科爱传播
KE'AI COMMUNICATIONS

21世纪信息安全大系

网络安全保护

Ido Dubrawsky, Chris Crayton, Michael Cross, Jeremy Faircloth,
Eli Faskha, Michael Gregg, Alun Jones, Marc Perez 著

贾军保 译

How to Cheat at
Securing Your Network

科学出版社

How to Cheat at Securing Your Network

网络安全保护

Ido Dubrawsky
Chris Crayton
Michael Cross
Jeremy Faircloth
Eli Faskha
Michael Gregg
Alun Jones
Marc Perez

著

贾军保 译

科学出版社

北京

图字：01-2008-2324 号

This is a translated version of
How to Cheat at Securing Your Network
Michael Cross，et al.

ISBN 13：978-1-59749-231-7

图书在版编目(CIP)数据

网络安全保护/(加拿大) 克劳斯（cross，M.）著；贾军保译. —北京：科学出版社，2009

ISBN 978-7-03-023638-8

Ⅰ. 网… Ⅱ. ①克…②贾… Ⅲ. 计算机网络-安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 026744 号

责任编辑：田慎鹏 霍志国/责任校对：刘小梅
责任印制：钱玉芬/封面设计：耕者设计工作室/封面图片：徐 湛

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销

*

2009 年 4 月第 一 版 开本：787×1092 1/16
2009 年 4 月第一次印刷 印张：22
印数：1—4 000 字数：495 000

定价：56.00 元

（如有印装质量问题，我社负责调换〈新欣〉）

作者简介

Michael Cross（MCSE、MCP+I、CAN、Network+） 互联网专家/尼亚加拉警察局（NRPS）计算机取证分析师。他还执行对涉嫌犯罪计算机的检查，在一些与计算机或网络有关的案件当中协助进行调查。此外，他还在 www. nrps. com 上设计并维护 NRPS 网站和 NRPS 内联网，也可以在编程、硬件和网络管理等领域提供支持。作为信息技术团队的一员，他还为一个超过 800 个民间和军方用户的用户群提供支持。他常说，如果用户是带枪的，解决问题的动力就会更大。

Michael 还拥有 KnightWare（www. knightware. ca），可以提供与计算机有关的服务，如网页设计；还有 Bookworms（www. bookworms. ca），我们可以在这个网站上在线购买收藏品和一些其他有趣的东西。他作为自由作家已经有好几年了，在许多书籍和文选当中发表了 20 多篇文章。目前，他居住在加拿大安大略省圣凯瑟琳市，妻子是 Jennifer，有一儿一女，儿子 Jason，女儿 Sara。

Jeremy Faircloth（Security+、CCNA、MCSE、MCP+I、A+等） 是 EchoStar Satellite 有限责任公司的 IT 经理，在这家公司中，他和他的团队建设并维护整个企业的客户端/服务器，还做一些基于 Web 的技术工作。他还为其他 IT 专家提供一些技术方面的资源，用他的专业技术帮助他人扩展知识面。作为一名有 13 年实际 IT 经历的系统工程师，他在许多领域都是专家，这些领域包括 Web 开发、数据库管理、企业安全、网络设计和工程管理。Jeremy 在 Syngress 出版社也出了几本书，如《Microsoft 分析器工具包》（Syngress 出版社，ISBN：1932266526）、《Cisco SWAN 的管理和保护》（ISBN：1932266917）、《Java 程序员的 C#》（ISBN：193183654X）、《Snort 2. 0 侵入探测》（ISBN：1931836744）和《安全+学习指导和 DVD 训练系统》（ISBN：1931836728）。

Eli Faskha（Security+、检查点认证主任工程师、CCS、CCSE、CCSE+、MCP）是 Soluciones Seguras 公司的创建人和总经理。这家公司专门从事网络安全方面的业务，是检查点金牌合作人和诺基亚授权合作人。他还是 Syngress 出版社《配置检查点 NGX VPN-1/防火墙-1》（ISBN：1597490318）一书的助理编辑、《为公司建立 DMZ》（ISBN：1597491004）一书的合作编撰人。Eli 是经验最丰富的检查点认证安全老师，也是该领域的诺基亚认证教师，在 20 多个国家以英语和西班牙语进行过教学。1993 年毕业于宾夕法尼亚大学沃顿学院和摩尔学院的工程专业，1995 年获得了乔治城大学的 MBA 学位。他具有 8 年多的网络工作经历，1999—2000 年在巴拿马就开始了大型门户网站的开发，2001 年管理 Verisign 的一家子公司，并且从那时起开始经营自己的公司。Eli 还在当地的媒体上发表过几篇文章，这些文章被当作对巴拿马互联网发展的贡献。下面这个电子邮件地址可以与他联系：eli@solucionesseguras. com。

Michael Gregg（CISSP、CISA、MCSE、MCT、CTT+、A+、N+、Security+、CAN、CCNA、CIW Security Analyst、CCE、CEH、CHFI、DCNP、ESDragon IDS、TICSA） 是 Superior Solutions 公司的首席运营官和创始人，这是一家坐落在休斯顿的 IT 安全咨询公司。Superior Solutions 公司执行对财富 1000 公司的安全评测和渗透测试。Michael 负责开发针对安全问题的新技术解决方案。他还监督客户预约，以便能够开发针对软件设计问题、系统管理问题、策略开发和安全系统测试的高质量解决方案。

Michael 有 20 多年的 IT 工作经历，有两个相关领域的证书——一个学士学位和一个硕士学位。他还单独或与人合作完成了多本专著，有 Que 的《正派黑客认证考试资料 2》和 Sam 出版的《内部网络安全评测》。他还是《黑客堆：运用 Snort 和 Ethereal 控制不安全网络 8 层》（Syngress 出版社，ISBN：1597491098）的作者，也是美国证书检查学院、独立计算机咨询学会和得克萨斯州教育技术学会的成员。

Alun Jones（MVP、MCP） 是得克萨斯帝国软件的总经理。得克萨斯帝国软件主要开发安全联网软件并提供安全工程咨询服务。得克萨斯帝国软件的旗舰产品就是 WFTPD Pro，这是一个 Windows 的 FTP 服务器，完全是用 Alun 写成的。

随着越来越多的 WFTPD 的支持表明，只有很少的公司在互联网上尝试满足安全方面的需求，Alun 就进入了安全工程的领域。他现在任职 Premera Blue Cross 公司的信息系统安全工程师，这是一家坐落在太平洋西北岸的医疗保险供应商。

Alun 先后在克里斯蒂分校、剑桥大学和巴斯大学学习过，但都没有完成学业，他现在与妻子 Debbie、儿子 Colin 生活在华盛顿州的本雅图。

Marc Perez（MCSE：Security，Security+） 是马萨诸塞州波士顿市网络信息系统的高级顾问、网络信息系统的 Microsoft 业务代表，他还为东北部的中型客户和企业级客户提供战略和技术方面的咨询。他主要用信息和协同的解决方案来安全整合目录服务，还为企业提供必要的指导，以使其网络更有效。

南缅因州大学毕业后，Marc 就是波士顿地区的多个组织的顾问，而且一直就职在新英格兰地区，有 4 年 MBNA 美国银行信息安全经理的经历。目前，他和妻子 Sandra，还有两个儿子 Aidan、Lucas，生活在北海岸。

技术编辑

Ido Dubrawsky（CISSP、CCNA、CCDA） 是北美 Microsoft 通信部的首席安全顾问，该机构是移动与嵌入设备组的一个分支机构。在 Microsoft 工作之前，Ido 为 AT&T 的 Callisma 子公司主动安全策略咨询提供指导。在进入 AT&T 之前，Ido 是 Cisco 系统公司安全工程小组的网络安全设计师。他还有 20 多年的系统和网络管理工作经历，涉及的网络环境既有政府网络也有学术性网络及企业性网络。不管是小型网络还是大型网络，也不管是简单的网络还是复杂的网络，他都有丰富的管理经验。Ido 还是 3 个主要安全白皮书的重要作者之一，写作或讲授过广泛的安全题材。他还是 SecurityFocus 网站的定期投稿人，对安全问题的各个方面都有过论述。之前，他供职于 Cisco 系统公司的安全顾问组，为许多客户提供网络安全状态评测和咨询方面的服务。此外，他提供一些渗透测试方面的咨询，领导了安全工程的评审以及策略和过程的评审。他还拥有得克萨斯大学奥斯汀分校航空和航天工程的理学学士和理学硕士学位。

技术评论

Christopher A. Crayton（MCSE、MCP＋I、A＋、Network＋） 是一名 A＋/Network＋认证的教师，2002 年被 Keiser 学院授予“年度教师”称号。他住在佛罗里达州的萨拉索塔，是 ECRM 公司的网络管理员。

译 者 序

互联网（Internet）起源于1969年的ARPANet，最初用于军事目的，1993年开始用于商业，进入快速发展阶段。到目前为止，互联网已经覆盖了175个国家和地区的数亿台计算机，用户数量超过10亿。随着计算机网络的普及，计算机网络的应用向深度和广度不断发展。企业上网、政府上网、网上学校、网上购物……，一个网络化的社会已经展现在我们面前。在网络给人们带来巨大便利的同时，也带来了一些不容忽视的问题，网络信息的安全保密问题就是其中之一。

近年来，网络犯罪急剧上升，已经成为普遍的国际性问题。据美国联邦调查局报告，计算机犯罪是商业犯罪中最大的犯罪类型之一，每年计算机犯罪造成的经济损失高达数百亿美元。

计算机犯罪大都具有瞬时性、广域性、专业性、时空分离性等特点。通常计算机罪犯很难留下犯罪证据，这大大刺激了计算机高技术犯罪案件的发生。计算机犯罪案率的迅速增加，使各国的计算机系统特别是网络系统面临很大的威胁，并成为严重的社会问题之一。

1994年末，俄罗斯黑客弗拉基米尔·利文与其伙伴从圣彼得堡的一家小软件公司的联网计算机上，向美国CITYBANK发动了一连串攻击，通过电子转账方式，从CITYBANK在纽约的计算机主机里窃取1100万美元。

1998年，美国国防部宣称黑客向五角大楼网站发动了“有史以来最大规模、最系统性的攻击行动”，打入了许多政府非保密性的敏感电脑网络，查询并修改了工资报表和人员数据。不久，警方抓获了两名加利福尼亚州少年黑客。3个星期后，美国警方宣布以色列少年黑客“分析家”被抓获。同年，马萨诸塞州伍切斯特机场导航系统因一名少年黑客入侵而中断6小时。

1999年5月，美国参议院、白宫和美国陆军网络以及数十个政府网站被黑客攻陷。同时，因北约导弹袭击中国驻南斯拉夫联盟使馆，中国黑客群体出击美国网站以示抗议。

2000年2月，在3天时间里，黑客使美国数家顶级互联网站——雅虎、亚马逊、电子港湾、CNN陷入瘫痪。黑客使用" 拒绝服务式" 攻击，即用大量无用信息阻塞网站的服务器，使其不能提供正常服务。同月，日本右翼分子举行集会，企图否认南京大屠杀暴行，引起中国黑客愤慨，中国黑客连番袭击日本网站。

防范黑客的入侵，提高计算机的安全性，涉及许多复杂的问题，包括物理环境、硬件、软件、数据、传输、体系结构等各个方面。除了传统的安全保密理论、技术及单机的安全问题以外，计算机网络安全技术包括了计算机安全、通信安全、访问控制的安全，以及安全管理和法律制裁等诸多内容，并逐渐形成独立的学科体系。换一个角度讲，当今社会是一个信息化社会，计算机通信网络在政治、军事、金融、商业、交通、电信、文教等方面的作用日益增大，社会对计算机网络的依赖也日益增强，尤其是计算

机技术与通信技术相结合，所形成的信息基础设施已经成为反映信息社会特征最重要的基础设施。人们建立了各种各样完备的信息系统，使得人类社会的一些机密和财富高度集中于计算机。但是，这些信息系统都是依靠计算机网络接收和处理信息，实现其相互间的联系和对目标的管理、控制。以网络方式获得令牌或交流信息已经成为现代信息社会的一个重要特征。随着网络的开放性、共享性及互联程度的扩大，以及电子商务（ElectronecCommerce）、电子现金（ElectronecCash）、数字货币（DigitalCash）、网络银行等的兴起，还有各种专用网络的建设，使安全问题显得越来越重要，因此对网络安全的研究已经成了现在计算机通信界的一个热点。

本书的特色是网络安全理论知识与实例代码的完美结合，使读者不仅可以从理论深度上对网络安全有宏观的认识，而且可以根据实例代码对网络安全措施有更直观的把握，特别值得一提的是本书还全面介绍了无线网络安全的有关知识，每章后面都有对本章内容的摘要性概括，还有作者对一些常见问题的解答。

本书共分 10 章，包括网络安全的基本概念、基本原理；远程访问和无线通信的安全性；各种攻击技术的特征；基于互联网的通信安全服务；设备和介质的安全使用；布局和 IDS；系统硬化；还介绍了密码学和公钥基础设施的基础知识。

本书可作为网络安全工程师、网络管理员等信息与网络安全领域从业人员学习、研究及探讨安全理论知识与实例代码的阅读参考用书。同时本书也可作为大专院校计算机类、网络类、通信类、信息安全类等专业高年级本科生和研究生学习网络安全的参考书。感谢马振晗同志在本书翻译过程中的大力协助与支持，在此表示衷心的感谢。

贾军保

2009 年 3 月 1 日

目　录

第 1 章　一般性安全概念：访问控制、验证和审计 …… 1
AAA 简介 …… 2
AAA 是什么 …… 2
访问控制 …… 3
MAC/DAC/RBAC …… 3
验证 …… 6
Kerberos …… 10
CHAP …… 12
证书 …… 12
用户名/口令 …… 13
令牌 …… 14
多因素 …… 15
相互验证 …… 15
生物特征 …… 16
审计 …… 16
审计系统 …… 16
日志 …… 21
系统扫描 …… 21
禁止非必要服务、协议、系统和程序 …… 22
非必要服务 …… 22
非必要协议 …… 23
禁止非必要系统 …… 23
禁止非必要程序 …… 23
小结 …… 26
快速解决方案 …… 27
常见问题 …… 28
第 2 章　一般性安全概念：攻击 …… 29
攻击 …… 30
主动攻击 …… 31
DoS 和 DDoS …… 31
软件利用和缓冲区溢出 …… 35
MITM 攻击 …… 36
TCP/IP 劫持 …… 37
重放攻击 …… 37

哄骗攻击 …… 37
战争拨号 …… 42
垃圾搜索 …… 42
社会工程 …… 42
漏洞扫描 …… 43
被动攻击 …… 44
嗅探与窃听 …… 45
口令攻击 …… 45
蛮力攻击 …… 46
基于字典的攻击 …… 46
恶意编码攻击 …… 46
病毒 …… 47
小结 …… 52
快速解决方案 …… 52
常见问题 …… 54
第 3 章 通信安全：远程访问与信息传输 …… 57
引言 …… 58
通信安全的必要性 …… 58
基于通信的安全性 …… 59
远程访问安全 …… 59
802.1x …… 60
VPN …… 63
RADIUS …… 66
TACACS/+ …… 67
PPTP/L2TP …… 68
SSH …… 72
IPSec …… 73
漏洞 …… 75
电子邮件安全 …… 76
MIME …… 77
S/MIME …… 78
PGP …… 78
漏洞 …… 80
小结 …… 88
快速解决方案 …… 90
常见问题 …… 90
第 4 章 无线通信的安全性 …… 93
引言 …… 94
无线网络的概念 …… 94

了解无线网络 …… 94
无线网络上的无线通信概述 …… 95
无线局域网 …… 98
WAP …… 98
WTLS …… 99
IEEE 802.11 …… 99
Ad-Hoc 和有基础设施的网络配置 …… 101
WEP …… 102
无线网络的一般利用 …… 107
无线网络的漏洞 …… 112
WAP 漏洞 …… 112
WEP 漏洞 …… 113
对普通危险和威胁的处理 …… 119
嗅探 …… 124
嗅探（窃听）和未授权的访问 …… 126
网络劫持与修改 …… 127
服务拒绝与淹没攻击 …… 129
IEEE 802.1X 漏洞 …… 131
网络监测 …… 131
对无线网络的附加安全性的检查 …… 131
无线网络安全性的执行：一般性的最佳操作 …… 135
小结 …… 137
快速解决方案 …… 139
常见问题 …… 141
第 5 章　通信安全：基于互联网的服务 …… 143
引言 …… 144
Web 安全 …… 144
Web 服务器锁定 …… 144
停止使用浏览器 …… 153
SSL 和 HTTP/S …… 158
即时通信 …… 161
基于 Web 的漏洞 …… 164
缓冲区溢出 …… 181
使浏览器和电子邮件客户端更安全 …… 182
Web 浏览器软件的保护 …… 184
CGI …… 187
由弱 CGI 脚本引起的中断 …… 190
FTP 安全 …… 192
主动 FTP 与被动 FTP …… 192

S/FTP ····· 193
安全复制 ····· 193
盲 FTP/匿名 ····· 194
FTP 共享与漏洞 ····· 194
用数据包嗅探 FTP 传输 ····· 195
目录服务和 LDAP 安全 ····· 198
LDAP ····· 199
小结 ····· 203
快速解决方案 ····· 203
常见问题 ····· 204
第 6 章 基础设施的安全性：设备与介质 ····· 207
引言 ····· 208
基于设备的安全性 ····· 208
防火墙 ····· 208
路由器 ····· 215
交换器 ····· 217
无线设备 ····· 219
调制解调器 ····· 219
RAS ····· 221
电信/PBX ····· 222
虚拟专用网络 ····· 223
IDS ····· 224
网络监测/诊断 ····· 228
工作站 ····· 228
服务器 ····· 231
移动设备 ····· 232
基于介质的安全性 ····· 232
同轴电缆 ····· 233
UTP/STP ····· 235
光导纤维 ····· 236
可移动介质 ····· 237
小结 ····· 240
快速解决方案 ····· 242
常见问题 ····· 243
第 7 章 布局与 IDS ····· 245
引言 ····· 246
安全布局 ····· 246
安全分区 ····· 246
VLANs ····· 255

网络地址转换 …… 257
隧道传送 …… 259
入侵检测 …… 260
IDSes 介绍 …… 261
基于签名的 IDSes 与检测逃避 …… 264
常见的商业 IDS 系统 …… 265
蜜罐与蜜网 …… 267
假阳性和否定状态的判断 …… 268
事件响应 …… 269
小结 …… 269
快速解决方案 …… 270
常见问题 …… 271
第 8 章　基础结构的安全性：系统硬化 …… 273
引言 …… 274
OS 硬化与 NOS 硬化的概念和过程 …… 274
文件系统 …… 276
升级 …… 276
网络硬化 …… 278
升级（固件） …… 278
配置 …… 279
应用程序硬化 …… 285
升级 …… 285
Web 服务器 …… 286
电子邮件服务器 …… 287
FTP 服务器 …… 288
DNS 服务器 …… 288
NNTP 服务器 …… 289
文件服务器和打印服务器 …… 289
DHCP 服务器 …… 290
数据储存库 …… 291
小结 …… 293
快速解决方案 …… 294
常见问题 …… 294
第 9 章　密码学基础 …… 297
引言 …… 298
算法 …… 298
什么是加密？ …… 298
对称加密算法 …… 299
非对称加密算法 …… 301

哈希算法 …… 304
应用密码学的概念 …… 305
机密性 …… 306
完整性 …… 306
验证 …… 309
不可否认性 …… 309
访问控制 …… 309
一次一密 …… 309
小结 …… 310
快速解决方案 …… 310
常见问题 …… 311
第 10 章 公钥基础设施 …… 313
引言 …… 314
PKI …… 314
可信模型 …… 315
证书 …… 320
撤销 …… 323
标准与协议 …… 325
密钥管理和证书生命周期 …… 326
集中和分散 …… 327
储存 …… 327
托管 …… 329
到期 …… 331
撤销 …… 331
暂停 …… 332
恢复 …… 333
更新 …… 332
销毁 …… 334
密钥的使用 …… 334
小结 …… 335
快速解决方案 …… 336
常见问题 …… 336

第 1 章
一般性安全概念：访问控制、验证和审计

本章主要内容：

- AAA 简介
- 访问控制
- 验证
- 禁止非必要服务、协议、系统和程序

- ✓ 小结
- ✓ 快速解决方案
- ✓ 常见问题

AAA 简介

AAA 是学习计算机、网络安全以及访问控制等知识的时候，必须要了解的基本概念。运用这些概念可以保护财产、数据和系统避免受到有意或无意的损害。AAA 是用来支持机密性、完整性和可用性（CIA）概念的，此外在运用远程用户拨入认证系统和终端访问控制器访问控制系统（TACACS/TACSCS+）访问网络或设备时提供框架。

我们将在 RFC 3127 中详细讨论 AAA，这些内容也可以在 http://tools. ietf. org/html/rfc3127网站上找到。RFC 包含针对 AAA 要求的各种现有协议，还可以有助于了解这些协议的特殊细节。在 http://tools. ietf. org/html/rfc2989也有关于 AAA 的内容。

AAA 是什么

AAA 是一组用来保护数据、设备和财产以及信息机密性的程序。正如以前提到的，AAA 的目标之一就是提供机密性、完整性和可用性（CIA）。CIA 可以简单描述如下：

- **机密性** 数据或内容不能泄露。
- **完整性** 数据或内容完整无缺且不被修改。
- **可用性** 如果允许，数据或内容是可以访问的。

AAA 是由 3 个相互联系的领域组成的。这些领域在网络资源和网络设备的控制访问方面提供一个层级的基本安全。为了更进一步地保护系统和财产，这种控制允许用户提供一些对 CIA 过程有帮助的服务。我们现在就描述一下这 3 个领域，然后再分别研究这些领域的用途以及在增强安全性方面的作用。最后，我们再用每个 AAA 的组成部分作为示例来进行实际操作。

访问控制

访问控制可以定义为一个用来允许或拒绝对资源进行访问的策略、软件或硬件成分。这可以是一个先进的成分；如智能卡、生物特征辨识设备或网络访问硬件；路由器、远程访问点，如远程访问服务（RAS）和虚拟专用网络（VPN），或者运用无线访问点（WAP）。也可以是通过运用网络操作系统（NOS），如运用新技术文件系统（NTFS）的 Windows 允许的文件夹或共享资源，与 Novell 目录服务（NDS）或者 eDirectory 相连接的 Novell NetWare，运用轻量级目录访问协议（LDAP）、Kerberos 或 Sun Microsystem 网络信息系统（NIS）及网络信息系统扩充版本的 UNIX 系统等。最后，可以设立一个规则，用来确定对软件成分限制进入一个系统或网络的操作，我们还会开发出大量的关于访问控制的选项和可能性。

验证

验证可以定义为一个过程，这个过程可以对试图访问网络和资源的计算机或用户进行验证，以证实计算机和用户就是所提供的实体。我们还要检查对远程资源主机证实用户身份的过程；也要对跟踪和确保验证结果的方法（参看第 9 章）进行重新检查。在本

章中，不可否认性就是一种用来确保需要验证的请求人不能在后来否认他就是原请求人的方法（时间戳、特别协议或验证方法）。在下面的部分中，验证方法包括把信任书（如用户名和密码，智能卡或个人识别号码（PIN））提交给 NOS（登录到一台计算机或网络上）、远程访问验证和证书服务以及数字证书的讨论。验证过程运用提供给 NOS（如用户名和密码）并允许 NOS 依据证书证实其身份的信息。

审计

审计是一个对事件、过错和有关系统的验证企图进行跟踪和回顾的过程。与会计跟踪资金流转的过程非常相似，要能够跟踪一个访问企图、访问允许或拒绝、计算机问题或错误以及其他对监控与控制系统都非常重要的事件的印迹。以安全审计为例，要学习有关的能够使管理员追踪对网络、本地计算机或资源进行访问（已验证或未验证）的策略和程序。在许多 NOS 中，审计不能缺省，并且管理员还要经常把要跟踪的事件和目标列入审计列表中。在网络系统的安全和监控中，这就是最基本要求。为了更好地理解，要经常阅读并分析审计过程中生成的日志和文件，如果访问控制正在运行，跟踪则与这些阅读和分析一起进行。

访问控制

随着 AAA 的进一步发展，我们还需要开发这些方面内容的子成分。以访问控制为例，我们必须开发应用于该领域的方法和分组。我们先学习几个新的术语，然后再通过一些实例进行开发，如子成分控制什么、如何才能使网络和设备更为安全等。

MAC/DAC/RBAC

在访问控制的讨论中，强制访问控制（MAC）、自主访问控制（DAC）和基于角色的访问控制（RBAC）是具有不同意义的 3 个领域。

- 从上下文看，MAC 并不是一个网络接口卡的硬件地址，而是一个称为强制访问控制的概念。
- DAC 是自主访问控制的简称，经常称为自主访问控制列表应用（DACL）。
- 不应当把 RBCA 与基于规则的访问控制相混淆，RBCA 这种访问控制方法基于个人或系统的特定角色。

如果要限制对资源、设备或网络的访问，这 3 种方法的用途并不相同。下面研究这些不同的访问控制方法。

MAC

虽然 MAC 也许会设计为应用软件，不过通常还是要嵌入到所运用的操作系统内并在操作系统内执行。在 UNIX、Linux、Windows、OpenBSD 和其他操作系统中都有 MAC 的成分。强制控制通常要进行硬编码并分别对各个目标和资源进行操作。MAC 可以在一个操作系统中应用于任何目标，并且在对目标访问的允许或拒绝方面有一个高阶粒度和功能。MAC 可以应用于每个对象，并且可以通过程序、应用程序和对象用户