

网络终端安全评估量化指标体系的设计与实现

廖辉, 凌捷

(广东工业大学 计算机学院, 广东 广州 510090)

摘要: 探讨了网络终端安全评估方法与技术, 利用综合评估方法对网络终端安全进行评估, 分析影响网络终端安全的因素. 在网络终端安全评估量化指标体系的基础上, 给出了评估模型中资产价值、安全威胁值和脆弱性值的赋值方法, 并通过实例给出了网络终端安全的评估过程.

关键词: 网络终端安全; 量化指标体系; 脆弱性; 威胁; 层次模糊综合评价; 终端安全评估

中图分类号: TP393.08

文献标识码: A

文章编号: 1007-7162(2010)02-0084-05

随着信息技术的高速发展和网络应用的迅速普及, 网络已经深入社会各个领域, 网络与信息安全问题正面临着极大的威胁和挑战. 信息系统安全风险已经成为人们关注的焦点, 而对信息系统进行客观有效的安全评估是信息系统安全的前提和基础, 也是网络安全防御中的一项重要技术. 目前安全防护措施主要集中于网络入口处, 使来自网络外部的安全威胁大大减小. 而网络终端是重要数据和文件存放的源头, 绝大多数信息安全事件都是从终端发起的, 来自网络内部终端的安全威胁已成为普遍存在的问题^[1]. 事先对网络终端安全进行评估, 分析其存在的安全隐患尤为重要. 网络终端安全状况评估通过采集网络终端的安全现状信息, 分析系统目前与未来的风险, 评估这些风险可能带来的安全威胁与影响程度, 有针对性地提出抵御威胁的安全等级防护对策和整改措施, 从而减少损失^[2]. 网络终端安全状况评估是信息安全风险评估的重要内容, 对提高网络信息系统的安全防护能力, 保障重要网络信息系统的平稳运行有重要意义.

本文将在网络终端安全状况指标体系和评估模型的基础上, 对终端安全状况进行全面、客观的分析评估, 并通过实例给出网络终端安全评估量化指标的实现过程.

1 网络终端安全评估方法与技术概述

风险评估方法的选择影响到评估过程中的每个环节和评估结果. 信息安全风险评估的方法分为定性方法、定量方法、综合评估方法等. 在信息系统风

险评估过程中, 层次分析法 (Analytic Hierarchy Process, AHP) 经常被用到, 它是一种典型的综合评估方法, 是一种定性与定量相结合的多目标决策分析方法, 其优点是评估最底层各个元素在总目标中的风险程度^[3].

网络安全评估采用的评估技术主要是安全扫描技术和面向工具技术. 评估过程中使用风险评估工具作为评估的辅助手段, 简化评估的工作量, 提高评估所需的脆弱性、威胁关键信息的可信度. 对系统的脆弱性进行分析, 可以采用脆弱性扫描工具和渗透性测试工具; 通过采集检查列表、入侵检测系统等数据, 来帮助完成终端安全现状分析和趋势判断.

当前的几种网络安全评估模型各有特色也各有不足, 还没有形成统一的量化指标及算法, 研究者分别是不同角度描述信息系统安全状况, 无法完全表达影响信息系统安全的各关键点.

本文基于网络终端安全评估量化指标体系, 采用层次分析方法评估网络终端安全状况, 将评估过程中各个风险要素的赋值和计算, 根据需要分别采取定性和定量的方法完成, 在不容易获得准确数据的情况下采用定性分析方法分析, 在定性分析的基础上使用定量方法进行计算以减少其主观性^[4]; 从影响网络终端安全的各关键方面确定了评估模型及评估算法, 得出量化分析结果, 并依据评估结果为信息系统选择有针对性的安全措施, 规避、转移和降低风险, 妥善应对可能发生的风险, 并将风险控制在可接受的范围内.

收稿日期: 2009-06-04

基金项目: 广东省自然科学基金资助项目(9151009001000043); 广东省科技计划项目(2007B010200071)

作者简介: 廖辉(1982-), 女, 硕士研究生, 主要研究方向为网络与信息安全技术.

2 终端安全评估量化指标体系

随着电子政务的蓬勃发展,信息系统评估领域已经得到政府部门的高度重视,对信息安全评估的需求也越来越多,网络终端安全评估量化指标体系将应用于电子政务网络,在指标体系的基础上进行的终端安全评估满足了政府部门的信息安全评估需求. 信息安全是一个动态的复杂过程,它贯穿于信息系统的整个生命周期. 信息安全的威胁可能来自于内部破坏、外部攻击、内外联合进行的破坏以及自然灾害,因此信息安全评估必须按照风险管理的思想,对可能的威胁、脆弱性和需要保护的信息资产进行分析. 对网络终端安全进行评估时,以资产、威胁、脆弱性 3 个基本要素构建 4 级网络终端安全评估量化指标体系,以量化的指标多方面、多层次来描述终端的安全状况,得出客观的评估结果. 根据国家对网络与信息系统安全性的基本要求,在制定网络终端安全评估量化指标体系时应遵循以下原则:依据国际、国内信息安全评估规范;满足用户提出的安全性要求;反映终端安全的各方面;按层次划分各个指标^[5]. 如表 1 所示的 4 层结构的网络终端安全评估量化指标体系.

表 1 网络终端安全状况评估的 4 级指标体系 ^[6]			
第 1 层	第 2 层	第 3 层	第 4 层
信息资产	硬件	计算机设备	服务器、工作站、台式机…
		存储设备	硬盘、光盘
		移动存储设备	移动硬盘、U 盘
		传输线路	光纤、双绞线
	软件	系统软件	操作系统、开发系统
		应用软件	数据库软件、业务系统…
	数据	数据库数据、源代码…	
	文档	纸质文件、财务报告…	
威胁	环境威胁	物理威胁	自然灾害、电磁干扰、灰尘…
		技术故障	硬件故障、软件故障、存储介质失效
	人为威胁	管理缺陷	管理制度和策略不完善、职责不明确…
		人为错误	操作失误、维护错误
		故意行为	病毒、木马、蠕虫、未授权使用…
脆弱性	技术脆弱性	物理环境	机房供电、机房防静电…
		系统软件	操作系统安装补丁、用户账号口令策略…
		应用系统	密码保护、审计机制…
		技术管理	访问控制、业务连续性…
	管理脆弱性	组织管理	安全培训、人员安全

3 终端安全评估过程与实现

在文献[6]提出的网络终端安全评估量化指

标体系的基础上进行网络终端安全评估的主要过程有:

- (1) 收集资料:通过收集的有关数据和信息对网络终端系统有一个全面的认识. 数据的来源可通过问卷调查、辅助工具、文档资料来获得.
- (2) 采用漏洞扫描工具和入侵检测技术并利用收集到的有关指标的数据和资料,对网络终端存在的脆弱性和威胁进行识别和分析,得出安全事件发生的原因、影响因素和最终结果. 利用层次模糊评价法,量化网络终端脆弱性和威胁指标.
- (3) 结合网络终端安全评估模型计算出终端安全评估值,进行综合的定性分析,对终端安全状况、后果的严重性进行估计和评价.
- (4) 确定高风险区域,并制定出合理可行的网络终端安全解决方案.

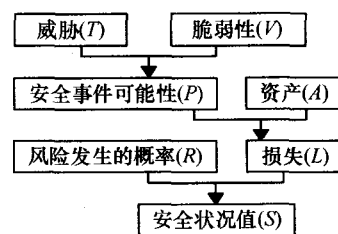
网络终端安全状况评估的最终目的是降低风险和保护资产. 资产的价值不是指以资产的经济价值来决定,更多的是指资产的影响价值决定. 脆弱性是资产本身存在的,威胁是对终端直接或间接的攻击,它可以利用脆弱性对资产造成损失. 在采取相应的安全策略控制安全风险时,信息资产的影响价值是一个重要的控制量,通过减少信息资产的潜在影响价值来降低安全风险,同时也可以通过降低威胁的方法、弥补系统漏洞的方法来降低安全风险.

网络终端安全状况评估主要是识别和分析资产价值、威胁及脆弱性. 信息资产综合其保密性 (confidentiality)、完整性 (integrity)、可用性 (availability) 3 个属性进行赋值. 根据资产在保密性、完整性、可用性要求的不同程度,将 3 个属性划分为 5 个等级,对不同的等级赋予不同的数值,级别越高数值越大. 资产的最终赋值 $Assets = f(C, I, A)$, 其中 f 是信息资产的 $C、I、A$ 映射到信息资产的函数, $Assets = Round(\sqrt[3]{C \times I \times A})$.

将资产划分为 5 个等级,级别越高数值越大,资产越重要. 网络终端安全评估根据资产的最终赋值来确定其是否为重要资产,主要是针对重要资产进行评估.

根据威胁 (T) 出现的频率对威胁进行赋值并划分为 5 个等级. 脆弱性 (V) 识别是针对每一项资产,识别可能被威胁利用的弱点,并对脆弱性的严重程度进行赋值. 可以利用漏洞扫描工具发现主机存在的漏洞. 对应不同环境下的相同弱点,其脆弱性的程度是不同的. 应从组织安全策略的角度确定脆弱性

的程度,同样对脆弱性划分为5个等级,对威胁和脆弱性的不同等级赋予不同的数值,级别越高数值越大,赋值范围为1~5之间的数.利用层次模糊综合评价法,计算威胁、脆弱性最终赋值.根据网络终端安全评估的3个基本要素,即资产、威胁、脆弱性的最终赋值,并结合网络终端安全状况评估模型,分析得出网络终端安全状况评估值,再进行综合的定性分析,主要评估算法和计算过程如下:安全事件可能性(P) = 威胁(T) + 脆弱性(V);损失程度(L) = 安全事件可能性(P) × 资产(A);终端安全状况值(S) = 终端安全事件的损失(L) × 风险发生的概率(R)^[6].终端安全状况评估模型如图1所示.终端安全状况由参数(T, V, A, R)决定,根据这4个参数值便可得到终端安全状况值.

图1 网络终端安全状况评估模型图^[6]

将网络终端安全状况值等级划分为5级,分别标识为“好”、“良好”、“中等”、“差”、“极差”.等级越高对终端及网络造成的影响也越大.根据评估结果的分布状况,给每个等级设定安全状况评估值范围并对评估结果进行相应的等级处理.表2是终端安全状况等级划分表,对终端安全状况的各个等级进行了具体的评估结果描述.

表2 终端安全状况等级划分^[6]

等级	安全状况评估值	标识	描述
5	51~100	极差	发生事件将造成重大的经济或社会影响,给终端及网络的正常运作造成严重影响
4	31~50	差	发生事件将造成较大的经济或社会影响,对终端的正常运作造成损害
3	21~30	中等	发生事件将造成一定的经济或社会的影响
2	11~20	良好	发生事件造成的影响低,可以用一定的安全措施解决
1	0~10	好	发生事件造成的影响几乎没有,可用简单的安全措施弥补

对网络终端安全评估量化指标体系的实现进行实验,实验环境为信息安全实验室内网.该实验室由8台微机组成,装有Windows2000/2003、Windows XP等不同操作系统及不同版本.网络环境内网是100M局域网,通过校园网接入互联网,评估其中一台未安装系统补丁和安全软件,并感染了病毒的终端机,采用漏洞扫描工具、渗透性测试工具及入侵检测系统分别获得了终端的漏洞和威胁数据,根据所获得的数据对脆弱性和威胁进行赋值^[6].通过收集的信息资产数据并采用风险评估定性的方法计算出信息资产的3个属性值,结合以上给出的资产公式计算出资产最终赋值为4,得知其属于重要资产.

利用层次模糊综合评价法计算得出威胁、脆弱性的最终赋值.层次模糊综合评价法是以模糊数学为基础、应用模糊关系合成原理、将一些边界不清、不易定量因素定量化并进行综合评价的一种方法.对通过入侵检测系统或漏洞扫描工具采集到的信息和威胁值、脆弱性值进行整理分析后,得到相应的模糊评价矩阵及权重系数集.设 $A = \{a_1, a_2, \dots, a_n\}$ 为指标权重系数集,且满足 $a_1 + a_2 + \dots + a_n = 1$.指标权重系数代表各因素的重要程度分配.模糊评价矩

阵中的值代表单因素被评定为相应等级的概率^[7].

根据表3,可得 T_{11} 的综合评价矩阵

$$M_{11} = (0.1 \quad 0.1 \quad 0.3 \quad 0.2 \quad 0.2 \quad 0.1) \times \begin{pmatrix} 0 & 0 & 0.1 & 0.3 & 0.6 \\ 0.1 & 0.1 & 0.1 & 0.2 & 0.5 \\ 0 & 0 & 0 & 0.5 & 0.5 \\ 0.1 & 0.1 & 0.1 & 0.2 & 0.5 \\ 0 & 0.1 & 0.1 & 0.3 & 0.5 \\ 0.1 & 0.1 & 0.1 & 0.2 & 0.5 \end{pmatrix} = (0.04 \quad 0.06 \quad 0.07 \quad 0.32 \quad 0.51).$$

同理可得其它指标的综合评价矩阵:

$$M_{12} = (0.2 \quad 0.4 \quad 0.4) \times \begin{pmatrix} 0 & 0.1 & 0.2 & 0.2 & 0.5 \\ 0 & 0 & 0.2 & 0.2 & 0.6 \\ 0 & 0.1 & 0.1 & 0.2 & 0.6 \end{pmatrix} = (0 \quad 0.06 \quad 0.16 \quad 0.20 \quad 0.58),$$

$$M_{21} = (0.3 \quad 0.2 \quad 0.3 \quad 0.2) \times \begin{pmatrix} 0 & 0.1 & 0.1 & 0.3 & 0.5 \\ 0 & 0.1 & 0.2 & 0.2 & 0.5 \\ 0 & 0.1 & 0.2 & 0.3 & 0.4 \\ 0 & 0.1 & 0.2 & 0.2 & 0.4 \end{pmatrix} =$$

$(0 \ 0.010 \ 0.17 \ 0.26 \ 0.45),$

$M_{22} = (0.6 \ 0.4) \times$

$\begin{pmatrix} 0 & 0 & 0.2 & 0.2 & 0.6 \\ 0 & 0.1 & 0.1 & 0.2 & 0.6 \end{pmatrix} =$

$(0 \ 0.04 \ 0.16 \ 0.20 \ 0.60),$

$M_{23} = (0.2 \ 0.1 \ 0.2 \ 0.2 \ 0.2 \ 0.1) \times$

$\begin{pmatrix} 0 & 0.1 & 0.1 & 0.2 & 0.6 \\ 0 & 0.1 & 0.2 & 0.3 & 0.4 \\ 0 & 0.1 & 0.1 & 0.2 & 0.6 \\ 0 & 0.1 & 0.1 & 0.3 & 0.5 \\ 0 & 0.1 & 0.1 & 0.2 & 0.6 \\ 0 & 0.1 & 0.2 & 0.3 & 0.4 \end{pmatrix} =$

$(0 \ 0.10 \ 0.12 \ 0.24 \ 0.54),$

$M_1 = (T_{11} \ T_{12}) \begin{pmatrix} M_{11} \\ M_{12} \end{pmatrix} =$

$(0.012 \ 0.060 \ 0.133 \ 0.236 \ 0.559),$

$M_2 = (T_{21} \ T_{22} \ T_{23}) \begin{pmatrix} M_{21} \\ M_{22} \\ M_{23} \end{pmatrix} =$

$(0 \ 0.082 \ 0.147 \ 0.234 \ 0.531).$

利用 M_1 、 M_2 构建 T_1 、 T_2 的综合评价矩阵:

$M = (T_1 \ T_2) \begin{pmatrix} M_1 \\ M_2 \end{pmatrix} =$

$(0.002 \ 0.077 \ 0.144 \ 0.234 \ 0.537).$

即得出网络终端安全评估指标体系中威胁因素的评估结果.按照加权平均法,可得威胁最终赋值 $T = 0.84$.加权平均法是以各评价等级的加权平均值作为评判结果,将各评价等级 $R = \{r_1, r_2, r_3, r_4, r_5\}$ 量化为 $R = \{1, 2, 3, 4, 5\}$, 设 $M = \{m_1, m_2, m_3, m_4, m_5\}$, 加权平均结果为: $r = \sum_{i=1}^5 m_i r_i / \sum_{i=1}^5 m_i, r = 4.2$, 评估结果表明网络终端的威胁水平介于“高”与“很高”之间,威胁、脆弱性最终赋值按其等级水平定义为 $0 \sim 0.2(1), 0.21 \sim 0.4(2), 0.41 \sim 0.6(3), 0.61 \sim 0.8(4), 0.81 \sim 1.0(5)$, 括号内为威胁、脆弱性的等级赋值,按相应比例计算得出威胁最终赋值 $T = 0.84$.同理,利用层次模糊评价法得出脆弱性的最终赋值为 $V = 0.75$.最后按照上述网络终端安全状况评估模型及其算法,得出安全事件发生的可能性 $P = 1.59$, 损失程度 $L = 6.36$.风险发生的概率 R 与终端存在的漏洞及已采取的控制措施有关, $R = 7$.终端安全状况值 $S = 44.52$.根据表2确定该网络终端安全状况为“差”.

表3 评估指标体系中威胁、权重分配及4级模糊评价矩阵

二级指标及其权重系数	三级指标及其权重系数	四级指标及其权重系数	四级模糊评价矩阵				
			很低	低	中等	高	很高
环境威胁 T_1 0.2	物理威胁 T_{11} 0.3	自然灾害 0.1	0	0	0.1	0.3	0.6
		电磁干扰 0.1	0.1	0.1	0.1	0.2	0.5
		灰尘 0.3	0	0	0	0.5	0.5
		静电 0.2	0.1	0.1	0.1	0.2	0.5
		断电 0.2	0	0.1	0.1	0.3	0.5
		温湿度 0.1	0.1	0.1	0.1	0.2	0.5
	技术故障 T_{12} 0.7	硬件故障 0.2	0	0.1	0.2	0.2	0.5
		软件故障 0.4	0	0	0.2	0.2	0.6
		存储介质失效 0.4	0	0.1	0.1	0.2	0.6
人为威胁 T_2 0.8	管理缺陷 T_{21} 0.3	管理制度和策略不完善 0.3	0	0.1	0.1	0.3	0.5
		职责不明确 0.2	0	0.1	0.2	0.2	0.5
		未对使用授权管理 0.3	0	0.1	0.2	0.3	0.4
		未对资源监控 0.2	0	0.1	0.2	0.2	0.4
	人为错误 T_{22} 0.3	操作失误 0.6	0	0	0.2	0.2	0.6
		维护错误 0.4	0	0.1	0.1	0.2	0.6
	故意行为 T_{23} 0.4	病毒 0.2	0	0.1	0.1	0.2	0.6
		木马 0.1	0	0.1	0.2	0.3	0.4
		蠕虫 0.2	0	0.1	0.1	0.2	0.6
		未授权使用 0.2	0	0.1	0.1	0.3	0.5
		对数据或软件篡改 0.2	0	0.1	0.1	0.2	0.6
		盗窃 0.1	0	0.1	0.2	0.3	0.4

为了进一步验证评估结果的客观性、可信性,在此终端机上更新系统补丁、安装安全软件和查杀了病毒后再进行评估,计算得出威胁最终赋值为 $T = 0.32$,脆弱性的最终赋值为 $V = 0.26$,安全事件发生的可能性 $P = 0.58$,由于资产值为4,损失程度 $L = 2.32$. 风险发生的概率 $R = 6$. 终端安全状况值 $S = 13.92$,确定该终端的安全状况为“良好”. 通过在不同的实验环境设置下多次对网络终端安全进行评估,得出的评估结果均是一致的,说明在网络终端安全评估量化指标体系基础上进行的终端安全评估过程及算法是有效的.

4 结束语

网络终端安全状况评估固有的主观因素对评估结果有很大的影响,为了尽可能减小这些主观因素,本文在网络终端安全评估量化指标体系的基础上确定了评估过程中参照的指标,全面、准确地反映网络终端安全状况,并对各项指标进行量化,采用评估模

型和结合实例给出了评估量化指标的具体实现过程,形成一个全局的更合理、更准确的网络终端安全状况量化分析结果.

参考文献:

- [1] 王义申. 终端安全管理系统在企事业单位内网应用的分析[J]. 计算机安全, 2007(7): 63-65.
- [2] 吴来非, 李新友, 禄凯. 信息安全风险评估[M]. 北京: 清华大学出版社, 2007: 4-9.
- [3] 冯登国, 张阳, 张玉清. 信息安全风险评估综述[J]. 通信学报, 2004, 25(7): 9-14.
- [4] 杨晓明, 罗衡峰, 范成瑜, 等. 信息系统安全风险评估技术分析[J]. 计算机应用, 2008, 28(8): 1920-1923.
- [5] 程学东. 电信网网络安全评估指标体系研究[J]. 现代电信科学技术, 2005(8): 10-13.
- [6] 廖辉, 凌捷. 网络终端安全状况评估指标体系的研究[J]. 计算机工程与设计, 2010, 31(10): 961-964.
- [7] 朱岩, 杨永田, 张玉清, 等. 基于层次结构的信息安全评估模型研究[J]. 计算机工程与应用, 2004(6): 40-43.

Design and Implementation of Network Terminal Security Assessment Index System

Liao Hui, Ling Jie

(Faculty of Computer, Guangdong University of Technology, Guangzhou 510090, China)

Abstract: Network terminal security assessment techniques and methods are introduced. Synthesis evaluation technique is used to evaluate network terminal security. The various kinds of factors that threaten network terminal security are analyzed. Based on the quantitative index system, the method of determining the value of the assets, security threat and vulnerability in the evaluation model is given. The process of network terminal security assessment is presented with examples.

Key words: network terminal security; quantitative index system; vulnerability; threat; multilevel fuzzy comprehensive judgment; terminal security assessment