Research of Network Behavior Hazard Assessment Method based on the Dynamic Area Method

Caihua Zhang[1, a], Jun Ren[2,b] and Zhenliang Dong[3,c]

[1]Hebei College of Industry and Technology ,Department of Adult Education Shijiazhuang,China

[2]Hebei Education Examination Authority, Information Section Shijiazhuang,China

[3] Hebei Education Examination Authority,Information Section Shijiazhuang,China

[a]zchcz@sina.com, [b]renj@hebeea.edu.cn, [c]dzl@hebeea.edu.cn

Keywords: network behaviors; interval distance; extension assessment; harm degree assessment

Abstract. The harm degree assessment of network behaviors is a measure of network security management. It provides key reference for formulating security policy, creating information system and safe running system. It also guarantees the security of network and information to the utmost. Present a method of calculating the harm degree of network behaviors which is based on dynamic interval distance of quantitative analysis, and provide relevant calculating methods to various assessment factors through utilizing extension assessment, at last, analysis with actual data validation. This method can get a more accurate assessment result under the conditions of the values of the network behavior parameters are not precise enough. It provides a basis for the network management systems automatically process appropriate policy based on the specific harm degree and efficient automatic management.

Introduction

The user's network behavior harm research mainly from the point of view of the attacker to analyze attack effect, such as literature [1] to network entropy method to calculate made into the harm degree, the literature [2, 3] respectively from the network type and specific host to analyze hazard degree model. In risk assessment studies are mainly with the whole network as the research object, the entire network's risk evaluation, such as literature [4, 5] respectively danger theory, attribute recognition theory applied in analyzing the whole network of risk.

Network behavior harm degree evaluation methods

Network behavior harm degree assessment model.

Quantitative hazard degree evaluation need to give value at risk of quantitative results, to evaluate the network behavior harm degree, this paper mainly based on the network center. In the literature [5] on the basis of summing up the literature [6] proposed based on LEC method of campus network user behavior of hazard assessment model and apply improvement, because before the harm degree evaluation parameters, although considered the static (T), dynamic (I, A, P) two kinds, but the same kind of behavior of the different behavior source and behavior target to the dangers of the Internet degree influence there's a big difference between size, so and can't fully reaction harm degree influence. Together with the source and behavior behavioral objective parameter is independent, the paper to join these factors and improved.

Mainly from the following aspects to consider:

$HDB = F(T, I, A, P); T = F'(T', S, D)$

The F stands for network behavior harm degree evaluation function, and F ' stands for network behavior types of evaluation function, can pass the function to calculate. The network types of evaluation degree; T stands for network behavior types of evaluation value, and T' stands for network behavior types of authority type parameters, namely the behavior get permissions level. Note here that the improvement on the type of network behavior to determine, corresponding behavior source

Published by Atlantis Press, Paris, France.

and behavior target together to determine network behavior parameters, in order to meet the requirements of the parameter selection of reality; I said monitoring the behavior of the strength parameters; A stands for this user behavior the scope of influence of parameter; P stands for the behavior duration parameter; S said the behavior focus; D stands for the behavior role goal; HDB stands for to the network behavior hazard degree evaluation result, namely the behavior affect the normal operation of the hazard value, as shown in figure 1.

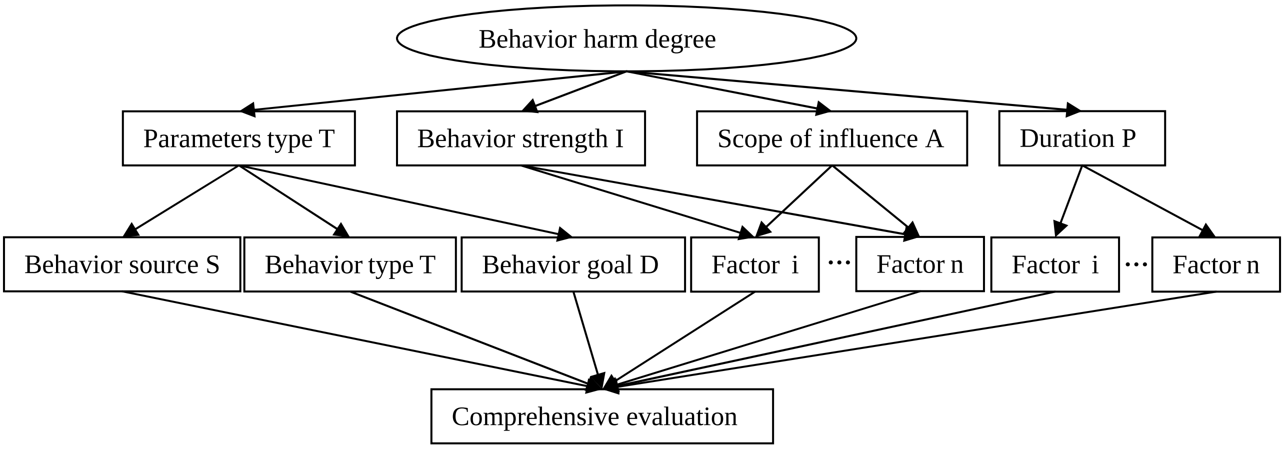

Figure 1. Network behavior harm degree assessment model

The above is the network behavior harm degree of quantitative analysis information, these are known as evaluation factors. In the assessment, not only should consider above elements of the measured value, but also considering these factors history value, etc., can also consider the safety of the factors such as object attribute.

The application of network behavior hazard degree evaluation method.

Evaluation index set $LEV = \{lev1, lev2, lev3, lev4, lev5, lev6\}$ is hierarchies of the harm degree evaluation. HDB evaluation system is divided into six subsystems {T, I, A, P, S, D}, respectively evaluation behavior type, behavior strength, influence scope, duration, behavior source, behavior target six factors about evaluation index correlation. Because each elements of the attributes and characteristics by multiple influence, so to multistage assessment process. By the school network center proposed hazard control strategy value, according to the extension evaluate party code field we can get:

$$R_0 = \begin{bmatrix} \text{LEV} & \text{lev1} & \text{lev2} & \text{lev3} \\ \text{HDB} & <0,10> & <10,60> & <60,120> \\ \text{lev4} & \text{lev5} & \text{lev6} & \\ <120,2000> & <2000,7000> & <7000,10000> & \end{bmatrix}$$

Using extension evaluation method of the evaluation system of various factors joint domain:

$$R_p = (P, C, V_P) = \begin{bmatrix} \text{P T} <0,10> \\ \text{I} <0,10> \\ \text{A} <0,10> \\ \text{P} <0,10> \\ \text{S} <0,1> \\ \text{D} <0,1> \end{bmatrix}$$

There are three ways to get the T value:

1) According to the experience value assignment, such as the network center with behavior management model of the applications.

2) Mathematical analysis method. By using the probability analysis, the simulation function analysis;

3) Summary induction. As Dr. ZhangYi in literature [2] mentioned unfriendly act classification. This paper improved from the network security of the three main characteristics to analyze all kinds of attack quantization value, as is shown in table 1.

Table 1. Improved behavior type

Number	Behavior source S	Behavior goal D	Authority type T’
1	LAN	Personal terminal	Access to information
2	Internet	Office terminal	Modify information
3		Server	Use the service
4		The router	Denial of service
5			Increase the service

To analyze the evaluation factor D: the same kind of network user behavior for behavior target is different, the normal operation of the whole network to the damage degree have quite big difference. We can get the domain according to the specific value system, as shown in table 2.

Table 2. Behavior target value table

Harmfulness	Small	General	Medium	Larger	Big
Behavior target	Personal terminal	DNS route	FTP route	WEB route	Core route
D	<0,0.2>	<0.2,0.4>	<0.4,0.6>	<0.6,0.8>	<0.8,1>

Experiment

In the experiments, the main data are taken from the school campus network 5 groups of different records, including T cpdump, S for data packets in the destination address types, D for destination address types, S_n for this behavior packet size, with the behavior from a source or destination address contact number of hosts. B_n netflow data taken from the access port bandwidth utilization size, use the utilization rate and rate, T "is taken from for packet forwarding rate and transceiver symmetric ratio of interval value. Pc and Ph from Syslog log information of this behavior duration and historical records of the time, H_{total} for historical records of the influence the number of maximum machine. As the table 3 shows, detected the parameter value, using the above analysis method for the corresponding values of interval domain, using the extension assessment method of comprehensive evaluation concluded HDB Lev, this data reflect the above analysis method.

Table 3. Network behavior harm degree data analysis

Parameters / NO.	T			I		A		P		HDB
	T’	S	D	B_n	S_n	a	H_{total}	P_c	P_h	LEV
Pretend IP	<6.8>	<0.4,0.6>	<0.8,1>	68	93	78	890	63	396	4
Pretend gateway	<9,10>	<0.9,1>	<0.1,0.2>	0.9	60	170	175	252	749	5
Worms	<8,10>	<0.9,1>	<0.6,0.8>	27	62	27	50	111	179	6
ARP attack	<7,8>	<0.8,1>	<0.3,0.4>	1.1	60	11	70	251	44	4
DOS	<7,8>	<0.5,0.6>	<0.1,0.2>	1.7	1518	2	148	227	142	2

Conclusion

This paper puts forward a dynamic area based on the distance network behavior harm degree evaluation method, this method will extenics multi-level and many factors on things for a comprehensive multi-level evaluation applied to network behavior harm degree evaluation, and the dynamic assignment and interval domain, combining increased assignment flexibility and strengthening of the parameter uncertainties of tolerance, and as the parameters given dynamic assignment method. Make value to the parameter is not enough precise conditions still results in a

Published by Atlantis Press, Paris, France.

more accurate results, network management system can be comprehensive analysis of various factors, the conclusion is drawn that this user's network behavior of the harm degree, let network management system automatically execute corresponding treatment strategy, to realize efficient automation management to provide the basis.

References

[1] Chang P T, Hung K C. Applying the Fuzzy-Weighted-Average Approach to Evaluate Network Security Systems[J].Computers and Mathematics with Application,2005,49:17-1814.

[2] Gupta A. Network Management: Current Trends and Future Perspective [J]. Journal of Network and Systems Management, 2006, 14 (4):483-491.

[3] Bernstein L. Network Management Isn’t Dying, it’s Just Fading Away [J].Journal of Network and Systems Management, 2007, 15(4):419-424.

[4] Goodall, J. R., Lutters, W. G., Komlodi, A. The Work of Intrusion Detection:Rethinking the Role of Security Analyst. in: Proceedings of the Tenth Americas Conference on Information Systems. New York: 2004.

[5] Ammann, P., Wijesekera, D., Kaushik, S. Scalable, Graph-based Network Vulnerability Analysis. in: Proceedings of 9th ACM Conference on Computer and Communications Security (CCS 2002): 2002.

[6] ARDA. Advanced Research and Development Activity. Exploratory Program Call for Proposals 2006. USA. 2005.

[7]Yanmei Li, Chen Zi. Analysis of Load Factors Based on Interpretive Structural Model. Journal o fComputers. Vol.7, No.7, 2012,7 :1704-1711.

Published by Atlantis Press, Paris, France.