

# 编译与反编译技术实战



[编译与反编译技术实战 下载链接1](#)

著者:

出版者:机械工业出版社

出版时间:

装帧:平装

isbn:9787111566175

全书共14章，第1章简要介绍了本书所基于的环境与工具；第2~6章针对编译的不同阶段，展开实践方面的相关阐述，并结合GCC和LLVM这两款具体的编译器进行论述；第7章介绍了多样化编译方面的实践；第8~13章从反编译的不同阶段介绍与反编译相关的可执行程序格式、程序解码和反汇编、中间表示生成、数据类型和控制流的恢复、过程定义恢复等内容；第14章简要介绍了反编译在信息安全方面的应用。

作者介绍:

目录: 前言	
第1章 实践的环境与工具	1
1.1 实践环境概述	1
1.2 词法分析生成器LEX	1
1.3 语法分析生成器YACC	3
1.4 编译器GCC	4
1.5 编译器LLVM	5
1.6 反汇编工具IDA	6
1.7 反汇编工具OllyICE	6
1.8 仿真与分析工具QEMU	6
1.9 动态分析工具TEMU	7
1.10 本章小结	8
第2章 编译器实践概述	9
2.1 编译器、解释器及其工作方式	9
2.2 编译器的结构	10
2.3 编译器的设计与实现概述	12
2.3.1 利用Flex和Bison实现词法和语法分析	12
2.3.2 利用LLVM实现代码优化和代码生成	12
2.4 本章小结	13
第3章 词法分析器的设计与实现	14
3.1 词法分析器的设计	14
3.1.1 词法分析器的功能	14
3.1.2 输入及其处理	15
3.2 词法分析器的手工实现	16
3.3 词法分析器的LEX实现	31
3.3.1 LEX源文件结构	32
3.3.2 LEX系统中的正规式	34
3.3.3 LEX的使用方式	36
3.3.4 LEX源文件示例——C语言词法分析器	37
3.4 本章小结	41
第4章 语法分析器的设计与实现	42
4.1 自上而下的语法分析器的设计与实现	42
4.2 自下而上的语法分析器的设计与实现	61
4.3 语法分析器的生成器	72
4.3.1 YACC的源文件结构	72
4.3.2 YACC和LEX的接口	76
4.3.3 YACC源程序示例——简单的台式计算器	77
4.4 本章小结	78
第5章 GCC编译器分析与实践	79
5.1 GCC编译器概述	79
5.2 GCC编译器的系统结构	80
5.3 GCC编译器的分析程序	81
5.4 GCC编译器的中间语言及其生成	82
5.5 GCC编译器的优化	82
5.6 GCC编译器的目标代码生成	87
5.7 本章小结	88
第6章 LLVM编译器分析与实践	89
6.1 LLVM编译器概述	89
6.1.1 起源	89
6.1.2 相关项目	90
6.2 经典编译器概述	91
6.2.1 经典编译器设计的启示	91
6.2.2 现有编译器的实现	92

6.3 LLVM的设计	93
6.3.1 LLVM中间表示	94
6.3.2 LLVM库文件	95
6.4 LLVM前端	96
6.4.1 前端库文件	97
6.4.2 词法分析	97
6.4.3 语法分析	99
6.4.4 语义分析	100
6.4.5 LLVM IR代码生成	100
6.5 LLVM的中间表示	100
6.5.1 LLVM IR语法	102
6.5.2 LLVM IR优化实例	104
6.6 LLVM后端	106
6.6.1 后端库文件	107
6.6.2 LLVM目标架构描述文件	108
6.7 应用实例	109
6.7.1 代码插桩	110
6.7.2 代码保护	110
6.8 本章小结	111
第7章 多样化编译实践	112
7.1 软件多样化的机会	112
7.1.1 应用层的多样化机会	112
7.1.2 Web服务层的多样化机会	113
7.1.3 操作系统层的多样化机会	115
7.1.4 组合后的多样化机会	116
7.1.5 虚拟层的多样化机会	116
7.2 多样化带来的管理复杂性	117
7.3 多样化编译技术	118
7.3.1 随机化技术	118
7.3.2 代码混淆技术	120
7.3.3 与堆栈相关的多样化技术	123
7.4 多样化编译的应用	125
7.4.1 多样化编译在安全防御方面的应用	126
7.4.2 多样化编译工具的结构组成及原理	127
7.5 本章小结	128
第8章 反编译的对象——可执行文件格式分析	129
8.1 可执行文件格式	129
8.1.1 PE可执行文件格式	129
8.1.2 ELF可执行文件格式	130
8.2 main函数的识别	133
8.2.1 程序启动过程分析	136
8.2.2 startup函数解析	137
8.2.3 main()函数定位	140
8.3 本章小结	142
第9章 反编译的基础——指令系统和反汇编	143
9.1 指令系统概述	143
9.1.1 机器指令及格式	145
9.1.2 汇编指令及描述	147
9.2 指令解码	149
9.2.1 SLED通用编解码语言	149
9.2.2 x64的SLED描述	154
9.2.3 IA64的SLED描述	159
9.3 反汇编过程	161
9.3.1 线性扫描反汇编	161

- 9.3.2 行进递归反汇编 162
- 9.4 反汇编工具IDA与OllyICE实践 163
  - 9.4.1 IDA实践 163
  - 9.4.2 OllyICE实践 166
- 9.5 本章小结 169
- 第10章 反编译的中点——从汇编指令到中间表示 170
  - 10.1 中间代码生成在经典反编译器中的实际应用 170
    - 10.1.1 低级中间代码 171
    - 10.1.2 高级中间代码 172
  - 10.2 中间表示从设计到应用的具体实例 175
    - 10.2.1 指令基本组件描述 176
    - 10.2.2 用UMSDL描述指令语义 179
  - 10.3 本章小结 184
- 第11章 反编译的推进1——数据类型恢复 185
  - 11.1 基本数据类型的分析和恢复 185
    - 11.1.1 数据类型分析的相关概念 186
    - 11.1.2 基于指令语义的基本数据类型分析 188
    - 11.1.3 基于过程的数据类型分析技术 190
  - 11.2 函数类型恢复 197
    - 11.2.1 问题引入 198
    - 11.2.2 函数类型的恢复 198
  - 11.3 本章小结 203
- 第12章 反编译的推进2——控制流恢复实例 205
  - 12.1 基于关键语义子树的间接跳转目标解析 205
    - 12.1.1 问题的提出 206
    - 12.1.2 相关工作 207
    - 12.1.3 跳转表的语义特征 208
    - 12.1.4 基于关键语义子树的间接跳转目标解析及翻译 210
  - 12.2 功能块概念的引入 222
    - 12.2.1 分析单位 222
    - 12.2.2 基于基本块的分析 223
    - 12.2.3 功能块 228
    - 12.2.4 针对功能块的验证 230
  - 12.3 基于功能块的间接转移指令目标地址的确定 233
    - 12.3.1 程序控制流图构建方法中存在的问题 233
    - 12.3.2 无法处理的代码 234
    - 12.3.3 程序执行路径的逆向构造 235
    - 12.3.4 逆向构造执行路径的控制执行 245
    - 12.3.5 针对程序执行路径逆向构造的验证 246
  - 12.4 本章小结 248
- 第13章 反编译的推进3——过程定义恢复 250
  - 13.1 过程分析概述 250
    - 13.1.1 过程抽象 250
    - 13.1.2 调用约定分析 251
  - 13.2 库函数恢复 255
    - 13.2.1 快速库函数调用识别方法 255
    - 13.2.2 基于特征数据库的模式匹配方法 256
    - 13.2.3 基于函数签名的库函数识别方法 257
    - 13.2.4 库函数参数的恢复 262
    - 13.2.5 隐式库函数调用 267
  - 13.3 用户自定义过程的数据恢复 279
    - 13.3.1 基于语义映射的数据恢复 280
    - 13.3.2 基于栈帧平衡的数据恢复 282
  - 13.4 用户函数与库函数同名的区分 283

- 13.4.1 函数同名问题 283
- 13.4.2 函数同名解决实例 286
- 13.5 本章小结 290
- 第14章 反编译在信息安全方面的应用实践 291
- 14.1 反编译在信息安全中的应用 291
- 14.1.1 反编译技术的优势 292
- 14.1.2 代码恶意性判定 292
- 14.1.3 代码敏感行为标注 293
- 14.1.4 恶意代码威胁性评估 293
- 14.2 反编译在恶意代码分析中的应用 294
- 14.2.1 基于文件结构的恶意代码分析 294
- 14.2.2 基于汇编指令的恶意代码分析 295
- 14.2.3 基于流图的恶意代码分析 296
- 14.2.4 基于系统调用的恶意代码分析 298
- 14.3 恶意代码与反编译技术的对抗 300
- 14.3.1 混淆 300
- 14.3.2 多态 304
- 14.3.3 变形 306
- 14.3.4 加壳 307
- 14.3.5 虚拟执行 308
- 14.4 反编译框架针对恶意行为的改进 309
- 14.4.1 条件跳转混淆 309
- 14.4.2 指令重叠混淆 314
- 14.4.3 子程序异常返回 319
- 14.4.4 不透明谓词混淆 324
- 14.5 实例分析 330
- 14.5.1 系统设计 330
- 14.5.2 系统模块划分 331
- 14.5.3 测试结果与分析 351
- 14.6 本章小结 355
- 参考文献 356
- • • • • [\(收起\)](#)

[编译与反编译技术实战\\_下载链接1](#)

标签

逆向

计算机

信息安全

编译器

编译原理

编译

技术

反编译

评论

信息量很大的一本书，读一半了，受益不少 2018/06/21 从11章开始就晕了 2018/06/22

-----  
[编译与反编译技术实战 下载链接1](#)

书评

-----  
[编译与反编译技术实战 下载链接1](#)