<<反编译技术与软件逆向分析>>

图书基本信息

书名：<<反编译技术与软件逆向分析>>

13位ISBN编号：9787118065466

10位ISBN编号：7118065463

出版时间：2009-11

出版时间：国防工业出版社

作者：赵荣彩，庞建民，张靖博　编著

页数：218

前言

随着计算机科学和相关技术的不断发展，尤其是各种编程语言的不断丰富与壮大，相关人员对贴近于硬件层的低级形式编码越来越陌生。
但是，事实表明计算机软件领域从来没有过，也不可能真正脱离对繁琐的低级代码进行分析的需求，而软件逆向分析技术在近年来重新成为计算机科学领域的研究热点。
在众多逆向分析技术中，反编译是对目标程序分析最为彻底，但也是最为困难的技术领域。
从名称上可以看出，反编译技术是编译技术的逆过程，即将低级目标可执行代码翻译为语义等价的高级语言表示形式。
本书希望能够为从事软件逆向分析的科研人员和工作者提供有效的帮助。
与其他相关的逆向分析书籍不同的是，编者没有局限于对二进制代码的反汇编分析，或者局限于对不同逆向分析辅助工具的使用指导，而是希望能够在反汇编层面分析的基础上对目标低级程序进行进一步挖掘，从而获取更多的有效信息。
毕竟现有的各种逆向分析工具的功能不一，不能完全满足业界复杂多变的需求。
“授人以鱼，不如授之以渔”，本书希望能够帮助读者深入了解并掌握一个完整反编译工具的各个部分，从而编写真正满足自己需求的逆向分析工具。
全书分为三大部分，共10章。
第一部分，包括第1章至第3章。
简要介绍了软件逆向分析技术的相关基础知识，为读者的进一步阅读奠定良好的基础。
包括软件逆向分析的背景知识、不同体系结构指令系统的相关背景，以及针对可执行文件格式的介绍。
在指令系统一章中介绍了两种完全不同的体系结构，即CISC体系结构和EPIC体系结构，并且着重针对Intel公司的64位安腾处理器的IA-64体系结构指令系统进行分析。
在可执行文件格式一章，则着重解析了在Linux操作系统中流行的ELF可执行文件格式。
第二部分，包括第4章、第5章。

<<反编译技术与软件逆向分析>>

内容概要

本书共分10章。
第1章到第3章简要介绍了软件逆向分析技术的相关基础知识；第4章和第5章从反汇编和中间表示两个方面为反编译奠定基础；第6章到第9章针对反编译的若干关键技术展开详细介绍；第10章则为反编译测试相关的一些可用资源。
全书以IA-64可执行代码为例进行讲解，但相关技术可以向其他平台推广。
本书可作为计算机软件专业本科高年级学生、硕士研究生的相关课程教科书或教学参考书，也可供从事软件逆向分析工作的工程技术人员参考。

<<反编译技术与软件逆向分析>>

书籍目录

章节摘录

插图：2. 逆向分析加密算法加密系统往往与隐私有关：一个人传递给另一个人的信息可能并不想让其他人知道。
可以粗略地将加密算法分为两组：有限加密算法和基于密钥的算法。
有限加密算法好比一些孩子们玩的游戏：写给一个朋友一封信，信中的每个字母都经过向上或向下的若干次移动。
有限加密算法的秘密在于算法本身，一旦算法被揭露，也就毫无秘密可言。
由于逆向分析可以分析出加密或解密算法，因此有限加密算法只能提供非常脆弱的安全性。
由于其算法也是保密的，因此逆向分析可以被看作是对算法的破解过程。
另一方面，基于密钥的算法的秘密是密钥，即一些类似于数字的值，它们可以由某些算法来对信息进行加密和解密。
在基于密钥的算法中，用户使用密钥对信息进行加密，并保证密钥的隐蔽性。
这种算法通常是公开的，而仅需要保护密钥即可。
由于算法是已知的，因此逆向分析变得毫无意义。
为了对一条经过基于密钥算法加密的信息进行解密，可能需要以下3种途径：①获取密钥；②尝试所有可能的组合；③寻找算法中的缺陷，从而解析出密钥或最初的信息。
尽管如此，对于基于密钥加密方法的逆向分析在某些方面却意义非凡。
即便加密算法广为人知，特定的实现细节也会对程序提供的所有安全级别造成意想不到的影响。
无论加密算法如何精巧，很小的实现错误也有可能使该算法提供的安全级别失效。
而确认一个安全产品是否真正地实现一个加密算法只有两种途径：要么分析它的源代码（假定是可行的），要么进行逆向分析。
3. 数字版权管理现代计算机系统已经将大多数类型的具有版权的材料转变为数字信息，包括音乐、影视，甚至书籍。
这些信息以前只能够通过具体的媒介获取，而现在可以通过数字化信息得到。
这种趋势为用户提供了巨大的好处，也为版权拥有者和内容提供商带来了一些问题。
对于用户来说，这意味着资料质量的提高，并且易于获取和管理。
对于提供商来说，这使得他们能够以很低的费用提供高质量的内容，但更为重要的是，这种方式使得对内容流向的控制无法完成。
数字化信息以难以想象的速度在流动，并且易于复制。
这种流动性意味着一旦带有版权的资料到达用户手中，用户能够很容易地对其进行移动和复制，因此盗版也变得相当容易。
通常软件公司通过在软件产品中嵌入复制保护技术防止被盗版，即通过在软件产品中嵌入代码片段来防止或限制用户对程序进行复制。

编辑推荐

《反编译技术与软件逆向分析》由国防工业出版社出版。

版权说明