

Оглавление

Об авторах	16
О научном редакторе	16
Предисловие	17
Благодарности	19
Введение	21
Как выглядят встроенные устройства	22
Способы взлома встроенных устройств	23
Что такое аппаратная атака	24
Для кого эта книга	25
Структура книги	25
От издательства	27
Глава 1. Следим за здоровьем. Введение в безопасность встроенных систем	28
Аппаратные компоненты	28
Компоненты ПО	31
Загрузочный код	32
Загрузчик	32
Доверенная среда выполнения ОС и доверенные приложения	33
Образы прошивки	34
Основное ядро ОС и приложений	34
Моделирование аппаратных угроз	35
Что такое безопасность	35
Дерево атак	38
Профилирование атакующих	39
Типы атак	41
Программные атаки на аппаратные средства	41
Атаки на уровне печатной платы	44
Логические атаки	46
Неинвазивные атаки	48
Чип-инвазивные атаки	48

Активы и цели безопасности	52
Конфиденциальность и целостность двоичного кода	54
Конфиденциальность и целостность ключей	54
Удаленная проверка загрузки	55
Конфиденциальность и целостность персональных данных	56
Целостность и конфиденциальность данных с датчика	56
Защита конфиденциальности контента	57
Безопасность и отказоустойчивость	57
Меры противодействия	58
Защита	58
Обнаружение	58
Реагирование	59
Пример дерева атак	59
Идентификация против эксплуатации	62
Масштабируемость	63
Анализ дерева атак	63
Оценка путей аппаратных атак	63
Раскрытие проблем безопасности	66
Резюме	68
Глава 2. На кончиках пальцев. Аппаратные периферийные интерфейсы	69
Основы электричества	70
Напряжение	70
Ток	70
Сопротивление	71
Закон Ома	71
Переменный и постоянный ток	71
О разных видах сопротивлений	72
Мощность	73
Связь с помощью электричества	73
Логические уровни	74
Высокий импеданс, подтягивания и стягивания	77
Односторонняя связь, три состояния, открытый коллектор, открытый эмиттер	77
Асинхронный, синхронный и встроенный тактовый сигнал	79
Дифференциальная сигнализация	80
Низкоскоростные последовательные интерфейсы	81
Универсальный последовательный асинхронный приемник/передатчик	82
Последовательный периферийный интерфейс	84
Интерфейс Inter-IC	86

Безопасный цифровой ввод/вывод и встроенные мультимедийные карты	91
CAN-шина	93
JTAG и другие интерфейсы отладки	94
Параллельные интерфейсы	99
Интерфейсы памяти	100
Высокоскоростные последовательные интерфейсы	101
Универсальная последовательная шина (USB)	102
PCI Express	103
Ethernet	104
Измерение	104
Мультиметр: вольты	105
Мультиметр: прозвонка	105
Цифровой осциллограф	106
Логический анализатор	111
Резюме	112
Глава 3. Что внутри. Идентификация компонентов и сбор информации	113
Сбор информации	114
Документы Федеральной комиссии по связи	114
Патенты	117
Спецификации и схемы	120
Пример поиска информации: устройство USB Armory	121
Вскрытие покажет	129
Поиск ИС на плате	129
Корпуса с мелкими выводами: SOIC, SOP и QFP	132
Корпуса без выводов: SO и QFN	134
Шаровая сетка	135
Корпус с габаритами чипа	138
DIP, сквозное отверстие и другие корпуса	139
Примеры корпусов ИС на печатных платах	139
Идентификация других компонентов на плате	142
Сопоставление печатной платы	147
Использование граничного сканирования JTAG для сопоставления	152
Извлечение информации из прошивки	154
Извлечение образа прошивки	154
Анализ образа прошивки	157
Резюме	165
Глава 4. Слон в посудной лавке. Внедрение ошибок	166
Внедрение ошибок в механизмы безопасности	167
Обход проверки подписи прошивки	168
Получение доступа к заблокированным функциям	168

Восстановление криптографических ключей	169
Упражнение по внедрению ошибок в OpenSSH	169
Внедрение ошибок в код С	170
Внедрение ошибок в машинный код	171
Тот самый слон	173
Целевое устройство и цель ошибки	174
Инструменты внедрения ошибок	174
Подготовка целевого устройства и мониторинг	175
Методы поиска неисправностей	181
Определение примитивов ошибок	181
Поиск эффективных ошибок	185
Стратегии поиска	193
Анализ результатов	196
Резюме	198
Глава 5. Руками не трогать. Как внедрять ошибки	199
Внедрение ошибок в тактовый сигнал	200
Метастабильность	204
Анализ чувствительности к ошибкам	207
Ограничения	207
Требуемое оборудование	208
Параметры внедрения ошибки	211
Внедрение ошибок по напряжению	211
Генерация скачков напряжения	212
Устройство внедрения с переключателем напряжения	213
Метод «лома»	218
Атака на Raspberry Pi с помощью «лома»	219
Поиск параметров для внедрения ошибки напряжения	227
Внедрение электромагнитных ошибок	227
Генерация электромагнитных неисправностей	229
Архитектуры для ввода электромагнитных неисправностей	231
Форма и ширина импульса EMFI	233
Выбор параметров для электромагнитной ошибки	233
Внедрение оптических ошибок	234
Подготовка микросхемы	235
Атаки на переднюю и заднюю часть чипа	236
Источники света	238
Настройка внедрения оптических ошибок	240
Настраиваемые параметры внедрения оптических ошибок	240
Внедрение ошибок в корпус	241
Параметры внедрения в корпус	243

Активация аппаратных сбоев	244
Случаи, когда время предсказать не удастся	245
Резюме	246
Глава 6. Рубрика «Эксперименты». Лаборатория внедрения ошибок	248
Этап 1. Простой цикл	249
Разрушительное барбекю	251
Этап 2. Внедрение полезных сбоев	254
Использование «лома» для внедрения сбоев в конфигурационное слово	254
Внедрение сбоя мультиплексора	271
Этап 3. Дифференциальный анализ ошибок	277
Немного математики RSA	277
Получение правильной подписи от целевого устройства	281
Резюме	285
Глава 7. Цель отмечена крестом. Дамп памяти кошелька Trezor One	286
Введение в атаку	287
Внутреннее устройство кошелька Trezor One	288
Ошибка запроса USB на чтение	289
Дизассемблирование кода	291
Сборка прошивки и проверка сбоя	292
Запуск и синхронизация по USB	296
Атака через корпус	301
Настройка	301
Разбор кода для внедрения ошибки	301
Запуск кода	305
Подтверждение перехвата данных	306
Точная настройка электромагнитного импульса	307
Настройка синхронизации на основе сообщений USB	307
Резюме	308
Глава 8. Мощный подход. Введение в анализ потребляемой мощности	310
Атаки по времени	311
Атака по времени жесткого диска	314
Измерение потребляемой мощности для атак по времени	318
Простой анализ потребляемой мощности	319
Применение SPA к RSA	320
Применение SPA к RSA, Redux	322
SPA на ECDSA	325
Резюме	331

Глава 9. Рубрика «Эксперименты». Простой анализ потребляемой мощности . . .	332
Домашняя лаборатория	332
Построение базовой лабораторной установки	333
Покупные варианты	337
Код целевого устройства	338
Сборка	340
Собираем все воедино: SPA-атака	343
Подготовка целевого устройства	343
Подготовка осциллографа	345
Анализ сигнала	346
Сценарий для связи и анализа	348
Сценарий атаки	351
Пример ChipWhisperer-Nano	353
Сборка и загрузка прошивки	354
Первый подход к организации связи	354
Трассировка	355
От трассировки к атаке	357
Резюме	360
Глава 10. Разделяй и властвуй. Дифференциальный анализ потребляемой мощности	362
Внутри микроконтроллера	363
Изменение напряжения на конденсаторе	364
От потребляемой мощности к данным и обратно	366
Пример с XOR	368
Атака дифференциального анализа потребляемой мощности	370
Предсказание потребляемой мощности с помощью предположения об утечке	371
Атака DPA на Python	375
Знай своего врага. Ускоренный курс по стандартам шифрования	378
Атака на AES-128 с помощью DPA	381
Атака корреляционного анализа потребляемой мощности	382
Коэффициент корреляции	383
Расчет данных для корреляции	385
Атака на AES-128 с помощью CPA	388
Общение с целевым устройством	394
Скорость захвата осциллографа	394
Резюме	395
Глава 11. Без формул никуда. Продвинутый анализ потребляемой мощности . . .	396
Основные препятствия	397
Более мощные атаки	398

Оценка успеха	400
Метрики успеха	400
Энтропийные метрики	401
Прогрессия пика корреляции	403
Высота пика корреляции	404
Измерения на реальных устройствах	405
Работа с устройством	405
Измерительный зонд	408
Определение чувствительных мест	411
Автоматическое сканирование зондом	412
Настройка осциллографа	414
Анализ и обработка трассировок	417
Методы анализа	418
Методы обработки	429
Глубокое обучение с помощью сверточных нейронных сетей	433
Резюме	436

Глава 12. Рубрика «Эксперименты». Дифференциальный анализ

потребляемой мощности	438
О загрузчиках	438
Протокол связи загрузчика	439
О шифровании AES-256 CBC	440
Атака на AES-256	441
Получение и сборка кода загрузчика	443
Запуск целевого устройства и захват кривых	444
Расчет CRC	444
Взаимодействие с загрузчиком	445
Захват обзорных кривых	445
Захват подробных кривых	447
Анализ	447
Ключ раунда 14	448
Ключ раунда 13	449
Восстановление IV	452
Что будем захватывать	452
Получение первой кривой	453
Получение остальных кривых	455
Анализ	455
Атака на подпись	459
Теория атаки	460
Кривые потребляемой мощности	460

Анализ	461
Все четыре байта	462
Что в коде загрузчика	462
Моменты проверки подписи	464
Резюме	465
Глава 13. Шутки в сторону. Примеры из жизни	467
Атаки внедрения ошибок	467
Гипервизор PlayStation 3	468
Xbox 360	471
Атаки с анализом потребляемой мощности	474
Атака Philips Hue	474
Резюме	479
Глава 14. Подумайте о детях. Контрмеры, сертификаты и полезные байты	483
Контрмеры	484
Реализация контрмер	484
Проверка контрмер	502
Отраслевые сертификаты	505
Как улучшить результаты	508
Резюме	509
Приложение А. Куда потратить деньги. Настройка лаборатории	510
Проверка подключения и напряжения: от 50 до 500 долларов	511
Пайка с мелким шагом: от 50 до 1500 долларов	513
Демонтаж сквозного отверстия: от 30 до 500 долларов	515
Пайка и демонтаж компонентов для поверхностного монтажа: от 100 до 500 долларов	516
Модификация печатных плат: от 5 до 700 долларов	520
Оптические микроскопы: от 200 до 2000 долларов	521
Фотографирование плат: от 50 до 2000 долларов	522
Питание: от 10 до 1000 долларов	523
Отображение аналоговых сигналов (осциллографы): от 300 до 25 000 долларов	524
Глубина памяти	525
Частота дискретизации	526
Полоса пропускания	528
Другие особенности	530
Отображение логических сигналов: от 300 до 8000 долларов	530
Триггеры на последовательных шинах: от 300 до 8000 долларов	532
Декодирование последовательных протоколов: от 50 до 8000 долларов	533

Анализ и триггер CAN-шины: от 50 до 5000 долларов	534
Анализ Ethernet: 50 долларов	535
Взаимодействие через JTAG: от 20 до 10 000 долларов	535
JTAG и граничное сканирование	535
Отладка через JTAG	536
Связь по PCIe: от 100 до 1000 долларов	537
Анализ USB: от 100 до 6000 долларов	538
USB-триггеры: от 250 до 6000 долларов	540
Эмуляция USB: 100 долларов	540
Подключение к флеш-памяти SPI: от 25 до 1000 долларов	541
Анализ потребляемой мощности: от 300 до 50 000 долларов	541
Триггер по аналоговым сигналам: от 3800 долларов	545
Измерение магнитных полей: от 25 до 10 000 долларов	546
Внедрение ошибок в тактовый сигнал: от 100 до 30 000 долларов	548
Внедрение ошибок по напряжению: от 25 до 30 000 долларов	549
Внедрение электромагнитных ошибок: от 100 до 50 000 долларов	550
Внедрение оптических ошибок: от 1000 до 250 000 долларов	551
Позиционирование щупов: от 100 до 50 000 долларов	552
Целевые устройства: от 10 до 10 000 долларов	553
Приложение Б. Ваша база — наша база. Популярные распиновки	556
Распиновка флеш-памяти SPI	556
Разъемы с шагом в 0,1 дюйма	557
Двадцатиконтактный разъем JTAG	557
Четырнадцатиконтактный разъем PowerPC JTAG	558
Разъемы с шагом в 0,05 дюйма	558
Arm Cortex JTAG/SWD	558
Разъем Ember Packet Trace Port	559