

信息安全风险评估模型的定性与定量对比研究

孙 强

(牡丹江师范学院 计算机科学与技术系, 黑龙江 牡丹 157012)

摘 要: 对信息安全风险评估的通用计算模型和定性计算模型进行了深入的分析, 提出了一种定量的信息安全风险评估模型. 该方法使信息安全风险评估过程中风险值的计算更加科学和准确, 解决了以往定性分析方法数据计算粗略、不准确和难于区分风险的重要程度等问题.

关键词: 信息安全; 风险评估; 定性分析; 定量分析

中图分类号: TP309

文献标识码: A

文章编号: 1000-7180(2010)06-0092-05

Contrastive Research on Qualitative and Quantitative Information Security Risk Assessment Models

SUN Qiang

(Department of Computer Science and Technology, Mudanjiang Teachers College, Mudanjiang 157012, China)

Abstract: Deep analysis and research has been made on general computer module and qualitative module of information security risk assessment. Based on the comparison of characters for qualitative and quantitative risk assessment models, a new quantitative method for information security risk assessment is proposed. This method makes it more scientific and accurate to calculate the risk in the process of assessing information security risk, thereby, solving the preexisting problems in quantitative analysis, such as rough calculation, inaccuracy and the difficulty in distinguishing the importance of risk.

Key words: information security; risk assessment; qualitative analysis; quantitative analysis

1 引言

随着各类组织信息化程度的提高和业务运作过程中大量数据的生成, 信息系统越来越复杂, 组织的发展对信息的依赖程度也越来越大, 这样信息安全管理成了组织风险管理的重要组成部分. 如何保障信息的安全是每个组织所面临的共同问题, 因此信息安全风险评估逐渐被引入组织的管理体系当中. 信息安全风险评估是信息安全保障体系建立过程中重要的评价方法和决策机制. 文献[1]中综述了信息安全风险评估所涉及的主要内容, 探讨了国内

外测评体系, 指出了需要解决的问题. 文献[2]中提出了基于效用的安全风险度量模型, 引入风险函数和相对损失效用度量风险. 文献[3]中引入信息熵风险分析算法, 采用定性分析与定量计算相结合, 构建一种信息系统风险分析模型. 文献[4]中借鉴人类免疫系统的研究成果, 建立了一个基于免疫规则的网络自适应系统模型.

各种风险评估方法使用范围各有不同, 风险评估方法总的来说可以分为定性分析、半定量分析和定量分析. 文中在详细分析定性风险评估模型的基础上, 对定性和定量风险评估模型的特点进行分析

收稿日期: 2009-05-11; 修回日期: 2009-07-11

基金项目: 黑龙江省教育厅科学技术研究面上项目(11551512, 11551513); 牡丹江师范学院博士科研启动基金项目(MSB200901); 牡丹江师范学院青年专项基金创新项目(QC200901); 牡丹江师范学院青年专项基金创新项目(QC200901); 牡丹江师范学院教学改革工程项目(10-XY01056)

比较,并提出了一种定量的信息安全风险评估模型。

2 信息安全风险评估相关理论

信息安全风险评估是按照国际和国内有关技术标准对信息及信息处理设施的威胁、影响、脆弱性及三者发生可能性的评估。风险是特定威胁利用资产的一种或一组漏洞,导致资产丢失或损害的潜在可能性,即特定威胁事件发生的可能性与后果的结合。风险的构成包括五个方面:起源、方式、途径、受体和后果。它们相互关系可表述为:风险的一个或多个起源,采用一种或多种方式,通过一种或多种途径,侵害一个或多个受体,造成不良后果。相关定义如下:

- (1) 风险的起源是威胁的发起方,叫做威胁源;
- (2) 风险的方式是威胁源实施威胁所采取的手段,称为威胁行为;
- (3) 风险途径是威胁源实施威胁所利用的薄弱环节,称为脆弱性或漏洞;
- (4) 风险的受体是威胁的承受方,即资产;
- (5) 后果是威胁源实施威胁造成的损失,即影响。

在风险理论中,资产代表着一种资源、程序、产品、计算模式,以及认为必须需要保护的东西总称。资产是风险存在的根源,是风险的受体。资产的流失会无形中影响信息安全的机密性、完整性和可用性^[5]。威胁是指某个特定威胁源利用某个特定的脆弱性对系统造成损失的潜在能力。威胁源即风险的起源,是威胁的发起方。威胁行为是形成风险的方式,不同的威胁源有各自的威胁行为。漏洞是指系统设计、实施、操作和控制过程中存在的可被威胁源利用造成系统安全危害的缺陷或弱点^[5]。漏洞往往需要与对应的威胁相结合,才会对系统的安全造成危害。

风险分析方法可以采取定性分析和定量分析。定性分析采用文字形式或描述性的数值范围来描述潜在风险的大小程度,以及这些风险发生的可能性^[1,5]。定性风险分析方法依据组织面临的威胁、脆弱点以及控制措施等元素来决定安全风险等级。定性方法较为粗糙,但在数据资料不够充分或分析者数学基础较为薄弱时比较适用,但它的主观性很强,对评估者本身的要求很高。定量分析在影响或可能性等值的分析中采用数值,而不是定性或半定量分析中所使用的叙述性数值范围。定量分析的品质取决于所用的数据精确性和完整性。定量分析方法的采用,可以使研究结果更科学、更严密、更深刻。

3 通用的风险评估计算模型

3.1 基于 ALE 的风险评估计算模型

1979 年美国国家标准局出版了一个联邦信息处理标准的文件,该文件为大型的数据处理中心设定了风险评估标准,并且提出了一个新的衡量计算机相关风险的制度:ALE。ALE 仅仅是将风险计算为多个潜在损失和发生频率的乘积之和,如式(1)所示:

$$ALE = \sum_{i=1}^n I(O_i) F_i \quad (1)$$

式中, $\{O_1, \dots, O_n\}$ 表示一组有害的后果, $I(O_i)$ 表示后果 i 在金钱上造成的影响, F_i 表示后果 i 发生的频繁程度。

ALE 风险分析法是一种效益价格比分析法,在求得每一个“威胁—脆弱性—资产”三联组合的 ALE 之后,再计算控制措施的价值。它将采取控制措施前后的 ALE 之差再减去控制措施开销,得出控制措施价值,如果价值较大,则采取该控制措施,否则放弃。ALE 方法将所有的风险合成为单一的数字,该方法的最大缺点是不能将高频率、低影响的事件和低频率、高影响的事件区分开来。在很多情况下,高频率、低影响的事件不会造成太大损失,是可以容忍的,但是低频率、高影响的事件却是很严重的、灾难性的。

3.2 基于风险要素的风险评估计算模型

基于风险要素的风险计算模型是以 ISO13335 中的核心安全风险模型为基础进行系统建模的。安全风险模型各要素的相互关系如图 1 所示,其中资产、漏洞、威胁和风险是模型的四大要素,它们的关系是,威胁利用资产的漏洞,使资产存在风险,可能造成资产价值的损失;同时可以针对资产存在的风险,提出防护需求,采取防护措施排除漏洞,从而降低资产的风险和减小价值的损失^[6]。

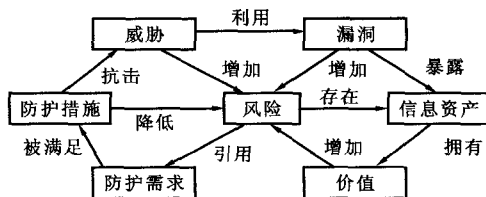


图1 安全风险模型各种要素的相互关系

不论采用定量还是定性的分析方法,都必须识别出以上各点内容才能正确地评价信息安全风险。威胁所对应的某一风险与信息及其相关资产的脆弱性、威胁、威胁发生的可能性、威胁发生所造成的后

果有关,因此风险的计算应为式(2)所示^[6].

$$R = f(V, T, T_P, I) \tag{2}$$

式中, R 表示风险, V 表示脆弱性, T 表示威胁, T_P 表示威胁发生的可能性, I 表示威胁发生的后果.

实际上, T_P 、 I 和 V 、 T 都有关系,因此只需考虑 T_P 和 I 即可.也就是说风险和威胁发生的可能性和一旦威胁发生以后对系统造成的影响存在直接关系.因此评估风险就是要评估威胁发生的后果和可能性,而脆弱性、威胁等只是评估的基础,作为风险评估计算模型的数据来源,是作为后果和可能性的参考.因此实际风险计算应为式(3) 所示.

$$R = f(T_P, I) \tag{3}$$

T_P 与脆弱性、威胁有关,具体的计算或定义依赖于实际系统和经验, T_P 还与采用的控制措施有关系,适当的控制措施可以降低 T_P 值或等级,如式(4).

$$T_P = f(V, T, C_t) \tag{4}$$

式中, V 表示脆弱性, T 表示威胁, C_t 表示控制措施.

而威胁发生的后果与脆弱性、威胁以及信息的机密性、完整性、可用性的破坏程度有关,具体的后果赋值或定义依赖于实际的系统和经验.同样, I 还与采用的控制措施有关系,有效的控制措施可以减少或降低 I 值和等级,如式(5).

$$I = f(V, T, C_x, I_x, A_x) \tag{5}$$

式中, C_x 表示机密性遭到破坏的程度及造成的后果, I_x 表示完整性遭到破坏的程度及造成的后果, A_x 表示可用性遭到破坏的程度及造成的后果.

4 定性的信息安全风险评估计算模型

4.1 风险等级矩阵及描述

信息系统的风险是由下面两个方面决定的:

- (1) 威胁源在现有控制措施下利用系统脆弱性;
- (2) 系统被攻击后产生的危害程度.

而威胁发生的可能性则与威胁源的能力和动机、信息系统的脆弱性和系统已实施的控制措施有关.信息系统风险的计算应该通过风险等级矩阵.表 1 是一个标准的风险等级矩阵结构,信息系统的风险由风险发生的可能性等级和危害等级相乘得出.表 1 是一个 3×3 的矩阵,根据组织的复杂程度,还可采用 4×4 或 5×5 的矩阵.矩阵越大,风险等级就越精细.根据计算得出的风险等级数值,表示风险的

危害程度.

表 1 风险等级矩阵

威胁	危害程度		
	高(100)	中(50)	低(10)
高(1.0)	100	50	10
中(0.5)	50	25	5
低(0.1)	10	5	1

可将风险等级矩阵的数值按照组织的具体情况定性地分成几个风险等级,以得到直观的风险状况.如表 2 所示,管理者可以根据等级范围来制定相应策略.

表 2 风险等级范围及相应对策

风险等级	描述及相应对策
高	如果信息系统的安全被评估为高风险,必须尽快地采取正确的行动方案.
中	如果信息系统的安全被评估为中风险,应制定正确的行动方案,并在确定时间内进行修补.
低	如果信息系统的安全被评估为低风险,系统负责人应确定是行动进行修补还是接受此风险.

4.2 定量的信息安全风险评估过程

定量的信息安全风险评估的操作步骤如下:

- (1)威胁源动机级别与威胁行为能力级别组合,产生威胁级别,表示威胁自身的潜力,如表 3 所示.

表 3 威胁源动机级别与威胁行为能力级别组合

威胁级别		威胁源动机级别		
		1(低)	2(中)	3(高)
威胁行为能力级别	1(低)	1	2	3
	2(中)	2	3	4
	3(高)	3	4	5

- (2)威胁级别与脆弱性利用级别组合,产生威胁/脆弱性对级别,表示威胁利用脆弱性的潜力,如表 4 所示.

表 4 威胁级别与脆弱性利用级别组合

威胁/脆弱性对级别		威胁级别				
		1	2	3	4	5
脆弱性被利用的级别	1	1	2	3	4	5
	2	2	3	4	5	6
	3	3	4	5	6	7

- (3)资产价值级别与影响程度级别组合,产生资产/影响对级别,表示资产的重要程度,如表 5 所示.

表 5 资产价值级别与影响程度级别组合

资产/影响对级别		资产价值级别		
		1(低)	2(中)	3(高)
影响程度级别	1(低)	1	2	3
	2(中)	2	3	4
	3(高)	3	4	5

(4) 威胁/脆弱性对级别与资产/影响对级别组合,产生风险级别,如表 6 所示。

由表 6 最终可以得出 11 级的风险评估结果。上述的单项评估采用的是“高、中、低”三级,也可根据实际需要采用四级或五级。单项评估的级别增加了,综合评估计算结果的级别也会随之增加。给定可接受的最高风险级别,通过风险评估计算,一方面可以判断当前的风险状态是否可接受,另一方面可以评判采用的风险控制手段是否适度。

表 6 威胁/脆弱性对级别与资产/影响对级别组合

风险级别		威胁/脆弱性对级别						
		1	2	3	4	5	6	7
资产/影响对级别	1	1	2	3	4	5	6	7
	2	2	3	4	5	6	7	8
	3	3	4	5	6	7	8	9
	4	4	5	6	7	8	9	10
	5	5	6	7	8	9	10	11

5 定量的风险评估计算模型

5.1 基本要素

模型基本要素为:资产价值、威胁、漏洞、风险。资产价值是指在评估范围内的资产的自身价值和资产在系统内重要性的统一值。威胁是指信息资产的安全可能受到的侵害,因为目前不可能实现事件和漏洞的精确对应,所以采用威胁来关联攻击行为(事件)和漏洞,定量的风险评估计算模型知识库自身定义的威胁由服务人员根据事件类和漏洞来建立^[7]。漏洞本身是无害的,是被威胁利用来影响资产的一个必要条件,定量的风险评估计算模型知识库自身定义了具体漏洞。风险是指某个时间范围内企业的安全状况。风险是在考虑事件发生的可能性及其可能造成的影响下,漏洞被威胁所利用后在资产上所产生的实际负面影响。风险是威胁可能性和威胁影响性的函数,前者指威胁源利用一个潜在漏洞的可能性,后者指不利事件对组织机构产生的影响,风险的后果同时也依赖于资产的价值。

5.2 定量计算公式

资产价值不仅仅为自身的价值,而是它在信息

系统中的价值,与资产的机密性、完整性和可用性有关。具体计算公式为

$$A_R = \log_2 \frac{2^C + 2^I + 2^A}{3}$$
 (6)

式中, A_R 表示资产的价值, C 表示资产的机密性值, I 表示资产的完整性值, A 表示资产的可用性值。

漏洞值 V 是漏洞的一个属性,具体参见定量的风险评估计算方法知识库中的安全漏洞库。威胁影响值分为影响初始值和影响资产值。影响初始值 T_L 是根据统计和经验判断某个威胁可能造成的影响的大小,固化在系统知识库中。

影响资产值指威胁发生后对特定属性(C 、 I 、 A)造成的影响,由三个权重(C 权重、 I 权重、 A 权重)构成影响资产权重数组,此数组中 CIA 权重分别与资产的 CIA 值相乘后求和除以 3,再开平方根得到影响资产值。威胁影响值则可以分为威胁初始影响值和威胁影响资产值两部分,可以由式(7)计算出来。

$$T_S = \frac{T_L + T_A}{2}$$
 (7)

式中, T_S 表示威胁对资产或系统的影响性, T_L 表示威胁初始影响值, T_A 表示威胁影响资产值,计算公式为

$$T_A = \sqrt{\frac{T_{CA} \times C + T_{IA} \times I + T_{AA} \times A}{3}}$$
 (8)

式中, T_{CA} 表示威胁对资产机密性的权重, T_{IA} 表示威胁对资产完整性的权重, T_{AA} 表示威胁对资产可用性的权重, C 表示资产的机密性值, I 表示资产的完整性值, A 表示资产的可用性值。

威胁可能性 T_P 的判断可以确定某安全对象(资产)是否面临某个威胁以及该威胁发生可能性大小。威胁可能性的计算包括三个参数:固定经验值、发生条件值和发生次数值。威胁的固定经验值是国际组织长期统计的结果,固化在系统知识库中。发生条件值由具体应用环境确定,在固定经验值基础上调整。

最后根据威胁、漏洞、资产都会增加风险值的原理,得到风险值计算公式。首先通过式(9)计算出风险中漏洞所能利用威胁的数值

$$T = \sqrt{T_P \times T_S}$$
 (9)

式中, T 表示风险中漏洞所能利用威胁的数值, T_P 表示风险中漏洞所能利用威胁产生的可能性, T_S 表示风险中漏洞所能利用威胁产生的严重程度,也就是影响值。再利用资产价值、漏洞值和风险中漏洞所能利用威胁的数值,使用式(10)计算出最终的风险值。

$$R_R = A_R \times V \times T \quad (10)$$

式中, R_R 表示该风险的风险值, A_R 表示资产的价值, T 表示风险中漏洞所能利用威胁的数值, V 表示风险中脆弱性的数值, 也就是漏洞值。

根据定量的风险评估方法的计算, 得出每个风险的具体数值, 可以根据这个风险值对风险进行等级划分。参考国家标准, 定义严重程度 4 级, 如表 7 所示。

6 结束语

文中对信息安全和安全风险的发展背景和

表 7 风险严重程度及其描述

风险严重程度	风险值的范围	描述及相应对策
告知	[0, 25]	正常网络状态, 没有显著的网络攻击事件, 只存在零星攻击。此时保持普通安全策略。
预警	[25, 70]	有一些严重漏洞发布或网络攻击事件增多。需对网络和主机进行安全评估、升级以及必要的监控。
报警	[70, 100]	某些严重漏洞或威胁正被攻击者利用, 网络攻击事件显著增加。此时需要立刻采取防御措施。
紧急	[100, 125]	网络安全态势非常严峻, 对全球互联网造成严重影响。此时需要与其他网络协作采取防御措施。

风险理论相关的概念和方法作了详细介绍。通过对

信息安全风险评估的通用计算模型和定性风险计算模型进行了深入的学习和研究, 总结它们的缺点和不足, 在此基础上提出了一种定量的风险评估计算模型, 解决了以往定性风险评估计算模型的缺点, 提高了风险值的准确性和精度。

参考文献:

- [1] 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): 10-18.
- [2] 彭俊好, 徐国爱, 杨义先, 等. 基于效用的安全风险度量模型[J]. 北京邮电大学学报, 2006, 29(2): 59-61.
- [3] 汤永利, 徐国爱, 钮心忻, 等. 基于信息熵的信息安全风险分析模[J]. 北京邮电大学学报, 2008, 31(2): 50-53.
- [4] 于璐, 吴振强. 基于免疫的自适应安全模型[J]. 微电子学与计算机, 2009, 26(1): 113-117.
- [5] 高寅生. 安全漏洞库设计与实现[J]. 微电子学与计算机, 2007, 24(3): 99-101.
- [6] ISO/IEC TR13335-1 Guide - lines for the management of IT security, part1: concepts and models for IT security [EB/OL]. [2004-11-19]. <http://www.din.de/ni/sc27>.
- [7] 孙强, 郭江鸿, 王慧. 基于消息通信的安全管理系统的设计与实现[J]. 计算机工程与应用, 2006, 30(10): 134-139.

作者简介:

孙强 男, 博士, CCF 会员. 研究方向为信息安全和电子设计自动化等。

(上接第 91 页)

参考文献:

- [1] James T Kajiya, Brian P von Herzen. Ray tracing volume densities[J]. Computer Graphics, 1984, 18(3): 165-174.
- [2] Jos Stam. Stable fluids[C]//Proceedings of SIGGRAPH. Los Angeles: ACM Press, 1999: 121-128.
- [3] Andrew Selle, Nick Pasmussen, Ronald Fedkiw. A vortex particle method for Smoke, water and explosions[J]. ACM Siggraph, 2005, 24(3): 910-914.
- [4] Bryan M Klingner, Bryan E Feldman, Nuttapong Chentanez, et al. Fluid animation with dynamic meshes[C]//In ACM SIGGRAPH. Boston, ACM Press, 2006: 820-825.
- [5] 柳有权, 刘学慧, 吴恩华. 基于 GPU 带有复杂边界的

三维实时流体模拟[J]. 软件学报, 2006, 17(3): 568-576.

- [6] 刘伟峰, 王智广. 细粒度并行计算编程模型研究[J]. 微电子学与计算机, 2008, 25(10): 103-106.
- [7] MacComack R W, Baldwin B s. A numerical method for solving the navier - stokes equations with application to shock boundary interactions[R]. AIAA-75-1, 1975.
- [8] Chorin A J, Marsden J E. A mathematical introduction to fluid mechanics[M]. 3rd ed. Berlin: Springer, 1993.

作者简介:

陈阁 男(1981-), 硕士研究生. 研究方向为虚拟现实。
何伟 女, (1983-), 硕士研究生. 研究方向为虚拟现实。
李云飞 男, (1958-), 教授. 研究方向为虚拟仪器 & 虚拟现实。