

# 《独辟蹊径的编程思维——“拿来主义”编程》

## 图书基本信息

书名：《独辟蹊径的编程思维——“拿来主义”编程》

13位ISBN编号：9787121223990

10位ISBN编号：7121223996

出版时间：2014-3

出版社：电子工业出版社

作者：李瑞民

页数：496

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《独辟蹊径的编程思维——“拿来主义”》

## 内容概要

与传统编程习惯于每一细节都亲历亲为所不同的是，如果在程序设计之初就综合考虑并合法应用第三方既有成果，就可在项目开发的时间、成本及质量这三个关键矛盾体“三要素”上进行统筹设计，这种技术就是“拿来主义”的编程技术。《独辟蹊径的编程思维——“拿来主义”编程》分别通过静态分析、功能调用、输出接收、界面嵌入、中间嗅探、控制交互等方法详细介绍了多达14种拿来技术。全书集编程思想、技术、实践为一体，融会贯通，灵活运用，势必大有裨益。

《独辟蹊径的编程思维——“拿来主义”编程》适用于对网络黑客攻防程序开发、反向工程及程序原理分析感兴趣的人员，也适用于监控类和测试类程序开发人员，还可作为高校编程实验用书。另外，本书所涉及的各项技术，除了原理阐述和技术分析之外，均附有完整的程序源代码，这些源代码可免费从网上下载，所以也适用于各类编程爱好者学习、验证和修改。

# 《独辟蹊径的编程思维——“拿来主”》

## 作者简介

李瑞民，男，工学博士，高级工程师，资深网络安全专家兼高级系统架构师。多年来一直专注于网络设备监控与信号监控、计算机安全技术等领域的研究与应用，对计算机监控、设备监控、网络攻防、物联网等领域有深刻的认识。目前拥有发明专利、软件著作权8项，出版和翻译的书籍有《网络扫描技术揭秘》、《设备监控技术》、《Hacking Exposed Wireless》等，发表专业核心论文数十篇。

## 书籍目录

第1章绪论.....	1
1.1 “拿来主义”编程技术简介.....	1
1.1.1 什么是“拿来主义”.....	1
1.1.2 为什么要采用“拿来主义”.....	2
1.2 常用的“拿来主义”编程技术.....	3
1.3 “拿来主义”编程技术的分类.....	5
1.3.1 静态分析型的拿来技术.....	5
1.3.2 功能型的拿来技术.....	6
1.3.3 输出型的拿来技术.....	7
1.3.4 嵌入型的拿来技术.....	8
1.3.5 中间嗅探型的拿来技术.....	8
1.3.6 控制交互型的拿来技术.....	9
第1部分静态分析型的拿来技术	
第2章操作系统数据的拿来.....	12
2.1 本章的预备知识.....	12
2.1.1 进制的表示与转换.....	12
2.1.2 DOS下的地址表示.....	14
2.1.3 Debug工具的使用.....	15
2.2 裸机时代的可用数据.....	19
2.2.1 裸机的启动过程.....	19
2.2.2 CMOS内存中的数据.....	20
2.2.3 中断与中断向量.....	25
2.2.4 BIOS数据区.....	28
2.2.5 ROM中的数据.....	36
2.3 DOS中的全局变量.....	42
2.3.1 曾经辉煌的DOS.....	43
2.3.2 DOS的内存映射.....	44
2.3.3 DOS数据区.....	46
2.3.4 DOS的“拿来”实例.....	47
2.4 Windows中的共享数据.....	49
2.4.1 如日中天的Windows.....	49
2.4.2 Windows中的环境变量.....	50
2.4.3	
Windows环境变量的意义.....	52
2.4.4	
Windows环境变量的编程.....	53
2.4.5	
修改Windows的全局环境变量...56	
2.5 编程实例：基于WinIO的CMOS数据读写.....	56
2.5.1	
程序主界面.....	57
2.5.2 程序代码.....	57
第3章系统共享文件中的拿来.....	61
3.1 操作系统配置文件的拿来.....	61
3.1.1	
对配置文件的读/写.....	62
3.1.2 Boot.ini.....	65

3.2 目录名称的拿来.....	66
3.2.1	
与用户名相同的目录名.....	67
3.2.2	
所安装的软件列表.....	68
3.2.3	
与用户相关的特定目录名.....	68
3.3 数据库访问式的共享.....	69
3.3.1	
ODBC数据访问方式.....	69
3.3.2	
ADO数据连接.....	82
3.4 注册表的共享.....	86
3.4.1	
基于注册表访问的 API.....	86
3.4.2	
注册表项的操作.....	92
3.5 文件级的拿来.....	93
3.5.1	
网络配置文件.....	93
3.5.2	
日志文件.....	97
3.5.3	
Windows目录自带的音频文件资源.....	103
3.6 编程实例 1：通过 ODBC对 txt文件进行读/写.....	108
3.6.1	
程序主界面.....	109
3.6.2	
程序代码.....	109
3.7 编程实例 2：通过 ADO对 Excel文件进行读/写.....	112
3.7.1	
程序主界面.....	112
3.7.2 程序代码.....	113
第 4章静态程序文件中资源的拿来.....	115
4.1 常见可执行文件的格式.....	115
4.1.1	
DOS下的 COM和 EXE文件的格式简介.....	115
4.1.2	
Windows下 PE文件的格式.....	118
4.2 VC软件编程人员眼中的程序资源.....	119
4.3 在可执行文件中调整资源.....	121
4.3.1	
从可执行文件中提取资源.....	121
4.3.2	
更换可执行文件中的资源.....	122
4.4 软件汉化与界面调整.....	122
4.4.1	
软件汉化.....	123
4.4.2 软件界面调整.....	125

4.5 界面复制.....	126
4.5.1 将可执行文件中的界面复制到工程中.....	126
4.5.2 对两个工程之间界面的复制.....	128
第 2 部分功能型的拿来技术	
第 5 章无界面程序命令行中的拿来.....	132
5.1 什么是命令行.....	132
5.1.1 常用的 DOS 内部命令.....	134
5.1.2 常用的 DOS 外部命令.....	138
5.2 命令行的组合使用.....	149
5.2.1 设备文件.....	149
5.2.2 重定向技术.....	151
5.2.3 管道技术.....	155
5.3 命令行的编程技术.....	156
5.3.1 可嵌入 DOS 命令行的几个函数.....	156
5.3.2 管道编程的几个函数.....	161
5.4 编程实例 1：使用重定向接收外部程序运行结果.....	162
5.4.1 程序主界面.....	162
5.4.2 程序代码.....	163
5.5 编程实例 2：使用管道接收外部程序运行结果.....	164
5.5.1 程序主界面.....	164
5.5.2 程序代码.....	165
第 6 章有界面程序消息式的拿来.....	167
6.1 消息机制.....	167
6.1.1 消息的定义.....	168
6.1.2 消息的队列和非队列模式.....	169
6.1.3 与消息有关的几个函数.....	170
6.2 Visual C++ 自带的消息处理工具.....	175
6.2.1 程序界面上的控件.....	175
6.2.2 Visual C++ 下提供的标准控件.....	176
6.2.3 消息查询工具 Spy++.....	177
6.3 通过消息控制程序.....	182
6.3.1 与窗口有关的几个函数.....	182
6.3.2 与消息控制有关的几个函数.....	186
6.4 编程实例：通过消息控制程序.....	191
6.4.1 程序主界面.....	191
6.4.2 程序代码.....	192
第 3 部分输出接收型的拿来技术	
第 7 章读取 B/S 界面上输出的数据.....	200
7.1 Web 服务器的安装和测试.....	201
7.1.1 Web 服务器的安装和验证.....	201
7.1.2 检验 Web 服务器的效果.....	205
7.2 基于 Web 应用的编程接口.....	207
7.2.1 CInternetSession 类.....	208
7.2.2 CInternetConnection 类.....	216
7.2.3 CHttpConnection 类.....	217
7.2.4 CFtpConnection 类.....	218
7.2.5 CInternetFile 类.....	222
7.2.6 CInternetException 类.....	224
7.3 编程实例：基于 Web 的拿来方式.....	225

7.3.1 原理分析.....	226
7.3.2 程序主界面.....	228
7.3.3 程序代码.....	228
第 8 章对 Office 文件输出的接收操作.....	231
8.1 Microsoft Office 简介.....	232
8.2 输出式的拿来简介.....	233
8.2.1 COM/DCOM 的概念.....	234
8.2.2 AfxOleInitt 函数.....	234
8.2.3 COleVariant 类.....	235
8.2.4 COleDispatchDriver 类.....	240
8.3 程序员眼中的 Office.....	241
8.3.1 Office 的结构框架.....	242
8.3.2 Office 组件的导入.....	242
8.4 Word 的结构输出.....	244
8.4.1 Word 简介.....	244
8.4.2 Word 中的要素.....	244
8.5 Excel 的结构输出.....	245
8.5.1 Excel 简介.....	246
8.5.2 Excel 中的要素.....	246
8.6 PowerPoint 的结构输出.....	247
8.6.1 PowerPoint 简介.....	248
8.6.2 PowerPoint 中的要素.....	248
8.7 输出式的拿来技术在信息安全领域内的应用.....	249
8.7.1 数字水印简介.....	249
8.7.2 Word 中格式输出类的数字水印.....	250
8.7.3 Word 中内容格式的数字水印.....	251
8.8 编程实例 1：读取 Word 文件中的纯文本内容.....	252
8.8.1 程序主界面.....	252
8.8.2 程序代码.....	253
8.9 编程实例 2：读写 Excel 中的数据.....	254
8.9.1 程序主界面.....	255
8.9.2 程序代码.....	255
8.10 编程实例 3：控制 PPT 的输出.....	258
8.10.1 程序主界面.....	258
8.10.2 程序代码.....	259
第 4 部分嵌入型的拿来技术	
第 9 章控件嵌入式的拿来.....	264
9.1 ActiveX 技术简介.....	264
9.2 在 Windows 程序中嵌入 ActiveX 控件.....	266
9.2.1 设置对 ActiveX 控件的支持.....	266
9.2.2 从系统注册的组件中导入要使用的 ActiveX 控件.....	267
9.2.3 从 DLL 文件中导入要使用的 ActiveX 控件.....	268
9.3 编程实例 1：嵌入式视频播放器.....	268
9.3.1 播放器编程的简介.....	268
9.3.2 VLC 简介.....	269
9.3.3 程序主界面.....	274
9.3.4 程序代码.....	274
9.4 编程实例 2：嵌入式 PDF 阅读器.....	276
9.4.1 在 VC 对 PDF 的可视化使用.....	276

9.4.2 程序主界面.....	277
9.4.3 程序代码.....	278
第 10 章界面嵌入式的拿来.....	280
10.1 屏幕式的嵌入.....	280
10.1.1 图形桌面.....	281
10.1.2 实现界面嵌入式要考虑的问题.....	283
10.1.3 实现像素级操作主要涉及的 API.....	286
10.1.4 实现桌面级操作主要涉及的 API.....	288
10.1.5 屏幕的截取.....	293
10.2 内容式的嵌入.....	297
10.2.1 通过 IE 调用访问网络地址.....	297
10.2.2 通过嵌入页面方式访问网络地址.....	297
10.2.3 通过资源管理器方式访问本地文件系统.....	298
10.2.4 CHtmlView 的 API.....	299
10.3 编程实例 1：将程序界面自己程序的一部分进行嵌入.....	301
10.3.1 程序主界面.....	302
10.3.2 程序代码.....	303
10.4 编程实例 2：嵌入整个 Web 页面和资源管理器.....	306
10.4.1 程序主界面.....	307
10.4.2 程序代码.....	307
第 5 部分中间嗅探型的拿来技术	
第 11 章程序调用时的数据过滤.....	310
11.1 DLL 文件的意义和用法.....	310
11.1.1 DLL 文件的意义.....	311
11.1.2 与 DLL 调用相关的函数.....	312
11.1.3 DLL 文件的调用步骤.....	315
11.2 从 EXE 或 DLL 文件中找到函数.....	316
11.2.1 Depends 的使用方式.....	316
11.2.2 从 ICMP.DLL 中抽取函数.....	317
11.2.3 ICMP.DLL 中各函数的用法.....	318
11.3 重载 DLL 文件.....	321
11.3.1 DLL 文件重载的原理.....	321
11.3.2 DLL 文件重载的意义.....	322
11.4 具有重载特性的 DLL 文件创建步骤.....	322
11.4.1 普通 DLL 文件的创建步骤.....	323
11.4.2 重载 DLL 文件的创建步骤.....	324
11.5 编程实例 1：通过 ICMP.DLL 制作 tracert 命令.....	325
11.5.1 程序主界面.....	326
11.5.2 程序代码.....	327
11.6 编程实例 2：重载 ICMP.DLL 以记录 ICMP 协议操作.....	330
11.6.1 程序主界面.....	330
11.6.2 程序代码.....	331
第 12 章网络通信时的数据监听.....	335
12.1 网络通信简介.....	336
12.1.1 网络嗅探技术.....	336
12.1.2 网络协议分析和行为分析.....	336
12.1.3 黑客级别的分析.....	339
12.2 数据流的截获.....	344
12.2.1 单机数据流的获取.....	344



12.2.2 网络数据流的获取.....	346
12.3 Socket编程接口.....	348
12.3.1 几个重要的概念.....	349
12.3.2 Windows Socket结构.....	350
12.3.3 Windows socket转换类函数....	353
12.3.4 Windows socket通信类函数返回值.....	357
12.3.5 Windows socket通信类函数.....	359
12.4 编程实例：RAW Socket嗅探器.....	368
12.4.1 程序主界面.....	368
12.4.2 程序代码.....	369
第 13章串口通信时的数据监控.....	377
13.1 串口的通信与监听.....	377
13.1.1 串口简介.....	377
13.1.2 串口通信中的“拿来”技术.....	379
13.2 基于 VSPE的串口开发技术.....	380
13.2.1 VSPE简介.....	381
13.2.2 VSPE的术语.....	381
13.2.3 VSPE的串口嗅探功能.....	386
13.2.4 VSPE的使用与开发.....	388
13.2.5 VSPE的 API.....	388
13.3 编程实例：串口嗅探器.....	392
13.3.1 程序主界面.....	393
13.3.2 程序代码.....	394
第 6部分控制交互型的拿来技术第	
14章从运行的程序中拿来.....	402
14.1 Windows内存模式.....	402
14.1.1 Windows的对内存读写的限制.....	403
14.1.2 Windows的内存管理.....	404
14.1.3 调试程序简介.....	407
14.2 基于 WinIO的内存读取编程.....	408
14.2.1 WinIO的 API.....	408
14.2.2 WinIO的编程.....	412
14.3 基于 API的程序调试函数.....	412
14.3.1 Windows调试程序的结构.....	413
14.3.2 Windows调试程序的 API.....	422
14.3.3 Windows的进程 API.....	428
14.3.4 Windows的动态内存 API.....	429
14.3.5 Windows调试程序的编写方式.....	433
14.4 编程实例：读正在执行程序的数据.....	434
14.4.1 程序主界面.....	435
14.4.2 程序代码.....	435
第 15章 Hook控制式的拿来.....	440
15.1 Hook简介.....	440
15.1.1 什么是 Hook.....	441
15.1.2 Hook的运行机制.....	442
15.1.3 怎么使用 Hook.....	443
15.2 Hook函数.....	443
15.2.1 SetWindowsHookEx函数.....	444
15.2.2 UnhookWindowsHookEx函数.....	446

15.2.3 CallNextHookEx函数.....	446
15.2.4 回调函数.....	447
15.3 Hook 的类型.....	447
15.3.1 WH_CALLWNDPROC.....	447
15.3.2 WH_CBT.....	448
15.3.3 WM_QUEUESYNC.....	452
15.3.4 WH_DEBUG .....	452
15.3.5 WH_FOREGROUNDIDLE.....	453
15.3.6 WH_GETMESSAGE .....	453
15.3.7 WH_HARDWARE.....	453
15.3.8 WH_JOURNALRECORD.....	453
15.3.9 WH_JOURNALPLAYBACK.....	454
15.3.10 WH_KEYBOARD .....	455
15.3.11 WH_MOUSE .....	455
15.3.12 WH_MSGFILTER.....	455
15.3.13 WH_SHELL.....	456
15.3.14 WH_SYSMSGFILTER.....	456
15.4 编程实例1：线程Hook 程序编写.....	456
15.4.1 程序主界面.....	456
15.4.2 程序代码.....	457
15.5 编程实例2：全局Hook 程序编写.....	459
15.5.1 程序主界面.....	459
15.5.2 DLL 程序代码.....	460
15.5.3 调用程序代码.....	462
附录A 本书容易混淆概念解析.....	464
A.1 同名不同义概念.....	464
A.2 同义不同名概念.....	464
A.3 易混概念.....	466
附录B 详解ASCII 码.....	468
附录C HTTP 错误返回码.....	474
参考文献.....	479
后记.....	481

## 《独辟蹊径的编程思维——“拿来主”》

### 精彩短评

- 1、全书集编程思想、技术、实践为一体，融会贯通，灵活运用，势必大有裨益。
- 2、买国人写的书一定要注意两点：1.看其他人评价 2.去书店翻一翻。这本是新书，没有评价。我又懒得跑书店只看了目录和试读部分，然后就呵呵了。。。

## 《独辟蹊径的编程思维——“拿来主”》

### 精彩书评

1、以往通常都是借用sf.net上的源码，那上面linux下代码和库文件比较多，win下的比较少。这本书介绍了一些直接借用win下闭源dll之类的方法，对于win环境下的程序员有着一定借鉴意义。可以当作手册来用，不会的时候再来翻翻。只要笼统过一遍，心里有个印象即可，没必要通篇细读。

## 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：[www.tushu000.com](http://www.tushu000.com)