基于威胁树的系统安全评价模型研究*)

杨 武[1] 王晓云[2] 李 波[1]

(重庆工学院计算机学院 重庆400050)[1] (涪陵师范学院 重庆408000)[2]

摘 要 本文提出一种针对系统威胁进行量化的分析方法,并建立了模型,该方法提供了一种类似系统的安全性评估、比较的途径。当然,当本分析方法应用于不同类型的系统时,需要对其部分参数进行初始化和修证。

关键词 威胁树,信息安全,评价因子

The Study about Evaluation Model for System Security Based on Attack Tree Analysis

YANG Wu[1] WANG Xiao-Yun[2] LI Bo[1]

(Department of Computer Science, Chongqing Institute of Technology Chongqing400050)[1]

(Fuling Normal university, Chongqing 408000)[2]

Abstract In this paper, information system attack tree model has be build based on analyses of attack pattern which system be likely to meet with and decompose security threaten to system according to application object of system. Finally security evaluation factor to information system has been put forward based on the model.

Keywords Attack tree, Information security, Evaluation factor

1 引言

信息安全是一个多元化的概念,它在不同的领域有不同的侧重点。例如,在企业,其安全性主要是体现在数据的一致性与完整性;在电子政务领域,是信息的完整性。因此,在评价信息系统的安全时,应与系统的应用紧密相关。即定义一套与安全相关,并且与应用相适应的属性。本文试图从信息系统本身的技术和管理方面,分析技术和管理环节可能存在的安全威胁和已经存在的脆弱性,建立系统安全树状模型,并根据该模型给出评价指标。

2 信息系统威胁树模型

2.1 威胁树定义与结构描述

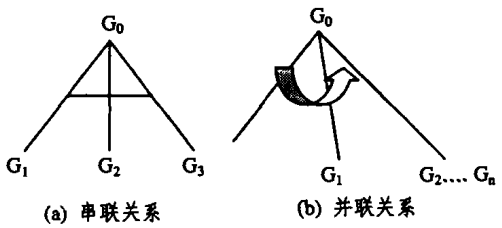
威胁树对信息系统而言,是一个威胁集,该集合中的任何一个威胁都可能是系统的隐患,从而影响系统功能或任务的实现。对威胁的描述是基于系统的攻击模式,即从外部入侵的可能性、途径。我们选择机密性、完整性、可用性作为三个结点,从根结点逐层向下分解。上层结点分别由下层结点构成,下层结点所代表的威胁分别可以触发上层的威胁。即:$T=\{G,E,Q\}$,其中,G 代表结点,E 代表结点间的通路,Q 代表影响系统功能的一个子树通路。对系统而言,由于攻击途径所造成的安全威胁分别由不同层次,不同关系构成,因此,安全威胁树内部结点的关系有如下两种:串联关系:对攻击而言,必须完成每一个步骤,可以达到目标,如图1(a)所示。记为:

$\langle G_1,G_2,G_3,\cdots\cdots\rangle \rightarrow Goal\ G_0$

并联关系:对攻击而言,攻破其中任何一个环节,即可达到目标,如图1(b)。记为:

$\{G_1,G_2,G_3,\cdots\cdots\} \rightarrow Goal\ G_0$

例如,对机密性而言,线路窃听和非法访问到可造成信息泄露,二者关系为并联(即"或");而对利用 OS 的漏洞窃取文件而言,必须经过漏洞扫描、获取漏洞、利用漏洞进入系统等三个步骤才能进入实现,三者关系为串联关系(即"与")。



(a)串联关系 (b)关联关系

图1 威胁树结点关系图

2.2 分解方法与实例

对一个系统而言,可根据实际应用、系统结构、管理策略等方面进行安全威胁的分析,构造相应的信息流程模型;然后以该流程为出发点,分析系统中可能存在的针对系统"三性"的潜在的威胁,以及上层威胁图可能面临的攻击模式进行分解。其基本方法如下:

(1) 定义一套有关安全的目标作为系统的分析主题,如机密性、可用性、完整性。

(2) 从攻击模式确定上述主题的威胁,进行分解,逐步形成中间层结点。例如,自顶向下的攻击模式分析。

(3) 检查子结点以确定是不是还需要进一步分解,如果需要的话,将子结点作为当前目标,重复分解步骤,将其分解为更小的功能模块。

(4) 当页结点不能再被分解时,终止分解过程。此时,所有的页结点应该都是相互独立的,而且是可以被评估的组件。

以机密性为例,可能的一个威胁子树(G_{Tc})如图2所示。

图2中,$G_i(U_j(V_k(X_m(y_0(Z_n\cdots)))))$表示某个结点。如果没有下层分支,称为叶子结点,括号内层次较少,如 $G_i(U_j)$、$G_2(U_1)$、$G_2(U_2)$;如果存在的分支较多,则层次也较多。

*)项目资助:教育部科技重点项目,编号:03315。杨 武 副教授,博士研究生,主要研究方向:分布式处理,计算机网络。

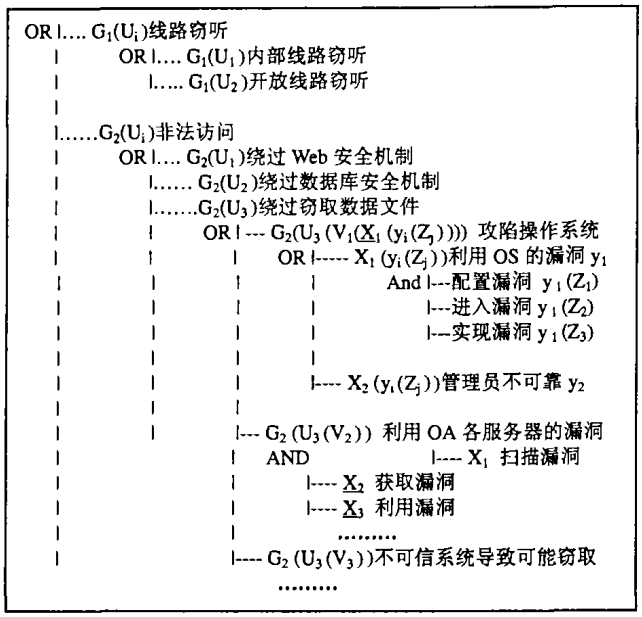


图2 一个可能的威胁树分级示例

因此，影响机密性的一个子树 Q_i 可表示为：q_1：

$\langle G_1(U_3(V_1(X_1(y_i(Z_j))))), G_2(U_3(V_1(X_1(y_i(Z_2))))), G_2(U_3(V_1(X_1(y_i(Z_3))))))\rightarrow G_2(U_3(V_1(X_1(y_i))))\rightarrow G_2(U_3(V_1(X_1)))\rightarrow G_2(U_3(V_1))\rightarrow G_2(U_3)\rightarrow G_2$

相应地，其它子树为：

$q_2: G_1(U_3(V_1))\rightarrow G_1(U_3)\rightarrow G_1$

$q_3: G_1(U_3(V_2))\rightarrow G_1(U_3)\rightarrow G_1$

$q_4: G_2(U_3(V_2(X_1)))\rightarrow G_2(U_3(V_2))\rightarrow G_2(U_3)\rightarrow G_2$

等。因此，对机密性的威胁集可以用各子树通路的集来表示：$TC=(q_1,q_2,\cdots,q_n)$。同样，可以构造对完整性、可用性的威胁子树。

3 安全评估方法

3.1 评价指标设计

根据专家经验或历史数据可以确定每个叶子结点所代表的威胁发生概率。对中间结点来说，若下层为串联型，则有：

$$P((G_i(U_j(V_k))))=P(G_i(U_j)(V_k)(X_m\cdots))*P(G_i(U_j(V_k(X_{m+1}\cdots))))\cdots,$$

其中，$m=0,1,2,\cdots$。若为并联型，则认为并联中所有概率最大的一个为其发生概率：

$$P((G_i(U_j)(V_k)))=\max\{P(G_i(U_j(V_k(X_m\cdots)))),P(G_i(U_j(V_k(X_{m+1}\cdots)))),\cdots\}$$

其中，$m=0,1,2,\cdots$。

对于威胁树的一个通路而言，包含该叶子结点的中间概率，该子树的发生概率由叶子节点（并联型）或叶子结点的运算（串联型）确定。

定义1 每一个根节点的各子树发生概率加权运算为该节点所代表的安全度。即：$T_c=1-\sum_i\omega_i*p(q_i)$，其中，$p(q_i)$为每个子树的发生概率；可根据节点概率进行运算得到；ω_i为每个子树的威胁发生概率权重，是根据不同系统机构、应用，不同安全要求而定义。该权重为两个相同和类似系统进行比较提供了依据，根据系统实际根节点的重要意义程度来划分，并且有：$\sum\omega_i=1$。

例如，对图3中的机密性（即根节点）而言，其安全度为：$T_c=1-\sum_i\omega_{ci}*P(q_{ci})$其中，$\omega_{ci}$为各子树的权重，$P(q_{ci})$为各子树的发生概率。同样可以得到对完整性、可用性的安全度T_{ia}，T_a。对整个系统而言，其总体安全度是所有根节点安全度的综合，即：$S=\lambda_cT_{ic}+\lambda_{ia}T_{ia}+\lambda_aT_a$。其中，$\lambda_c$、$\lambda_{ia}$、$\lambda_a$分别为系数，取决于被评估系统在各方面的侧重点。对两个系统而言，若有 $S_1>S_2$，则表明系统1相对系统2能够防御较多的外部攻击威胁。

对某些系统而言，只要有任何一个自节点出现问题，即一个子树出现问题，整个系统就会瘫痪，即有：$S_T=\max\{(P(tree1),P(tree2),\cdots,P(treen))\}$，其中：$P(tree1)$代表子树的评估值，而 n 是子树的数目。或：$S_T=\max\{P((G_i(U_j(V_k)))),\cdots\}$，其中，串联的叶子节点不包括在内。称为系统的最弱安全因子。指标 S_T 给出了系统最弱也是最需要保护的内容，是对总体安全度的一个补充。可见，这个，因子越小越好。

3.2 概率因素的确定

节点概率 P 表明一般情况下的可能性，可根据类似系统的历史数据得到相对标准值。但是对具体系统而言，由于其安全建设的不同以及安全管理策略，发生的概率可能低于标准值。例如，对网络饶过数据库安全机制来说，假设一般标准发生值为0.3，而对于一般安装了数据库审计与检查的系统来说，由于系统能够抵御一般饶过数据库安全机制，其概率可能为0.1。

权重 ω 是对每类威胁的标示，可根据具体应用对系统的重要程度来划分。权重较高的威胁是需要加以防范的威胁，从而为系统的安全建设提供指导意义，同时也提供了类似系统的比较依据。

3.3 组件敏感度分析

组件的敏感度体现在威胁树中任一个叶子节点（即相对独立的评价点，称为独立组件）的改动会对整个系统产生多大的影响，由此便可得知某一个组件或者某一组件对整个系统安全性的重要程度。假如某一组件发生变化，整个系统的评估值发生显著变化，则有必要对这组组件进行特别的检查，由此可以得到改善系统安全性的一些建议。对中间级组件，其安全属性评估值可以从基本组件得到，即计算出每个组件的评估值，由此得到中间级的安全属性评估值。假设其它的组件评估值保持不变，使某个组件的评估值变动，定义该组件和整个系统评估值相关的组件敏感度 MG 为：$MG=\partial S(tree)/\partial T_c(subtree)$。

敏感度分析还可以用来检查所建模型的健全性。例如，某些组件的值明显高于其他组件，则模型的分解过程可能会存在某些错误。经过充分敏感度分析的分解过程，对于应该怎样将易受攻击的部分从系统中划分出来，将会起到有用的指导作用。

3.4 动态模型的调整与自适应

本模型是建立在静态的基础上的，实践中我们可以根据实际的调查结果、先验概率资料以及实际过程中的实际参数进行调整。例如，可以将上述根据专家经验、历史数据或调查表得到的 ω_{ci}，ω_{cai}，ω_{ai}，λ_{ca}，λ_{ic}，λ_{ia}，$p(G_i(U_j(V_k(X_m\cdots))))$设计成参数形式并根据实验和实践结果结论动态调整参数，以保证模型和经验公式的准确性和递进能力，即对上述理论框架进行动态自适应调整与优化。

结束语 本文从信息系统本身的技术和管理方面，分析技术和管理环节可能存在的安全威胁和已经存在的脆弱性，建立系统安全树状模型，并根据该模型给出评价指标。该模型可为系统的安全性评估、比较提供一种方法。

理想状态下泛逻辑的形式演绎系统 B 的完备性*)

罗敏霞　何华灿

(西北工业大学计算机学院　西安710072)

摘　要　UB代数是理想状态(广义相关系数 $h=0.5$,广义自相关系数 $k=0.5$)下泛逻辑的代数系统。本文引入UB代数滤子的概念,讨论了UB代数的一系列性质。证明了理想状态下泛逻辑形式演绎系统 B 的完备性与强完备性。

关键词　泛逻辑,形式演绎系统 B,UB代数,完备性

The Completeness of the Formal Deductive System B of Universal Logic in the Ideal Condition

LUO Min-Xia　HE Hua-Can

(School of Computer Science, Northwestern Polytechnical University, Xi'an 710072)

Abstract　UB algebra is universal logic algebra system in the ideal condition(the generalized correlative coefficient $h=0.5$ and the generalized self-correlative coefficient $k=0.5$). In this taper, we introduce the concept of filter in UB algebra. Some properties of UB algebra are discussed. Moreover, we prove the completeness and strong completeness of the formal deductive system B of universal logic in the ideal condition.

Keywords　Universal logic, Formal deductive system B, UB algebra, Completeness

1965年 Zadeh 建立了模糊集理论[1],他提出用三角范数 $T_M(x,y)=\min(x,y)$、三角余范 $S_M(x,y)=\max(x,y)$、标数非 $N_S(x)=1-x$ 分别作为模糊集的交、并和补运算,随即形成一种初始形态的模糊逻辑[2]。然而模糊逻辑的理论远不完善,模糊推理的方法还没有严格的逻辑基础。近年来,以王国俊教授为首的一批学者成功地将模糊逻辑的模糊推理结合起来,取得了一系列有意义的成果[3~8]。一种新的模糊逻辑形式演绎系统 L^* 被建立[3];1998年模糊逻辑的广义重言式理论被提出[4];1999年模糊推理三 I 方法问世[5];2002年成功地解决了形式系统 L^* 的完备性问题[7],从而为模糊推理在语构上奠定了严格的逻辑基础。

本文第二作者为了探索逻辑的一般规律,提出建立能包容各种逻辑形态和推理模式的泛逻辑学理论[9,10]。在长期从事人工智能理论和实用专家系统的研究中发现,模糊命题之间的关系柔性是不可回避的客观存在,需要用连续可变的逻辑运算模型来描述,也就是说,在对立不充分的柔性世界中,不仅要考虑模糊性对命题逻辑真值的影响,而且要考虑关系柔性对命题联结词运算模型的影响。事物之间的广义相关性和广义自相关性是引起关系柔性的根本原因。泛逻辑学给出了命题联结词的运算模型:

(1)泛非命题联结词 $\neg_\lambda$ 的运算模型:

$N(x,k)=(1-x^n)^{1/n}$

(2)泛与命题联结词 $\wedge_{\lambda,k}$ 的运算模型:

$T(x,y,h,k)=\Gamma^1[(x^m+y^m-1)^{1/m}]$

(3)泛或命题联结词 $\vee_{\lambda,k}$ 的运算模型:

$S(x,y,h,k)=(1-\Gamma^1[((1-x^n)^m+(1-y^n)^m-1)^{1/m})^{1/n}]$

(4)泛蕴涵命题联结词 $\rightarrow_{\lambda,k}$ 的运算模型:

$I(x,y,h,k)=ite\{1|x\leqslant y;0|m\leqslant 0$且 $y=0$且 $x\neq 0;\Gamma^1[(1-x^m+y^m)^{1/m}]\}$

其中:$n=-1/\log_2 k$,$k\in[0,1]$。$m=(3-4h)/(4h(1-h))$,$h\in[0,1]$。$\Gamma^1[x]$ 表示把 x 限制在[0,1]内,$x>1$取1;$x<0$或为虚数时取0。$S=ite\{\beta|\alpha;\gamma\}$ 是条件表达式,表示"如果 α 为真,则 $S=\beta$;否则 $S=\gamma$"。

除了上面四个运算模型之外,还有泛等价命题联结词,泛平均命题联结词和泛组合命题联结词的运算模型,详细内容参阅文[10]。泛逻辑学的研究目标是提供一个逻辑生成器,通过运用各种规则,可以构造出满足某种需要的具体逻辑。这个目标的标准命题泛逻辑学层在上已经实现[10]。

泛逻辑学的研究思想是从现实世界的柔性逻辑出象出发,通过一个连续单调映射,在理想世界中建立理想柔性推理,再通过这个映射的塑映射,把它应用于现实世界中。几年来,泛逻辑学已经成为人工智能领域最具活力的研究方向之一。文[11]从理想世界($h\equiv 0.5$,$k\equiv 0.5$)出发,给出理想状态下泛逻辑的形式演绎系统 B。完备性对一个形式系统来说至关重要,它反映了一个系统在语法与语义两个方面的和谐性。经典逻辑系统之所以成为数学、计算机科学以及其它学科的严格的逻辑基础,就是因为它具有语法与语义的和谐性。这种和谐性也是泛逻辑形式系统研究的目标,本文的目的是解决理想状态下泛逻辑形式系统 B 的完备性。

本文只讨论广义相关系数 $h=0.5$ 与广义自相关系数 $k=$

*)本文得到中国国家自然科学基金(60273087)和北京市自然科学基金(4032009)资助。罗敏霞　副教授,博士生,主要研究方向为代数学,人工智能原理及应用;何华灿　教授,博士生导师,主要研究方向为人工智能原理及应用,泛逻辑学。

参 考 文 献

1　ISO/IEC 1799-1. 1999 Information Security Management. 2000. 2
2　Alberts C J, Dorofee A J. OCTAVE[SM] Method Implementation Guide Version 2.0. June 2001
3　Bhatia R. Policy Evaluation for network management. IEEEE INFOCOM, 2000. 1107~1116
4　Haimes Y Y, James H. Risk modeling, Assessment, and Management of interdependent Critical infrastructures. In: 16th Annual security technology symposium Williamsburg, VA june 2000
6　李波. 复合离散对数与安全认证研究. 计算机科学, 2004(6)
7　李波. 分布式入侵检测系统中事件关联方法的研究. 计算机科学, 2004(8)