

Blue Fox

взлом и реверс-
инжиниринг ARM

Мария Маркстедтер



Санкт-Петербург • Москва • Минск

2025

Краткое содержание

ЧАСТЬ I. ВНУТРЕННЕЕ УСТРОЙСТВО АРХИТЕКТУРЫ ARM

Глава 1. Введение в реверс-инжиниринг.....	18
Глава 2. Внутреннее устройство файлов ELF.....	35
Глава 3. Основы операционных систем.....	81
Глава 4. Архитектура Arm.....	106
Глава 5. Инструкции обработки данных.....	143
Глава 6. Инструкции доступа к памяти.....	207
Глава 7. Условное выполнение.....	256
Глава 8. Поток команд.....	288

ЧАСТЬ II. РЕВЕРС-ИНЖИНИРИНГ

Глава 9. Среды разработки Arm.....	318
Глава 10. Статический анализ.....	331
Глава 11. Динамический анализ.....	373
Глава 12. Реверс-инжиниринг вредоносных программ для macOS arm64.....	412
Указатель.....	444

Оглавление

Об авторе.....	12
Введение.....	13
Благодарности.....	15
От издательства.....	16
О научных редакторах русского издания.....	16

ЧАСТЬ I. ВНУТРЕННЕЕ УСТРОЙСТВО АРХИТЕКТУРЫ ARM

Глава 1. Введение в реверс-инжиниринг.....	18
Введение в ассемблер.....	18
Биты и байты.....	18
Кодировка символов.....	20
Машинный код и ассемблер.....	21
Написание кода ассемблера.....	24
Языки высокого уровня.....	29
Дизассемблирование.....	30
Декомпиляция.....	32
Глава 2. Внутреннее устройство файлов ELF.....	35
Структура программы.....	35
Высокоуровневые и низкоуровневые языки.....	36
Процесс компиляции.....	38
Кросс-компиляция для других архитектур.....	39
Ассемблирование и компоновка.....	41
Обзор файла ELF.....	44
Заголовки файла ELF.....	45
Информационные поля заголовка файла ELF.....	46
Поля целевой платформы.....	46
Поле точки входа.....	47
Поля расположения таблиц.....	48
Заголовки программ ELF.....	48
PHDR.....	49
INTERP.....	49
LOAD.....	50
DYNAMIC.....	51

NOTE.....	51
TLS.....	51
GNU_EH_FRAME.....	52
GNU_STACK.....	52
GNU_RELRO.....	54
Заголовки секций ELF.....	56
Метасекции ELF.....	58
Основные секции ELF.....	59
Символы.....	61
Динамическая секция и динамическая загрузка.....	64
Загрузка зависимостей (NEEDED).....	65
Перемещение программ.....	66
Разделы инициализации и завершения программы ELF.....	70
Локальное потоковое хранилище.....	72
Модель доступа к TLS local-exec.....	76
Модель доступа к TLS initial-exec.....	77
Модель доступа к TLS general-dynamic.....	78
Модель доступа к TLS local-dynamic.....	79
Глава 3. Основы операционных систем.....	81
Обзор архитектуры ОС.....	81
Пользовательский режим и режим ядра.....	81
Процессы.....	82
Системные вызовы.....	84
Потоки.....	91
Управление памятью процесса.....	93
Страницы памяти.....	94
Защитные средства памяти.....	95
Рандомизация размещения адресного пространства.....	99
Реализации стека.....	102
Совместно используемая память.....	104
Глава 4. Архитектура Arm.....	106
Архитектуры и профили.....	106
Архитектура Armv8-A.....	108
Уровни исключений.....	108
Состояния выполнения Armv8-A.....	114
Состояние выполнения AArch64.....	116
Набор инструкций A64.....	116
Регистры AArch64.....	117
Регистры SIMD и регистры с плавающей точкой.....	123
PSTATE.....	125

Состояние выполнения AArch32	127
Наборы инструкций A32 и T32	127
Регистры AArch32	132
Регистр текущего состояния программы	135
Регистры состояния выполнения	138
Глава 5. Инструкции обработки данных	143
Операции сдвига и циклического сдвига	145
Логический сдвиг влево	146
Логический сдвиг вправо	146
Арифметический сдвиг вправо	147
Циклический сдвиг вправо	148
Циклический сдвиг вправо с расширением	148
Формы инструкций	149
Операции манипулирования битовым полем	154
Логические операции	166
Побитовый оператор И	167
Побитовый оператор ИЛИ	169
Побитовый оператор ИЛИ НЕ	170
Побитовое исключающее ИЛИ	171
Инструкция TEQ	172
Исключающая операция ИЛИ НЕ	172
Арифметические операции	172
Сложение и вычитание	173
Операция сравнения	175
Операции умножения	178
Умножение в наборе A64	179
Умножение в A32/T32	181
Операции деления	200
Операции перемещения	201
Перемещение непосредственной константы	201
Перемещение регистра	205
Перемещение с отрицанием	206
Глава 6. Инструкции доступа к памяти	207
Обзор инструкций	207
Режимы адресации и формы смещения	209
Адресация со смещением	212
Режим предварительной индексации	222
Постиндексная адресация	225
Литеральная (относительно PC) адресация	227

Инструкции загрузки и сохранения	235
Загрузка и сохранение слова или двойного слова.....	235
Загрузка и сохранение полуслова или байта	237
Множественная загрузка и сохранение (A32).....	242
Парная загрузка и сохранение (A64).....	251
Глава 7. Условное выполнение	256
Обзор условного выполнения.....	256
Коды условий.....	257
Флаги условий NZCV	257
Коды условий.....	261
Условные инструкции	262
Инструкция If-Then (IT) в Thumb.....	263
Инструкции установки флагов.....	265
Суффикс S в инструкции.....	266
Инструкции для проверки и сравнения.....	271
Инструкции условного выбора	279
Инструкции условного сравнения	281
Условия с булевым И с помощью CCMP	282
Условия с булевым ИЛИ с помощью CCMP	285
Глава 8. Поток команд	288
Инструкции перехода	288
Условные переходы и циклы.....	289
Проверка и сравнение переходов	294
Табличные переходы (T32).....	295
Переход и замена.....	296
Переходы подпрограмм	301
Функции и подпрограммы.....	303
Стандарт вызова процедур	303
Временные и неизменяемые регистры	305
Аргументы и возвращаемые значения.....	306
Передача больших значений.....	308
Терминальные и нетерминальные функции.....	310
ЧАСТЬ II. РЕВЕРС-ИНЖИНИРИНГ	
Глава 9. Среды разработки Arm.....	318
Платы Arm	319
Эмуляция с помощью QEMU	321
Эмуляция пользовательского режима QEMU.....	321
Полная эмуляция системы в QEMU	325

Глава 10. Статический анализ	331
Инструменты статического анализа.....	332
Инструменты командной строки.....	332
Дизассемблеры и декомпиляторы.....	332
Binary Ninja Cloud.....	333
Пример вызова по ссылке.....	338
Анализ потока команд.....	345
Функция Main.....	346
Подпрограмма.....	347
Преобразование в char.....	351
Оператор if.....	353
Деление с неполным частным.....	355
Цикл for.....	357
Анализ алгоритма.....	359
Глава 11. Динамический анализ	373
Отладка с помощью командной строки.....	374
Команды GDB.....	375
Многопользовательский GDB.....	376
Расширение GDB — GEF.....	378
Radare2.....	390
Удаленная отладка.....	396
Radare2.....	396
IDA Pro.....	397
Отладка повреждений памяти.....	398
Отладка процесса с помощью GDB.....	407
Глава 12. Реверс-инжиниринг вредоносных программ для macOS arm64	412
Предыстория.....	413
Бинарные файлы macOS arm64.....	414
Hello World для macOS (arm64).....	417
Охота за вредоносными бинарными файлами arm64.....	420
Анализ вредоносного ПО arm64.....	427
Методы антианализа.....	428
Логика защиты от отладки с помощью ptrace.....	429
Логика защиты от отладки с помощью sysctl.....	433
Логика антиVM (с помощью SIP Status и обнаружения артефактов VM).....	437
Заключение.....	443
Указатель	444