

基于动态区间距的网络行为危害度评估方法

黄烟波, 刘展宏, 黄家林

(中南大学 信息科学与工程学院, 湖南 长沙 410083)

摘要:网络行为危害度的评估是网络安全管理的一种措施,为安全策略的制定、信息系统的建立及安全运行提供重要依据,最大限度地保证网络和信息的安全。提出了一种基于动态区间距的定量计算网络行为危害度的方法,并为各项影响因素提供了相应的参数计算方法,并用实际数据进行了分析验证。该方法能在网络行为评估参数取值不够精确的条件下评估出较准确的结果,为网管系统根据具体的行为危害度自动执行相应的处理策略和实现高效自动化管理提供了依据。

关键词:网络行为;区间距;可拓评价方法;危害度评估

中图分类号:TP301

文献标识码:A

文章编号:1673-629X(2010)10-0163-04

Harm Degree Assessment Method of Network Behaviors Based on Dynamic Interval Distance

HUANG Yan-bo, LIU Zhan-hong, HUANG Jia-lin

(Department of Information Science and Engineering, Center South University, Changsha 410083, China)

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.

Key words: network behaviors; interval distance; extension assessment; harm degree assessment

0 引言

用户的网络行为的危害研究主要从攻击者的角度来分析攻击效果,如文献[1]以网络熵的方法来计算造成的危害度,文献[2,3]分别从网络类型和具体主机来分析危害度模型。在危害评估方面的研究主要以整个网络作为研究对象,对整个网络承担的风险进行评估,如文献[4,5]分别将危险理论、属性识别理论应用于分析整个网络的风险。

在研究方法上,现在对危害评估主要有定性、定量和综合方法。如 Delphi, 专家系统法等都是定性的评估方法,主要是根据分析者的知识、经验、教训、业界的标准和特殊变例等非量化资料对系统的安全状况和危害性做出判断的过程。这种方法能进行全面而深刻的

评估,但主观性很强,精确性得不到保证。如概率模型、信息熵模型等都是定量的评估方法:采用数量指标对网络的安全状况进行评估,大大增加了可操作性。定量分析方法能够使研究结果更科学,但常常为了量化,使事物简单化、模糊化,甚至误解某些因素。层次分析法、文献[6]的模糊评价法等都是综合实现定量与定性的互补,主观与客观统一,目前主要方向是实现定性到定量的转化。

随着网络管理的发展,文献[7,8]提到网络管理的未来,现代园区网管理需要网络管理系统能判断特定的行为是否友好,及行为给网络造成多大影响。要提高网络管理的反应速度,降低网管人员的工作强度,然后根据影响的具体大小调用相关的策略等等,这就需要实时地取得相应的定量数据,才能实现网络管理自动化。然而用户的网络行为的危害度研究涉及到多层次多角度的相关因素,其数量众多难以准确量化,往往需要进行定性分析。可拓评价方法^[9]不仅可以利用多层次、多角度的因素对事物进行评价,而且具有综合利

收稿日期:2010-01-30;修回日期:2010-04-28

基金项目:国家自然科学基金资助项目(60673164)

作者简介:黄烟波(1959-),男,湖南邵阳人,教授,研究方向为计算机网络。

用定性和定量分析的能力,特别是基于区间距的评价方法能够容忍一定程度的评价因素取值的不确定性。

1 网络行为危害度评估方法

1.1 网络行为危害度评估模型

定量的危害度评估需要给出风险值的量化结果,要评估网络行为危害度,文中主要依据本校网络中心在文献[10,11]的基础上总结文献[12]中提出的基于LEC方法的园区网用户行为的危害评价模型并加以改进,由于之前的危害度评估参数,虽然考虑了静(T)、动态(I,A,P)两种,但是同一种行为的不同行为源和行为目标对网络的危害度影响大小是有很区别的,所以并没能充分反应危害度影响。加之行为源和行为目标参数又是各自独立的,文中加入这些影响因素,并加以改进。

主要从以下几方面来考虑:

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

其中F表示网络行为危害度的评估函数,而F'表示网络行为类型的评估函数,可以通过该函数计算出该网络类型的评估度;T表示网络行为类型的评估度值,而T'表示网络行为类型的权限类型参数,也就是该行为获得的权限级别。这里需要注意的是,文中改进在网络行为的类型确定上,把对应的行为源与行为目标一起用来确定网络行为参数,以满足参数取值现实性的要求;I表示监控的该行为的强度参数;A表示该用户行为影响的范围参数;P表示该行为持续时间参数;S表示该行为发动者;D表示该行为作用的目标;HDB表示对该网络行为危害度评估的结果,即该行为影响网络正常运行的危害值,如图1所示。

以上是对网络行为危害度进行定量分析的信息,这些被称为评估要素。在进行评估时,不仅要考虑以上要素的实测值,还要综合考虑这些因素的历史值等,还可以考虑对象的安全属性等因素。

1.2 动态区间距应用到网络行为危害度评估中

在对模型中的各参数进行赋值时,为了满足各参数对不同环境的影响,可以对区间距以动态的方式赋予。在进行危害度评估中注意几点:

(1)取值区间尽量精确,量值区间的半径要尽可能的小,并且限定在各评价因素的值的取值区间半径不大于该特征在各级别上经典域的半径。即满足前面要求函数中限定的前项半径总是小于后项半径。这就要求尽量减小参数在具体值上的取值范围。所以在赋值的时候可以根据历史记录来确定参数将要产生的发展趋势。

(2)动态区间确定中危害最大化原则,在方法取值中,遵循尽量让取值在上限的危害度区间变化,因为当危害行为发生时,在保证精确度的基础上,尽量最大化值的危害度。在文中动态区间的取值基本是以历史记录和数学函数为主。如:当以历史记录进行赋值时,遵循的原则是,如果实测数据小于历史记录的平均值,取值区间为 $\langle \text{data_current}, \text{data_average} \rangle$,如果实测数据大于或等于历史平均值,取值区间为 $\langle \text{data_current}, \text{data_max} \rangle$ 。

(3)多数确定原则,当区间 $\langle x, y \rangle$ 的绝大部分位于区间 $\langle a, b \rangle$ 内时,就可以根据实际需要对该值的范围适度调整再确定其边界。

1.3 网络行为危害度评估方法应用

取评价指标集 $LEV = \{\text{lev1}, \text{lev2}, \text{lev3}, \text{lev4}, \text{lev5}\}$,

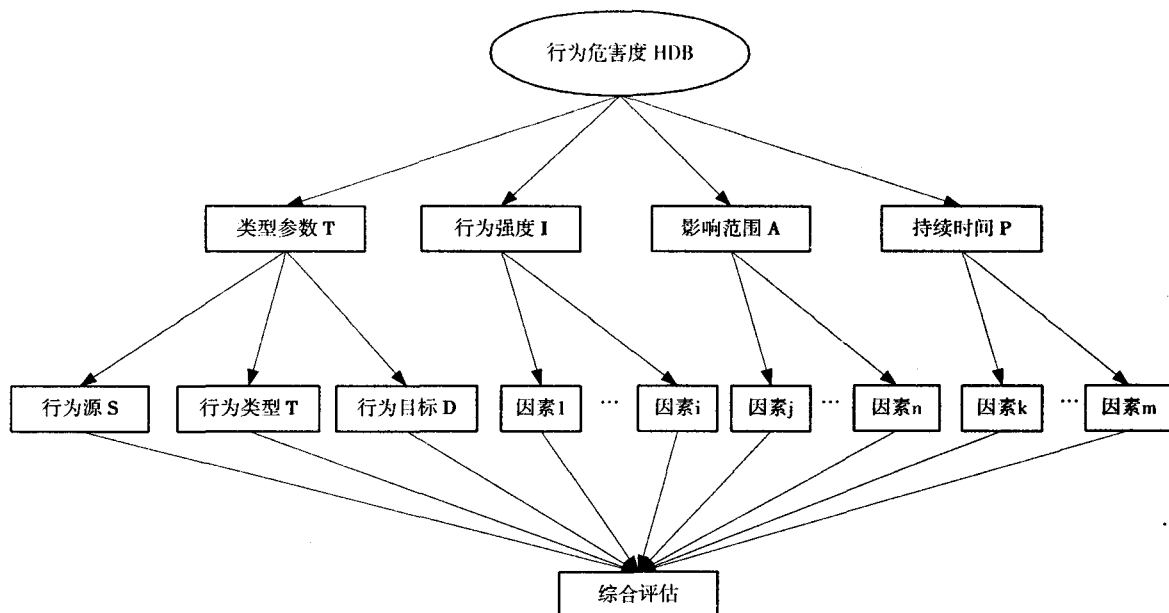


图1 网络行为危害度的评估模型

lev6}, 是进行评估的危害度等级划分。将 HDB 评估系统分为六个子系统 {T, I, A, P, S, D}, 分别评估行为类型、行为强度、影响范围、持续时间、行为源、行为目标六个因素关于评价指标的关联度。由于各要素的属性又由多个特征影响, 所以进行多级评估过程。由本校网络中心提出的危害控制策略取值, 根据可拓评价方法典域得:

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

利用可拓评价方法评估系统中各因素的节域:

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

下面对评价因素 T 进行分析:

对 T 取值可以有三种方式:

- 1) 根据经验赋值, 如本校网络中心用的行为管理模型中的应用;
- 2) 数学分析方法。利用概率分析、模拟函数分析;
- 3) 总结归纳法。如张怡博士在文献[2]中提到的不友好行为分类。文中加以改进从网络安全的三个主要特性来分析各种攻击中量化值, 如表 1 所示。

表 1 改进的行为类型

序号	行为源 S	行为目标 D	权限类型 T'
1	内网	个人终端	获取信息
2	外网	办公终端	修改信息
3		服务器	利用服务
4		路由器	拒绝服务
5			增加服务

对评价因素 D 进行具体分析: 同一种网络用户行为因行为目标的不同, 给整个网络正常运行造成的危害度有相当大的差别。取值区间域可以根据具体的系统取值, 如表 2 所示。

表 2 行为目标取值表

危害性	小	一般	中	较大	大
行为目标	个人终端	DNS 服务器	FTP 服务器	WEB 服务器	核心路由器
D	<0, 0.2>	<0.2, 0.4>	<0.4, 0.6>	<0.6, 0.8>	<0.8, 1>

下面对评价因素 I(Intensity)进行分析:

行为强度在文中不再使用与攻击频率一致的概念, 这主要是以频率计算, 如果时间段太长, 则取的是

平均值, 如果时间段太短, 又很难精确时刻, 所以选择检测行为产生的包数量来定义该行为的行为强度。由于网络有一定的载荷范围, 超过这个范围, 网络就无法提供服务甚至崩溃, 当达到这个阈值时, 更大的强度对其影响也就没什么特别大的区别。当某一时刻用户网络行为的强度即包的数量达到特定的临界值时, 将无法服务, 如图 2 所示。

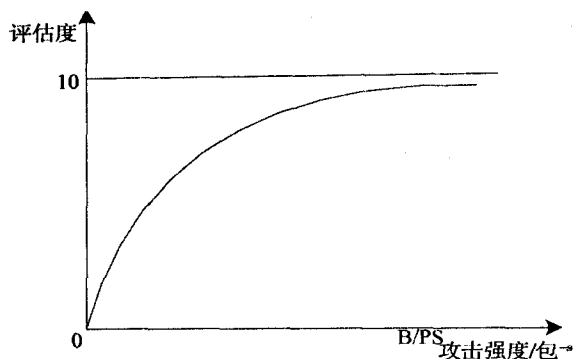


图 2 攻击强度模拟图

在以太网中, 数据包(包括头部)的大小范围是在一定字节之间。所以要知道网络对特定网络行为的承受能力, 需要对不同行为产生数据包的大小 S (Packet Size) 和带宽 (Bandwidth) 实时的计算, 即可得出系统中监控的端口带宽利用率 U_n 与变化率 T_n 等相关数据。

由于评估度在初期受攻击强度影响比较大, 当攻击强度达到 B_n/S_n 时评估度取值必定等于 10, 至于在 n 时刻某特定行为强度为 B_n/S_n , 则该行为在极点与零点连接直线取值为:

$$\frac{B_n/S_n}{I_n} = \frac{B/S}{10} \approx I_n = \frac{10 * B_n/S_n}{B/S}$$

B : 带宽 (Bandwidth)

S : 包大小 (Packet Size)

B_n/S_n : 表示 n 时刻占有带宽 B_n 与行为包大小的比值, 即该行为包的数量最大值, 即攻击强度。

I_n : 表示强度评估度

评估度 I 的取值区间为 $< 10 * (B_n/S_n) / (B/S), I_i >$, 在实际操作中, I_i 就表示最接近的区间域上限, 也可以操作变化率 T_n 等相关数据, 如 I 的取值区间为 $< 10 * U_n - T_n, 10 * U_n + T_n >$ 等。

下面对评价因素 A(Area)进行分析:

范围参数 A 是指用户本次网络行为在网络中影响的范围。因为有传播能力的危害度远不同于没有传播能力的危害度, 所以涉及到该网络行为的传播性(亦可以将其放入网络类型中一起讨论), 由于传播性很大程度上与行为类型有关系, 所以可以将历史记录 A_n 引入进来, 可以根据系统的记录进行相应的赋值(如与 T

值形成对应的映射等等)。也可以根据传播性的强弱来赋值或网络行为对易感区域设备影响赋值。表 3 为仅考虑传播性强弱评估的取值方法。其中 H_{total} 表示园区网内该易感区域设备数量, a 表示被行为影响的机器数量, 表中表示起初被传染的易感区域内的机器数量。

表 3 仅考虑传播性强弱评估的取值方法表

传播性	无传播性	弱传播性	强传播性
范围参数	常数 a	传染性低于 3	传染性高于 3
A	$<0, a/H_{total} * 10>$	$<a/H_{total} * 10, 3a/H_{total} * 10>$	$<3a/H_{total} * 10, 10>$

下面对评价因素 P(Persist) 进行分析:

持续时间参数是被考虑的动态评价因素之一, 本校网络中心将历史时间数据 P_h 与次数 C_h 实测数据 P_c 综合考虑, 考虑到实测数据正现实的影响网络, 所以在综合考虑中其占重大比率。根据前面提到的最大危害度考虑, 在系统实现中加入 P_{max} 用于对历史上该行为 P 的持续时间最大值的取得。所以当系统 P_c 小于 P_{max} 时 P_c 区间取值为 $<P_c, P_{max}>$, 当系统 P_c 不小于 P_{max} 时 P_c 区间取值为 $<P_{max}, P_c>$, 历史记录中的数据也可以根据最大危害度原则考虑。

实验中, 主要数据均取自本校校园网 5 组不同记录, 其中 Tcpdump 中, S 为数据中数据包目的地址类

型, D 为目标地址类型, S_n 为该行为包的大小, a 取自与该行为源或目的地址联系的主机数量。 B_n 数据取自 Netflow 中接入端口带宽利用大小, 使用其利用率和变化率, T' 则取自为包转发率和收发对称比率的区间值。 P_c 和 P_h 取自 Syslog 日志信息中的该行为持续时间和历史记录中的时间, H_{total} 为历史记录中影响机器最大值的数量。如表 4 所示, 检测到的各参数值, 利用上述分析方法取值为相应的区间域, 利用可拓评价方法综合评估得出的 HDB 的 Lev, 该数据体现了上述分析方法。

2 结束语

文中提出了一种基于动态区间距的网络行为危害度评估方法, 该方法将可拓学多层次、多因素对事物进行综合的多级评价应用到网络行为危害度评价中, 且将动态赋值与区间域相结合, 加大了赋值灵活性与加强了对参数不确定性的容忍程度, 并为参数给予了动态赋值的方法。使取值能够在参数不够精确的条件下依然得出较精确的结果, 网管系统可以综合分析各因素, 得出该用户的网络行为的危害度, 让网管系统自动执行相应的处理策略, 为实现高效自动化管理提供了依据。

表 4 网络行为危害度数据分析

参数 序号	T			I		A		P		HDB
	T'	S	D	B_n	S_n	a	H_{total}	P_c	P_h	LEV
冒充 IP	$<6, 8>$	$<0.4, 0.6>$	$<0.8, 1>$	68	93	78	890	63	396	4
冒充网关	$<9, 10>$	$<0.9, 1>$	$<0.1, 0.2>$	0.9	60	170	175	252	749	5
蠕虫	$<8, 10>$	$<0.9, 1>$	$<0.6, 0.8>$	27	62	27	50	111	179	6
ARP 攻击	$<7, 8>$	$<0.8, 1>$	$<0.3, 0.4>$	1.1	60	11	70	251	44	4
DCS	$<7, 8>$	$<0.5, 0.6>$	$<0.1, 0.2>$	1.7	1518	2	148	227	142	2

参考文献:

- [1] 张义荣, 鲜明, 王国玉. 一种基于网络熵的计算机网络攻击效果定量评估方法[J]. 通信学报, 2004, 25(11): 158-165.
- [2] 张怡. 一种新的网络攻击危害度定义方法[J]. 计算机工程, 2002, 28(8): 33-34.
- [3] 王磊, 于洪奎, 谢慧. 一种基于主机的攻击危害度定义方法[J]. 计算机工程与设计, 2005, 26(6): 1519-1521.
- [4] 彭凌西, 陈月峰, 刘才铭. 基于危险理论的网络风险评估模型[J]. 电子科技大学学报, 2007, 36(6): 1198-1201.
- [5] 李永新. 基于属性识别理论的网络威胁评估方法[J]. 计算机应用, 2009, 29(4): 956-958.
- [6] 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: 1797-1814.
- [7] Gupta A. Network Management: Current Trends and Future Perspective[J]. Journal of Network and Systems Management, 2006, 14(4): 483-491.
- [8] Bernstein L. Network Management Isn't Dying, It's Just Fading Away[J]. Journal of Network and Systems Management, 2007, 15(4): 419-424.
- [9] 肖敏. 基于可拓学的网络安全管理相关技术[D]. 武汉: 华中师范大学, 2008.
- [10] 甘妙金. 网络安全事件集中管理系统的设计与实现[D]. 长沙: 中南大学, 2008.
- [11] 程暄. 基于日志的网络入侵检测系统研究[D]. 长沙: 中南大学, 2007.
- [12] 梅震琨. 基于用户行为的园区网网络管理模型[D]. 长沙: 中南大学, 2009.