计算机研究与发展
Journal of Computer Research and Development
ISSN 1000-1239/CN 11-1777/TP
48(6): 945-954, 2011

基于威胁传播模型的层次化网络安全评估方法

陈 锋[1,2] 刘德辉[2] 张 怡[2] 苏金树[2]
[1](第二军医大学网络信息中心 上海 200433)
[2](国防科学技术大学计算机学院 长沙 410073)
(chenfeng@nudt.edu.cn)

A Hierarchical Evaluation Approach for Network Security Based on Threat Spread Model

Chen Feng[1,2], Liu Dehui[2], Zhang Yi[2], and Su Jishu[2]
[1](*Network Information Center*, *Second Military Medical University*, *Shanghai* 200433)
[2](*College of Computer*, *National University of Defense Technology*, *Changsha* 410073)

Abstract Network system is generally faced with invasion of the external and internal threat agents. Moreover, threat agents have the capability of spreading threats via the interrelation among vulnerabilities and components in the network, bringing about potential threats. Designing a reasonable model to identify, analyze and quantitatively measure the consequences resulting from potential threats is one of the main challenges that the research of network security evaluation faces. For this issue, a hierarchical evaluation approach based on the threat spread model for the network security is proposed. Firstly the threat spread model is put forward to identify the threat agents, analyze the spread paths of threats, and predict potential threats. The threat spread model includes target network model, threat agent model, threat spread graphs and threat spread algorithm. On this basis, the security measure model is presented to compute the danger indexes of services, hosts and network system respectively. The security measure model is composed of spread graphs, metrics, metric computing functions and index computing functions. Based on the novel approach, the prototype system is implemented and applied by an enterprise local network system. The result demonstrates the correctness of the threat spread model and the advantage of the approach compared with traditional methods.

Key words network security; threat spread; security measure; danger index; hierarchical evaluation

摘 要 网络系统不仅面临外部和内部威胁主体的入侵,同时威胁主体会利用脆弱点间、网络组件间的相互作用关系进行威胁传播,产生严重的潜在威胁.设计合理的模型对潜在威胁进行识别、分析,并量化测度其对网络安全的影响,是当前网络安全评估所面临的主要挑战之一.针对该问题,提出了一种基于威胁传播模型的层次化网络安全评估方法.首先提出了威胁传播模型识别目标网络系统的威胁主体,分析其传播路径,预测其对网络系统的潜在破坏;在此基础上提出了层次化网络安全测度模型来计算服务、主机和网络系统3个层次的危险指数.通过将原型系统应用于某企业局域网络系统,验证了威胁传播模型的正确性及其评估方法相比传统方法的优势.

关键词 网络安全;威胁传播;安全测度;危险指数;层次化评估

中图法分类号 TP393.08

收稿日期:2009-03-14;**修回日期**:2010-04-01
基金项目:国家自然科学基金项目(90604006)

近年来,随着企业网络的规模和复杂性不断增大,网络安全脆弱点的数量和种类也在不断增多.根据 CERT/CC 的统计,2006 年报告的脆弱点数量为 8 064,远远高于 2005 年的 5 990 件和 2004 年的 3 780件,2007 年虽略有回落但仍高达 7 236 个[1].面对每年几千个新的脆弱点,安全管理员常常因为各种原因而无法立即为网络系统打上安全补丁[2].网络中脆弱点以及威胁主体的存在是导致安全事故发生的主要原因,另一方面,除了利用单个脆弱点进行攻击以外,网络系统所面临的外部威胁和内部威胁还可能利用多个脆弱点以及网络组件之间的相互作用关系不断进行威胁传播,产生大量破坏网络系统安全策略的潜在威胁,造成更为严重的安全隐患.因此,针对网络系统中存在的各种脆弱点及其所面临的不同威胁,如何结合网络组件之间的相互作用关系,采用合理的模型对潜在威胁进行识别、分析,并量化测度它们对网络安全的影响,是当前网络安全评估所面临的主要挑战之一.

本文提出了一种基于威胁传播模型的层次化网络安全评估方法.该方法包括两个模型:威胁传播模型和层次化网络安全测度模型.首先利用威胁传播模型识别目标网络系统的威胁主体、分析其产生的传播路径、预测对网络系统的潜在破坏;在此基础上利用层次化网络安全测度模型来计算服务、主机和网络系统 3 个层次的危险指数.本文基于该方法实现了一个网络安全评估原型系统,通过将其应用于某企业局域网络系统,验证了威胁传播模型的正确性,并分析了该方法相比传统网络安全评估方法的优势.

1 相关研究

网络安全评估方法研究按照研究角度可以分为基于脆弱点的、基于威胁的和基于模型的 3 类.

基于脆弱点的网络安全评估方法利用各种脆弱点自动扫描工具发现网络中存在的脆弱点,根据各个脆弱点的危害度评估它们对网络安全的影响程度.Skaggs 等人[3]和 Wales[4]对多种网络脆弱点自动发现技术进行了综述,认为它们能够对目标网络系统进行有效定性的安全评估.Ahmed 等人[5-6]提出了一个网络安全测度框架,它不仅对网络中存在的脆弱点进行定量安全评估,同时根据其历史信息预测未来的脆弱点并对它们进行定量安全评估.基于脆弱点的方法虽然能够有效发现网络系统的脆弱点,但是它孤立地评估脆弱点,忽略了脆弱点之间的相互关系以及由此产生的潜在安全风险.

基于威胁的网络安全评估方法利用多种传感器采集网络安全事件信息,如 IDS 预警日志等,根据各种安全事件的危害度来评估它们对网络的影响程度.陈秀真等人[7]基于 IDS 海量预警信息和网络性能指标,结合服务、主机本身的重要性及网络系统的组织结构提出了一种层次网络安全威胁态势量化评估方法.Ambrosio 等人[8]开发了 SSARE 系统用于广域的计算机攻击检测和态势、响应评估.Porras 等人[9]提出基于系统任务影响的预警优先级评估方法,结合预警造成的严重后果、系统相关性和攻击目标的关键性等因素,评估预警流中每个预警的威胁程度.基于威胁的方法虽然能够实时评估和预测网络系统所面临威胁的发展态势,但是忽略了威胁与脆弱点之间的关系,即在脆弱点存在的前提下,与之对应的威胁才会产生安全风险.

基于模型的网络安全评估方法是以面向网络攻击的方式对目标网络建模,采用规则对威胁主体建模,根据二者之间的相互作用分析各脆弱点之间的关系和由此产生的潜在威胁,然后评估这些潜在威胁对网络安全危害程度.Schneier[10]提出攻击树模型,用 AND-OR 形式的树结构对攻击行为进行建模,评估网络系统安全性;Ortalo 等人[11]运用特权提升图的概念,利用通往攻击目标的不同路径表示攻击者的不同攻击过程,以此反映出攻击者提升权限的过程,并依据经验来计算入侵行为的平均攻击代价;Sheyner 等人[12-13]使用改进的模型检测方法来构建攻击图,并在攻击图基础上,利用原子攻击的平稳状态分布和 Markov 决策过程来计算攻击者完成攻击目标的最大平均概率.虽然这些方法综合考虑了威胁与脆弱点之间相互作用关系,但是没有提出有效的方法来识别威胁主体,同时缺乏从各个层次给出网络系统全局的安全评估.

本文所提出的网络安全评估方法属于第 3 类,它以 IDS 的预警日志来识别系统内部和外部威胁主体,利用可扩展的威胁传播模型来发现系统潜在威胁,从服务、主机和网络系统 3 个层次来计算危险指数,弥补了当前基于模型的安全评估方法的不足.

2 威胁传播模型

目标网络系统的威胁传播模型可描述为四元组 $SpreadModel = \langle LAN,\ ThreatAgent,\ TSAlgorithm,$

$TSGraph\rangle$,其中 LAN 是目标网络系统,$ThreatAgent$ 是网络威胁主体,它利用网络中存在的脆弱点和网络组件间的相互关系不断传播威胁,$TSAlgorithm$ 是网络威胁在目标网络系统中的传播算法,$TSGraph$ 是由网络威胁传播算法产生的威胁传播图.下面详细介绍威胁传播模型的各个元素.

2.1　目标网络建模

目标网络系统按规模和层次关系可分解为网络系统、主机、服务 3 个层次.本文从面向网络安全的角度提出了一个图 1 所示的基于属性的目标网络系统层次化模型 $LAN=A_L\cup A_H\cup A_S$.

A_L 是对目标网络系统级的属性描述集合,包括主机之间逻辑连接关系、主机之间信任关系等.

$A_H=\bigcup A_{h_i}(i\in\mathbb{N}_+)$是对主机级的属性描述集合,包括威胁主体在主机上的拥有哪些权限、能否运行任意程序、能否窃取数据以及篡改数据等.

$A_S=\bigcup A_{s_i}(i\in\mathbb{N}_+)$是对服务级的属性描述集合,包括主机上运行何种服务、服务是否会被拒绝服务攻击、服务存在何种脆弱点等.

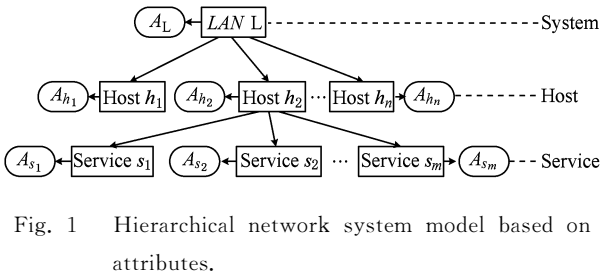

Fig. 1　Hierarchical network system model based on attributes.

图 1　基于属性的网络系统层次化模型

2.2　威胁主体建模

威胁主体模型可表示成二元组 $ThreatAgent=\langle IC, APS\rangle$,这里 IC 是威胁主体的初始能力,APS 是威胁行为模式知识库.

1) 威胁主体初始能力

目标网络系统面临的威胁主体包含内部威胁主体和外部威胁主体.本文利用 IDS 产生预警事件来识别这些威胁主体的初始能力,在网络系统边界和系统内部部署 IDS,以三元组 $A=\langle sIP,dIP,time\rangle$ 表示其产生的预警事件,其中 sIP 是攻击源主机,dIP 是攻击目标主机,$time$ 是攻击时间.该预警事件表明 sIP 受威胁主体控制,并试图利用它进行威胁传播,由此本文假设威胁主体的初始能力 IC 为它能在攻击源主机上以最高级用户权限运行任意程序.

2) 威胁行为模式知识库

威胁主体通过从初始能力出发不断改变网络系统的属性值进行威胁的传播,这些行为操作可抽象成行为模式.

定义 1. 行为模式.威胁主体通用攻击方式的抽象描述,称之为行为模式,它包含一组可被实例化的局部变量.

行为模式知识库 $APS=IAP\cup AP$,其中,IAP 为非法行为模式集合,由威胁主体针对软件脆弱点的非法渗透行为模式构成,如远程内存溢出攻击行为模式;AP 为合法行为模式集合,由威胁主体在获取主机控制权限后实施的正常操作行为模式构成,如远程登入操作行为模式.目前,行为模式需安全专家根据经验手工分析产生.

对任意行为模式 $p\in APS$,$p=\langle Name,Vuls,Var,Pre,Eff\rangle$,其中,$Name$ 是行为模式的名称,$Vuls$ 是此行为模式可利用的脆弱点集合(若 $p\in AP$,$Vuls=\varnothing$),Var 是其局部变量集合,Pre 是此行为模式可被利用时目标网络系统所必须具有的前提属性集合,Eff 是该行为模式被实施后网络系统被改变的后果属性集合.

威胁主体在威胁传播过程中,传播行为具有单调性[14]:对网络的控制能力不断增强,并且不会失去已获取的能力.因此,本文约定行为模式的 Pre 集合和 Eff 集合中表示属性的谓词不允许出现“否定词”,其直观含义就是威胁主体凭借已有的能力利用该行为模式实施威胁传播获得新能力后,现有能力不会失去.

定义 2. 传播行为.威胁主体在威胁传播过程中根据网络系统环境实例化行为模式的相关变量产生的具体操作行为,称之为传播行为.

2.3　威胁传播图

定义 3. 威胁传播图.令 AP 是一阶谓词集合,它描述目标网络系统的属性值.$(IA\cup IC\cup RA)\subset AP$.其中,$IA$ 是目标网络系统的初始属性值集合;IC 是威胁主体初始能力的属性值集合;RA 是目标网络系统在威胁主体实施传播行为后可达的属性值集合,这些可达属性值都违反了安全策略,是网络系统的潜在威胁.$Actions$ 是传播行为集合.威胁传播图 $TSGraph=(A_0\cup A_r,T,E,L)$,其中,$A_0$ 为初始节点集合,A_r 为可达节点集合,T 为传播行为节点集合,$L=(A_0\rightarrow(IA\cup IC))\cup(A_r\rightarrow RA)\cup(T\rightarrow Actions)$是标签函数,$E$ 为有向边集合.$TSGraph$ 满足下列约束:

1) $E\subset((T\times A_r)\cup((A_0\cup A_r)\times T))$,即威胁传播图的两个节点之间的关系仅包含 $A_0\rightarrow T$,$A_r\rightarrow$

T, $T\rightarrow A_r$, 其中 $T\rightarrow A_r$ 为传播行为的后果边; $A_0\rightarrow T$, $A_r\rightarrow T$ 为传播行为的前提边.

2) 对 $\forall\tau\in T$, 令 $Pre(\tau)$ 是 τ 的父节点集合, $Post(\tau)$ 是 τ 的子节点集合, 则父节点之间存在"与"关系, 且满足 $(\wedge Pre(\tau))\Rightarrow(\wedge Post(\tau))$, 表示当传播行为的所有前提都被满足后, 该传播行为成功实施, 从而使其后果集被全部满足.

3) 对 $\forall a\in A_r$, P_a 是 a 的父节点集合, 则父节点之间存在"或"关系, 且满足 $(\vee P_a)\Rightarrow a$, 表示 P_a 任何一个传播行为实施成功都会使属性值 a 被满足.

定义 4. 传播路径. 设 $path(a_g)=\tau_1\rightarrow\tau_2\rightarrow\cdots\rightarrow\tau_l(\tau_i\in T, 1\leqslant i\leqslant l)$ 是威胁传播图中的传播行为序列, 它满足下面条件, 则称该序列为到达属性值 a_g 的一条传播路径:

1) 后面任意传播行为的前提条件都是前面传播行为的后果或是初始属性值, 即 $\forall a\in Pre(\tau_i)$, $a\in\bigcup_{k=1}^{i-1}Post(\tau_k)\cup A_0$, 其中 $\tau_i\in T, 1\leqslant i\leqslant l$;

2) 任意传播行为至少存在一个后果是后面传播行为的前提, 即 $\exists b\in Post(\tau_i)$, $b\in\bigcup_{k=i+1}^{l}Pre(\tau_k)$, 其中 $\tau_i\in T, 1\leqslant i<l$;

3) 该序列中最后一个传播行为产生的后果集包含属性值 a_g, 即 $a_g\in Post(\tau_l)$.

在图 2 显示的威胁传播图例中, $A_0=\{a_1,a_2,a_3,a_4\}$, $T=\{\tau_1,\tau_2,\tau_3,\tau_4\}$, $A_r=\{a_5,a_6,a_7,a_8\}$. 威胁主体可以通过传播路径 $\tau_1\rightarrow\tau_4$ 或 $\tau_2\rightarrow\tau_3\rightarrow\tau_4$ 到达属性值 a_7, 或者通过传播路径 $\tau_2\rightarrow\tau_3$ 到达属性值 a_8.

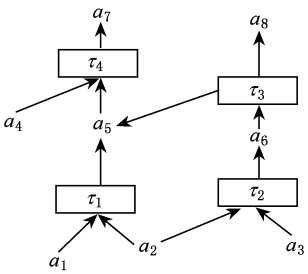

Fig. 2 Example of the threat spread graph.

图 2 威胁传播图例

2.4 威胁传播算法

对于具有脆弱点的目标网络系统, 威胁主体在进行威胁传播时可利用的行为模式集 P_APS 有两部分构成, 即 $P\_APS=P\_IAP\cup AP$, 其中 $P\_IAP\subset IAP$ 为与目标网络系统中脆弱点相关的非法行为模式集.

由于行为模式的 Pre 集合和 Eff 集合中的谓词没有"否定"量词, 故行为模式之间不存在前提互斥问题. 基于该事实, 本文提出了一种具有良好可扩展性的威胁传播算法 $TSAlgorithm$ 来产生威胁传播图, 算法详细描述如图 3 所示. 其中, 实例化函数 $Instantiate$ 根据各传播模式局部变量的域值空间实例化这些模式生产可能的传播行为集, 前提检查函数 $satisfy$ 检查传播行为 at 的所有前提是否被可达属性值集合 RA 满足, $DrawTSGraph$ 是威胁传播图绘制函数.

```
Input:
  P_APS /* Set of action patterns possibly used */
  IA /* Set of initial attributes values of the network
      system */
  IC /* Set of initial capability attributes values of
      threat agents */
Output:
  TSGraph=(A0∪Ar,T,E,L) /* threat spread graph */
Procedure TSAlgorithm
    /* AQ is the dispatch queue of attribute values */
①   AQ←IA∪IC;
    /* RA is the set of reachable attribute values of
    network system */
②   RA←∅;
③   While (AQ! =∅)
④     f←AQ.Dequeue();
⑤     RA←RA∪{f};
      /* P_APSf is the subset of action patterns P_
      APS where the action pattern's precondition set
      includes the same predicate as the predicate of f */
      /* AT is the set of spread actions from action
      patterns instantiated */
⑥     AT←Instantiate(P_APSf);
      /* Actions is the set of spread actions */
⑦     For each at∈AT  Do
⑧       If (at∉Actions)&&(satisfy(at, RA)) Then
⑨         Actions←Actions∪{at};
⑩           For each e∈at.Eff  Do
⑪             AQ.Enqueue(e);
⑫   TSGraph←DrawTSGraph(Actions,IA,IC,RA);
```

Fig. 3 Detailed description of the threat spread algorithm.

图 3 威胁传播算法 $TSAlgorithm$ 的详细描述

3 层次化网络测度模型

网络安全测度模型描述为四元组 $MetricModel=\langle TSGraph, Metric, MetricFunc, IndexFunc\rangle$, 其中, $TSGraph$ 是由威胁传播模型产生的威胁传播图, $Metric$ 是测度指标集合, $MetricFunc$ 是测度指

标计算函数集合,$IndexFunc$ 是危险指数计算函数集合.危险指数计算函数将测度指标函数计算出的测度指标值作为输入,计算出服务、主机和网络系统 3 个层次的危险指数,下面详细介绍模型中各个元素.

3.1　测度指标和计算函数

威胁传播图 $TSGraph=(A_0 \cup A_r, T, E, L)$ 展示了威胁的传播过程以及网络系统可能到达的属性值,A_r 中的属性值都违反了安全策略,是目标网络系统的潜在威胁.

测度指标主要包括潜在威胁发生概率 PV、潜在威胁对服务的危害度 DV、服务重要性 KV_S 和主机重要性 KV_H.下面阐述各测度指标函数.

1) 潜在威胁的发生概率指标函数

威胁主体利用网络系统中的脆弱点进行威胁传播.对于脆弱点 v,在利用前提都满足的情况下,它被威胁主体成功利用的概率 $p(v)$ 与该脆弱点被发现公布的时间 t(月)满足图 4 所示的分布.脆弱点被发现的初期威胁主体迅速开发攻击技术,攻击成功率快速增长,到第 β 月时到达最大值 δ,但随着时间增长,安全专家迅速开发防御技术,更新 IDS 规则库和杀毒软件规则库,它的成功率迅速下降,然后逐渐衰弱.根据该规律,本文设计脆弱点 v 成功利用概率函数如下:

$$p(v)=\begin{cases} e^{t\lambda_1}-1, & t<\beta, \\ \delta \times e^{-(t-\beta)\lambda_2}, & t\geqslant\beta, \end{cases} \tag{1}$$

这里,λ_1 是控制成功概率增长速度的参数,λ_2 是控制成功概率衰减速度的参数.

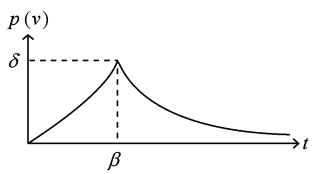

Fig. 4　Vulnerability v successfully exploiting probability $p(v)$ distribution function with respect to the time t.

图 4　脆弱点利用成功概率 $p(v)$关于时间 t 的分布

为了确定概率函数的参数,将脆弱点按其对应的行为模式进行分类,假设每类脆弱点具有相同的脆弱点利用成功概率分布函数,该函数中的参数通过分析其典型脆弱点的相关统计值来确定,如该脆弱点的发现公布时间、补丁发布时间、针对该脆弱点的攻击事件首次出现时间、各时间段的攻击发生频率和成功攻击频率等.

对于威胁传播图中的任意传播行为 τ_i,若属于非法行为模式,根据它所利用的脆弱点 v_i 可以确定其传播行为实施成功概率 $d(\tau_i)=p(v_i)$,若属于合法行为模式,则令 $d(\tau_i)=1$.

威胁主体沿着传播路径 $path(a)$到达潜在威胁 $a\in A_r$,则威胁传播到 a 的累计概率是 $path(a)$中各传播行为实施成功概率的联合概率.在威胁传播图中,一般存在多条传播路径到达,基于保守的系统安全评估原则,本文假设威胁主体具有智能性,即为了传播威胁 a,它总能选择累计概率最大的传播路径 $path^*(a)$.假设威胁行为之间相互独立,由此定义潜在威胁的发生概率指标函数:

$$PV(a)=\prod d(\tau_i), \tag{2}$$

这里 τ_i 是 $path^*(a)$中的传播行为.

2) 服务危害度指标函数

威胁 $a\in A_r$ 会分别对服务 s_i 的数据安全三要素:保密性 C、完整性 I 和可用性 A 产生危害,安全专家根据经验分别对这三要素给出危害等级 $\langle X(C), X(I), X(A)\rangle$,这里 $X(C), X(I), X(A)\in\{H, M, L\}$对应高、中、低 3 个等级.由此以向量定义威胁 a 对服务 s_i 产生的危害度:

$$DV(a, s_i)=\langle DV_C(a, s_i), DV_I(a, s_i), DV_A(a, s_i)\rangle, \tag{3}$$

这里 $DV_C(a, s_i)=w_a(X(C))$,$DV_I(a, s_i)=w_a(X(I))$,$DV_A(a, s_i)=w_a(X(A))$,$w_a:\{H, M, L\}\rightarrow\{10, 5, 0\}$是打分函数.

3) 服务重要性指标函数

本文以服务 s_i 的所属服务类型以及它的两个重要统计值,即用户数 $UN(s_i)$和平均日访问频率 $AF(s_i)$来评价服务的重要性.服务类型分为基础服务集合 BS 和非基础服务集合 IBS.基础服务是指支撑其他服务的服务,如为 Web 服务提供数据的数据库服务等.$Y:UN(s_i)AF(s_i)\rightarrow\{H, M, L\}$是分段评定函数,按照服务统计值将之评定为高、中、低 3 个等级.由此定义服务重要性指标函数:

$$KV_S(s_i)=\begin{cases} w_S(Y(UN(s_i)AF(s_i))), & s_i\in IBS, \\ 10w_S(Y(UN(s_i)AF(s_i))), & s_i\in BS, \end{cases} \tag{4}$$

这里 $w_S:\{H, M, L\}\rightarrow\{10, 6, 2\}$是打分函数.

4) 主机重要性指标函数

本文以主机 h_j 上运行的服务 s_i 的重要性 KV_S 以及该主机的网络报文平均日吞吐量 $NF(h_j)$(M/日)来评价主机的重要性.$Z:NF(h_j)\rightarrow\{H, M, L\}$是分段评定函数,按照主机的网络报文统计值将之

评定为高、中、低 3 个等级. 由此定义主机重要性指标函数:

$$KV_H(h_j) = w_H(Z(NF(h_j))) \sum_{s_i \in h_j} KV_S(s_i), \quad (5)$$

这里 $w_H:\{H,M,L\}\rightarrow\{10,6,1\}$ 是打分函数.

3.2 危险指数计算函数

定义 5. 服务危险指数. 具有一定重要程度的服务在遭受威胁主体破坏后,其对应安全策略被违反的程度,称之为服务危险指数 T_S.

威胁传播图中潜在威胁集合 A_r 根据图 1 所示的基于属性的目标网络系统层次化模型可分为服务级威胁、主机级威胁和网络系统级威胁. 对于服务 s_i,它面临的服务级威胁会直接违反它的安全策略,同时它所在的主机级威胁以及网络系统级威胁也可能会间接破坏服务的安全策略. 令集合 $DA(s_i)$ 是破坏 s_i 安全策略的所有潜在威胁集合,由此定义服务危险指数 T_S 计算函数:

$$T_S(s_i) = \sum_{Z\in\{C,I,A\}} \max_{a\in DA(s_i)} (DV_Z(a,s_i)PV(a)). \quad (6)$$

定义 6. 主机危险指数. 主机上多个不同重要程度的服务在遭受威胁主体破坏后,对主机安全策略的违反程度,称之为主机危险指数 T_H.

对于主机 $h_j=\{s_i \mid s_i$ 是运行在主机 h_j 上的服务$\}$,定义其主机危险指数计算函数:

$$T_H(h_j) = \sum_{s_i \in h_j} T_S(s_i)W_S(s_i), \quad (7)$$

这里,$W_S(s_i)$ 是对主机上运行的服务的重要性归一化处理后得到服务重要性权重,即

$$W_S(s_i) = \frac{KV_S(s_i)}{\sum KV_S(s_k)}. \quad (8)$$

定义 7. 网络系统危险指数. 网络系统内多个不同重要程度的主机在遭受威胁主体破坏后,对网络系统安全策略的总体违反程度,称之为网络系统危险指数 T_L.

对于网络系统 $l=\{h_j \mid h_j$ 是网络系统 l 内的主机$\}$,定义其危险指数计算函数:

$$T_L(l) = \sum_{h_j \in l} T_H(h_j)W_H(h_j), \quad (9)$$

这里,$W_H(h_j)$ 是对网络系统内的主机的重要性归一化处理后得到主机重要性权重,即

$$W_H(h_j) = \frac{KV_H(h_j)}{\sum KV_H(h_k)}. \quad (10)$$

根据式(6)~(10)容易确定各危险指数的值域,即 $T_S, T_H, T_L \in [0,30]$.

4 原型系统实现和实验验证

4.1 原型系统实现

在原型系统中选取了 10 个谓词从网络系统层、主机层和服务层来描述网络系统的属性,它在模型中对应的层次和详细描述如表 1 所示:

Table 1 The Predicates Used to Describe the Attributes of the Network System

表 1 描述网络系统属性的谓词

Hierarchy	Attribute	Description
Network	Connection(s: Host, d: Host, pro: Protocol, $port$: Port)	The source host s has the capability to access to the port $port$ of destination host d via the protocol pro.
Host	HasPrivilege(h:host, $priv$:Privilege)	Threat agents have the privilege $priv$ on host h.
	RunCode(h:Host, $priv$:Privilege)	Threat agents have the privilege $priv$ on host h to run code.
	InfoLeakage (h:Host, $data$:Data)	Threat agents are able to steal the data $data$ on the host h.
	DataModification(h:Host, $data$:Data)	Threat agents are able to tamper with the data $data$ on the host h.
Service	NetworkService(h:Host,sn:ServiceName, pro:Protocol,$port$:Port)	The service sn runs on the host h, which listens to the port $port$ and communicates via the protocol pro.
	Dos(h:Host, sn: ServiceName)	The service sn of the host h denies access.
	VulExists(h:Host, sn:ServiceName, $cveId$:CveID)	The vulnerability $cveId$ exists in the service sn of the host h.

图 5 是原型系统的系统结构图,其输入模块包括:由脆弱点扫描工具收集的网络系统中服务存在的脆弱点信息;由网络管理工具通过收集网络系统中路由策略、拓扑结构和防火墙规则信息分析出的主机之间网络通信的可达关系;由入侵检测系统产生的预警事件分析出的威胁主体的初始能力;由安全专家分析并提取出的威胁行为模式. 在原型系统中,我们基于公开脆弱点数据库 CVE[15] 和威胁主体的常见威胁行为,分析并提取产生了 18 种常见的行为模式,覆盖了公开脆弱点数据库 CVE 中大部分常见脆弱点.

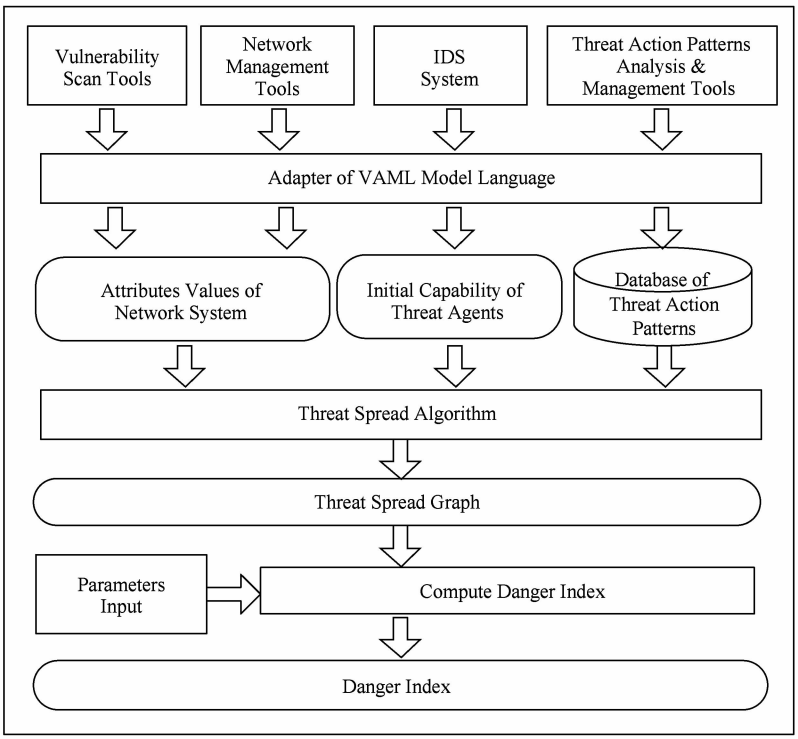

Fig. 5　The architecture of the prototype system.

图 5　原型系统结构

4.2　应用实例及正确性验证

在 2008 年 11 月 18 日,将原型系统应用于某企业局域网络进行安全评估. 图 6 是该局域网络拓扑图. 192.168.1.1/24 网段是对外交流区域,其中,IP 为 192.168.1.254 的服务器上运行 Apache 对外提供 Web 服务、Smtpd 提供邮件服务和 Sshd 提供远程管理控制服务;用户区的IP地址范围是 192.168.1.1～192.168.1.253. 内部服务区网段是 192.168.0.1/24,其中 192.168.0.1 为 Apache 服务器提供数据库服务,192.168.0.2 为内部用户提供 Ftp 服务. 192.168.2.1/24 是数据备份区,这里 192.168.2.2 上运行的 SQL Server 数据库每天定时对 192.168.0.1 上的数据库进行备份. 各防火墙允许访问规则配置如表 2 所示,“*”表示任意值,且每条规则的协议和端口都为任意值. IDS 部署在路由器的某个镜像端口上检测网络中可能的攻击行为.

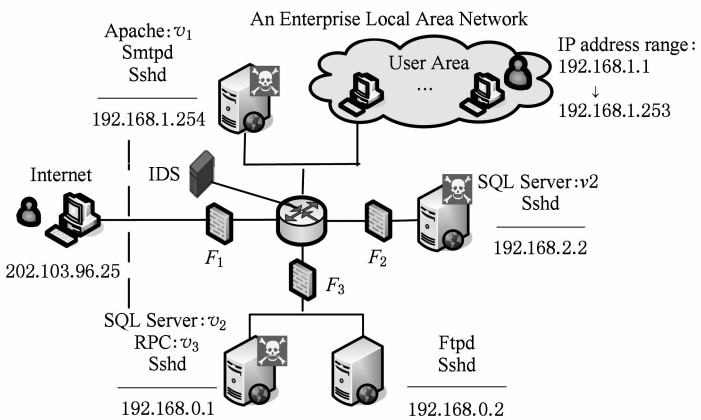

Fig. 6　The enterprise local network topologies.

图 6　企业局域网络拓扑图

Table 2 The Configured Rules Permission to Access in The Firewalls

表 2 防火墙允许访问规则配置表

Firewall	Source Host	Destination Host
F_1	192.168.1.1/24	*
	*	192.168.1.254
F_2	192.168.0.1/24	192.168.2.2
F_3	192.168.1.1/24	192.168.0.1/24

为了对该目标网络系统进行安全评估,使用Nessus脆弱点扫描器对各网段内进行扫描,发现3台服务器上存在严重的脆弱点,如表3所示.这3个脆弱点都可以被"远程内存溢出"行为模式$R_bof(h,d,sn)$利用,它的语义是威胁主体可以从源主机h对目标主机d上的sn服务发起攻击,其具体描述如表4所示.同时,从IDS预警事件中分析发现了以202.103.96.25和192.168.1.253为源主机的攻击事件,由此可确定它们是威胁主体.

Table 3 The Vulnerabilities in Hosts

表 3 主机上的脆弱点信息

Host 192.168.	Service	Vulnerability	CVE No.
1.254	Apache	v_1	CVE-2006-3747
0.1	SQL Server	v_2	CVE-2002-1123
0.1	RPC	v_3	CVE-2008-4250
2.2	SQL Server	v_2	CVE-2002-1123

Table 4 The Action Pattern Description of the Remote Buffer Overflow Exploit

表 4 远程内存溢出行为模式描述

Name	R_bof
vuls	CVE-2003-0245, CVE-2006-2372, CVE-2006-3747, CVE-2002-1123, CVE-2008-4250, …
Var	$s,d,sn,port,pro,cveId$
Pre	VulExists($d,sn,cveId$) NetworkService($d,sn,pro,port$) Connection($s,d,pro,port$) RunCode(s,ROOT)
Eff	RunCode(d,ROOT) Dos(d,sn)

将上述信息整理后输入到原型系统中,产生了图7的威胁传播图,图中各个节点对应的语义如表5所示(为方便表述,在不影响其含义的前提下,省略了一些初始属性值节点).该图与手工绘制的威胁传播图相同,表明传播算法是正确的.

根据统计信息确定该类成功概率分布函数参数$\delta=0.85$,$\lambda_1=0.1025$,$\lambda_2=0.0172$,$\beta=6$,由式(1)计算得到$p(v_1)=0.47$,$p(v_2)=0.23$,$p(v_3)=0.23$,进一步根据传播行为与脆弱点之间的关系可以得到$d(\tau_1)=d(\tau_5)=p(v_1)=0.47$,$d(\tau_2)=d(\tau_4)=d(\tau_6)=p(v_2)=0.23$,$d(\tau_3)=d(\tau_7)=p(v_3)=0.23$.根据各服务器配置信息、相关统计信息、利用测度指标计算函数(式(2)~(5))确定的测度指标以及利用危险指数计算函数(式(6)~(10))计算的服务、主机和网络系统的危险指数如表6所示.从服务层次看,危险指数最高的是192.168.1.254上的Apache服务、Smtpd服务和Sshd服务,最低的是

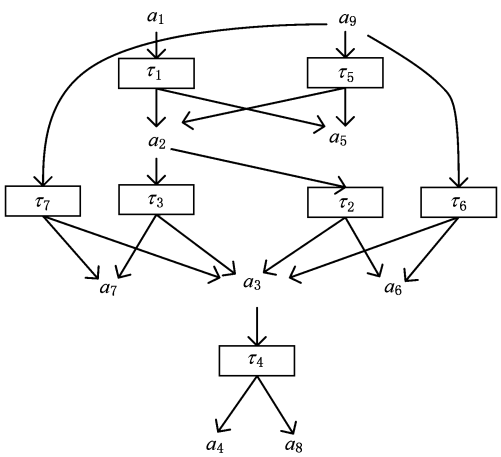

Fig. 7 The threat spread graph of the enterprise local network.

图7 某企业局域网络威胁传播图

Table 5 The Semantic of the Nodes in the Threat Spread Graph

表 5 威胁传播图中各节点语义

Node n	Label Function $L(n)$
a_1	RunCode(202.103.96.25,ROOT)
a_2	RunCode(192.168.1.254,ROOT)
a_3	RunCode(192.168.0.1,ROOT)
a_4	RunCode(192.168.2.2,ROOT)
a_5	Dos(192.168.1.254,Apache)
a_6	Dos(192.168.0.1,SQL Server)
a_7	Dos(192.168.0.1,RPC)
a_8	Dos(192.168.2.2,SQL Server)
a_9	RunCode(192.168.1.253,ROOT)
τ_1	R_bof(202.103.96.25,192.168.1.254,Apache)
τ_2	R_bof(192.168.1.254,192.168.0.1,SQL Server)
τ_3	R_bof(192.168.1.254,192.168.0.1,RPC)
τ_4	R_bof(192.168.0.1,192.168.2.2,SQL Server)
τ_5	R_bof(192.168.1.253,192.168.1.254,Apache)
τ_6	R_bof(192.168.1.253,192.168.0.1,SQL Server)
τ_7	R_bof(192.168.1.253,192.168.0.1,RPC)

192.168.2.2 上的 SQL Server 服务和 Sshd 服务;从主机的层次看,危险指数最高的是 192.168.1.254,最低的是192.168.2.2;网络系统的危险指数为8.8,由于危险指数值域是[0,30],故它的危险处于较低级别.

Table 6　The Deployment of the Servers, the Value of the Metrics and Danger Index

表 6　服务器配置、测度指标和危险指数

Host h 192.168.	Service Name s	Set of Threats $DA(s)$	Metric		Weight of Importance		Danger Index		
			$DV(a)$	$PV(a)$	$W_S(s)$	$W_H(h)$	T_S	T_H	T_L
1.254	*Apache*	a_2	⟨10,10,10⟩	0.47	0.49	0.43	14.1	14.1	8.8
		a_5	⟨0,0,10⟩	0.47					
	Smtpd	a_2	⟨10,10,10⟩	0.47	0.42		14.1		
	Sshd	a_2	⟨10,10,10⟩	0.47	0.09		14.1		
0.1	*SQL Server*	a_3	⟨10,10,10⟩	0.23	0.92	0.35	6.9	6.8	
		a_6	⟨0,0,10⟩	0.23					
	RPC	a_3	⟨0,0,10⟩	0.23	0.02		2.3		
		a_7	⟨0,0,10⟩	0.23					
	Sshd	a_3	⟨10,10,10⟩	0.23	0.06		6.9		
2.2	*SQL Server*	a_4	⟨10,10,10⟩	0.05	0.93	0.21	1.5	1.5	
		a_8	⟨0,0,10⟩	0.05					
	Sshd	a_4	⟨10,10,10⟩	0.05	0.07		1.5		

4.3　优势分析

以上述某企业局域网的安全评估为例,与传统的网络安全评估方法比较,本文提出的评估方法的优势主要体现在下面 4 个方面:

1) 利用 IDS 预警事件有效识别了网络系统面临的外部威胁主体 202.103.96.25 和内部威胁主体 192.168.1.253;

2) 不仅对威胁主体在主机 192.168.1.2 以及主机 192.168.0.1 产生的直接威胁进行评估,而且通过威胁传播图对 192.168.2.2 上面临的间接威胁进行了有效评估;

3) 分别从服务、主机和网络系统 3 个层次给出了不同测度对象的危险指数,便于安全管理员对所处同一层次对象的安全性进行比较,从而有侧重的采取安全措施;

4) 集成了多种不同的安全分析数据源,如网络脆弱点扫描数据、IDS 预警数据、网络拓扑扫描数据、网络流量统计数据以及公开脆弱点数据库等,从而可以保证评估结果的客观性.

5　结　　论

本文提出了一种基于威胁传播模型的层次化网络安全评估方法.该方法能够利用威胁传播模型识别目标网络系统中存在的直接威胁和潜在威胁,并利用层次化安全测度模型分别计算服务、主机和网络系统 3 个层次的直观网络安全态势,使安全管理员能对网络系统的安全状况有准确的了解,科学指导网络系统安全保障技术体系的建设.但该方法评估结果的准确性依赖于行为模式库的完备性,我们已初步构建了该知识库,由于网络攻击技术在不断发展,因此需要不断完善该知识库.此外,在层次化安全测度模型中,脆弱点利用成功概率是其重要的基础数据,虽然本文设计了脆弱点利用成功概率函数,但是针对不同的脆弱点如何准确确定该函数参数,需要作进一步深入研究.

参　考　文　献

[1] Software Engineering Institute Carnegie Mellon. CERT Statistics [EB/OL]. [2009-01-02]. http://www.cert.org/stats

[2] Arbaugh A, Fithen L, John McHugh. Windows of vulnerability: A case study analysis [J]. IEEE Computer, 2000, 33: 52-29

[3] Skaggs B, Blackburn B, Manes G, et al. Network vulnerability analysis [C] //Proc of the 45th IEEE Midwest Symp on Circuits and Systems. Piscataway, NJ: IEEE, 2002: 493-495

[4] Wales E. Vulnerability assessment tools [J]. Network Security, 2003 (7): 15-17

[5] Abedin M, Nessa S, Al-Shaer E, et al. Vulnerability analysis for evaluating quality of protection of security policies [C] //Proc of the 2nd ACM CCS Workshop on Quality of Protection. New York: ACM, 2006: 49-52

[6] Ahmed M, Al-Shaer E, Khan L. A novel quantitative approach for measuring network security [C] //Proc of the 27th Conf on Computer Communications. Piscataway, NJ: IEEE, 2008: 1957-1965

[7] Chen Xiuzhen, Zheng Qinghua, Guan Xiaohong, et al. Quantitative hierarchical threat evaluation model for network security [J]. Journal of Software, 2006, 17(4): 885-897 (in Chinese)
(陈秀真, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885-897)

[8] Ambrosio B, Takikawa M, Upper D, et al. Security situation assessment and response evaluation [C] //Proc of DARPA Information Survivability Conf & Exposition II. Piscataway, NJ: IEEE, 2001: 387-394

[9] Porras P, Fong M, Valdes A. A mission-impact-based approach to INFOSEC alarm correlation [C] //Proc of the 15th Int Symp on Recent Advances in Intrusion Detection. Berlin: Springer, 2002: 95-114

[10] Schneier B. Attack Trees [J]. Dr. Dobb's Journal, 1999, 24 (12): 21-29

[11] Ortalo R, Deswarte Y, Kaaniche M. Experimenting with quantitative evaluation tools for monitoring operational security [J]. IEEE Trans on Software Engineering, 1999, 25 (5): 633-650

[12] Sheyner O, Jha S, Wing J, et al. Automated Generation and Analysis of Attack Graphs[C] //Proc of the 2002 IEEE Symp on Security and Privacy. Piscataway, NJ: IEEE, 2002: 273-284

[13] Jha S, Sheyner O, Wing J. Two formal analyses of attack graphs [C] //Proc of the 15th IEEE Computer Security Foundations Workshop. Piscataway, NJ: IEEE, 2002: 49-63

[14] Ammann P, Wijesekera D, Kaushik S. Scalable, graph-based network vulnerability analysis [C] //Proc of the 9th ACM Conf on Computer and communications Security. New York: ACM, 2002: 217-224

[15] CVE. The MITRE corporation common vulnerability and exposures [EB/OL]. [2009-01-02]. http://cve.mitre.org/

Chen Feng, born in 1979. PhD and Engineer. His current research interests include computer network, network security and cryptography.

Liu Dehui, born in 1979. PhD candidate in the School of Computer Science, National University of Defense Technology. His current research interests include computer network, network security.

Zhang Yi, born in 1973. PhD and associate professor. Her current research interests include information security and network security.

Su Jinshu, born in 1962. Professor and PhD supervisor. Senior member of China Computer Federation. His current research interests include computer network and information security.