Network Security in a Mixed Environment

混合环境下的网络安全

防止黑客入侵的
最佳策略和锦囊妙计

Windows NT

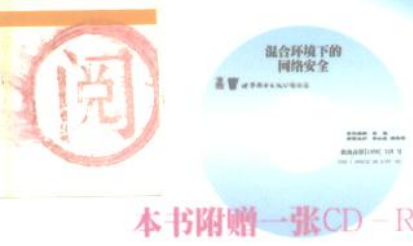
Internet

UNIX

Intranet

NetWare

Extranet



本书附赠一张CD－ROM

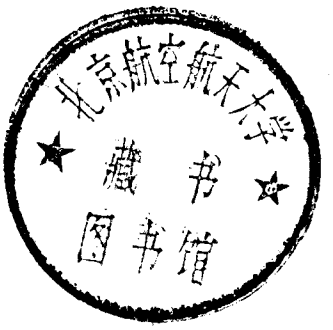
[美] Dan Blacharski 著
许少云 熊勇 袁强男 译

IDG BOOKS WORLDWIDE

世界图书出版公司

混合环境下的网络安全

[美]Dan Blacharski 著
许少云 熊勇 袁弱男 译



世界图书出版公司
广州·上海·西安·北京

内容提要

本书以独特的视角分析和论述了网络安全问题及确保混合环境下网络安全应采取的各种措施，许多材料都是此前未曾公开的。全书分为五个部分，详细介绍了美国政府关于网络安全的条例与法规、网络的安全等级、加密的方法等，还介绍了一些可供借鉴的政策范例。书中分析了 NetWare、Windows NT 和 Unix 的安全特性；重点讨论了防止“黑客”入侵和灾害袭击的保护策略；对多用户网络安全必需的硬件和软件进行了详细分析；提供了提高网络安全性的必要手段；并且对 Internet 和电子商务的安全措施进行了严格的评估。

本书适合于广大从事安全、保密、档案和计算机网络管理的读者使用，同时也是计算机网络爱好者不可多得的参考书和工具书。

书　　名：**混合环境下的网络安全**
著　　者：[美]Dan Blacharski
译　　者：许少云　熊　勇　袁弱男
责任编辑：舒　强
印 刷 者：广东省肇庆新华印刷有限公司
出版发行：广东世界图书出版公司
　　广州市新港西路大江冲 25 号　　邮政编码：510300
　　发行部电话：84451969
　　E - mail: gzwpcgd@ public1. guangzhou. gd. cn
经　　销：各地新华书店
开　　本：787 × 1092　1/16　　印张：21　　字数：400 千字
版　　次：1998 年 11 月第 1 版　1998 年 11 月第 1 次印刷
印　　数：0001 - 3000
书　　号：ISBN 7 - 5062 - 3866 - 7/TN · 0015
版权贸易合同登记号：19 - 1998 - 020
出版社注册号：粤 014
定　　价：38 元

译 者 序

Internet 技术已经被广泛应用于现代社会。网上新闻发布、电子邮件、无纸办公、远程检索、视频会议、多媒体培训系统、商务贸易、电子银行等等已经在 Internet 上实施。Internet 极大地改变了人们的生活方式，并造福于人类社会。然而，网络也成为犯罪分子的一种新型犯罪工具，网络“黑客”等计算机犯罪的出现，给人们造成了无可估量的损失。因此，网络安全提到了重要的议事日程。

《混合环境下的网络安全》一书全面论述了网络安全的重要性，推介了保证网络安全应采取的各种措施。本书共分为五个部分，介绍了美国政府关于网络安全的条例与法规、网络的安全等级、加密的方法等，还包括了一些政策范例。书中介绍了 NetWare、Windows NT 与 UNIX 的安全特性；讨论了防止“黑客”入侵与自然灾害袭击的保护策略；对使多用户网络安全所必需的硬件与软件进行了详细分析；提供了提高网络安全性的必要手段；对 Internet 和电子商务的安全措施进行了严格的评估。本书具有较高的实用价值和参考价值，可供我国广大从事安全、保密、档案工作的人士和计算机网络管理人员阅读、分析与借鉴，也可供计算机网络爱好者参考。

由于译者水平有限，错误和不妥之处难免，恳请广大读者指正。

本书由许少云（前言、第 1－5 章、词汇、安装指南）、熊勇（第 6－14 章）和袁弱男（第 15－21 章、附录 A－F）合译。杨勇克协助袁弱男做了部分工作。许少云研究员负责全书的审校工作。王丹妮、李桂华、李敏秋、黄育和等为本书的计算机录入做了大量工作。在本书的翻译过程中，中国科学院广州分院熊国炎高级工程师、广东世界图书出版公司给予了大力支持与协助。在此，译者谨表示深切的谢意。

译 者

1998 年 10 月

致　谢

作者感谢 IDG Books Worldwide 公司众多努力工作的编辑，他们耐心地等待作者完成了本书的著作，这些编辑包括 Kerrie Klein、Anne Hamilton、Jennifer Rowe、Jim Sumser 和 Michael Welch。

同时，感谢众多的销售商、顾问和专家给作者提供了大量信息，包括 Dan Farmer 和 Charles Cresson Wood，同时也感谢 Haystack 实验室 (Trusted Information Systems) 的同事、Cheyenne Software 公司（Computer Associates）和本书提及的所有其他公司。

还要感谢我的儿子 Shanti、我的父母以及与我度过这个特别困难的夏天的朋友们。

——*Dan Blacharski*

前 言

当网络由锁在机房里的大型计算机及几台笨终端组成时，保证网络安全一般是较容易的。但是，由于我们采用了分布式的客户机／服务器计算，公司网络变得比以往更加复杂。一个典型的网络可以包括广泛的地理区域，将许多分公司与总部连接起来，而且包括了 PC 局域网、大型机和小型机。网络上可能运行多种网络协议和网络操作系统，包含千兆字节、甚至兆兆字节的数据，并运行数百个程序。正因为如此，不管使用哪一种类型的系统，重要的是制定一个公司范围内的计划，考虑每一个地方、每一个部门和企业内部每一台机器以及每一个用户的需要。

网络安全的目标取决于企业本身，但总的来说包括如下内容：

- 控制对网络的访问
- 控制对特定文件和应用的访问
- 保护传输的信息
- 检测任何安全缺陷，采取适当的措施
- 防止出现意外的损坏
- 在系统出故障的情况下，启动恢复计划
- 防止物理盗贼与破坏
- 抗灾计划

网络安全通常是不受欢迎的题目，因为一般使人感到不便，限制了能做什么、不能做什么，不提供直接的收益或回报。实施者最终可能会得到赞许，但只有在灾害冲击之后才会得到。更经常地，安全政策与其实施者经常会被咒骂。然而，安全对网络的生存是绝对必要的。

本书的构成

拥有一个安全的网络不只是运行抗病毒软件和做备份。本书尽可能地包括广泛的内容，以探讨所有不同因素为目标，在你真正拥有一个安全网络之前，必须强调这些因素。作者已经将各种因素安排到下面各章节中。

第一部：政策与理论

在本书的第一部分，作者讨论政策与理论。在实施任何类型的硬件或软件方案之前，有一份明确规定的政策是相当重要的。安全目标并不一定很明确，并且各公司的目标可能相当不同。一份综合性的政策文件将是详尽而难以达到的，将概括了过程、对灾害的反应和网络的入侵，以及在一旦抓到入侵者后如何作出处理。

令人惊讶的是，网络攻击和其它破坏安全的行为经常来自公司内部——有时是无意的。当然，应对这种类型的破坏的最佳方法是教育，使系统文件和其它脆弱区不让没理由访问的人去访问。另一方面，对付有意的攻击需要更强有力的措施。防止对网络进行有意的攻击不仅需要硬件、软件投资，而且大部分情况下肯定比预料的要多。保护网络免受损害要求准确地制定政策，政策应概括你的目标，鉴别物理的和基于知识的资产，对谁能访问什么进行严格的控制。一旦制定了政策文件，该文件将指导你作出购买哪类安全软件和硬件的决策。

第一部分还谈到了抗灾计划，它应被视为整个网络安全计划的一部分。在制定网络安全计划时，你不仅必须预防网络“黑客”，而且要预防诸如地震、火灾、骚动或龙卷风这样的灾害。任何这些事件都能产生毁坏，在某些情况下可能比入侵者入侵网络还要严重。

第二部：软件

在形成了政策文件之后，就可以购买软件与硬件。第二部分阐述了软件问题，讨论了网络管理系统、监视软件、加密编码和网络操作系统的安全特性。这一部分包括了 NetWare、Windows NT 和 UNIX，专门讨论了诸如 Legato System 公司的 NetWorker 这样的安全产品，该产品可以运行于以上三个系统。我们的目标是保证混合网络环境的安全；因此，诸如 NetWorker 这样的产品对达到我们的目的是理想的，这些产品借助单独的接口保证了异种网络的安全。

用于网络安全的软件是变化且多种类的。网络操作系统本身通常提供某些原先的安全特性，但这些特性通常在缺省状态下被取消。使用哪一个特性与能不能使用这些特性完全取决于你自己。网络与系统管理软件也提供一些安全特性。最后，特定的安全软件能填补安全间隙，为你的网络提供特定的安全服务。这些软件可能包括抗病毒软件包、网络监视器或诸如 SATAN 这样众所周知的程序，用于检测网络的脆弱性。

第三部：硬件和网络设计

这一部介绍硬件和网络设计，以及虚拟 LAN、虚拟私人网和段的配置的优点。防火墙与路由器通常作为整个安全策略的一部分。虽然防火墙本身不组成整个安全环境，但的确是安全策略规划中的重要部分。

网络计算机是网络计算的最新趋势，也可用于安全方面。这些小的廉价设备给它们本身提供了安全环境。这对于缺乏系统知识的面向任务的用户来说是最理想的，这是因为非熟练工人试图安装软件或编辑系统文件引起的无意安全损坏。因为网络计算机通常没有软驱或硬盘，没有机会让工人由于安装最新版本的游戏软件而引入病毒。此外，网络计算机给它们自身提供了集中式控制。

第四部：INTERNET

第四部介绍了 Internet 和电子商务。在不久的将来，Internet 将成为各种类型金融交易的可行的市场。目前，在 Internet 上进行的金融交易的数目还是比较少的，但是，随着人们觉得借助 Internet 进行金融交易更加方便，且越来越安全，交易的数目将不断增加。

第五部：资源

为结束本书，作者搜集了大量的网络安全资源。这些资源包括以下的附录：服务端口号、安全标准和协议、安全外壳程序、样板安全政策、本书所述产品与销售商清单、关于所附 CD－ROM 的信息。同时，还包括了有关网络安全术语的词汇表。

可信任的网络安全

多年来，作者经历了网络安全的最佳状况与最坏状况，本书给出了这些例子。网络安全计划与抗灾成功的关键是做最坏的打算——因为最坏的情况可能发生。

如果网络安全是你的责任，你又是一个非常执着的人，则本书对你很有帮助。你必须考虑可能降临你公司的每种可能的危险。你必须考虑构成潜在威胁的每一个人。任何人都可能是网络入侵者；入侵者可能来自内部、外部或来自销售商的公司或合作者的公司。或许，确保网络安全的最佳哲理就是“消除一切可能出现攻击的机会”。尽管需要访问网络的每一个人都应清楚这一点，但仍有必要采取每一种安全措施。

作者相信，通过以上的介绍和本书推荐的资源，你所在的机构很快就会走上可信赖的网络安全之路。

目 录

第一部 政策与理论 …… 1

第一章 已经损失了什么? …… 3

评估你的安全要求 …… 3

政策文件 …… 4

风险与可怕的事件 …… 6

安全的种类 …… 12

Internet 安全 …… 12

网络安全 …… 14

物理安全 …… 18

政府政策与条例 …… 20

政府安全类别 …… 22

特定的法规 …… 24

小结 …… 25

第二章 安全政策的实施 …… 27

制定安全政策 …… 27

安全政策的执行 …… 28

使安全过程自动化 …… 28

限制访问 …… 29

发布你的政策 …… 29

避免出现危险 …… 30

演习与分级入侵 …… 30

执行背景检查 …… 31

一种新型的犯罪 …… 31

警告标志 …… 31

建立安全与隐私权之间的平衡 …… 32

对违反条例作出回应 …… 33

这是真正的威胁吗? …… 33

制定一个有效计划 …… 33

对不同类型的违反者制定政策 …… 35

非技术性安全政策 …… 35

能存活的系统 …… 37

小结 ……37
第三章 抗灾计划 ……39
做最坏的打算 ……39
成立抗灾计划委员会 ……40
挑选备用的工作场地 ……43
附加资源的计划 ……43
自动数据备份 ……44
混合环境下的数据备份 ……45
UNIX 为基础的备份 ……46
分层存储管理 ……47
重要的记录 ……48
小结 ……49
第四章 安全等级 ……51
国防部指南 ……51
橙皮书 ……51
红皮书 ……52
棕皮书 ……52
C2 安全 ……52
Microsoft Windows NT 与 C2 安全条例 ……53
Novell Intranet Ware 和 C2 安全条例 ……54
IBM OS/400 和 C2 安全条例 ……54
无条件访问控制 ……55
访问控制矩阵 ……55
检查能力 ……57
小结 ……58
第五章 加密 ……59
公共与私人密钥 ……60
加密机制 ……62
RSA 和 DES ……62
PGP ……63
IBM 的普通加密结构(CCA) ……64
数字证书 ……66
使用 VeriSign ……67
VeriSign 类结构 ……68

Internet 内容鉴定 …… 69
Microsoft 的 Authenticode …… 70
Netscape 对象标记协议(Object Signing Protocol) …… 71
Sun Microsystem 的 Java 安全 …… 72
数字邮戳 …… 73
合法的方位 …… 73
小结 …… 75

第二部 软件 …… 77

第六章 网络操作系统的安全性能 …… 79

NetWare …… 79
NetWare 安全类别 …… 81
授权 …… 83
远程控制台的脆弱性 …… 85
NetWare 的其它弱点 …… 86
Windows NT …… 89
Windows NT Registry …… 90
安全性访问令牌 …… 90
Registry 的脆弱性 …… 90
安全等级 …… 91
Unix …… 93
内部功能 …… 93
Solaris …… 94
单一签名 …… 97
HP—UX …… 97
IBM 平台 …… 99
DEC MLS+ 和 SEVMS …… 101
小结 …… 103

第七章 系统管理平台 …… 105

系统管理标准 …… 105
桌面管理接口 …… 106
系统网络管理协议(SNMP) …… 107
HP OpenView …… 108
HP 安全产品 …… 108
HP 的鉴别 …… 111
HP TOP 工具 …… 112

Solstice 域管理模块 …… 113
Intranet 的 Solstice 安全管理模块 …… 114
桌面系统的 Solstice 安全管理器 …… 116
应用程序的 Solstice 安全管理模块 …… 116
小结 …… 117

第八章 网络监视器和其他安全程序 …… 119

欢迎显示屏 …… 119
监视 Web 服务器 …… 120
企业安全联网的开放性平台 …… 121
应用程序管理 …… 122
代理服务器（Proxy Server） …… 124
风险分析工具 …… 124
SATAN …… 126
SATAN 补充材料 …… 131
小结 …… 131

第九章 安全审核 …… 133

审核的作用 …… 133
网络审核工具 …… 134
审核进程 …… 134
人与人之间的关系因素 …… 134
安全练习 …… 135
测试 …… 135
审核步骤 …… 136
资产管理 …… 136
小结 …… 138

第三部 硬件及网络设计 …… 139

第十章 远程访问 …… 141

远程控制的安全问题 …… 141
远程控制 …… 142
远程访问软件 …… 143
小结 …… 144
第十一章 虚拟网络 …… 145

虚拟局域网(VLAN) …… 145
VLAN 的优越性 …… 145
VLAN 的类型 …… 146
虚拟专用网络 …… 147
VPN 的安全 …… 148
VPN 软件 …… 150
小结 …… 154

第十二章 防火墙 …… 155

防火墙的种类 …… 156
数据包过滤防火墙 …… 156
双位置网关防火墙 …… 159
主机屏蔽防火墙 …… 160
子网屏蔽防火墙 …… 160
防火墙的编程和配置 …… 161
编程(PRO) …… 161
关于配置 …… 162
防火墙政策 …… 163
下一代防火墙 …… 164
第二代防火墙 …… 164
第三代防火墙 …… 164
允许用户远程访问 …… 166
非管制区(DMZ) …… 166
实施防火墙服务 …… 167
访问控制 …… 168
鉴别 …… 169
内容安全 …… 169
防火墙的运行记录 …… 170
小结 …… 171

第十三章 安全设备 …… 173

脸部特征识别设备 …… 173
被盗追回软件及服务 …… 174
Web 站点阻断工具 …… 174
物理安全设备 …… 175
电源开关的有限访问 …… 176
磁盘驱动器锁 …… 176

笔记本电脑的安全 …… 176
智能卡 …… 177
硬件锁 …… 178
小结 …… 179

第十四章 冗余 …… 181

可靠性、有效性及服务性 …… 181
Gigaplane－XB 纵横互连结构 …… 182
动态重配置 …… 182
集成系统服务处理器 …… 183
冗余电缆 …… 183
冗余服务器 …… 185
冗余存贮 …… 185
磁盘复制 …… 186
磁盘镜像 …… 187
磁盘分割 …… 187
RAID …… 187
高速网络中的冗余 …… 189
快速以太网 …… 190
FDDI …… 190
SONET …… 190
小结 …… 191

第四部 Internet …… 193

第十五章 防止电话诈骗 …… 195

对移动电话的认识 …… 195
移动电话的并机 …… 196
电话计费 …… 196
保护服务 …… 197
移动电话的未来 …… 198
Internet 电话 …… 199
小结 …… 200

第十六章 保护你的 Web 连接 …… 201

保证安全的 Web 通讯 …… 201
安全超文本传输协议(S－HTTP) …… 202

安全的应用程序接口层(SSL) …… 203
Cookie …… 203
版本控制软件 …… 205
Microsoft 代理服务器 …… 205
Web 上的安全威胁 …… 207
CGI 应用程序 …… 207
可下载的小程序 …… 208
Java …… 209
ActiveX …… 210
Web 浏览器的缺陷 …… 210
搜索引擎缺陷 …… 211
小结 …… 212
第十七章 病毒 …… 213
病毒类型 …… 214
抗病毒安全政策 …… 214
保护系统不受病毒攻击 …… 216
病毒防护的种类 …… 216
检测和防止病毒 …… 217
特殊的威胁 …… 219
E - mail 网关 …… 219
Linux 和 UNIX 病毒 …… 220
不同机种的病毒的攻击 …… 222
宏病毒 …… 223
小结 …… 225
第十八章 保证电子贸易安全 …… 227
在 Web 上经商 …… 227
为安全的事务处理做计划 …… 228
潜在问题 …… 228
信息传送 …… 229
使电子商务用户感到亲切友好 …… 230
CyberCash Internet 安全付款服务 …… 231
Java Commerce API …… 232
Netscape Merchant System …… 232
在 Internet 上使用信用卡 …… 234
来自山姆大叔的一点指导 …… 235

小结 …… 236

第十九章 Intranets …… 239

Intranet 的安全 …… 239
远程访问 Intranet …… 240
F－安全虚拟专用网络 …… 241
Extranet …… 242
用 Novell IntranetWare 建立 Intranet …… 243
小结 …… 244

第二十章 识别和防止普通的攻击 …… 245

攻击的种类 …… 245
强力攻击 …… 245
拒绝服务攻击 …… 245
同步(SYN)攻击 …… 246
IP 欺骗攻击 …… 246
Web 欺骗攻击 …… 248
目录攻击 …… 249
发现攻击 …… 250
易受攻击的外部设备 …… 252
小结 …… 252

第二十一章 安全和 TCP/IP 服务 …… 253

使用 TCP/IP 服务 …… 253
IP 名字 …… 254
IPv6 …… 255
IPSec …… 256
TCP Wrapper …… 258
小结 …… 260

第五部 资 源 …… 263

附录 A 服务端口号 …… 265
附录 B 安全标准和协议 …… 279
附录 C 安全外壳程序 …… 287
附录 D 样板安全政策 …… 293
附录 E 产品和供应商 …… 297

附录 F　关于 CD－ROM …… 307
词　汇 …… 311
安装指南 …… 317