HZ BOOKS

加解密高手
技术档案

完全掌握

加密解密

实战超级手册

深入内涵，全盘理解，掌握精髓

- 来自安全技术一线培训师与程序员的经验之谈，从入门到实践，深入浅出地介绍最新、最实用的软件加解密技术
- 结合实战案例，详析编程思路，教你掌握方法，快速成长为加解密职业高手

DVD

7小时
多媒体视频讲解

张晓新　孙国岭　杨平等 编著

机械工业出版社
China Machine Press

完全掌握
加密解密实战
超级手册

张晓新　孙国岭　杨平等 编著

机械工业出版社
China Machine Press

本书紧紧围绕软件的加密与解密来进行讲解，在详细讲述加密/解密技术的同时，还介绍了相应的实现原理，并配合案例分析，使读者能够系统、深入地了解加密/解密技术，能够更深层次地理解他人的编程思路，从而更好地提高自己的编程水平。全书共分为14章，包括：加密解密技术基础、常用代码分析工具、不同的加密解密算法、静态分析解密工具、动态调试解密工具、辅助工具、壳的不同应用技术、为程序打上补丁、网络验证技术、常用加密工具、不同的注册保护方式、编辑安装包程序、不同软件的保护措施、常用软件加密解密技术等。

本书讲解通俗，深入浅出，注重实践，适用于广大计算机软件加密解密技术新手、爱好者，适用于软件开发从业人员和编程爱好者，也非常适合大专院校相关专业学生，以及有志于从事安全或加解密行业的准专业人员快速掌握实用技术。

图书在版编目（CIP）数据

完全掌握加密解密实战超级手册 /张晓新 孙国岭 杨平等 编著. - 北京：机械工业出版社，2010.5

ISBN 978-7-111-30360-2

Ⅰ. ①完… Ⅱ. ①张… ②孙… ③杨… Ⅲ. ①软件－密码－加密 ②软件－密码－解密译码
Ⅳ. ①TP311.56

中国版本图书馆CIP数据核字（2010）第064433号

机械工业出版社（北京市西城区百万庄大街22号　邮政编码　100037）
责任编辑：夏非彼　迟振春
北京科普瑞印刷有限责任公司印刷
2010年5月第1版第1次印刷
188mm×260mm · 27.75印张
标准书号：ISBN 978-7-111-30360-2
　　ISBN 978-7-89451-489-9（光盘）
定价：55.00元（附1DVD）

凡购本书，如有缺页、倒页、脱页，由本社发行部调换
客服热线：（010）88378991；82728184
购书热线：（010）68326294；88379649；68995259
投稿热线：（010）82728184；88379603
读者信箱：booksaga@126.com

完全掌握

加密解密实战 超级手册

加解密高手技术档案

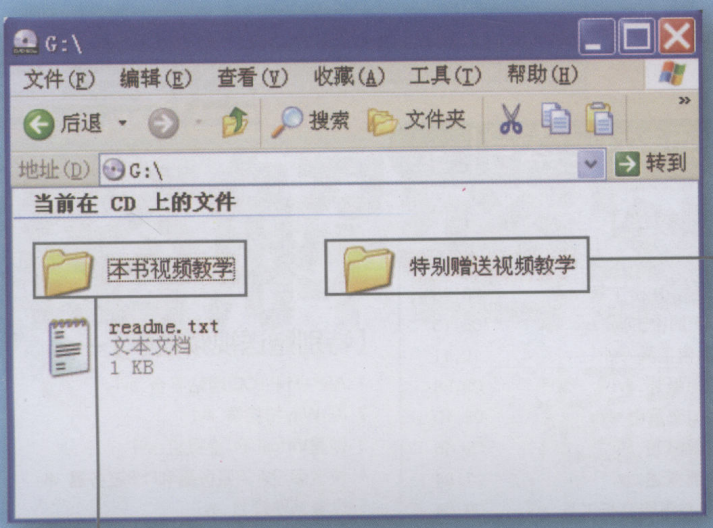
多媒体教学光盘

DVD

多媒体教学光盘使用说明

32 个	28 个	总播放时长近 7 小时
与本书配套视频教学文件	赠送与黑客技术相关的视频教学文件	

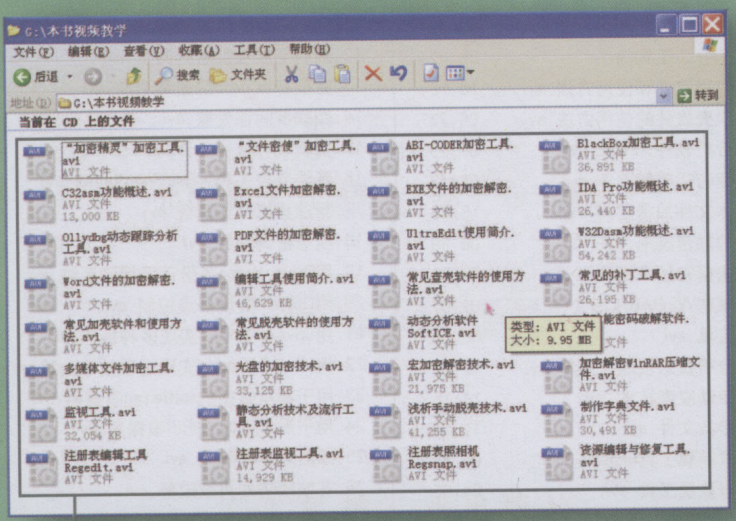
1. 本书光盘附赠作者亲自录制的多媒体语音视频讲解，涵盖32个本书关键课程的视频教学，28个常用黑客工具与安全技术课程，视频教学播放总时长近7小时，超值实用。



黑客与安全工具技术视频教程

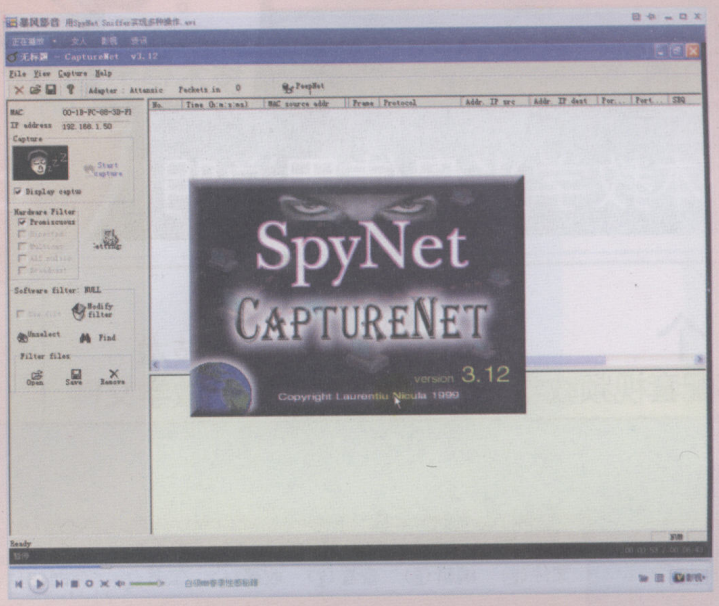
本书关键内容的视频教程

2. 视频教学存放在本光盘的两个文件夹中，打开光盘下的文件夹，即可找到视频教学文件。



视频教学文件

3．双击光盘下的视频教学文件，即可以使用Windows 的视频播放器Windows Media Player播放，如果你安装了其他的视频播放软件，如暴风影音，同样也可以使用这些软件来播放教学视频。



多媒体视频教程索引

【本书视频教学】

1．“加密精灵”加密工具.avi	06:42
2．“文件密使”加密工具.avi	08:28
3.ABI—CODER加密工具.avi	06:15
4.BlackBox加密工具.avi	10:11
5.C32asm功能概述.avi	03:58
6.Excel文件加密解密.avi	08:10
7.IDA Pro功能概述.avi	09:46
8.IDA Pro功能概述.avi	07:54
9．Ollydbg动态跟踪分析工具.avi	09:04
10.PDF文件的加密解密.avi	09:47
11.UltraEdit使用简介.avi	07:58
12.W32Dasm功能概述.avi	18:09
13.Word文件的加密解密.avi	10:32
14.编辑工具使用简介.avi	14:45
15.常见查壳软件的使用方法.avi	03:23
16.常见的补丁工具.avi	08:32
17.常见加壳软件和使用方法.avi	10:19
18.常见脱壳软件的使用方法.avi	06:22
19.动态分析软件SoftICE.avi	07:29
20.多功能密码破解软件.avi	02:48
21.多媒体文件加密工具.avi	15:48
22.光盘的加密技术.avi	08:39
23.宏加密解密技术.avi	06:24
24.加密解密WinRAR压缩文件.avi	02:07
25.监视工具.avi	08:30
26.静态分析技术及流行工具.avi	12:23
27.浅析手动脱壳技术.avi	14:15
28.制作字典文件.avi	10:01
29.注册表编辑工具Regedit.avi	09:39
30.注册表监视工具.avi	04:35
31.注册表照相机Regsnap.avi	04:12
32.资源编辑与修复工具.avi	09:34

【特别赠送视频教学】

1.ASP+PHP+CGI网站平台.avi	09:58
2.X—Way扫描器.avi	05:20
3.创建Virtual PC虚拟机.avi	06:18
4.快速架设ASP服务器和PHP服务器.avi	04:54
5.设置系统项目.avi	04:57
6.设置邮箱的反垃圾功能.avi	01:52
7.设置桌面项目.avi	03:39
8.生成木马服务器.avi	03:21
9.使用FinaData恢复数据.avi	08:08
10.使用驱动精灵备份硬件驱动.avi	01:47
11.顺利下载被保护的图片.avi	04:09
12.顺利下载被加密的网页.avi	05:32
13.完美卸载2008的杀毒功能.avi	03:02
14.微软反间谍专家.avi	11:09
15.伪装成可执行文件.avi	04:53
16.系统监控工具：RealSpyMonitor.avi	04:21
17.新建虚拟操作系统.avi	05:17
18.星号密码查看.avi	05:12
19.用Drive Image备份还原操作系统.avi	05:31
20.用QuickIP实现多点控制.avi	10:44
21.用SpyNet Sniffer实现多种操作.avi	06:43
22.用URLY Warning实现远程信息监控.avi	03:55
23.用于捕获数据的snifferpro嗅探器.avi	04:15
24.用于局域网嗅控IRIS嗅探器.avi	08:29
25.邮箱炸弹的防范.avi	04:24
26.有效预防网页被破解.avi	09:13
27.预防远程控制的“QQ远控精灵”.avi	04:06
28.运行组策略.avi	03:23

前言

随着网络技术的发展，在互联网上进行文件传输、电子邮件商务往来存在着许多不安全因素，特别是在网络上传输的一些大公司的机密文件。因此，数据安全已成为不可回避的话题。

加密与解密技术可有效确保用户的数据信息不被别人拦截和窃取，但加密与解密是一种辩证的关系，两者相互矛盾、相互依存、缺一不可，解密可以促进软件加密水平的进一步提高，加密水平的提高又需要解密技术的验证。

本书内容

本书以图释、标注、指引线框等丰富的图解手段，再辅以浅显易懂的语言，不但介绍了加密解密技术的一般方法、步骤，而且可使读者在了解日常加密解密技术的前提下，注重对操作技巧的剖析，使读者在遇到不同的疑难时，能够尽可能的心中有数，采取相关的方法来制定相应措施。全书共分为 14 章，主要内容包括：常用代码分析工具、加密解密算法、静态分析工具、动态调试工具、辅助工具、壳、补丁、网络验证、常用加密工具、注册保护方式、安装包程序、不同软件的保护措施以及常用软件加密解密技术等。

本书特色

本书以情景教学、案例驱动与任务进阶为鲜明特色，在书中可以看到一个个生动的情景案例。通过完成一个个实践任务，读者可以轻松掌握各个知识点，在不知不觉中快速提升实战技能。

- 从基础到实践，完全站在实用的角度，介绍加密解密技术。与大量传统教材不同的是，突出了实用性和案例分析，所举实例来自于实际应用，学以致用，真正解决问题。
- 通俗易学，结合图解、标注和多媒体教学，使神秘、高深、难以掌握的加密解密技术学习起来省时、省力，易于上手，非常适合新手、大专院校学生，以及有志于从事安全或加密解密行业的准专业人员快速掌握实用技术。
- 紧扣“理论+实战+图文+视频=全面提升学习效率!”的主导思想，详细分析每一个操作案例，以实现读者用更少的时间尽快掌握加密解密技术的操作，并对实战过程中常见问题作必要的说明与解答。
- 当前最新技术、热点技术、常用相关工具软件都在本书有所涉及，对加密解密的编程技术、方法与思路也做了重要讲解，并通过实例介绍综合技术的运用手段，能够达到举一反三的效果。

- 超值的多媒体配套教学光盘。在随书多媒体配套教学光盘中，尽可能使读者在阅读时参考光盘中的视频教程，轻松、快速地实现自己的网络化办公需求。

读者对象

本书面对的读者可分为3个层次：

- 入门读者。这类读者往往需要为自己的日常文档、邮箱等加密，或简单破解忘了密码的文件。本书注重实用，可以满足这类读者的需要。
- 进阶读者。这类读者对诸多专业软件和技术的原理一知半解，达不到系统掌握的阶段，所以他们的实践运用能力也就总停滞不前。本书注重学好理论基础并举一反三，达到各种技术的综合运用，完全适合这类读者。
- 从业人员。这类读者需要各种技术的灵活运用和丰富的临场发挥，成功的实例是该类读者不断提高自己的阶梯，并有助于拓展视野，直接获得实践经验。

本书由多名经验丰富的高校教师及安全专家编写，其中大多数长期从事安全技术教学软件开发和培训工作，同时也得到了众多网友的支持，在此一并表示衷心的感谢。参与本书编写的老师有：刘双红负责第1章，陈艳艳负责第2章，段玲华负责第3章，杨平负责第4章，余建国负责第5章，张晓新负责第6、7、8章，李防负责第9章，李伟负责第10章，孙国岭负责第11、12章，安向东负责第13、14章，最后由武新华统审全稿。我们虽满腔热情，但限于自己的水平，书中仍难免有失误、遗漏之处，因此，还望大家以宽容为本，本着共同探讨、共同进步的平和心态来阅读本书。作者心存谨敬，随时恭候您提出宝贵意见，联系邮箱：lly69@vip.sina.com。

编者

2010年3月

目录

第1章

初识加密解密技术

重点提示

- 加密解密技术基础
- 动态链接库（DLL）文件
- 设计与发布 BPL 组件
- 解密与注册保护
- 试用期限制功能

本章精粹

本章主要介绍了关于加密解密的基础知识，其中包括加密基础技术、文件读写、BPL 组件设计、软件试用期，以及几种常用软件解密方法和软件注册保护方式，展现了比较全面的加密解密技术知识。

1.1 加密解密技术基础

加密解密技术长期以来只应用在很小的范围内，如军事、外交、情报等部门使用。计算机加密技术是研究计算机信息加密、解密及其变换的科学，是数学和计算机的交叉学科，也是一门新兴的学科。

很多人都曾不止一次地面对过网络上的安全问题，黑客程序、病毒、邮件炸弹、远程侦听等安全问题，让人一听就胆战心惊。病毒、黑客的肆意猖獗，更是使人时刻感觉到危险无处不在。因此，人们就想到了要对自己的数据进行加密。

对数据进行加密，在国外已成为计算机安全主要的研究方向，也是计算机安全课程教学中的主要内容。一个密码系统的安全性只在于密钥的保密性，而不在于算法的保密性。

1.1.1 密码学简述

密码学可细分为编码学和破译学两个方面，编码学主要研究密码变化的客观规律，一般应用于编制密码，以确保通信过程中的信息安全；破译学主要用于破译密码，以获取通信过程中的情报。

随着先进科学技术的应用，密码学已成为隐藏通信信息内容的重要保密手段。通信双方按一些约定的准则对信息进行特殊变换，其中若是变明文为密文，则称加密变换；若是变密文为明文，则称脱密变换；而进行明密变换的准则，被称为密码的体制；指示这种变换的参数，就是所谓的密钥。密码的体制和密钥均是密码编制过程中的重要组成部分，而密码体制的基本类型一般有4种：错乱、代替、密本和加乱。

- 错乱：按照规定的图形和线路，改变明文字母或数码等的位置成为密文。
- 代替：用一个或多个代替表将明文字母或数码等代替为密文。
- 密本：用预先编定的字母或数字密码组，代替一定的词组单词，从而变明文为密文。
- 加乱：用有限元素组成的一串序列作为乱数，按照一定的算法，同明文序列相结合后变成密文。

对于上述4种密码体制，为编制出各种复杂度很高的实用密码，既可对其单独使用，也可将它们混合使用。密码破译是随着密码的使用而逐步产生和发展的。它利用文字和密码的规律，通过采取各种技术手段对密文进行认真而细致地分析，以还原密码编制并最终获得加密前的明文信息。

1.1.2 常用汇编语言命令

汇编语言是面向机器的程序设计语言，描述了机器最终要执行的指令序列，是人和计算机沟通的最直接方式。它主要由三部分内容组成：汇编指令、伪指令和其他符号。其中，汇编指令即机器码的助记符，汇编后直接由机器执行；而伪指令或其他符号均由编译器识别。

由于在加密解密过程中，往往会遇到或用到一些常见的汇编语言的概念或命令，为了便于