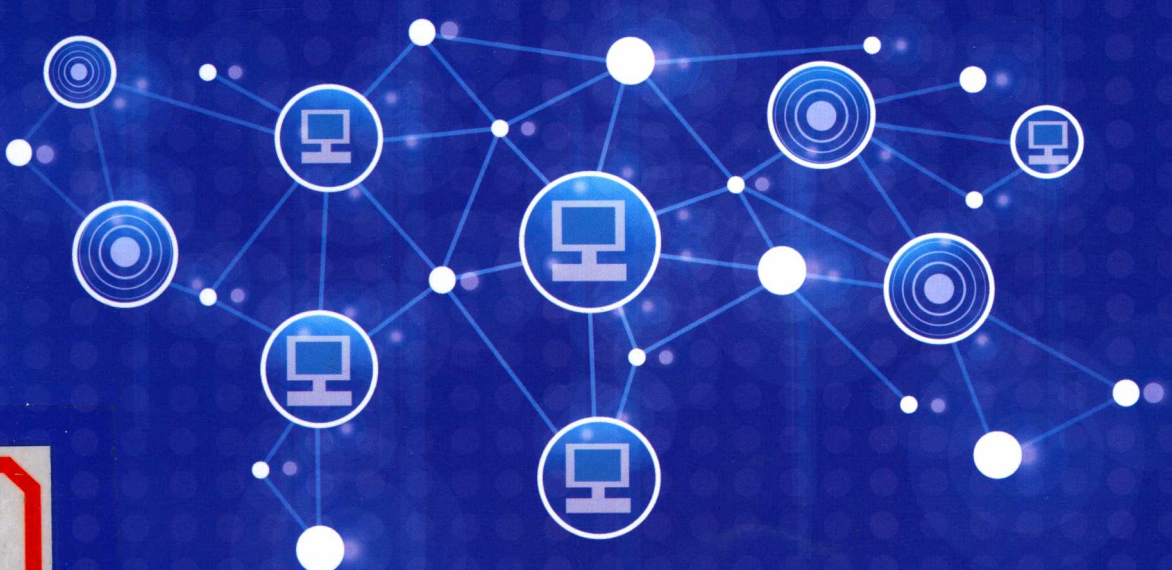
计算机网络安全

实践教程

严小红　靳　艾　主编



电子科技大学出版社

计算机网络安全

实践教程

严小红　靳　艾　主编

电子科技大学出版社

图书在版编目（CIP）数据

计算机网络安全实践教程 / 严小红，靳艾主编. —
成都：电子科技大学出版社，2017.7
ISBN 978-7-5647-4685-8

Ⅰ. ①计… Ⅱ. ①严… ②靳… Ⅲ. ①计算机网络－
安全技术－高等学校－教材 Ⅳ. ① TP393.08

中国版本图书馆 CIP 数据核字（2017）第 143165 号

计算机网络安全实践教程

严小红 靳艾 主编

出　　版：电子科技大学出版社（成都市一环路东一段 159 号电子信息产业大厦 邮编：610051）
策划编辑：罗　雅
责任编辑：罗　雅
特邀编辑：朱　丹
主　　页：www.uestcp.com.cn
电子邮箱：uestcp@uestcp.com.cn
发　　行：新华书店经销
印　　刷：成都市火炬印务有限公司
成品尺寸：185mm×260mm　　印张 12.5　　字数 300 千字
版　　次：2017 年 7 月第一版
印　　次：2017 年 7 月第一次印刷
书　　号：ISBN 978-7-5647-4685-8
定　　价：42.00 元

前　言

目前，计算机网络安全教材百花齐放，各有特色，但总体上可以分成三类。第一类着重讨论加密、鉴别算法及其他安全协议，这一类教材的特点是比较详细地讲述网络安全理论，尤其对各种算法和协议做了深入讨论，但缺乏和当前主流网络安全技术的结合，很难让读者学以致用。第二类主要讨论黑客攻击手段和防御技巧，这一类教材不介绍系统、完整的网络安全理论，有点像黑客攻防大全。第三类是大杂烩，把操作系统安全机制、应用程序安全机制和网络安全机制放在一起讨论，当然，所有内容都是浅尝辄止。这三类教材虽然侧重点不同，但是存在同样的问题：一是不对当前主流网络安全技术进行深入讨论；二是不在具体网络环境下讨论安全网络的设计方法和过程，对许多问题只是空对空地介绍一些基本概念和方法，没有具体结合目前面临的网络安全问题，更没有应用实例。因此，无法培养读者解决网络安全问题的实际能力。

一本真正以实现将读者领进计算机网络安全知识殿堂为教学目标的教材必须具备如下几点：(1)必须提供完整、系统的网络安全理论，这样才能让读者理解网络安全技术的实现机制，具有进一步研究网络安全技术的能力；(2)必须深入讨论当前主流网络安全技术，同时，结合网络安全理论讨论这些安全技术的实现原理，让读者知其所以然，也让读者具备用主流网络安全技术解决实际网络安全问题的能力；(3)需要在具体网络环境下讨论运用网络安全技术设计安全网络的方法和过程，给读者提供解决实际网络安全问题的方法和思路，解决读者学以致用的问题。

作为计算机网络安全教材，应该着重讨论和网络有关的安全问题，和操作系统及应用程序有关的安全问题应该在“操作系统”和“算法与程序设计”课程中予以解决，因为离散地讨论一些安全问题会降低该教材的系统性和连贯性，同时，不和整个操作系统结构和程序设计环境结合来讨论操作系统和应用程序安全问题的解决机制，也不利于读者理解、掌握。计算机网络安全教材不可避免地会涉及黑客攻击和防御，但必须从网络总体结构出发，讨论防御黑客攻击的技术，而不是逐个列出攻击手段和防御方法，将教材变成黑客攻防大全，背离了教材着重于基本理论、基本技术和基本方法的宗旨。

本书编写过程中参考了有关专著和其他文献，在此向有关作者致以崇高的敬意和深深的感激。本书中肯定存在疏漏或不足之处，恳切希望同行和广大读者不吝指正。

编　者

目　录

项目一　计算机网络安全概述

任务一　网络安全简介

一、网络安全的重要性

随着信息科技的迅速发展以及计算机网络的普及，计算机网络深入国家的政府、军事、文教、金融、商业等诸多领域，可以说网络无处不在。资源共享和计算机网络安全一直作为一对矛盾体而存在着，计算机网络资源共享进一步加强，信息安全问题日益突出。

互联网在我国政治、经济、文化以及社会生活中发挥着愈来愈重要的作用，作为国家关键基础设施和新的生产、生活工具，互联网的发展极大地促进了信息流通和共享，提高了社会生产效率和人民生活水平，促进了经济社会的发展。互联网的影响日益扩大、地位日益提升，维护网络安全工作的重要性日益突出。

网络系统失灵会造成通信瘫痪、基础设施损坏、大范围停电、船只停航等重大事故。1992 年，美国联邦航空管理局的一条光缆被无意间挖断，所属的 4 个主要空中交通管制中心关闭 35 小时，成百上千航班被延误或取消。1996 年，世界最大计算机信息服务网络公司——美国联机公司，在正常维护中更换一款新软件后发生故障，造成了大规模服务中断事件，包括众多企业在内的 600 多万用户 19 小时无法使用电子邮件、互联网接入等，有的企业遭受了巨大的经济损失。2008 年 3 月，英国伦敦希斯罗机场第五航站楼的电子网络系统在启用当天就发生故障，致使五号航站楼陷入混乱。

据国家计算机网络应急技术处理协调中心（CNCERT）监测，每年都会有非常多的网络安全攻击事件发生。除了攻击事件，病毒对网络安全的影响也越来越大，金山网络公司为近几年来的新增病毒/木马数量进行了对比，如图 1 - 1 所示。2009 年，计算机病毒/木马仍处于一种高速“出新”的状态。2010 年病毒/木马增长速度与 2009 年相比有所放缓，但仍处于大幅增长状态，总数量还是非常庞大的。各种计算机病毒和网上黑客对 Internet 的攻击越来越猛烈，网站遭受破坏的事例不胜枚举。

2006 年第 38 个世界电信日暨首个世界信息社会日的主题是“Promoting Global Cyber Security”（推进全球网络安全）。这充分体现出网络安全不再是一个潜在的问题，已经成为当前信息社会现实存在的重大问题，与国家安全息息相关，涉及国家政治和军事命脉，影响国家的安全和主权。

一些发达国家如英国、美国、日本、俄罗斯等把国家网络安全纳入了国家安全体系。信息安全空间将成为传统的国界、领海、领空的三大国防和基于太空的第四国防之外的第五国防，称为 Cyber-Space。美国政府在 2009 年 5 月发表的《网络空间政策评估报告》，将网络空

间定义为“全球相互连接的数字信息和通信基础设施”。

因此，网络安全不仅成为商家关注的焦点，还是技术研究的热门领域，同时也是国家和政府关注的焦点。

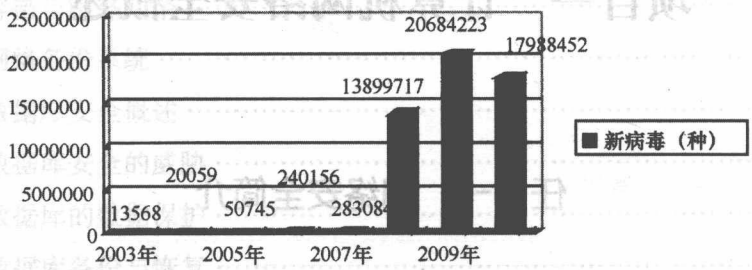


图 1－1　新增加病毒统计(2003～2010 年)

二、网络脆弱性的原因

(一)开放性的网络环境

正如一句非常经典的语句所说：“Internet 的美妙之处在于你和每个人都能互相联结，Internet 的可怕之处在于每个人都能和你互相联结。”

网络空间之所以易受攻击，是因为网络系统具有开放、快速、分散、互联、虚拟、脆弱等特点。网络用户可以自由访问任何网站，几乎不受时间和空间的限制。信息传输速度极快，病毒等有害信息可在网上迅速扩散和放大。网络基础设施和终端设备数量众多，分布地域广阔，各种信息系统互联互通，用户身份和位置真假难辨，构成了一个庞大而复杂的虚拟环境。此外，网络软件和协议存在许多技术漏洞，为攻击者提供了可乘之机。这些特点都给网络空间的管控造成了巨大的困难。

Internet 是跨国界的，这意味着网络的攻击不仅仅来自本地网络的用户，也可以来自 Internet 上的任何一台机器。Internet 是一个虚拟的世界，所以无法得知联机的另一端是谁。图 1－2 所示为网上非常出名的一幅图片。在这个虚拟的世界里，已经超越了国界，某些法律也受到了挑战，因此网络安全面临的是一个国际化的挑战。

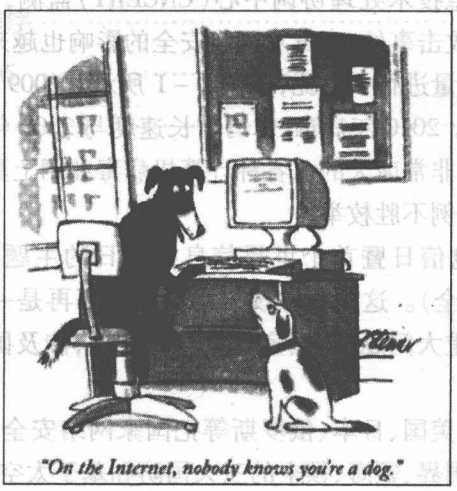


图 1－2　网上图片

网络建立初期只考虑方便性、开放性，并没有考虑总体安全构想，因此任何一个人、团体都可以接入，网络所面临的破坏和攻击可能是多方面的。例如，可能是对物理传输线路的攻击，也可能是对网络通信协议及应用的攻击；可能是对软件的攻击，也可能是对硬件的攻击。

（二）协议本身的脆弱性

网络传输离不开通信协议，而这些协议也有不同层次、不同方面的漏洞，针对 TCP/IP 等协议的攻击非常多，在以下几个方面都有攻击的案例。

1. 网络应用层服务的安全隐患。例如，攻击者可以利用 FTP、Login、Finger、Whois、WWW 等服务来获取信息或取得权限。

2. IP 层通信的易欺骗性。由于 TCP/IP 本身的缺陷，IP 层数据包是不需要认证的，攻击者可以假冒其他用户进行通信，即 IP 欺骗。

3. 针对 ARP 的欺骗性。ARP 是网络通信中非常重要的协议，基于 ARP 的工作原理，攻击者可以假冒网关，阻止用户上网，即 ARP 欺骗。近一年来 ARP 攻击更与病毒结合在一起，破坏网络的连通性。

4. 局域网中以太网协议的数据传输机制是广播发送，使系统和网络具有易被监视性。在网络上，黑客能用嗅探软件监听到口令和其他敏感信息。

（三）操作系统的漏洞

网络离不开操作系统，操作系统的安全性对网络安全同样有非常重要的影响，有很多网络攻击方法都是从寻找操作系统的缺陷入手的。操作系统的缺陷有以下几个方面。

1. 系统模型本身的缺陷。这是系统设计初期就存在的，无法通过修改操作系统程序的源代码来弥补。

2. 操作系统程序的源代码存在 Bug。操作系统也是一个计算机程序，任何程序都会有 Bug，操作系统也不会例外。例如. ，冲击波病毒针对的就是 Windows 操作系统的 RPC 缓冲区溢出漏洞。那些公布了源代码的操作系统所受到的威胁更大，黑客会分析其源代码，找到漏洞进行攻击。

3. 操作系统程序的配置不正确。许多操作系统的默认配置安全性很差，进行安全配置比较复杂，并且需要一定的安全知识，许多用户并没有这方面的能力，如果没有正确地配置这些功能，也会造成一些系统的安全缺陷。

Microsoft 公司在 2010 年发布了 106 个安全公告，修补了 247 个操作系统的漏洞，比 2009 年多 57 个。漏洞的大量出现和不断快速增加补丁是网络安全总体形势趋于严峻的重要原因之一。不仅仅操作系统存在这样的问题，其他应用系统也一样。比如：微软公司在 2010 年 12 月推出 17 款补丁，用于修复 Windows 操作系统、IE 浏览器、Office 软件等存在的 40 个安全漏洞。在我们实际的应用软件中，可能存在的安全漏洞更多。

（四）人为因素

许多公司和用户的网络安全意识薄弱、思想麻痹，这些管理上的人为因素也影响了安全。

三、网络安全的定义

国际标准化组织（ISO）引用 ISO 74982 文献中对安全的定义：安全就是最大程度地减少

数据和资源被攻击的可能性。

《计算机信息系统安全保护条例》的第三条规范了包括计算机网络系统在内的计算机信息系统安全的概念:“计算机信息系统的安全保护,应当保障计算机及其相关的和配套的设备、设施(含网络)的安全,运行环境的安全,保障信息的安全,保障计算机功能的正常发挥,以维护计算机信息系统的安全运行。”

从本质上讲,网络安全是指网络系统的硬件、软件和系统中的数据受到保护,不受偶然的或者恶意的攻击而遭到破坏、更改、泄露,系统连续、可靠、正常地运行,网络服务不中断。广义上讲,凡是涉及网络上信息的保密性、完整性、可用性、可控性和不可否认性的相关技术和理论都是网络安全所要研究的领域。

欧共体对信息安全给出如下定义:“网络与信息安全可被理解为在既定的密级条件下,网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将危及所存储或传输的数据,以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和秘密性。”

网络安全的具体含义会随着重视“角度”的变化而变化。例如,从用户(个人、企业等)的角度来说,希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私。从网络运行和管理者的角度来说,希望对本地网络信息的访问、读、写等操作受到保护和控制,避免出现后门、病毒、非法存取、拒绝服务和网络资源非法占用和非法控制等威胁,制止和防御网络黑客的攻击。从安全保密部门的角度来说,希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵,避免机要信息泄露,避免对社会产生危害、对国家造成巨大损失。从社会教育和意识形态的角度来说,网络上不健康的内容会对社会的稳定和人类的发展造成阻碍,必须对其进行控制。

四、网络安全的基本要素

网络安全的目的:保障网络中的信息安全,防止非授权用户的进入以及事后的安全审计。

上述目的也就是网络安全的5个基本要素,即保密性(Confidentiality)、完整性(Integrity)、可用性(Availability)、可控性(Controllability)与不可否认性(Non-Repudiation)。

(一)保密性

保密性是指保证信息不能被非授权访问,即非授权用户得到信息也无法知晓信息内容,因而不能使用。通常通过访问控制阻止非授权用户获得机密信息,还通过加密阻止非授权用户获知信息内容,确保信息不暴露给未授权的实体或者进程。

(二)完整性

完整性是指只有得到允许的人才能修改实体或者进程,并且能够判断实体或者进程是否已被修改。一般通过访问控制阻止篡改行为,同时通过消息摘要算法来检验信息是否被篡改。

(三)可用性

可用性是信息资源服务功能和性能可靠性的度量,涉及物理、网络、系统、数据、应用和用户等多方面的因素,是对信息网络总体可靠性的要求。授权用户根据需要,可以随时访问

所需信息，攻击者不能占用所有的资源而阻碍授权者的工作。使用访问控制机制阻止非授权用户进入网络，使静态信息可见，动态信息可操作。

（四）可控性

可控性主要是指对危害国家信息（包括利用加密的非法通信活动）的监视审计，控制授权范围内的信息的流向及行为方式。使用授权机制，控制信息传播的范围、内容，必要时能恢复密钥，实现对网络资源及信息的可控性。

（五）不可否认性

不可否认性是对出现的安全问题提供调查的依据和手段。使用审计、监控、防抵赖等安全机制，使攻击者、破坏者、抵赖者“逃不脱”，并进一步对网络出现的安全问题提供调查依据和手段，实现信息安全的可审查性，一般通过数字签名等技术来实现不可否认性。

五、典型的网络安全事件

网络安全事件不计其数，典型的网络安全事件如表 1－1 所示。

表 1－1　典型安全事件

时间	发生的主要事件
1983 年	美国联邦调查局首次逮捕了 6 名少年黑客，因其所居住的地区密尔沃基电话区号是 414 而被称做“414 黑客”。这 6 名少年黑客被控侵入 60 多台计算机，其中包括斯洛恩. 凯特林癌症纪念中心和洛斯阿拉莫斯国家实验室
1988 年	康奈尔大学研究生罗伯特·莫里斯（22 岁）向 Internet 上传了一个“蠕虫”程序。这个程序是他为攻击 UNIX 系统的缺陷而设计的，能够进入网络中的其他计算机并自我繁衍。当时使得美国 6000 多个系统（几乎占当时 Internet 的 1/10）陷入瘫痪，专家称这个“蠕虫”程序造成了 1500 万到 1 亿美元的经济损失
1995 年	米特尼克被逮捕。他被指控闯入许多计算机网络，偷窃了 2 万个信用卡号和复制软件。他曾闯入“北美空中防务指挥系统”，破译了美国著名的“太平洋电话公司”在南加利福尼亚州通信网络的“改户密码”，入侵过美国 DEC 等 5 家大公司的网络。专家们测算，米特尼克一人就造成了美国一些公司 8000 万美元的巨额损失
1999 年 4 月	台湾大同工学院资讯工程系学生陈盈豪所制造的“CIH”病毒，在 26 日发作，引起全球震撼。保守估计全球有 6 千万台计算机受害
2000 年 2 月	以“雅虎”为首的美国一系列大型网站遭到了黑客有组织的攻击，他们攻击的目标包括雅虎、电子港湾、亚马孙、微软网络等美国大型网站。据统计，在 2 月 7、8、9 日这短短的 3 天里，这些受害公司的损失就超过了 10 亿美元，其中仅营销和广告收入一项便高达 1 亿美元
2001 年 9 月	“9·11”事件促使人们更加重视网络安全以及灾后恢复能力，事件后，美国国务院在贝尔茨维尔建立了一个网络监视中心。美国加大了网络安全技术的研发力度，并积极采取措施，在网络防御实践中使用新的安全防护技术
2002 年 10 月	黑客用 DoS 攻击影响了 13 个根 DNS（DomainNameServer）中的 8 个，作为整个 Internet 通信路标的关键系统遭到严重的破坏

时间	发生的主要事件
2003 年 1 月	出现“蠕虫王”病毒，利用 Microsoft SQL Server 的漏洞进行传播，由于 Microsoft SQL Server 在世界范围内都很普及，因此此次病毒攻击导致全球范围内的 Internet 瘫痪，全世界范围内损失额高达 12 亿美元
2004 年 10 月	国内的腾讯 QQ、神州数码、江民公司、一家著名电子商务网站陆续被黑客攻陷或入侵。其中一些网站还受到了黑客的巨额敲诈勒索，这是国内首起网络黑客勒索事件
2006 年	防止恶意软件对内核的非授权修改，Microsoft 通过 Patch Guard 技术能够封杀对 64 位版 Windows Vista 内核的访问，以赛门铁克、McAfee 为代表的安全厂商声称，它们需要访问操作系统内核，探测 rootkit 等恶意软件。在受到来自欧盟委员会和韩国监管机构的压力后，Microsoft 同意开放访问内核的 API，但是，厂商需要等到 Microsoft 发布 Vista SP1 后才能够使用这些 API
2007 年	超过 9400 万名用户的 Visa 和 MasterCard 信用卡信息被黑客窃取
2008 年	云安全无疑是 2008 年网络安全行业最热的关键词
2009 年	奥巴马在竞选期间就一直强调网络安全对美国的重要性，他甚至将来自网络空间的威胁等同于核武器和生物武器对美国的威胁
2010 年	2010 年 11 月 3 日晚，腾讯发布公告，在装有 360 软件的电脑上停止运行 QQ 软件。360 随即推出了“WebQQ”的客户端，但腾讯随即关闭 WebQQ 服务，使客户端失效

任务二　计算机网络不安全因素

一般来说，计算机网络本身的脆弱性和通信设施的脆弱性共同构成了计算机网络的潜在威胁。一方面，计算机网络的硬件和通信设施极易遭受自然环境（如温度、湿度、灰尘度和电磁场等）的影响，以及自然灾害（如洪水、地震等）和人为（故意破坏和非故意破坏）的物理破坏；另一方面，计算机网络的软件资源和数据信息易受到非法的窃取、复制、篡改和毁坏；再有，计算机网络硬件的自然损耗和自然失效，以及软件的逻辑错误，同样会影响系统的正常工作，造成计算机网络系统内信息的损坏、丢失和安全事故。

一、不安全的主要因素

对计算机网络安全构成威胁的因素很多，综合起来包括以下三个方面。

1. 偶发因素：如电源故障、设备的功能失常及软件开发过程中留下的漏洞或逻辑错误等。

2. 自然灾害：各种自然灾害（如地震、风暴、泥石流及建筑物破坏等）对计算机系统构成严重的威胁。此外，火灾、水灾和空气污染也对计算机网络构成严重威胁。

3. 人为因素：不法之徒利用计算机网络或潜入计算机机房，篡改系统数据、窃用系统资源、非法获取机密数据和信息、破坏硬件设备，以及编制计算机病毒等。此外，管理不好、规章制度不健全、有章不循、安全管理水平低、人员素质差、操作失误及渎职行为等都会对计算机网络造成威胁。

人为因素对计算机网络的破坏，也称为人对计算机网络的攻击，可分为几个方面。

（一）被动攻击

这类攻击主要是监视公共媒体（如无线电、卫星、微波和公共交换网）上传送的信息，典型的被动攻击如表1－2所示。抵抗这类攻击的对策主要包括：使用虚拟专用网VPN，加密被保护网络，以及使用加保护的分布式网络。

表1－2　典型被动攻击举例

攻击	描述
监视明文	监视网络，获取未加密的信息
解密通信数据	通过密码分析，破解网络中传输的加密数据
口令嗅探	使用协议分析工具，捕获用于各类系统访问的口令
通信量分析	不对加密数据进行解密，而是通过对外部通信模式的观察，获取关键信息。例如，通信模式的改变可以暗示紧急行动

（二）主动攻击

主动攻击主要是避开或突破安全防护，引入恶意代码（如计算机病毒），破坏数据和系统的完整性，典型的主动攻击如表1－3所示。抵抗这类攻击的对策主要包括：增强内部网络的保护（如防火墙和边界护卫），采用基于身份认证的访问控制、远程访问保护、质量安全管理、自动病毒检测、审计和入侵检测等技术。

表1－3　典型主动攻击举例

攻击	描述
修改传输中的数据	截获并修改网络中传输的数据，如修改电子交易数据，从而改变交易的数量或者将交易转移到别的账户
重放	将旧的消息重新反复发送，造成网络效率降低
会话拦截	未授权使用一个已经建立的会话
伪装成授权的用户或服务器	这类攻击者将自己伪装成他人，从而未授权访问资源和信息。一般过程是，先利用嗅探或其他手段获得用户/管理员信息，然后作为一个授权用户登录。这类攻击也包括用于获取敏感数据的欺骗服务器，通过与未产生怀疑的用户建立信任服务关系来实施攻击
利用系统软件的漏洞	攻击者探求以系统权限运行的软件中存在的脆弱性。几乎每天都能发现软件和硬件平台中新的脆弱性
利用主机或网络信任	攻击者通过操纵文件，使虚拟/远方主机提供服务，从而获得信任。典型的攻击有rhost和rlogin
利用恶意代码	攻击者通过系统的脆弱性进入用户系统，并向系统内植入恶意代码；或者将恶意代码植入看起来无害的供下载的软件或电子邮件中，致使用户执行恶意代码
利用协议或基础设施的系统缺陷	攻击者利用协议中的缺陷来欺骗用户或重定向通信量。这类攻击包括：哄骗域名服务器以进行未授权远程登录；使用ICMP炸弹使某个机器离线；源路由伪装成信任主机源；TCP序列号猜测获得访问权；为截获合法连接而进行TCP组合等
拒绝服务	攻击者有很多实施拒绝服务的攻击方法，包括：有效地将一个路由器从网络中脱离的ICMP炸弹；在网络中扩散垃圾包；向邮件中心发送垃圾邮件等

(三)邻近攻击

邻近攻击是指未授权者可物理上接近网络、系统或设备,从而可以修改、收集信息,或使系统拒绝访问,典型的临近攻击如表1-4所示。接近网络可以是秘密或公开进入,也可以是两者都有。

表1-4 古典型邻近攻击举例

攻击	描述
修改数据或收集信息	攻击者获取系统管理权,从而修改或窃取信息,如IP地址、登录的用户名和口令等
系统干涉	攻击者获取系统访问权,从而干涉系统的正常运行
物理破坏	攻击者获取系统物理设备访问权,从而对设备进行物理破坏

(四)内部人员攻击

内部工作人员具有对系统的直接访问权,可轻易地对系统实施攻击。内部人员攻击分为恶意和非恶意(不小心或无知行为)两种。非恶意行为也会导致安全事件,因此,非恶意破坏也被认为是一种攻击,典型的内部人员攻击如表1-5所示。

表1-5 典型内部人员攻击举例

攻击		描述
恶意	修改数据或安全机制	内部人员直接使用网络,具有系统的访问权。因此,内部人员攻击者比较容易实施未授权操作或破坏数据
	擅自连接网络	对涉密网络具有物理访问能力的人员,擅自将机密网络与密级较低的网络或公共网络连接,违背涉密网络的安全策略和保密规定
	隐通道	隐通道是未授权的通信路径,用于从本地网向远程站点传输盗取的信息
	物理损坏或破坏	对系统具有物理访问权限的工作人员,对系统故意破坏或损坏
非恶意	修改数据	由于缺乏知识或粗心大意,修改或破坏数据或系统信息
	物理损坏或破坏	由于渎职或违反操作规程,对系统的物理设备造成意外损坏或破坏

1. 内部人员的恶意攻击。根据美国联邦调查局的评估,80%的攻击和入侵来自于内部。内部人员知道系统的布局、有价值的数据在何处,以及系统所采用的安全防范措施。而且,内部人员的攻击常常是最难检测和防范的。

2. 内部人员的非恶意攻击。这类攻击,并非故意破坏信息或信息处理系统,而是由于无意的行为对系统产生了破坏,这些破坏一般是由于缺乏知识或不小心所致。

典型对策包括:加强安全意识和技术培训;对系统的关键数据和服务采取特殊的访问控制机制;采用审计和入侵检测等技术。

(五)分发攻击

分发攻击是指在软件和硬件开发出来后和安装之前,当它从一个地方送到另一个地方时,攻击者恶意地修改软硬件,典型的分发攻击如表1-6所示。可以通过受控分发,以及由最终用户检验软件签名和访问控制来消除分发威胁。

表 1-6　典型分发攻击举例

攻击	描述
在设备生产时修改软硬件	当软件和硬件在生产线上时，通过修改软硬件配置来实施这类攻击
在产品分发时修改软硬件	在产品分发期内修改软硬件配置（如安装窃听设备）

二、不安全的主要原因

计算机网络系统安全的脆弱性是伴随计算机网络一同产生的，换句话说，安全脆弱是计算机网络与生俱来的致命弱点。在网络建设中，网络特性决定了不可能无条件、无限制地提高其安全性能。既要使网络方便快捷，又要保证网络安全，这是一个非常棘手的“两难选择”，而网络安全只能在“两难选择”所允许的范围中寻找平衡点。因此，可以说任何一个计算机网络都不是绝对安全的。

（一）互联网具有不安全性

最初，互联网用于科研和学术目的，它的技术基础存在不安全性。互联网是对全世界所有国家开放的网络，任何团体或个人都可以在网上方便地传送和获取各种各样的信息，具有开放性、国际性和自由性，这就对安全提出了更高的要求，主要表现在以下三个方面。

1. 开放性的网络。网络开放性导致网络技术全开放，使得网络所面临的破坏和攻击来自多方面。可能来自物理传输线路的攻击，也可能来自对网络通信协议的攻击，以及对软件和硬件实施的攻击。

2. 国际性的网络。网络的攻击不仅仅来自本地网络的用户，而且可以来自互联网上的任何一台计算机。也就是说，网络安全面临的是国际化的挑战。

3. 自由性的网络。网络最初对用户的使用并没有提供任何的技术约束，用户可以自由地访问网络，自由地使用和发布各种类型的信息。

另外，互联网使用的 TCP/IP（传输控制协渺网际协议），以及 FTP（文件传输协议）、E-mail（电子邮件）、RPC（远程程序通信规则）和 NFS（网络文件系统）等都包含许多不安全的因素，存在许多安全漏洞。

（二）操作系统存在安全问题

操作系统软件自身的不安全性，以及系统设计时的疏忽或考虑不周而留下的“破绽”，都给危害网络安全的人留下了许多“后门”。

操作系统体系结构造成的不安全隐患是计算机系统不安全的根本原因之一。操作系统的程序是可以动态连接的。例如，I/O 的驱动程序和系统服务可以通过打“补丁”的方式进行动态连接。许多 UNIX 操作系统的版本升级、开发也都是采用打补丁的方式进行的。这种动态连接的方法容易被黑客所利用，而且还是计算机病毒产生的好环境。另外，操作系统的一些功能也带来不安全因素。例如，支持在网络上传输可以执行的文件映像，以及网络加载程序的功能等。

操作系统不安全的另一个原因在于它可以创建进程，支持进程的远程创建与激活，支持被创建的进程继承创建进程的权利，这些机制提供了在远端服务器上安装“间谍”软件的条件。若将间谍软件以打补丁的方式“打”在一个合法的用户上，尤其是“打”在一个特权用户上，黑客

或间谍软件就可以使系统进程与作业的监视程序都监测不到它的存在。操作系统的无口令入口及隐蔽通道(原是为系统开发人员提供的便捷入口),也都成为黑客入侵的通道。

(三)数据的安全问题

在网络中,数据存放在数据库中,供不同的用户共享。然而,数据库存在着许多不安全性,例如:授权用户超出了访问权限进行数据的更改活动;非法用户绕过安全内核,窃取信息资源等。对于数据库的安全而言,要保证数据的安全可靠和正确有效,即确保数据的安全性、完整性和并发控制。数据的安全性就是防止数据库被故意破坏和非法存取;数据的完整性是防止数据库中存在不符合语义的数据,以及防止由于错误信息的输入、输出而造成的无效操作和错误结果;并发控制就是在多个用户程序并行地存取数据库时,保证数据库的一致性。

(四)传输线路安全问题

尽管在光缆、同轴电缆、微波或卫星通信中窃听其中指定一路的信息是很困难的,但是从安全的角度来说,没有绝对安全的通信线路。

(五)网络安全管理问题

网络系统缺少安全管理人员,缺少安全管理的技术规范,缺少定期的安全测试与检查,缺少安全监控,是网络最大的安全问题之一。

任务三　网络安全威胁产生的根源

网络安全威胁若不及时得到有效遏制,产生的负面影响将会越来越大;为了最大限度地防范网络安全威胁,首先需要对网络安全威胁产生的根源进行分析。

一、系统及程序漏洞

系统及程序漏洞是指应用软件或操作系统软件在编写时产生的逻辑错误,这个缺陷或错误可以被不法用户或者黑客利用。目前系统漏洞被发现的速度加快,攻击的时间变短。

对于这类漏洞和缺陷,人们能做的就是选择更安全的操作系统和软件,及时地更新操作系统或应用程序发布的补丁。

现在微软公司针对 Windows 操作系统已有了自动更新功能,人们只需开启自动更新功能,在保证连接互联网的情况下,Windows 操作系统会自动检测到最新的安装补丁。

具体操作如下。

(1)在“控制面板”中双击“自动更新”功能选项(如图 1-3 所示)。

(2)打开“自动更新”对话框,如图 1-4 所示,选择“自动”单选按钮,然后选择设置自动更新的频率。

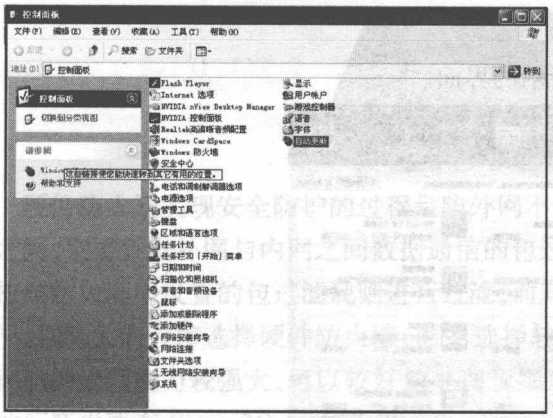


图 1-3　“自动更新”选项

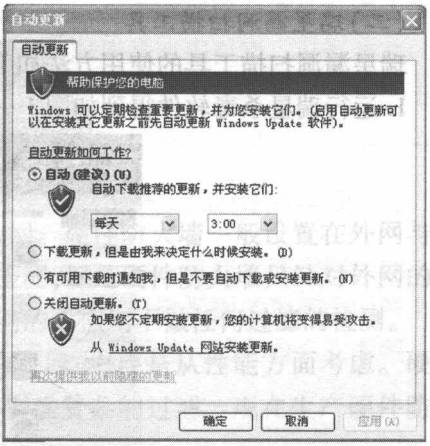


图 1-4　“自动更新”对话框

下面介绍几种常用的漏洞扫描工具。

(一)360 安全卫士

现在有一些安全工具可以帮助分析、扫描系统中存在的各种系统漏洞方面的安全隐患，360 安全卫士就是其中之一，如图 1-5 所示。它不仅可以自动搜索存在的系统漏洞，还可以自动搜索系统存在的其他漏洞，如注册表配置等。

图 1-5　360 安全卫士界面

使用 360 安全卫士进行漏洞扫描的方法如下。

在 360 安全卫士的主界面中，选择“漏洞修复”选项卡，在图 1-6 中选择要修复的系统漏洞，单击“立即修复”按钮，就可以完成漏洞补丁的安装。

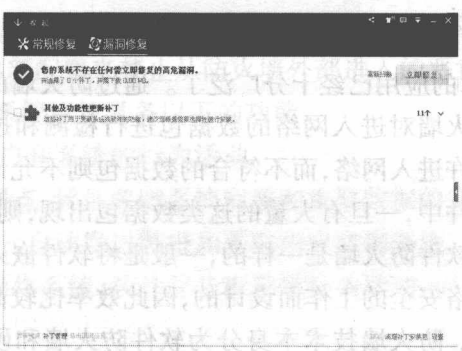


图 1-6　“修复系统漏洞”选项卡