

Всем, кто верит в науку и принятие решений на основе фактов,
а также первым, кто ответил на угрозу COVID-19 и чья
самоотверженность и тяжкий труд стали лучиком надежды в эпоху
глобального кризиса.

Всем девушкам, которые питают страсть к технологиям,
а также взрослым мужчинам и женщинам, оказывающим
им помощь и поддержку.

Мечтайте по-крупному и исследуйте дальше!

ОБ АВТОРАХ

Крис Игл занимается обратной разработкой уже 40 лет. Он автор книги «The IDA Pro Book», вышедшей в издательстве No Starch Press, и пользуется большим авторитетом как преподаватель обратной разработки. Его перу принадлежат многочисленные статьи по инструментам обратной разработки, он часто выступает на таких мероприятиях, как Blackhat, Defcon и Shmooscon.

Кара Нэнс – частный консультант по безопасности. В течение многих лет работала профессором информатики. Была членом совета директоров проекта Honeynet и много раз выступала с докладами на различных конференциях по всему миру. Обо- жает разрабатывать расширения Ghidra и регулярно читает курсы по Ghidra.

О ТЕХНИЧЕСКОМ РЕЦЕНЗЕНТЕ

Брайан Хэй много лет занимался обратной разработкой, был профессором и разработчиком программного обеспечения. Вы- ступал на многих конференциях, читал курсы, а в настоящее время работает старшим научным сотрудником в компании, занимающейся исследованиями в области безопасности. Спе- циализируется на проектировании и разработке виртуализи- рованных сред для обучения и тестирования новых впечатля- ющих инструментов, таких как Ghidra.

КРАТКОЕ СОДЕРЖАНИЕ

Об авторах.....	6
О техническом рецензенте	6
Оглавление	8
Благодарности.....	17
Введение	18
Часть I. Введение	25
Глава 1. Введение в дизассемблирование	27
Глава 2. Обратная разработка и инструменты дизассемблирования	43
Глава 3. Первое знакомство с Ghidra	65
Часть II. Основы использования Ghidra	73
Глава 4. Начало работы с Ghidra	75
Глава 5. Отображение данных в Ghidra	93
Глава 6. Дизассемблирование в Ghidra	135
Глава 7. Управление дизассемблированием.....	175
Глава 8. Типы данных и структуры данных	211
Глава 9. Перекрестные ссылки	259
Глава 10. Графы	277
Часть III. Поставить Ghidra себе на службу	299
Глава 11. Коллективная обратная разработка программ	301
Глава 12. Настройка Ghidra	331
Глава 13. Расширение взгляда на мир Ghidra	355
Глава 14. Основы написания скриптов для Ghidra	387
Глава 15. Eclipse и GhidraDev.....	423
Глава 16. Необслуживаемый режим Ghidra	457
Часть IV. Дополнительные темы	483
Глава 17. Загрузчики Ghidra	485
Глава 18. Процессорные модули в Ghidra	537
Глава 19. Декомпилятор Ghidra	571
Глава 20. Зависимость от компилятора	591
Часть V. Реальные приложения.....	623
Глава 21. Анализ обфусцированного кода	625
Глава 22. Изменение двоичного кода	673
Глава 23. Определение разности двоичных файлов и отслеживание версий.....	705
Приложение. Ghidra для пользователей IDA	731

ОГЛАВЛЕНИЕ

ЧАСТЬ I. ВВЕДЕНИЕ..... 25

Глава 1. Введение в дизассемблирование.....	27
Теория дизассемблирования.....	28
Что делает дизассемблер.....	29
Зачем нужен дизассемблер.....	30
Анализ вредоносного ПО.....	31
Анализ на уязвимость.....	31
Анализ интероперабельности.....	32
Проверка компилятора.....	32
Отображение команд в процессе отладки.....	33
Как работает дизассемблер.....	33
Базовый алгоритм дизассемблирования.....	33
Алгоритм линейной развертки.....	35
Алгоритм рекурсивного спуска.....	37
Резюме.....	42
Глава 2. Обратная разработка и инструменты дизассемблирования.....	43
Средства классификации.....	44
file.....	44
PE Tools.....	47
PEiD.....	48
Обзорные инструменты.....	49
nm.....	49
ldd.....	52
objdump.....	55
otool.....	56
dumpbin.....	56
c++filt.....	57
Инструменты глубокой инспекции.....	59
strings.....	59
Дизассемблеры.....	61
Резюме.....	63
Глава 3. Первое знакомство с Ghidra.....	65
Лицензионная политика Ghidra.....	66
Версии Ghidra.....	66
Ресурсы поддержки Ghidra.....	66
Скачивание Ghidra.....	68
Установка Ghidra.....	68
Запуск Ghidra.....	70
Резюме.....	71

ЧАСТЬ II. ОСНОВЫ ИСПОЛЬЗОВАНИЯ GHIDRA..... 73

Глава 4. Начало работы с Ghidra	75
Запуск Ghidra	75
Создание нового проекта	77
Загрузка файла в Ghidra.....	78
Использование простого двоичного загрузчика	82
Анализ файлов в Ghidra.....	84
Результаты автоматического анализа	88
Поведение рабочего стола во время начального анализа	89
Сохранение работы и выход.....	90
Советы по организации рабочего стола Ghidra	91
Резюме.....	92
Глава 5. Отображение данных в Ghidra.....	93
Браузер кода	94
Окна браузера кода	97
Окно листинга.....	100
Создание дополнительных окон дизассемблера	105
Представление графа функции в Ghidra	106
Окно деревьев программы.....	112
Окно дерева символов.....	113
Импортируемые объекты.....	114
Экспортируемые объекты.....	115
Функции	115
Метки	116
Классы.....	116
Пространства имен.....	117
Окно диспетчера типов данных.....	117
Окно консоли.....	118
Окно декомпилятора	118
Другие окна Ghidra	121
Окно байтов	121
Окно определенных данных	123
Окно определенных строк	125
Окна таблицы символов и ссылок на символы.....	126
Окно карты памяти	130
Окно графа вызовов функции.....	131
Резюме.....	132
Глава 6. Дизассемблирование в Ghidra	135
Навигация по листингу дизассемблера	136
Имена и метки	136
Навигация в Ghidra	137
Перейти к	139
История навигации	139
Кадры стека.....	141
Механизмы вызова функций	141

Соглашения о вызове	144
Дополнительные сведения о кадре стека	150
Размещение локальных переменных	151
Примеры кадров стека	152
Представления стека в Ghidra	157
Анализ кадров стека в Ghidra	158
Кадры стека в листинге дизассемблера	159
Анализ кадра стека с помощью декомпилятора	162
Локальные переменные как операнды	164
Редактор кадра стека в Ghidra	165
Поиск	168
Поиск по тексту программы	169
Поиск в памяти	171
Резюме	173
Глава 7. Управление дизассемблированием	175
Манипулирование именами и метками	176
Переименование параметров и локальных переменных	177
Переименование меток	182
Добавление новой метки	183
Редактирование меток	185
Удаление метки	187
Навигация по меткам	187
Комментарии	187
Концевые комментарии	189
Предварительные и заключительные комментарии	190
Вводные комментарии	190
Повторяемые комментарии	192
Комментарии для параметров и локальных переменных	192
Аннотации	193
Базовые преобразования кода	194
Изменение параметров отображения кода	194
Форматирование операндов команд	196
Манипулирование функциями	198
Преобразование данных в код (и наоборот)	202
Основы преобразования данных	203
Задание типов данных	204
Работа со строками	206
Определение массивов	208
Резюме	209
Глава 8. Типы данных и структуры данных	211
В чем смысл этих данных?	212
Распознавание структур данных в коде	215
Доступ к элементам массива	215
Доступ к полям структуры	228
Массивы структур	234
Создание структур в Ghidra	236

Создание новой структуры	237
Редактирование полей структуры	240
Наложение структур	242
Введение в обратную разработку кода на C++	244
Указатель this	245
Виртуальные функции и vftаблицы	246
Жизненный цикл объекта	251
Декорирование имен	253
Идентификация типа во время выполнения	254
Отношения наследования	256
Справочные материалы по обратной разработке кода на C++	257
Резюме	258
Глава 9. Перекрестные ссылки	259
Базовые сведения о ссылках	260
Перекрестные (обратные) ссылки	261
Пример анализа ссылок	265
Окна управления ссылками	271
Окно перекрестных ссылок	272
Ссылки на	273
Ссылки на символы	273
Дополнительные способы работы со ссылками	274
Резюме	276
Глава 10. Графы	277
Простые блоки	278
Графы функций	279
Графы вызовов функций	290
Деревья	297
Резюме	297
 ЧАСТЬ III. ПОСТАВИТЬ GHIDRA	
СЕБЕ НА СЛУЖБУ	
299	
Глава 11. Коллективная обратная разработка программ	301
Коллективная работа	302
Подготовка сервера Ghidra	303
Разделяемые проекты	307
Создание разделяемого проекта	307
Управление проектом	310
Меню окна проекта	311
Меню File	311
Меню Edit	314
Меню Project	316
Репозиторий проекта	319
Управление версиями	321
Пример	324
Резюме	330

Глава 12. Настройка Ghidra.....	331
Браузер кода	332
Реорганизация окон	332
Редактирование параметров инструментов.....	334
Редактирование параметров инструмента.....	337
Специальные средства редактирования для некоторых инструментов.....	338
Сохранение конфигурации браузера кода.....	340
Окно проекта в Ghidra	340
Меню Tools.....	346
Рабочие пространства	352
Резюме.....	353
Глава 13. Расширение взгляда на мир Ghidra	355
Импорт файлов	356
Анализаторы	359
Модели слов	360
Типы данных.....	362
Создание новых архивов типов данных	365
Идентификаторы функций	369
Плагин Function ID.....	371
Пример применения плагина Function ID: UPX.....	374
Пример применения плагина Function ID: профилирование статической библиотеки.....	379
Резюме.....	385
Глава 14. Основы написания скриптов для Ghidra	387
Диспетчер скриптов	388
Окно диспетчера скриптов	388
Панель инструментов диспетчера скриптов	390
Разработка скриптов	391
Написание скриптов на Java (не JavaScript!).....	391
Пример редактирования скрипта: поиск по регулярному выражению	393
Скрипты на Python.....	399
Поддержка других языков	401
Введение в Ghidra API.....	402
Интерфейс Address.....	403
Интерфейс Symbol.....	403
Интерфейс Reference.....	403
Класс GhidraScript	404
Функции манипулирования программой	410
Класс Program.....	411
Интерфейс Function	413
Интерфейс Instruction	413
Примеры скриптов Ghidra.....	414
Пример 1: перечисление функций.....	414
Пример 2: перечисление команд.....	415

Пример 3: перечисление перекрестных ссылок	416
Пример 4: нахождение вызовов функции	417
Пример 5: эмуляция поведения языка ассемблера.....	419
Резюме.....	422
Глава 15. Eclipse и GhidraDev	423
Eclipse	423
Интеграция с Eclipse.....	424
Запуск Eclipse	425
Редактирование скриптов в Eclipse	426
Меню GhidraDev	427
GhidraDev ▶ New	428
Навигация в обозревателе пакетов	434
Пример: проект модуля анализатора	441
Шаг 1: постановка задачи	443
Шаг 2: создать модуль в Eclipse.....	443
Шаг 3: написать анализатор	443
Шаг 4: протестировать анализатор в Eclipse	451
Шаг 5: добавить анализатор в Ghidra.....	451
Шаг 6: тестирование анализатора в Ghidra	452
Резюме.....	455
Глава 16. Необслуживаемый режим Ghidra	457
Приступая к работе	458
Шаг 1: запуск Ghidra	459
Шаги 2 и 3: создать новый проект Ghidra в указанном месте	459
Шаг 4: импортировать файл в проект.....	460
Шаги 5 и 6: автоматический анализ файла, сохранение и выход	460
Флаги и параметры.....	465
Написание скриптов	475
HeadlessSimpleROP	475
Автоматизированное создание базы данных FidDb.....	480
Резюме.....	482
ЧАСТЬ IV. ДОПОЛНИТЕЛЬНЫЕ ТЕМЫ	483
Глава 17. Загрузчики Ghidra	485
Анализ неизвестного файла.....	487
Загрузка PE-файла Windows вручную	488
Пример 1: модуль загрузчика SimpleShellcode.....	502
Шаг 0: шаг назад.....	503
Шаг 1: поставить задачу	506
Шаг 2: создать модуль в Eclipse.....	507
Шаг 3: разработать загрузчик.....	507
Шаг 4: добавить загрузчик в Ghidra	514
Шаг 5: протестировать загрузчик в Ghidra	515
Пример 2: простой загрузчик шелл-кода из исходных файлов.....	517

Обновление 1: изменить ответ на опрос импортера.....	518
Обновление 2: найти шелл-код в исходном коде.....	518
Обновление 3: преобразовать шелл-код в байтовые значения.....	519
Обновление 4: загрузить преобразованный байтовый массив	520
Результаты	520
Пример 3: простой загрузчик шелл-кода в формате ELF	522
Организационные мероприятия.....	523
Формат заголовков ELF.....	524
Определение поддерживаемых спецификаций загрузки	525
Загрузить содержимое файла в Ghidra	527
Отформатировать байты данных и добавить точку входа	528
Файлы определений языков	529
Opinion-файлы	530
Результаты	532
Резюме.....	535
Глава 18. Процессорные модули в Ghidra.....	537
Знакомство с процессорным модулем Ghidra	539
Процессорные модули в Eclipse.....	539
SLEIGH.....	541
Руководства по процессорам	543
Модификация процессорного модуля Ghidra	545
Постановка задачи	547
Пример 1: добавление команды в процессорный модуль	547
Пример 2: модификация команды в процессорном модуле.....	556
Вариант 1: записать в EAX константу	556
Пример 3: добавление регистра в процессорный модуль.....	567
Резюме.....	570
Глава 19. Декомпилятор Ghidra	571
Анализ с помощью декомпилятора	571
Параметры анализа	572
Окно декомпилятора	575
Пример 1: редактирование в окне декомпилятора	576
Пример 2: функции, не возвращающие управление	582
Пример 3: автоматизированное создание структуры	584
Резюме.....	590
Глава 20. Зависимость от компилятора	591
Высокоуровневые конструкции	592
Предложения switch	592
Пример: сравнение компиляторов gcc и Microsoft C/C++.....	599
Параметры компилятора.....	602
Пример 1: оператор деления по модулю	603
Пример 2: тернарный оператор	606
Пример 3: встраивание функций	608
Реализация зависящих от компилятора особенностей C++	610
Перегрузка функций.....	611
Реализации RTTI	612

Нахождение функции main	617
Пример 1: от _start к main с компилятором gcc для Linux x86-64	618
Пример 2: от _start к main с компилятором clang для FreeBSD x86-64.....	619
Пример 3: от _start к main с компилятором Microsoft's C/C++	620
Резюме.....	621

ЧАСТЬ V. РЕАЛЬНЫЕ ПРИЛОЖЕНИЯ 623

Глава 21. Анализ обфусцированного кода	625
Противодействие обратной разработке.....	626
Обфускация.....	626
Методы противодействия статическому анализу	627
Обфускация импортированной функции	643
Методы противодействия динамическому анализу	648
Статическая деобфускация двоичных файлов в Ghidra.....	654
Скриптовая деобфускация	654
Эмуляторная деобфускация.....	661
Резюме.....	670
Глава 22. Изменение двоичного кода.....	673
Планирование заплатки	674
Поиск того, что нуждается в изменении.....	675
Поиск в памяти.....	675
Поиск прямых ссылок	676
Поиск командных паттернов	677
Поиск конкретных типов поведения	682
Наложение заплатки.....	683
Внесение простых изменений	683
Внесение нетривиальных изменений.....	690
Экспорт файлов	694
Форматы экспорта из Ghidra	695
Двоичный формат экспорта	696
Экспорт с применением скрипта	697
Пример: латание двоичного файла.....	699
Резюме.....	703
Глава 23. Определение разности двоичных файлов и отслеживание версий.....	705
Разность двоичных файлов	706
Инструмент Program Diff.....	708
Пример: объединение двух проанализированных файлов.....	712
Сравнение функций.....	717
Окно сравнения функций.....	717
Пример: сравнение криптографических функций.....	720
Отслеживание версий	727
Концепции, относящиеся к отслеживанию версий	728
Резюме.....	730

Ghidra для пользователей IDA.....	731
Основы	731
Создание базы данных	732
Основные окна и навигация	734
Дерево символов	737
Скрипты.....	738
Резюме.....	738
Предметный указатель.....	739

БЛАГОДАРНОСТИ

Эта книга не состоялась бы без помощи и поддержки со стороны исключительно профессионального коллектива издательства No Starch Press. Билл Поллок и Барбара Яин поддержали идею написать книгу о Ghidra, отражающую наше видение, и мы глубоко ценим их веру в нас, не ослабевавшую на протяжении всего пути. Отзывы Атабаска Уитши о первых главах стали для нас ценным подспорьем и указали верное направление. Постоянная поддержка Лорел Чан и ее терпеливые ответы на все наши вопросы помогли превратить книгу в готовый продукт, которым мы очень гордимся. Мы также хотим поблагодарить всех, кто оставался «за кулисами», за тяжелую работу по претворению мечты в реальность, в т. ч. Катрину Тэйлор, Бартона Д. Рида, Шарон Уилки и Даниэля Фостера.

Мы также благодарим технического редактора Брайана Хэя, который проштудировал наши пространные словеса и примеры. Его знания и опыт работы с Ghidra стали гарантией безошибочности содержания книги с технической точки зрения, а его опыт преподавания позволил изложить материал так, чтобы он представлял интерес как для начинающих, так и для опытных инженеров.

Мы признательны всей команде разработчиков Ghidra, прошлых и нынешних, из Агентства национальной безопасности за то, что они создали Ghidra и поделились ей со всем миром, сделав проектом с открытым исходным кодом.

Кара выражает благодарность Бену за терпение, которое он проявлял, когда она изучала технологию, и Кэти за терпение, проявленное во время написания книги. Она также благодарит Йена за вдохновляющее введение и Дики и Ленору, которые никогда не теряли веру в нее. Наконец, она благодарит Брайана за юмор и непрекращающуюся ежедневную и ежечасную поддержку. Не будь этой поддержки, книга не увидела бы свет.

ВВЕДЕНИЕ



Принимаясь за написание этой книги, мы ставили себе целью познакомить с Ghidra нынешних и будущих специалистов по обратной разработке. В руках опытного инженера Ghidra упрощает процесс анализа и позволяет настраивать и расширять свои возможности под потребности конкретного пользователя, так чтобы они соответствовали привычному ему технологическому процессу. Также Ghidra вполне доступна начинающим инженерам, чему немало способствует включенный в нее декомпилятор, который позволяет лучше понять связи между высокоуровневым языком программирования и листингами дизассемблера человеку, только вступающему в мир анализа двоичного кода.

Писать книгу о Ghidra нелегко. Ghidra – сложный инструмент с открытым исходным кодом, который постоянно развивается. Наш текст описывает движущуюся мишень, поскольку сообщество Ghidra продолжает улучшать и расширять возможности программы. Как и во многих других новых проектах с открытым исходным кодом, рождение Ghidra ознаменовалось серией быстро сменяющих друг друга выпусков. Основная цель авторов состояла в том, чтобы на фоне развития Ghidra все же предложить читателям широкий и глубокий фундамент для понимания и эффективного использования текущей и будущих версий Ghidra в их работе по обратной разработке. Насколько это возможно, мы старались сделать книгу независимой от версии. По счастью, новые

выпуски Ghidra хорошо документированы и содержат подробные списки изменений, которые помогут оценить различия между тем, что написано в книге, и вашей текущей версией.

Об этой книге

Это первая полная книга о Ghidra. Она задумана как всеобъемлющий источник для изучающих обратную разработку с помощью Ghidra. В ней имеется вводный материал, облегчающий начинающим вступление в мир обратной разработки, материал повышенной сложности, который поможет опытным инженерам расширить свое видение мира, а также примеры, которые будут полезны как новобранцам, так и ветеранам, желающим расширить возможности Ghidra и стать членами сообщества разработчиков.

На кого рассчитана эта книга?

Эта книга предназначена для начинающих и опытных специалистов по обратной разработке. Если у вас еще нет опыта в этой области, ничего страшного – в начальных главах достаточно материала, чтобы овладеть основами обратной разработки и приступить к исследованию и анализу двоичного кода с помощью Ghidra. Опытные инженеры, желающие добавить Ghidra в свой арсенал, могут быстро просмотреть первые две части, чтобы получить общее представление о Ghidra, а затем перейти к тем главам, которые им особенно интересны. Опытные пользователи и разработчики Ghidra могут сконцентрироваться на более поздних главах, где описывается, как создавать новые расширения, и применить свои знания и опыт для обогащения проекта Ghidra.

Структура книги

Эта книга разделена на пять частей. Часть I содержит введение в дизассемблирование, обратную разработку и сам проект Ghidra. В части II рассматриваются базовые приемы использования Ghidra. Часть III демонстрирует настройку и автоматизацию Ghidra. В части IV более глубоко объясняются конкретные типы модулей Ghidra и вспомогательные концепции. В части V показано, как применить Ghidra в некоторых реальных ситуациях, с которыми может столкнуться специалист по обратной разработке.

Часть I. Введение

Глава 1. Введение в дизассемблирование

В этой вводной главе мы познакомимся с теорией и практикой дизассемблирования и обсудим некоторые плюсы и минусы двух наиболее распространенных алгоритмов дизассемблирования.

Глава 2. Инструменты дизассемблирования и обратной разработки

В этой главе обсуждаются основные категории инструментов обратной разработки и дизассемблирования.

Глава 3. Первое знакомство с Ghidra

Здесь мы впервые встретимся с Ghidra, узнаем о ее истоках, о том, как ее получить и начать пользоваться этим свободным комплектом инструментов с открытым исходным кодом.

Часть II. Основы использования Ghidra

Глава 4. Начало работы с Ghidra

В этой главе начинается наше путешествие в мир Ghidra. Мы увидим Ghidra в действии, для чего создадим проект, проанализируем файл и познакомимся с графическим интерфейсом Ghidra.

Глава 5. Отображение данных в Ghidra

Здесь мы познакомимся с браузером кода (CodeBrowser), главным аналитическим средством Ghidra, и его основными окнами.

Глава 6. Дизассемблирование в Ghidra

В этой главе мы изучим концепции, необходимые для понимания процесса дизассемблирования в Ghidra.

Глава 7. Управление дизассемблированием

В этой главе мы научимся дополнять анализ Ghidra и управлять процессом дизассемблирования в своих целях.

Глава 8. Типы данных и структуры данных

В этой главе мы научимся распознавать и манипулировать простыми и сложными структурами данных, встречающимися в скомпилированных программах.

Глава 9. Перекрестные ссылки

Эта глава посвящена подробному рассмотрению перекрестных ссылок, их графическому представлению и той важной роли, которую они играют в понимании поведения программы.

Глава 10. Графы

В этой главе мы познакомимся с графическими возможностями Ghidra и графами как средством анализа двоичного кода.

Часть III. Поставить Ghidra себе на службу

Глава 11. Коллективная обратная разработка программ

В этой главе представлена уникальная возможность Ghidra – использование в качестве инструмента коллективной работы. Мы узнаем, как сконфигурировать сервер Ghidra и сделать проект доступным другим аналитикам.

Глава 12. Настройка Ghidra

Здесь мы начнем настраивать Ghidra, конфигурируя проекты и инструменты, так чтобы они отвечали нашему технологическому процессу анализа.

Глава 13. Расширение взгляда на мир Ghidra

В этой главе мы научимся генерировать и применять сигнатуры библиотек и другого специального содержимого, чтобы Ghidra могла распознавать новые конструкции в двоичном коде.

Глава 14. Основы написания скриптов для Ghidra

В этой главе мы познакомимся с основами написания скриптов для Ghidra на Python и Java с применением встроенного редактора Ghidra.

Глава 15. Eclipse и GhidraDev

В этой главе мы поднимем написание скриптов на новый уровень, интегрировав Eclipse с Ghidra и воспользовавшись мощными скриптовыми возможностями, предоставляемыми этой конфигурацией, в частности приведем рабочий пример построения нового анализатора.

Глава 16. Необслуживаемый режим Ghidra

Здесь мы познакомимся с использованием Ghidra в необслуживаемом режиме, когда не требуется никакого GUI. Вы, без сомнения, оцените преимущества этого режима в типичных крупномасштабных повторяющихся задачах.

Часть IV. Дополнительные темы

Глава 17. Загрузчики Ghidra

Здесь мы более глубоко познакомимся с тем, как Ghidra импортирует и загружает файлы. У нас будет возможность создать новые загрузчики для обработки ранее не распознаваемых типов файлов.

Глава 18. Процессоры Ghidra

В этой главе мы рассмотрим язык Ghidra SLEIGH, предназначенный для определения архитектуры процессора. Мы изучим процесс добавления новых процессоров и команд в Ghidra.

Глава 19. Декомпилятор Ghidra

Здесь мы подробнее рассмотрим одну из самых популярных возможностей Ghidra: декомпилятор. Вы увидите, как он работает на внутреннем уровне и какой вклад вносит в процесс анализа.

Глава 20. Зависимость от компилятора

Эта глава посвящена вариациям кода в зависимости от компилятора и целевой платформы.

Часть V. Реальные приложения

Глава 21. Анализ обфусцированного кода

Мы узнаем, как использовать Ghidra для анализа обфусцированного кода в статическом контексте, так чтобы код не нужно было исполнять.

Глава 22. Изменение двоичного кода

В этой главе мы узнаем о некоторых способах использования Ghidra для изменения двоичного кода в процессе анализа — как внутри самой Ghidra, так и для создания «залатанных» версий оригинальных двоичных файлов.

Глава 23. Определение разности двоичных файлов и отслеживание версий

В этой, последней, главе приводится обзор средств Ghidra, позволяющих вычислить дельту между двумя двоичными файлами, а также краткое введение в дополнительные средства отслеживания версий.

Приложение. Ghidra для пользователей IDA

Опытные пользователи IDA найдут в этом приложении информацию о соответствии между терминологией и сходной функциональностью IDA и Ghidra.

ПРИМЕЧАНИЕ

Код, встречающийся в листингах, можно найти на сайтах <https://nostarch.com/GhidraBook/> и

<https://ghidrabook.com/>, а также на сайте издательства

<https://dmkpress.com/catalog/computer/security/978-5-97060-942-2/>



Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru