

目 录

第 1 章 如何分析 macOS 软件	1	3.1.1 开发环境	51
1.1 分析环境搭建	1	3.1.2 Objective-C 语言特性	54
1.1.1 安装 Clang	1	3.1.3 内存管理	60
1.1.2 HT Editor	2	3.2 Swift 语言	65
1.1.3 Homebrew	6	3.2.1 Playground	65
1.2 第一个 macOS 程序	8	3.2.2 Swift 语法简介	67
1.3 使用 HT Editor 进行破解	10	3.3 其他语言	88
1.4 本章小结	14	3.4 框架	88
第 2 章 系统安全架构	15	3.4.1 框架的开发与使用	88
2.1 系统架构概述	15	3.4.2 在 Objective-C 中使用 Swift 编 写的框架	93
2.1.1 shell 环境	16	3.4.3 常用的框架	94
2.1.2 目录结构	16	3.5 第三方开发工具	94
2.1.3 文件权限	17	3.5.1 Qt Creator	94
2.2 系统调用	17	3.5.2 Xamarin Studio	95
2.3 进程间通信	18	3.5.3 JetBrains 系列开发工具	96
2.4 安全框架	19	3.5.4 Visual Studio Code	97
2.4.1 CommonCrypto	19	3.6 完整的 Cocoa GUI 程序	97
2.4.2 Keychain	20	3.6.1 创建工程	98
2.4.3 安全传输	25	3.6.2 Storyboard 和 xib	98
2.5 系统安全机制	28	3.6.3 Outlet 和 Action 机制	101
2.5.1 FileVault 2	29	3.7 本章小结	103
2.5.2 代码签名	31	第 4 章 软件内幕	104
2.5.3 ASLR / kASLR	33	4.1 可执行文件	105
2.5.4 沙盒	37	4.2 下载与安装软件	106
2.5.5 Rootless	39	4.2.1 免费与付费软件	106
2.5.6 Gatekeeper	42	4.2.2 安装软件	106
2.6 软件安全开发建议	50	4.3 Bundle	107
2.7 本章小结	50	4.3.1 Bundle 目录结构	107
第 3 章 软件开发基础	51	4.3.2 在代码中访问 Bundle	109
3.1 Objective-C 语言	51		

2 目 录

4.4	通用二进制格式	109	5.5.1	与 C 语言互相调用	197
4.5	Mach-O 文件格式	112	5.5.2	使用系统调用	200
4.5.1	Mach-O 简介	112	5.6	本章小结	201
4.5.2	Mach-O 头部	113	第 6 章	软件静态分析	202
4.5.3	加载命令	116	6.1	代码分析与二进制分析	202
4.5.4	LC_CODE_SIGNATURE	117	6.2	分析工具	203
4.5.5	LC_SEGMENT	129	6.2.1	Radare2	203
4.6	动态库	131	6.2.2	IDA Pro	207
4.6.1	构建动态库	132	6.2.3	Hopper	209
4.6.2	dyld	135	6.3	代码分析技术	211
4.6.3	动态库的加载	136	6.3.1	行为分析	211
4.7	静态库	151	6.3.2	资源分析	212
4.7.1	构建静态库	152	6.3.3	数据分析	215
4.7.2	静态库格式	154	6.3.4	流量分析	216
4.7.3	管理静态库	156	6.3.5	API 分析	218
4.8	框架	156	6.4	反汇编工具的使用	219
4.8.1	构建框架	157	6.4.1	反汇编	219
4.8.2	框架的使用与安装	158	6.4.2	流程图	224
4.9	pkg	160	6.4.3	伪代码	225
4.9.1	构建 pkg	160	6.5	破解 Mach-O 程序	227
4.9.2	pkg 的安装与卸载	167	6.5.1	定位修改点	227
4.9.3	pkg 文件格式	170	6.5.2	修改程序	228
4.9.4	破解 pkg	173	6.5.3	代码签名处理	230
4.10	dmg	177	6.5.4	重新打包	234
4.10.1	构建 dmg	177	6.5.5	Keygen	234
4.10.2	管理 dmg	179	6.6	本章小结	235
4.11	本章小结	181	第 7 章	软件动态调试与跟踪	236
第 5 章	汇编基础	182	7.1	DTrace	236
5.1	搭建汇编语言开发环境	182	7.1.1	DTrace 简介	236
5.2	Hello World 代码概览	185	7.1.2	DTrace 示例	236
5.3	伪指令	186	7.2	D 脚本语言	237
5.4	x86_64 汇编基础	189	7.2.1	脚本加载方式	237
5.4.1	寄存器	190	7.2.2	D 语言与 C 语言	238
5.4.2	汇编语法	192	7.2.3	D 语言语法	238
5.4.3	数据传送指令	195	7.2.4	变量	241
5.4.4	控制转移指令	195	7.2.5	参数传递	243
5.4.5	栈操作指令	196	7.2.6	聚合	243
5.4.6	运算指令	197	7.2.7	内置函数与变量	244
5.5	与其他模块的交互	197			

7.3 调试器.....246	9.4.1 DYLD_INSERT_LIBRARIES.....352
7.3.1 GDB.....246	9.4.2 SymbolTable Hook.....355
7.3.2 LLDB.....248	9.4.3 Inline Hook.....358
7.3.3 IDA Pro.....258	9.4.4 Method Swizzling.....359
7.3.4 Hopper.....267	9.5 代码注入.....362
7.4 本章小结.....269	9.5.1 静态注入.....362
第 8 章 调试器开发.....270	9.5.2 动态注入.....365
8.1 概述.....270	9.5.3 Hook 与注入框架.....366
8.2 开发环境搭建.....270	9.6 补丁&注册机.....373
8.2.1 安装所需环境.....271	9.7 本章小结.....375
8.2.2 编译 Saber.....280	第 10 章 反破解技术.....376
8.3 系统调试接口.....285	10.1 反破解技术类型.....376
8.3.1 ptrace 简介.....286	10.2 校验保护.....377
8.3.2 Mach 调试接口.....287	10.2.1 完整性检查.....377
8.4 macOS 异常机制.....292	10.2.2 代码签名验证.....377
8.4.1 异常与 Mach RPC/IPC.....292	10.2.3 沙盒检测.....382
8.4.2 信号.....300	10.2.4 来源检测.....386
8.5 调试器功能实现.....302	10.3 代码保护.....386
8.5.1 调试器架构.....302	10.3.1 代码混淆.....386
8.5.2 开始调试.....303	10.3.2 SMC.....387
8.5.3 异常处理循环.....305	10.3.3 代码校验.....387
8.5.4 读写被调试进程内存.....308	10.3.4 壳保护.....387
8.5.5 获取基地址与入口点.....309	10.4 数据保护.....391
8.5.6 单步调试.....310	10.4.1 数据清除.....391
8.5.7 断点.....311	10.4.2 数据存储.....395
8.5.8 继续运行.....312	10.4.3 数据传输.....400
8.5.9 反汇编.....313	10.5 调试器对抗.....408
8.6 本章小结.....316	10.5.1 调试器检测.....408
第 9 章 破解技术.....317	10.5.2 反调试.....410
9.1 软件破解步骤.....317	10.6 Hook 检测.....411
9.2 常见的保护类型.....318	10.6.1 Method Swizzling 检测.....411
9.2.1 试用版&序列号.....319	10.6.2 dyld Hook 检测.....412
9.2.2 License 授权.....319	10.7 本章小结.....413
9.2.3 重启验证与暗桩.....330	第 11 章 游戏安全.....414
9.2.4 防拷贝技术.....338	11.1 游戏类型.....414
9.2.5 网络验证.....338	11.2 游戏框架与引擎.....414
9.2.6 混合验证.....342	11.2.1 SpriteKit 与 SceneKit.....415
9.3 App Store 内购机制.....342	11.2.2 GameplayKit & ReplayKit.....417
9.4 Hook 技术.....351	11.2.3 Cocos2d-x.....417

4 目 录

11.2.4	Unity3D	419	12.3.1	Launch Items	439
11.3	游戏分析工具	422	12.3.2	Login Items	441
11.3.1	静态分析工具	423	12.3.3	StartupItems	442
11.3.2	动态调试工具	424	12.3.4	Login/Logout Hooks	444
11.3.3	资源修改工具	424	12.3.5	Cron Jobs	444
11.3.4	内存修改工具	427	12.3.6	Periodic Scripts	446
11.4	游戏分析方法	427	12.3.7	Authorization Plugins	446
11.4.1	对比分析	427	12.3.8	Browser Extensions	447
11.4.2	动态调试	429	12.3.9	Spotlight Importers	448
11.4.3	静态补丁	429	12.3.10	QuickLook Plugins	448
11.4.4	动态补丁	430	12.3.11	Kernel Extensions	448
11.5	防破解技术	430	12.4	Rootkit	449
11.6	本章小结	431	12.4.1	文件隐藏	449
第 12 章	恶意软件与 Rootkit	432	12.4.2	进程隐藏	451
12.1	安全趋势	432	12.4.3	内核模块隐藏	452
12.1.1	知名恶意软件	432	12.4.4	Root 提权	453
12.1.2	安全漏洞	433	12.5	本章小结	454
12.1.3	安全软件	435	附录	macOS 工具一览表	455
12.2	文件关联技术	435	参考资料	460
12.3	软件自启动技术	439			