ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*, Vol.18, No.1, January 2007, pp.137−145
DOI: 10.1360/jos180137
© 2007 by *Journal of Software*. All rights reserved.

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

# 用于评估网络信息系统的风险传播模型*

张永铮+, 方滨兴, 迟 悦, 云晓春

(哈尔滨工业大学 计算机网络与信息安全技术研究中心,黑龙江 哈尔滨 150001)

# Risk Propagation Model for Assessing Network Information Systems

ZHANG Yong-Zheng+, FANG Bin-Xing, CHI Yue, YUN Xiao-Chun

(Research Center of Computer Network and Information Security Technology, Harbin Institute of Technology, Harbin 150001, China)

+ Corresponding author: Phn: +86-10-62600996, E-mail: zhangyongzheng@software.ict.ac.cn

**Zhang YZ, Fang BX, Chi Y, Yun XC. Risk propagation model for assessing network information systems. *Journal of Software*, 2007,18(1):137−145**. http://www.jos.org.cn/1000-9825/18/137.htm

**Abstract**: To assess the security risk of network information systems, this paper proposes a risk propagation model including a risk network and a risk propagation algorithm. A representative example is given to illustrate the application of this model to network risk assessment and validate the correctness of the propagation algorithm. The analysis of the example indicates that the evaluating method using the risk propagation model is superior to the traditional methods in the accuracy of evaluating conclusions and making cost-effective security advices.
**Key words**: network security; network risk assessment; risk propagation; risk analysis

摘 要: 为了评估网络信息系统的安全风险,提出了一个由风险网络和风险传播算法构成的风险传播模型,并以一个具有代表性的实例阐明了该模型在网络风险评估中的应用,验证了传播算法的正确性.实例分析表明,应用风险传播模型的评估方法较传统方法在评估结论的准确性和制定符合最优成本效应的安全建议等方面更具优势.
关键词: 网络安全;网络风险评估;风险传播;风险分析
中图法分类号: TP393 文献标识码: A

随着 Internet 技术的快速发展,针对网络信息系统的恶意攻击变得越来越多样化和复杂化,其中,计算机及网络病毒则是以一种自动化的方式,借助软件的安全弱点来扩散、蔓延并攻击计算机系统.据估计,目前大约有 580 00 多种已知病毒[1],同时,一些组织也在不断地更新和发布各种软件的安全弱点信息.由此可见,诸如上述的不安全因素正在严重地危及着网络信息系统的安全.为了使系统更加安全和健壮,系统的管理员和开发者正在寻求一种主动的安全防范技术——风险评估.与入侵检测技术相比,风险评估能够帮助用户更主动地识别系统所面临的潜在的安全威胁,提前评估其安全态势,从而根据需求来制定安全建议,最终避免危险事件的发生.

从自动化程度来看,风险评估方法可以分为:1) 人工评估[2],通常以问卷调查的方式开展,依赖专家经验,尽管评估比较全面,但易引入主观因素,而且,复杂的评估过程导致用户面对庞大的开销;2) 自动评估,通常采用自

* Supported by the National Natural Science Foundation of China under Grant No.60403033 (国家自然科学基金); the Defense Pre-Research Project of the ‘Tenth Five-Year-Plan’ of China under Grant No.4131571 (国家“十五”国防预研基金)

Received 2005-12-29; Accepted 2006-04-10

© 中国科学院软件研究所 http://www.jos.org.cn

动识别弱点或攻击的方法对目标网络进行评估,由于这种方法的自动性、高效性和易管理性,所以深受使用者的青睐.目前,针对自动评估技术的相关研究工作较多:李涛[3]提出了一种基于免疫的网络安全风险检测模型,但主要侧重于对网络系统面临攻击时的实时风险评估;Ritchey 与 Ammann[4]提出了一种网络弱点的模型检测方法;Jajodia 等人[5]设计了一种拓扑弱点分析工具 TVA,它可以检测网络系统弱点,并以网络攻击图的形式分析网络系统的安全风险;汪渊等人[6]基于安全案例推理的方法生成可能的攻击图来分析网络安全性.上述工作主要从攻击的角度评估网络安全性,且大多数属于定性分析,而本文将从风险以及定量分析的角度展开研究.

在此方面,传统方法是将自动弱点扫描工具[7,8]获得的弱点实施量化后进行风险累加,但这种方法往往忽略了风险的传播性这一事实:由于计算机的高度互联,受害计算机引起的风险可能会传播给其他主机甚至整个网络,使得那些原本不直接具有风险的计算机,因受害计算机的风险传播,而遭到安全威胁.

为此,本文提出了一个风险传播模型来描述网络系统客观的风险状况.该模型主要包括风险网络和风险传播算法.风险网络描述了网络系统的访问关系结构和风险态势,风险传播算法则给出了风险的运动规则.随后,本文以一实例阐明了该模型在网络风险评估中的应用,验证了传播算法的正确性,对应用该模型的评估方法和传统方法进行了深入的比较、分析.本文的目的在于:1) 通过引入风险传播思想,建立风险传播模型,从而提高风险评估的准确性;2) 给出一种有效的方法能够在网络系统中找到最具安全威胁的风险源,以便制定最优成本效应的安全建议.

## 1 风险传播模型

### 1.1 模型定义

首先给出一系列相关概念及定义.

定义 **1**(部件). 我们把网络信息系统中的一台计算机设备称为一个网络节点,并将网络节点上的用户、操作系统、应用程序或服务称为网络节点上的主体,而对网络节点 $n$ 及其上的主体 $s$ 构成的数对$(n,s)$,我们称其为节点 $n$ 上的一个部件,记为 $C_{ns}$.

在网络信息系统中,功能各异的计算机被电缆互联起来,传输于电缆上的各种服务信息和数据操作往往使计算机的部件之间形成了众多特殊的访问逻辑关系.在文献[9]中,Yau 提出了一个所谓“安全依赖关系”的概念,并以此来描述两个部件之间潜在的逻辑关系.引入这一思想,本文针对安全风险方面的问题也引入一个“网络节点之间的关联关系”,称之为 NNC,下面对 NNC 进行定义:

定义 **2**(网络节点关联(**network node correlation**,简称 **NNC**)). 如果一个攻击者在成功入侵网络节点 $A$ 之后,利用 $A$ 上的某部件 $C_{Ai}$ 对节点 $B$ 上某部件 $C_{Bj}$ 的访问关系,从而继续攻击节点 $B$,那么,我们就把这种可被利用的访问关系称为部件 $C_{Ai}$ 到 $C_{Bj}$ 的 NNC,书写为 $NNC_{Ai:Bj}$,在不混淆的情况下,亦可简写为节点 $A$ 到 $B$ 的一个 $NNC_{AB}$.我们用一个有序六元组$\langle A,i,B,j,P,W\rangle$来描述 $NNC_{Ai:Bj}$ 的风险信息,其中:$i,j$ 分别为节点 $A,B$ 上的主体;$P$ 表示利用该 NNC 进行攻击的成功的概率,$P\in[0,1]$;$W$ 表示一个部件对另一个部件的影响程度,$W\in[0,+\infty)$.需要强调的是:1) 本文所指的访问关系均是已授权的,即符合各节点主机的安全策略,而不考虑攻击、入侵等非授权访问关系;2) 属性 $P$ 和 $W$ 的量化标准应取决于具体的实践经验、历史数据及主观期望等方面.

文献[9]指出,“安全依赖关系”可以通过手动和自动的方法来建构.我们有理由相信利用同样的方法也可以获得所有网络节点间的 NNC,然而,如何获得 NNC 并不是本文讨论的重点.

定义 **3**(访问关系网络). 由网络节点、部件和 NNC 构建的网络,我们称之为访问关系网络,如图 1 所示.其中:$A$~$D$ 为网络节点;$i,j$ 分别为节点 $A,B$ 上的主体;有向边 $e(Ai,Bj)$表示 $NNC_{Ai:Bj}$;黑色表示该节点具有安全弱点.

为了便于在访问关系网络中讨论部件之间的关系,我们进行如下定义:

定义 **4**(父亲、祖先与儿子、子孙). 我们把有向边的起始部件称为终止部件的父亲;相反,我们称终止部件为儿子.进一步地,我们给出祖先与子孙的递归定义,把满足以下任一条件的部件称为部件 $C$ 的祖先:1) 部件 $C$ 的父亲是 $C$ 的祖先;2) 部件 $C$ 父亲的祖先是 $C$ 的祖先.同理,也可以定义子孙.

定义 **5**(风险传播). 设在访问关系网络中存在 3 个网络节点 $A,B,C$,两个有向边 $e(Ai,Bj)$和 $e(Bj,Ck)$,且节点 $A$

© 中国科学院软件研究所 http://www.jos.org.cn

存在弱点.从攻击者的角度看,他可以利用弱点侵入节点 $A$,进而利用 $e(Ai,Bj)$对节点 $B$ 进行攻击,依此类推,侵入节点 $B$ 后利用 $e(Bj,Ck)$攻击节点 $C$;而从安全风险的角度看,由于 $e(Ai,Bj)$和 $e(Bj,Ck)$的存在,使得具有弱点的节点 $A$ 将自身的风险不同程度地转移给原本没有风险的节点 $B$ 和 $C$.因此,我们称风险具有可传播性,而风险转移的这一过程称为风险传播.事实上,风险传播是可能发生的攻击过程在风险上的体现.

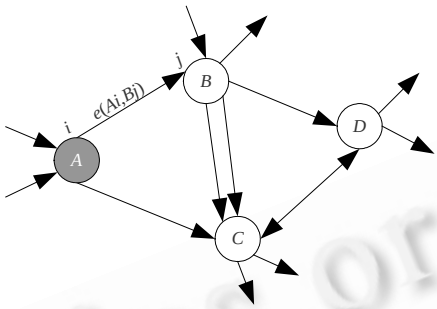


Fig.1 Access relation network

图 1 访问关系网络

定义 **6**(风险源与风险传播途径). 我们把具有弱点的部件称为风险源.特别地,具有不同弱点的同一部件,可以被看作是不同的风险源;而网络中的有向边称为风险传播途径.控制风险的有效方法就是按照最优成本效应适当消除风险源或风险传播途径.

定义 **7**(风险网络). 我们把一个能够表述风险状况的访问关系网络称为风险网络,定义为 $D=(N,E)$.其中,$N$ 是带有风险信息的网络节点的集合,$N=\{N_i|F,R,S\}$.$N_i$ 是网络节点,$N_i$ 的风险属性由 $F,R,S$ 来描述.$F$ 表示 $N_i$ 在功能上的价值,包括信息服务器、数据库、个人主机等[10];$R$ 用于存放 $N_i$ 的总风险,$F,R\in[0,+\infty)$;$S$ 是 $N_i$ 上受威胁主体的集合,$S=\{S_i|P,R,V\}$.$S_i$ 表示节点上的主体,$S_i$ 的风险属性由 $P,R,V$ 来描述.$P$ 用于存储 $S_i$ 发生危险的概率,$P\in[0,1]$;$R$ 用于存储 $S_i$ 的风险,$R\in[0,+\infty)$;$V$ 是危及 $S_i$ 安全的弱点集合,$V=\{V_i|P,W,R\}$.其中,$V_i$ 表示弱点,$V_i$ 的风险属性由 $P,W,R$ 来描述.$P$ 是弱点被成功攻击的概率,$P\in[0,1]$;$W$ 是弱点的安全影响,$W\in[0,+\infty)$;$R$ 是弱点所带来的风险,通常将 $P$ 与 $W$ 的乘积作为风险 $R$[11,12],即 $R=P\times W$.我们应用前期工作中提出的弱点分类法[13]可以获得弱点的这些风险信息.最后,$E$ 表示有向边的集合.风险网络 $D$ 的层次结构如图 2 所示.风险网络 $D$ 不仅形式化地描述了网络信息系统的访问关系结构,而且可以存储和表达每个节点相应的风险状态.

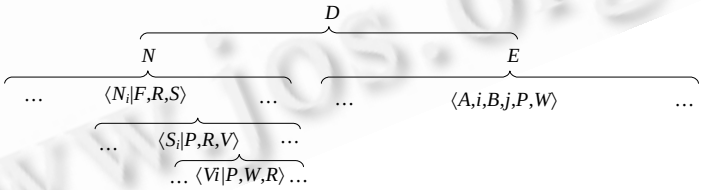


Fig.2 Hiberarchy of risk network

图 2 风险网络的层次结构

一个部件的风险由多种因素所构成,按风险来源的不同可分为内部风险和外界风险两类,我们将其分别表示为 $R_i$ 和 $R_o$.内部风险通常是由部件自身的弱点所引起的,一个部件 $C_{Aj}$ 的总的内部风险 $R_{ij}^A$ 是由一系列的内部风险 $R_{ij_1}^A \sim R_{ij_n}^A$ 所构成,其中 $R_{ij_1}^A = A.j.i.R$, 表示部件 $C_{Aj}$ 的弱点 $i$ 所带来的风险;而外界风险是由邻接部件的相关风险传播而来,部件 $C_{Aj}$ 的总的外界风险 $R_{oj}^A$ 是由一系列的外界风险 $R_{oj_1}^A \sim R_{oj_n}^A$ 所构成,其中风险 $R_{oj_i}^A$ 是来自于部件 $C_{Bk}$ 的风险通过 $e(Bk,Aj)$传递而来,则 $R_{oj_i}^A = B.k.P\times e(Bk,Aj).P\times e(Bk,Aj).W$.

基于风险网络的概念,最后我们给出风险传播模型的定义.

定义 **8**(风险传播模型). 我们将风险传播模型定义为 $M=(D,A)$,其中:$D$ 表示风险网络;$A$ 表示传播算法集合,

© 中国科学院软件研究所 http://www.jos.org.cn

$A$ 中的每个元素都是相互独立的算法,它们描述了风险源将其风险沿着传播途径扩散到网络中的过程.在模型 $M$ 中,网络 $D$ 用于存储网络信息系统的风险状态,而每种传播算法体现了风险的运动规则,改变了网络 $D$ 的风险状态.

### 1.2 传播算法

由于风险网络 $D$ 中可能存在有向回路,所以我们必须面临风险循环传播的问题,即一个部件可能将自身内部风险或已有的外界风险循环传播给自己.为了解决这一问题,我们采用还原论(reductionism)与整体论(holism)相结合的方法.根据还原论的思想我们可知:由若干风险源共同作用所形成的各互联部件的总风险,是各个风险源分别单独作用时各互联部件风险的综合体现.因此,我们首先依次将每个风险源单独作用时的风险传播给所有可达节点.在传播过程中,并不将这些风险综合起来计算(因为在判断是否传给儿子部件时,我们无法得知综合后的风险结果中是否存在来自于儿子部件的风险成分),而是要求每个部件分别保存其自身风险以及每个风险源通过有向边传递而来的风险.这样,我们就可以根据风险来源来决策是否传给儿子部件,从而去除自身循环风险.然后应用整体论思想,根据各类风险的概率分布情况计算每个部件发生危险的联合概率及其综合风险,进一步地,通过对节点上所有部件风险的累加,我们可以计算出节点的综合风险.同理,可以获得整个网络的综合风险.我们将上述基于还原论和整体论思想的精确传播算法记为 RH 算法,$RH\in A$.

RH 算法的具体实现如下:

输入:风险网络 $D=(N,E)$,弱点集合 $V=\{n.s.v_i|n.s.v_i$ 表示部件 $C_{ns}$ 的弱点 $v_i,n\in N,s\in n.S\}$.

输出:$D$ 和网络系统的总风险 $R(D)$.

(1) 初始化:部件集合 $Q=\varnothing$;对所有 $n\in N,s\in n.S,n.R=0,n.s.P=0,n.s.R=0,n.s.PS=\varnothing$;

(2) while ($V\neq\varnothing$)

{

(3) 取(移)出一个弱点 $m.i.v_j\in V$,将字符串“$m.i.v_j.P$”移入 $m.i.PS$,将 $C_{mi}$ 移入 $Q$;

(4) 调用独立传播子算法 $RH_1(C_{mi},$“$m.i.v_j.P$”$,Q)$;

(5) 从 $Q$ 中删除 $C_{mi}$;

}

(6) 对所有 $n\in N,s\in n.S$,调用综合风险子算法 $RH_2(C_{ns},n.s.PS)$,并计算 $n.R=\sum_{s\in n.S}n.s.R, R(D)=\sum_{n\in N}(n.R\times n.F)$;

(7) 返回 $D$ 和 $R(D)$;

RH 算法主要由初始化(第 1 行)、风险独立传播(第 2~5 行)和综合风险(第 6 行)3 个部分构成.为了存储概率乘积算式的字符串,我们为 $D$ 中的每个部件增加一个临时属性——集合 $PS$,每次传播给该部件的概率乘积算式字符串将被保存为集合 $PS$ 的一个元素,而不必计算出它们具体的数值.此外,集合 $Q$ 按风险传播顺序记录了有向路径上经过的所有部件.

子算法 $RH_1$ 的具体实现如下:

输入:部件 $C_{mi}$,字符串 $Pstr$,部件集合 $Q$.

输出:空.

(1) 对所有有向边 $e(mi,nj)\in E$,

{

(2) 如果 $C_{nj}\in Q$,则取下一个;

(3) 否则,将字符串“$Pstr\times e(mi,nj).P$”移入 $n.j.PS$,将 $C_{nj}$ 移入 $Q$;

(4) 递归调用 $RH_1(C_{nj},$“$Pstr\times e(mi,nj).P$”$,Q)$;

(5) 从 $Q$ 中删除 $C_{nj}$;

}

独立传播子算法 $RH_1$ 在风险源单独作用的情况下,以部件 $C_{mi}$ 为祖先,将概率乘积算式的字符串 $Pstr$ 按深

© 中国科学院软件研究所 http://www.jos.org.cn

度优先遍历顺序递归地传播给子孙部件.这里,我们利用集合 $Q$ 中的信息来避免因自身风险(内部风险或已有的外界风险)循环传播给自己而误增加风险值,即如果发现要传播的下一个部件在 $Q$ 中(如第 2 行),说明出现了循环,则终止传播.

子算法 $RH_2$ 的具体实现如下:

输入:部件 $C_{ns}$,集合 $PS$.

输出:$PS$ 的字符串形式的联合概率值.

(1) while ($PS$ 中存在具有公共右因子的元素)

{

(2) 取出一组元素"$Pleft_i \times e(ai,bj).P$"$\in PS$,其中 $Pleft_i$ 为元素中除公共右因子以外的左部分字符串;

(3) 将字符串"$RH_2(0,\{Pleft_i\}) \times e(ai,bj).P$"移入 $PS$;

}

(4) 计算联合概率 $P = 1 - \prod_{i=1}^{|PS|}(1 - number(Pstr_i)), Pstr_i \in PS$;

(5) 如果 $C_{ns} \neq 0$,则

$$n.s.R = \sum_{i=1}^{|PS|} \begin{cases} number(Pstr_i) \times e(vw,xy).W, & \text{如果}Pstr_i\text{的最右因子是有向边,则设为“}e(vw,xy).P\text{”} \\ n.s.v_i.R, & \text{否则设}Pstr_i = \text{“}n.s.v_i.P\text{”} \end{cases},$$

$n.s.P=P$;

(6) 返回 $string(P)$;

综合风险子算法 $RH_2$ 根据集合 $PS$ 计算出部件 $C_{ns}$ 的联合概率 $n.s.P$ 以及综合风险 $n.s.R$.由前文可知,部件 $C_{ns}$ 的风险可以由内部风险和外界风险构成.对外界风险而言,我们需要考虑部件的有向边的概率,它等于自身概率与其父亲部件联合概率的乘积.然而,在风险传播的过程中,不同祖先部件的风险独立传播到父亲部件时并没有计算出具体的联合概率值,而是以不同的概率乘积算式字符串与有向边自身概率字符串的乘积形式,保存为集合 $PS$ 中不同的元素,所以,我们需要通过提取公共右因子的方法计算父亲乃至祖先部件的联合概率.于是,考察集合 $PS$ 中的每个元素,如果存在公共右因子,则提取公共右因子使得父亲节点各风险的概率汇集到一个新的集合中,递归这一过程,直至新集合中不存在任何公共右因子(第 1~3 行);如果不存在公共右因子,则对集合中的每个元素应用概率公式计算出该集合的联合概率(第 4 行)或部件的联合概率及综合风险(第 5 行).算法中符号 $number()$和 $string()$分别表示转换成数字形式和字符串形式.

## 2 网络风险评估应用

为了验证风险传播模型的正确性,阐明该模型在网络风险评估领域中的应用及优势,我们给出了一个用风险传播模型评估网络信息系统的实例分析.

### 2.1 评估应用及正确性验证

一个典型的网络信息系统实例如图 3 所示,其中,$A$~$D$ 为 4 台 Linux 主机系统:$A$ 为科学实验服务器,为研究人员提供实验环境;$B$~$D$ 提供了各种信息服务,分别为邮件服务器、网页服务器、数据库系统.为了提供使用上的便利或满足业务上的需求,实践中,人们通常会启动或设置远程控制、访问等服务;另一方面,由于未及时对网络系统打补丁或其他管理上的疏忽等原因,使得网络系统中存在着或多或少的弱点.而实践中,这样的情形具有一定程度的普遍性,所以我们考虑在实例中适当地体现出该情形,以便通过评估这种具有普遍性的实例来表现风险传播模型的现实意义.于是作以下设定:$A$ 存在危及系统管理员 root 的弱点 $v_1$ 和危及系统普通用户 user 的弱点 $v_2$;$B$ 开启 rshd 服务,允许 $A$ 和 $D$ 的 root 用户以 root 身份执行远程 shell 命令;$C$ 开启 telnetd 和 rshd 服务,$B$ 的 root 用户能够以 root 身份通过 telnet 访问 $C$,rshd 服务仅允许 $D$ 的 root 用户以 root 身份执行远程 shell 命令,且 $C$ 具有危及 root 的弱点 $v_4$ 和 $v_5$;$D$ 开启 sshd 服务,具有危及 root 的弱点 $v_3$,$A$ 的用户 user 和 $C$ 的用户 root 能够以 root 身份通过 ssh 访问 $D$.

© 中国科学院软件研究所 http://www.jos.org.cn

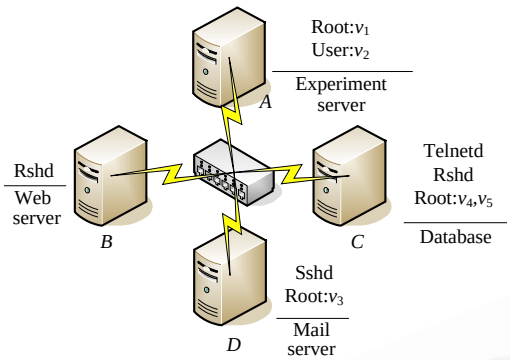


Fig.3 An example of network information system

图 3 网络信息系统实例

根据我们提出的风险传播模型理论,对该网络系统进行建模,可将其抽象成为一个风险网络图,如图 4 所示.我们分别对节点和主体进行编号,用 1~4 分别代表节点 $A$~$D$,用 1 和 2 代表主体 root 和 user,“1.1.$v_1$”表示节点 $A$ 主体 root 上的弱点 $v_1$,$E_1$ 表示有向边 $e$(11,21),其他类同.从图中可以看出:该实例具有一定的代表性,涵盖了风险网络理论中所有可能的网络状况:1) 图中存在有向回路;2) 两节点间存在多条有向边;3) 同一节点上有多主体;4) 同一主体存在多弱点.

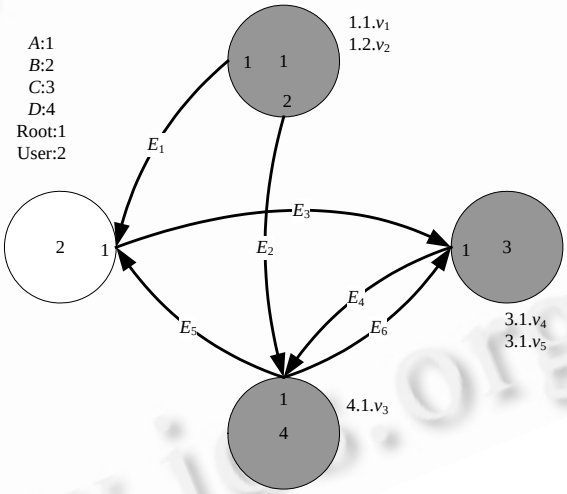


Fig.4 Risk network graph of the example

图 4 风险网络图

事实上,利用每个弱点或有向边进行攻击的难易程度是不同的,所以概率也是不同的.然而,为了突出后文的实验效果,我们不妨假设所有弱点和有向边的概率相等、危害性相等,并且节点的功能价值属性也相等,即设 $v_i.P=E_j.P=0.8$,$v_i.W=E_j.W=1$($i$=1~5,$j$=1~6),$n.F=1$($n$=1~4).将此风险网络输入给 RH 算法,可以计算出该网络系统的风险状况,见表 1.经验证,该结果与人工计算结果相同.这表明,从实例的角度,风险传播模型的传播算法 RH 是正确的.

**Table 1** Risk status of the network system

**表 1** 网络系统的风险状况

| Network risk | 8.319 2 | | | |
|---|---|---|---|---|
| Node risk | ① 1.600 0 | ② 1.426 6 | ③ 3.068 2 | ④ 2.224 4 |
| Subject risk/probability | ① 0.8000/0.8000<br>② 0.8000/0.8000 | ① 1.4266/0.9232 | ① 3.0682/0.9972 | ① 2.2244/0.9845 |

© 中国科学院软件研究所 http://www.jos.org.cn

### 2.2 优势分析

以上述网络信息系统的评估为例,我们将从评估结论和安全建议两个方面对基于风险传播模型的评估方法(简称模型方法)和传统评估方法进行比较和分析.

(1) 评估结论

传统方法通常是将孤立弱点的自身风险累加起来,作为网络系统的总体风险,而模型方法在此基础上增加了风险传播的影响.图 5 给出了两种方法评估结论的对比情况.从图中可以看出:两种方法仅对节点①的评估结论相同,其他情况均是模型方法给出的风险值较高.以节点②为例,事实上,其中的一种可能是:攻击者可以利用弱点 $v_1$ 入侵节点①后,继而利用节点②的 rshd 服务对节点①的信任关系攻击节点②,所以,节点②是存在一定风险的.传统方法低估了这一风险,而模型方法却予以适当的体现.由此可以看出,模型方法的评估结论较传统方法更为准确.

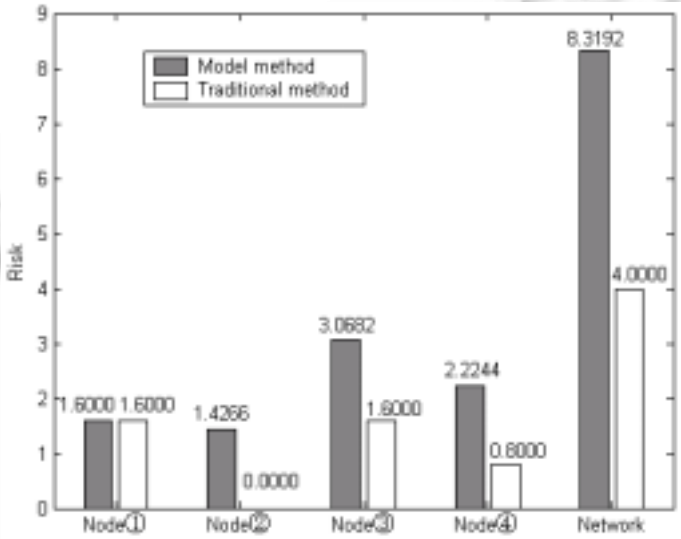


Fig.5 Contrast of evaluating conclusions drawn by the model method and the traditional method

图 5 模型方法与传统方法评估结论的对比

(2) 安全建议

在风险评估领域中,制定安全建议的前提是要知道哪些风险源的安全影响最大.如前文假设,所有弱点和有向边的概率相等、危害性相等,并且节点的功能价值属性也相等.在这种情况下,传统方法无法判定哪个风险源(具有弱点的部件)或风险传播途径(有向边)对网络或各节点的安全威胁最大.而在模型方法中,我们可以给出一个有效的算法找到最具安全威胁的风险源或风险传播途径的序列,其算法如下:

a) 计算网络和各节点风险,见表 1;

b) 每次仅从所有弱点(或有向边)中去掉其中一个未被处理过的,重新计算网络和各节点风险;

c) 被去掉的弱点(或有向边)对网络和各节点的安全影响为 a),b)中计算出的网络和各节点风险的差;

d) 重复 b)和 c),直至所有弱点(或有向边)都被处理过一次.对所有弱点(或有向边)的风险差进行降序排列.

通过上述算法,我们可以得到各风险源或风险传播途径对网络和各节点的安全影响序列,见表 2.从而,我们就可以针对网络或各节点的不同安全需求制定符合最优成本效应的安全建议.例如:欲降低节点②的风险,我们需要考虑去掉或控制有向边 $E_5$,$E_1$ 和弱点 $v_1$.由此可见,模型方法在制定安全建议方面也比传统方法更优.

与传统方法相比,模型方法之所以能够找到这样的序列,是因为我们增加了对风险沿有向边传播这一事实的考虑.所以说,各风险源(或风险传播途径)对网络的安全威胁不仅受到其自身概率和危害性的影响,而且也与风险网络结构以及风险源分布情况密切相关.

© 中国科学院软件研究所 http://www.jos.org.cn

**Table 2** Security impact sequences of risk sources and risk propagation approaches

表 2 各风险源或风险传播途径的安全影响序列

| Impact object | Network | Node ① | Node ② | Node ③ | Node ④ |
|---|---|---|---|---|---|
| Vulnerability (directed edge): risk difference | $V_2$:1.595 6 | $V_1$:0.800 0 | $E_5$:0.786 6 | $V_4$:0.800 0 | $V_3$:0.800 0 |
| | $V_1$:1.588 3 | $V_2$:0.800 0 | $E_1$:0.640 0 | $V_5$:0.800 0 | $E_4$:0.784 4 |
| | $V_3$:1.150 2 | $V_3$:0.000 0 | $V_1$:0.640 0 | $E_6$:0.742 4 | $E_2$:0.640 0 |
| | $E_5$:1.000 4 | $V_4$:0.000 0 | $V_3$:0.053 5 | $E_3$:0.725 8 | $V_2$:0.640 0 |
| | $V_5$:0.869 8 | $V_5$:0.000 0 | $E_4$:0.044 2 | $V_3$:0.296 8 | $V_4$:0.062 5 |
| | $V_4$:0.869 8 | $E_1$:0.000 0 | $V_2$:0.023 8 | $E_5$:0.213 8 | $V_5$:0.062 5 |
| | $E_4$:0.828 6 | $E_2$:0.000 0 | $E_2$:0.023 8 | $E_2$:0.131 9 | $V_1$:0.016 4 |
| | $E_2$:0.795 6 | $E_3$:0.000 0 | $V_4$:0.007 4 | $V_2$:0.131 9 | $E_3$:0.016 4 |
| | $E_1$:0.788 3 | $E_4$:0.000 0 | $V_5$:0.007 4 | $V_1$:0.131 9 | $E_1$:0.016 4 |
| | $E_6$:0.742 4 | $E_5$:0.000 0 | $E_3$:0.000 0 | $E_1$:0.131 9 | $E_5$:0.000 0 |
| | $E_3$:0.742 2 | $E_6$:0.000 0 | $E_6$:0.000 0 | $E_4$:0.000 0 | $E_6$:0.000 0 |

## 3 结 论

为评估网络信息系统的安全风险,本文提出了一个由风险网络和风险传播算法构成的风险传播模型,并以一个实例阐明了该模型在网络风险评估中的应用,验证了传播算法的正确性.与传统评估方法相比,应用风险传播模型的评估方法具有以下优势:

1) 评估结论适当地反映了客观现实,故更完善、更准确;

2) 能够找到最具安全威胁的风险源或风险传播途径的序列,在制定安全建议方面更优.

在两种评估方法的对比分析中,我们也发现:各风险源(或风险传播途径)对网络的安全威胁不仅受到其自身概率和危害性的影响,而且也与风险网络结构以及风险源分布情况密切相关.

致谢 真诚感谢审稿人为本文提出的宝贵意见.

**References**:

[1] Bruce L. Managed vulnerability assessment (MVA)—Mprove security by understanding your own vulnerabilities! Network Security, 2002,(4):8–9.

[2] Bennett SP, Kailay MP. An application of qualitative risk analysis to computer security for the commercial sector. In: Proc. of the 8th IEEE Annual Computer Security Applications Conf. San Antonio: IEEE Computer Society Press, 1992. 64–73.

[3] Li T. An immunity based network security risk estimation. Science in China Series E-Information Sciences, 2005,35(8):798–816 (in Chinese with English abstract).

[4] Ritchey R, Ammann P. Using model checking to analyze network vulnerabilities. In: Titsworth FM, ed. Proc. of the IEEE Symp. on Security and Privacy. Berkeley: IEEE Computer Society Press, 2000. 156–165.

[5] Jajodia S, Noel S, O'Berry B. Topological analysis of network attack vulnerability. In: Kumar V, Srivastava J, Lazarevic A, eds. Managing Cyber Threats: Issues, Approaches and Challenges. Springer-Verlag, 2005. 248–266.

[6] Wang Y, Jiang F, Chen GL. A network security analysis method research and application based on case-based reasoning. Mini-Micro Systems, 2003,24(12):2082–2085 (in Chinese with English abstract).

[7] Skaggs B, Blackburn B, Manes G, Shenoi S. Network vulnerability analysis. In: Soderstrand MA, Yarlagadda R, eds. Proc. of the 45th IEEE Midwest Symp. on Circuits and Systems, Vol.3. Tulsa: IEEE Computer Society Press, 2002. 493–495.

[8] Wales E. Vulnerability assessment tools. Network Security, 2003,(7):15–17.

[9] Yau SS, Zhang XY. Computer network intrusion detection, assessment and prevention based on security dependency relation. In: Baldwin T, ed. Proc. of the 23rd Annual Int'l Computer Software & Applications Conf. Phoenix: IEEE Computer Society Press, 1999. 86–91.

[10] Zhang YZ, Fang BX, Yun XC. A risk assessment approach for network information system. In: Yeung D, Wang XZ, eds. Proc. of the 3rd IEEE Int'l Conf. on Machine Learning and Cybernetics, Vol.5. Shanghai: IEEE Computer Society Press, 2004. 2949–2952.

[11] Biswas G, Debelak KA, Kawamura K. Applications of qualitative modeling to knowledge-based risk assessment studies. In: Ali M, ed. Proc. of the 2nd Int'l Conf. on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems. Tullahoma: ACM Press, 1989. 92–101.

© 中国科学院软件研究所 http://www.jos.org.cn

[12] Strutt JE, Patrick JD, Custance NDE. A risk assessment methodology for security advisors. In: Sanson LD, ed. Proc. of the 29th IEEE Annual Int'l Carnahan Conf. on Security Technology. Sanderstead: IEEE Computer Society Press, 1995. 225−229.

[13] Zhang YZ, Yun XC, Hu MZ. Research on privilege-escalating based vulnerability taxonomy with multidimensional quantitative attribute. Journal on Communications, 2004,25(7):107−114 (in Chinese with English abstract).

附中文参考文献:

[3] 李涛.基于免疫的网络安全风险检测.中国科学(E 辑-信息科学),2005,35(8):798−816.

[6] 汪渊,蒋凡,陈国良.基于安全案例推理的网络安全分析方法研究与应用.小型微型计算机系统,2003,24(12):2082−2085.

[13] 张永铮,云晓春,胡铭曾.基于特权提升的多维量化属性弱点分类法的研究.通信学报,2004,25(7):107−114.

张永铮(1978－),男,黑龙江哈尔滨人,博士,主要研究领域为网络与信息安全,风险评估,安全性分析.

迟悦(1979－),女,博士生,主要研究领域为网络与信息安全.

方滨兴(1960－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为网络与信息安全,并行计算,系统结构.

云晓春(1971－),男,博士,教授,博士生导师,主要研究领域为网络与信息安全.

☺☺☺