面向对比评估的软件系统安全度量研究

张 鑫 顾 庆 陈道蓄
(南京大学计算机软件新技术国家重点实验室 南京 210093)

摘 要 保护质量是指安全模块在进行安全处理时需要达到的安全目标。它是以一定的量化标准来衡量的。如何客观有效地评估现有软件系统是否满足保护质量的要求已成为研究热点之一。目前,大多数安全领域的从业者使用的是具有较高主观性的定性评估方法,使得评估结果依赖于个人经验而并不可靠,从而需要独立、客观、定量的安全度量方法。针对安全度量的复杂性和实施困难的情况,提出了基于对比评估的安全度量模型,分别从攻击面、拒绝服务和攻击图的角度讨论了两个或多个软件系统之间的相对安全性,并对评估的过程和结果进行了综合分析与研究。

关键词 保护质量,安全度量,攻击面,拒绝服务,漏洞,攻击图
中图法分类号 TP306 **文献标识码** A

Study of Security Metrics of Software System for Comparative Evaluation

ZHANG Xin GU Qing CHEN Dao-xu
(National Laboratory of Novel Software Technology, Nanjing University, Nanjing 210093, China)

Abstract Quality of protection can be seen as the security target of security modules when doing their security treatments, which can be judged by quantitative criteria. The question of how to evaluate whether the current software system has fulfills the quality of protection target objectively and effectively has become one of the hotspots of research. Currently, however, most security professionals use the qualitative method for security evaluation, which is highly subjective and makes the evaluation result dependent on the individual experience and thus unreliable. So what needed are substantive and quantitative security metrics. Because of the complexity and the difficulty of implementing the security metrics, a novel security evaluation model was presented in this paper, which analyzed the relative security level of given systems from the views of attack surface, denial of service and attack graph. At last, a general discussion for the process and the result of the evaluation were given.

Keywords Quality of protection, Security metrics, Attack surface, Denial of service, Vulnerability, Attack graph

1 引言

随着社会的进步与科学技术的发展,软件系统的功能越来越多,规模也越来越大,用户对其依赖性也越来越强。因此,一个高质量、高可靠性和高安全度的软件产品就成为用户需求中的重要组成部分。尤其是大量的用户个人数据资料等较为隐私和机密的文件都以电子文件的形式等存放在计算机中,这样就凸显出安全问题。如何保障用户使用软件系统的安全性且使得业界在安全方面的投资能得到有效的回报,成为领域内专家学者研究的重点。

保护质量是指安全模块在进行安全处理时需要达到的安全目标。它以一定的量化标准来衡量,是组织、执行安全任务和选择安全服务的准则[15,16]。然而,目前大多数软件系统安全领域的从业者使用的是具有较高主观性的定性评估方法,使得评估结果依赖于个人经验,且没有具体的指标支持使得对系统安全程度的认定不能取得一致,从而需要独立的客观的定量评估方法。通过量化的度量方法,可以提供控制、评估和预测软件安全性的框架,亦即安全度量[11]。安全度量考虑的问题是如何度量和评估一个系统的安全性以及评估结果达到一个什么样的程度才能满足保护质量的目标。现有的主要安全度量研究包括:

(1)基于对系统安全要素建立数学模型的评估方法[12];
(2)基于安全管理的度量方法[13];
(3)基于过程能力评估的SSE-CMM安全度量[14];
(4)基于特定安全目标的度量方法[3,6,7]。

其中,前三者虽然在理论上进行了充分的分析及验证,但并不针对具体的安全问题进行考虑;而后者则缺乏相应的综合考虑,使得评估结果只局限于系统的某个安全问题,因此对于软件系统的整体安全性仍然不能得到令人信服的评估结果。由于用户在对某个软件系统的选择使用上,关注的往往是具有相似功能的软件系统或是同一软件系统的不同演化版本之间的相对安全性,即从比较的角度而非从绝对的安全级别数值

到稿日期:2008-10-27 返修日期:2009-01-04 本文受国家863项目(2006AA01Z177),江苏省自然科学基金基础研究项目(BK2006115),国家自然科学基金项目(NSFC60873027)资助。
张 鑫(1984—),男,研究生,主要研究方向为软件工程,E-mail:zhangxin@dislab.nju.edu.cn;顾 庆(1972—),男,博士,副教授,主要研究方向为分布式计算与并行处理、软件工程;陈道蓄(1947—),男,教授,博士生导师,主要研究方向为分布式计算与并行处理。

角度出发考虑安全问题，因此需要相应的度量评估模型。针对此问题，本文提出了面向对比评估(comparative evaluation)的安全度量模型，将多个具有相似功能的软件系统或某个软件系统的不同版本按照相同的安全度量方案得到的不同安全度量值进行比较，得到的结果可以帮助用户选择出具有较高安全性的软件系统。这种方法虽然并未给出是否符合保护质量的量化标准，但是能够给出多个系统之间安全性的全序关系，即可以评估出某个最能满足用户保护质量要求的系统。

本文第2节提出了一个安全度量框架以及用于解释的网络系统模型，并从不同的角度划分不同的安全度量方法；第3节分别介绍相关的安全度量方法并对方法进行了综合；第4节对不同的度量方法进行了综合评估讨论；最后是总结和展望。

2 安全度量框架

针对一个软件系统可以考虑的安全问题有许多，如常见的病毒攻击、系统文件信息被非法读取或非法删改、由黑客发起的泛洪攻击使得网络拥塞导致通讯受损，或者是系统存在的安全漏洞被攻击者利用导致其获得合法权限从而对系统进行破坏等等。这些安全问题的出现就触发了对系统安全的保护，如使用各种防病毒攻击软件、入侵检测和防御系统等。然而这是一种被动的解决方式，真正的解决方法仍在系统的本身，即在系统开发阶段就对安全问题进行考虑。这就牵涉到一个重要的问题，即如何对生产出的软件系统的安全级别进行评估。有两种方法可以运用：一种是定性评估方法；另一种则是定量评估方法；前者实现简单，但过于依赖主观判断，缺乏数据支持，可信度较低；后者针对问题给出具体指标，有数据支持，但实现困难，且在指标的标准确定上还未成熟。综合来看，定量评估方法是今后的趋势，且以安全度量为代表的定量评估方法也取得了一定的进展。

由于现实中的软件系统都是针对某一类问题而产生的，且一些成熟的主流软件系统会随时间产生一系列的演化版本，因此对所有的系统考虑其安全度量采用统一的标准是不合适的。即使针对同类软件系统，由于其规模大、复杂度高，制订标准的难度也很大。针对这一问题，本文提出对比评估的方法，根据某些指标的综合值，将具有相似功能的软件系统或者是同一系统的不同演化版本之间的安全程度做比较，具体模型如图1所示。其中 $ASM(i)$($Aspect\_Security\_Metrics(i)$)表示针对系统某一方面的安全度量值，$aw(i)$($Aspect\_Weight(i)$)表示其相应的权重；$SI(j)$($Security\_Index(j)$)表示某一方面的安全度量指标，$w(j)$为该指标的权重；$SSM$($System\_Security\_Metrics$)则表示 $ASM(i)$经过综合后得到的整个系统的安全度量值。

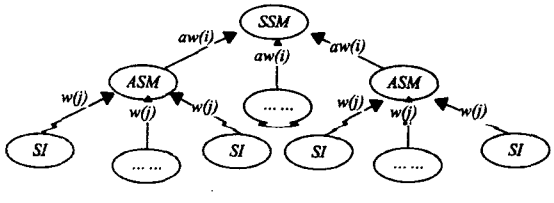

图1 评估模型

经过综合后的 SSM，其表示方式有标量表示法与矢量表示法。标量表示法即将得到的所有 ASM 进行加权和处理，从而得到某一单一的值；矢量表示法为类似〈$ASM(1)$，$ASM(2)$，…，$ASM(n)$〉的形式。使用标量表示法可以横向直接比较各个系统的安全级别，但单一的值较为模糊且缺乏说服力；使用矢量表示法则较为清晰地表示出各个方面的安全性，但比较的方法较为复杂，即需要对各个方面的安全性分别进行比较，然后综合。本文使用的是综合二者的表示法，即使用单一的值对各个系统进行比较，如果该值相差不大，则针对具体的安全方面再进行权衡。

目前主流的网络系统模型有 C/S，B/S 和 P2P 3种方式，其中 C/S 和 B/S 方式占有很大比例，网络攻击的客体也大多是各类服务器系统，而主体即为攻击者所在的客户端。基于此建立的网络模型如图2所示，其中用户(U)与攻击者(A)对服务器(S)进行访问，三者使用路由器进行连接，攻击者则对该服务器进行攻击。常见的网络攻击方式有恶意入侵和泛洪等等，攻击者要达到的主要目的通常为恶意读取和修改系统资源、影响系统与外界通讯以及非法获取高级权限从而对系统进行破坏等。因此针对上述模型，可以从3个角度来考虑整个系统的安全问题：

1. 从系统资源角度出发，给出攻击面度量；
2. 从系统通讯的角度出发，给出拒绝服务度量；
3. 从系统权限保护出发，给出攻击图初始节点度量。

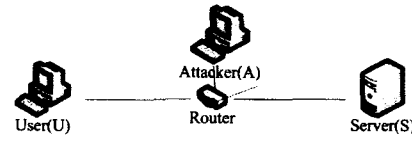

图2 网络系统模型

3 安全度量方法

3.1 攻击面度量

文献[1-5]提出了一种进行安全评级的方法，称为攻击面度量(attack surface metric)，即用静态的方法对系统内在资源进行安全评估，得到的结果是基于概率的，表示攻击所造成的对系统的破坏程度。

3.1.1 攻击面相关定义

定义1(系统资源，system resource) 包括方法(method)、通道(channel)和数据(data)。通常情况下，攻击者都是通过利用系统部分资源的漏洞从而使用该资源来攻击这个系统的。然而，并不是所有的系统资源都是可以被攻击者利用的，它们之间存在着可能性大小的区别。比如以“root”权限运行的方法要比以普通“user”权限运行的方法更易遭到攻击者的攻击。

定义2(成本效益比，cost-benefit ratio) 成本(cost)代表攻击者实施该攻击所花费的代价，由于攻击者若想使用该项资源就需要先获得该资源的存取权(access right)，因此成本就取决于要获得的存取权的对应值，该值与存取权的重要性成正比；效益(benefit)代表攻击者实施攻击后造成该系统的破坏程度。对于方法，取决于它的权限(privilege)。例如攻击者利用权限为“root”的方法比利用权限为普通“user”的方法造成的破坏更严重，获得的效益也越大；对于通道，则取决于其类型(type)，如套接字类型的通道允许字节流的传送而其它某些类型的通道则不允许，且字节流的数据由于没有内容限制，对系统可能造成潜在的破坏就很大；对于数据集，也是取决于其类型(type)，如file类型的数据可以存放可执行的恶

意代码，造成的破坏就非常大。成本效益比用公式表示为：r=benefit/cost，其中 benefit 对应的方法、通道和数据分别为 privilege，type 和 type。成本和效益的取值目前仍取决于经验和直觉，如何更有效地赋值也是值得研究的方向。

定义 3(攻击类，attack class) 由于同一类别的不同资源被攻击者利用的可能性不尽相同，因此不能把所有的资源同等看待，需要根据成本效益比的不同将不同的资源归属于不同的类别中，形成多个攻击类。具体体现在方法、通道和数据 3 个层次上。

• 方法攻击类(MAC，method attack class)：系统中方法的子集，其中所有的方法拥有相同的权限和存取权；

• 通道攻击类(CAC，channel attack class)：系统中通道的子集，其中所有的通道拥有相同的类型和存取权；

• 数据攻击类(DAC，data attack class)：系统中数据的子集，其中所有的数据拥有相同的类型和存取权。

定义 4(攻击面，attack surface) 攻击面由各系统资源的可攻击性的总和计算得出。可攻击性(attackability)是指该资源被攻击者利用的可能性，其值由该资源的成本效益比计算公式 r=benefit/cost 得出。攻击面的表现形式可为三元组：$\langle MA, CA, DA\rangle$，其中，

• MA(method attackability)：表示方法攻击类计算出的可攻击性的总和；

• CA(channel attackability)：表示通道攻击类计算出的可攻击性的总和；

• DA(data attackability)：表示数据攻击类计算出的可攻击性的总和。

攻击面度量值越大，这个系统就越容易遭受到攻击，从而认定这个系统就越不安全。此认定的根据是统计和计算出来的度量值，从而明确其可信度较高。

3.1.2 攻击面度量举例

在第 2 节的网络模型中，假设 S 配备了 IMAP 邮件服务，工作流程为 U 使用 UDP 套接字与 S 连接，然后在 S 端进行登录。列出存储在 S 上的 email 文件。从该列表中取出某个文件查看其内容，最后关闭与 S 端的连接。S 端的文件系统中存储有配置信息文件和 email 文件。

假设 S 中方法的权限有“root”和“user”，通道的类型为“UDP”，数据的类型为“file”，存取权有“root”，“authenticated”和“unauthenticated”，且对于相同的资源、不同的类型或权限以及存取权均存在着全序关系，如表 1 所列。

表 1 S 中的资源权限/类型与存取权

Method privilege	Channel type	Data type	Access right
root>user	UDP	file	root>authenticated >unauthenticated

S 中的资源如表 2 所列。

表 2 S 中的资源

Method	Channel	Data
login(), list(), fetch(), close()	port143, port993	/etc/passwd, /etc/shadow, /etc/user. conf, /var/lib/user

下一步则根据可攻击性划分出攻击类：

• login()方法的权限是“root”，存取权是“unauthenticated”；

• list(), fetch(), close()方法的权限是“user”，存取权是“authenticated”；

• 通道 Port143, port993 的类型是“UDP”，存取权是“unauthenticated”；

• 数据项/etc/shadow, /etc/user. conf 的类型是“file”，存取权是“root”；

• 数据项/etc/passwd, /var/lib/user 的类型是“file”，存取权是“authenticated”。

由此可划分出 5 个攻击类，如表 3 所列。其中最右列表示的是对应攻击类的可攻击性。

表 3 S 中攻击类的划分

attack class	set	Privilege/ type	access right	value
MAC 1	{ login() }	root(2)	unauthenticated(1)	2
MAC 2	{ list(), fetch(), close() }	user(1)	authenticated(2)	1.5
CAC 1	{ port143, port993 }	UDP (1)	unauthenticated(1)	2
DAC 1	{ /etc/shadow, /etc/user. conf }	file(1)	root(3)	0.66
DAC 2	{ /etc/ passwd, /var/lib/user }	file(1)	authenticated(2)	1

由表 3 可得 S 的 MA 值为 2+1.5=3.5，CA 为 2，DA 为 0.66+1=1.66，从而得到了 S 的攻击面度量为$\langle 3.5, 2, 1.66\rangle$，其中括号中赋予权限/类型和存取权的整型参数为方便计算所用。如对于另一个系统 S′，若得到的攻击面度量为$\langle 5, 2, 1.33\rangle$，即相比之下 S 的 MA 值略低，DA 值略高。然而由于 S 配置了诸如 Microsoft 的 EFS 这种有较高安全性的文件系统，则攻击者选择使用系统方法进行攻击的可能性就会增大，从而使 S 的整体安全性就要高于 S′。

3.2 拒绝服务度量

由于因特网在规模上和功能上不断扩大，拒绝服务式攻击目前在很大程度上降低了网络服务的质量。通过网络泛洪造成的主要影响有长时间的延迟、数据包的过量丢失和服务的中断等。而拒绝服务的防范工作重点也放在限制这种不良影响且能够尽快恢复到用户可以接受的水平上。为了能客观地评估针对拒绝服务式攻击的防御，必须能够精确地度量出拒绝服务式攻击的破坏程度。在以前的研究中，学者们提出了很多用来度量拒绝服务式攻击的破坏程度的具体参数：

• 合法用户数据包丢失的比例；

• 请求/应答延迟；

• 整个事务的持续时间；

• …

然而，度量出来的数据如果不对情况加以分类就用于评估一个防御的好坏，其结果往往与现实不相符。比如，5min 的数据延迟对一个在线通话系统的打击是致命的，而对一个电子邮件系统来说却又是微不足道的。另外，如果一个针对 DoS 的防御能将延迟的时间缩短为 1s，对一个网页浏览者来说改进是巨大的，然而对于一个在线游戏用户所要求的 150ms 这个标准来说又相差甚远。因此，这些度量并不能满足用于不同应用的服务质量(QoS，quality of service)的需求。对此，文献[6]提出了拒绝服务影响(DoS-impact)度量，用来表示拒绝服务攻击对各个应用的影响程度。

3.2.1 拒绝服务影响度量

一个系统可以由不同的应用类别(application category)组成,如 http,ftp 等。而一个应用类别又由若干事务组成。事务(transaction)表示一个高层的任务,它的开始与结束对用户来说应是有意义且可见的,如浏览一个网页、下载一个文件或进行一段 VoIP 谈话。针对每一个事务,度量以下 5 个通讯参数(communication parameter)。

· 请求/应答延迟(request/response delay):针对交互式应用程序;

· 事务持续时间(transaction duration):针对非交互式应用程序(可以允许有中断但需要在一定时间内完成);

· 单路延迟(one-way delay)、数据包丢失(packet loss)、延迟变动(delay variation/ Jitter):针对多媒体或游戏应用程序。

一个事务需要被划分到某个应用类别中,且度量出来的通讯参数用来跟该应用类别相关的阈值做比较,以判断该事务是成功的还是失效的。然后针对每一个应用类别计算出失效的事务的百分比(PFT, percentage of failed transactions),即为拒绝服务影响度量。表 4 为 HTTP,FTP,TELNET,ICMP 和 DNS 的 5 个应用类别的服务质量需求,由网络传输参数形成的阈值表示。若没有要求,则用"—"表示,其中 Any delay 表示从服务器端接收的任意两个数据包之间的延迟时间,Whole delay 表示从最后发出请求到所有应答数据包接收完毕的延迟时间。

表 4 主要应用类别与 QoS 需求

Category	Req/resp delay	Dur.
HTTP	Any, RTT<4s	<60s
FTP	Any, RTT<10s	<300%
TELNET	Any, RTT<250ms	-
ICMP	Whole, <4s	-
DNS	Whole, <4s	-

3.2.2 DoS-hist 度量和 DoS-level 度量

定义 5(DoS-hist 度量) 在给定攻击强度的前提下横跨各个应用类别显示失效比例的直方图。

定义 6(DoS-level 度量) 将 DoS-impact 的度量进行累加,得到一个单一的数据,即 $\sum_k PFT(k) * w_k$,其中 k 用于区分不同的应用类别,w_k 表示相应的权重,权重的赋值则依据系统的具体要求,将系统中重要程度高的应用类别赋予较高的权重。此度量可以用来评定一个系统对 DoS 攻击的防御程度。

整个拒绝服务度量思路如下:根据泛洪攻击强度的变化,各应用类别的失效比例也随之变化,即当泛洪强度为 0 时不存在任何的攻击,各应用类别的失效比例接近于 0。随着泛洪强度越来越大,各服务的失效比例随之上升,且阈值低的或非可靠传输的应用类别的失效比例达到百分之百的时间越短,由此可以看出系统中各应用类别在平均泛洪强度下的防御能力。通过模拟实验,在客户端收集事务数据并统计其失效比率,即得到各应用类别的 DoS-impact 度量。将所有应用类别的 DoS-impact 度量进行综合,得到单一的值,即为 DoS-level 度量,且该值取值越大,表明其安全性越差,从而可以分析出整个系统对拒绝服务攻击的防御能力。

3.3 攻击图初始节点度量

从一个规模较小的局域网到一个规模较大的企业内部网,用户权限的保护问题是一个较为严重的问题。较高的用户权限就意味着对整个系统的较高的控制权。若被攻击者取得该权限,也就意味着系统的安全性受到极大的威胁。因此,需要采取有效的手段来对此类攻击进行有效的度量,可以使用攻击图方法进行建模。

3.3.1 漏洞

漏洞(Vulnerability)[9,10]是指一个系统在需求、设计、实现等阶段存在的缺陷,这些缺陷可能被用户无意中触发或是被攻击者利用,从而导致安全失效。即漏洞可以理解为安全领域的缺陷、导致安全问题的缺陷。通常情况下,业界多采用查找和统计系统中的漏洞来评定其安全性,但前提是这些漏洞是相互独立的。如果这些漏洞存在相互依赖的关系,统计的数据就会不准确甚至是错误的。因此,漏洞越多并不意味着越不安全。如果这些漏洞需要攻击者全部利用才能发动攻击,则漏洞的数量越多便意味着攻击者发动攻击的难度越大,从而意味着系统就越安全,即要考虑漏洞之间的相互关联性。

3.3.2 攻击图

一种较为流行的用于评估网络安全性的技术是攻击图(attack graph)[8],它可以表示所有可能用来对一个网络进行渗透式攻击的路径的归总。攻击图的根节点表示攻击者要达到的目标;路径代表的是攻击者为达到目标所采取的攻击方式;节点代表的是攻击的某个阶段,可以表示为攻击过程中的某个状态,也可以表示为对系统中某个漏洞的利用。

借助上述思想,可以使用攻击图来模拟攻击者利用漏洞实施攻击的过程。由于攻击者在发起整个攻击之前需要达到某些特定状态,如与被攻击的服务器建立连接等等,达到这些状态就需要攻击者花费相应的成本。即攻击者花费的成本越大,系统相对来说就越安全。因此,可以考虑将攻击图的初始节点作为度量对象对系统进行安全评估。文献[7]使用状态转换系统(state transition system)建模,其中状态被定义为一系列的谓词,比如 $reach(s,d,p)$ 表示目标端口号为 p 的网络数据包在网络中可以由源地址 s 到达目标地址 d;$shell(A, user)$ 表示一个用户可以在主机 A 上执行权限为"user"的 shell 程序。转换系统的初始状态集(initial states)代表的是攻击者进行攻击的初始状态集合,目标状态集(goal states)代表的是攻击完成的状态集合,在本节中设定为攻击者最终获得了"root"级别的权限,攻击路径则是状态之间的转换。

3.3.3 攻击图初始节点度量举例

在本文所示的网络模型中,假设服务器端存在两个漏洞:①匿名 FTP. rhosts 远程登录;②本地缓冲区溢出。攻击者可以利用该漏洞非法进入网络内部,达到既定目标,即在 S 上拥有"root"权限。攻击图如图 3 所示,其中,

· 灰色填充椭圆:初始的状态节点;

· 无色椭圆:中间状态节点;

· 矩形:利用漏洞/动作;

· 菱形:目标状态节点。

攻击者若要达到目标状态,首先要利用匿名 FTP. rhosts 远程登录漏洞获取 S 上的"user"权限,然后利用本地缓冲区溢出漏洞将权限 l3 提升到"root"。为了得到攻击者成功完成一次攻击所花费的最小代价,根据图 3,可以得到初始状态集合为{$sh(A, user)$, $service(vulFTP, S, 21, l2)$, $reach(A, S, 21)$, $reach(A, S, 513)$}。对不同的系统,对其内在已知的漏洞进行分析,均可得到不同的攻击图,从而得到不同的初始节点

集。对于两个初始节点集合 I_1，I_2，判断其对应的系统 S_1，S_2 之间的相对安全性分 3 种情况进行讨论：

(1)若 I_1 为 I_2 的真子集，则 S_2 比 S_1 安全性高，反之亦然；

(2)若两集合相等，则 S_1 与 S_2 安全性相同；

(3)若非以上两种情况，即两者不存在包含与被包含关系时，可以根据集合中的元素所代表的攻击者达到此状态的难易程度对其赋予权重。此时将不同集合中相异的状态对应的指标按照难易程度取值。若该状态较难达到，则取值大，否则取值小，相应的权重则根据该状态相对于整个攻击的重要性取值：重要性越高，则取值大，否则取值小。

另外，值得注意的是，本文讨论的攻击图初始节点度量仅讨论一条攻击路径的情况。对于存在多条攻击路径的情况，就不能将所有初始节点一起考虑，而是取各路径中最小的初始节点集合作为其安全程度的评估标准。

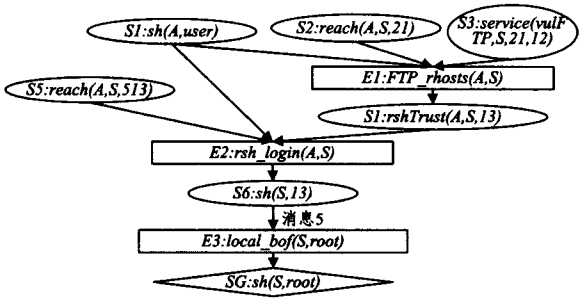

图 3　攻击图

4　综合评估

随着软件系统的安全性得到越来越多的重视，相关的度量方法也变得越来越重要。由于软件系统规模庞大且功能复杂，在很大程度上难以对其安全性进行整体的定量评估，因此需要一种评估方法，该方法能够解决具体的安全问题且实现简易，并确保其评估结果能够被用户接受。本文提出的对比评估(comparative evaluation)就是这样一种方法，即根据某几种安全度量指标，将多个具有相似功能的软件系统或某个软件系统的不同版本进行比较，用户可以根据不同的安全功能考虑，从中选择出具有较高安全性的软件系统。此方法可以充分利用各种较为成熟的安全度量技术，如攻击面、攻击图等，易于扩展，因此可以更全面地评估出软件系统的安全程度；并且选择了用户最关心的相对安全级别，从而避开了争议颇大的绝对安全级别。综合来看，对比评估方法的侧重点仍是根据量化的安全指标来评估软件系统，并且定位于系统之间的相互比较，因此其评估结果也满足保护质量的要求。

根据图 2 所示的现实中主流的网络模型，本文提出的对比评估方法从攻击面、拒绝服务和攻击图 3 种度量维度展开，分别对一个系统中的静态资源安全程度、对外通讯受影响程度以及系统中的用户权限保护程度进行度量。3 者之间既有联系又有区别，攻击面和攻击图方法考虑的都是系统中的资源保护问题，只是其对资源定义略有不同。攻击面中的资源限定于系统中的方法、与外界建立连接的通道以及系统内部与方法相交互的数据；而攻击图中的用户权限保护问题属于动态范畴，与攻击面中的静态资源度量视角不同。二者度量指标的选取也不相同：攻击面中的度量指标是软件系统中资源的成本效益比的总和，而攻击图中的度量指标则是攻击者进行攻击的状态集。即二者的区别在于静态分析与动态建模以及被动防御与主动攻击。对于拒绝服务，则是从对外通讯另一完全不同的层面进行考虑。

根据图 1 中的评估模型可知，根据攻击面、拒绝服务和攻击图 3 种度量方法得到的度量值分别对应于各个 ASM 值，然后将以上得到的 3 个 ASM 值进行规范化处理(normalization)，统一为分布于[0,100]区间上的值。然后根据系统具体的安全需求对 aw 进行赋值，即对关注的问题取值大，否则取值小。若取值为 1，则表明系统仅关注该问题；取值为 0，则表明系统对此问题不做考虑。最后将所有的 ASM 值进行加权和得到的总的 SSM 值即为该软件系统的总的安全度量值。度量值大，则表示安全性差，否则表示安全性好。因此，根据该值可以比较出系统之间的相对安全性。

软件系统涉及的安全方面是多样的。将所有的方面考虑周全从而给出该系统的安全级别是不现实的。然而，尽可能地从多角度出发考虑安全问题是必要的。本文给出的 3 个安全角度，即静态资源安全程度、对外通讯受影响程度以及系统中的用户权限保护程度，只是在一定程度上给出了一个软件系统安全度量值。由于对安全进行量化的工作并不成熟，并不能将各类系统安全问题全部纳入度量框架之内，因此该框架具有一定的局限性。随着安全度量的发展，将会出现更多的度量方法，从而使该框架越来越丰富，使整个软件系统的安全评估结果越来越准确。

结束语　随着对软件系统安全性要求的不断提高，如何达到保护质量的目标，逐渐成为领域内研究的热点。本文通过从攻击面、拒绝服务和攻击图 3 个角度分别考虑了一个系统的资源、通讯及权限保护 3 种安全问题，给出了相应的度量指标并对整个系统的安全程度使用加权和的处理方式来考虑，得出的结果即可用于对同类系统或同一系统的其他版本进行综合的对比评估，解决了安全度量领域由于缺乏统一标准使得度量过程困难与度量结果缺乏说服力的问题，且方式灵活。然而，现有的工作仍需进一步完善，如对目前考虑的 3 个方面做进一步的验证和对系统某一方面的安全问题进行更多的评估以及使用某个具体的软件系统进行验证。

参 考 文 献

[1] Howard M, Pincus J, Wing J M. Measuring relative attack surfaces[C]// Proc. of Workshop on Advanced Developments in Software and Systems Security. Taipei, 2003

[2] Manadhata P, Wing J M. Measuring a system's attack surface [R]. CMU-CS-04-102. Computer Science Department of Carnegie Mellon University, 2004

[3] Manadhata P, Wing J M. An attack surface metric[R]. CMU-CS-05-155. Computer Science Department of Carnegie Mellon University, 2005

[4] Manadhata P, Wing J, Flynn M, et al. Measuring the attack surfaces of two FTP daemons[C]// Proceedings of the 2nd ACM Øorkshop on Quality of Protection. Alexandria VA, USA, 2006

[5] Manadhata P, Kaynar D K, Wing J M. A formal model for a system's attack surface[R]. CMU-CS-07-144. Computer Science Department of Carnegie Mellon University, 2007

(下转第 195 页)

$$cer(C,D)=\frac{\sum_{i=1}^{t} card(\|C\wedge D\|_i)*\prod_{j=1}^{n}P_{a_j}(\|C\|_i)}{\sum_{i=1}^{t} card(\|C\|_i)*\prod_{j=1}^{n}P_{a_j}(\|C\|_i)} \quad (4)$$

$$P_{a_j}(\|C\|)=\begin{cases}1, & a_j(x)\neq *,\forall a_j\in\|C\|\\ \dfrac{1}{V_{a_j}}, & a_j(x)=*,\forall a_j\in\|C\|\end{cases} \quad (5)$$

同时覆盖度 $cov(C,D)$定义为：

$$cov(C,D)=\frac{\sum_{i=1}^{t} card(\|C\wedge D\|_i)*\prod_{j=1}^{n}P_{a_j}(\|C\|_i)}{card(\|D\|)} \quad (6)$$

a_i 为符合规则的条件属性，$P_{a_j}(\|C\|)$为该属性对应的概率值，$\sum_{i=1}^{t} card(\|C\wedge D\|_i)*\prod_{j=1}^{n}P_{a_j}(\|C\|_i)$ 是完全符合规则和可能符合规则的对象的个数，对于一个对象来说，如果它完全符合某条决策规则，则其概率值 $P_{a_j}(\|C\|)=1$，如果它可能符合某规则，则其概率值 $P_{a_j}(\|C\|)$为对象中缺失的条件属性值域的倒数之乘积。

例如，对表 2 所生成的某条决策规则 $(P,high)\wedge(M,high)\wedge(X,low)\rightarrow(d,poor)$，由于对象 3 有可能符合该条规则，对象 3 的个数为 5，但属性 P,M 的值缺失，以上两个属性的值域范围均为 2，因此，计算其确信度和覆盖度如下：

$$Cer((P,high)\wedge(M,high)\wedge(X,low)\rightarrow(d,poor))=\frac{5*0.5*0.5}{5*0.5*0.5}=1$$

$$cov((P,high)\wedge(M,high)\wedge(X,low)\rightarrow(d,poor))=\frac{5*0.5*0.5}{5}=0.25$$

3.3 规则对知识分类的反映程度

对于某一规则 $C\rightarrow D$ 记为 R，$X=\|R_x\|$ 为符合规则 R 中的条件属性集的对象集合，E 为条件属性全集的某个分类。如果 $X\cap E=E$，则称规则 R 与 E 有关，如果 $X\cap E=\emptyset$，则称规则 R 与 E 无关[1]。如果某规则 R 只与某一个分类有关，则定义该规则的反映程度如下：

$$\mu_R(E)=cer(R_i) \quad (7)$$

即某规则对分类的反映程度为其确信度。如果某一分类 R 与多个规则有关，则规则对分类的平均反映程度为：

$$\mu_{rule}(E)=\frac{\sum_{i=1}^{m} cer(R_i)}{m}=\frac{\sum_{i=1}^{m}\mu_{R_i}(E)}{m} \quad (8)$$

m 表示该条件属性全集的某个分类 E 中含有的规则数。对于表 2 来说，6 个对象组成 6 个分类，对于第 6 个分类来说，有第 5，6，7 和 8 条规则同它相关，因此这些规则对该分类的平均反映程度为：

$$\mu_{rule}(E_6)=\frac{\mu_{R_5}(E_6)+\mu_{R_6}(E_6)+\mu_{R_7}(E_6)+\mu_{R_8}(E_6)}{4}=0.50$$

结束语 针对完备信息系统中规则的不确定性度量为确定值的情况，本文将不确定性的度量引入到不完备信息系统中。由于部分属性值的缺失，对于某条规则，无法判定那些具有缺失属性值的对象是否符合该规则。由此在不完备信息系统中，如符合该规则的对象条件属性值无缺失，则其支持度、强度、确信度和覆盖度为固定值，如符合该规则的对象条件属性值有缺失，则其不确定性度量是一个区间范围。在分析了不完备信息系统中规则的不确定表示的特性后，提出以近似概率值来表示不完备信息系统的确信度和覆盖度，并依据确信度的近似值来计算规则对条件属性全集分类的反映程度。对不完备信息系统整个规则集的不确定性的衡量还需要作进一步讨论。

参 考 文 献

[1] 王国胤. Rough 集理论与知识获取[M]. 西安：西安交通大学出版社，2001

[2] Pawlak Z. Rough classification[J]. Human-computer Studies, 1999,51:369-383

[3] Pawlak Z. Rough sets and intelligent data analysis[J]. Information Science,2002,147:1-12

[4] Pawlak Z. Rough sets, decision algorithms and Bayes' theorem [J]. European Journal or Operational Research,2002,136:181-189

[5] Greco S, Pawlak Z, Slowinski R. Can Bayesian confirmation measures be useful for rough set decision rules [J]. Engineering Application of Artificial Intelligence,2004,17:345-361

[6] Kryszkiewicz M. Rough Set Approach to Incomplete Information System [J]. Information Sciences,1998,112:39-49

[7] Kryszkiewicz M. Rules in incomplete information systems [J]. Information Science,1998,113:274-292

[8] 黄冰. 基于粗糙集的不完备信息系统知识理论获取理论与方法[M]. 南京：南京理工大学，2004

(上接第 126 页)

[6] Mirkovic J, Reiher P, Fahmy S, et al. Measuring Denial of Service[C]//Proceedings of the 2nd ACM Workshop on Quality of Protection. Alexandria VA, USA, 2006

[7] Pamula J, Jajodia S, Ammann P, et al. A Weakest-adversary Security Metric for Network Configuration Security Analysis[C]//Proceedings of the 2nd ACM Workshop on Quality of Protection. Alexandria VA, USA, 2006

[8] Wang Lingyu, Singhal P A, Jajodia P S. Toward measuring network security using attack graphs[C]//Proceedings of the 2nd ACM Workshop on Quality of Protection. Alexandria VA, USA, 2007

[9] Ozment A. Improving vulnerability discovery models[C]//Proceedings of the 2nd ACM Workshop on Quality of Protection. Alexandria VA, USA, 2007

[10] Abedin M, Nessa S, Al-Shaer E, et al. Vulnerability analysis for evaluating quality of protection of security policies[C]//Proceedings of the 2nd ACM Workshop on Quality of Protection. Alexandria VA, USA, 2006

[11] Payne S C. A Guide to Security Metrics [EB/OL]. http://www.sans.org/reading_room/whitepapers/auditing/55.php, 2008-07-25

[12] 闫强，陈钟，段云所，等. 信息系统安全度量与评估模型[J]. 电子学报，2003，31(9)：1351-1355

[13] 刘学忠，刘增良，余达太. 基于 AHP 度量模型的安全管理度量方法[J]. 微计算机信息，2007，23(18)：33-34

[14] SSE-CMM Author Group. SSE-CMM (V2.06) [M]. SSE-CMM Author Group, 1999

[15] McHugh J. Quality of Protection: Measuring the Unmeasurable [C]//Proceedings of the 2nd ACM Workshop on Quality of Protection. Alexandria VA, USA, 2006

[16] 王涛，郭荷清，姚松涛. 基于综合安全保护质量的安全服务协商模型[J]. 计算机工程与科学，2006，28(4)：26-29