计算机网络技术系列教材

孙建华 主编

网络安全应用技术

安继芳 李海建 编

人民邮电出版社
POSTS & TELECOM PRESS

计算机网络技术系列教材

网络安全应用技术

安继芳　李海建　编

人民邮电出版社
北京

图书在版编目（CIP）数据

网络安全应用技术 / 安继芳，李海建编．—北京：人民邮电出版社，2007.9
（计算机网络技术系列教材）
ISBN 978-7-115-16443-8

Ⅰ．网… Ⅱ．① 安… ②李… Ⅲ．计算机网络—安全技术—教材 Ⅳ．TP393.08

中国版本图书馆 CIP 数据核字（2007）第 091877 号

内 容 提 要

本书以实际应用为出发点，以实际应用为最终目的，结合目前网络安全应用技术，通过 9 章的篇幅介绍了主流的网络安全技术的原理、方法、产品、应用及实践。内容包括：概述、备份与容灾、病毒与反病毒、数据加密技术、防火墙、入侵检测、黑客攻击与防护策略、无线网络安全以及安全管理与安全评估。

本书可以作为高职高专院校和高等学校相关专业的教材，还可以作为网络爱好者的自学教材或参考书。

计算机网络技术系列教材

网络安全应用技术

◆ 编　　安继芳　李海建
责任编辑　潘春燕

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街 14 号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
北京铭成印刷有限公司印刷
新华书店总店北京发行所经销

◆ 开本：787×1092 1/16
印张：15.5
字数：373 千字　　2007 年 9 月第 1 版
印数：1－3 000 册　　2007 年 9 月北京第 1 次印刷

ISBN 978-7-115-16443-8/TP

定价：25.00 元

读者服务热线：(010)67170985　印装质量热线：(010)67129223

编 者 的 话

当今，网络已经改变了我们的生活方式。然而，网络的危险又是无时不在，无处不在。

目前，在人们眼中“网络安全”似乎是一种不可达到的理想状态，即便投入大量资金进行安全建设，依然会因为各种威胁而蒙受巨大损失。数不胜数的黑客故事、攻击案例、免费工具、破坏性事实，让人们对网络安全给予了极大的关注。

目前，各学校的许多学科专业都开设了“网络安全”课程，开设这门课程的初衷是建立在“应用”基础上的。安全用网——是现今无论哪个专业的学生都应该建立起来的一种思想。但对于计算机网络技术的相关专业来说，不仅要建立起这种思想，更要领会其原理，实践其技术，发挥其作用。

本书编者在数轮授课的基础上，结合教学的体会及实践经验编写了此书。全书按照以下思路编写：

首先，每一章都不从概念说起，而是由事件引发出对一类问题的思考，继而激起学生对相关理论问题的探究；而后，介绍主要名词及技术的概述；接下来，详细介绍技术核心，讲解时注意简单、明确、适度；再下面，是针对当前市面上这类技术的流行产品及应用的实例，让学生和所学的技术联系起来；最后，给出相关的实训，从中巩固所学习的技术要点，深刻领会技术内涵及实用价值。

全书共分 9 章，分别讲述网络安全概述、备份与容灾、病毒与反病毒、数据加密技术、防火墙、入侵检测、黑客攻击与防护策略、无线网络安全以及安全管理与安全评估的相关内容。每章都配有相关的实训环节，并对实训过程做了详尽的描述及图解。

本书由安继芳主笔。在编写过程中参考了互联网上公布的一些有关资料，由于互联网上的资料较多，引用复杂，无法一一注明原出处，故在此声明，原文版权属于原作者。其他参考文献列出在本书后。

在此，感谢给予我指导和帮助的孙建华老师及众位同事同仁；感谢给我全力支持的先生李海建；感谢给我动力的珮珮及父母。

由于作者水平有限，书中难免疏漏和错误之处，希望读者批评指正，以期修订更新。

安继芳

2007 年 1 月 15 日

目　录

第1章 概 述

本章提要：

- 计算机网络信息安全的实质
- 国内外安全立法概述，安全管理概述，安全技术概述
- 实现物理安全需要考虑的内容
- 系统平台的安全风险及安全加固方案

引言

提到网络安全，人们就会想到最近几年给社会生活带来巨大震荡的一系列事件：2001 年的“尼姆达”，2002 年的“求职信”，2003 年的“冲击波”，2004 年针对网络银行账户的“网络钓鱼”，2005 年 4 月中国电信部分省市宽带网大面积中断……每一次事件的爆发，其后果都是一样的，那就是直接、间接的巨大经济损失。

网络改变着我们的生活方式。中国互联网络信息中心（CNNIC）于 2005 年 1 月 19 日发布了第 15 次互联网调查报告（注：此项调查从 1997 年开始，至今共进行了 15 次。由 CNNIC 联合四个互联网络单位实施，是关于我国 Internet 发展状况最全面、准确的权威性统计报告）。报告显示：网民数、上网计算机数分别达到了 9400 万户、4160 万台；CN 下注册的域名数、网站数分别达到了 432 077 个、668 900 个；网络国际出口带宽总数达到 74429Mbit/s；我国内地的 IPv4 地址数达到了 59945728 个。

然而，网络的危险却无时不在，无处不在。“网络安全”在人们眼中似乎成为一种不可求得的理想状态，即便是投入大量资金进行安全建设的企业，依然会因为各种威胁而蒙受损失。那么，我们能做些什么呢？我们该做些什么呢？我们该怎么做呢？

1.1 计算机网络信息安全体系

计算机网络是指把地理上分散的多台独立自主的计算机通过软、硬件设备互连，以实现资源共享和信息交换的系统。

信息安全涉及信息的保密性（Confidentiality）、完整性（Integrity）、可用性（Availability）、可控性（Controllability）。综合起来说，就是要保障电子信息的有效性。“保密性”就是对抗对手的被动攻击，保证信息不泄漏给未经授权的人；“完整性”就是对抗对手的主动攻击，防止信息被未经授权的篡改；“可用性”就是保证信息及信息系统确实为授权使用者所用；“可

控性”就是对信息及信息系统实施安全监控。

计算机网络信息安全的实质就是安全立法、安全管理和安全技术的综合实施。正如“木桶原理”所说的：你的能力是由你最弱的那个环节决定的。因此，保护计算机网络信息的安全，应该从上述三个方面考虑，而不能只偏重其中的某一个部分。在本书中，我们将计算机网络信息安全体系用图 1-1 表示。

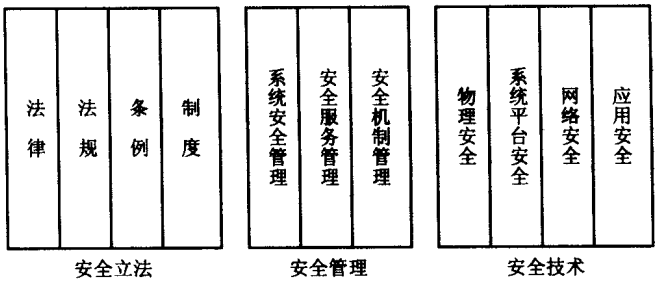

图 1-1　计算机网络信息安全体系

1.1.1　安全立法概述

当今社会，计算机网络犯罪活动猖獗的一个主要原因，在于各国的计算机网络信息安全方面的立法不健全。随着各种形式网络犯罪、信息犯罪的不断出现，对互联网进行必要的管制和立法，日益完善安全立法，已成为世界性的趋势。

1. 国外安全立法简介

（1）英国

1996 年以前，英国主要依据《黄色出版物法》、《青少年保护法》、《录像制品法》、《禁止泛用电脑法》和《刑事司法与公共秩序修正法》，惩处利用电脑和互联网络进行犯罪的行为。1996 年 9 月 23 日，英国政府颁布了第一个网络监管行业性法规《3R 安全规则》，其中“3R”代表分级认定、举报告发、承担责任。

英国广播电视的主管机关——独立电视委员会（ITC）公开宣称，依照英国 1990 年的《广播法》，它有权对因特网上的电视节目以及包含静止或活动图像的广告进行管理，但它目前并不打算直接行使其对因特网的管理权力，而是致力于指导和协助网络行业建立一种自我管理的机制。

英国政府 1999 年公布了《电子通信法案》的征求意见稿。这一草案酝酿已久，其主要目的是为促进英国电子商务发展，并为社会各界树立对电子商务的信心而提供法律上的保证。

（2）德国

德国是欧洲信息技术最发达的国家，其电子信息和通信服务已涉及该国所有经济和生活领域。德国政府出台了《信息和通信服务规范法》，即《多媒体法》。《多媒体法》于 1997 年 6 月 13 日在联邦会议获得通过，1997 年 8 月 1 日生效。《多媒体法》规定：服务提供者根据一般法律对自己提供的内容负责；若提供的是他人的内容，服务提供者只有在了解这些内容、在技术上有可能阻止其传播的情况下对内容负责；他人提供的内容，在服务提供者的途径中传播，服务提供者不对其内容负责；根据用户要求自动和短时间地提供他人的内容被

认为是传播途径的中介；若服务提供者在不违背电信法有关保守电信秘密规定的情况下了解这些内容、在技术上有可能阻止且进行阻止不超过其承受能力，则有义务按一般法律阻止违法的内容。

此外，德国政府还通过了《电信服务数据保护法》，并根据发展信息和通信服务的需要对《刑法》法典、《传播危害青少年文字法》、《著作权法》和《报价法》作了必要的修改和补充。

（3）美国

美众院司法委员会要求，色情邮件须加标注，使得用户可以不打开邮件直接将邮件删除。另外，因特网接入服务提供商可以起诉滥发垃圾邮件者，索赔100万美元以上的费用。

此外，《儿童网上保护法》已经获得美国国会批准，并在1998年经美国前总统克林顿签署成为法律。该法要求商业网站的运营者在允许互联网用户浏览对未成年人有害的内容之前，先使用电子年龄验证系统对互联网用户的年龄进行鉴别。第一次违反者将面临最高6个月的监禁和50 000美元的罚款。但是，这条法律由于网站运营商缺乏有效的措施来阻止未成年人接触有害内容而从未正式实施过。

（4）法国

法国在国际互联网的使用上起步较晚，此前它使用的是自建的一套商业电信系统。在意识到因特网的重要性及其存在的问题之后，法国政府积极地关注因特网的发展并制订了有关法律。1996年6月，法国邮电、电信及空间部长级代表对一部有关通信自由的法律进行补充并提出《菲勒修正案》。该法案根据互联网的特点，为在互联网从业人员和用户之间自律解决互联网带来的有关问题提出以下三方面措施：迫使上网服务的网络信道提供者向客户提供封锁某些信道的软件设备，从而使成年人通过技术控制对未成年人负责；建立一个委员会负责制订上网服务的职业规范，对被告发的服务提出处理意见，特别是重新负责原由网络信息委员会管辖的终端视讯服务；若网络信道提供者违反技术规定，为进入已存异议的上网提供信道，或在知情的情况下为被控告的服务进入网络提供信道，则追究其刑事责任。

（5）新加坡

新加坡广播管理局（SBA）1996年7月11日宣布对互联网络实行管制，宣布实施分类许可证制度。该制度自1996年7月15日起生效。它是一种自动取得许可证的制度，目的是鼓励正当使用互联网络，促进其在新加坡的健康发展。它依据计算机空间的最基本标准，谋求保护网络用户，尤其是年轻人，免受非法和不健康的信息传播之害。

（6）韩国

韩国情报通信部目前正在积极推进有关利用信息通信网的法律修改工作，以加强对信息通信网的管理。按照该法案，韩国将制定一部《关于保护个人信息和确立健全的信息通信秩序》的法律。这一法律将明确规定个人信息管理者和使用者的权限和责任，对向第三者泄漏个人信息者将加重处罚，刑期从过去的1年以下增加至7年以下，并将处以10亿韩元以下的罚款（1100韩元合1美元）。与此同时，这一法律还将加强对淫秽、暴力、犯罪等非法信息流通的管理。

2. 我国计算机网络信息安全立法简介

从20世纪90年代初起，为配合网络信息安全管理的需要，国家、相关部门、行业和地

方政府相继制定了《中华人民共和国计算机信息网络国际联网管理暂行规定》、《商用密码管理条例》、《互联网信息服务管理办法》、《计算机信息网络国际联网安全保护管理办法》、《计算机病毒防治管理办法》、《互联网电子公告服务管理规定》、《软件产品管理办法》、《电信网间互联管理暂行规定》、《电子签名法》等有关网络信息安全的法律法规文件。

我国网络信息安全立法体系框架分为以下三个层面。

第一层面：法律

指由全国人民代表大会及其常委会通过的法律规范。

我国与信息网络安全相关的法律主要有：《宪法》、《人民警察法》、《刑法》、《治安管理处罚条例》、《刑事诉讼法》、《国家安全法》、《保守国家秘密法》、《行政处罚法》、《行政诉讼法》、《行政复议法》、《国家赔偿法》、《立法法》、《全国人大常委会关于维护互联网安全的决定》等。

例如《刑法》第二百八十五条规定，违反国家规定，侵入国家事务、国防建设、尖端科学技术领域的计算机信息系统的，处三年以下有期徒刑或者拘役。

第二层面：行政法规

指国务院为执行宪法和法律而制定的法律规范。

与信息网络安全有关的行政法规主要有《中华人民共和国计算机信息系统安全保护条例》、《中华人民共和国计算机信息网络国际联网管理暂行规定》、《计算机信息网络国际联网安全保护管理办法》、《商用密码管理条例》、《中华人民共和国电信条例》、《互联网信息服务管理办法》、《计算机软件保护条例》等。

例如《中华人民共和国计算机信息网络国际联网管理暂行规定》中规定计算机信息网络进行国际联网的原则：a. 必须使用邮电部国家公用电信网提供的国际出入口信道；b. 接入网络必须通过互联网络进行国际联网；c. 用户的计算机或计算机信息网络必须通过接入网络进行国际联网。

第三层面：地方性法规、规章、规范性文件

指国务院各部、委根据法律和国务院行政法规，在本部门的权限范围内制定的法律规范，以及省、自治区、直辖市和较大的市的人民政府根据法律、行政法规和本省、自治区、直辖市的地方性法规制定的法律规范。这些规范性文件。

例如公安部制定了《计算机信息系统安全专用产品检测和销售许可证管理办法》、《计算机病毒防治管理办法》、《金融机构计算机信息系统安全保护工作暂行规定》、《关于开展计算机安全员培训工作的通知》等。

信息产业部制定了《互联网电子公告服务管理规定》、《软件产品管理办法》、《计算机信息系统集成资质管理办法》、《国际通信出入口局管理办法》、《国际通信设施建设管理规定》、《中国互联网络域名管理办法》、《电信网间互联管理暂行规定》等。

1.1.2 安全管理概述

长期以来，人们对保障计算机网络信息安全的手段偏重于依靠技术，从早期的加密技术、数据备份、防病毒，到近期网络环境下的防火墙、入侵检测、身份认证等。厂商在安全技术和产品的研发上不遗余力，新的技术和产品不断涌现；消费者也更加相信安全产品，把仅有的预算都投入到安全产品的采购上。但仅仅依靠技术和产品来保障网络信息安全的

愿望却往往难尽人意，许多复杂、多变的安全威胁和隐患靠产品是无法消除的。“三分技术，七分管理”这个在其他领域总结出来的实践经验和原则，在信息安全领域也同样适用。据有关部门统计，在所有的计算机安全事件中，约有52%是人为因素造成的，25%由火灾、水灾等自然灾害引起，技术错误占10%，组织内部人员作案占10%，仅有3%左右是由外部不法人员的攻击造成。由此可知，属于管理方面原因产生的安全事件比重高达70%以上，其中的95%是可以通过科学的安全管理来避免的。安全管理已成为为计算机网络信息安全保障能力的重要基础，它包括系统安全管理、安全服务管理以及安全机制管理三个方面。

1. 系统安全管理

系统安全管理是指涉及环境安全方面的管理。属于这一类安全管理的典型活动有如下几个方面。

（1）总体安全策略的管理，包括一致性的修改与维护。

（2）与其他安全管理功能的相互作用。

（3）与安全服务管理和安全机制管理的交互作用。

（4）事件处理管理，包括远程报告那些违反系统安全的明显企图，以及对用来触发事件报告的阈值的修改。

（5）安全审计管理，包括选择将被记录和被远程搜集的事件，授予或取消对所选事件进行审计跟踪日志记录的能力，审计记录的远程搜集，准备安全审计报告。

（6）安全恢复管理，包括维护那些用来对实有的或可疑的安全事故做出反应的规则，远程报告对系统安全的明显违规，安全管理者的交互作用。

2. 安全服务管理

安全服务管理是指涉及特定安全服务的管理。在管理一种特定安全服务时，可能执行的典型活动有如下几个方面。

（1）为该服务决定与指派安全保护的目标。

（2）指定与维护选择规则（存在可选情况时），用以选取为提供所需的安全服务而使用的特定的安全机制。

（3）对那些需要事先取得管理者同意的可用安全机制进行协商。

（4）通过适当的安全机制管理功能调用特定的安全机制。

（5）与其他的安全服务管理功能和安全机制管理功能的交互作用。

3. 安全机制管理

安全机制管理是指涉及特定安全机制的管理。典型的安全机制管理功能有如下几个方面。

（1）密钥管理；

（2）加密管理；

（3）数字签名管理；

（4）访问控制管理；

（5）数据完整性管理；

（6）鉴别管理；

（7）通信业务填充管理；

（8）路由选择控制管理；

（9）公证管理。

1.1.3 安全技术概述

安全技术包括以下四个方面的内容：物理安全、系统平台安全、网络安全和应用安全。

1. 物理安全

物理安全是保护计算机设备、设施（含网络）免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施和过程。

本章 1.2 节将对其做出说明。

2. 系统平台安全

系统平台安全主要是保护主机上的操作系统与数据库系统的安全，这是两类非常成熟的产品，安全功能较为完善。为了保证系统平台安全，总体思路是先通过安全加固解决企业管理方面安全漏洞，然后采用安全技术设备来增强其安全防护能力。本章 1.3 节将做详细的说明。

3. 网络安全

计算机网络是应用数据的传输通道，并控制流入、流出内部网的信息流。网络安全最主要的任务是规范其连接方式，加强访问控制，部署安全保护产品，建立相应的管理制度并贯彻实施。建设网络安全体系应注意以下几个方面。

（1）计算机网络边界的保护强度与其内部网中数据、应用的重要程度紧密相关，网络安全等级应根据节点的网络规模、数据重要性和应用重要性进行划分并动态调整。

（2）可以根据不同数据和应用的安全等级以及相互之间的访问关系，将内部网络划分为不同的区域，建立以防火墙为核心的边界防护体系。

（3）项目规划阶段就要考虑防火墙、漏洞扫描、入侵检测和防病毒等各安全产品之间的互相协作关系，以实现动态防护。

网络安全是一项动态的、整体的系统工程，一个单独的组件是无法确保信息网络安全性的。一套网络安全完整解决方案包括以下一些技术环节。

- 应用防病毒技术，建立全面的网络防病毒体系，本书第 3 章介绍。
- 应用数据加密技术，保证数据的保密性和完整性，本书第 4 章介绍。
- 应用防火墙技术，控制访问权限，实现网络安全集中管理，本书第 5 章介绍。
- 应用入侵检测技术保护主机资源，防止内外网攻击，本书第 6 章介绍。
- 应用安全漏洞扫描技术主动探测网络安全漏洞，进行定期网络安全评估与安全加固，本书第 1 章与第 7 章介绍。
- 应用网络实时监控与恢复系统，实现网络安全可靠的运行，防范突发事件，本书第 2 章与第 9 章介绍。

4. 应用安全

应用安全是保护应用系统安全、稳定的运行，保障企业和企业用户的合法权益。保证应用系统安全，应加强以下两个方面的建设。

（1）建立统一的密码基础设施，保证在此统一的基础上实现各项安全技术。

（2）实施合适的安全技术，如身份鉴别、访问控制、审计、数据保密性与完整性保护、备份与恢复等。

1.2　物理安全

物理安全是整个计算机网络信息安全的前提，如果物理安全得不到保证，则整个计算机网络信息系统的安全也就不可能实现。

目前，物理安全防范日益重要，特别是对于大型数据中心和网络系统的安全防范。为此各国针对物理安全防范需求，制定了详细的技术标准，我国出台了以下一些技术规范：

- GB50173-93《电子计算机机房设计规范》；
- 《计算机站场地技术条件》；
- GB9361-88《计算机站场安全要求》；
- 《计算机信息系统安全通用技术规范》。

具体地说，实现物理安全需要考虑的问题如表 1-1 所示。

表 1-1　　物理安全包含的内容

考 虑 因 素	具 体 描 述
防火	消除火灾隐患 设置火灾报警系统 配置灭火设备 加强防火管理和操作规范
防水	不在机房内铺设水管和蒸汽管道 墙壁、天花板、地面应选择防水防潮材料 不将机房设在楼房底层或地下室
防震	机房所在建筑特应具抗震能力 机柜和网络设备要固定牢靠，并安装防震装置 不搬动在线运行的网络设备等
防盗	设置报警器 加装锁定装置 摄像监控 严格限制无关人员进入安全区域
防鼠虫害	减少不必要的洞口 利用超声波驱鼠、投放杀鼠药物、安装捕鼠器械 在电缆外施加毒饵，防止鼠虫啃食电缆，造成漏电、电源短路等现象
防雷	所在建筑物应安装避雷针 网络设备需安全接地 对重要网络设备安装专用防雷设施
防电磁	网络设备应可靠接地 利用屏蔽方法对信号线及重要设备进行电梯屏蔽，防止电样信号的泄露 远离电磁干扰源

续表

考 虑 因 素	具 体 描 述
防静电	人员服装要控制静电、带防静电手套 工作鞋应采用低阻值材料 控制室内温度（18℃～22℃）、湿度（40%～60%） 工作台、柜等选用产生静电小的材料
安全供电	使用专用供电线路 使用不间断电源（UPS）为网络中重要设备供电 在长时间断电时，启用备用发电机使网络运转

1.3 系统平台安全

系统平台是指网络操作系统平台。目前，较流行的网络操作系统有 Windows 9X 系列、Windows NT/2000/XP 系列、UNIX 系列、Linux 系列、NetWare 系列。

网络操作系统的主要功能是实现资源共享。根据共享资源的方式不同，网络操作系统划分为两大类型。如果网络操作系统软件同等地分布在网络上的所有计算机上，这种机制下的网络操作系统称之为对等式网络操作系统。如 Windows 9X/Me、Windows NT Workstation/2000 Professional/XP Professional/XP Home，Novell 公司的 Personal NetWare，它们代表了当今流行的对等式网络操作系统。如果网络操作系统的主要部分驻留在服务器上，其他计算机使用由服务器所管理的资源，这种机制下的网络操作系统称之为“客户机/服务器”式网络操作系统。如 IBM 的 OS/2 LAN Server Advanced 3.0、Windows NT/2000 Server、Banyan Vines 等。

实施系统平台安全应注意以下几个方面的问题。

（1）加强主机操作系统、数据库系统的账户与口令管理，系统建设过程中可能遗留有无用账户、缺省账户和缺省口令，应注意清查并及时删除；如无法确认，必须修改缺省口令；账户口令要符合设置要求，对重要设备的系统级（ROOT）账户口令每个月至少要变更一次，重要操作后要及时变更口令。

（2）要建立操作系统、数据库和应用系统相关应用和端口的对应关系，关闭主机系统上与应用服务无关的端口。

（3）企业应用系统对不间断运行的要求较高，若采用打补丁的方式进行加固，风险大，工作量大，即便是表面看起来很普通的补丁也可能造成整个系统瘫痪。因此，打补丁的最佳时机是在应用系统上线投产前的安装调试阶段；应用上线后，尽量不要采用打补丁加固的方法，如要确实要打补丁，必须要经过严格的测试并做好数据备份和回退措施。

（4）如果系统平台中存在较大安全漏洞而无法打补丁加固的，可利用安全保护措施的互补性，在网络边界处采取合适安全保护措施，并加强对主机系统的审计与管理，以弥补该问题遗留的安全隐患。

（5）对于由企业外公司开发的应用系统，如需要开发公司工程师远程登入查找故障，应

贯彻最小授权原则，开放的账户只能给予满足要求的最小权限；并对远程登入时间、操作完成时间、操作事项等进行记录，及时关闭开放的用户；有条件的，可打开系统平台自带的审计工具，或配备第三方的监控、审计和身份认证工具。

1.3.1 系统平台的安全风险

风险是威胁和漏洞的组合。如果没有漏洞，也就没有风险。每个平台，无论是硬件还是软件，都存在着漏洞。作为网络安全的基础，网络操作系统也不例外。从某种意义上说，系统平台的风险大小取决于网络操作系统漏洞的多少及严重程度。尽管众多的操作系统厂商和安全服务提供商花费大量人力财力来发现系统漏洞、修补漏洞，但是漏洞仍不断被发现出来，甚至有愈演愈烈的态势。

1. Windows 系统平台的安全风险

因为 Windows 的简单易用，个人电脑用户普遍使用 Windows 作为自己电脑的操作系统平台，现在许多厂家也已经使用 Windows 作为自己的服务器操作系统平台。但是，Windows 操作系统却存在着诸多方面的安全风险。

（1）Windows 口令

账号和口令是进入 Windows 系统的重要凭证，获取账号和口令信息是入侵者攻击 Windows 系统的重要途径。例如：Windows 2000 的默认安装允许任何用户通过空用户得到系统所有的账号和共享列表，这本来是为了方便局域网用户共享资源和文件的，但是，任何一个远程用户通过同样的方法都能得到账户列表，进而可以使用非法手段破解账户密码，对用户的计算机进行攻击。

（2）Windows 恶意代码

由于 Windows 系统自身的安全隐患，许多计算机病毒、网络蠕虫、特洛伊木马等安全事件都与 Windows 系统相关，例如，“冲击波”蠕虫。

（3）Windows 应用软件漏洞

近年来，运行在 Windows 平台的应用软件安全隐患日益暴露，这些安全隐患常常导致 Windows 系统被非授权访问、非法滥用等。例如，IE 浏览器的安全漏洞导致远程攻击者植入木马，进而危及整个系统的安全。

（4）Windows 系统程序的漏洞

Windows 系统程序中设计、实现的安全隐患通常带来不少安全问题。例如，RPC 程序的漏洞导致缓冲区溢出攻击。

（5）Windows 注册表安全

注册表是有关 Windows 系统配置的重要文件，存储在“系统安装目录\system32\Config”下。由于所有配置和控制系统数据都存于注册表中，而且注册表的缺省权限设置是对“所有人”都具有“完全控制”和“创建”的权限，因此，这种设置可能会使恶意用户删除或者替换掉注册表文件。例如，入侵者通过修改、创建注册表的相关参数设置，让系统启动恶意进程。

（6）Windows 文件共享安全

Windows 98 以后的系统都提供文件共享安全，但是共享带来的问题是造成信息的泄露。比如，Windows 2000/XP 在默认安装后允许任何用户通过空用户连接（IPC$）得到系统的所