<<加密与解密>>

图书基本信息

书名：<<加密与解密>>

13位ISBN编号：9787121066443

10位ISBN编号：7121066440

出版时间：2008-7

出版时间：电子工业出版社

作者：段钢

页数：543

<<加密与解密>>

内容概要

本书以加密与解密为切入点，讲述了软件安全领域许多基础知识和技能，如调试技能、逆向分析、加密保护、外壳开发、虚拟机设计等。
读者在掌握本书的内容，很容易在漏洞分析、安全编程、病毒分析、软件保护等领域扩展，这些知识点都是相互的，彼此联系。
国内高校对软件安全这块领域教育重视程度还不够，许多方面还是空白，而近年来许多企业对软件安全技术人才需求量越来越大。
从就业角度来说，掌握这方面技术，可以提高自身的竞争能力；从个人成长角度来说，研究软件安全技术有助于掌握一些系统底层知识，是提升职业技能的重要途径。
作为一名合格的程序员，除了掌握需求分析、设计模式等外，如能掌握一些系统底层知识，熟悉整个系统的底层结构，对自己的工作必将获益良多。
本书可以作为学校或培训机构的软件安全辅助教材，是安全技术爱好者、调试人员、程序开发人员不可多得的一本好书。

作者简介

本书由看雪软件安全网站（看雪学院）站长段钢主持编著。
在本书的编写过程中，参与创作的每位作者倾力将各自擅长的专业技术毫无保留地奉献给广大读者，使得本书展现出了极具价值的丰富内容。
如果读者在阅读本书后，能够感受到管窥技术奥秘带来的内心的喜悦，并愿意与大家分享这份感受，这是作者最大的愿望。
主编：段钢编委：（按章节顺序排列）Blowfish，沈晓斌，丁益青，单海波，王勇，赵勇，唐植明，softworm，afanty，李江涛，林子深，印豪，冯典，罗翼，林小华，郭春杨Blowfish看雪首席版主。
经验丰富的大龄程序员。
1992年上大学始接触电脑，1997年读研期间接触网络并自学加密解密技术，一发不可收拾，其时常在教育网BBS灌水。
喜多方涉猎，亦能抓住一点深入钻研，对逆向分析技术尤为痴迷。
多年来常在看雪论坛灌水，见证了论坛的风风雨雨，也结识了一些不错的朋友。
参与章节：第5章 5.1 序列号保护方式第14章 14.5 软件保护的若干忠告沈晓斌看雪核心专家团队成员。
看雪论坛ID为cnbragon，现攻读密码学专业硕士学位。
最初的爱好是网络安全，进而研究软件的逆向工程，对密码学的兴趣由此而发。
对密码学的各个方面都有所涉猎，尤其擅长密码学在软件保护中的应用研究。
独立完成了一个加密算法库CryptoFBC。
译作有《程序员密码学》。
参与章节：第6章 加密算法丁益青看雪技术专家。
看雪论坛ID为cyclotron，复旦大学在读硕士研究生，复旦大学日月光华BBS黑客与系统安全版版主，致力于Windows环境下可执行文件的加密解密与逆向工程研究。
主要作品有EmbedPE、IDT Protector、PEunLOCK等。
参与章节：第8章 8.3 伪编译单海波看雪核心专家团队成员。
看雪论坛ID为tankaiha，生于六朝古都南京，硕士研究生毕业，现任某研究所工程师，工作之余好与计算机为伴。
2002年接触汇编并热衷于病毒技术学习，后偶遇看雪学院，遂终日游戏于程序加密与解密，不可自拔。
2006年与kanxue及坛中数位好友成立.net安全小组DST（Dotnet Reverse Team），共同探讨.net平台下的软件安全技术。
参与章节：第9章 .Net平台加解密王勇看雪技术专家。
毕业于石油大学（华东）计算机科学与技术专业。
擅长C/C++、ASM和驱动程序开发。
对面向对象程序设计和Windows系统底层的研究有丰富的经验。
很高兴这次能与各位高手一起合作，也希望能与编程爱好者及加密解密爱好者更多的交流。
参与章节：第10章 10.15 编写PE分析工具赵勇看雪技术专家。
来自江苏江阴，计算机业余爱好者，兴趣爱好广泛。
参与章节：第13章 13.6 附加数据唐植明看雪技术核心权威。
看雪论坛ID为DiKeN，2002年毕业于兰州大学，计算机科学与技术专业。
爱好逆向工程，iPB（inside Pandora's Box）组织创始人（在这儿更是要感谢组织的兄弟姐妹们，大家团结友好，互相学习，为iPB的成功作出了巨大努力），曾在2002年编写过《加密与解密实战攻略》算法部分。
参与章节：第13章 13.10 静态脱壳softworm看雪技术天才。
70后一代，非计算机专业的业余爱好者。
1998年开始接触逆向与破解，迄今已近10年，终于达到了“ 知道自己不知道 ”的境界。

感兴趣的方向包括壳、虚拟机保护、病毒引擎、Rootkit。
后两项还处于只知道名字的水平，愿与有共同爱好的朋友一起学习。
参与章节：第13章 13.9.2 Thmedia的SDK分析afanty看雪技术专家。
多年专业研究软件加解密技术。
参与章节：第14章 14.1 防范算法求逆李江涛看雪技术核心权威。
看雪论坛ID为ljtt，喜欢学习编程技术，常用编程语言为VC/MASM。
对PB、VFP的反编译有深入的研究，写过DePB、FoxSpy等程序。
平时大多数时间都在电脑上耕作，最大的希望是能够领悟到编程的精髓，写一个自己比较满意的作品。
参与章节：第14章 14.2.2 SMC技术实现林子深看雪技术导师。
看雪论坛ID为forgot，1989年生，看雪论坛外壳开发小组组长。
熟悉Win32平台和80x86汇编，擅长代码的逆向，对壳的研究比较多。
参与章节：第12章 12.4.1 虚拟机介绍第14章 14.2.4 简单的多态变形技术第15章 反跟踪技术印豪看雪资深技术权威。
看雪论坛ID为Hying，擅长加壳技术，拥有独立创作的加密利器。
参与章节：第16章 外壳编写基础冯典看雪技术天才。
看雪论坛ID为bughoho，1990年生，来自四川，看雪论坛虚拟机开发小组组长，目前工作主要是从事逆向研究。
个人自述：记得14岁时家里买了台电脑，使我对编程有了极大的兴趣。
16岁上高一时已对读书彻底不感兴趣，于是退学（现在的我才发现，我并不是对读书感兴趣，而是对教育制度的反感）。
后来听了家人的意见，转读四川新华电脑学校，感受颇多，一月之后便退学，至于为什么我就不说了。
17岁时，一个偶然的机会，使我对逆向有了浓厚的兴趣，并接触到看雪论坛，也认识到了kanxue。
承蒙kanxue抬举，让我执笔虚拟机这一章，由于我并不是一个才高八斗的人，所以写得也没有那么的妙笔生花、鬼斧神工了。
参与章节：第17章 虚拟机的设计

<<加密与解密>>

书籍目录

章节摘录

第1篇 基础篇第1章　基础知识研究加密与解密，必须要了解一些Windows系统的基础知识，这样在分析的过程中才能有的放矢地处理各种问题。
1.1　文本字符在学习过程中会与各类字符打交道，它们在Windows里扮演着重要角色。
1.1.1 字节存储顺序多字节数据是按怎样的顺序存放的呢？
实际情况和CPU有关，微处理机中的存放顺序有正序（BiG-Endian）和逆序（Little-Endian）之分。
常见的Intel体系芯片使用的编码方式属于Little—Endian类；某些RISC架构的CPU，如IBM的Power—PC等属于BiG—Endian类。
两种编码区别：·BiG—Endian 高位字节存入低地址，低位字节存入高地址，依次排列；·Little—Endian 低位字节存入低地址，高位字节存入高地址，反序排列。
例如，将12345678h写入到以1000h开始的内存中，则结果如图1.1所示。
本书以运行在Intel x86 CPU上的Windows为讲解平台，因此涉及的编码皆为Little.Endian类。
1.1.2　ASCIl与Unicode字符集美国信息交换标准码（ASCII）是一个7位的编码标准，包括26个小写字母、26个大写字母、10个数字、32个符号、33个控制代码和一个空格，总共128个代码。
由于计算机通常用“字节”（byte）这个8位的存储单位来进行信息交换，因此不同的计算机厂家对ASCIl进行了扩充，增加了128个附加的字符来补充ASCII。

编辑推荐

《加密与解密(第3版)》畅销书升级版，值得期待；看雪软件安全学院众多一流高手合力历时4年精心打造；全面揭示Windows平台的加密与解密技术。

软件安全是信息安全领域的重要内容，涉及到软件相关的加密、解密、逆向分析、漏洞分析、安全编程以及病毒分析等。

目前，国内高校对软件安全教育重视程度不够，许多方面还是空白。

随着互联网应用的普及和企业信息化程度的不断提升，社会和企业对软件安全技术人才需求逐年上升，在计算机病毒查杀、网游安全、网络安全、个人信息安全等方面人才缺口很大，相关职位待遇较高。

从就业角度来看，掌握软件安全相关知识和技能，不但可以提高自身的职场竞争能力，而且有机会发挥更大的个人潜力，获得满意的薪酬；从个人成长方面来说，研究软件安全技术有助于掌握许多系统底层知识，是提升职业技能的重要途径。

作为一名合格的程序员，除了掌握需求分析、设计模式等，如能掌握一些系统底层知识，熟悉整个系统的底层结构，对自己的工作必将获益良多。

揭示软件加密与解密最核心，看雪安全技术团队全力支持。

专家讲坛，全面探讨，软件安全问题与解决之道。

技术剖析，深入浅出，分析加密与解密技术核心。

共同进步，循序渐进。

迅速提升读者的专业水平。

《加密与解密(第3版)》技术支持：看雪软件安全网站提供《加密与解密(第3版)》的全面技术支持服务，阅读此书过程中，如有什么问题或学习心得，欢迎光临论坛与这些传说中的好手共同交流。

版权说明