

<<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

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：<http://www.tushu007.com>

<<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。

<<加密与解密>>

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。

<<加密与解密>>

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，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

前言	第1篇 基础篇	第1章 基础知识	1.1 文本字符	1.1.1 字节存储顺序	1.1.2 ASCII
	与Unicode字符集	1.2 WINDOWS 操作系统	1.2.1 Win API简介	1.2.2 常用Win32 API函数	
		1.2.3 什么是句柄	1.2.4 Windows 9x与Unicode	1.2.5 Windows NT/2000/XP与Unicode	
		1.2.6 Windows 消息机制	1.3 保护模式简介	1.3.1 虚拟内存	1.3.2 保护模式的权限级别
		1.4 认识PE格式	第2篇 调试篇	第2章 动态分析技术 33	2.1 OLLYDBG调试器
	OllyDbg界面	2.1.2 OllyDbg的配置	2.1.3 加载程序	2.1.4 基本操作	2.1.5 断点
		2.1.6 插件	2.1.7 Run trace	2.1.8 Hit trace	2.1.9 符号调试技术
					2.1.10 OllyDbg常见问题
		2.2 SOFTICE调试器	第3章 静态分析技术 31	3.1 文件类型分析	3.1.1 PEiD工具
		3.1.2 FileInfo工具	3.2 静态反汇编	3.2.1 打开文件	3.2.2 IDA的配置
					3.2.3 IDA主窗口界面
		3.2.6 交叉参考	3.2.7 参考重命名	3.2.8 标签的用法	3.2.9 进制的转换
		3.2.10 代码和数据转换	3.2.11 字符串	3.2.12 数组	3.2.13 结构体
		3.2.15 堆栈变量	3.2.16 IDC脚本	3.2.17 FLIRT	3.2.18 插件
		3.2.20 小结	3.3 可执行文件的修改	3.4 静态分析技术应用实例	3.4.1 解密初步
	逆向工程初步	第4章 逆向分析技术 35	4.1 启动函数	4.2 函数	4.2.1 函数的识别
	函数的参数	4.2.3 函数的返回值	4.3 数据结构	4.3.1 局部变量	4.3.2 全局变量
		4.3.3 数组	4.4 虚函数	4.5 控制语句	4.5.1 IF-THEN-ELSE语句
					4.5.2 SWITCH-CASE语句
		4.5.3 转移指令机器码的计算	4.5.4 条件设置指令	4.5.5 纯算法实现逻辑判断	
		4.6 循环语句	4.7 数学运算符	4.7.1 整数的加法和减法	4.7.2 整数的乘法
					4.7.3 整数的除法
		4.8 文本字符串	4.8.1 字符串存储格式	4.8.2 字符寻址指令	4.8.3 字母大小写转换
		4.8.4 计算字符串的长度	4.9 指令修改技巧	第3篇 解密篇	第5章 常见的演示版保护技术 34
		5.1 序列号保护方式	5.1.1 序列号保护机制	5.1.2 如何攻击序列号保护	
		5.1.3 字符串比较形式	5.1.4 注册机制作	5.2 警告 (NAG) 窗口	5.3 时间限制
					5.3.1 计时器
		5.3.2 时间限制	5.3.3 拆解时间限制保护	5.4 菜单功能限制	5.4.1 相关函数
		5.4.2 拆解菜单限制保护	5.5 KEYFILE保护	5.5.1 相关API函数	5.5.2 拆解KeyFile保护
		5.6 网络验证	5.6.1 相关函数	5.6.2 网络验证破解一般思路	5.7 CD-CHECK
		5.7.1 相关函数	5.7.2 拆解光盘保护	5.8 只运行一个实例	5.8.1 实现方案
		5.9 常用断点设置技巧	第6章 加密算法	6.1 单向散列算法	6.1.1 MD5算法
	SHA算法	6.1.3 小结	6.2 对称加密算法	6.2.1 RC4流密码	6.2.2 TEA算法
					6.2.3 IDEA算法
		6.2.4 BlowFish算法	6.2.5 AES算法	6.2.6 对称加密算法小结	6.3 公开密钥加密算法
		6.3.1 RSA算法	6.3.2 ElGamal公钥算法	6.3.3 DSA数字签名算法	6.3.4 椭圆曲线密码编码学
		6.4 其他算法	6.4.1 CRC32算法	6.4.2 Base64	6.5 常见加密库接口及其识别
		6.5.1 Miracl大数运算库	6.5.2 FGInt	6.5.4 其它加密算法库介绍	第4篇 语言和平台篇
		7.1 认识DELPHI	7.2 DEDE反编译器	7.3 按钮事件代码	7.4 模块初始化与结束化
		7.2 DEDE反编译器	8.1 基础知识	8.1.1 字符编码方式	8.1.2 编译模式
		8.2 自然编译 (NATIVE)	8.2.1 相关VB函数	8.2.2 VB程序比较方式	8.3 伪编译 (PCODE) (cyclotron编写)
			8.3.1 虚拟机与伪代码	8.3.2 动态分析VB P-code程序	
		8.3.3 伪代码的综合分析	8.3.4 VB P-code攻击实战	第9章 .NET平台加解密 (tankaiha 编写)	
		9.1 .NET概述	9.1.1 什么是.Net	9.1.2 几个基本概念	9.1.3 第一个.Net程序
					9.2 MSIL与元数据
		9.2.1 PE结构的扩展	9.2.2 .Net下的汇编MSIL	9.2.3 MSIL与元数据的结合	
		9.3 代码分析技术	9.3.1 静态分析	9.3.2 动态调试	9.3.3 代码修改
					9.4 代码保护技术及其逆向
		9.4.1 强名称	9.4.2 名称混淆	9.4.3 流程混淆	9.4.4 压缩
		9.4.5 加密	9.4.6 其它保护手段	9.5 深入.NET	9.5.1 反射与CodeDOM
		9.5.3 Rotor、MONO与.Net内核	第5篇 系统篇	第10章 PE文件格式 54	10.1 PE的基本概念
		10.1.1 基地址	10.1.2 相对虚拟地址	10.1.3 文件偏移地址	10.2 MS-DOS头部
		10.3 PE文件头	10.3.1 Signature字段	10.3.2 IMAGE_FILE_HEADER 结构	

<<加密与解密>>

10.3.3 Optional Header 10.4 区块 10.4.1 区块表 10.4.2 各种区块的描述 10.4.3 区块的对齐值 10.4.4 文件偏移与虚拟地址转换 10.5 输入表 10.5.1 输入函数的调用 10.5.2 输入表结构 10.5.3 输入地址表 10.5.4 输入表实例分析 10.6 绑定输入 10.7 输出表 10.7.1 输出表结构 10.7.2 输出表结构实例分析 10.8 基址重定位 10.8.1 基址重定位概念 10.8.2 基址重定位结构定义 10.8.3 基址重定位结构实例分析 10.9 资源 10.9.1 资源结构 10.9.2 资源结构实例分析 10.9.3 资源编辑工具 10.10 TLS初始化 10.11 调试目录 10.12 延迟装入数据 10.13 程序异常数据 10.14 .NET头部 10.15 PE分析工具编写 10.15.1 文件格式检查 10.15.2 FileHeader和OptionalHeader内容的读取 10.15.3 得到数据目录表信息 10.15.4 得到区块表信息 10.15.5 得到输出表信息 10.15.6 得到输入表信息

第11章 结构化异常处理 11 11.1 基本概念 11.1.1 异常列表 11.1.2 异常处理的基本过程 11.1.3 SEH的分类 11.2 SEH相关数据结构 11.2.1 TEB结构 11.2.2 EXCEPTION_REGISTRATION结构 11.2.3 EXCEPTION_POINTERS、EXCEPTION_RECORD、CONTEXT 11.3 异常处理回调函数第6篇 脱壳篇 第12章 专用加密软件 11 12.1 认识壳 12.1.1 壳的概念 12.1.2 压缩引擎 12.2 压缩壳 12.2.1 UPX 12.2.2 ASPack 12.3 加密壳 12.3.1 ASProtect 12.3.2 Armadillo 12.3.3 EXECryptor 12.3.4 Themida 12.4 虚拟机保护软件 12.4.1 虚拟机介绍 12.4.2 VMProtect简介 第13章 脱壳技术64 13.1 基础知识 13.1.1 壳的加载过程 13.1.2 脱壳机 13.1.3 手动脱壳 13.2 寻找OEP 13.2.1 根据跨段指令寻找OEP 13.2.2 用内存访问断点找OEP 13.2.3 根据堆栈平衡原理找OEP 13.2.4 根据编译语言特点找OEP 13.3 抓取内存映像 13.3.1 Dump原理 13.3.2 反DUMP技术 13.4 重建输入表 13.4.1 输入表重建的原理 13.4.2 确定IAT的地址和大小 13.4.3 根据IAT重建输入表 13.4.4 ImportREC重建输入表 13.4.5 输入表加密概括 13.5 DLL文件脱壳 13.5.1 寻找OEP 13.5.2 Dump映像文件 13.5.3 重建DLL的输入表 13.5.4 构造重定位表 13.6 附加数据 13.7 PE文件的优化 13.8 压缩壳 13.8.1 UPX外壳 13.8.2 ASPack外壳 13.9 静态脱壳 13.9.1 外壳Loader的分析 13.9.2 编写静态脱壳器 13.10 加密壳 13.10.1 ASProtect 13.10.2 Thmedia的SDK分析第7篇 保护篇 第14章 软件保护技术 26 14.1 防范算法求逆 14.1.1 基本概念 14.1.2 堡垒战术 14.1.3 游击战术 14.2 抵御静态分析 14.2.1 花指令 14.2.2 SMC技术实现 14.2.3 信息隐藏 14.2.4 简单多态变形技术 14.3 文件完整性检验 14.3.1 磁盘文件校验实现 14.3.2 校验和 (Checksum) 14.3.3 内存映像校验 14.4 代码与数据结合技术 14.4.1 准备工作 14.4.2 加密算法选用 14.4.3 手动加密代码 14.4.4 使.text区块可写 14.5 软件保护的若干忠告 第15章 反跟踪技术 (forgot编写) 52 15.1 由BEINGDEBUGGED引发的蝴蝶效应 15.1.1 BeingDebugged 15.1.2 NtGlobalFlag 15.1.3 Heap Magic 15.1.4 从源头消灭BeingDebugged 15.2 回归NATIVE:用户态的梦魇 15.2.1 CheckRemoteDebuggerPresent 15.2.2 ProcessDebugPort 15.2.3 ThreadHideFromDebugger 15.2.4 Debug Object 15.2.5 SystemKernelDebuggerInformation 15.2.6 Native API 15.2.7 Hook和AntiHook 15.3 真正的奥秘:小技巧一览 15.3.1 SoftICE检测方法 15.3.2 OllyDbg检测方法 15.3.3 调试器漏洞 15.3.4 防止调试器附加 15.3.5 父进程检测 15.3.6 时间差 15.3.7 通过Trap Flag检测 15.3.8 双进程保护 第16章 外壳编写基础 (Hying编写) 35 16.1 外壳的结构 16.2 加壳主程序 16.2.1 判断文件是否为PE格式 16.2.2 文件基本数据读入 16.2.3 附加数据读取 16.2.4 输入表处理 16.2.5 重定位表处理 16.2.6 文件的压缩 16.2.7 资源数据处理 16.2.8 区块的融合 16.3 外壳部分编写 16.3.1 外壳的加载过程 16.3.2 自建输入表 16.3.4 外壳引导段 16.3.5 外壳第二段 16.4 将外壳部分添加至原程序 第17章 虚拟机的设计 17.1 原理 17.1.1 反汇编引擎 17.1.2 指令分类 17.2 启动框架和调用约定 17.2.1 调度器VStartVM 17.2.2 虚拟环境:VMContext 17.2.3 平衡堆栈:VBegin和VCheckEsp 17.3 HANDLER的设计 17.3.1 辅助Handler 17.3.2 普通Handler和指令拆解 17.3.3 标志位问题 17.3.4 相同作用的指令 17.3.5 转移指令 17.3.6 转移跳转指令的另一种实现 17.3.7 CALL指令 17.3.8 retn指令 17.3.9 不可模拟指令 17.4 托管代码的异常处理

<<加密与解密>>

17.4.1 VC++的异常处理 17.4.2 Delphi的异常处理 17.5 小结第8篇 PEDIY篇 第18章 补丁技术
18.1 文件补丁 18.2 内存补丁 18.2.1 跨进程内存存取机制 18.2.2 Debug API机制
18.2.3 利用调试寄存器机制 18.2.4 DLL劫持技术 18.3 SMC补丁技术 18.3.1 单层SMC补丁技术
18.3.2 多层SMC补丁技术 18.4 补丁工具 第19章 代码的二次开发 19.1 数据对齐
19.2 增加空间 19.2.1 区块间隙 19.2.2 手工构造区块 19.2.3 工具辅助构造区块
19.3 获得函数的调用 19.3.1 增加输入函数 19.3.2 显式链接调用DLL 19.4 代码的重定位
19.4.1 修复重定位表 19.4.2 代码的自定位技术 19.5 增加输出函数 19.6 消息循环
19.6.1 WndProc函数 19.6.2 寻找消息循环 19.6.3 WndProc汇编形式 19.7 修改WNDPROC扩充功能
19.7.1 扩充WndProc 19.7.2 扩充Exit菜单功能 19.7.3 扩充Open菜单功能
19.8 增加接口 19.8.1 用DLL增加功能 19.8.2 扩展消息循环附录 附录A 浮点指令
附录B 在Visual C++中使用内联汇编术语表参考文献

<<加密与解密>>

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 ASCII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ASCII进行了扩充，增加了128个附加的字符来补充ASCII。

<<加密与解密>>

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。

<<加密与解密>>

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:<http://www.tushu007.com>