<<C++反汇编与逆向分析技术揭秘>>

图书基本信息

书名：<<C++反汇编与逆向分析技术揭秘>>

13位ISBN编号：9787111356332

10位ISBN编号：7111356330

出版时间：2011-10

出版时间：机械工业出版社华章公司

作者：钱林松,赵海旭

页数：411

<<C++反汇编与逆向分析技术揭秘>>

内容概要

《C++反汇编与逆向分析技术揭秘》本书既是一本全面而系统地讲解反汇编与逆向分析技术的安全类专著，又是一部深刻揭示C++内部工作机制的程序设计类著作。
理论与实践并重，理论部分系统地讲解了C++的各种语法特性和元素的逆向分析方法和流程，重在授人以渔；实践部分通过几个经典的案例演示了逆向分析技术的具体实施步骤和方法。

全书共分为三大部分：第一部分主要介绍了VC++6.0、OllyDBG和反汇编静态分析工具的使用，以及反汇编引擎的工作原理；第二部分以C/C++语法为导向，以VC++6.0为例，深入解析了每个C/C++知识点的汇编表现形式，包括基本数据类型、表达式、流程控制语句、函数、变量、数组、指针、结构体、类、构造函数、析构函数、虚函数、继承和多重继承、异常处理等，这部分内容重在修炼“内功”，不仅讲解了调试和识别各种C/C++语句的方法，而且还深入剖析了各知识点的底层机制；第三部分是逆向分析技术的实际应用，通过对PEiD、“熊猫烧香”病毒、OllyDBG调试器等的逆向分析将理论和实践很好地融合在了一起。

本书适合所有软件安全领域的工作者、想了解C++内部机制的中高级程序员，以及对Windows底层原理感兴趣的技术人员阅读。

作者简介

钱林松，资深安全技术专家、软件开发工程师和架构师，从事计算机安全和软件开发工作12年，实践经验极其丰富。
尤其精通软件逆向分析技术，对C/C++技术和Windows的底层机制也有非常深入的研究。
武汉科锐软件技术有限公司创始人，教学经验丰富，多年来，为国内计算机安全领域培养和输送了大量的人才。
活跃于看雪论坛，有较高的知名度和影响力。

<<C++反汇编与逆向分析技术揭秘>>

书籍目录

前言
第一部分　准备工作
第1章　熟悉工作环境和相关工具
1.1　调试工具Microsoft Visual C++ 6.0和OllyDBG
1.2　反汇编静态分析工具IDA
1.3　反汇编引擎的工作原理
1.4　本章小结
第二部分　C++反汇编揭秘
第2章　基本数据类型的表现形式
2.1　整数类型
2.2　浮点数类型
2.3　字符和字符串
2.4　布尔类型
2.5　地址、指针和引用
2.6　常量
2.7　本章小结
第3章　认识启动函数，找到用户入口
3.1　程序的真正入口
3.2　了解VC++ 6.0的启动函数
3.3　main函数的识别
3.4　本章小结
第4章　观察各种表达式的求值过程
4.1　算术运算和赋值
4.2　关系运算和逻辑运算
4.3　位运算
4.4　编译器使用的优化技巧
4.5　一次算法逆向之旅
4.6　本章小结
第5章　流程控制语句的识别
5.1　if语句
5.2　if…else…语句
5.3　用if构成的多分支流程
5.4　switch的真相
5.5　难以构成跳转表的switch
5.6　降低判定树的高度
5.7　dowhilefor的比较
5.8　编译器对循环结构的优化
5.9　本章小结
第6章　函数的工作原理
6.1　栈帧的形成和关闭
6.2　各种调用方式的考察
6.3　使用ebp或esp寻址
6.4　函数的参数
6.5　函数的返回值

6.6 回顾
6.7 本章小结
第7章 变量在内存中的位置和访问方式
7.1 全局变量和局部变量的区别
7.2 局部静态变量的工作方式
7.3 堆变量
7.4 本章小结
第8章 数组和指针的寻址
8.1 数组在函数内
8.2 数组作为参数
8.3 数组作为返回值
8.4 下标寻址和指针寻址
8.5 多维数组
8.6 存放指针类型数据的数组
8.7 指向数组的指针变量
8.8 函数指针
8.9 本章小结
第9章 结构体和类
9.1 对象的内存布局
9.2 this指针
9.3 静态数据成员
9.4 对象作为函数参数
9.5 对象作为返回值
9.6 本章小结
第10章 关于构造函数和析构函数
10.1 构造函数的出现时机
10.2 每个对象都有默认的构造函数吗
10.3 析构函数的出现时机
10.4 本章小结
第11章 关于虚函数
11.1 虚函数的机制
11.2 虚函数的识别
11.3 本章小结
第12章 从内存角度看继承和多重继承
12.1 识别类和类之间的关系
12.2 多重继承
12.3 虚基类
12.4 菱形继承
12.5 本章小结
第13章 异常处理
13.1 异常处理的相关知识
13.2 异常类型为基本数据类型的处理流程
13.3 异常类型为对象的处理流程
13.4 识别异常处理
13.5 本章小结
第三部分 逆向分析技术应用
第14章 PEiD的工作原理分析

14.1 开发环境的识别
14.2 开发环境的伪造
14.3 本章小结
第15章 “熊猫烧香”病毒逆向分析
15.1 调试环境配置
15.2 病毒程序初步分析
15.3 “熊猫烧香”的启动过程分析
15.4 “熊猫烧香”的自我保护分析
15.5 “熊猫烧香”的感染过程分析
15.6 本章小结
第16章 调试器OllyDBG的工作原理分析
16.1 INT3断点
16.2 内存断点
16.3 硬件断点
16.4 异常处理机制
16.5 加载调试程序
16.6 本章小结
第17章 反汇编代码的重建与编译
17.1 重建反汇编代码
17.2 编译重建后的反汇编代码
17.3 本章小结
参考文献

章节摘录

版权页：插图：下标寻址方式也可以被指针寻址方式所代替，但指针寻址方式需要两次间接访问才能访问到数组内的元素，第一次是访问指针变量，第二次才能访问到数组元素，故指针寻址的执行效率不会高于下标寻址，但是在使用的过程中更加方便。
数组下标和指针的寻址如此相似，如何在反汇编代码中区分它们呢？
只要抓住一点即可，那就是指针寻址需要两次以上间接访问才可以得到数据。
因此，在出现了两次间接访问的反汇编代码中，如果第一次间接访问得到的值作为地址，则必然存在指针。
图8.6就使用寄存器作为指针变量，保存全局数组的地址，从而利用保存了全局数组首地址的寄存器对该数组进行间接访问操作。
数组下标寻址的识别相对复杂，下标为常量时，由于数组的元素长度固定，siZeof（type）*n也为常量，产生了常量折叠，编译前可直接算出偏移量，因此只需使用数组首地址作为基址加偏移即可寻址相关数据，不会出现二次寻址现象。
当下标为变量或者变量表达式时，会明显体现出数组的寻址公式，且发生两次内存访问，但是和指针寻址明显不同，第一次访问的是下标，这个值一般不会作为地址使用，且代入公式计算后才得到地址。
值得注意的是，在打开优化选项02后，需留心各种优化方式。

媒体关注与评论

“ 工欲善其事，必先利其器 ”。
我经常对课题组的研究生说：“ 学习知识要把握事物本质（即夯实基础），基础牢固了，学习任何技术都能事半功倍，反之亦然。
”这是一本能为程序员（尤其是C++程序员）打牢基础的专业书籍，它将引导你一步一步去深入探究和分析程序的本质，从而逐渐让你在专业上感到踏实和自信，并在这个领域有豁然开朗的感觉。
本书非常适合那些想通过反汇编与逆向分析等技术手段探究C++应用底层奥秘的人，当然，你还要能耐得住寂寞！
——彭国军 武汉大学计算机学院副教授我与老钱相识已经相当长时间了，他给我的印象是为人简单、厚道、仗义。
他的书一如他的为人，用简单、精炼、易懂的语言诠释了程序世界里晦涩难懂的反汇编与逆向分析技术，是一本不可多得的好书。
——霄建云 中南民族大学计算机科学学院副院长随着互联网技术的不断发展，以及互联网应用的不断暴增和普及，计算机系统的安全保护在今天已经成为一个重要的课题。
有一群默默无闻的工作者，他们的职业是“ 病毒分析 ”，一个合格的病毒分析人员必须具备过硬的软件逆向技术。
本书是一本可以给病毒分析人员系统而全面的指导的专业书籍，对反汇编与逆向分析技术进行了深入且全面的讲解，对有志于从事软件安全相关工作的人来说，本书将对他们大有裨益，值得推荐。
——蠕辉 金山网络安全副总监一口气读完本书的初稿，细细回味，有几点突出的感受：第一，视角独特、内容丰富，是作者多年实践和教学经验的结晶；第二，深入浅出、重视基础，不适合走马观花式地阅读，而是要慢慢研读；第三，内容严谨、语言精炼，从中可以看出作者对逆向分析技术之精通和写作本书的良苦用心。
如果你想系统且深入地学习反汇编与逆向分析技术，本书是非常不错的选择，强烈推荐！
——单海波 安全技术专家／《微软，NET程序的加密与解密》一书的合著者软件逆向工程主要是通过研究和分析现有的软件产品来发现其规律，从而改进并超越现有产品的过程。
通过逆向工程技术，研究人员可以学习他人的编程技术和技巧，窥探商业软件的秘密，或开发与其兼容的软件。
同时，利用逆向工程技术可以对现有软件进行改造，可以在没有源代码的情况下修改目标程序的二进制代码，扩展程序的功能。
掌握一定的逆向技术，对程序员和安全工作者十分有好处。
但由于技术比较复杂，初学者往往不知从何入手，既不知道学习的方向，又缺少经验和有效的分析工具，大都事倍功半。
本书是学习逆向工程技术的一个很好的选择，它从软件逆向技术的基础开始讲解，逐步深入，在注重阐述逆向技术理论的同时，又结合生动的案例分析，深入浅出地向读者展示了软件逆向技术的精髓和实用技巧，能够帮助读者快速深入逆向工程技术的核心领域，获得宝贵的知识和经验。
诚然，要深入理解并熟练应用逆向工程技术，需要大家的勤奋与毅力，这个过程可能有时是枯燥的，但是当你的功力达到一定水平的时候，你会在软件分析的过程中产生一种直觉，看到目标的汇编代码，就能知道它们的作用和隐藏在其中的奥秘。
这时，你会发现逆向工程是一门优雅的数码艺术展现形式，它的精神是“ 自由 ”。
——段钢看雪软件安全网站创始人

编辑推荐

《C++反汇编与逆向分析技术揭秘》：深度揭秘软件逆向分析技术的流程与方法，理论与实践完美结合，由安全领域资深专家亲自执笔，看雪软件安全网站创始人段钢等多位安全领域专家联袂推荐。

版权说明