加密与解密
实战全攻略

范洪彬　裴要强　编著

- 从加密、解密和欺骗防范三个方面，全面讲解数据安全的知识
- 涵盖硬件、操作系统、办公软件、常用软件和驱动器中的数据加密和解密技术
- 主流的防范黑客盗密技术，如系统漏洞补救，Windows、QQ密码攻防，欺骗攻击防范，网络监听防范和防火墙应用等

人民邮电出版社
POSTS & TELECOM PRESS

HACKING

加密与解密
实战全攻略

范洪彬　裴要强　编著

人民邮电出版社
北京

图书在版编目（CIP）数据

加密与解密实战全攻略 / 范洪彬，裴要强编著. --
北京 : 人民邮电出版社，2010.1
ISBN 978-7-115-21464-5

Ⅰ. ①加… Ⅱ. ①范… ②裴… Ⅲ. ①电子计算机—
密码术 Ⅳ. ①TP309.7

中国版本图书馆CIP数据核字(2009)第195161号

内 容 提 要

本书从加密、解密和欺骗防范3个方面，以理论结合实际的方式讲解了如何确保计算机中数据安全的知识。具体包括硬件、操作系统、办公软件、常用软件和驱动器中的数据加密和解密的技术。另外，还详细介绍了各种网络安全知识，如系统漏洞补救、常用网络安全软件应用、欺骗攻击防范、网络监听防范和防火墙应用等当前较流行的防范黑客盗密技术。

书中的案例图文并茂，结合各种防范技术的应用生动地加以讲解，引导读者较容易地把所学知识应用到实践中。

本书内容丰富，实用性和可操作性强。适合于网络技术爱好者、网络系统管理员阅读，也可作为相关专业学生的学习书籍和参考资料。

加密与解密实战全攻略

◆ 编　　著　范洪彬　裴要强
责任编辑　魏雪萍
执行编辑　张　涛

◆ 人民邮电出版社出版发行　　北京市崇文区夕照寺街14号
邮编　100061　　电子函件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
三河市潮河印业有限公司印刷

◆ 开本：787×1092　1/16
印张：14.75
字数：350千字　　2010年1月第1版
印数：1－3 500册　　2010年1月河北第1次印刷

ISBN 978-7-115-21464-5

定价：35.00元

读者服务热线：(010)67132692　印装质量热线：(010)67129223
反盗版热线：(010)67171154

在网络应用如此普遍的今天，人们在享受网络带来便捷的同时，也在担心无孔不入的黑客入侵给网络安全带来的隐患。如果有一天，一个不曾相识的网友在 QQ 或 MSN 上告诉你："你的计算机密码是×××，你的 QQ 和邮箱密码是×××，你的×××文件……"你一定会在气愤的同时感到非常惊讶，自己加密处理过的数据信息为什么会被陌生人掌握了呢？ 这就是黑客利用加密和解密以及网络欺骗技术实现的。

上述的黑客攻击手段用户很难防范，他们往往属于利用相对较低端的技术来获取极高的计算机权限来达到目的。为了帮助读者更好地保护自己隐私数据的安全，学习到必备的加密和解密以及网络安全知识，提高防范此类攻击的能力，特意撰写了本书。

本书从加密、解密和欺骗防范 3 个方面，以理论结合实际的方式来讲解如何保护计算机中的数据安全，具体内容如下。

第 1 章 千里之行，始于足下——加密解密概述。简要介绍了密码学基础、加密和解密技术的发展趋势，以及密码破解技术的分类。

第 2 章 保护好自己的秘密——本地密码破击与防范。介绍了针对计算机本地存储密码的处理方式，如 BIOS 密码破解与设置、Office 文档加密与解密、邮箱密码的加密和解密等实战技术。

第 3 章 千里奔袭——远程密码破解与防范。讲解了针对存储在远程网络服务器中的账号及密码的加密和解密技术，如 ADSL 用户密码破解与防护、远程 FTP 密码加密、论坛和网络社区密码的防范等。

第 4 章 巧用保密利器——加密解密常用工具。介绍了当前加密和解密技术中一些常用的工具软件。读者通过了解各种工具的特性，可以有针对性地选择使用，以便更有效地对自己的数据进行加密保护，也就可以真正达到"工欲善其事，必先利其器"的目的。

第 5 章 雨疏风骤——Windows 登录密码破解及防范。讲解了远程连接 Windows 系统，远程桌面和终端服务连接、Telnet 远程连接、远程解密 Windows 登录密码等。在了解自己的隐私数据通过另一个出口泄露的原理后，可以有针对性地采取各种补救措施，以加固好自己系统的安全。

第 6 章 雾里看花——网络骗局揭秘及防范。针对网络上的一些常见骗局进行了比较详细地剖析和讲解，例如，修改考试成绩骗局、虚假的 QQ 中奖信息等都是非常常见而且很容易让人受骗的黑客欺诈手段；另外，如网络钓鱼、跨站攻击等行为都蕴藏着极大的破坏能力。在分析这些网络欺骗的基础上，给出了有效的防范措施，以帮助读者及时识破它们。

第 7 章 保卫 QQ 安全——QQ 欺骗招数揭秘。自从 QQ 这个聊天软件诞生以来，一股使用潮流就以不可阻挡之势席卷了网络用户，成千上万的网友为其痴迷，更有甚者将其作为交友联系的惟一方式。但是，正所谓“树大招风”，针对 QQ 的欺骗招数层出不穷，令 QQ 用户防不胜防。本章针对与 QQ 有关的一系列欺骗招数和作弊行为进行了详细的分析，并提出了一些比较有效的防范建议，可以帮助读者安全放心地使用自己的 QQ 聊天工具。

第 8 章 选票时代——认识网络投票欺骗。在互联网上，投票的活动很频繁，如一个网站的一篇新闻、一句留言，都能让许多网友参与其中，更不用说一些网络热门话题了。不过需要指出的是，这种网络选票得出的结果有时是没有任何实际价值的。一些人为了某些目的，用欺骗的手段可以很轻松地以几个简单的招式完全修改投票的结果，如变换 IP 地址，加密代理隐藏 IP 地址等，那么如何防范这些行为呢，本章给出了有效的应对措施。

第 9 章 包罗万象——其他窃密技术揭秘与防范。对网络上一些其他窃密技术进行了详细的分析，如 RM 影音文件挂马、U 盘窃密等均是网络生活中经常会遇到的情况，剖析这些技术特点，并给出了具体的防御方法。

第 10 章 加固城池——巧用工具保护密码安全。通过讲解一些软件的使用，给读者提供了另一种防范窃密的手段，如 QQ 密码安全保卫战、另辟捷径保护机密文件、利用虚拟机困住入侵者等。读者可以通过介绍的软件使用技术与技巧，有目的选择适合自己的工具，以便更好地保护自己的信息安全。

第 11 章 为秘密再上一把锁——加密编程。讲解了一些比较深入的加密编程内容，例如 DES、RSA、MD5 这 3 种典型加密算法的原理和程序实现，以进一步提高读者的加密实战技术能力。

第 12 章 防止暗流——数据包的窃听与还原。通过剖析黑客常用的几款数据窃听工具，介绍了一些针对这些攻击需要采取的防御措施。

第 13 章 御敌于城门之外——巧用主流防火墙防范密码破解。在计算机的安全防护中，防火墙是大家最常用的安全软件。本章通过实例为读者讲解了几款主流防火墙的应用，以给自己的密码增加更好的保护。

本书由范洪彬和裴要强编著，在编写过程中，张博、叶凤云、刘教青、王洪、陈芳、管西京、夏添、柯华坤、王大平、林丁报、张英男、张鹏、温才燚、刘冉、李新峰、李连闯、李绍文等提供了很大帮助，在此表示衷心的感谢。

由于时间仓促，加上编者水平有限，书中难免存在一些不足和错误之处，望广大读者批评指正，联系邮箱为 zhangtao@ptpress.com.cn。

本书内容丰富，实战性和可操作性强，适合于网络技术爱好者、网络系统管理员阅读，也可作为相关专业学生的学习书籍和参考资料。

编　者

目录

第 1 章 千里之行，始于足下——加密解密概述 ……1
1.1 密码技术简介 ……1
1.2 密码破解技术分类 ……1
1.3 总结 ……4
第 2 章 保护好自己的秘密——本地密码破解与防范 ……5
2.1 主板 BIOS 密码破解与设置 ……5
2.1.1 主板 BIOS 密码设置 ……6
2.1.2 CMOS 密码设置与破解 ……6
2.1.3 BIOS 开机密码破解 ……8
2.2 Office 文档加密与解密 ……8
2.2.1 Word 和 Excel 文档加密方法 ……9
2.2.2 Word 和 Excel 文档解密方法 ……9
2.2.3 Word 和 Excel 文档的密码清除 ……11
2.3 找回丢失的宽带账号和 FoxMail 账号 ……12
2.3.1 找回本地宽带密码 ……12
2.3.2 找回本地 FoxMail 密码 ……12
2.4 总结 ……15
第 3 章 千里奔袭——远程密码破解与防范 ……16
3.1 ADSL 用户密码破解与防护 ……16
3.1.1 ADSL 密码终结者简介 ……16
3.1.2 ADSL 密码终结者功能剖析 ……18
3.1.3 ADSL 密码防范 ……19
3.2 E-mail 密码剖解及防范 ……20
3.2.1 流光破解 E-mail 密码剖析 ……20
3.2.2 保护 E-mail 密码 ……23
3.3 破解远程 FTP 密码 ……24
3.3.1 My FTP Cracker 破解 FTP 密码 ……24
3.3.2 Entry 破解 FTP 密码 ……26
3.4 论坛和网络社区密码防范 ……28
3.4.1 论坛和网络社区密码破解原理剖析 ……29
3.4.2 利用 HDSI 获取论坛和网络社区密码 ……30
3.4.3 防止论坛资料被泄露 ……31
3.5 总结 ……31
第 4 章 巧用保密利器——加密解密常用工具 ……32
4.1 密码恢复工具——Cain & Abel ……32
4.2 远程密码解密工具——流光 ……37
4.2.1 流光界面简介 ……37
4.2.2 流光破解密码剖析 ……37
4.2.3 流光其他常用功能介绍 ……39
4.3 易用的加密解密工具——X-SCAN ……42
4.3.1 X-SCAN 功能简介 ……42
4.3.2 X-SCAN 使用指南 ……43
4.4 兼具数据修复的加密工具——WinHex ……48
4.5 用 WinHex 检查文件安全性 ……49

4.6 字典生成器……51
4.6.1 黑客字典剖析……51
4.6.2 超级字典生成器——Superdic……54
4.7 总结……56

第 5 章 雨疏风骤——Windows 登录密码破解及防范……57
5.1 远程登录 Windows 系统……57
5.1.1 远程连接 Windows 系统……57
5.1.2 远程桌面和终端服务连接……62
5.1.3 Telnet 远程连接……66
5.2 远程解密 Windows 登录密码剖析……68
5.2.1 获取目标用户名……69
5.2.2 解密 Windows 登录密码……69
5.3 总结……71

第 6 章 雾里看花——网络骗局揭秘及防范……72
6.1 揭穿修改考试成绩骗局……72
6.2 揭穿入侵知名网站的骗局……73
6.3 查出社区论坛的冒名顶替……76
6.3.1 虚假管理员……76
6.3.2 空格法欺骗……77
6.3.3 特殊符号法欺骗……77
6.4 揭穿网络钓鱼骗局……78
6.5 揭露虚假 QQ 中奖信息……81
6.5.1 揭露 QQ 中奖信息骗局……81
6.5.2 揭露假冒域名……82
6.5.3 识破假客服电话……83
6.5.4 识破虚假通知信息……83
6.5.5 防范欺骗信息……83
6.5.6 识破虚假用户名……84
6.6 揭露虚拟主机的骗术……84
6.6.1 个人 PC 充当试用空间……85
6.6.2 租用网络空间陷阱……85
6.6.3 “肉鸡”服务器……86
6.6.4 防范支招……86
6.6.5 其他骗术揭秘……86
6.7 防不胜防的跨站攻击……86
6.7.1 认识动态网页……87
6.7.2 认识跨站攻击……87
6.7.3 跨站攻击的危害……89
6.7.4 防范跨站攻击……90
6.8 域名劫持……90
6.9 总结……91

第 7 章 保卫 QQ 安全——QQ 欺骗招数揭秘……92
7.1 “QQ 连连看”游戏作弊剖析……92
7.1.1 “QQ 连连看”游戏作弊测试……92
7.1.2 防范“QQ 连连看”游戏作弊……94
7.2 “QQ 斗地主”游戏作弊……94
7.2.1 “QQ 斗地主”游戏作弊剖析……94
7.2.2 防范“QQ 斗地主”游戏作弊……97
7.3 查看 QQ 好友是否隐身……98
7.4 QQ 号码争夺战……99
7.5 识别其他的 QQ 欺骗技术……103
7.6 QQ 欺骗其他招数揭秘……105
7.7 总结……109

第 8 章 选票时代——认识网络投票欺骗……110
8.1 变换 IP 进行无限投票……110
8.1.1 ADSL 用户改变 IP 投票……111
8.1.2 加密代理隐藏 IP 地址投票……112
8.2 修改 Cookies 突破投票限制……115
8.2.1 删除本地 Cookies 文件……115

8.2.2 禁止 Cookies 文件写入 ……116
8.3 刷票工具的使用及原理剖析 ……118
8.4 总结 ……120

第 9 章 包罗万象——其他窃密技术揭秘与防范 ……121

9.1 SEO（搜索引擎优化） ……121
9.2 互刷联盟 ……123
9.3 防范利用病毒和流氓软件搞欺诈排名 ……124
9.4 识破欺骗信息广告 ……125
9.5 防范拒绝服务攻击（DDoS） ……126
9.6 U 盘窃密的攻与防 ……127
9.6.1 U 盘搬运工剖析 ……127
9.6.2 防范支招——对 U 盘进行加密 ……128
9.7 警惕潜伏的欺骗危机 ……131
9.7.1 防范 RM 影音文件挂马 ……131
9.7.2 CHM 电子书木马剖析 ……134
9.7.3 防范 CHM 电子书木马 ……137
9.8 实现压缩超过 1000 倍的效果 ……138
9.9 总结 ……139

第 10 章 加固城池——巧用工具保护密码安全 ……140

10.1 密码安全防护常识 ……140
10.1.1 几种绝不能使用的密码 ……140
10.1.2 安全设置密码 ……141
10.2 QQ 密码安全保卫战 ……143
10.2.1 巧用 QQ 医生 ……143
10.2.2 在线查杀 QQ 病毒 ……145
10.2.3 徒手力擒 QQ 病毒 ……146
10.3 另辟捷径保护机密文件 ……151
10.3.1 文件夹隐身术 ……151
10.3.2 设置拒绝访问的文件夹 ……153
10.4 利用虚拟机困住入侵者 ……155
10.4.1 虚拟机种类简介 ……155
10.4.2 虚拟机安装方法 ……156
10.4.3 虚拟机使用指南 ……159
10.4.4 虚拟机网络设置 ……162
10.5 巧用工作组信息文件保护敏感信息 ……165
10.5.1 工作组信息文件基础知识 ……165
10.5.2 工作组信息文件的使用 ……167
10.5.3 工作组信息文件保护数据库技巧 ……168
10.6 总结 ……170

第 11 章 为秘密再上一把锁——加密编程 ……171

11.1 密码学基础 ……171
11.1.1 密码学简介 ……171
11.1.2 分组密码技术 ……172
11.1.3 公钥密码技术 ……174
11.2 DES 算法分析 ……175
11.2.1 DES 加密原理 ……175
11.2.2 DES 程序实例与分析 ……181
11.2.3 DES 实例运行结果 ……185
11.3 RSA 算法分析 ……186
11.3.1 RSA 加密原理 ……186
11.3.2 RSA 程序实例与分析 ……187
11.3.3 RSA 实例运行结果 ……188
11.4 MD5 算法分析 ……189
11.4.1 MD5 原理 ……190
11.4.2 MD5 程序实例与分析 ……192
11.4.3 MD5 实例运行结果 ……193
11.5 总结 ……194

第 12 章 防止暗流——数据包的窃听与还原 ····· 195
12.1 黑客窃听和还原数据包剖析 ····· 195
12.2 黑客窃听和还原数据包原理解析 ····· 197
12.3 黑客窃听和还原数据包实例分析 ····· 199
12.3.1 程序功能分析 ····· 200
12.3.2 程序代码实现 ····· 200
12.4 黑客窃听和还原数据包的防范 ····· 202
12.5 总结 ····· 203
第 13 章 御敌于城门之外——巧用主流防火墙防范密码破解 ····· 204
13.1 防火墙基础知识 ····· 204
13.2 Windows 防火墙 ····· 205
13.3 天网防火墙 ····· 207
13.4 黑冰（BlackICE）防火墙 ····· 213
13.5 Comodo 防火墙 ····· 215
13.6 Outpost Firewall 防火墙 ····· 220
13.7 总结 ····· 228

第1章 千里之行，始于足下——加密解密概述

1.1 密码技术简介

加密技术是一门古老而深奥的学科，它对一般人来说是陌生的，因为长期以来，它只在很少的范围内，如军事、外交、情报等部门使用。

虽然密码技术已经经过了很长时间的发展，但是它最核心的部分却从来都没有改变过：加密方将想要传达的信息以一种不被别人所了解的方式保存起来并安全地发送给接收方；解密方利用各种手段将信息截获，并且设法了解信息中想要传达的真实意图。而到了今天的互联网时代，加密与解密的斗争同时将目光放到了一个焦点之上：密码口令——一种在 IT 领域独有的身份识别方式。

1.2 密码破解技术分类

在目前的计算机及互联网安全中，密码占据了举足轻重的地位，所以黑客们对密码破解技术的热情也从来没有消退过。虽然密码技术经过了很多年的发展，不过对应的破解方法却从来都是万变不离其宗。

1．穷举式破解

在大多数情况下，试图破解密码的黑客所掌握的只有一个输入密码的提示界面（如图 1-1 所示），这种情况下能做的只有利用工具进行穷举式破解。

穷举式破解的工作原理非常简单，利用相关软件针对密码界面进行自动猜解。自动猜解的方式通常分为两种：字典攻击与强行攻击（又称暴力破解）。

因为多数人使用普通词典中的单词作为口令，发起词典攻击通常是较好的开端。词典攻击使用一个包含大多数词典常用单词或常用字符的文件，文件的内容为每个单词占一行（如图 1-2 所示），工具自动提取这些单词来猜测用户口令。

图 1-1 最常见的管理员登录界面

图 1-2 字典内容

词典攻击的一大缺点就是，如果实际密码没有被放到字典文件中，那么密码将永远都不可能被猜解出来。而强行攻击则不需要字典文件的支持，工具会从最基本的字符开始一直猜解下去，直到密码被猜解出来，只要有足够的时间，任何密码都会被最终猜解出来。

由于软件的猜解速度与计算机本身的运算速度和网络延时速度有很大的关系，所以选择穷举式破解时应该选择 CPU 运算速度较高的计算机，以及相对较好的网络环境下进行。

虽然从理论上讲穷举式破解可以猜出任何密码，但是此方法成功与否的决定因素取决于密码的复杂程度而非破解者的技术与工具，可以说完全是一种依靠运气的行为，所以在有其他选择的情况下几乎没有破解者使用穷举式破解方法。

2．密码截取

对于试图获取密码的黑客来说，最理想的状态是对目标计算机拥有操作的权限。这样黑客就可以将截取密码的程序植入目标计算机中以获取其全部的密码信息，这类截取密码的程序被统称为“特洛伊木马”（以下简称“木马”）。

木马虽然拥有巨大的破坏力，不过它的使用方法却十分简单。图 1-3 所示便是一款典型的木马程序，只要黑客填写几个最基本的选项并执行木马程序，就可以等待目标计算机有人输入密码，这样木马就会自动记录密码并将其发送到黑客已打开的电子邮件或网络空间中（如图 1-4 所示）。

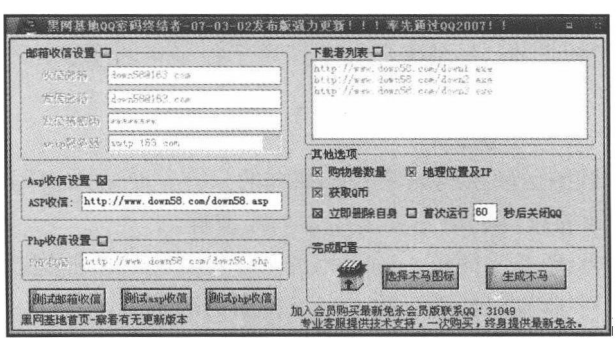

图 1-3 木马程序标准界面

木马的出现可以说为互联网安全性带来了一场翻天覆地的变革，使用木马来获取密码是

最简单也是最快捷的方法，只要目标执行了黑客准备的木马程序，无论多么安全的防护措施都会在瞬间变的毫无意义。对于黑客来说虽然使用木马有着各种各样的优势，但是它也同样存在一个巨大的缺陷：黑客必须通过某种方式让木马程序在目标计算机中成功执行。随着人们安全意识的逐渐提高，这一步骤将会越来越困难。如何将自己这份外表善意的古希腊礼物送入比特洛伊城还要坚固百倍的计算机中，将是黑客们永远不会停止的话题。

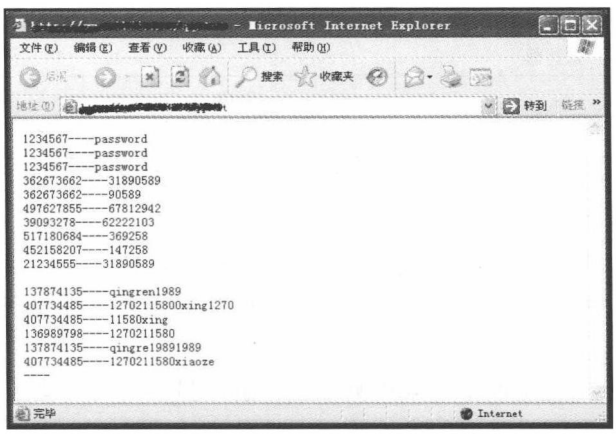

图 1-4 盗取的 QQ 与密码列表

3．破解密文

很多时候，黑客通过各种方式获得了对方的密码信息，但是却发现获得的密码信息是一段被加密之后的代码（如图 1-5 所示），这个时候就要将密码还原回最初的明文形式。

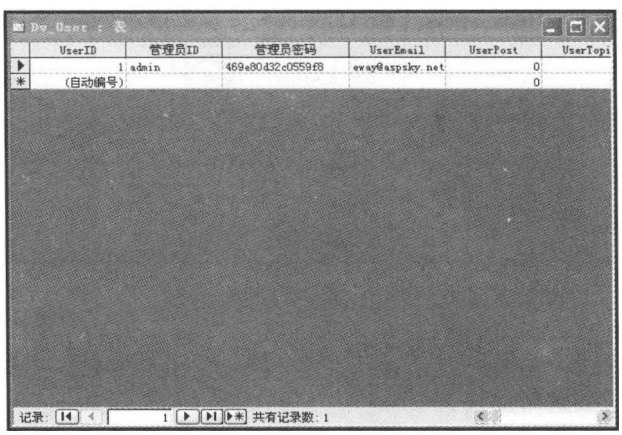

图 1-5 常用的加密方式

破解密文首先要清楚密码的加密方式，获得对方加密方式的方法有两种：找到加密程序代码或是根据加密前明文与加密后密文的对比运算出加密方式。

通常，获取加密后密码信息的情况普遍发生在查找本地计算机的某些存储文件或是下载网站中的数据库，所以只要找到该文件的相关信息以及利用搜索引擎下载网站中的程序代码就可以轻松获取加密方式。

因为一种程序的加密方式与存放密码文件的路径都是固定的，所以大多数程序都会被人写出密码读取工具，只要瞬间就可以将本地计算机程序中的密码破解。

根据加密前后信息的对比看上去是一种十分深奥的问题，不过实际上在大多数情况下，破解一段程序的加密方式比解开一道中学时期的数学方程式还要简单。表 1-1 所示是一段在网络上颇为流行的加密方式。

表 1-1　　加密前后的对比

加　密　前	加　密　后
admin	bfpms
11111	23456

只要稍微思考一下，就可以知道这种加密方式是如何运算的：根据密码的位数将相应的字符向后移位就变成了加密后的密文。

并不是所有的密文都可以被成功地转换为明文。例如，图 1-5 中【管理员密码】一栏中显示出的“469e80d32c0559f8”便是利用著名的 md5 加密方式进行加密的，这种加密方式在目前是不可以被逆向还原成原来的明文的。

对于不可逆向还原的密文通常应采用穷举式破解，虽然同为穷举式破解，但是在知道密文的情况下破解时不需要网络验证的本地破解，其猜解速度要远高于网络上穷举式破解。

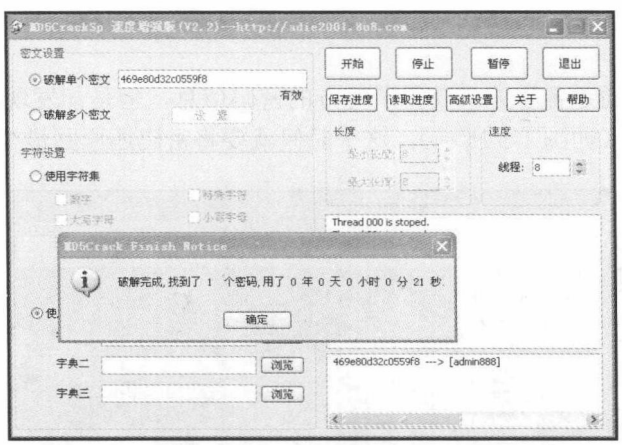

图 1-6　成功破解密码

如图 1-6 所示，在网络中破解一个 8 位字母与数字混合的密码大概需要几个月的时间，但是用在本地计算机的破解时间仅为 21s。

1.3　总结

本章仅仅为读者介绍了一些密码的基础知识，密码技术并没有想象的那样充满了惊奇，在大多数时候我们要面对的都是漫长而又充满枯燥的破解过程。在第 2 章中，我们将进入密码破解技术中相对较容易的部分——本地密码破解。

第2章 保护好自己的秘密——本地密码破解与防范

对于一名学习密码破解的初学者来说，更多的时候是要面对计算机本机中的各式密码：开机密码、文档密码、各种软件的解锁密码，等等。这些存储在本机中的密码大多都只有很低的安全系数，即使是完全没有计算机安全相关知识的人，只要利用适当的软件就可以轻松将这些密码破解。本章将介绍的是一些计算机常用密码的相关知识以及破解方法。

2.1 主板 BIOS 密码破解与设置

BIOS（Basic Input Output System，即基本输入输出系统）设置程序是被固化到计算机主板上的 ROM 芯片中的一组程序，其主要功能是为计算机提供最底层的、最直接的硬件设置和控制。CMOS 主要用于存储 BIOS 设置程序所设置的参数与数据，如图 2-1 所示；而 BIOS 设置程序主要对技巧的基本输入/输出系统进行管理和设置，当系统运行在最好状态时，使用 BIOS 设置程序还可以排除系统故障或者诊断系统问题。利用 BIOS 设置的密码分为两种：开机密码和 CMOS 设置密码。

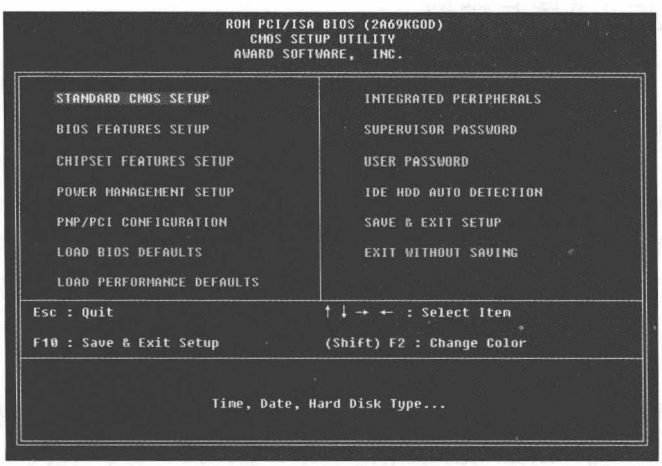

图 2-1 CMOS 的设置界面

2.1.1 主板 BIOS 密码设置

开启计算机或重新启动计算机后，在屏幕显示“Waiting...”时，按下【Del】键就可以进入 CMOS 的设置界面，如图 2-1 所示。要注意的是，如果按得太晚，计算机将会启动系统，这时只有重新启动计算机了。可以在开机后立刻按住键盘中的 Del 键直到进入 CMOS。进入后，可以用方向键移动光标选择 CMOS 设置界面上的选项。

1．CMOS 设置密码

界面中左侧的【USER PASSWORD】项为进入 CMOS 的管理员密码，将光标移到此选项并按下【回车】键后将弹出如图 2-2 所示的输入密码窗口。当下次重新进入 CMOS 设置时就会出现与图 2-2 所示的相同窗口，只有输入正确的密码才可以进入。

2．开机密码

（1）选择 CMOS 的设置界面左侧的【SUPERVISOR PASSWORD】选项，按【回车】键并输入密码。

（2）选择【BIOS FEATURES SETUP】按【回车】键进入下一级菜单，如图 2-3 所示。

图 2-2 输入密码窗口

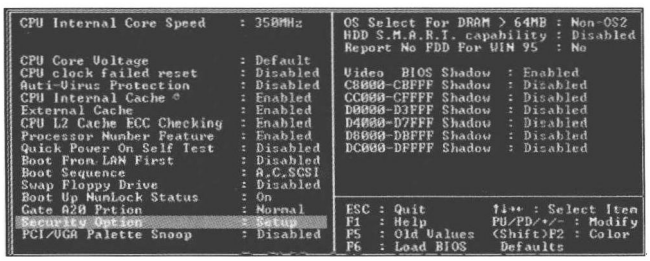

图 2-3 开启开机密码功能

（3）选择【Security Option】并按下键盘上的【Page up】键，将“SETUP”改为“SYSTEM”。

（4）按下键盘上的【Esc】键退至图 2-1 所示的主菜单中，选择【SAVE & EXIT SETUP】选项保存并退出 BIOS 系统即可。

2.1.2 CMOS 密码设置与破解

正如上文所说，CMOS 中的密码还是处于计算机刚刚普及的时代，所以从安全性的角度上看，这些密码的破解方法简直是不值一提。

1．万能密码

在计算机安全知识不是很普及的时代，将密码忘记是一件很麻烦的事情，所以在早期的软件设计中开发者都会留下一些万能密码以防止不小心将密码忘记带来的困扰。而 BIOS 系统的制作商至今仍保持着这一习惯，一些 BIOS 系统最常使用的万能密码为：

Wantgirl、Syxz 、dirrid 、eBBB 、h996 、wnatgirl 和 Award。

2．BiosPwds

如果万能密码无法进入 BIOS 系统，则可以使用软件 BiosPwds 来直接读取密码，如图 2-4 所示为 BiosPwds 界面。BiosPwds 的用法十分简单，只需要单击【Get Passwords】按钮，密码就会自动显示出来。BiosPwds 的缺陷是只能读取 Award 型号的 BIOS。虽然 Award 目前

占据着市场的主流，不过仍然有许多用户在使用非 Award 的 BIOS，其弹出界面如图 2-5 所示，提示用户无法破解密码。

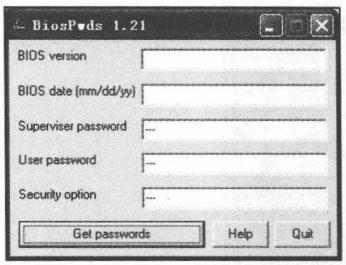

图 2-4 BiosPwds 主界面

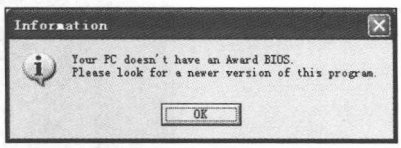

图 2-5 程序无法读出密码

3．利用 DEBUG 清空密码

Debug 是一款系统自带的命令，在 DOS 系统下运行用于对计算机的测试和调试。从 1980 年的 DOS 1.0 版本到目前的 Windows Vista 都可以看到此命令的身影。虽然此命令的功能非常强大，可以解决许多问题，可是使用此命令需要操作人员掌握熟练的汇编语言，这对许多连 DOS 都没用过的初学者来说，实在很困难。不过本书只是介绍它在具体情况下的具体用法，读者只需要按着文中所提示的步骤进行操作即可，操作步骤如下。

（1）单击【开始】按钮，在弹出的 Windows 菜单中单击【运行】选项。

（2）在弹出的窗口中输入 command 并单击【确定】按钮（如图 2-6 所示），接下来会弹出一个命令提示符窗口，如图 2-7 所示。

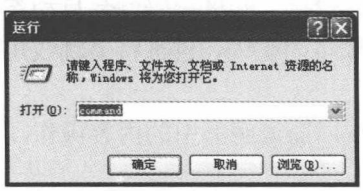

图 2-6 “运行”界面

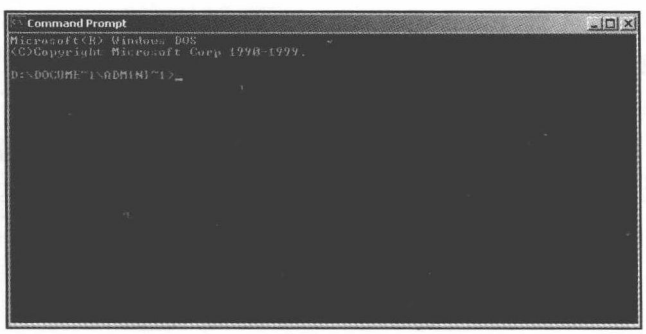

图 2-7 Command 命令提示符窗口

小贴士：在微软公司推出 Windows 系统之前，DOS 系统曾经是辉煌一时的操作系统。由于 DOS 采用的是字符操作界面，用户对计算机的操作一般是通过键盘输入命令来完成的，所以想要操作 DOS 系统就必须学习相应的命令。另外，它的操作也不如图形界面来得直观，对 DOS 系统的学习还是比较费力的，这对普通用户造成了很多的困难。当 Windows、Linux 等图形界面系统推出后，DOS 系统被迅速地抛进了垃圾箱中。不过对于热爱网络安全相关技术的人来说，熟悉使用 DOS 系统是一项必备的技能。在本书以后的相关章节中，笔者会以这种小贴士的形式向大家讲述 DOS 系统的操作以及其他重要的内容。

（3）在命令提示符窗口下输入如下命令（如图 2-8 所示）。

```
debug
70 2e
71 00
```

```
70 2f
71 00
q
```

图 2-8 消除 CMOS 设置的密码

此命令的作用是消除 CMOS 设置的密码，将以上命令输入完毕后，重新启动计算机进入 CMOS 设置时，会发现不会再有提示输入密码的窗口了。需要注意的是，此方法只在 Windows 2000/NT 及以前的系统中适用，Windows XP 及以后的系统由于命令行下无法直接对硬件进行操作，所以不能使用此方法破解 CMOS 设置的密码。

2.1.3 BIOS 开机密码破解

关于 BIOS 开机密码，互联网上流传着很多版本的破解方法，但无论用哪种方法都有一个大前提：在成功地登录到系统的情况下。因为 BIOS 开机密码是在计算机执行其他程序之前就已生效，如果不输入正确的密码甚至连驱动程序都不会启动，所以任何软件及命令在 BIOS 开机密码前都是不管用的。想清除密码只有打开机箱从硬件部分入手。

1．跳线短接

有些主板设置了主板密码清除跳线，这时只需要将该跳线短接，开机密码就会自动被清除。即使主板上没有密码清除跳线，至少会有一条给 CMOS 放电的跳线，也可将该跳线短接后密码也会自动被清空。

对计算机硬件不是很了解的用户在使用此方法时一定要按厂商说明书中的内容操作，一旦把跳线接错很可能会出现硬件被烧的后果。

2．电池放电

计算机的主板有一块电池是用来供电的，如果该电池的电量不足，那么主板的一切设置都会进入初始化状态。所以将主板上的电池取下来并取一根导线为电容放电，同样可以达到清除密码的效果。使用此方法的缺点是，所有的 CMOS 设置都会被清空，重新设置 CMOS 是一件十分烦琐的事情。

2.2 Office 文档加密与解密

作为世界上最优秀的自动办公软件之一，微软的 Office 系列软件中的每一个组件都有一