findings not reflect the size of the network, the associated topology, resource value and other factors, most of them only to observe, not guide defense. Difficult to compare different networks lateral appraised value.

To solve these problems, we propose a framework for intrusion detection and access control on an assessment model, easy to use without restriction assessed value replaces the abstract concrete weights, according to security vulnerabilities, intrusion alarms, resource value, dependencies and other assessment situation. Time-varying trend values contain vector-type risks, threats and loss of three components, specifically, means that there are loopholes in the risk of attacks, attacks occurred after the evolution of threats, attacks, after the success of energy losses.

1.1. System and Concept

Figure 1 in concept describes the relationship between the safety factor, for example, $N[x]$ subnet of $H[3]$, host deployed $S[2]$, $S[3]$ two kinds of service, $S[2]$ have $V[1]$ and $V[3]$ two kinds of weaknesses. And we can use $A[1]$ method against $V[1]$, also can take $C[1]$ countermeasure to defense against $A[1]$ and so on. It is distinct to describe the conceptual description and instantiation. For example, Different host on the same $S[sid]$ on behalf of the same service, but because of the deployment of version and the installing the patch are different. And it's regarded as different instances of the same service.

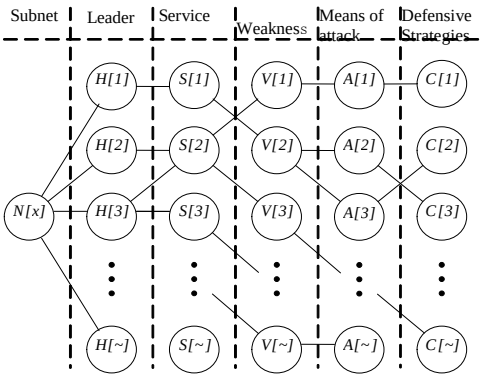

Figure 1. Security Elements and Relationships

Uppercase and lowercase characters represent a collection and element. Set of resources $O = O_D \cup O_S = \{\text{data}\} \cup \{\text{service}\}$, abbreviated as $O = D \cup S = \{d \mid d \in D\} \cup \{s \mid s \in S\}$. Set of the type of operation $И = И_D \cup И_S = \{ⓡ, ⓦ, ⓞ\} \cup \{ⓧ, ⓞ\} = \{\text{read, write, control}\} \cup \{\text{call / execution, control}\}$. Harmful type set $Л = \{ⓒ, ⓘ, ⓤ\} = \{\text{confidentiality, integrity, availability}\}$, another said security feature set, and so on. Permission set $R = R_D \cup R_S = O_D \times И_D \cup O_S \times И_S$. Hazard set $B = B_D \cup B_S = O_D \times Л \cup O_S \times Л = O \times Л$. Authorization set $ЮO = R \times U$. Permission entry $r = (o, и) \in R$. Hazardous items $b = (o, л) \in B$. Mandate $ю = (o, и, u) \in ЮO$. Introducing an expression of the form $\Gamma_{Xa\,Y}(x)$ and x refer to a collection of elements related to the Y and unambiguous form can be abbreviated as $x.Y$, $\Gamma_{Xa\,Y}(X) = \bigcup_{x \in X} \Gamma_{Xa\,Y}(x)$ refers to X collection related to the Y set to meet $\Gamma_{Xa\,Z}(x) = \Gamma_{Ya\,Z}(\Gamma_{Xa\,Y}(x))$ -transitive by x expansion to X when empathy. For example, $\Gamma_{Sa\,R}(s)$ denotes the set of permissions granted to s services, $\Gamma_{Sa\,V}(s)$ refers to the spread of service vulnerability set s, $\Gamma_{Va\,A}(v)$ refers to the set of methods vulnerability attack v, $\Gamma_{Sa\,A}(s) = \Gamma_{Va\,A}(\Gamma_{Sa\,V}(s))$ refers to the set of methods that attack s service, $\Gamma_{Aa\,S}(a)$ refers to the set of services for a attack, and so on.

1.2. Authorization and Rely On

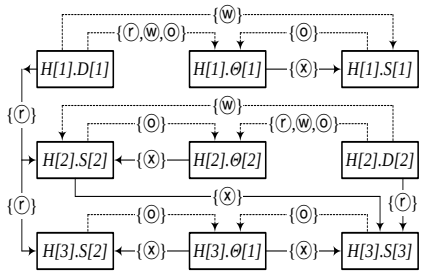

Figure 2. Authorization and Depend on the Sample

Figure 2 shows an example of environment, $D[i] \in D$ refer to the data, $S[i] \in S$ refer to general service and $Θ[i] \in S$ specifically refer to the operating system. From the resource node

refers to the dotted line arc single refers to the authorized user nodes, dot-dash line arc single refers to rely on, arc standard is set operation, the same start-stop, direction and arc arc mark dotted line and point crossed into solid line arc overlay welding. For example, $H[3].S[3]$ run depend on the reading of $H[2].D[2]$, also has been authorized.

Φ and Ψ only describe the dominant direct dependence, recessive indirect dependence or transfer rely on see later. Strict segmentation of dependencies should be able to form a directed acyclic graph, or illegal infinite recursion relies on, but no this requirement for authorization.

2. Juche Idea

2.1. The Attack Position

In view of the s services, according to attack the point of discussion: (1) $s.u$ user attempts to steal passwords endanger $s.u$ set of permissions $\Gamma_{UaR}(s.u)$, If you can succeed under the constraints of the $\Gamma_{UaR}(s.u)$ victimizers. (2) $s.v$ weakness of the attempt to overcome endanger $s.v$ set of permissions $\Gamma_{VaR}(s.v)$ that can be exposed, such as the use of a buffer overflow vulnerability to execute code injected illegal and legal codes usually have execute permissions equivalent. Attack $\Theta.u$ or $\Theta.v$ can cause a collapse of the host. $\Gamma_{ZaR}(s.z), z \sim [u \mid v]$ unified expression using these two permission sets to meet $\Gamma_{ZaR}(s.z) \subseteq \Gamma_{SaR}(s)$.

(DoS/DDoS) denial of service attack, also known as the point of weakness, even though it may not be exposed to permissions, but the threat of attacks over the direct infringement of availability.

If $\Gamma_{ZaR}(s.z)$ is an attacker to steal, then that has lost its legitimacy authorization set $\{(o, и, s) \mid (o, и) \in \Gamma_{ZaR}(s.z)\}$ to spend any authorized entries are judged illegal infringement.

2.2. The Attack Position

Relying on the discrete-time model, the slot δ is the frequency of the measurement interval of attack, the attacker is defined as the number of contiguous window $\Xi(t_i, t_j)$ counting time slots even into $(t_i, t_i + (j-i)\times\delta]$, with the passage of a new δ Change：(1) Adjust the current time $t_j \leftarrow t_j + \delta$. (2) If δ has a new attack occurs, the starting time of t_i unchanged otherwise be adjusted to $t_i \leftarrow t_i + \delta$ and then follow up to the next non-empty slot, or directly to the right boundary of t_j.

Risk measure $P(a,t)$ is a probability indicators to measure the degree of risk attack strength. According to formula (2) to calculate, e belongs to $P(a,t)$ which specifically refers to the base of natural logarithms, σ_a called the attack equivalent, to measure the efficiency and severity of attacks, thus easily measured $N(a,t)$ value based on estimated value of $P(a,t)$ unpredictable. Not difficult to see, Ξ time-varying changes function dominates $N(a,t)$ and $P(a,t)$ rise and decay, specifically, sustained attack resulted in cumulative threats to suspend attacks does not mean that the threat has been completely eliminated.

$$P(a,t) = 1 - 1/\ln(\mathrm{e} + \sigma_a \times N(a,t)) \quad (1)$$

Formula (3) expresses the multiple attacks against the same target measurement synthesis, extend from $P(a,t)$ to $P(A,t)$, the formula of $1 \le k < n$, and a_k divided by the subset.

$$\begin{aligned} P(\{a_1, a_2, ..., a_n\}, t) &= 1 - (\prod_{i=1}^{n} (1 - P(a_i, t))) \\ &= 1 - (\prod_{i=1}^{k} (1 - P(a_i, t))) \times (\prod_{i=k+1}^{n} (1 - P(a_i, t))) \\ &= 1 - (1 - P(\{a_1, ..., a_k\}, t)) \times (1 - P(\{a_{k+1}, ..., a_n\}, t)) \end{aligned} \quad (2)$$

Occurred or not the elapsed attack a corresponding inactive Ξ is empty, that is $N(a,t) = 0$, given by formula (2) we $P(a,t) = 0$, given by formula (3) we measure no contribution on the synthesis.

It supports both element level, collection-level synthesis, and also supports a complete type, incremental superimposed random attack in a variety of environments initiation and disappear quickly calculate the time-variant Joint Strike measure.

Extended from three perspectives, expand its meaning and form of specialization: (1) Items from the attack perspective, the introduction of $P_A(a,t)$ refers to the $P(a,t)$. (2) From the perspective of hazardous items, if b by threat, but A_x does not have to be difficult or expression, use a $P_B(b,t)$ expression. (3)Items from the vulnerability perspective, the introduction of non-time-dependent $P_V(v)$ v indicates weakness or vulnerability degree of vulnerability.

$$P_V(v) = 1 - \prod_{a \in v.A} (1 / \ln(e + \sigma_a)) \quad (3)$$

Formula (4) for v first sort attack set $v.A$, the $v.A$ in accordance with the sharpness of the attack synthetic $P_V(v)$. In the $(0, \delta]$ period, if $(0, \delta]$ is an attack occurs once for each v, there are $P_V(v) = P_A(v.A, \delta)$, this time both equivalence.

2.3. The Attack Position

Formula (5) in the loss function $f_L(o, л, t)$ is to t closing time, o resource item security losses $л$, the former polynomial if and only if $(o, л) \in \{(d, ©), (d, ⓘ)\}$ exists, of the latter type empathy. $\alpha_{(o,л)}$ measure of the value of units of data, $\lambda_{(o,л)}(t)$ records $[0,t]$ documented period monitored illegal data traffic, if $t_1 \le t_2$ then there are $\lambda_{(o,л)}(t_1) \le \lambda_{(o,л)}(t_2)$, $\beta_{(o,л)}$ called nominal loss rate, $\mu_{(o,л)}(t)$ computes t times $(o, л)$ measure the extent of the infringement, to meet $0 \le \mu_{(o,л)}(t) \le 1$, non-invasive security session at the $\mu_{(o,л)}(t) \equiv 0$ value.

$$f_L(b,t) = f_L(o, л, t) = \underbrace{\alpha_{(o,л)} \times \lambda_{(o,л)}(t)}_{Only\ for\ b \in D \times \{®, ⓘ\}} + \underbrace{\beta_{(o,л)} \times \int_t \mu_{(o,л)}(t) dt}_{Only\ for\ b \in D \times \{ⓘ, ℗\} \mathrm{US} \times Л} \quad (4)$$

$(d, ⓡ)$ peep data theft permissions d, the hazards of d confidentiality $(d, ©)$, $\lambda_{(d,®)}(t)$ record with an illegal flow of data read. $(d, ⓦ)$ privilege corrupted data when theft the $(d, ⓘ)$, $\lambda_{(d,ⓘ)}(t)$ record with an illegal flow of data is written, $\beta_{(d,ⓘ)}$ measurement unit time consequential damages, such as data such as confusion continued to mislead users, $\mu_{(d,ⓘ)}(t)$ metering data corruption ratio. $(d, ⓞ)$ privilege interdiction data theft hazards d when d

usability $(d,ⓤ)$, measured data can not be accessed with $\beta_{(d,⊗)}$ caused loss rate, then $\mu_{(d,⊗)}(t) \equiv 1$. Coefficient, meaning the function, the value increased with $(o,л)$ and change, for example, $\alpha_{(d,⊗)}$ to measure the losses caused by leaks, $\alpha_{(d,⊗)}$ measure permanent loss of data or recover costs , the two values are not the same.

When jurisdiction $(s,ⓧ)$ stealing and thiefing s services, endanger the confidentiality of s — $(s,ⓒ)$, the $\beta_{(s,⊗)}$ measure s 's timing Unit, $\mu_{(s,⊗)}(t)$ measures periods theft frequency of $(t-\Delta t,t]$, that the percentage of the total number of illegal calls. Stealing right $(s,◎)$ and tracking s is also harmful processes and state confidentiality, this time is $\mu_{(s,⊗)}(t) \equiv 1$. Superposition of multiple hazards, $\beta_{(o,л)}$ is cumulative and take, $\mu_{(o,л)}(t)$ and $P(a,t)$ synthesis method similar. Right $(s,◎)$ tampered status or permission to steal inject code endanger the integrity of s — $(s,ⓘ)$, the measurement error consideration longer than $\beta_{(s,⊗)}$, $\mu_{(s,⊗)}(t)$ measure error response proportion, because it is difficult to measure temporarily set $\mu_{(s,⊗)}(t) \equiv 1$. Against acts of service availability, including the right to steal $(s,ⓧ)$ contention Services, steal $(s,◎)$ right to terminate the service launched DoS / DDoS attacks, $\beta_{(s,⊗)}$ and $\beta_{(s,⊗)}$ meaning similar, $\mu_{(s,⊗)}(t)$ measure performance degradation extent that unauthorized access to the proportion accounted for rated load.

s dynamic text refers specifically to the service process, the corresponding static code image by data processing.

2.4. Right Harm Conversion

For threated assessment, using covering and clustering methods, to speculate attack intention and to guide dynamic defense.

Covering method based on attack counts, let $\xi(b,t)$ refers the attacking counts to threat b at the moment of t. First using $(\forall b \in B)(\xi(b,t)=0)$ to initialize $\xi(b,t)$, then using $(\forall Hb(a,t) \in Hb(A,t))\ (\forall b \in Hb(a,t).J)\ \ (\xi(b,t) \leftarrow \xi(b,t)+1)$ to count, and then using $\xi(b,t)$ to sequence.

Clustering method based on kernel similarity, using $K(\{a\},t)$ to refer $Hb(a,t).J$, J is called the core. The intersection of two nuclear nucleus remains. For example, $K(\{x,y\},t)=K(\{x\},t)\,\mathrm{I}\,K(\{y\},t)$ the expression is $K(X\,\mathrm{U}\,Y,t)=K(X,t)\,\mathrm{I}\,K(Y,t)$. Two nuclei are not referring to the union. According to formula (6) calculating the similarity between two nuclear.

$$Sim(K(X,t),K(Y,t))= \left|K(X,t)\,\mathrm{I}\,K(Y,t)\right| \Big/ \left|K(X,t)\,\mathrm{U}\,K(Y,t)\right| \tag{6}$$

Suppose there are n attacks. First using $\forall(a_i \neq a_j)$ to calculate the similarity between $K(\{a_j\},t)$ and $K(\{a_i\},t)$ .Getting C_n^2 counts. If $Sim(K(\{a_i\},t),K(\{a_j\},t)) \neq 0$ and it is the maximum, then shielding $K(\{a_i\},t)$ and $K(\{a_j\},t)$ adding the new item $K(\{a_i,a_j\},t)$. Calculating the similarity of the new term and the rest. This process is repeated. Forests constitute hierarchical clustering, the composition of the same root, the Joint Strike. For each tree from the root to the leaf trace shows intent to attack at all levels.

Both can be used alone, may also be used in combination. To using the former counts excluding the small one, then analyzing the latter.

3. Experimental Analysis

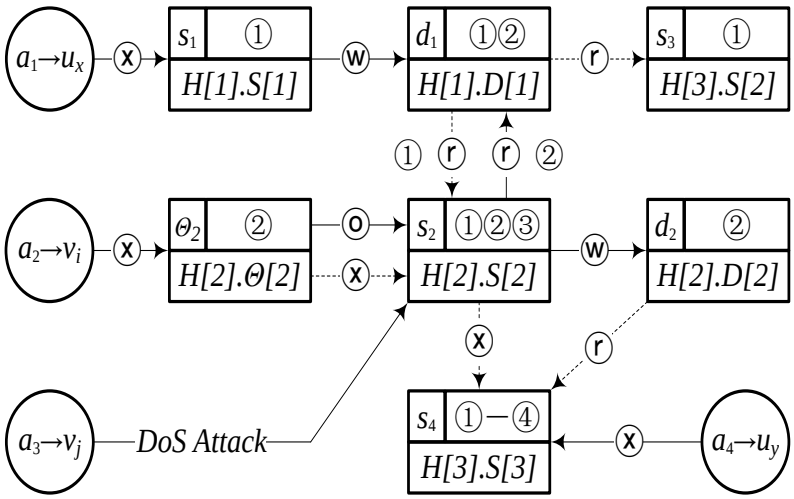

Figure 3.Experimental Environment and Process

Figure 3 lists the simulation parameters related to four attacks, defense and repair response includes two areas, covering more value due to breakdown and are not listed. Front-end system detects an attack, self-starting distributed infringement monitor, repair, infestation can be manually stopped, will not last impact properties.

Figure 3 $(s_1, ①, H[1].S[1])$ -type node structure, s_1 is $H[1].S[1]$'s short, circled numbers marked nodes and edges attached to the diffusion map , the solid line, dotted line direct , indirect infringement.

For example, threat assessment explore the dangerous measure overlay track. For example, when $t = 4$, $P_B(s_3, ①, t) = P_A(\{a_1\}, t) = 0.27$, $P_B(s_2, ①, t) = P_A(\{a_1, a_2\}, t) = 0.66$, $P_B(s_3, ①, t) < P_B(s_2, ①, t)$. We can see, $(s_3, ①)$ separate threat only by a_1, and $(s_2, ①)$ by a_1 and a_2 in combination threat more dangerous situation.

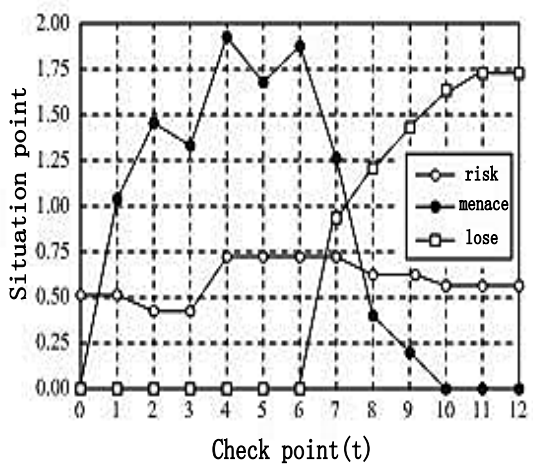

Figure 4. Confidentiality Related to Changes in Posture

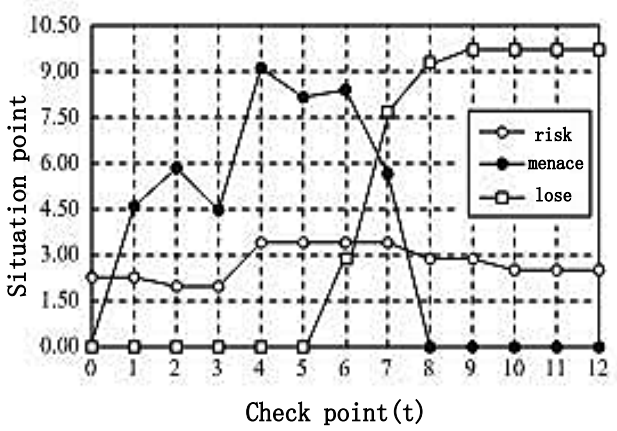

Figure 5. Integrity-related Changes in Posture

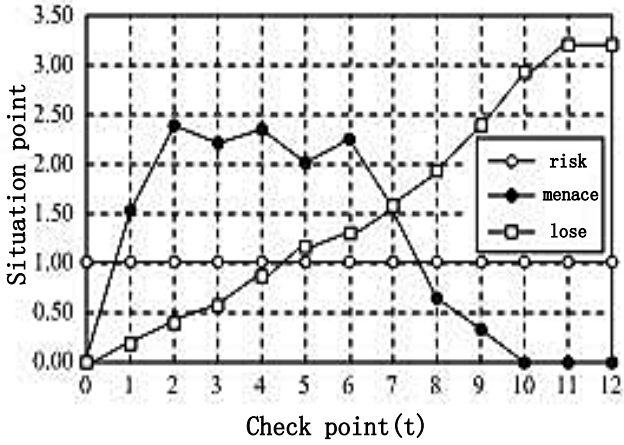

Figure 6. Availability-related Changes in Posture

Figures 4, 5 and 6, respectively, describe the confidentiality, integrity and availability of the situation changes. Overall, the trend in the value of the experiment integrated structure, integrity-related values had the largest share, followed by availability, and confidentiality.

Figures 4 and 5, the value at risk with the amount of data d_1 and d_2 fluctuate; Figure 5 is not, whether the concern is the availability of access to d_i.

4. Conclusion

This paper reviews the research situation, analyzes the flaws exposed. Then expounded the security elements, authorization relations and dependencies, discusses the attack position, risk measure, superposition algorithm and the right to harm conversion. And then propose a vector-based evaluation algorithm, from three levels assess posture, with the intention of both methods speculation. Finally be analyzed and validated by means of experiments. In contrast, the model to eliminate or weaken the defects previously summarized, with good size scalability, support for different coarse-grained assessment can more truly reflect the security posture.

The system is open, gradually expanded to support further research include: the introduction of a more complete index system, expanding scope of the assessment, evaluation efforts to deepen; explore more reasonable presentation of the trend value, and strive to be more comprehensive and deeper, more aptly reveals the security situation; explore practical trend forecasting method, developed to show the trend of more practical tools; strengthen the linkage with smart defense, improve assessment of the effect on the defense, developed pre-simulation tool.

References

[1] W. Juan, Z. Fengli and F. Chong, "Study on index system in network situation awareness", Computer Applications, (in Chinese), vol. 27, no. 8, **(2007)**, pp. 1907-1909.
[2] T. Bass, "Intrusion detection systems and multisensor data fusion: creating cyberspace situational awareness", Communications of the ACM, vol. 43, no. 4, **(2000)**, pp. 99-105.
[3] B. D'Ambrosio, M. Takikawa and D. Upper, "Security situaion assessment and response evaluation(SSARE)", Proc of the DARPA Information Survivability Conference & Exposition II. Los Alamitos: IEEE Computer Society, **(2001)**, pp. 387-394.
[4] C. Xiuzhen, Z. Qinghua and G. Xiaohong, "Quantitative hierarchical threat evaluation model for network security", Journal of Software, (in Chinese), vol. 17, no. 4, **(2006)**, pp. 885-897.
[5] X. Haidong, "Analysis of security situational awareness of cyberspace", Shanghai: School of Electronics and Electric Engineering, Shanghai Jiao Tong University (in Chinese), **(2007)**.
[6] L. Ying, W. Huiqing and L. Jibao, "A method of network security situation awareness based on rough set theory", Computer Science, (in Chinese), vol. 34, no. 8, **(2007)**, pp. 95-97.
[7] W. Yong, L. Yifeng and F. Dengguo, "A network security situational awareness model based on information fusion", Journal of Computer Research and Development, (in Chinese), vol. 46, no. 3, **(2009)**, pp. 353-362.
[8] C. Tianping, Q. Xiangdong and Z. Lianqing, "Application of graph theory in threat situation analysis of network security", Journal of Beijing University of Posts and Telecommunications, (in Chinese), vol. 32, no. 1, **(2009)**, pp. 113-117.
[9] Z. Yongzheng, F. Binxing and C. Yue, "Risk propagation model for assessing network information systems", Journal of Software, (in Chinese), vol. 18, no. 1, **(2007)**, pp. 137-145
[10] W. Yong and L. Yifeng, "A network security situational awareness model based on log audit and performance correction", Chinese Journal of Computers, (in Chinese), vol. 32, no. 4, **(2009)**, pp. 763-772.