

软件项目管理世界经典教材丛书·影印版

Microsoft Press

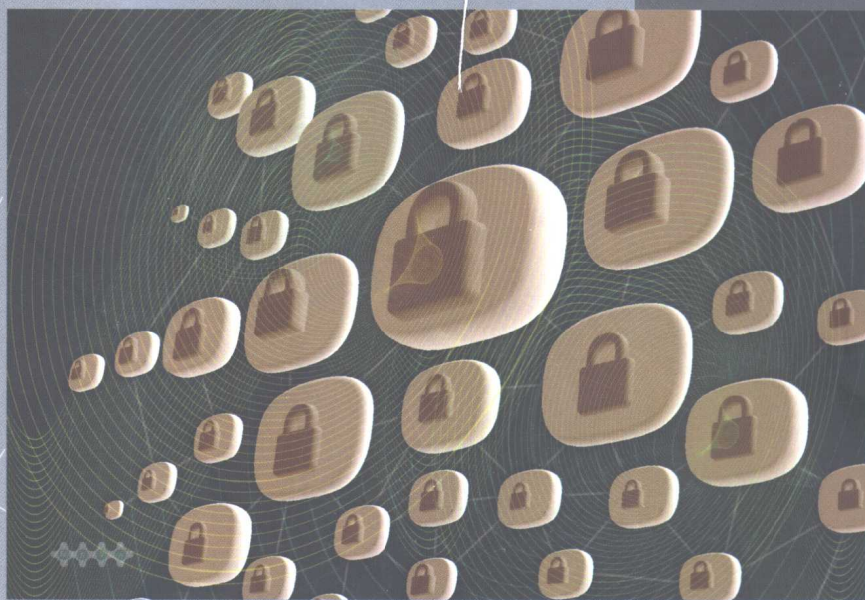
编写 安全的代码

2

(第2版)

Writing Secure Code (Second Edition)

Michael Howard,
David LeBlanc



网络时代保护应用程序代码安全的实战策略和技术

- 安全的原则，实战策略和技术
- 成功阻击黑客攻击的要领
- 解决最为棘手的安全问题

“微软员工必读。”

——比尔·盖茨



清华大学出版社

软件项目管理世界经典教材丛书

编写安全的代码 (第2版)

(影印版)

[美] Michael Howard, David L. Blanc

江苏工业学院图书馆
藏书章

清华大学出版社
北 京

内 容 简 介

本书的两位作者是曾经击败过世界上最难缠的恶意黑客的代码武士,他们在书中披露了经过实战考验的保护代码安全的各种绝招。比尔·盖茨将此书钦定为“微软员工必读”。

本书分为五大部分。第 I 部分介绍了为什么要保护系统安全,使之免遭攻击,以及设计这种系统的原则和分析技术。第 II 部分和第 III 部分是本书的重点,分别介绍了几乎适用于任何一种应用程序的关键性安全编码技术,以及网络应用程序和.NET 代码安全技术。第 IV 部分讲述了一些特殊的、在一般的图书中很少讨论的安全问题。第 V 部分包括 5 个附录,分别介绍危险的 API 以及安全措施核对清单等。

本书告诉您应用程序怎么会不安全,为什么人们不愿意构建安全的系统,最重要的是如何构建安全的系统。本书是软件设计、开发、测试、系统管理等人员必读的教材,也是软件学院、计算机专业或软件公司首选的软件安全教材。

Writing Secure Code, Second Edition(ISBN 0-7356-1722-8)

Michael Howard, David LeBlanc

Copyright © 2002 by Microsoft Corporation

Original English language edition published by Microsoft Press, a Division of Microsoft Corporation

All rights reserved.

No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the Publisher. For sale in the People's Republic of China only.

本书中文简体版由 Microsoft Press 授权清华大学出版社在中国境内(香港、澳门特别行政区和台湾地区除外)独家出版发行,未经出版者书面许可,不得以任何方式复制或抄袭本书的任何部分。

北京市版权局著作权合同登记号:图 01-2003-0832 号

版权所有,翻印必究。

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

图书在版编目(CIP)数据

编写安全的代码=Writing Secure Code: Second Edition/(美)霍华德,(美)勒布朗克著.—2 版(影印本).

—北京:清华大学出版社,2003

(软件项目管理世界经典教材丛书)

ISBN 7-302-06461-X

I. 编... II. ①霍... ②勒... III. 电子计算机—安全技术 IV. TP309

中图版本图书馆 CIP 数据核字(2003)第 018868 号

出 版 者:清华大学出版社(北京清华大学学研大厦,邮编 100084)

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

<http://www.tup.tsinghua.edu.cn>

责任编辑:郭福生 杨志娟

印 刷 者:北京牛山世兴印刷厂

发 行 者:新华书店总店北京发行所

开 本:787×960 1/16 印张:49.5

版 次:2003 年 4 月第 1 版 2003 年 4 月第 1 次印刷

书 号:ISBN 7-302-06461-X/TP·4863

印 数:0001~2000

定 价:72.00 元

前 言

在 2002 年 2、3 月份，Windows 所有正常的安全特性都停止了工作。在此期间，整个开发组的注意力都转向如何提高此产品的下一版本即 Windows .NET Server 2003 的安全上。众所周知，“Windows 安全运动”的目标是使开发组全体成员了解最新的安全编码技术，以找出设计和代码缺陷，改进测试代码和文档。在此运动期间，本书的第 1 版是 Windows 开发组全体成员的必读教材，而第 2 版收录了在这场运动中以及在针对微软其他产品的后续安全运动中的许多新发现，这些产品包括 SQL Server、Office、Exchange、Systems Management Server、Visual Studio .NET、.NET 公共语言运行库，等等。

Windows 安全运动(以及许多其他的安全运动)的原动力，来自比尔·盖茨 2002 年 1 月 15 日的名为 Trustworthy Computing (值得信赖的计算)的备忘录，其中概括说明了一种关于向用户提交新型计算机系统的高级策略，这种新型系统将更安全、更可靠。自从有了那个备忘录以来，我们两人已经与微软公司内外的数千名开发人员交谈过或合作过，而他们均异口同声地告诉我们同一件事情：“我们要做正确的事情——我们要开发安全的软件——但我们知道的还不够。”那种愿望和不确定性，直接道明了本书的目的：向他们传授学校里从来就学不到的技术——如何设计、生成、测试和注解安全的软件。所谓“安全的软件”，并不是指安全码或实现安全特性的代码，而是指为抵挡恶意攻击而设计的代码。安全的代码也是健壮的代码。

本书的目标是要绝对的切实可行，这反倒使您认识到您的代码可能会受到攻击。更确切地说就是，如果您创建的应用程序要在一台或多台计算机上运行，而这台或这些计算机已经连接到一个网络上，或已连接到最大的网络 Internet 上，那么您的代码就可能会受到攻击。

系统安全受到损害后会造成各种严重后果，包括产量下降、客户信誉受损以及财产损失。例如，如果攻击者能够损害应用程序的安全(如使之无法使用)，您的客户就会转用其他的产品。在使用基于 Internet 的服务时，大多数人都不是很有耐心。如果您的服务不可用，许多客户就会弃您而去，投奔您的竞争对手。

对于众多软件开发商来说，真正的问题是安全不像开发过程那样盈利作用显而易见。因此，管理层不愿意花钱去培训开发人员编写安全的代码，在攻击得逞之前，他们不想在安全技术上投资。而一旦攻击得逞，则为时已晚——损失已然造成。事后的修补工作，无论是在财力上还是在信誉上，都要付出高昂的代价。

历史证明，保护财产使之免遭盗窃和攻击是上策。我们的祖先早就制定了对盗窃、损坏或侵占他人财产者进行惩罚的法律。的确，人们都明白属于私人的动产和财物应当受到保护。这些道德准则也适用于数字世界，因此，作为开发人员，我们的部分职责就是创建可保护数字资产的应用程序和解决

方案。

您将会注意到,本书内容中包括一些基本的问题,在学校课程里介绍“设计和构建安全的系统”这一主题时,应当讲述过这些内容。您可能会认为,设计是设计师或程序经理们的事情,但作为开发人员和测试人员,您也需要了解设计能够抵御攻击的系统结构的有关过程。

众所周知,无论您花费多少时间和精力,所开发出来的软件总是会存在一些弱点,这只是因为您无法预测未来的安全问题。我们知道,对于 Windows .NET Server 2003 来说,同样会存在一些弱点;但我们也知道,按照本书中所建议的方法,可以减少弱点的总数,大大增加发现和利用代码中弱点的难度。

本书读者对象

在设计应用程序,或生成、测试以及注释解决方案时,您需要本书。如果您的应用程序是基于 Web 的或基于 Win32 的,您也需要本书。如果您正在学习或开发基于 Microsoft .NET 框架的应用程序,您还需要本书。总之,如果您的工作涉及到应用程序开发,您会在本书中找到许多值得学习的内容。

即使您正在编写不在 Microsoft 平台上运行的代码,本书中的许多内容依然非常有用。除了个别几章是完全针对 Microsoft 平台以外,同一类型的问题日渐与平台无关。即便有时某种东西似乎仅适用于 Windows,但其通常有更加广泛的应用。例如,Everyone 用户的“完全控制”访问控制列表和 UNIX 系统上设置给 World Writable 的文件,其实是同一问题,而跨网站的脚本问题是普遍存在的。

本书组织结构

本书分为五个部分。第 I 部分(第 1~4 章),“当前的安全问题”,概括说明了为什么要保护系统安全使之免遭攻击,以及设计这种系统的原则和分析技术。

本书的主要内容集中在第 II 部分和第 III 部分。第 II 部分,“安全的编码技术”,包括第 5~14 章,概括介绍了几乎适用于任何一种应用程序的重要的编码技术。第 III 部分,“更安全的编码技术”,包括 4 章(第 15~18 章),重点介绍了网络应用程序和 .NET 代码。

第 IV 部分,“特殊的安全问题”,包括 6 章(第 19~24 章),讲述了一般的图书中很少讨论的主题,如测试、进行安全代码审查、隐私策略以及安全的软件安装等问题。第 23 章介绍了放在其他各章都不太合适的一些一般原则。

第 V 部分,“附录”,包括 5 个附录,分别介绍危险的 API、我们所听到的未考虑安全问题的一些荒谬的借口以及分别针对设计人员、开发人员和测试人员设计的安全措施核对清单。

与其他关于安全的图书的作者不同,我们不仅告诉您应用程序怎么会不安全,而且告诉您为什么

人们不愿意构建安全的系统。本书是绝对实用的，也是绝对切实可行的。本书解释了系统怎么会受到攻击，人们常犯的错误，以及最重要的、如何构建安全的系统。(顺便说一句，请注意页边的图标，它们表示与安全有关的奇闻轶事。)

安装和使用范例文件

通过连接到站点 <http://www.microsoft.com/mspress/books/5957.asp>，可以从 Web 上下载本书的 Companion Content 页下载范例文件。要访问范例文件，请单击该页右侧 More Information 菜单框中的 Companion Content 链接，打开 Companion Content 页，此页中包括下载范例文件的链接，也可以连接到 Microsoft Press Support 站点。下载链接可打开一个包含有许可协议的可执行文件。要想把范例文件复制到硬盘上，请单击运行可执行文件的链接，然后接受显示的许可协议。默认情况下，范例文件将被复制到【我的文档】\Microsoft Press\Secureco2 文件夹下。在安装过程中，可以改变目标文件夹。

系统要求

尽管可以使用包括 Visual C++ 6.0 在内的大多数编译器来编译本书中用 C/C++编写的大多数范例，但还是要求您安装 Microsoft Visual Studio .NET。用 Perl 编写的范例已经使用 ActiveState Perl 5.6 或 ActivateState Visual Perl 1.0 (可从 <http://www.activestate.com> 下载)测试过。VBScript 和 JScript 代码已经用 Windows Scripting Host 测试过，Windows 2000 及其以后的版本中包含 Windows Scripting Host。所有 SQL 范例都使用 SQL Server 2000 进行了测试。而 Visual Basic .NET 和 Visual C#应用程序均是使用 Visual Studio .NET 编写和测试的。

本书中的所有应用程序(两个例外)，均可以在符合建议的操作系统要求的、运行 Windows 2000 的计算机上运行。第 7 章的 Safer 范例和第 11 章的 UTF8 MultiByteToWideChar 范例，必须在 Windows XP 或 Windows .NET Server 上才能正确运行。编译代码时必须使用比符合编译器要求的机器更加健壮的机器。

支持信息

为了降低书的成本，减轻读者负担，对于因内容很少而不值得单独配盘的图书，我们将其范例代码或练习文件放在我们的网站上，供读者下载。敬请访问以下网址：<http://www.wenyuan.com.cn>，查找本书的有关链接。

如果您对本书或配书文件有任何建议、意见或想法，请通过以下电子邮件与清华大学出版社计算机应用编辑二室客户服务部取得联系：

service@wenyuan.com.cn

或致函：

北京 100084-157 信箱

读者服务部

邮编：100084

亦可致电：010-62792098-220。

请注意，上述地址并不提供软件产品的支持。

目 录

第 I 部分 当前的安全问题

第 1 章 人们对安全的系统的需求	3
“野蛮网”上的应用程序	5
对值得信赖的计算的需求	7
在游戏中干掉对手	7
巧妙地向企业推销安全	8
通过颠覆推销安全	11
灌输安全意识的一些主意	13
向老板发送 E-mail	14
推荐一名安全传道士	15
攻击者的优势和防御者的困境	19
根源 1: 防御者必须防御所有的点, 而攻击者可以选择最弱的点	19
根源 2: 防御者只能防御已知的攻击, 而攻击者可以刺探未知的弱点	20
根源 3: 防御者必须始终保持警惕, 而攻击者可以随意地攻击	20
根源 4: 防御者必须遵守游戏规则, 而攻击者可以不守规矩	21
本章小结	21
第 2 章 主动的安全开发过程	23
不断改进开发过程	25
安全教育角色	26
强制培训的阻力	29
不断更新的培训	29
安全科学的进步	29
教育证明“更多的眼睛”不代表更安全	31
有力的证据!	31
设计阶段	32
访问调查期间的安全问题	33
定义产品的安全目标	34
安全是产品的一种特性	37
要有足够的时间考虑安全问题	40

安全的设计源于威胁建模	41
终结不安全的特性	41
设置 Bug 栏	41
安全小组审阅	43
开发阶段	43
只有核心成员能够查看新代码(签字确认)	43
新代码的同级安全审查(签字确认)	44
定义安全的编码准则	44
审查旧的缺陷	44
外部安全审查	45
安全运动	45
留心自己的错误数量	46
记录错误	46
没有惊喜, 也没有礼物	47
测试阶段	47
发货和维护阶段	47
如何知道已完成	47
响应过程	48
责任制	49
本章小结	49
第3章 赖以生存的安全法则	51
设计、默认和部署安全(SD3)	51
设计安全	51
默认安全	53
部署安全	53
安全法则	54
从错误中吸取教训	54
尽可能缩小攻击面	57
采用安全的默认设置	57
纵深防御	59
使用最小的特权	60
向下兼容总是令人伤心	62
假设外部系统是不安全的	63
故障的应对计划	64

安全模式失败	64
切记：安全特性!=安全的特性	66
决不要将安全仅维系于隐匿	66
不要将代码与数据混合在一起	67
正确地解决安全问题	67
本章小结	68
第 4 章 威胁建模	69
通过威胁建模进行安全的设计	70
成立威胁建模小组	72
分解应用程序	73
确定系统所面临的威胁	83
按风险大小依次排列威胁	93
选择应付威胁的方法	106
选择缓和威胁的技术	107
安全技术	108
身分验证	109
授权	114
防篡改和增强保密性的技术	115
保护秘密或最好不要保存秘密	116
加密、哈希、MAC 和数字签名	116
审核	117
筛选、截流和服务质量	118
最小特权	118
缓和工资表范例程序的威胁	118
各种威胁及解决方案	120
本章小结	124

第 II 部分 安全的编码技术

第 5 章 1 号公敌：缓冲区溢出	127
堆栈溢出	129
堆溢出	138
数组下标错误	144
格式字符串错误	147

Unicode 和 ANSI 缓冲区大小不匹配	153
一个真实的 Unicode 错误示例	154
预防缓冲区溢出	155
安全的字符串处理	156
关于字符串处理函数的警告	166
Visual C++ .NET 的/GS 选项	167
本章小结	170
第 6 章 确定适当的访问控制	171
ACL 何以如此重要	171
题外话: 修复注册表代码	173
ACL 的组成	175
选择好的 ACL 的方法	178
有效的拒绝 ACE	180
创建 ACL	181
在 Windows NT 4 中创建 ACL	181
在 Windows 2000 中创建 ACL	185
用活动模板库创建 ACL	189
正确排序 ACE	191
留意终端服务器和远程桌面的 SID	193
NULL DACL 和其他的危险 ACE 类型	195
NULL DACL 和审核	197
DangerousACETypes	197
如果无法改变 NULL DACL 该怎么办	198
其他的访问控制机制	199
.NET 框架的角色	199
COM+的角色	201
IP 限制	202
SQL Server 触发器和权限	203
一个医学方面的示例	203
关于访问控制机制的重要说明	205
本章小结	206
第 7 章 以最小特权运行	207
现实中的最小特权	208
病毒和特洛伊木马	209

丑化 Web 服务器.....	210
访问控制简介	211
特权简介	211
SeBackupPrivilege 问题.....	212
SeRestorePrivilege 问题.....	215
SeDebugPrivilege 问题	215
SeTcbPrivilege 问题.....	216
SeAssignPrimaryTokenPrivilege 和 SeIncreaseQuotaPrivilege 问题	217
SeLoadDriverPrivilege 问题	217
SeRemoteShutdownPrivilege 问题	217
SeTakeOwnershipPrivilege 问题	217
令牌简介	218
令牌、特权、SID、ACL 和进程之间的关系.....	218
SID 和访问检查, 特权和特权检查	219
应用程序要求提高特权的三个理由.....	220
ACL 问题	220
特权问题	221
使用 LSA 秘密.....	221
解决提高特权的问题.....	222
解决 ACL 问题	222
解决特权问题	223
解决 LSA 问题.....	223
确定适当特权的过程.....	223
步骤 1: 找到应用程序使用的资源.....	224
步骤 2: 找到应用程序使用的特权 API	224
步骤 3: 哪一个账户是必需的	226
步骤 4: 获取令牌的内容	226
步骤 5: 所有 SID 和特权是否都是必需的	232
步骤 6: 调整令牌	233
Windows XP 和 Windows .NET Server 2003 中的低特权服务账户	248
模拟特权和 Windows .NET Server 2003	250
调试最小特权问题	251
为什么以普通用户运行时应用程序失败.....	251
如何判断应用程序失败的原因	252
本章小结	258

第8章 加密的弱点	259
使用不良的随机数	259
问题: rand	260
Win32 中的加密随机数	262
托管代码中的加密随机数	268
Web 页中的加密随机数	269
使用密码导出加密密钥	269
测量密码的有效位长度	270
密钥管理问题	272
长期密钥和短期密钥	274
使用合适的密钥长度保护数据	274
将密钥保存在靠近数据源的地方	276
密钥交换问题	279
创建自己的加密函数	281
使用相同的流码加密密钥	283
人们为何使用流码	284
流码的缺陷	284
如果必须使用相同的密钥怎么办	287
针对流码的位翻转攻击	289
解决位翻转攻击	290
何时使用哈希、键控哈希或数字签名	290
重用明文和密文的缓冲区	296
使用加密技术缓和威胁	297
在文档中说明你使用的加密算法	298
第9章 保护机密数据	299
攻击机密数据	300
有时并不需要保存秘密	301
创建伪装的哈希	302
使用 PKCS #5 增加攻击的难度	303
获取用户的秘密	305
保护 Windows 2000 及其以后版本中的秘密	305
特殊案例: Windows XP 中的客户证书	309
保护 Windows NT 4 中的秘密	311
保护 Windows 95/98/Me/CE 中的秘密	315

使用 PnP 获得设备的详细资料	316
不要选择最小公分母解决方案	320
管理内存中的秘密	321
编译器优化停止警告	322
对内存中的机密数据进行加密	326
锁定内存以防敏感数据被分页	327
保护托管代码中的机密数据	329
管理托管代码存放在内存中的秘密	335
提高安全门槛	336
把数据存储在 FAT 文件中	337
使用嵌入密钥和 XOR 对数据进行编码	337
使用嵌入密钥和 3DES 加密数据	337
使用 3DES 加密数据并把密码存放在注册表中	337
使用 3DES 加密数据并把强密钥存储在注册表中	337
使用 3DES 加密数据, 把强密钥存储在注册表中, 并使用 ACL 控制文件和注册表项	338
使用 3DES 加密数据, 把强密钥存储在注册表中, 要求用户输入密码, 并使用 ACL 控制文件和注册表项	338
保护机密数据时的折衷方案	338
本章小结	339
第 10 章 一切输入都是有害的	341
问题	342
误信他人	343
防御输入攻击的策略	345
如何检查合法性	347
Perl 中被污染的变量	349
使用正则表达式检查输入	350
仔细检查发现的数据是否有效	352
正则表达式和 Unicode	353
正则表达式的“罗塞塔石碑”	358
Perl 中的正则表达式	358
托管代码中的正则表达式	359
脚本中的正则表达式	360
C++ 中的正则表达式	360
不使用正则表达式的最佳做法	361

本章小结	362
第 11 章 规范表示的问题	363
规范的含义及其存在的问题	364
规范文件名的问题	364
绕过 Napster 名称过滤	364
AppleMacOSX 和 Apache 的弱点	365
DOS 设备名的弱点	365
Sun 公司的 StarOffice/tmp 目录的符号链接的弱点	366
常见的 Windows 规范文件名错误	367
基于 Web 的规范问题	373
绕过 AOL 的父母控制	373
绕过 eEye 的安全检查	374
安全区域和 IE 4 的“无点 IP 地址”错误	374
IIS 4.0 的::\$DATA 的弱点	375
何时一行变成了两行	377
另一个 Web 问题——换码	378
视觉等效攻击和同形异义词攻击	382
预防规范化错误	383
不要根据文件名进行决策	383
使用正则表达式限制文件名的格式	383
停止生成 8.3 格式的文件名	385
不要相信 PATH 环境变量——使用完整的路径名	385
尝试规范化文件名	386
安全地调用 CreateFile	390
基于 Web 的规范化问题的补救措施	391
限制合法输入	391
处理 UTF-8 字符时要谨慎	391
ISAPI——岩石和硬地之间	392
最后的考虑：非基于文件的规范化问题	393
服务器名	393
用户名	394
本章小结	396
第 12 章 数据库输入问题	397
问题	398

伪补救措施 1: 用引号把输入括起来	401
伪补救措施 2: 使用存储过程	402
补救措施 1: 永不以 sysadmin 身份连接	403
补救措施 2: 以安全的方式创建 SQL 语句	404
以安全的方式创建 SQL 存储过程	406
深层防御示例	407
本章小结	411
第 13 章 Web 特有的输入问题	413
跨网站脚本: 输入何时变坏了	413
有时攻击者不需要<SCRIPT>块	417
攻击者不需要用户单击链接!	418
与 XSS 有关的其他攻击	418
针对本地文件的 XSS 攻击	418
针对 HTML 资源的 XSS 攻击	420
XSS 的补救措施	421
将输出编码	422
在所有标记属性两端添加双引号	422
将数据插入 innerText 属性	423
强制使用代码页	423
IE 6.0 SP1 的 cookie 选项 HttpOnly	424
IE 的“Web 标记”	425
IE 的<FRAME SECURITY>属性	426
ASP.NET 1.1 的 ValidateRequest 配置选项	427
不要指望不安全的构造	428
我只是想让用户向我的 Web 站点发送 HTML	430
如何审查代码中的 XSS 错误	431
基于 Web 的其他安全主题	431
eval()可能是坏的	431
HTTP 信任问题	432
ISAPI 应用程序和筛选器	433
警惕“可预知的 Cookie”	436
SSL/TLS 客户端的问题	437
本章小结	438

第 14 章 国际化问题.....	439
I18N 安全的黄金准则	440
在应用程序中使用 Unicode	440
预防 I18N 缓冲区溢出	441
字和字节	442
验证 I18N	443
可视验证	443
不要使用 LCMapString 验证字符串	443
使用 CreateFile 验证文件名	443
字符集转换问题	444
调用 MultiByteToWideChar 时使用 MB_PRECOMPOSED 和 MB_ERR_INVALID_CHARS	444
调用 WideCharToMultiByte 时使用 WC_NO_BEST_FIT_CHARS 比较和排序	448
Unicode 字符属性	448
范式	450
本章小结	451

第 III 部分 更安全的编码技术

第 15 章 套接字安全.....	455
避免服务器劫持	456
TCP 窗口攻击	463
选择服务器接口	464
接受连接	464
编写防火墙友好的应用程序.....	470
只使用一个连接	471
不要求服务器从后端连接到客户机.....	471
使用基于连接的协议	472
不要在另一个协议上多路复用应用程序.....	472
不要把主机的 IP 地址嵌入应用层数据	473
使应用程序成为可配置的	473
电子欺骗与基于主机和基于端口的信任	473
IPv6 即将发布	474
本章小结	476