

高等学校教材·计算机科学与技术

可下载课件

<http://www.tup.com.cn>

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

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

4

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。

本书封面贴有清华大学出版社防伪标签,无标签者不得销售。

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

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

中国版本图书馆 CIP 数据核字(2005)第 071281 号

责任编辑：李江涛

装 订 者: 三河市新茂装订有限公司

开 本: 185×260 印张: 19 字数: 471 千字

书 号: ISBN 7-302-11295-9/TP · 7438

定价: 29.00 元

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

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,它需要我們进行长期的研究。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	1
1.1 Windows NT 基础与安全	1
1.2 Windows 2000 基础与安全	2
1.2.1 活动目录	3
1.2.2 域控制器	5
1.2.3 公钥基础结构	6
1.2.4 组策略对象	8
1.2.5 Kerberos 协议	9
1.2.6 IPSec 协议	10
1.2.7 加密文件系统	11
1.2.8 安全配置工具集	12
1.2.9 智能卡	12
1.2.10 其他安全性	13
1.3 Windows Server 2003 基础与安全	14
1.3.1 身份验证	15
1.3.2 访问控制	16
1.3.3 审计	17
1.3.4 公钥基础结构	17
1.3.5 网络安全	18
1.3.6 数据加密	19
习题	20
第 2 章 Windows NT 安全原理	21
2.1 Windows NT 系统安全体系	21
2.2 Windows NT 和 C2 级安全	22
2.3 Windows NT 的文件系统	23
2.3.1 FAT 文件系统	23

2.3.2	NTFS 文件系统	24
2.4	Windows NT 的用户和用户组	24
2.4.1	用户账户	24
2.4.2	用户组账户	25
2.4.3	用户和组账户的管理工具	25
2.4.4	本地作用域和全局作用域	26
2.5	Windows NT 的工作组和域	26
2.5.1	工作组	26
2.5.2	域	27
2.5.3	信任关系	27
2.6	Windows NT 的访问控制	29
2.6.1	安全标识符	29
2.6.2	安全访问令牌	30
2.6.3	访问控制项	30
2.6.4	访问控制列表	30
2.6.5	文件系统的访问控制	31
2.6.6	注册表的访问控制	33
2.6.7	打印机的访问控制	34
2.7	Windows NT 的安全审核	34
2.7.1	安全审核的内容	34
2.7.2	安全审核数据的存储	35
2.7.3	客体访问和审计	35
习题		36
第 3 章	Windows 2000 安全基础	37
3.1	Windows 2000 系统结构	37
3.2	Windows 2000 安全模型	38
3.3	Windows 2000 安全子系统组件	38
3.4	Windows 2000 安全协议概述	40
3.5	Windows 2000 安全程序开发	41
习题		42
第 4 章	活动目录	43
4.1	活动目录基础	43
4.1.1	活动目录的作用	43
4.1.2	活动目录的内容和工作方式	44
4.1.3	活动目录的优势	45
4.2	活动目录的体系结构	46
4.2.1	活动目录与域名服务(DNS)	47

4.2.2	活动目录与域控制器	50
4.3	活动目录对象	52
4.3.1	架构	52
4.3.2	对象命名规则	54
4.3.3	对象发布	57
4.4	域	58
4.4.1	目录树	59
4.4.2	目录林	60
4.4.3	信任关系	60
4.4.4	组织单元	61
4.4.5	混合模式域与本地模式域	62
4.5	站点	62
4.5.1	站点提供的服务	62
4.5.2	站点和域	63
4.5.3	站点信息的使用	63
4.5.4	站点内复制	63
4.5.5	站点间复制	64
4.6	活动目录的使用	65
4.6.1	活动目录的规划	65
4.6.2	安装活动目录	67
4.6.3	活动目录工具	70
习题		71

第5章 身份验证

73

5.1	身份验证概述	73
5.2	交互式登录	74
5.2.1	交互式登录组件	74
5.2.2	身份验证程序包	74
5.2.3	本地安全授权机构	75
5.2.4	交互式登录到本地计算机	75
5.2.5	交互式登录到域账户	76
5.3	网络身份验证	77
5.4	NTLM 身份验证协议	78
5.5	Kerberos 身份验证协议	78
5.5.1	Kerberos 身份验证概述	79
5.5.2	Kerberos 的身份验证过程	79
5.5.3	Kerberos 的票据	80
5.5.4	Kerberos 和 Active Directory	81
5.5.5	Kerberos 的身份验证委派	81

5.5.6 Kerberos 协议的优缺点	82
5.5.7 启用 Kerberos 协议	83
5.5.8 Kerberos 协议的其他应用	83
5.6 智能卡	83
5.6.1 何为智能卡	83
5.6.2 智能卡的作用	83
5.6.3 安装智能卡阅读器	84
5.6.4 智能卡的使用	84
习题	85
第 6 章 访问控制	86
6.1 访问控制概述	86
6.2 访问控制机制	86
6.2.1 安全标识符	87
6.2.2 访问令牌	88
6.2.3 安全描述	90
6.2.4 访问控制列表和访问控制项	91
6.3 用户和组基础	94
6.3.1 组类型	94
6.3.2 组作用域	94
6.3.3 本地组	95
6.4 内置本地组	96
6.4.1 Administrators 组	96
6.4.2 Users 组	97
6.4.3 Power Users 组	98
6.5 默认组成员	98
6.6 默认访问控制设置	100
6.6.1 文件系统和注册表的默认设置	100
6.6.2 用户权限的默认指派	101
习题	103
第 7 章 文件系统的安全	105
7.1 Windows 2000 的文件系统	105
7.2 NTFS 的权限控制	108
7.2.1 标准的 NTFS 权限	108
7.2.2 NTFS 权限控制原则	109
7.2.3 NTFS 权限继承	109
7.2.4 特殊的 NTFS 权限	110
7.2.5 Cacls 命令行工具	111

7.3	加密文件系统(EFS)	112
7.3.1	加密文件系统概述	112
7.3.2	EFS 的结构	113
7.3.3	EFS 的数据加解密过程	114
7.3.4	EFS 的故障恢复	115
7.3.5	加密文件系统的优势	117
7.3.6	加密文件系统的局限性	118
7.3.7	加密文件系统的使用	119
7.4	磁盘配额	125
7.4.1	磁盘配额基础	125
7.4.2	深入了解磁盘配额	126
7.4.3	磁盘配额的管理	128
7.5	网络共享的安全	129
7.5.1	文件夹共享	129
7.5.2	分布式文件系统	132
7.6	备份工具	133
7.6.1	数据备份	134
7.6.2	Windows 2000 备份工具	135
	习题	136
第 8 章	网络传输的安全	138
8.1	网络的不安全性	138
8.1.1	网络监听	138
8.1.2	IP 欺骗	139
8.1.3	拒绝服务攻击	140
8.1.4	应用层攻击	140
8.2	IPSec	141
8.2.1	IPSec 标准	141
8.2.2	IPSec 基础	142
8.2.3	Windows 2000 中的 IPSec	144
8.2.4	Windows 2000 的 IPSec 组件	146
8.2.5	实现 Windows 2000 的 IPSec	148
8.3	SSL	158
8.3.1	SSL 概述	158
8.3.2	SSL 的典型应用	158
8.3.3	使用 SSL 保护 Web 站点	159
8.4	VPN	163
8.4.1	VPN 基础	164
8.4.2	VPN 的基本应用	166

8.4.3 在 Windows 2000 中实现 VPN	167
习题	171
第 9 章 应用服务的安全	172
9.1 Internet 信息服务(IIS)	172
9.1.1 IIS 简介	172
9.1.2 IIS 的安全需求	172
9.1.3 IIS 安全特性概述	173
9.1.4 IIS 的身份验证	174
9.1.5 IIS 的访问控制	178
9.1.6 IIS 的应用程序保护和应用程序权限	181
9.1.7 IIS 的安全配置	182
9.2 终端服务	195
9.2.1 终端服务简介	195
9.2.2 终端服务的操作模式	197
9.2.3 终端服务的组件	198
9.2.4 终端服务配置	200
9.2.5 终端服务管理	205
9.2.6 终端服务安全性增强	207
习题	208
第 10 章 组策略	210
10.1 组策略概述	210
10.1.1 组策略的基础结构	211
10.1.2 使用组策略的管理要求	211
10.1.3 Windows 2000 与 Windows NT 策略的比较	212
10.2 组策略的存储	213
10.2.1 本地组策略对象的存储	213
10.2.2 非本地组策略对象的存储	214
10.3 组策略的配置	215
10.4 组策略的应用	217
10.4.1 组策略的应用顺序	217
10.4.2 使用安全组筛选组策略	219
10.4.3 组策略对启动和登录的影响	220
10.5 组策略的实现	221
10.5.1 访问组策略管理单元	221
10.5.2 设置组策略	223
10.5.3 禁用未使用的组策略设置	223
10.5.4 指定组策略对象的特殊应用顺序和继承	224

习题	227
第 11 章 安全配置与分析	228
11.1 安全配置工具集概述	228
11.1.1 安全配置工具集的用途	228
11.1.2 安全配置工具集的特性	229
11.2 安全配置工具组件	230
11.3 安全模板管理单元	232
11.3.1 安全模板	232
11.3.2 预定义的安全模板	233
11.4 安全配置和分析管理单元	234
11.4.1 安全配置和分析数据库	235
11.4.2 分析系统安全性	236
11.4.3 查看安全性分析结果	236
11.4.4 配置系统安全性	237
11.5 组策略管理单元的安全设置扩展	237
11.5.1 账户策略	237
11.5.2 本地策略	239
11.5.3 事件日志	242
11.5.4 受限制的组	243
11.5.5 系统服务	244
11.5.6 注册表和文件系统	244
11.6 Secedit 命令	244
习题	246
第 12 章 安全审核	248
12.1 Windows 2000 安全审核概述	248
12.2 审核策略的设置	249
12.3 事件日志的管理	258
12.3.1 事件日志属性设置	259
12.3.2 事件日志的筛选	261
12.3.3 事件日志的转储	262
习题	263
第 13 章 公钥基础结构	264
13.1 PKI 基础	264
13.1.1 公钥加密算法	264
13.1.2 公钥基础结构	266
13.2 Windows 2000 中的 PKI	268

13.3 使用 Windows 2000 中的 PKI	269
13.3.1 创建证书颁发机构	269
13.3.2 为用户分发证书	272
13.3.3 证书和密钥的导出	275
13.3.4 证书的更新	276
13.3.5 证书的撤销	276
13.3.6 备份和恢复证书服务	278
习题	279
第 14 章 Windows Server 2003 的安全	280
14.1 NTFS 和共享权限	280
14.2 文件和文件夹的所有权	281
14.3 服务配置	282
14.4 身份验证	283
14.5 IIS 6.0	284
习题	285
参考文献	286

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、UNIX、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

了相应调整。Windows NT Server 具有更多的高级功能,可把 Windows NT Workstation 看做是它的子集。

Windows NT 在系统和网络安全上引入了以下一些新的概念。

- NTFS(Windows NT file system): Windows NT 采用的新型文件系统,可提供安全存取控制及容错能力,在大容量磁盘上,它的效率比 FAT 高。
- 共享权限: 支持对网络资源设置一定的权限许可,没有得到权限许可,就无法访问网络资源。
- 用户账户(User Account): 要想使用网络资源,就必须有用户账户。Windows NT 对用户和服务程序,都要求提供合法账户。专为应用程序或服务进程创建的账户即服务账户,在系统启动时,服务进程使用服务账户登录以获得在系统中使用资源的权利和权限。普通用户账户由用户登录时提供,用于 Windows NT 控制该用户在系统中的权利和权限,与服务账户本质上没有区别。
- 域(Domain): 域是 Windows NT 中数据安全和集中管理的基本单位。网络由域组成,域具有惟一的名称。域可以看做由运行 Windows NT 的服务器组成的系统,一组电脑共用相同的账户及安全数据库。
- 工作组(Workgroup): 工作组是一种资源与系统管理都分散的网络结构。在工作组的范围内,每台电脑既可以充当服务器的角色,也可以充当工作站的角色,彼此之间是平等关系。
- 权限(Right): 权限是授权某用户可以在系统上执行某些操作。权限用来保护系统整体。
- 许可(Permission): 许可用来保护特定对象。许可规定可以使用某一对象的用户以及该用户用什么方法使用。
- 安全审核: Windows NT 将记录发生在电脑上各项与安全系统相关的过程。

1.2 Windows 2000 基础与安全

Windows 2000 代表着 Microsoft 公司在其 Windows NT 产品系列的发展中,又向前迈出了重要的一步。Windows 2000 在保留了 Windows NT 部分内核的同时,为了提供业界所需的额外功能又增加了大量的内容,其中大部分新增内容都集中在安全方面。这其中以活动目录为核心,丰富了安全功能的众多方面。

Windows 2000 操作系统包含下面四个版本。

- Windows 2000 Professional: 作为 Windows NT 4.0 Workstation 的替代产品, Windows 2000 Professional 的设计目标是成为桌面用户和移动用户共同的标准操作系统,提供更高层次的安全性、稳定性和系统性能。
- Windows 2000 Server: 作为 Windows NT 4.0 Server 的替代产品, Windows 2000 Server 的设计目标是通过支持基础设施服务、文件打印与包括 Web 在内的应用服务以及通信服务来成为主流的工作组和部门商务服务器。它引入了活动目录,通过 MMC 统一管理任务并引入了组策略,从而使管理(尤其是安全管理)得到简化。
- Windows 2000 Advanced Server: 作为 Windows NT 4.0 Server Enterprise Edition