计算机网络脆弱性评价研究

董良喜　王嘉祯
（军械工程学院控制工程系，石家庄 050003）
E-mail：dlxhle@163.net

摘　要　计算机网络的应用越来越广泛，而计算机网络的信息安全问题也越来越突出。造成安全问题的根本原因在于计算机网络系统本身存在脆弱性。脆弱性评价是有效解决网络系统安全问题的必不可少的手段。首先介绍了脆弱性的基本概念，然后介绍了脆弱性评价的基本步骤及内容，包括评价的准备、脆弱性的识别、脆弱性的排序，其中对脆弱性识别作了重点的研究。

关键词　脆弱性评价　信息安全　网络安全　风险评价　脆弱性

文章编号 1002-8331-(2003)20-0157-04　**文献标识码** A　**中图分类号** TP393.08

A Study of Computer Network Vulnerability Assessment

Dong Liangxi　Wang Jiazhen
(Dept.of Control Engineering, Ordnance Engineering College, Shijiazhuang 050003)

Abstract: The computer network has played an important role in the society.But the problem of information security also becomes more severe.There are many causes that lead to insecure problem, but the inherent vulnerability is the most essential.So it is essential to understand the vulnerability and to conduct a comprehensive vulnerability assessment. First, the concept of vulnerability is introduced; then the steps of vulnerability assessment are presented, concluding identifying the vulnerabilities and prioritizing the vulnerabilities.

Keywords: Vulnerability assessment, Information security, Network security, Risk assessment, Vulnerability

1　引言

计算机网络的应用越来越广泛，而计算机网络的信息安全问题也越来越突出。造成计算机网络安全问题的原因很多，但是可以把它们归纳为两大类：即外在的威胁和内在的脆弱性。从威胁的角度来看，潜在的威胁源增多，威胁发生的可能性增大。这主要表现在：拥有计算机知识的人数的迅速增长，使得数以百万计的人拥有攻击技能；网络系统广泛采用公共协议、“黑客”工具库很容易获得、进行一次有效攻击所需代价降低，攻击更容易进行；人们对网络的依赖性增强，对网络进行成功的攻击可使攻击者获得较大的利益，可使被攻击者遭受重大损失。如果把威胁看作外因，那么系统不安全的内因，也可以说最根本的原因，在于计算机网络本身存在脆弱性，而且这种脆弱性问题也越来越严重。这主要表现在：网络结构越来越复杂；网络越来越庞大；网络中采用的新技术有些还不能为使用者和管理者掌握；网络中一些软件、硬件由于各种原因在还未完善时就开始被应用；为克服系统中原始的脆弱性而采用的各种控制措施带来新的脆弱性；……。对已知的攻击者或入侵者行为进行监测的传统安全方法已经不能完全适应网络安全的要求，基础设施防卫的第一线应当是在脆弱性被利用前去识别和减少或消除脆弱性[1]。

2　脆弱性基本概念

2.1　脆弱性概念

系统如果遭受损失，最根本的原因在于系统本身存在脆弱性。因为攻击者只有利用了系统的脆弱性，攻击才能成功。系统的脆弱性包括系统最初存在的脆弱性和后来增加的安全措施存在的脆弱性。所谓脆弱性，是指系统中存在的漏洞：各种潜在威胁通过对这些漏洞的利用而给系统造成损失。图 1 给出了威胁、脆弱性、系统间的关系示意图。脆弱性存在于系统安全程序、设计、应用或内部控制等方面。

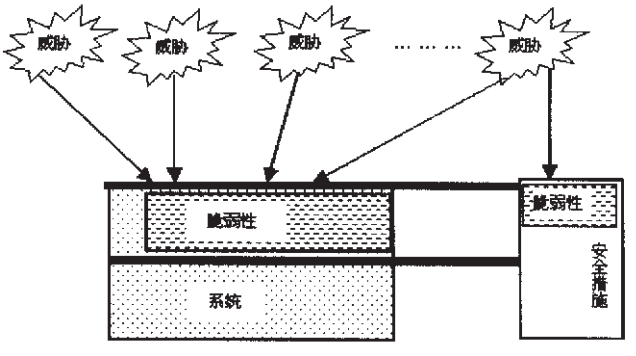

图 1　脆弱性、威胁、系统关系图

2.2　脆弱性基本类型

脆弱性有四种基本类型[2]，它与两个因素有关，一个是脆弱性影响的目标，包括人员和计算机，二是脆弱性影响的快慢。可以用表 1 来表示。

作者简介：董良喜(1969-)，男，博士生，研究方向：装备保障指挥及其自动化。王嘉祯，男，博士生导师，主要研究方向：计算机技术及应用，信息安全。

表 1　脆弱性基本类型

	影响人员	影响计算机
瞬间	社会工程	逻辑错误
需要一段时间	策略疏忽	弱点

表 1 中，横向表示的是影响的目标，纵向表示的是影响的快慢。如“社会工程”、“策略疏忽”主要与人有关，“逻辑错误”、“弱点”主要与计算机有关；“逻辑错误”对计算机安全的影响要比“弱点”影响快。

逻辑错误是改变安全效果的捷径，通常指的是基本的“bug”。该错误是在软件设计或软件编程时存在的，它将导致安全违反情况的发生。尽管现代技术、增强的设计及严格的标准将对软件的安全起到重要作用，但是现在的软件在编程、操作系统、及安全设计上的复杂性，使总的安全风险增加。此外，方便用户的同时也方便了入侵者，好的意图经常产生大的安全漏洞。逻辑错误最显著的一个特点是，它只需极短的时间和计算机交互就可危及安全，而且在作用时只需非常少的人力。它造成了最危险的计算机安全问题。

弱点。通常系统中都运用了安全控制措施，但是许多安全措施在设计上存在能导致违反安全的缺点，这被称为系统的弱点。逻辑错误和弱点的明显区别是：逻辑错误绝对地缺少安全——或是安全措施不正确，或是在设计时就缺少安全考虑，而弱点则是运用了安全措施，只是这些安全措施本身有缺点。

社会工程。通过社会工程，“黑客”可获得许多私人信息，这和其它方法相比往往是比较简单的。黑客往往通过日常交往及在电话、网上交流中获取需要的信息，有时候还可能通过相关人员丢弃的垃圾而获取对他来说有用的信息。此外，还可通过破坏、敲诈等更恶劣的手段来获取相关信息。因此，此种脆弱性主要和人有关。

策略疏忽是指系统安全策略中存在的缺陷。如，安全策略没有支持系统管理人员对计算机犯罪人员进行追踪，这将导致所有的已经建立的安全措施不能有效地保护组织的利益。

3　脆弱性评价基本方法

脆弱性评价是计算机系统和网络防护中的一种重要手段。正确地进行脆弱性评价，可以帮助管理人员明白计算机网络系统当前安全状态，使其明白当前需要做什么，并帮助其制定控制计划。

3.1　评价准备

3.1.1　系统描述

在这一步中，系统的边界被确定，同时被确定的还有构成系统的资源和信息。对 IT 系统的描述，建立了评价对象，提供了确定脆弱性所必需的基本信息（如，硬件、软件、系统连接及负责的部门或保障人员）。网络映射和确定网络体系结构是这一步中的重要内容。

通过网络映射和网络体系结构的确定，理解整个网络系统的基本情况并确定关键网络资产，为进行网络系统的脆弱性评价作准备。

网络映射是用于帮助理解要评价的网络体系结构是什么样的，还包括从这个网络上能得到什么样的信息。市场上有许多好的工具可以帮助进行网络映射工作。这一阶段用于确定网络上的各个单个系统及它们相互间的关系。随后将进行个人主机上服务的映射。这一阶段不应单纯地依赖映射工具。

评价者有着入侵者所不具有的优势，即可以访问系统管理员、评论网络映射并讨论网络的规划。进行网络映射的目标是：明白系统体系结构并确定可以运行扫描工具的种类、位置及评价所需的技能。如果仅在网络的一个位置进行扫描，将会遗漏某些关键的节点。如，把扫描器安装在运用网络集线器的子网中，只能获得有关这个子网的情况。运用网络映射，可以确定扫描策略并选择用于网络上每个部分的特定工具。

一旦有了网络映射，就可以对网络体系结构进行考察。可以考虑类似下面的问题：

（1）有 DMZ 吗？

（2）有哪些主机（域名服务器 DNSs 不应当和 Web 服务器处于同一系统中）？

（3）有防火墙吗？

体系结构的另一个重要方面是数据流。可以考虑类似下面的问题：

（1）网络中不同的服务器如何相互信任？

（2）数据之间是如何流通的？

找出网络应用中用扫描工具难以发现的可能的缺陷。这个阶段，没有工具可以足够自动地帮助评价，必须依靠评价者的评价训练和渊博的知识。

在系统描述过程中，不仅要了解网络的基本情况，还应掌握关键的网络资产，以便在进行评价时有重点地进行。这在大型网络中尤其重要。对于信息资产的敏感性或重要性，一般应基于完整性、机密性、可用性来进行评价。对于有形的资产，如硬件，可直接用定量的方法来衡量。人员要素应当作为重要的考虑因素。这不仅是由人的生命价值决定的，还由于有些具有关键技能、处于关键位置的人，不容易有候补的，不容易被替代。因此应确定处于关键位置的人员。

3.1.2　评价计划的编制

在这个阶段，需要与网络管理员和其它一些人员协调，因为在评价时，网络流量可能要影响到某些实体。如果还涉及到商业 ISP，这时也应把要做的事通知他们。

计划的编制包括确定评价的类型（如，对一个主机进行评价、对 Web 服务器进行评价等）及准备进行的特定测试。工具和方法的选取完全依赖于要进行的评价。如，当计划在一个 Web 服务器上对一个主机进行评价，就没必要进行子网的映射。

计划编制可能包括以下步骤[3]：

（1）接受任务/验证需求；

表 2　脆弱性

脆弱性	威胁源	威胁行为
被解雇的雇员的 ID 没有从系统中去掉	解雇的雇员	拨号进入公司的网络并访问公司所有的数据
销售商已经发现了系统在安全设计上的缺点，但是系统中没有使用新的安全补丁	未授权的用户（如，黑客、不满的雇员、计算机犯罪分子、恐怖主义分子）	基于已知的脆弱性获得对敏感系统文件的未授权访问
数据中心用喷水装置来灭火，保护硬件和设备不受水灾损害的防水布没有在位	火、疏忽的人员	打开数据中心的喷水装置

(2)开发初步计划；

(3)指定职责；

(4)进行评价前的协调工作。

一旦接受评价任务，就应当和用户进行协商，如一些敏感信息是否可以看，对有些主机或其它设备是否可以进行渗透性测试等。

一般说来，评价组规模较小。如果有好几个评价成员，可以进行任务分工，如分为技术/扫描组、管理/策略检查组等。评估组应当由熟悉审计、通信、网络、信息安全、人员的安全、训练、教育等方面的人员组成。

3.2 脆弱性识别

这一步的目的是制定可能被潜在威胁源利用的系统脆弱性清单。表 2 给出了脆弱性的例子。

确定脆弱性的方法有：运用脆弱性原始资料；系统性能安全测试；开发安全需求一览表[4]。

需要注意的是，可能存在的脆弱性各种各样，脆弱性和用于确定具体的脆弱性是否存在的方法通常都随系统的性质及其所处于的系统开发生命周期(SDLC)的阶段而变化。

与系统处理环境有关的技术上的和非技术的脆弱性，可以通过以下的收集信息的方法来识别：

(1)简会。召集相关的行政管理人员，召开简会，收集信息。

(2)现场调查。会见系统的保障和管理人员能使评价人员收集到有关系统有用的信息(如，系统是如何运行和管理的)。现场调查还可观察和收集有关系统物理的、环境的及运行安全方面的信息。

(3)文档审查。策略文档(如，法规文件、指示)、系统文档(如，系统用户指南、系统管理员手册、系统设计和需求文档、采购文档)、及安全相关的文档(如以前的审计报告、风险评估报告、系统测试结果、系统安全计划、安全策略)都可提供系统使用的或计划的安全控制方面的信息。任务影响分析或资产重要性评估可提供有关系统和数据重要性及敏感性的信息。

(4)测试、仿真等。包括运用自动化扫描工具。

(5)问题调查表法。为收集相关的信息，评价人员可以开发与系统管理和运行控制相关的问题调查表。调查表应当分发给那些设计和保障网络系统的技术和非技术人员。这些表还可用于现场访问和会见。随着网络的广泛运用，基于 web 的问题调查表，可大大方便调查的进行，同时也便于对调查结果的处理。

3.2.1 利用脆弱性原始资料

在为确定特定系统(如，一个特定操作系统的特定版本)的脆弱性而准备会见以及在开发有效的问题调查表时，仔细查看相关的信息源(如，确定系统"bug"和缺点的销售商的网页)是非常有用的。Internet 是一个关于销售商提供的已知的系统脆弱性的信息源，包括紧急修补、服务包、补丁及其它可用于消除和减少脆弱性的补救措施。在进行全面的脆弱性分析时应当考虑的脆弱性原始资料包括：

(1)被评价的系统以前的风险评价文档；

(2)系统的审计报告、系统异常报告、安全审查报告及系统测试和评价的报告；

(3)脆弱性清单；

(4)安全咨询组织；

(5)销售商咨询人员；

(6)商业计算机事件/紧急响应组及邮递列表(如，Secury Focus.com 论坛邮件)；

(7)军事系统的信息保障脆弱性警告和公告；

(8)系统软件安全分析员。

3.2.2 系统安全测试

系统测试，是一种主动的方法，可有效确定系统的脆弱性。这种方法的有效性依赖于系统的重要性及可用的资源（如，分配的资金、可用的技术、用于测试的具有专业技能的人员)。测试方法包括：自动化脆弱性扫描工具；安全测试与评价(ST&E)；渗透性测试。这三种方法各自并不具有排它性。

自动化脆弱性扫描工具用于一组主机或一个网络，用以获取脆弱性服务(如，系统允许匿名的 FTP、发送邮件中继)。然而，应当注意由自动化扫描工具识别的一些潜在的脆弱性可能并不代表在系统真实环境下会出现。例如，有些自动化扫描工具在为脆弱性分等级时没有考虑场所的环境和需求。有些被自动化扫描工具标为脆弱性可能对于特定的场所来说实际上并不脆弱，有些配置可能是因为环境的需要。因此这种方法可能产生"虚警"。而又由于新的脆弱性不断地被发现，自动化工具的脆弱性数据库不可能包含所有的脆弱性，因此，它又可能产生"漏报"。扫描工具的选择要综合考虑工具的性能、成本、专业需求、可靠性等方面。此外扫描工具的使用时机对扫描的结果也有着较大的影响[5]。

ST&E 是另一种用于识别系统脆弱性的方法。它包括开发和执行测试计划(如，测试脚本、测试程序及预期的测试结果)。系统安全测试的目的是测试已经运用于运行环境中的系统安全控制的效力。目标是确保所采用的控制措施满足已经批准的软件和硬件规范，而且这些措施应用了组织的安全策略或满足工业/军用标准。

渗透性测试可用于对安全控制审查的补充并确保系统的不同侧面都是安全的。渗透性测试，可用于评价一个系统抗御企图攻破系统的能力。它的目标是从威胁源的角度来测试系统并确定系统保护计划中潜在的疏忽。渗透性测试有两种，一种通常称为"红色评价(Red Teaming)"，测试时，进行有控制的攻击，测试者扮演入侵者的角色；另外一种称为"蓝色评价(Blue Teaming)"，用于验证脆弱性。

3.2.3 开发安全需求清单

在这一步中，评价人员确定现有的或计划的安全控制是否满足系统所规定的及在系统描述期间所收集的安全需求。典型的系统安全需求可用表格的形式给出，其中每个需求都有一个关于在系统设计或实现过程中如何满足及不满足安全控制需求的说明。

安全需求清单包含基本的安全标准，这些标准可用于系统地评价和识别资产、自动化程序、过程及信息传输的脆弱性，主要包括下列范围：

(1)管理安全。主要的安全准则有：指定责任；连续支持；事件响应能力；周期性安全控制审查；人员安全调查和背景调查；风险评价；安全和技术训练；权力分割；系统授权或再授权；系统或应用安全计划。

(2)操作安全。主要的安全准则有：空气污染(如，烟、尘、化学制品)的控制；确保电力供应的控制；数据媒介的访问和处理；外部数据的分发和标记；设施的保护(如，计算机室、数据中心、办公室)；湿度控制；温度控制；工作站、膝上型电脑及独立运行的 PC。

(3)技术安全。主要的安全准则有:通信(如,拨号、系统互连、路由器);加密;自主访问控制;识别和认证;入侵检测;目标滥用;系统审计。

可用于制定安全需求清单的资料包括下列政府法规、安全指示及可适用于系统处理环境的其它资料:

(1)与计算机或网络安全相关的法律、法规。

(2)相关的标准或其它出版物。

(3)系统安全计划。

(4)组织安全策略、指南和标准。

(5)工业实践。

3.3 脆弱性排序

对一个大的网络系统来说,通过严格的测评,可能会发现上百个脆弱性。为补救和减少脆弱性而建立一个优先顺序,是这一步的目的所在。

通常,排序是按一定的级别来排序,如按脆弱性的严重性来排序,其严重性可分为高、中、低或类似的等级来划分。严重性可按脆弱性被利用后可能产生的影响大小来分,也可按攻击者对系统获取的权限来分,具体划分可根据情况来定。前者常用信息完整性、机密性、可用性、审计性的危害程度来表示。表3给出了一个示例。

表3 脆弱性排序表

脆弱性	完整性	机密性	可用性	审计性	抗否认性	可控性
脆弱性1	高	中	中	低	高	中
脆弱性2	中	高	中	高	低	低
脆弱性3	高	中	低	低	中	中
脆弱性“n”	高	高	中	低	低	低

对于脆弱性比较多的情况,以图形的形式来总结每个优先类别的脆弱性数目,往往比较直观。

最后,和一般的评价相似,评价应提交评价报告,在报告中,对系统中的脆弱性进行总结,并提出相应的减少或消除脆弱性的安全措施。

4 结束语

脆弱性评价是保证网络信息安全不可缺少的手段,但是它本身只是保证网络安全的一个环节,在它之前要进行威胁评价,之后要进行控制分析、采取控制措施。需要指出的是,信息安全是一个动态的概念,因此,脆弱性评价需要周期性地进行。这一方面是由于网络新的脆弱性不断被发现,另一方面,网络系统本身也是动态的,它的组成要素是变化的,可能会产生新的脆弱性,而与此同时,原先的存在的脆弱性有些可能仍然存在,也可能不再存在。(收稿日期:2002年7月)

参考文献

1.KPMG Peat Marwick LLP.Vulnerability Assessment Framework 1.1[M].CIAO publications,1998

2.Eric Knight.Computer Vulnerabilities[M].2000

3.John R Sciandra.Holistic Vulnerability Assessment Methodologies.http://www.nacon.com/papers/whitepaper.pdf,2001

4.Gary Stoneburner,Alice Goguen,Alexis Feringa.NIST Special Publication 800-30:Risk Management Guide for Information Technology System[M].WASHINGTON:U S GOVERNMENT PRINTING OFFICE,2001

5.ISS.Network and Host-based Vulnerability Assessment:A guide for information systems and network security professionals.http://documents.iss.net/whitepapers/nva.pdf,2001

(上接138页)

产品 m,M 将得到正确的支付。他们的交易是公平的。如果双方中有一方有不诚实行为,支付网关将卷入协调他们的争执。以使双方交易达到公平。

4.2.1 M 不诚实

当 M 在收到支付网关 P 所发的已讫消息 Msg 后,不向客户 C 发送密钥 $K1$,或发送不正确的密钥 $K1$。那么客户只需与支付网关取得联系,支付网关只需查本服务器所保留的交易记录,确定客户确实支付,支付网关同商家 M 联系,要求商家发送密钥 $K1$,若商家不同意或消失,支付网关就将自己保存密钥 $K1$ 送给客户 C。

4.2.2 C 不诚实

若客户 C 已收到正确的密钥 $K1$,却声称没有收到,解决方法同上(注:客户 C 多次得到同一密钥 $K1$ 是不会多得任何额外利益)。

可见该协议流程能保证双方的公平交易。

4.3 交易原子性分析

由于原有的SET协议已满足钱的原子性,这里主要分析商品原子性和发送确认原子性。

4.3.1 商品原子性分析

从协议的执行和公平交易分析可知,商家只有在收到支付网关返回的已讫消息 Msg 后,才会向客户发送解密密钥 $K1$,同时,只有当客户 C 正确支付商品 m 的款后,才会得到加密商品的解密密钥 $K1$。这样该协议就保证了购买者如果付了款就一定会得到商品,不存在得了商品而未曾付款或付了款而得不到商品的情况。

4.3.2 确认发送原子性分析

从协议的消息4,5,7中可分析得,客户 C 在最后解密出的商品 m,是客户 C 和支付网关所验证正确的商品,并且只有是正确后,支付网关才将客户的支付送发卡行 I。因此,修改后的协议就满足确认发送原子性,即客户 C 所得的商品是他所订购的商品,产家也发送了客户所订购的商品。

5 结束语

文章基于SET协议提出了一个更有效的安全电子协议方案,该方案保持了原有SET协议的安全特性,同时在针对数字商品的交易上,该方案能保证顾客与商家的公平交易,以及协议流程交易的原子性。(收稿日期:2002年8月)

参考文献

1.Visa and Master Card:SET Sepecification.Books,1997-05

2.Tygar J D.Atomicity in Electronic Commerce[C].In:Proceedings of the 15th Annual ACM Symposium on principles of Distributed Computing,1996:8~26

3.Kailer R.Accounability in Electronic Commerce Protocols[J].IEEE Transactions on Software Engineering,1996;22(5):313~328

4.周龙骧.电子商务协议研究综述[J].软件学报,2001;12(7):1015~1029

5.Putland P A,Hill J,Tsapikidis D.Electronic payment systems[J].BT Technology Journal,1997;15(2):32~38