高等学校教材·计算机科学与技术

Windows 系统安全原理与技术

薛　质　王轶骏　李建华　编著

清 华 大 学 出 版 社
北　京

内 容 简 介

本书主要介绍 Windows 系统的基本安全原理和安全技术。本书以 Windows 2000 系统为重点，全面系统地讲述了 Windows 系统的安全体系结构和构成组件，内容涵盖了活动目录、身份验证、访问控制、文件系统安全、网络传输安全、应用服务安全、组策略、安全配置与分析、安全审核和公钥基础结构等。书中各章都附有习题，目的是作为课堂教学的巩固和延续，其中的某些实践性习题可供学生开展练习和讨论。

本书适合作为高等学校信息安全类专业的教材，也可供计算机信息安全领域的科技工作者和对计算机信息安全技术感兴趣的读者作为参考资料。

图书在版编目(CIP)数据

Windows 系统安全原理与技术/薛质，王轶骏，李建华编著．—北京：清华大学出版社，2005．8
(高等学校教材·计算机科学与技术)
ISBN 7-302-11295-9

Ⅰ．W…　Ⅱ．①薛…　②王…　③李…　Ⅲ．窗口软件，Windows—安全技术—高等学校—教材
Ⅳ．TP316．7

中国版本图书馆 CIP 数据核字(2005)第 071281 号

出 版 者：清华大学出版社　　**地　　址**：北京清华大学学研大厦
http://www.tup.com.cn　　**邮　　编**：100084
社 总 机：010-62770175　　**客户服务**：010-62776969
责任编辑：李江涛
封面设计：
印 刷 者：
装 订 者：
发 行 者：新华书店总店北京发行所
开　　本：185×260　**印张**：19　**字数**：471 千字
版　　次：2005 年 8 月第 1 版　2005 年 8 月第1 次印刷
书　　号：ISBN 7-302-11295-9/TP·7438
印　　数：1～　000
定　　价：　.00 元

高等学校教材·计算机科学与技术

编审委员会成员

（按地区排序）

清华大学	周立柱　教授
	覃　征　教授
	王建民　教授
	刘　强　副教授
	冯建华　副教授
北京大学	杨冬青　教授
	陈　钟　教授
	陈立军　副教授
北京航空航天大学	马殿富　教授
	吴超英　副教授
	姚淑珍　教授
中国人民大学	王　珊　教授
	孟小峰　教授
	陈　红　教授
北京交通大学	阮秋琦　教授
北京信息工程学院	孟庆昌　教授
北京科技大学	杨炳儒　教授
石油大学	陈　明　教授
天津大学	艾德才　教授
复旦大学	吴立德　教授
	吴百锋　教授
	杨卫东　副教授
华东理工大学	邵志清　教授
华东师范大学	杨宗源　教授
	应吉康　教授
东华大学	乐嘉锦　教授
上海第二工业大学	蒋川群　教授
浙江大学	吴朝晖　教授
	李善平　教授
南京大学	骆　斌　教授
南京航空航天大学	秦小麟　教授
南京理工大学	张功萱　教授
南京邮电学院	朱秀昌　教授

苏州大学	龚声蓉　教授
江苏大学	宋余庆　教授
武汉大学	何炎祥　教授
华中科技大学	刘乐善　教授
中南财经政法大学	刘腾红　教授
华中师范大学	王林平　副教授
	魏开平　教授
武汉理工大学	李中年　教授
国防科技大学	赵克佳　教授
	肖　侬　副教授
中南大学	陈松乔　教授
湖南大学	林亚平　教授
	邹北骥　教授
西安交通大学	沈钧毅　教授
	齐　勇　教授
西北大学	周明全　教授
长安大学	巨永峰　教授
西安石油学院	方　明　教授
西安邮电学院	陈莉君　副教授
哈尔滨工业大学	郭茂祖　教授
吉林大学	徐一平　教授
	毕　强　教授
长春工程学院	沙胜贤　教授
山东大学	孟祥旭　教授
	郝兴伟　教授
山东科技大学	郑永果　教授
中山大学	潘小轰　教授
厦门大学	冯少荣　教授
福州大学	林世平　副教授
云南大学	刘惟一　教授
重庆邮电学院	王国胤　教授
西南交通大学	杨　燕　副教授

出版说明

改革开放以来,特别是党的十五大以来,我国教育事业取得了举世瞩目的辉煌成就,高等教育实现了历史性的跨越,已由精英教育阶段进入国际公认的大众化教育阶段。在质量不断提高的基础上,高等教育规模取得如此快速的发展,创造了世界教育发展史上的奇迹。当前,教育工作既面临着千载难逢的良好机遇,同时也面临着前所未有的严峻挑战。社会不断增长的高等教育需求同教育供给特别是优质教育供给不足的矛盾,是现阶段教育发展面临的基本矛盾。

教育部一直十分重视高等教育质量工作。2001 年 8 月,教育部下发了《关于加强高等学校本科教学工作,提高教学质量的若干意见》,提出了十二条加强本科教学工作提高教学质量的措施和意见。2003 年 6 月和 2004 年 2 月,教育部分别下发了《关于启动高等学校教学质量与教学改革工程精品课程建设工作的通知》和《教育部实施精品课程建设提高高校教学质量和人才培养质量》文件,指出“高等学校教学质量和教学改革工程”是教育部正在制定的《2003—2007 年教育振兴行动计划》的重要组成部分,精品课程建设是“质量工程”的重要内容之一。教育部计划用五年时间(2003—2007 年)建设 1500 门国家级精品课程,利用现代化的教育信息技术手段将精品课程的相关内容上网并免费开放,以实现优质教学资源共享,提高高等学校教学质量和人才培养质量。

为了深入贯彻落实教育部《关于加强高等学校本科教学工作,提高教学质量的若干意见》精神,紧密配合教育部已经启动的“高等学校教学质量与教学改革工程精品课程建设工作”,在有关专家、教授的倡议和有关部门的大力支持下,我们组织并成立了“清华大学出版社教材编审委员会”(以下简称“编委会”),旨在配合教育部制定精品课程教材的出版规划,讨论并实施精品课程教材的编写与出版工作。“编委会”成员皆来自全国各类高等学校教学与科研第一线的骨干教师,其中许多教师为各校相关院、系主管教学的院长或系主任。

按照教育部的要求,“编委会”一致认为,精品课程的建设工作从开始就要坚持高标准、严要求,处于一个比较高的起点上;精品课程教材应该能够反映各高校教学改革与课程建设的需要,要有特色风格、有创新性(新体系、新内容、新手段、新思路,教材的内容体系有较高的科学创新、技术创新和理念创新的含量)、先进性(对原有的学科体系有实质性的改革和发展、顺应并符合新世纪教学发展的规律、代表并引领课程发展的趋势和方向)、示范性(教材所体现的课程体系具有较广泛的辐射性和示范性)和一定的前瞻

性。教材由个人申报或各校推荐(通过所在高校的“编委会”成员推荐),经“编委会”认真评审,最后由清华大学出版社审定出版。

目前,针对计算机类和电子信息类相关专业成立了两个“编委会”,即“清华大学出版社计算机教材编审委员会”和“清华大学出版社电子信息教材编审委员会”。首批推出的特色精品教材包括:

(1)高等学校教材·计算机应用——高等学校各类专业,特别是非计算机专业的计算机应用类教材。

(2)高等学校教材·计算机科学与技术——高等学校计算机相关专业的教材。

(3)高等学校教材·电子信息——高等学校电子信息相关专业的教材。

(4)高等学校教材·软件工程——高等学校软件工程相关专业的教材。

(5)高等学校教材·信息管理与信息系统。

清华大学出版社经过近20年的努力,在教材尤其是计算机和电子信息类专业教材出版方面树立了权威品牌,为我国的高等教育事业做出了重要贡献。清华版教材经过20多年的精雕细刻,形成了技术准确、内容严谨的独特风格,这种风格将延续并反映在特色精品教材的建设中。

清华大学出版社教材编审委员会

E-mail:dingl@tup.tsinghua.edu.cn

前言

随着网络技术的发展以及网络应用的普及化，网络安全正面临着前所未有的挑战。信息安全已经成为一个系统的工程，甚至将成为一个新兴的研究学科，它需要我们进行长期的研究。多年来，黑客对计算机信息系统的攻击一直没有停止过，其手段也越来越高明，从最初的猜测用户口令、利用计算机软件缺陷，发展到现在的通过操作系统源代码分析操作系统漏洞。同时我们还发现，网络的普及使得攻击工具和代码更容易被一般用户获得，这无疑给网络安全带来了更大的挑战。解决网络安全问题，任重而道远。如何走好网络安全之路，第一步就是对操作系统多做研究。

操作系统是一切软件运行的基础，而安全在操作系统的含义则是在操作系统的工作范围内，我们应该提供尽可能严密的访问控制和审计机制，在用户应用程序和系统硬件资源之间进行符合安全策略的调度，限制非法的访问，在整个软件信息系统的最底层进行保护。

众所周知，微软公司的 Windows 操作系统以其功能强大、使用方便得到了广大用户的认可，成为联网计算机的主流操作系统，但同时其安全漏洞也层出不穷，除非在操作系统中予以合理配置、管理和监控。要做到这点似乎很深奥，其实只需要少许精力。秘诀在哪里？要想减少操作系统的安全漏洞，关键是在操作系统已提供的安全功能基础上予以合理配置、管理和监控。在日常工作中，有的管理员在安装和配置操作系统时不注意做好安全防范工作，导致系统安装结束了，计算机病毒也入侵到操作系统里了。如何才能搭建一个安全的操作系统是安全管理人员所关心的一个问题。

计算机系统的核心是操作系统。因此，操作系统的安全与否直接决定着信息是否安全。在现代操作系统中，按源代码是否公开来划分可以分为两大类，一类是不开放源代码的系统，如 Microsoft 公司的 DOS、Windows 系列产品；另一类是开放源代码的操作系统，如 FreeBSD、Linux 等。是开放源代码的操作系统安全还是不开放源代码的操作系统安全？这一点在业界有不同的意见。但有一点可以肯定的是，开放源代码有利于迅速发展缺乏安全性的代码并及时进行修改。正是考虑到 Windows 系统是不开放源代码的，所以笔者认为很有必要将 Windows 的安全体系做一全面介绍，以便于用户或系统管理员安全地使用计算机和网络。

业界普遍认为，对于操作系统的安全性来说，管理和配置要比操作系统本身更重要。根据 Forrester 研究公司收集的从 2002 年 6 月 1 日到 2003 年 5 月 31 日之间的数

据,微软公司每25天公布一次新漏洞并发布安全更新,微软公布的漏洞中有67%被标为高级漏洞,而且微软已经就所有的漏洞发布了安全补丁。

本书内容基本覆盖了Windows操作系统的安全原理和安全技术,介绍了活动目录、身份验证、访问控制、文件系统安全、网络传输安全、应用服务安全、组策略、安全配置与分析、安全审核和公钥基础结构等相关知识。阅读本书可以了解Windows系统的安全体系结构和构成组件,掌握具体的安全防护措施和技术,具备对Windows操作系统的安全进行加固配置,对系统及服务安全问题进行分析和跟踪处理的能力。

应当说明的是,安全是相对的,也是动态的,由于攻击手段的提升决定了操作系统安全防护并非一件一劳永逸的事情,需要我们牢固树立安全意识,不断完善和丰富安全策略与手段。微软公司也正是由于此才在后来的Windows XP和Windows Server 2003中增加了更强大的安全功能。同时,安全也是一个系统工程,操作系统安全只是其中的一个层次,还需要各个环节的配合,安全操作系统应该与各种安全软硬件解决方案(如防火墙、杀毒软件、加密产品)等配合使用,才能达到信息系统安全的最佳状态。

限于时间及编著者的学识水平,书中不当之处恳望指正。

编著者

2005年1月于上海交通大学

目 录

第1章

Windows系统安全概述

从1983年Microsoft公司宣布Windows的诞生到现在Windows Server 2003的推出，Windows已经走过了20多年的历史。早期Windows之所以取得成功，主要归功于它友好美观、易学易用的面向对象的图形用户界面，它降低了用户学习和掌握的门槛。而就从Windows系统本身而言，多任务执行、丰富的与设备无关的图形操作、提供大量开发接口和软件等特性，无疑为Windows的推广起到了加速作用。

早期的Windows系统，如Windows 3.x、Windows 95和Windows 98，由于设计目的等其他因素的限制几乎无安全性可言。而从以Windows NT为核心的系统开始，Microsoft便为Windows系统引入了越来越多的安全特性。

1.1 Windows NT基础与安全

Windows NT是Microsoft推出的面向工作站、网络服务器和大型计算机的网络操作系统，也可作为个人计算机的操作系统。它与通信服务紧密集成，提供文件和打印服务，能运行客户机/服务器应用程序，内置了Internet/Intranet功能。从操作系统本身来看，Windows NT主要有以下特点。

- 32位操作系统，多重引导功能，可与其他操作系统共存。
- 实现了“抢先式”多任务和多线程操作。
- 采用SMP(对称多处理)技术，支持多CPU系统。
- 支持CISC(如Intel系统)和RISC(如Power PC、R4400等)多种硬件平台。
- 可与各种网络操作系统实现互操作，如：UNIX、Novell Netware、Macintosh等系统；对客户操作系统提供广泛支持，如MS-DOS、Windows、Windows NT Workstation、UINX、OS/2、Macintosh等；支持多种协议：TCP/IP、NetBEUI、DLC、AppleTalk、NWLINK等。
- 安全性达到美国国防部的C2标准。

Windows NT包含两个版本，分别是Windows NT Workstation和Windows NT Server。Windows NT Workstation的设计目标是工作站操作系统，适用于交互式桌面环境；而Windows NT Server的设计目标是企业级的网络操作系统，能提供容易管理、反应迅速的网络环境。两者在系统结构上完全一样，只是为适应不同应用环境而在运行效率上做