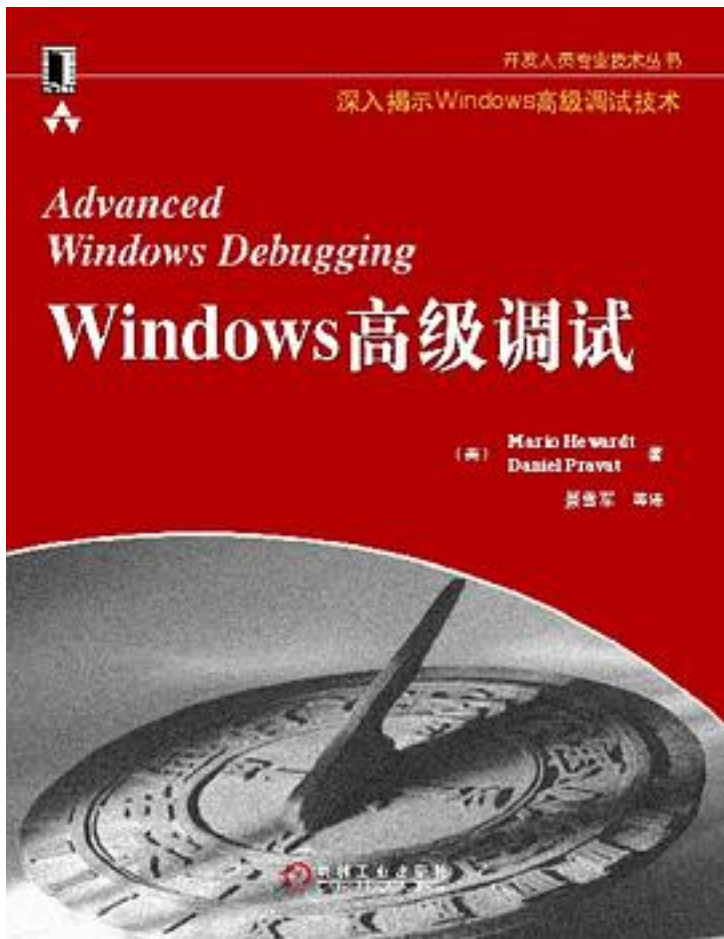


Windows高级调试



[Windows高级调试_下载链接1](#)

著者:Mario Hewardt

出版者:机械工业出版社

出版时间:2009-5

装帧:平装

isbn:9787111266396

本书主要讲解Windows高级调试思想和工具，并涉及一些高级调试主题。本书内容主要包括：工具简介、调试器简介、调试器揭密、符号文件与源文件的管理、栈内存破坏、堆内存破坏、安全、进程间通信、资源泄漏、同步、编写定制的调试扩展、64位调试、

事后调试、Windows

Vista基础以及应用程序验证器的测试设置等。本书内容详实、条理清楚。

本书适合Windows开发人员、Windows测试人员和Windows技术支持人员等参考。

作者介绍:

目录: 译者序

序言

前言

作者简介

第一部分 概述

第1章 调试工具简介 1

1.1 泄漏诊断工具 1

1.2 Windows调试工具集 3

1.3 UMDH 4

1.4 Microsoft 应用程序验证器 4

1.5 全局标志 9

1.6 进程浏览器 11

1.7 Windows驱动程序开发包 12

1.8 Wireshark 14

1.9 DebugDiag 15

1.10 小结 15

第2章 调试器简介 16

2.1 调试器的基础知识 16

2.1.1 调试器类型 17

2.1.2 调试器命令 18

2.1.3 调试器的配置 19

2.1.4 通过内核态调试器重定向用户态调试器 24

2.1.5 是否使用KD 26

2.2 基本的调试任务 26

2.2.1 键入调试命令 27

2.2.2 解析调试器的提示信息 27

2.2.3 配置和使用符号 29

2.2.4 使用源文件 38

2.2.5 分析命令 40

2.2.6 修改上下文的命令 60

2.2.7 其他的辅助命令 67

2.2.8 示例 68

2.3 远程调试 70

2.3.1 Remote.exe 70

2.3.2 调试服务器 71

2.3.3 进程服务器与内核服务器 73

2.3.4 远程调试中的符号解析 74

2.3.5 远程调试中的源代码解析 75

2.4 调试场景 75

2.4.1 调试非交互式进程（服务或者COM服务器） 76

2.4.2 在没有内核态调试器的情况下调试非交互式进程（服务或者COM服务器） 77

2.5 小结 77

第3章 调试器揭秘 78

3.1 用户态调试器的内幕 78

3.1.1 操作系统对用户态调试器的支持 78

3.1.2 调试事件的顺序 83

- 3.1.3 控制来自调试器的异常和事件 84
- 3.1.4 内核态调试器中的调试事件处理 105
- 3.2 控制调试目标 106
 - 3.2.1 断点的工作原理 107
 - 3.2.2 内存访问断点的工作原理 108
 - 3.2.3 处理器跟踪 109
 - 3.2.4 实时调试中的线程状态管理 109
 - 3.2.5 通过用户态调试器来挂起线程 112
- 3.3 小结 113
- 第4章 符号文件与源文件的管理 114
 - 4.1 调试符号的管理 114
 - 4.1.1 公有符号的生成 115
 - 4.1.2 在符号库中存储符号 117
 - 4.1.3 在HTTP服务器上共享公有符号 119
 - 4.2 源文件的管理 120
 - 4.2.1 收集源文件信息 120
 - 4.2.2 源文件信息的使用 122
 - 4.2.3 不带源文件修订控制的源文件服务器 123
 - 4.3 小结 125
- 第二部分 调试实践
- 第5章 内存破坏之一——栈 127
 - 5.1 内存破坏的检测过程 128
 - 5.1.1 步骤1：状态分析 128
 - 5.1.2 步骤2：源代码分析 129
 - 5.1.3 步骤3：使用内存破坏检测工具 133
 - 5.1.4 步骤4：调整源代码 133
 - 5.1.5 步骤5：定义回避策略 133
 - 5.2 栈内存破坏 133
 - 5.2.1 栈溢出 142
 - 5.2.2 异步操作与栈顶指针 147
 - 5.2.3 调用约定的不匹配 154
 - 5.2.4 回避策略 164
 - 5.3 小结 166
- 第6章 内存破坏之二——堆 167
 - 6.1 堆简介 167
 - 6.1.1 前端分配器 168
 - 6.1.2 后端分配器 169
 - 6.2 堆破坏 181
 - 6.2.1 使用未初始化状态 181
 - 6.2.2 堆的上溢与下溢 185
 - 6.2.3 堆句柄的不匹配 195
 - 6.2.4 重用已删除的堆块 199
 - 6.3 小结 205
- 第7章 安全 206
 - 7.1 Windows安全概述 206
 - 7.1.1 安全标识符 207
 - 7.1.2 访问控制列表 208
 - 7.1.3 安全描述符 209
 - 7.1.4 访问令牌 211
 - 7.2 安全信息的来源 213
 - 7.2.1 访问令牌 213
 - 7.2.2 安全描述符 215
 - 7.3 如何执行安全检查 217
 - 7.4 在客户端/服务器程序中传播标识 218

7.4.1 远程认证与安全支持提供者接口	218
7.4.2 模拟级别	220
7.5 系统边界上的安全检查	220
7.6 安全故障的分析	221
7.6.1 本地安全故障	221
7.6.2 延迟初始化中的安全问题	226
7.6.3 身份模拟的潜在安全问题	231
7.6.4 分布式COM错误	232
7.6.5 扩展命令!token的故障	241
7.6.6 在Windows XP SP2上安装了某个程序后发生DCOM激活故障	243
7.6.7 通过跟踪工具来分析安全故障	247
7.7 小结	248
第8章 进程间通信	249
8.1 通信机制	249
8.2 本地通信分析	250
8.2.1 LPC的背景知识	251
8.2.2 调试LPC通信	251
8.2.3 调试本地DCOM以及MSRPC通信	254
8.3 远程通信分析	260
8.3.1 RPC故障测定状态信息的使用..	260
8.3.2 网络流量分析	270
8.3.3 打破调用路径	275
8.4 一些其他的技术信息	277
8.4.1 远程认证	277
8.4.2 RPC扩展错误信息	278
8.4.3 其他工具	278
8.5 小结	279
第9章 资源泄漏	280
9.1 什么是资源泄漏	280
9.2 高层流程	280
9.2.1 步骤1: 找出潜在的资源泄漏	281
9.2.2 步骤2: 什么东西正在泄漏	282
9.2.3 步骤3: 初步分析	282
9.2.4 步骤4: 资源泄漏检测工具	282
9.2.5 步骤5: 制定回避策略	283
9.3 资源泄漏的可重现性	283
9.4 句柄泄漏	284
9.4.1 存在泄漏的程序	285
9.4.2 步骤1和步骤2: 它是不是一个句柄泄漏	286
9.4.3 步骤3: 初始分析	287
9.4.4 更复杂的程序	290
9.4.5 步骤4: 利用泄漏检测工具	292
9.4.6 句柄注入与!htrace	298
9.4.7 步骤5: 为句柄泄漏制定回避策略	300
9.5 内存泄漏	301
9.5.1 一个简单的内存泄漏	301
9.5.2 步骤1和步骤2: 是否存在泄漏, 以及泄漏的是什么资源	302
9.5.3 步骤3: 使用内存检测工具	303
9.5.4 步骤4: 回避策略	322
9.6 小结	322
第10章 同步	323
10.1 同步的基础知识	323
10.1.1 事件	323
10.1.2 临界区	325

- 10.1.3 互斥体 329
- 10.1.4 信号量 330
- 10.2 高层流程 331
 - 10.2.1 步骤1：识别问题的征兆 331
 - 10.2.2 步骤2：转储所有线程 331
 - 10.2.3 步骤3：分析线程中的同步问题 332
 - 10.2.4 步骤4：修复问题 334
 - 10.2.5 步骤5：制定回避策略 334
- 10.3 同步情况 334
 - 10.3.1 死锁 334
 - 10.3.2 第1种孤立临界区情况—异常 338
 - 10.3.3 第2种孤立临界区情况—线程结束 343
 - 10.3.4 DllMain函数的注意事项 347
 - 10.3.5 锁竞争 353
 - 10.3.6 管理临界区 358
- 10.4 小结 361
- 第三部分 高级主题
- 第11章 编写定制的调试扩展 363
 - 11.1 调试扩展简介 363
 - 11.2 调试扩展示例 365
 - 11.2.1 调试扩展模型 369
 - 11.2.2 调试扩展示例的需求 371
 - 11.2.3 头文件和代码组织 372
 - 11.2.4 调试扩展的初始化 374
 - 11.2.5 调试会话状态的变化 379
 - 11.2.6 KnownStructOutput 379
 - 11.2.7 退出调试扩展 379
 - 11.2.8 Help命令的实现 380
 - 11.2.9 dumptree命令的实现 381
 - 11.2.10 KnownStructOutput函数的实现 384
 - 11.2.11 取消命令的实现 387
 - 11.2.12 版本 389
 - 11.2.13 调试扩展的构建 389
 - 11.3 小结 390
- 第12章 64位调试 391
 - 12.1 Microsoft 64位系统 391
 - 12.1.1 操作系统简介 392
 - 12.1.2 在WOW64中运行的32位程序 393
 - 12.2 Windows x64带来的变化 395
 - 12.2.1 第1章—调试工具简介 396
 - 12.2.2 第2章—调试器简介 397
 - 12.2.3 第3章—调试器揭密 407
 - 12.2.4 第5章—内存破坏之一—栈 411
 - 12.2.5 第6章—内存破坏之二—堆 411
 - 12.2.6 第7章—安全 412
 - 12.2.7 第8章—进程间通信 413
 - 12.2.8 第11章—编写定制的调试扩展 414
 - 12.3 小结 414
- 第13章 事后调试 415
 - 13.1 转储文件基础 415
 - 13.1.1 通过调试器来生成转储文件 417
 - 13.1.2 通过ADPlus来生成转储文件 420
 - 13.1.3 内核态转储文件的创建 421
 - 13.2 转储文件的使用 423

13.2.1 转储文件的分析：访问违例	424
13.2.2 转储文件的分析：句柄泄漏	425
13.3 Windows错误报告	429
13.3.1 Dr.Watson	429
13.3.2 Windows错误报告的系统架构	434
13.4 企业错误报告	446
13.4.1 设置企业错误报告	447
13.4.2 通过企业错误报告来报告错误	449
13.5 小结	451
第14章 功能强大的工具	452
14.1 调试诊断工具	452
14.1.1 分析内存泄漏或者句柄泄漏	453
14.1.2 编写定制的分析脚本	455
14.2 扩展命令!analyze	457
14.2.1 故障程序	457
14.2.2 分析结果	458
14.2.3 故障的跟进人员	462
14.3 小结	463
第15章 Windows Vista基础	464
15.1 第1章—调试工具简介	464
15.2 第2章—调试器简介	465
15.2.1 用户访问控制的副作用	465
15.2.2 启用内核态调试器	467
15.2.3 地址空间布局的随机化	468
15.3 第6章—内存破坏之二—堆	469
15.4 第7章—安全性	473
15.4.1 用户访问控制	474
15.4.2 调试器中的UAC	475
15.4.3 注册表和文件虚拟化	479
15.5 第8章—进程间通信	481
15.6 第9章—资源泄漏	482
15.7 第10章—同步	482
15.7.1 轻量读写锁	482
15.7.2 条件变量	483
15.7.3 单次初始化	484
15.7.4 增强线程池	484
15.8 第11章—编写定制的调试扩展	484
15.9 第13章—事后调试	485
15.10 小结	487
附录A 应用程序验证器的测试设置	488
• • • • •	(收起)

[Windows高级调试 下载链接1](#)

标签

调试

windows

debug

Windows编程

计算机

编程

程序调试

programming

评论

微软员工写的。有一些深度。没看完。如果要学习windows底层感觉这样的书应该要搞定。

关于调试的书不多，这是本经典。系统而深入。

还是lin好用。

太...不知道定位在哪

算看过一些，很不错的书，以后可能不干这行了

今天看完，这前对windows相关基本不太了解，看了不但了解了调试相关的内容，工具。对windows很多东西有一种一通百通的感觉

前几日聊天到调试，朋友说有书推荐。朋友不知我已转linux。今天还特地从家里带来给我。看了一下，第6章 内存破坏一栈 相关的内容很好很强大。其中有些笔误，翻译的人居然没有将笔误修正过来。

比较深入的windbg调试书籍，难度较高，可作为身边常用工具书。

Windbg 自学 恶补 自虐必备工具书，对Windows堆的介绍很精彩

和软件调试一起看，相辅相成

[Windows高级调试_下载链接1](#)

书评

记得几年前我们对一款核心产品进行升级，测试人员发现了一个会导致整个程序崩溃的BUG。这个BUG在程序的运行过程中随机出现，很难重现。更为棘手的是，当开发人员用VC以调试模式运行该程序，BUG就再也不重现了。根据以往的经验，这种情况多和多线程处理导致缓冲区非法操作有...

软件测试大师Boris Beizer
博士曾经说过：“测试的目的是显示存在错误，而调试的目的是发现错误或导致程序失效的错误原因，并修改程序以修正错误。调试是测试之后的活动。”可见软件的测试与调试是分不开的是相辅相成的。作为一名程序员总是希望自己的程序更高...

“我编写了WinDbg符号处理器、符号服务器以及源文件服务器。即便如此，我仍然无法教会我妻子使用WinDbg。她认为这个工具非常难用，因此并不了解这个工具的强大

之处。我买了这本书送给她，这样她就可以知道如何使用WinDbg。本书中关于事后调试（Postmortem Debugging）和内存破...

[illegible]

The First In-Depth, Real-World, Insider's Guide to Powerful Windows Debugging For Windows developers, few tasks are more challenging than debugging—or more crucial. Reliable and realistic information about Windows debugging has always been scarce. Now, w...

不过可以作为科普读物来阅读。如果想要提高自己的调试能力，应该拿windbg的帮助手册，并多进行实践，此书能提供的帮助实在不大。

[Windows高级调试_下载链接1_](#)