一种定量的信息安全风险评估模型

程湘云[1]，　王英梅[1]，　刘增良[2]
(1. 北京科技大学，北京　100083;2. 国防大学，北京　100011)

摘　要:目前人们采用的信息安全风险评估方法基本局限于定性或半定量的方法。采用概率风险分析的方法,通过故障树分析网络系统被攻击的根本原因,并对网络构成的实质进行了剖析,同时分析了系统漏洞的类型及对攻击结果进行了分类,在此基础上建立了定量风险计算模型。

关键词:网络安全;风险评估;故障树;漏洞;威胁
中图分类号:TP393.08　　**文献标识码**:A　　**文章编号**:1009-3516(2005)06-0056-04

风险评估在航天、核工业、经济等领域已经得到广泛的应用,产生了多种风险评估方法。信息安全的风险评估方法主要有OCTAVE方法[1]、风险矩阵法[2]和调查问卷法。Thomas R. Peltier在他的著作中对风险评估方法进行了总结,但这些方法都是基于过程的定性风险分析方法。国内对风险评估方法的研究建立在ISO13335之上,因此从根本上也没有脱离定性的方向。其实,在网络环境的风险评估方面,随着人们对系统漏洞的不断了解,对攻击方式的不断熟悉,可以形成进行定量风险评估的知识库,实现定量的风险评估。本文提出一种基于概率风险分析的信息安全风险评估方法,这种方法适于对网络环境和信息系统的风险评估。

1　概率风险分析的基本思想

概率风险分析(PRA)是以前多种方法的一种综合。PRA方法中使用的风险分析方法主要有事故链、主逻辑图、功能事件顺序图、事件树和故障树等。其中使用最为广泛的是故障树分析[3]。它是一种在系统设计过程中,通过对可能造成系统失效的各种因素(如硬件、软件、环境、人为因素等)进行分析,画出故障树,从而确定系统失效原因的各种可能组合方式及其发生概率,来计算系统失效概率,并采取相应的纠正措施,提高系统可靠性、安全性的一种设计分析方法和评估方法。

2　信息安全风险评估基本思想

信息安全风险评估(以下简称风险评估)是对信息和信息处理设备所受到的威胁、影响和脆弱性以及发生威胁事件的概率进行评估[4]。它是自上而下与自下而上的综合分析过程。自上而下分析造成损失的可能原因,自下而上总结风险形成的过程。由此可见,风险分析是对信息系统的价值、漏洞、可能存在的威胁以及威胁发生后所造成损失的分析过程。

2.1　网络环境的构成

网络中的设备通过IP地址存在于网络中,因此从逻辑上讲,计算机网络是由一系列IP地址和程序构成。网络中IP地址具有唯一性,并且每个IP地址可以对应若干个软件程序。针对计算机软件的分类方式有很多种,根据软件在网络中的互连作用,本文将软件程序分为3类:服务程序、应用程序和操作系统。

2.2　漏洞分类

软件的缺陷(漏洞),在一定情况下可以造成软件被他人利用。一种漏洞可以造成多种被利用的机会,

收稿日期:2005-06-13
基金项目:国家自然科学基金资助项目(60572162)
作者简介:程湘云(1963-),女,山东济宁人,高级工程师,博士生,主要从事网络安全研究.

同样,一次攻击的成功可以是由多种漏洞造成的。根据 ICAT,SecurityFocus 的分类方法以及漏洞产生的根源,漏洞类型可分为:输入有效性错误、访问验证错误、异常处理错误、环境错误、配置错误、竞争条件及设计错误。

2.3 攻击结果分类

漏洞被利用的结果导致系统被不同程度的访问,称之为利用结果或攻击结果。对于信息安全的损害后果通常考虑信息的3个安全属性(可用性、保密性和完整性)的破坏。考虑到网络环境的特殊情况,这里将网络攻击的结果分为5类:可用性被破坏、机密性被破坏、完整性被破坏、部分拥有系统及完全控制系统。

2.4 攻击方式

攻击方式按攻击者与被攻击对象之间的位置关系,分为本地攻击和远程攻击。本地攻击是指攻击者与攻击对象位于同一台主机。远程攻击表示攻击者与被攻击对象位于不同主机。

3 网络安全风险评估模型

通过以上分析可知,存在一种可能当攻击者获得部分软件和数据的处理权限后,利用软件间的相互作用,达到获得全部权限的结果。因此计算风险既要考虑到直接达到攻击结果存在的风险,也要考虑到间接到达攻击结果的风险。本文将风险计算的过程分为两部分,基本风险和提升风险。

3.1 基本风险

本部分从服务程序面临的风险入手,建立风险评估模型,但是对应用程序也同样适用。风险的一般计算公式为

$$\text{risk}_{(v,i,c)} = p_{v,c}(t) \times \text{loss}_{i,c} \tag{1}$$

其中:c 为攻击结果,$c \in C$;C 表示受到攻击产生结果的集合,$C \in \{\text{availability}, \text{confidentiality}, \text{integrity}, \text{process}, \text{full}\}$;$v$ 表示攻击的途经(远程攻击或本地攻击)$v \in \{v_r, v_l\}$;$\text{loss}_{(i,c)}$ 表示一个特定的网络设备 i 被攻击后的损失,$i \in I, I = \{i | 1, 2, \cdots, n\}$;$P_{v,c}(t)$ 表示通过某一路径 r 造成攻击结果 c 的概率结果损失 $\text{loss}_{(i,c)}$,依据 IP 设备的功能和他所存储的数据的价值,由风险管理员来设定;$P_{v,c}(t)$ 是该设备中存在的服务程序的联合失效概率,该设备存在缺陷可潜在地导致后果 c。这个概率是基于时间的,随时间改变。对 $P_{v,c}(t)$ 的分析可通过图1表示。图1描述了一个攻击结果故障树,它是由于两个服务程序存在漏洞,这两个漏洞可造成同一个攻击结果。其中,$F_{c,k}$ 为导致结果 v 的服务程序 k 中存在的漏洞的集合,K_c 为存在漏洞的服务程序的集合。图中有两条路径可以产生结果 c。一个路径对应一个服务程序,这个服务程序中可能存在多个漏洞导致结果 c。比如,一个输入验证错误和一个竞争条件漏洞都会导致对被攻击系统的任意访问。

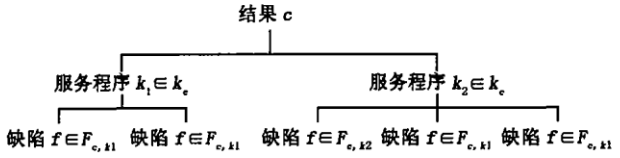

图1　造成结果 c 的故障树

对于远程的攻击风险(访问路径 $v = v_r$)导致结果 c 的概率为

$$P_{V_r}c(t) = 1 - \prod_{k \in K_c} (1 - P_{c,k}(t)) \tag{2}$$

其中:$P_{c,k}(t)$ 表示一个特定的服务 k 被攻击后导致结果 c 的概率。式(2)表示了系统受到相互独立的攻击情况。$1 - \prod_{k \in K_c} (1 - P_{c,k}(t))$ 是设备中安装的程序(它们潜在地会造成后果 c)的联合被攻击概率。程序漏洞产生了导致攻击结果 c 的相互独立的路径。由图1同样可知式(2)中 $P_{c,k}(t)$ 为

$$P_{c,k}(t) = 1 - \prod_{f \in F_{c,k}} (1 - q_f(t)) \tag{3}$$

其中:$q_f(t)$ 为漏洞 f 在时刻 t 被利用的概率。

对于一个漏洞的利用方式通常为两种:采用自动的攻击工具和手工攻击。有些时候,针对某一漏洞的攻击工具还没有开发出来,攻击者采用手工的方式,主要是通过一些脚本文件。因此,对于漏洞 f 被利用的概率可表示为

$$q_f(t) = p_{\text{automated}}(\delta t, f)\,\text{prop}_{\text{tool}}(f) + \text{prop}_{\text{manual}}(f) \tag{4}$$

$$\delta t = t_{\text{post}} - t_{\text{disc}} \tag{5}$$

其中:$p_{\text{automated}}(\delta t, f)$ 表示针对漏洞 f 的自动攻击工具被开发出来的概率方程,从时间 t_{disc} 算起,$f \in F_{c,k}$,$F_{c,k}$ 为导致结果 c 的服务程序 k 存在的漏洞集合;t_{disc} 表示漏洞被发现的时间;t_{post} 表示攻击工具被广泛使用的时间;$prop_{\text{tool}}(f)$ 为利用自动工具攻击漏洞攻击者的比例,随着时间的发展,最为可能的是这部分攻击者会越来越多。$prop_{\text{manual}}(f)$ 为不使用自动工具利用漏洞攻击者的比例。由上可见,通过式(1) 至式(5) 可以计算出系统受到远程攻击的风险值。该方法也适用于对系统的本地攻击。

3.2 风险提升

程序之间的交互增加了被攻击的机会,扩大了造成攻击后果的可能性。远程攻击者利用软件程序的漏洞作为跳板从而利用其他软件程序中的漏洞。攻击结果提升的直接结果是增加了远程访问对主机造成完全占有的攻击结果的风险,这样就影响了结果概率 $p_{v_r,\text{full}}$。图 2 描述了造成风险提升的两条路经。一个路径是从远程系统进入本地系统的服务程序,接着利用本地系统应用程序的漏洞进行攻击,如图2 中的路径(1),可称为 Remote2Local - User2Root(R2L - U2L)。它是由于一个服务程序存在一个漏洞,该漏洞可导致一个非授权用户获得对部分软件和数据访问权限(Process) 或对数据的写权限(Integrity),使得这个服务可被远程利用。通过此服务程序,攻击者可进入一个应用程序 a,而 a 中存在一个缺陷导致对系统的完全占有(full)。另一个路径是由远程系统进入本地系统,利用本地系统的服务程序的漏洞进行攻击,如图 2 中(2) 的路径,可称为 Remote2Local - Remote2Root(R2L - R2R)。它是由于一个服务程序存在一个漏洞,该漏洞可导致一个非授权的用户获得对部分软件和数据访问权限(Process) 或对数据的写权限(Integrity),使此服务可以被远程利用。这种攻击的结果使一些服务程序的安全状态发生改变,通常是改变服务程序的配置,使得攻击者进一步攻陷服务程序 k_2 导致一个计算机被完全占有。

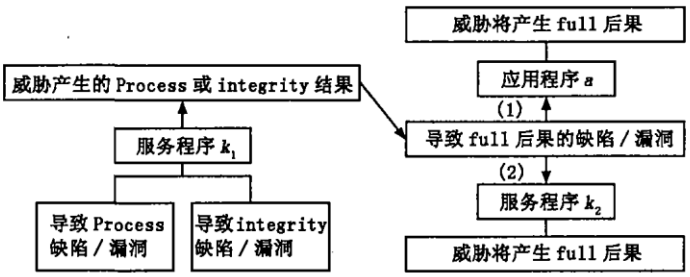

图 2 攻击扩大化描述

因此提升权限的攻击结果概率为

$$P_{\text{Escalation}}(t) = P_{v_r,\text{PI}}(t)\left(P_{v_l,\text{full}}(t) + S_{v_r,\text{full}}(t) - O_{v_l,\text{full}}(t)S_{v_r,\text{full}}(t)\right) \tag{6}$$

其中:$E_{\text{scalation}}$ 为 R2L - U2L 和 R2L - R2R 攻击扩大事件的集合;PI = Process ∪ Integrity ;$S_{v_r,\text{full}}(t)$ 为远程获得对所有软件和数据的完全访问权限的结果概率,此结果是配置错误引起的;$P_{v_l,\text{full}}(t)$ 为本地获得对所有软件和数据的完全访问权限的结果概率。因此,由远程对本地的攻击造成"full" 结果,是通过两种途径,一是利用直接造成"full" 后果的漏洞,另一是由于攻击的扩大化造成的。于是,对"full" 结果概率 $P_{v_r,\text{full}}(t)$ 综合表示为

$$P_{v_r,\text{full}}(t) = t_{v_r,\text{full}}(t) + P_{\text{Escalation}}(t) - f_{v_r,\text{full}}(t)P_{\text{Escalation}}(t) \tag{7}$$

其中:$t_{v_r,\text{full}}(t)$ 为远程攻击直接造成的"full" 结果概率。

3.3 整体风险

通过对攻击方式及攻击造成后果的分析,可以对不同攻击路径造成的风险概率进行计算,根据式(5) 计算风险值。其中,$\text{loss}_{(i,c)}$ 的值由风险管理员或设备的拥有者来确定,因为他们对该设备被攻击后造成的损失最了解。对于每个 IP 设备 i 来说,它面临着产生后果 c 的各种攻击,因此它的综合风险为式(8),其中 C 的定义同基本风险。同理可以计算整个网络的风险。

$$\text{risk}_{(i)} = \sum_{c \in C} \text{risk}_{(i,c)} \tag{8}$$

4　基于模型的系统设计

根据风险评估所涉及的要素及评估模型,我们设计出基于网络环境的风险评估系统的体系结构并进行了原型实现[5]。系统是在漏洞数据库、网络信息数据库的支持下完成风险评估的,其结构如图 3 所示。系统的各个模块包含了风险评估所需要的数据,是风险评估的基础。而概率风险分析是对大量经验数据进行分析的结果,为了验证模型的可行性,作者根据单因素方差分析(ANOVA)对风险评估各要素之间的相互影响关系,以及系统面临的影响进行了分析。由于目前人们对信息安全中的关键问题,如攻击者攻击能力变化分布等还有待于进一步的研究,因此作者主要分析了软件漏洞与攻击结果之间的关系。

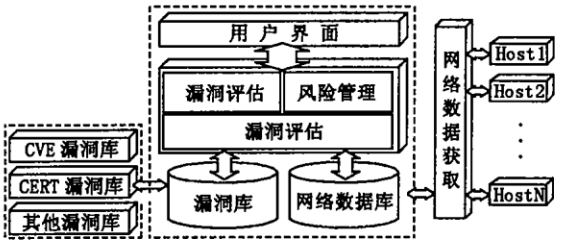

图 3　风险评估系统体系结构

5　结论

本文采用概率风险分析方法建立风险评估模型,概率风险分析通过对可能造成攻击的各种因素进行分析,从而确定系统遭到攻击原因的各种可能组合方式及发生概率,以计算系统遭到攻击的概率。作者根据风险评估模型进行了网络风险评估系统的设计与原型实现,下一步的工作是在进一步积累相关要素数据的基础上分析系统访问类型、漏洞类型、攻击结果在系统漏洞生命周期上的分布,从而分析他们对系统面临风险的进一步的影响。

参考文献:

[1] Tim Bedford, Roger Cooke. Probabilistic Risk Analysis[M]. Cambridge:Cambridge University Press , 2001.
[2] 陈　魁. 应用概率统计[M]. 北京:清华大学出版社,2002.
[3] ISO/IEC17799 2000. Information Technology Code of Practice for Information Security Management[S].
[4] 朱斌红,胡　明. 办公网的信息安全模型研究[J]. 空军工程大学学报(自然科学版),2000,1(5):48 - 50.
[5] 夏靖波,胡曦明. 基于 Agent 的远程故障诊断系统的实现[J]. 空军工程大学学报(自然科学版),2003,4(2):37 - 40.

(编辑:田新华)

A Quantitative Risk Assessment Model for Information Security

CHENG Xiang - yun[1], WANG Ying - mei[1], LIU Zeng - liang[2]
(1. University of Science and Technology Beijing, Beijing 100083, China; 2. National Defense Academy, Beijing 100011, China)

Abstract:The current methods of risk evaluation on information security are basically related to qualitative or semi - quantitative ones. So, in this paper, by using a method of probability risk analysis, analyzing the fundamental reasons why network systems are attacked through fault tree, making a serious study of the essence of network composition and of the different types of system vulnerabilities, and classifying the consequences of network attacks, a quantitative model of information security risk assessment is proposed.

Key words:network security; risk assessment; fault tree; vulnerability; threat