

文章编号:1001-9081(2010)01-0190-06

基于粗糙图的网络风险评估模型

黄光球, 李 艳

(西安建筑科技大学 管理学院, 西安 710055)

(huangnan93@sohu.com)

摘 要:针对在进行网络安全分析时所获得的信息系统是不完备的、粗糙的这一特性,将网络攻击过程类比为粗糙不确定性问题的关系挖掘过程,提出基于粗糙图的网络风险评估模型。该模型由部件节点粗糙关联网络、攻击图的粗糙图生成算法以及网络风险最大流分析算法三部分主要内容组成;并以一个具有代表性的网络系统实例阐明了该模型的使用方法,验证了模型的正确性。模型优势分析表明其较以往的攻击图、风险评价模型更能真实地反映实际情况,所获得的评估结论、安全建议等也更加准确、合理。

关键词:网络风险评估;网络攻击模型;攻击图;粗糙图;粗糙网络

中图分类号: TP393.08; TP309.5 **文献标志码:** A

Network risk assessment model based on rough graph

HUANG Guang-qiu, LI Yan

(School of Management, Xi'an University of Architecture and Technology, Xi'an Shaanxi 710055, China)

Abstract: Concerning the characteristic that the information system obtained from doing network security analysis is rough and incomplete, this paper compared the process of attack to the rough and uncertain relationship mining process by analogy, and proposed a new network risk assessment model based on rough graph. The model is made up of three parts of main contents including node rough correlation network, attack graph generation algorithm based on rough graph and network risk maximum flow analysis algorithm. In the end, this paper used a representative example of network system to explain the method of model, and verified the correctness. Model advantage analysis shows that the model can reflect the actual situation better than the previous attack graph model and risk assessment model, and the conclusion and safety recommendations are more accurate and reasonable.

Key words: network risk assessment; network attack model; attack graph; rough graph; rough network

0 引言

随着 Internet 技术以及计算机网络的飞速发展,计算机网络已经成为人类生活中不可或缺的一部分;同时,针对计算机网络信息系统的恶意攻击也越来越频繁,而且攻击方式正朝着简单化、智能化的方向发展,基于入侵检测技术的被动防御显然已经不能满足系统安全与健壮性的要求,这时一种主动的安全防御技术—网络风险评估引起了科研人员的广泛关注,其能够在攻击者入侵之前发现网络系统所存在的潜在威胁,在攻击之前评估网络的安全态势,进而采取相应的措施来保证系统安全,避免恶意攻击事件的发生。

网络风险评估主要分为两类:1)人工评估或静态评估^[1-2],以问卷的方式静态的评价目标网络的风险等级,但是该类方法容易混入主观因素,只能粗略给出网络长期所处的风险状态,缺乏对实时风险评估的自适应能力,而且不适宜于对大规模的复杂网络进行风险评估;2)自动评估或实时评估,该类方法能够自动识别系统所存在的脆弱性,对目标网络进行风险评估,具有自动、高效、实时以及易于管理等特性。目前针对自动评估的研究已经有很多,国外的研究主要是进行定性分析,多采用模型检测的方法来模拟攻击者的攻击行为,进而对网络的安全进行评估,例如:Schneider B^[3]提出的攻击图模型、特权图模型^[4-5],状态转移模型(基于状态的随机模型)^[6-8],高级随机模型^[9-12]等;国内的研究多致力于进行

量化分析,将网络的安全状态以数值的方式直观的显现出来,例如:李涛^[13]提出了一种基于免疫的网络安全风险检测模型,张永铮等人^[14-15]通过对节点关联性的研究来提高检测网络弱点和网络攻击的准确性,汪渊等人^[16]使用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。但上述安全评估模型绝大多数都是以扫描工具所得到的网络参数、连接状况、漏洞等为出发点,认为经过扫描所得到的网络模型信息都是完备的,而忽略了任何工具或者攻击者所获得的信息都是不完备的、粗糙的这一特性,例如对于同一个漏洞,不同的攻击者对其认识程度不同,采用的攻击方法可能也不同,造成的后果也很迥异。而从错综复杂的网络连接中寻求到某一特定目标的连接来进行攻击,恰可以类比为粗糙不确定性问题的关系挖掘问题。

因此本文参考文献[17,18]中对于粗糙图、粗糙网络的描述,提出了基于粗糙图的网络风险评估模型(New Network Risk Assessment Model based on Rough Graph, RNRAM),其主要包括部件粗糙网络和攻击图的粗糙图生成算法以及网络风险最大流分析三部分内容。部件粗糙网络描述了网络系统部件级上的访问逻辑关系及由于访问所导致的风险值,基于粗糙图所生成的网络攻击图给出了由于部件节点上存在脆弱性所导致的网络系统的访问关系的变化,风险最大流算法可以对整个网络的风险状况予以评价。最后本文以一个实际的例子展示了该模型的应用及相应算法的正确性,并与传统的评

收稿日期:2009-07-26。 基金项目:陕西自然科学基金资助项目(2007E217);陕西省教育厅专项基金资助项目(09JK524)。

作者简介:黄光球(1964-),男,湖南桃源人,教授,博士,主要研究方向:网络安全、计算智能、计算机仿真;李艳(1984-),男,河北承德人,硕士,主要研究方向:网络安全、电子商务实现技术。

估方法进行了比较分析。本文的主要目的在于:1)通过将粗糙图、粗糙网络的理论引入到网络风险评价中,进而提高风险评估的准确性;2)通过对部件粗糙网络的风险最大流分析确定导致网络风险最大的路径,以便向网络管理员提出最优成本的安全建议。

1 RNRAM 模型

1.1 模型定义

网络系统中,某一用户或攻击者对某一主机或服务器进行访问或攻击,实际上是对存在于主机或服务器上的某一应用程序或服务进行访问或攻击,文献[15]引入了文献[19]所提出的“安全依赖关系”,提出了网络节点关联性的概念,以此来描述两个部件之间潜在的逻辑关系。在前面研究的基础上,针对网络信息系统中的粗糙现象,本文引入了一个“节点粗糙关联图”,称之为 NRCC,下面给出其相关的定义。

定义1 部件为一个二元组:

$$C_{vs} = (v, s)$$

表示节点 v 上提供的一个部件。其中, v 为网络节点,是网络中各个独立的计算机设备; s 为主体,是这个节点所提供的用户、应用程序或服务。

定义2 部件之间的权限关系为一个三元组:

$$C_{prvl} = (C_{xi}, C_{yj}, prvl)$$

表示节点 x 上部件主体 i 在节点 y 的部件 j 上拥有 $prvl$ 权限。其中 $x, y \in V$, V 是网络中设备节点的集合; C_{xi}, C_{yj} 分别为节点 x 和 y 上的一个部件; $prvl \in \{None, Access, User, Superuser, Root\}$, 满足 $None < Access < User < Superuser < Root$ 的关系。

定义3 部件之间除权限之外的所有连接关系为一个三元组:

$$C_{conn} = (C_{xi}, C_{yj}, L)$$

表示节点 x 上的部件主体 i 在节点 y 的部件主体 j 上除了权限关系 $prvl$ 外还拥有连接关系 L ; 其中 L 是部件之间的普通连接关系集合,例如所使用的网络协议关系、部件之间的所属关系等。

定义4 表示部件之间访问关系的连接弧为一个有向边:

$$e_k^a(C_{xi}; C_{yj}) = (C_{xi}, C_{yj}, C_{prvl}, C_{conn})$$

其中: $k \in [1, +\infty]$ 为相同两个部件之间不同连接的索引标识; a 为方向属性,若弧带正方向,即 a 为正,则 $e_k^+(C_{xi}; C_{yj})$ 表示节点 x 上的部件主体 i 在节点 y 的部件主体 j 上具有 C_{prvl} 的访问权限,同时具有 C_{conn} 的连接关系,此时称 C_{xi} 为 $e_k^+(C_{xi}; C_{yj})$ 的头, C_{yj} 为 $e_k^+(C_{xi}; C_{yj})$ 的尾; 若弧带负方向,即 a 为负,则 $e_k^-(C_{xi}; C_{yj})$ 表示表示节点 y 上的部件主体 j 在节点 x 的部件主体 i 上具有 C_{prvl} 的访问权限,同时具有 C_{conn} 的连接关系,此时称 C_{yj} 为 $e_k^-(C_{xi}; C_{yj})$ 的头, C_{xi} 为 $e_k^-(C_{xi}; C_{yj})$ 的尾。

利用上述的四个定义,我们可以对实际的物理连接网络进行抽象,抽象为一个有向逻辑连接图,但是在该图中没有对两个部件的连接进行细分,粗糙地认为两个部件之间的连接是同一个类型的,不加区别,这与实际是不相符的^[17]。例如在图1(a)中通过主机A上的部件 m 可以对主机B上的部件 n 进行攻击,攻击的方式有3种:特洛伊木马(虚线表示)、口令破解(实线表示)和缓冲区溢出攻击(点线表示),且每种攻击方式又有多种攻击方法(例如:口令破解包括字典攻击和暴力攻击两种方式),但是由于攻击者的水平较低不能使用缓冲区溢出进行攻击,只能使用口令破解和现有的特洛伊木马植入工具进行简单攻击(如图1(b)所示)。若采用粗糙图的相关理论进行分析^[17-18],则图1(a)可认为是对于此攻击的论域图,图1(b)即为攻击者经过扫描、分析后所获得的粗糙图。

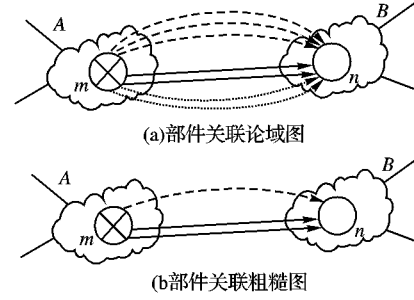


图1 基于部件的粗糙关联图

由传统图向粗糙图进行转化是在顶点属性的基础上对边集增加了属性的描述,同样,我们在上述的定义基础上增加属性集 \mathcal{R} 即可获得基于部件节点的粗糙关联图,定义如下。

定义5 节点粗糙关联图(Node Rough Correlation Graph, NRCC)为一个四元组:

$$NRCC = (V, C, E, \mathcal{R})$$

其中: $V = (v_1, v_2, \dots, v_n)$ 是网络系统中各个独立的计算机的集合; C 是当前节点所拥有的部件集合; $E = \cup e_k^a(C_{xi}; C_{yj})$ 表示当前部件节点之间的访问关系的边的集合; $\mathcal{R} = (r_1, r_2, \dots, r_{|\mathcal{R}|})$ 是属性集,用来描述当前网络所构成的知识系统,且 \mathcal{R} 中包含顶点属性 (C_{xi}, C_{yj}) 。

文献[15]和[19]等均明确指出“安全依赖关系”,“网络节点关联”等可以通过手动或自动的方式来构建,本文也足可以相信能获得网络的部件节点、边、属性集等相关信息来构建粗糙关联图,如何构建粗糙关联图不是本文研究的重点。

这样对于 \mathcal{R} 上的任意属性集 $R \subseteq \mathcal{R}$, E 中的元素(边)就可以分为不同的等价类 $[e_k^a(C_{xi}; C_{yj})]_R$, 同样我们可以使用两个精确图 $NRCC(T) = (W, NRCC(X))$ 和 $NRCC(T) = (W, NRCC(X))$ 来对粗糙图 NRCC 进行定义:

$$NRCC = \{e_k^a(C_{xi}; C_{yj}) \in E \mid [e_k^a(C_{xi}; C_{yj})]_R \subseteq X\}$$

$$NRCC = \{e_k^a(C_{xi}; C_{yj}) \in E \mid [e_k^a(C_{xi}; C_{yj})]_R \cap X \neq \emptyset\}$$

其中 $T = (W, X)$ 是粗糙图 NRCC 的子图, $W \subseteq V, X \subseteq E$ 。

这里的 NRCC 上、下近似图根据实际情况,可能会有一些不同的现实意义,例如:若决策属性为是否能够确定进行攻击,则 NRCC-下近似图就代表那些已经公开了漏洞攻击方法,攻击难度不大的攻击方式;而 NRCC-上近似图则表示没有明确的攻击工具和方法,攻击难度较大只有特定的专业人士才能发起的攻击,但是这样的攻击往往会产生巨大的破坏风险,为了对这些风险进行评估,本文在节点粗糙关联图 NRCC 边中增加由于访问所导致的风险值权重,构成了节点粗糙关联网络,相关定义如下:

定义6 由于访问关系的存在一个部件对另一个部件产生的影响为一个三元组:

$$C_{effect} = (e_k^a(C_{xi}; C_{yj}), P, W)$$

表示由代表访问关系的一条边所带来的风险值,其中: $P \in [0, 1]$ 表示头节点对尾节点成功攻击的概率; $W \in [0, +\infty]$ 表示由于头节点对尾节点访问关系的产生所导致的影响程度。本文使用 P 与 W 的乘积作为风险值^[20-21], 即: $Risk(e_k^a(C_{xi}; C_{yj})) = P \times W$, P 和 W 的量化标准参照文献[15]和[19]中的分类描述及量化,这里不再讨论。

定义7 将节点粗糙关联图连同访问导致的风险权值称为节点粗糙关联网络(Node Rough Correlation Network, NRCCN), 记为 $NRCCN = (NRCC, C_{effect})$ 。对于粗糙网络有邻接矩阵、边目录等多种表示方法^[17-18], 本文为了节省存储空间且方便后面算法分析,使用弧目录的方式存储。

基于上述定义可以将物理连接网络抽象成一个包含主机

节点、部件节点、属性集、部件之间的连接弧及其上风险权值的粗糙网络,仍可以使用文献[15]所提出的风险传播算法等来对每个部件节点的风险传播情况进行分析。但本文试图说明网络攻击中存在的粗糙现象及其对攻击者的攻击过程和网络的整体安全造成的影响,因此本文提出了两种分析方法:攻击图的粗糙图生成算法以及网络风险最大流算法。

1.2 基于粗糙图的攻击图生成算法

传统的攻击图中包含着对网络系统的所有攻击路径,一条攻击路径就是攻击者针对攻击目标进行一次攻击时所进行的部件访问先后逻辑关系。在传统的攻击图生成算法中是否存在一条边是通过能否满足前件集中的一定约束条件来判断的,但是在本文所提出的节点粗糙关联图大为不同,由于引入了粗糙性,两个部件之间是否存在一条边是由攻击者当前的知识状态水平所决定的,例如:攻击者认为通过缓冲区溢出攻击即可通过某一部件节点 m 获取某一部件节点 n 的Root权限,则在节点 m 和 n 之间就存在着一条有向边。为了描述节点粗糙关联图中攻击者的攻击逻辑关系和攻击能力,本文参照文献[22]中使用初始粗糙集构造粗糙图,进而挖掘粗集之间动态关系的方法,提出了基于粗糙图的攻击图生成算法。

在给出算法之前首先要对攻击者的攻击能力进行定义,在传统的攻击图中攻击者的攻击能力是确定的,即要不就确定能够进行攻击(存在一条到目标节点的攻击路径),要不就确定不能对目标节点进行攻击。但是在节点粗糙关联图中节点之间的有向弧只是对攻击者当前知识水平的描述,依据粗糙集的特性,本文使用可能性有向类路和确定性有向类路来对攻击者攻击能力的上、下限进行定义。

定义8 部件 v_0 与部件 v_n 存在着确定性攻击路径 $Can_Attack_Path(v_0, v_n, NRCG) = TRUE$,如果在部件 v_0 和部件 v_n 之间存在着一个由 $NRCG$ 中的有限非空序列组成的确定性有向类路^[18]:

$$Path = v_0[e_k^a(v_0:v_1)]_R v_1[e_k^a(v_1:v_2)]_R v_2 \cdots, \\ v_{n-1}[e_k^a(v_{n-1}:v_n)]_R v_n$$

其各项交替的为 $NRCG$ 中部件节点和 \overline{NRCG} 中的等价类, $R \subseteq \mathcal{R}; \forall i, j = 0, 1, \cdots, n$ 有 $[e_k^a(v_i:v_{i+1})]_R$ 与 $[e_k^a(v_j:v_{j+1})]_R$ 都属于由 R 所确定的同一弧等价类,这样就保证了攻击路径在部件节点之间的连续性;且若 $\forall i \neq j, i, j = 0, 1, \cdots, n-1$ 都有 $v_i \neq v_j$,即攻击过程遵从单调性假设。

定义9 部件 v_0 与部件 v_n 存在可能性攻击路径 $Possible_Attack_Path(v_0, v_n, NRCG) = TRUE$,如果在部件 v_0 和部件 v_n 之间存在着一个由 $NRCG$ 中的有限非空序列组成的可能性有向类路^[18]:

$$Path = v_0[e_k^a(v_0:v_1)]_R v_1[e_k^a(v_1:v_2)]_R v_2 \cdots, \\ v_{n-1}[e_k^a(v_{n-1}:v_n)]_R v_n$$

其各项交替的为节点粗糙关联图($NRCG$)中部件节点和 \overline{NRCG} 中的等价类, $R \subseteq \mathcal{R}; \forall i, j = 0, 1, \cdots, n-1$ 有 $[e_k^a(v_i:v_{i+1})]_R$ 与 $[e_k^a(v_j:v_{j+1})]_R$ 都属于由 R 所确定的同一弧等价类,这样就保证了攻击路径在部件节点之间的连续性;且若 $\forall i \neq j, i, j = 0, 1, \cdots, n-1$ 都有 $v_i \neq v_j$,即攻击过程遵从单调性假设。

显然定义8中的确定性攻击路径的集合 $\cup Can_Attack_Path(v_0, v_n, NRCG)_{TRUE}$ 是当前知识水平下攻击者能够确定进行攻击的攻击路径集合;定义9中的可能性攻击路径的集合 $\cup Possible_Attack_Path(v_0, v_n, NRCG)_{TRUE}$ 是当前知识水平下攻击者所有可能进行攻击的攻击路径集合。这样要对当前粗糙状态下的攻击能力进行评价就要生成所有的确定性攻击路径和可能性攻击路径,其可分别由粗糙

代数中的交算子 $\underline{R}(E_{\cap})$ 和 $\overline{R}(E_{\cup})$ 来构造^[22],要生成节点粗糙关联图中任意两个部件节点之间的所有确定性攻击路径和可能性攻击路径,可以参照经典图论中生成任意两点间最小路径的方法,下面给出算法的伪代码表示。

算法 Genarate_roughAttackGraph($NRCG, step, nowNode, startNode, endNode$)。

/* Pre: 经过自动或手动生成的节点粗糙关联图($NRCG$);

Post: 所有可能性攻击路径组成的上近似粗糙攻击图 $U_AttackGraph$ 和所有确定性攻击路径组成的下近似粗糙图 $L_AttackGraph$;

Uses: 使用深度优先的递归查找任意两点之间的攻击路径 */

```
1) 初始化:  $U\_AttackGraph = \emptyset; L\_AttackGraph = \emptyset; n =$ 
    $|NRCG.C|; bVisit[1..n] = false;$ 
2) 对于  $NRCG$  中的任意两个节点调用如下函数;
3) Genarate_roughAttackGraph( $NRCG, step, nowNode, startNode,$ 
    $endNode$ )
4) {
5) If ( $nowNode = endNode$ )
6) {
7) //将新的攻击路径加入到攻击图中;
8)  $U\_AttackGraph = U\_AttackGraph \cup U\_AttackPath;$ 
9)  $L\_AttackGraph = L\_AttackGraph \cup L\_AttackPath;$ 
10) //将当前的攻击路径置空
11)  $U\_AttackPath = \emptyset;$ 
12)  $L\_AttackPath = \emptyset;$ 
13) }
14) else
15) {
16) For ( $i = 1; i < n; i++$ )
17) {
18) If ( $e_k^a(C_{nowNode}; C_i).k > 0$ ) && ( $bVisit[i] = false$ )
   //有边连接且访问标志为假
19) {
20) //使用交算子和并算子进行运算生成攻击路径
21)  $U\_AttackPath = U\_AttackPath \cup i \cup (\overline{R}(nowNode) \cap$ 
    $\overline{R}(i));$ 
22)  $L\_AttackPath = L\_AttackPath \cup i \cup (\underline{R}(nowNode) \cap$ 
    $\underline{R}(i));$ 
23)  $bVisit[i] = true$ 
24) //递归调用
25) Genarate_roughAttackGraph( $NRCG, step + 1, i, startNode,$ 
    $endNode$ )
26)  $bVisit[i] = false$ 
27) }
28) }
29) }
```

上述算法使用递归的思想在节点粗糙关联图中的任意两个部件顶点所构成的粗糙集之间分别使用并算子和交算子来构造可能性和确定性攻击路径,其中6)~13)行是当搜索到目标节点时将路径加入到攻击图中;第16)~28)行中首先对两个节点之间是否存在边和节点 i 是否已经被遍历过进行判断,如符合条件则使用并算子和交算子来构造可能性和确定性攻击路径,并修改遍历标志后进行递归调用。

1.3 网络风险最大流算法

基于粗糙图的攻击图生成算法可以给出当前知识水平下的攻击路径,但是作为网络的管理员似乎对那些能够对网络造成最大破坏的路径感兴趣,而且需要知道当前网络所处的风险等级,那么仅仅对节点粗糙关联图($NRCG$)进行分析是不够的,下面提出的网络风险最大流算法从不同的角度,依托

节点粗糙关联网络(NRCN),得到任意两个部件节点之间的确定性风险最大流和可能性风险最大流帮助网络管理员进行安全分析。

已经有大量的文献将传统图论的算法成功推广到粗糙图中^[18,22],本文提出的网络风险最大流算法以自动或手动生成的节点粗糙关联网络(NRCN)为论域图,使用P算法^[23]对边集进行分类,进而应用成熟的L算法和R算法^[23]生成上、下近似网络,最后采用Ford-Fulkerson算法^[24]进行风险最大流分析(Risk Maximum Flow Analysis Algorithm, RMFLA),RMFLA算法的具体实现过程如下。

输入:当前网络的知识系统 (U, \mathcal{R}) ,系统的节点粗糙关联网络 $NRCN = (W, X)$,其中的 V, C ,是节点集合, $E = \cup e_k^a(C_{x_i}; C_{y_j})$ 是边集,属性集 $R \subseteq \mathcal{R} = (r_1, r_2, \dots, r_{|\mathcal{R}|})$ 同时包含顶点属性和方向属性以及风险权重属性;

输出:确定性风险最大流 $RMFLA_{E_m}^*(v_s, v_t)$ 和可能性风险最大流 $RMFLA_{E_m}^*(v_s, v_t)$;

步骤1 通过手动或自动的方法生成节点粗糙关联网络(NRCN),输入相应的节点集 V, C ,属性集 \mathcal{R} ,边集 E ;并进行相应的初始化操作;

步骤2 对输入的边集 E 使用经典的P算法,得到所有的弧等价类集合 $E/R = \{E_1, E_2, \dots, E_n\}$;

步骤3 对于 X 分别使用经典的L算法和R算法,得到 X 的下近似 $NRCN(T) = (W, NRCN(X))$ 和上近似 $NRCN(T) = (W, NRCN(X))$;

步骤4 对于任意两个部件节点 v_s, v_t ,依据下近似网络 $NRCN(T) = (W, NRCN(X))$,按照弧等价类 $E_m(m = 1, 2, \dots, n)$ 构造类图 T_{E_m} ,对 T_{E_m} 应用Ford-Fulkerson算法,若自出发点 v_s 到收点 v_t 的任一弧等价类都非可达则无确定性最大类流,否则可得自出发点 v_s 到收点 v_t 的确定性 E_m 风险最大流 $RMFLA_{E_m}^*(v_s, v_t)$;

步骤5 对于任意两个部件节点 v_s, v_t ,依据上近似网络 $NRCN(T) = (W, NRCN(X))$,按照弧等价类 $E_m(m = 1, 2, \dots, n)$ 构造类图 T_{E_m} ,对 T_{E_m} 应用Ford-Fulkerson算法,若自出发点 v_s 到收点 v_t 的任一弧等价类都非可达则无可能性最大类流,否则可得自出发点 v_s 到收点 v_t 的可能性 E_m 风险最大流 $RMFLA_{E_m}^*(v_s, v_t)$ 。

步骤6 算法结束。

本算法的实现过程是对粗糙网络类最大流算法的扩展,使其能够对基于部件节点的粗糙关联网络进行分析,算法的充要性证明这里不再论述^[18],而且算法使用经典的P算法(时间复杂度为 $O(|E|^2)$),L算法和R算法(时间复杂度为 $O(|E|)$),以及Ford-Fulkerson算法(时间复杂度为 $O(|W|^2 |X|)$),所以其时间复杂度应该与文献^[18]的算法相同,不会超过 $O(|E|^4)$ 。

2 模型应用与分析

为了对本文提出的模型及相应算法的正确性进行验证,说明本模型在网络风险评估中的应用方法及优势,本章给出了一个利用本模型对网络系统进行实例分析的例子。

2.1 模型应用

本文所采用的试验网络如图2所示,其由网页服务器(WebSever)、数据库服务器(DBSever)以及文件服务器(FileSever)组成,网络为交换网络,各服务器与外界通过防火墙使用TCP/IP协议相互连接。其中的WebSever提供Appach和HTTP服务,但是HTTP服务上存在着NULL字符远程缓冲

区溢出漏洞;DBSever提供User和SSH服务,但是User上存在着弱密码漏洞,SSH服务存在着畸形密码内存破坏漏洞。假设攻击者Eve的攻击目标是位于FileSever上的Doc1的Root权限,但是攻击者目前只能获得Access权限,要达到此目的就要获得位于WebSever上的HTTP的Root权限或位于BDSever上SSH的Root权限。

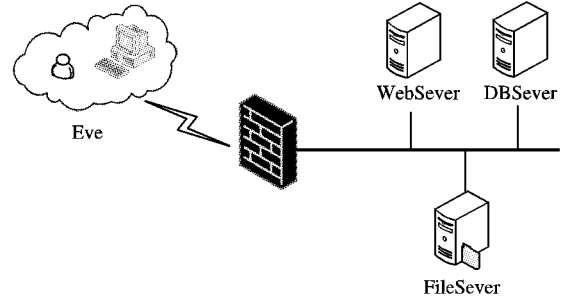


图2 实验网络拓扑结构

上面的试验网络中包含着三种脆弱性漏洞:缓冲区溢出漏洞、弱密码漏洞、畸形密码内存破坏漏洞。由于每种方法有不同的攻击方法所以可得到本实验网络的论域图(如图3(a)所示,其中的实线表示正常的访问关系,点线表示对漏洞的攻击所产生的访问关系,由于有多种攻击方法,所有可能有多条点线);但是由于攻击者的攻击水平较浅,只能确定使用暴力攻击和简单的组合攻击对存在着弱密码漏洞的DBSever>User进行攻击和使用缓冲区溢出漏洞攻击工具对WebSever.Http进行攻击(图3(b)中的点线所示),除此之外的攻击方式只是略知一二,能否成功攻击不能确定(图3(b)中点的虚线所示)。

使用算法Generate_roughAttackGraph可分别生成下、上近似粗糙攻击图(图3(c),(d)所示),自图3(c)的下近似粗糙攻击图可以看到两条确定能对FileSever.Doc1进行攻击的路径:1)Eve利用DBSever>User上的弱密码漏洞获得其Root权限,进而获得SSH的Root权限后进行操作;2)Eve访问WebSever.Apach后利用WebSever.Http的缓冲区溢出漏洞获得HTTP的Root权限后获得FileSever.Doc1的Root权限。在图3(d)所示的上近似粗糙攻击图中可以看到由于目前知识水平下对攻击者的最大攻击能力不能准确判定,就导致了许多的可能攻击方式的出现,进而导致了多条攻击路径。

假设攻击者在现有知识水平下,在部件节点之间所能采用的连接手段包括 a_1, a_2, a_3 三种方式: $a_1 = \{a_{11}, a_{12}, a_{13}\}$,其中 a_{11} 代表以管理员的身份进行登录, a_{12} 代表以普通用户的身份进行登录, a_{13} 代表以注册用户的身分登录,但不能执行相应命令; $a_2 = \{a_{21}, a_{22}\}$,其中 a_{21} 表示使用暴力攻击的方式进行弱密码攻击, a_{22} 表示使用组合攻击的方式对弱密码进行攻击; $a_3 = \{a_{31}, a_{32}\}$, a_{31} 表示针对溢出漏洞采用专门的工具进行攻击, a_{32} 表示针对溢出漏洞自己编写攻击代码进行攻击。则可得实验网络粗糙图(图3(b))弧目录的表示形式,如表1所示。

表1 试验网络粗糙图的弧目录表示形式

部件节点	部件节点					
	Eve	Apach	HTTP	User	SSH	Doc1
Eve		a_{12}		a_{12}, a_{21}, a_{22}		
Apach			a_{11}, a_{31}, a_{32}	a_{13}, a_{21}, a_{22}	a_{13}, a_{32}	
HTTP						a_{12}
User					a_{12}, a_{13}, a_{32}	
SSH			a_{12}, a_{13}, a_{32}			a_{12}, a_{13}
Doc1						

实际上由于攻击的难度不同,攻击的成功概率也会不同,但为了突出本文的实验效果,假设所有边的概率均相等且为 1,即 $P = 1$,认为每次攻击都是成功的, W 的量化参考文献

[14] 中的表 1 对于网络节点关联性 (Network Node Correlation, NNC) 的描述,即可的本文试验粗糙网络的弧目录表示形式,如表 2 所示。

表 2 试验粗糙网络的弧目录表示形式

部件节点	部件节点					
	Eve	Apach	HTTP	User	SSH	Doc1
Eve						
Apach	0.6					
HTTP		0.6, 0.1, (0.5, 0.8)			0.2, (0.3, 0.9)	
User	0.6, (0.3, 0.7)	0.2, (0.1, 0.2)				
SSH		0.1, (0.1, 0.3)		0.5, (0.1, 0.2)		
Doc1			(0.3, 0.6)		(0.1, 0.3)	

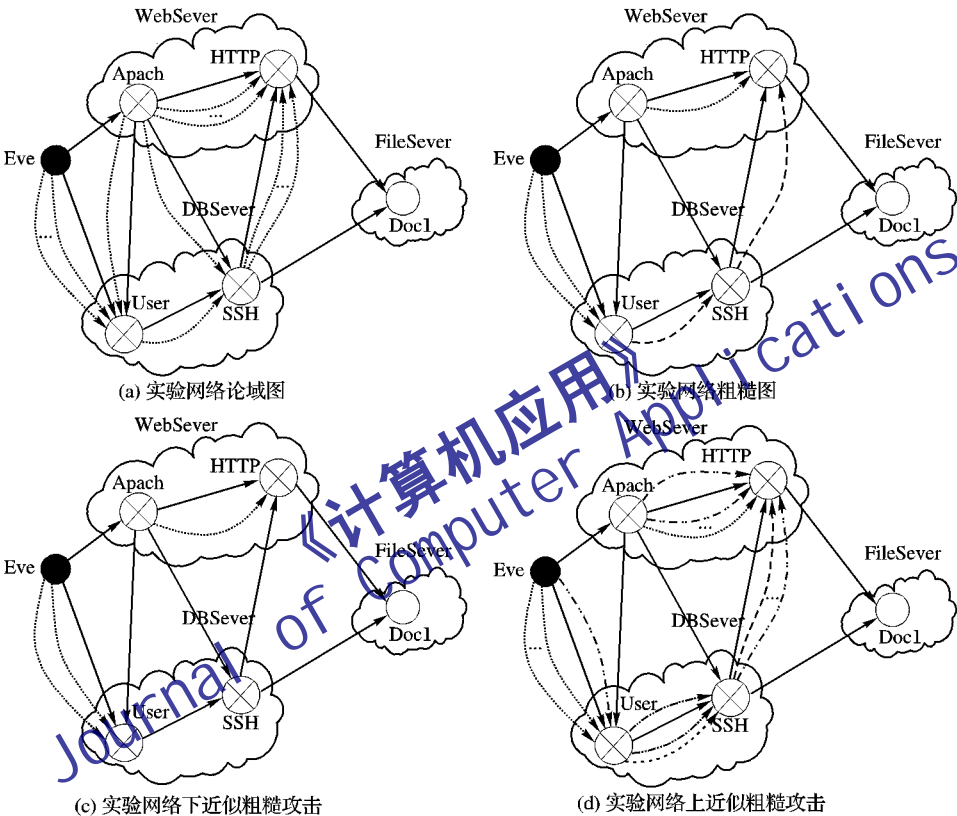


图 3 实验网络建模结果

应用算法 RMFLA 可得确定性风险最大流以及可能性风险最大流如表 3、4 所示。

表 3 确定性风险最大流

部件节点	部件节点					
	Eve	Apach	HTTP	User	SSH	Doc1
Eve						
Apach	0.6					
HTTP		0.7			0.6	
User	0.5	0.1				
SSH		0.2		0.3		
Doc1			0.3		0.2	

将上述分析进行综合可知,攻击者 Eve 对当前网络能够造成的最大风险确定性攻击路径为:Eve 首先通过普通用户的身份登录 Apach 后利用 HTTP 上的缓冲区溢出漏洞获得权限后对 Doc1 进行访问,虽然若能对 SSH 进行攻击则破坏性会更大,但是由于 SSH 的攻击难度较高攻击者知识不够不能确定进行攻击,相反的可能性最大风险攻击路径就包含这种情况:Eve 首先通过普通用户的身份登录 Apach 后利用 SSH

上的内存畸形密码漏洞进行攻击,获得权限后再利用 HTTP 上的缓冲区溢出漏洞获得 HTTP 的 Root 权限后对 Doc1 进行任意操作。若对风险最大流取大来获得网络的风险最大流则可知网络可能受到的确定性最大风险为 0.5(如表 3 所示),可能性最大风险为 0.9(如表 4 所示)。

表 4 可能性风险最大流

部件节点	部件节点					
	Eve	Apach	HTTP	User	SSH	Doc1
Eve						
Apach	0.6					
HTTP		0.8			0.9	
User	0.7	0.2				
SSH		0.3		0.5		
Doc1			0.6		0.3	

2.2 模型优势分析

上节给出了模型的使用过程及分析结果,本节将从分析结果的合理性及安全建议的合理性和以往的攻击图、风险分析模型进行对比分析说明本模型的优势。

1) 分析结果合理性。传统的攻击图生成模型使用前件集判断攻击条件是否成立,若成立,则攻击图存在一条对应的边来对攻击进行表示,并使用后件集对攻击所造成的影响进行描述。但是在这些攻击图模型中没有对图中各条边加以区分,认为对同一漏洞的攻击造成的影响是相同的,这与实际极为不符,例如同样针对缓冲区溢出漏洞进行攻击,攻击者可使用已有的攻击工具进行攻击,或自己根据实际情况编写相应攻击代码,后面一种攻击造成的影响可能会远远大于前面使用现有的工具进行的攻击,这是由于攻击者的知识水平不同所造成的,而在进行网络攻击分析时,由于各方面的原因这种粗糙性大量存在,在本模型中将粗糙集理论引入攻击分析中,对于同一种攻击的不同攻击方法加以区别,并通过属性集对攻击条件和攻击结果进行描述,根据当前的知识水平来确定攻击者所能进行的确定性攻击和可能性攻击,以此区间来对攻击者的攻击能力进行描述,并不盲目夸大或缩小攻击者的攻击能力,与此同时,应用相应的风险最大流算法可对攻击影响进行量化后所形成的部件关联粗糙网络进行分析,得到网络受到确定性攻击和可能性攻击的大小等相应结论,上节的实例分析可以明显看出本模型的评估结论更为准确、实用。

2) 安全建议合理性。进行网络安全风险评估的目的在于:在网络的攻击者攻击之前找到可能的攻击路径并采取相应的措施,来保证网络的正常运行,因此如何对风险分析的结果进行处理,提出合理的安全建议是一个十分重要的方面,而传统的分析模型大部分只是对分析模型进行改进,往往忽略了对此的分析,再者依据传统的分析方法例如最小割集,最大关键度节点等分析方法只是简单分析节点在攻击路径中的出现次数,以此来简单的判断节点的重要性,例如对于实验网络,传统的分析方法是向管理员提出对 HTTP 和 User 的漏洞进行修复的建议,这样开销会很大,但根据本模型的风险最大流分析知道攻击者所能造成的最大风险是由于其通过 Apache 攻击 SSH 后获得 HTTP 的权限进而进行攻击的,那么管理员可以简单地降低 Apache 对外网的访问权限级别同时对 SSH 的内网漏洞进行修复即可,如此一来攻击者对此网络的任何攻击都无从下手,能够得出这样的合理性结论正是由于本模型对攻击过程中的粗糙特性予以了考虑,同时使用了合理的粗糙攻击图生成算法以及风险最大流分析方法。

3 结语

为了对网络攻击过程中的粗糙特性进行准确描述,本文提出了一个由部件粗糙网络和攻击图的粗糙图生成算法以及网络风险最大流分析三部分主要内容所组成的基于粗糙图的网络攻击分析模型,并以一个实际的例子对模型应用方法进行了阐述,通过和传统分析方法的比较分析得知,由于加入了粗糙性的描述,本模型能更加准确地反映实际情况,同时提出的算法能够判别网络将会受到的确定性和可能性攻击,进而向管理员提出更加合理、优化的安全建议。

参考文献:

- [1] BENNETT S P, KILAY M P. An application of qualitative risk analysis to computer security for the commercial sector[C]// Proceedings of the 8th IEEE Annual Computer Security Applications Conference. San Antonio: IEEE Computer Society Press, 1992: 64-73.
- [2] VISINTINE V. An introduction to information risk assessment[R]. SANS Institute, 2003.
- [3] SCHNEIER B. Secrets and lies: Digital security in a networked world[M]. New York: John Wiley and Sons, 2000.
- [4] DACIER M. Towards quantitative evaluation of computer security[D]. Toulouse, France: Institute National Polytechnique de Toulouse, 1994.
- [5] ORTALO R, DESWARTE Y, KANICHE M. Experimenting with quantitative evaluation tools for monitoring operational security[J]. IEEE Transactions on Software Engineering, 1999, 25(5): 633-650.
- [6] PORRAS P A, KEMMERER R. A penetration state transition analysis: A rule-based intrusion detection approach[C]// Proceedings of the 8th Annual Computer Security Applications Conference. New York: IEEE, 1992: 220-229.
- [7] STEVENS F, COURTNEY T, SINGH S, et al. Model-based validation of an intrusion-tolerant information system[C]// Proceedings of the 23rd Symposium on Reliable Distributed Systems. New York: IEEE, 2004: 184-194.
- [8] MADAN B, POPSTOJANOVA K, VAIDYANATHAN K, et al. A method for modeling and quantifying the security attributes of intrusion tolerant systems[J]. Performance Evaluation, 2004, 56(1): 167-186.
- [9] HELMER G, WONG J, SLAGELL M, et al. Software fault tree and colored Petri net based specification, design and implementation of agent based intrusion detection system[J]. Requirements Engineering, 2000, 7(4): 207-220.
- [10] McDERMOTT J. Attack net penetration testing[C]// Proceedings of 2000 New Security Paradigms Workshop. New York: ACM, 2000: 15-21.
- [11] DACIER M, DESWARTE Y, KANICHE M. Quantitative assessment of operational security: Models and tools[R]. Laboratory for Analysis and Architecture of Systems, 1996.
- [12] McDERMOTT J. Attack-potential-based survivability modeling for high-consequence systems[C]// Proceedings of the 3rd IEEE International Workshop on Information Assurance. New York: IEEE, 2003: 119-130.
- [13] LI TAO. An immunity based network security risk estimation[J]. Science in China Series E: Information Sciences, 2005, 35(8): 798-816.
- [14] 张永铮, 方滨兴, 迟悦, 等. 网络风险评估中网络节点关联性的研究[J]. 计算机学报, 2007, 30(2): 234-240.
- [15] 张永铮, 方滨兴, 迟悦, 等. 用于评估网络信息系统的风险传播模型[J]. 软件学报, 2007, 18(1): 137-145.
- [16] 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[J]. 小型微型计算机系统, 2003, 24(12): 2082-2085.
- [17] 何童, 卢昌荆, 史开泉. 粗糙图与它的结构[J]. 山东大学学报: 理学版, 2006, 41(6): 46-50.
- [18] 何童, 史开泉. 粗糙网络及其应用[J]. 系统工程与电子技术, 2009, 31(3): 588-592.
- [19] YAU S S, ZHANG XINYU. Computer network intrusion detection, assessment and prevention based on security dependency relation [C]// Proceedings of 23rd International Computer Software and Applications Conference. Washington, DC: IEEE Computer Society Press, 1999: 86-91.
- [20] BISWAS G, DEBELAK K A, KAWAMURA K. Applications of qualitative modeling to knowledge-based risk assessment studies [C]// Proceedings of the 2nd International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems. New York: ACM, 1989: 92-101.
- [21] STRUTT J E, PATRICK J D, CUSTANCE N D E. A risk assessment methodology for security advisors [C]// Proceedings of the 29th IEEE Annual International Carnahan Conference on Security Technology. Washington, DC: IEEE Computer Society Press, 1995: 225-229.
- [22] 何童, 史开泉. 粗糙集代数关系的图结构分析[J]. 系统工程与电子技术, 2008, 30(9): 1679-1682.
- [23] 张文修, 吴伟志, 梁继业. 粗糙集理论与分析方法[M]. 北京: 科学出版社, 2003.
- [24] EDMONDS J, KARP R M. Theoretical improvements in algorithmic efficiency for network flow problem[J]. Journal of the ACM, 1972, 19(2): 218-264.