

<<揭秘数据解密的关键技术>>

图书基本信息

书名：<<揭秘数据解密的关键技术>>

13位ISBN编号：9787115196705

10位ISBN编号：7115196702

出版时间：2009-4

出版时间：人民邮电出版社

作者：刘颖东

页数：394

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>

## <<揭秘数据解密的关键技术>>

### 前言

**感谢** 本书献给国内所有热爱修改游戏，以及不求回报无私奉献自己的时间和精力奋战在游戏汉化第一线的朋友们，非常感谢出版社黄焱为本书所做的编辑工作，同时还要感谢我的同学张介淑和孙庚教授，多谢你们审校本书，指出书中的错误并提出宝贵的修改意见，没有你们的工作和帮助本书是不可能完成的。

**写作背景** 在国内，数据解密的普及程度明显相当不足，在高校里也不太重视这个领域的知识，甚至在市面上的技术书籍也未曾见过一本专门讨论数据解密的书籍，而最接近这个领域的书籍在国内有“看雪论坛”的《加密与解密》，但此书重点是研究代码的逆向分析而非数据的逆向分析。

数据解密在日常的应用非常广泛，包括游戏资源提取、游戏外挂和游戏脚本修改器这些软件的开发都与数据解密形影不离。

本书以研究和分析游戏中的资源文件数据结构作为学习数据解密的例子，通过学习这些例子读者能将此技术应用到其他软件领域。

技术是一把双刃剑，本书的写作目的并不是鼓励读者通过学习本书的内容后去搞破坏和谋取利益，本书的写作目的很简单，那就是尽笔者最大的努力和能力告诉读者数据解密是怎么一回事罢了。

本书包含了笔者早年学习数据解密技术的资料、经验和研究成果，读者可以将此书作为一本数据解密的入门书籍来学习。

本书并没有什么高深莫测的知识，研究和分析非公开数据结构只需读者具备耐性、时间和精力，如果读者已经具备了这三个条件，那么相信本书能很好地引导您入门。

## <<揭秘数据解密的关键技术>>

### 内容概要

《揭秘数据解密的关键技术》是一本以游戏资源文件格式为研究对象的数据逆向工程的技术书籍，主要讲解如何分析和研究自定义文件格式的数据结构。

《揭秘数据解密的关键技术》内容包含反汇编的阅读和理解，数据在计算机中的存储原理，常用媒体格式的解析，加密和解密的识别和分析，数据压缩的特征识别，打包文件格式的识别和游戏窗口化的方法。

《揭秘数据解密的关键技术》对每一个问题都给出了详细和完整的分析过程，力求用最通俗和简单的方法让读者学会分析和研究自定义文件格式。

《揭秘数据解密的关键技术》适合对数据解密、游戏资源提取、软件逆向工程感兴趣的读者以及广大编程爱好者阅读。

## <<揭秘数据解密的关键技术>>

### 作者简介

刘颖东：网名“小猫”，擅长逆向工程与游戏开发，从接触反汇编开始便一发不可收拾，对操作系统底层控制有强烈的征服欲望，现致力于研究嵌入式操作系统的开发。

## &lt;&lt;揭秘数据解密的关键技术&gt;&gt;

## 书籍目录

第1章 走进数据解密1.1 数据解密是什么1.1.1 代码逆向工程和数据逆向工程1.2 数据解密的方法1.2.1 黑盒分析法1.2.2 白盒分析法1.2.3 黑盒分析法与白盒分析法的比较1.3 万能的汇编语言1.3.1 为什么选择汇编语言1.3.2 16位和32位的80x86汇编语言1.4 通用寄存器1.4.1 EAX、EBX、ECX和EDX寄存器1.4.2 EAX、EBX、ECX和EDX寄存器的用途1.5 变址寄存器1.5.1 ESI和EDI寄存器1.5.2 ESI和EDI寄存器的用途1.6 指针寄存器1.6.1 EBP和ESP寄存器1.6.2 EBP和ESP寄存器的用途1.7 标志寄存器1.7.1 EFLAGS寄存器1.7.2 EFLAGS寄存器的用途1.8 灵活的寻址方式1.8.1 寻址方式的分类1.8.2 高级语言中的数据结构和80386寻址方式的关系1.9 80386指令1.9.1 Intel格式和AT&T格式的指令1.9.2 数据传送指令MOV、XCHG、PUSH、POP1.9.3 地址传送指令1.9.4 算数运算指令1.9.5 逻辑运算指令1.9.6 移位指令1.9.7 条件转移指令1.9.8 函数调用指令1.10 函数调用约定1.10.1 3种常用的调用约定1.10.2 调用约定的参数传递顺序1.11 字节码1.11.1 代码和数据的区别1.11.2 PE文件第2章 识别汇编代码的高级模式2.1 汇编中的常量、指针和变量——C语言中的常量、指针和变量2.1.1 常量、指针和变量的定义2.1.2 常量、指针和变量的实现机制2.2 汇编中的字符串——C语言中的字符串2.2.1 字符串的定义2.2.2 字符串的实现机制2.3 汇编中的数组——C语言中的数组2.3.1 数组的定义2.3.2 数组的实现机制2.3.3 二维数组的实现机制2.4 汇编中的结构体——C语言中的结构体2.4.1 结构体的定义2.4.2 结构体的实现机制2.5 汇编中的条件分支语句——C语言中的条件分支语句2.5.1 条件分支语句的定义2.5.2 if的实现机制2.5.3 包含复杂表达式的if语句的实现机制2.5.4 switch语句的实现机制2.6 汇编中的循环——C语言中的循环2.6.1 循环的定义2.6.2 while语句的实现机制2.6.3 do...while语句实现机制2.6.4 for语句的实现机制2.6.5 continue和break的实现机制2.7 汇编中的函数——C语言中的函数2.7.1 函数的定义2.7.2 按值传递的函数的实现机制2.7.3 按地址传递的函数的实现机制2.7.4 函数的返回值实现机制第3章 资源文件简介3.1 资源文件概述3.1.1 将游戏资源文件打包3.1.2 游戏的发动机——游戏引擎3.1.3 游戏的皮肤——图像3.1.4 游戏的声音——音频3.1.5 游戏的导演——脚本3.2 提取游戏资源的利器3.2.1 Susie33.2.2 MultiExCommander3.2.3 GameExtractor3.2.4 3DRipper3.2.5 RPGViewer3.2.6 GameViewer3.3 逆向数据结构的应用3.3.1 检测数据的安全性3.3.2 增加软件的兼容性3.3.3 挖掘未公开的技术3.3.4 游戏的修改3.3.5 网络协议的分析第4章 揭秘文件数据基础——0和4.1 文件数据存储原理4.1.1 位4.1.2 字节4.1.3 数据类型4.2 十六进制编辑器介绍4.2.1 Winhex功能介绍4.2.2 计算器4.2.3 位置管理器和书签4.2.4 文件同步比较4.2.5 数据解释器4.3 字符串4.3.1 字符串存储原理4.3.2 ASCII和UNICODE4.4 数值的表示方法4.4.1 十六进制表示方法4.4.2 有符号数和无符号数4.5 文件数据的存储顺序4.5.1 Little-Endian4.5.2 Big-Endian4.6 数据存储实验第5章 媒体数据格式解析5.1 BMP图像文件格式5.1.1 BMP图像文件介绍5.1.2 BMP图像文件存储结构5.1.3 分析BMP图像文件结构5.2 PNG图像文件格式5.2.1 PNG图像文件介绍5.2.2 PNG图像文件存储结构5.2.3 分析PNG图像文件结构5.3 3D模型文件介绍5.3.1 3D中的术语5.3.2 X文件介绍5.3.3 X文件存储结构5.3.4 分析静态X文件结构5.3.5 动画原理5.3.6 分析动态X文件结构5.4 md3模型文件格式5.4.1 md3模型文件介绍5.4.2 md3模型文件存储结构5.4.3 分析md3模型文件结构第6章 数据加密vs数据解密6.1 数据加密的基础6.1.1 AND运算6.1.2 OR运算6.1.3 XOR运算6.1.4 NOT运算6.1.5 SHL运算6.1.6 SHR运算6.1.7 位运算的应用6.2 游戏中常用的加密算法6.2.1 对称加密和非对称加密6.2.2 对称加密/解密和非对称加密/解密的区别6.2.3 XOR加密6.2.4 XOR加密解密分析实例6.2.5 MD5加密6.2.6 CRC加密6.2.7 BlowFish加密6.2.8 TEA加密6.3 自定义的加密/解密算法6.3.1 查找主程序中的字符串6.3.2 查找DLL的导出函数表6.3.3 使用内联汇编调用加密/解密函数6.3.4 调用DLL中的加密/解密函数6.4 实例：分析一个游戏的资源文件解密方式6.4.1 收集信息6.4.2 详细分析第7章 神奇的数据压缩算法7.1 RLE编码的识别7.1.1 RLE编码介绍7.1.2 如何识别RLE7.2 Zlib编码的识别7.2.1 Zlib编码介绍7.2.2 如何识别Zlib编码7.3 LZSS编码的识别7.3.1 LZSS编码介绍7.3.2 如何识别LZSS编码7.4 LZO编码的识别7.4.1 LZO和MiniLZO编码介绍7.4.2 如何识别LZO编码7.5 QuickLZ编码7.5.1 QuickLZ编码介绍7.5.2 如何识别QuickLZ7.6 破解未知的压缩编码7.6.1 如何识别数据被压缩了7.6.2 如何破解未知的压缩编码7.6.3 常见的压缩编码特征第8章 分析打包数据存储结构的模式8.1 常见的打包文件的数据结构存储模式8.1.1 目录结构8.1.2 分目录结构8.1.3 外部目录结构8.1.4 数据块结构8.1.5 分数据块结构8.1.6 树型结构8.2 验证常见的数据类型8.2.1 文件大小8.2.2 文件偏移量8.2.3 文件数量8.2.4 文件头标记8.2.5 文件名8.2.6 哈希散列值8.2.7 数据填充8.2.8 验证数据的准确性8.3 打包文件格式分析实例8.3.1 pak打包文件格

<<揭秘数据解密的关键技术>>

式分析8.3.2 GPP打包文件格式分析8.3.3 Pack打包文件格式分析8.3.4 CCK打包文件格式分析8.3.5 PCK打包文件格式分析第9章 将游戏窗口化9.1 2D游戏窗口化9.1.1 2D游戏窗口化理论9.1.2 2D游戏窗口化实例9.2 3D游戏窗口化9.2.1 3D游戏窗口化理论9.2.2 3D游戏窗口化实例

## <<揭秘数据解密的关键技术>>

### 章节摘录

#### 第1章 走进数据解密 1.2 数据解密的方法 1.2.3 黑盒分析法与白盒分析法的比较

通常如果使用黑盒分析法能获取文件的数据结构就不会使用白盒分析法，因为一般来说使用白盒分析法需要破解人员具备一定的汇编知识和经验，对于新手来说比较困难，但对于有经验的人员来说白盒分析法往往是解决问题的万能方法。

很多时候通过黑盒分析法无法得到有用的信息时，唯一的办法就是进行白盒分析了。

白盒分析也就是俗称的反汇编，一般不会对数据进行反汇编，因为对数据进行反汇编是没有意义的，反汇编针对的是使用文件数据的程序。

解密者通过分析、跟踪程序的反汇编代码，定位到程序读取或写入数据的代码段位置，通过分析反汇编代码研究文件的数据结构。

现在的程序大多数都使用了强悍的加密壳保护自己，直接反汇编加了壳的程序是没意义的，解密者通常需要自行将加了壳的程序脱壳并修复后才能正常反汇编分析程序，而脱壳这一环节无形中又增加了解密文件数据结构的难度。

如果为了锻炼自身的计算机技能水平，想要深入学习计算机编程，那么学习汇编、看懂反汇编是必经之路，如图1-2所示为使用白盒分析法在OilyICE中通过反汇编分析程序的指令。

<<揭秘数据解密的关键技术>>

编辑推荐

学数据解密，从《揭秘数据解密的关键技术》开始.....



<<揭秘数据解密的关键技术>>

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>