模糊综合评判在网络安全评价中的应用*

刘　洋

(军械工程学院,石家庄　050003)

摘要:当前网络安全面临的最大威胁主要是外部的各种网络攻击,因此,为了从定量的角度分析网络攻击所造成的危害,归纳了大部分攻击的特点,借鉴了多属性网络攻击分类的思路,提出了评估网络攻击效果的多项主要因素,并在此基础上应用模糊综合评判方法的现有成果对各项因素进行了量化和处理,其方法具有普遍性,分析结果有一定的参考性.

关键词:网络攻击;效果评估;模糊综合评判

中图分类号:TP393　　**文献标识码**:A　　**文章编号**:1006 - 0707(2009)08 - 0120 - 03

6 月 23 日,美国国防部长盖茨正式下令组建网络司令部,以统一协调保障美军网络安全和开展网络战等与电脑网络相关的军事行动. 而实际早在 2005 年 3 月,美国国防部公布的《国防战略报告》中就明确将网络空间与陆、海、空,以及太空定义为同等重要的、需要美国维持决定性优势的五大空间.

由于全球对网络依赖程度不断加深,故一旦重要网络资源遭到目的明确、组织严密的协同式网络攻击,国家金融、交通、通信、供电,以及军事等战略资源和战略目标必将遭受重大损失,国家的安全也将面临威胁,因此,若不能清楚地知道所面临的危险就不能有效地保证安全. 所以,如何保证己方网络的安全,客观有效地判断各种网络攻击所造成的危害,就成为了维护网络安全的一个重要方面,故在网络安全的研究中有必要对网络攻击进行综合评估.

1　评价指标的确定

对网络安全的最大威胁主要是外部的各种恶意攻击行为,其目的多种多样,手段日渐丰富,并且各种攻击方法的侧重点也不相同,因此,想要从定量的角度综合评估所遭受攻击的严重性,必须建立一个能够对绝大多数攻击手段进行描述且反映网络攻击多方面属性的指标体系. 为了对不同攻击手段的多属性进行量化描述,以反映该攻击手段的综合结果,借鉴了网络攻击多属性分类[1]的现有成果,并加以改进. 这种基于多个属性对网络攻击进行描述的方法在普适性(既可以满足大多数需求)、全面性(可以覆盖攻击的各个属性)、准确性(对各个属性进行定量描述)、可扩展性(可以适用于新型的攻击)等方面都具有较好的表现,如图 1 所示.

2　模糊综合评判的应用

模糊综合评判法是模糊数学理论的一个重要分支,它能应用模糊变换原理对其考虑的事物做出综合评价. 根据图 1 中对网络攻击综合效果评估的多属性分析,建立了下表 1. 从表中可见决定评估效果的各级因素和子因素及其权重,并在指标评估标准中对各项子因素做了说明.

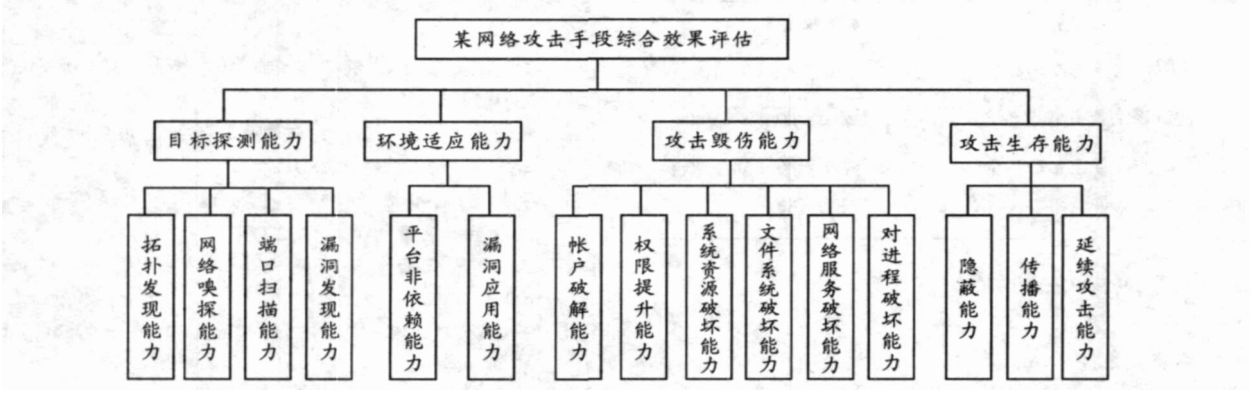

图 1　网络攻击效果综合评估指标体系结构

* **收稿日期**:2009 - 07 - 09

作者简介:刘洋(1980 —),男,内蒙古集宁人,硕士研究生,主要从事网络对抗研究.

表 1　因素集及其权重

因素	主因素及权重	子因素及权重	指标评估标准
某网络攻击手段综合效果评估	目标探测能力 $U_1(0.15)$	拓扑发现能力 $U_{11}(0.2)$	对目标拓补情况进行多方面了解,包括层次结构、*IP* 范围等.
		网络嗅探能力 $U_{12}(0.3)$	衡量发现有价值目标的能力,如能否截获邮件、文件等.
		端口扫描能力 $U_{13}(0.2)$	探测可以利用的端口.
		漏洞发现能力 $U_{14}(0.3)$	发现目标可能存在的各类漏洞,包括设计漏洞、实现漏洞、配置漏洞等.
	环境适应能力 $U_2(0.25)$	平台非依赖能力 $U_{21}(0.4)$	表示攻击手段不受目标平台的约束能力,针对任何目标都能够起作用的攻击,则非依赖能力为强,针对特定版本操作平台或应用平台的为弱,针对某一品牌或者某系列平台的为中.
		漏洞应用能力 $U_{22}(0.6)$	表示该攻击手段利用漏洞的能力.
	攻击毁伤能力 $U_3(0.35)$	帐户破解能力 $U_{31}(0.3)$	包括系统账户、用户账户等. 一般指攻击者对账户的猜测和字典攻击及强力破解等,以便达到其非法进入的目的,另外还包括安装木马后所创建的后门账户等.
		权限提升能力 $U_{32}(0.1)$	利用某种手段或者利用系统的弱点,获得本不应具有的权限,如植入木马、预留后门等.
		系统资源破坏能力 $U_{33}(0.2)$	指目标系统的硬件资源或者相对固定的信息,如系统的硬件资源的参数、系统的配置参数、文件访问的参数、软件信息等.
		文件系统破坏能力 $U_{34}(0.2)$	指被攻击系统的文件系统. 涉及的攻击主要是修改、删除、增加、获取文件等操作.
		网络服务破坏能力 $U_{35}(0.1)$	包括占用或利用网络资源与服务、影响网络性能和网络服务质量、增加网络流量、探测网络及相关服务的信息、利用网络提供的功能完成其它非法操作等,即对网络本身及服务的正常运行产生不利影响.
		对进程破坏能力 $U_{36}(0.1)$	指被攻击系统内存空间中运行的进程. 包括操作系统进程以及应用进程,涉及的攻击如杀死特定进程、探测进程活动、利用该进程对其他部分进行攻击等.
	攻击生存能力 $U_4(0.25)$	隐蔽能力 $U_{41}(0.4)$	表示攻击穿透防火墙、避开检测系统、杀毒软件的能力.
		传播能力 $U_{42}(0.4)$	以能够不依赖其他条件自动传播为强传播能力,以有条件激活有条件传播为弱.
		延续攻击能力 $U_{43}(0.2)$	表示非法利用攻击目标服务,继续攻击其他目标的能力,如使目标成为傀儡机、跳板机.

2.1　**基本概念建立**

1) 评语集:评语集是以评判者对被评价对象可能做出的各种总评判结果为元素组成的集合,通常用 V 表示,即

$$V=\{v_1, v_2, v_3, \cdots, v_n\}$$

式中,v_i 代表各种可能的总评判结果,共有 n 个.

2) 权重集:一般而言,各个因素的重要程度是不一样的,为了反映各因素的重要程度,各因素 u_i 应赋予相应的权重数 a_i. 由各权重数组成的集合称为因素的权重集 A

$$A=\{a_1, a_2, \cdots, a_m\}$$

同时,各权重数还应满足归一和非负的条件,即

$$\sum a_i = 1 \quad (i=1,2,\cdots,m \text{ 且 } a_i \geq 0)$$

3) 因素集:因素集是以影响评判对象的各种因素为元素组成的集合,用 U 表示,即

$$U=\{u_1, u_2, \cdots, u_m\}$$

式中,u_i 代表影响因素,共有 m 个影响因素.

4) 对于单因素评判矩阵 R,建立单因素模糊评判矩阵 $R(r_{ij})$

$$R=\begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \cdots & \cdots & & \cdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix}$$

判断矩阵有多种方法,例如德尔菲法、模糊统计法、三分法、二元排序法等[3],在此使用德尔菲法.

5) 考虑多因素下的权数分配,模糊综合评判决策模型为 $B = A \cdot R$. 由于需要让每个因素都对结果做出贡献,因此通过对模糊评判模型"主因素突出型"和"加权平均型"进行比较后[2],选用"加权平均型",即

$$B=\sum_{i=1}^{m} a_i r_{ij}$$

2.2 应用实例

假定己方网络遭到某种恶意攻击行为,则由专家对该攻击手段的各因素按照弱、较弱、一般、较强、强的等级进行判断,结果如表2所示.

表2 专家对子因素能力的判断结果

子因素	U_{11}	U_{12}	U_{13}	U_{14}	U_{21}	U_{22}	U_{31}	U_{32}	U_{33}	U_{34}	U_{35}	U_{36}	U_{41}	U_{42}	U_{43}
专家评定	一般	强	较弱	较强	弱	较强	弱	弱	强	较强	一般	一般	强	弱	较强

通过专家打分法的判断,并根据表3中隶属度的设定确定单因素评判矩阵.

表3 隶属度表

评分	隶属度向量[弱,较弱,一般,较强,强]
弱	[0.8,0.2,0,0,0]
较弱	[0.2,0.6,0.2,0,0]
一般	[0,0.2,0.6,0.2,0]
较强	[0,0,0.2,0.6,0.2]
强	[0,0,0,0.2,0.8]

在上述概念的基础上,结合网络攻击的评价因素指标,以目标侦察能力为例,$U_1=\{u_{11},u_{12},u_{13},u_{14}\}$,从表1可知,权重向量为 $A_1=[0.2,0.3,0.2,0.3]$,对目标侦察能力包括子因素的专家打分情况,可以得到其判断矩阵为

$$R_1=\begin{bmatrix}0 & 0.2 & 0.6 & 0.2 & 0\\ 0 & 0 & 0 & 0.2 & 0.8\\ 0.2 & 0.6 & 0.2 & 0 & 0\\ 0 & 0 & 0.2 & 0.6 & 0.2\end{bmatrix}$$

用"加权平均法"模糊评判模型计算

$$B_1=\sum_{i=1}^{m}a_i\cdot r_{ij}=\begin{bmatrix}0.2 & 0.3 & 0.2 & 0.3\end{bmatrix}\cdot\begin{bmatrix}0 & 0.2 & 0.6 & 0.2 & 0\\ 0 & 0 & 0 & 0.2 & 0.8\\ 0.2 & 0.6 & 0.2 & 0 & 0\\ 0 & 0 & 0.2 & 0.6 & 0.2\end{bmatrix}$$

可得到 $B_1=[0.04\quad 0.16\quad 0.22\quad 0.28\quad 0.3]$.依次类推,可以得出其它一级因素评估向量 B_2、B_3、B_4,对其归一化后可得矩阵

$$R=\begin{bmatrix}0.04 & 0.16 & 0.22 & 0.28 & 0.3\\ 0.32 & 0.08 & 0.12 & 0.36 & 0.12\\ 0.32 & 0.12 & 0.16 & 0.2 & 0.2\\ 0.36 & 0.2 & 0.04 & 0.08 & 0.32\end{bmatrix}$$

由表1可得一级因素的权重向量为 $A=[0.15,0.25,0.35,0.25]$,进一步通过模糊判断模型可得 $B=A\cdot R=[0.288,0.136,0.129,0.222,0.225]$.根据评语集中 v_i 的打分,即强对应1,较强对应0.8,一般对应0.6,较弱对应0.4,弱对应0.2,通过计算其总分为

$$0.288\times0.2+0.136\times0.4+0.129\times0.6+0.222\times0.8+0.225\times1=0.592$$

可见此种网络攻击方法总体效果一般.

3 结束语

为了在网络管理中及时有效地评估各种攻击手段对网络安全的危害,寻找一种时效性强、实现简单的评估方法已成为网络安全研究的当务之急.在已经出现的关于网络攻击评估的方法中,几乎全部是通过对己方网络重要技术指标(例如误码率、网络吞吐量、延迟时间、延时抖动、丢包率等)的数据收集作为依据的,这样的方法主要反映是外部攻击行为对己方网络的技术破坏情况,而不能体现全部恶意网络行为的动机,且算法复杂、条件繁复、耗时太长,在面临大范围的协同式网络攻击的情况下,缺乏时效性.

从保证网络安全的角度看,对网络攻击应进行综合评估,用以全面反映某种攻击手段多方面的有效性,本文中着眼网络安全中管理人员最关心的网络攻击的危害程度,应用模糊综合评判法对网络攻击进行评估研究,与实际需要和客观情况是相符合的.

参考文献:

[1] 鲜明,包卫东.网络攻击效果评估导论[M].长沙:国防科技大学出版社,2007.

[2] 韩立岩,汪培庄.应用模糊数学[M].北京:首都经济贸易大学出版社,1998.

[3] 杨正飞.网络攻击分类及网络攻击系统模型研究[D].兰州:兰州大学,2006.

[4] 高鲁,宋辉,刘明.信息化军事装备作战效能模糊综合评判及仿真分析[J].四川兵工学报,2006(2):17-19.

[5] 肖慧鑫,王静滨,焦利明.基于层次分析与模糊评判法的防空C^3I系统作战效能综合评估[J].兵工自动化,2006(6):13-15.