Нашим возлюбленным семьям

СОДЕРЖАНИЕ

От издательства ... 17

Предисловие ... 18

Благодарности ... 24

Глава 1. Введение в аппаратную безопасность ... 26

1.1. Вычислительная система: обзор ... 27
1.2. Уровни вычислительной системы ... 29
1.2.1. Электронная аппаратура ... 30
1.2.2. Типы электронной аппаратуры ... 31
1.3. Что такое аппаратная безопасность? ... 31
1.4. Безопасность или доверие ... 34
1.4.1. Что подрывает доверие к аппаратуре? ... 34
1.4.2. Какие проблемы безопасности вызваны недоверенными организациями? ... 36
1.5. Атаки, уязвимости и контрмеры ... 37
1.5.1. Векторы атаки ... 38
1.5.2. Поверхность атаки ... 38
1.5.3. Модель безопасности ... 40
1.5.4. Уязвимости ... 40
1.5.5. Контрмеры ... 41
1.6. Конфликт между обеспечением безопасности и тестированием/отладкой ... 43
1.7. Эволюция аппаратной безопасности: краткая ретроспектива ... 44
1.8. Взгляд с высоты ... 46
1.9. Практический подход ... 46
1.10. Упражнения ... 50
1.10.1. Вопросы, предполагающие ответ «да» или «нет» ... 50
1.10.2. Вопросы, предполагающие краткий ответ ... 50
1.10.3. Вопросы, предполагающие развернутый ответ ... 51
Ссылки ... 51

Часть I. Базовые сведения в области электронной аппаратуры ... 53

Глава 2. Краткий экскурс в электронную аппаратуру ... 54

2.1. Введение ... 54
2.2. Нанотехнологии ... 56
2.2.1. Кремний на изоляторе (SOI) ... 56
2.2.2. Технология FinFET ... 57
2.2.3. Трехмерные интегральные схемы (3D-ИС) ... 57
2.2.4. Технология объемного кремния ... 58
2.3. Цифровая логика ... 59
2.3.1. Двоичная логика ... 59
2.3.2. Логические элементы (вентили) ... 60
2.3.3. Булева алгебра ... 60

2.3.4. Последовательностные схемы ... 61
2.4. Теория электрических схем ... 64
2.4.1. Резисторы и сопротивление ... 64
2.4.2. Конденсаторы и емкость ... 64
2.4.3. Катушки и индуктивности ... 65
2.4.4. Законы Кирхгофа ... 66
2.5. Специализированные ИС и ПЛИС ... 68
2.5.1. Специализированные ИС (ASIC) ... 68
2.5.2. ПЛИС (FPGA) ... 68
2.5.3. Различия между специализированными ИС и ПЛИС ... 69
2.6. Печатные платы ... 71
2.6.1. Классификация печатных плат ... 72
2.6.2. Процесс проектирования печатных плат ... 72
2.6.3. Создание печатной платы ... 74
2.7. Встраиваемые системы ... 75
2.7.1. Аппаратное обеспечение ... 76
2.7.2. Программное обеспечение ... 76
2.7.3. Характеристики встраиваемых систем ... 77
2.8. Взаимодействие аппаратного обеспечения, прошивки и программного обеспечения ... 78
2.9. Упражнения ... 80
2.9.1. Вопросы, предполагающие ответ «да» или «нет» ... 80
2.9.2. Вопросы, предполагающие краткий ответ ... 81
2.9.3. Вопросы, предполагающие развернутый ответ ... 81
Ссылки ... 81

Глава 3. СнК: проектирование и тестирование ... 83

3.1. Введение ... 83
3.1.1. Стоимость тестирования и качество продукции ... 84
3.1.2. Генерация тестов ... 88
3.2. Разработка СнК на основе заказных блоков ... 97
3.3. Проектирование СнК ... 99
3.4. Верификация СнК ... 100
3.5. Тестирование СнК ... 102
3.6. Нацеленность на отладку ... 104
3.6.1. Требования к средствам отладки ... 105
3.6.2. Архитектура встроенных отладочных средств ... 106
3.6.3. Примеры архитектур встроенных отладочных средств ... 107
3.7. Обзор методов обеспечения тестопригодности ... 108
3.7.1. Тестопригодное проектирование ... 108
3.7.2. Сканирование: триггеры, цепи, сжатие тестов ... 109
3.7.3. Схемы с частичным сканированием ... 113
3.7.4. Граничное сканирование ... 114
3.7.5. Методы встроенного самотестирования ... 116
3.8. Тестирование на рабочей частоте с учетом задержек ... 117
3.8.1. Необходимость тестирования на рабочей частоте ... 117
3.8.2. Основы тестирования на рабочей частоте: launch-off-capture (LOC) and launch-off-shift (LOS) ... 118
3.8.3. Проблемы тестирования на рабочей частоте ... 120
3.9. Упражнения ... 121
3.9.1. Вопросы, предполагающие ответ «да» или «нет» ... 121

3.9.2. Вопросы, предполагающие краткий ответ 121
3.9.3. Вопросы, предполагающие развернутый ответ 122
Ссылки 123

Глава 4. Печатные платы: проектирование и тестирование 126
4.1. Введение 126
4.2. Эволюция печатных плат и их компонентов 127
4.2.1. Развитие печатных плат: хронология 128
4.2.2. Компоненты современных печатных плат 130
4.3. Жизненный цикл печатных плат 132
4.3.1. Инженер-конструктор печатных плат 132
4.3.2. Проектная организация 133
4.3.3. Завод печатных плат 133
4.3.4. Современная бизнес-модель 134
4.3.5. Анализ и выбор компонентов 135
4.3.6. Схемотехническое проектирование 135
4.3.7. Моделирование 136
4.3.8. Размещение компонентов на плате 137
4.3.9. Тестирование прототипа 137
4.3.10. Избранные практики проектирования 138
4.4. Сборка печатных плат 138
4.4.1. Технология монтажа в отверстия 139
4.4.2. Технология поверхностного монтажа 140
4.4.3. Увеличение сложности печатных плат: влияние на безопасность 140
4.5. Верификация печатных плат 142
4.5.1. Введение в инспекцию и тестирование печатных плат 143
4.5.2. Дефекты печатных плат 144
4.5.3. Инспекция печатных плат 144
4.5.4. Тестирование печатных плат 147
4.6. Практикум: атаки с использованием обратной инженерии 151
4.6.1. Цель 151
4.6.2. Метод 151
4.6.3. Получаемые знания/навыки 152
4.6.4. Дополнительные опции 152
4.7. Упражнения 152
4.7.1. Вопросы, предполагающие ответ «да» или «нет» 152
4.7.2. Вопросы, предполагающие короткий ответ 153
4.7.3. Вопросы, предполагающие развернутый ответ 153
Ссылки 154

Часть II. Атаки на аппаратуру: анализ, примеры и модели угроз 156

Глава 5. Аппаратные закладки 157
5.1. Введение 157
5.2. Проектирование систем на кристалле 158
5.2.1. Внедрение аппаратных закладок: потенциальные враги 160
5.3. Аппаратные закладки 160
5.3.1. Структура аппаратной закладки 161
5.3.2. Моделирование закладок 162
5.3.3. Примеры аппаратных закладок 162
5.4. Аппаратные закладки в ПЛИС 164

5.4.1. Характеристика активации 165
5.4.2. Характеристика работы 165
5.5. Классификация аппаратных закладок 166
5.5.1. Стадия внедрения 166
5.5.2. Уровни абстракции 168
5.5.3. Механизм активации 169
5.5.4. Влияние в результате работы 170
5.5.5. Расположение 171
5.6. Тесты доверия 172
5.6.1. Соглашение об именовании тестов 173
5.6.2. Примеры тестов на доверие 174
5.7. Противодействие аппаратным закладкам 176
5.7.1. Обнаружение закладок 176
5.7.2. Доверенное проектирование 183
5.8. Практикум: атаки с использованием аппаратных закладок 190
5.8.1. Цель 190
5.8.2. Метод 190
5.8.3. Результаты обучения 191
5.8.4. Углубленный практикум 191
5.9. Упражнения 191
5.9.1. Вопросы, предполагающие ответ «да» или«нет» 191
5.9.2. Вопросы, предполагающие развернутый ответ 191
5.9.3. Математические задачи 192
Ссылки 192

Глава 6. Жизненный цикл электроники 198

6.1. Введение 198
6.2. Жизненный цикл современной электроники 199
6.2.1. Проектирование 199
6.2.2. Производство 201
6.2.3. Сборка 202
6.2.4. Распространение 203
6.2.5. Срок службы 203
6.2.6. Окончание срока службы 203
6.3. Особенности жизненного цикла электронных компонентов 203
6.4. Проблемы безопасности 204
6.4.1. Аппаратные закладки 204
6.4.2. САПР 205
6.4.3. Ошибки в проектных моделях 206
6.4.4. Подсистемы тестирования и отладки 207
6.5. Вопросы доверия 209
6.5.1. Нелегальное использование СФ-блоков 210
6.5.2. Пиратство 210
6.5.3. Перепроизводство интегральных схем 211
6.5.4. Поставка некорректных и бракованных компонентов 213
6.5.5. Обратная инженерия ИС 213
6.5.6. Поддельная документация 213
6.5.7. Перемаркировка ИС 214
6.5.8. Переработка интегральных схем 215
6.6. Меры противодействия 217
6.6.1. Обнаружение и противодействие аппаратным закладкам 217

6.6.2. Проверка норм безопасности 217
6.6.3. Шифрование....218
6.6.4. Обфускация....219
6.6.5. Водяные знаки....220
6.6.6. Учет количества ИС....220
6.6.7. Проверка подлинности с использованием ECID и физически неклонируемых функций....221
6.6.8. Идентификационные отпечатки задержек распространения....221
6.6.9. Свипирование частоты....222
6.6.10. Схемы противодействия переработке кристаллов и ИС....223
6.6.11. Электрические тесты....224
6.6.12. Физическая инспекция....225
6.7. Упражнения....226
6.7.1. Вопросы, предполагающие ответ «да» или «нет»....226
6.7.2. Вопросы, предполагающие развернутый ответ....226
6.7.3. Математические задачи....227
Ссылки....228

Глава 7. Пиратство и обратная инженерия блоков аппаратуры....235

7.1. Введение....235
7.2. Заказные блоки аппаратуры....237
7.3. Безопасность систем, основанных на заказных блоках....238
7.3.1. Атаки с применением аппаратных закладок....239
7.3.2. Пиратство и нелегальное производство заказных блоков....240
7.3.3. Обратная инженерия....241
7.4. Безопасность ПЛИС....244
7.4.1. Введение в ПЛИС....245
7.4.2. Жизненный цикл системы на основе ПЛИС....247
7.5. Практикум: обратная инженерия и изменение схемы....255
7.5.1. Цель....255
7.5.2. Метод....255
7.5.3. Результаты обучения....255
7.5.4. Углубленный практикум....256
7.6. Упражнения....256
7.6.1. Вопросы, предполагающие ответ «да» или «нет»....256
7.6.2. Вопросы, предполагающие краткий ответ....256
7.6.3. Вопросы, предполагающие развернутый ответ....257
Ссылки....258

Глава 8. Атаки по сторонним каналам....261

8.1. Введение....261
8.2. Основы атак по сторонним каналам....263
8.2.1. Классификация атак по сторонним каналам....263
8.2.2. Нестандартные атаки на сторонние каналы....265
8.3. Атаки на основе анализа энергопотребления....265
8.3.1. Источники утечек через сторонние каналы энергопотребления....266
8.3.2. Получение сигналов энергопотребления....267
8.3.3. Типы анализа энергопотребления....268
8.3.4. Меры противодействия атакам на сторонние каналы по энергопотреблению....272
8.3.5. Атаки на сторонние каналы высоких порядков....273

8.3.6. Метрика безопасности при атаках через энергопотребление 274
8.4. Атаки через электромагнитный сторонний канал 275
8.4.1. Источник электромагнитных сигналов 275
8.4.2. Электромагнитное излучение 276
8.4.3. Считывание электромагнитных сигналов 277
8.4.4. Типы анализа электромагнитных излучений 278
8.4.5. Методы защиты от атаки, проводимой с помощью электромагнитного анализа 279
8.5. Атаки с внесением сбоя 279
8.5.1. Методы атак с внесением сбоя 282
8.5.2. Меры противодействия атакам с внесением сбоя 283
8.6. Атаки по времени выполнения операций 284
8.6.1. Атаки на временные характеристики в криптографическом оборудовании 284
8.6.2. Атака на временные характеристики работы кеш-памяти в процессоре 285
8.6.3. Меры противодействия атакам по времени выполнения операций 286
8.6.4. Метрики утечки по времени выполнения операций 287
8.7. Скрытые каналы 287
8.8. Практикум: атака по стороннему каналу 290
8.8.1. Цель 290
8.8.2. Метод 290
8.8.3. Результаты обучения 290
8.8.4. Углубленный практикум 291
8.9. Упражнения 291
8.9.1. Вопросы, предполагающие ответ «да» или «нет» 291
8.9.2. Вопросы, предполагающие краткий ответ 291
8.9.3. Вопросы, предполагающие развернутый ответ 292
Ссылки 293

Глава 9. Атаки с помощью тестов 295

9.1. Введение 295
9.2. Атаки с помощью цепей сканирования 296
9.2.1. Классификация атак с использованием цепей сканирования 297
9.2.2. Модели угроз 299
9.2.3. Модели угроз при тестировании на различных этапах жизненного цикла 300
9.2.4. Динамически обфусцированное сканирование 302
9.2.5. Недорогая безопасная цепь сканирования 305
9.2.6. Блокировка и ключ 309
9.2.7. Шифрование интерфейса сканирования 314
9.2.8. Обфусцированное сканирование 314
9.2.9. Переупорядочивание цепи сканирования 315
9.3. Атаки на основе JTAG 316
9.3.1. Взлом JTAG 318
9.3.2. Механизмы защиты JTAG 319
9.4. Практикум: атака через JTAG 320
9.4.1. Цель 320
9.4.2. Метод 320
9.4.3. Результаты обучения 320
9.4.4. Углубленный практикум 321
9.5. Упражнения 321
9.5.1. Вопросы, предполагающие ответ «да» или «нет» 321

9.5.2. Вопросы, предполагающие краткий ответ 321
9.5.3. Вопросы, предполагающие развернутый ответ 322
Ссылки 322

Глава 10. Физические атаки и контрмеры 326
10.1. Введение 326
10.2. Обратная инженерия 327
10.2.1. Оборудование 332
10.2.2. Обратная инженерия на уровне микросхемы 334
10.2.3. Защита микросхем от обратной инженерии 341
10.2.4. Обратная инженерия на уровне платы 344
10.2.5. Защита от обратной инженерии на уровне платы 350
10.2.6. Обратная инженерия на уровне системы 351
10.2.7. Защита от обратной инженерии на системном уровне 358
10.3. Зондирующая атака 364
10.3.1. Основы зондирующей атаки 366
10.3.2. Существующие меры защиты и ограничения 371
10.4. Атака на основе инвазивного внедрения ошибки 374
10.5. Упражнения 376
10.5.1. Вопросы, предполагающие ответ «да» или «нет» 376
10.5.2. Вопросы, предполагающие краткий ответ 376
10.5.3. Математические задачи 377
Ссылки 379

Глава 11. Атаки на печатные платы: уязвимости и угрозы безопасности 387
11.1. Введение 387
11.2. Проблемы безопасности печатных плат: атаки 390
11.2.1. Аппаратные закладки на уровне печатных плат 390
11.2.2 Модификация во время эксплуатации 393
11.2.3. Пиратство и подделка 395
11.3. Модели атак 396
11.3.1. Примеры атак 397
11.3.2. Модификация во время эксплуатации 401
11.4. Практикум: атака с отслеживанием назначения шины передачи данных 404
11.4.1. Цель 404
11.4.2. Метод 404
11.4.3. Результаты обучения 405
11.4.4. Углубленный практикум 405
11.5. Упражнения 405
11.5.1. Вопросы, предполагающие ответ «да» или «нет» 405
11.5.2. Вопросы, предполагающие краткий ответ 406
11.5.3. Вопросы, предполагающие развернутый ответ 406
Ссылки 407

Часть III. Контрмеры: предотвращение атак на аппаратуру 408

Глава 12. Примитивы аппаратной безопасности 409
12.1. Введение 409
12.2. Общие сведения 410

12.2.1. Основные примитивы аппаратной безопасности 410
12.2.2. Производительность КМОП-схем....411
12.2.3. Производительность и надежность vs безопасность 413
12.3. Физически неклонируемые функции....415
12.3.1. Общие сведения о физически неклонируемых функциях 415
12.3.2. Классификация физически неклонируемых функций 416
12.3.3. Качественные свойства физически неклонируемых функций 416
12.3.4. Архитектуры физически неклонируемых функций....417
12.3.5. Приложения физически неклонируемых функций 423
12.4. Генератор истинно случайных чисел....426
12.4.1. Общие сведения о генераторе истинно случайных чисел....426
12.4.2. Качественные свойства генераторов истинно случайных чисел 427
12.4.3. Архитектуры генераторов истинно случайных чисел 427
12.4.4. Применение генераторов истинно случайных чисел 431
12.5. Защита от подделок 432
12.5.1. Общие сведения о защите от подделок....432
12.5.2. Примеры защиты от подделок....433
12.6. Существующие уязвимости и атаки 435
12.6.1. Физически неклонируемые функции 435
12.6.2. Генераторы истинно случайных чисел....440
12.7. Примитивы на основе наноустройств 442
12.7.1. Структура физически неклонируемых функций на основе памяти с фазовым переходом 443
12.7.2. Физически неклонируемые функции на основе мемристоров и резистивной RAM-памяти....444
12.7.3. Физически неклонируемые функции на основе оперативной памяти с передачей спинового момента и магнитной оперативной памяти....445
12.7.4. Композиции физически неклонируемых функций для новых приложений....446
12.8. Практикум: примитивы аппаратной безопасности (физически неклонируемые функции и генераторы истинно случайных чисел)....447
12.8.1. Цель....447
12.8.2. Метод 447
12.8.3. Результаты обучения 448
12.8.4. Углубленный практикум 448
12.9. Упражнения 448
12.9.1. Вопросы, предполагающие ответ «да» или «нет»....448
12.9.2. Вопросы, предполагающие развернутый ответ 449
Ссылки 452

Глава 13. Оценка безопасности и доверенности. Проектирование с упором на безопасность....457

13.1. Введение 457
13.2. Активы и модели атак....459
13.2.1. Активы....459
13.2.2. Потенциальные атаки 461
13.2.3. Потенциальные злоумышленники....462
13.3. Допроизводственная оценка безопасности и доверенности СнК....464
13.3.1. Проверка правил безопасности проектирования 464
13.3.2. Рабочий процесс инфраструктуры DSeRC 475
13.4. Постпроизводственная безопасность и оценка доверенности ИС....477

13.4.1. Фаззинг....477
13.4.2. Негативное тестирование....478
13.4.3. Хакатоны....478
13.4.4. Тестирование проникновением....478
13.4.5. Функциональное тестирование элементов проекта с повышенными требованиями безопасности....480
13.4.6. Валидация детерминированных требований безопасности....481
13.5. Проектирование с упором на безопасность....481
13.5.1. Архитектура безопасности....481
13.5.2. Модуль проверки соблюдения политики безопасности....484
13.5.3. Проектирование с упором на устойчивость к атакам по сторонним каналам....485
13.5.4. Предотвращение внедрения аппаратных закладок....487
13.6. Упражнения....487
13.6.1. Вопросы, предполагающие ответ «да» или «нет»....487
13.6.2. Вопросы, предполагающие развернутый ответ....487
Ссылки....488

Глава 14. Обфускация аппаратуры....494

14.1. Введение....494
14.1.1. Предварительные сведения....496
14.1.2. Почему нельзя просто зашифровать аппаратные СФ-блоки?....497
14.2. Обзор методов обфускации....498
14.2.1. Обфускация на уровне регистровых передач....498
14.2.2. Обфускация на схемотехническом уровне....499
14.2.3. Обфускация на топологическом уровне....500
14.2.4. Обфускация системы команд....501
14.2.5. Обфускация печатной платы....502
14.3. Методы обфускации аппаратуры....502
14.3.1. Блокирование логики....502
14.3.2. Обфускация на основе камуфлирования вентилей....507
14.3.3. Обфускация на основе конечных автоматов....509
14.4. Перспективные методы обфускации....513
14.4.1. Обфускация битового потока ПЛИС....513
14.5. Использование обфускации для противодействия атакам с внедрением троянов....516
14.6. Практикум: обфускация аппаратного СФ-блока....517
14.6.1. Цель....517
14.6.2. Метод....518
14.6.3. Получаемые знания/навыки....518
14.6.4. Дополнительные возможности....518
14.7. Упражнения....518
14.7.1. Вопросы, предполагающие ответ «да» или «нет»....518
14.7.2. Вопросы, предполагающие краткий ответ....519
14.7.3. Вопросы, предполагающие развернутый ответ....519
Ссылки....521

Глава 15. Аутентификация печатных плат и проверка целостности....524

15.1 Аутентификация печатных плат....524
15.2. Источники изменений параметров процесса, используемые для генерации подписей....526

15.2.1. Изменения импеданса дорожек 527
15.2.2. Непостоянство времени задержки 528
15.2.3. Изменения, индуцированные конденсатором 529
15.2.4. Различия рельефа поверхности 531
15.3. Извлечение подписей и методы аутентификации 532
15.3.1. Использование вариаций импеданса печатной платы 533
15.3.2. Аутентификация на основе непостоянства времени задержки 534
15.3.3. Использование изменений, вызванных конденсатором 536
15.3.4. Аутентификация на основе различий рельефа поверхности 537
15.4. Метрики для оценки подписи 538
15.5. Другие методы аутентификации 540
15.5.1. Взаимная аутентификация на уровне системы 540
15.5.2. Аутентификация на основе резонансной частоты 541
15.6. Проверка целостности печатной платы 542
15.6.1. Проверка целостности на основе импеданса дорожек 542
15.6.2. Проверка целостности на основе JTAG 543
15.7. Практикум: вредоносная модификация печатной платы (мод-чип) 544
15.7.1. Цель 544
15.7.2. Метод 544
15.7.3. Получаемые знания/навыки 545
15.7.4. Углубленный практикум 545
15.8. Упражнения 545
15.8.1. Вопросы, предполагающие ответ «да» или «нет» 545
15.8.2. Вопросы, предполагающие краткий ответ 546
15.8.3. Вопросы, предполагающие развернутый ответ 546
Ссылки 547

Часть IV. Новые тенденции в атаках на аппаратуру и методах защиты 548

Глава 16. Атаки на системном уровне и меры противодействия 549

16.1. Введение 549
16.2. Устройство СнК 550
16.3. Требования безопасности СнК 551
16.3.1. Активы СнК 552
16.3.2. Потенциальные злоумышленники 552
16.3.3. Инфраструктура отладки в СнК 553
16.3.4. Политики безопасности СнК 553
16.4. Реализация политики безопасности 557
16.4.1. Централизованная архитектура безопасности 557
16.5. Проектирование безопасной СнК 560
16.5.1. Проверка безопасности на ранних этапах проектирования 560
16.5.2. Предпроизводственная проверка безопасности 561
16.5.3. Постпроизводственная проверка безопасности 562
16.5.4. Пример сценария: обеспечение безопасности информационного потока 562
16.6. Моделирование угроз 565
16.6.1. Аппаратные неисправности, вызванные программными средствами 567
16.6.2. Аппаратные закладки, управляемые программными средствами 573
16.6.3. Атаки по сторонним каналам, инициированные программными средствами 576
16.7. Практикум: политика безопасности СнК 582

16.7.1. Цель 582
16.7.2. Метод 582
16.7.3. Результаты обучения 582
16.7.4. Углубленный практикум 583
16.8. Упражнения 583
16.8.1. Вопросы, предполагающие ответ «да» или «нет» 583
16.8.2. Вопросы, предполагающие краткий ответ 584
16.8.3. Вопросы, предполагающие развернутый ответ 584
Ссылки 585

Приложение А. Платформа Hardware Hacking (HaHa) для выполнения практических заданий 588

A.1. О плате HaHa 594
A.1.1. Топология и компоненты 594
A.1.2. Блок-схема платы HaHa 596
A.1.3. Компоненты HaHa 598
A.2. Рекомендации по использованию 600
A.2.1. Подключение питания 600
A.2.2. Установка программных модулей на компьютер 601
A.2.3. Настройка ПЛИС Altera MAX 10 601
A.2.4. Настройка микроконтроллера через USB 602
A.2.5. Настройка источника напряжения 604
A.2.6. Соединение микросхем 604
A.2.7. Переключатели и светодиоды 605
A.2.8. 7-сегментный дисплей 606
A.2.9. Разъемы расширения 607
A.2.10. Генератор тактового сигнала 607
A.2.11. Подключение и использование SPI-устройств 608
A.2.12. Измерение параметров по сторонним каналам 609
A.3. Примеры программирования ПЛИС и микроконтроллера 610
A.3.1. Программирование ПЛИС 610
A.3.2. Программирование микроконтроллера 618
A.4. Спецификации проекта 625

ОТ ИЗДАТЕЛЬСТВА

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте *www.dmkpress.com*, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу *dmkpress@gmail.com*; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу *http://dmkpress.com/authors/publish_book/* или напишите в издательство по адресу *dmkpress@gmail.com*.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу *dmkpress@gmail.com*. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательство «ДМК Пресс» очень серьезно относится к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты *dmkpress@gmail.com*.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

ПРЕДИСЛОВИЕ

Перевод Сергея Козлова

Кибербезопасность стала темной стороной цифровой эпохи, а масштабы мировых проблем кибербезопасности превратились в ежедневные новости. В условиях конвергенции вычислительной техники и коммуникаций, а также экспоненциального роста объема данных в Интернете она остается все более актуальной и критически важной проблемой. Аппаратное обеспечение играет все более важную и неотъемлемую роль в кибербезопасности, поскольку многие возникающие уязвимости систем и приложений коренятся в аппаратном обеспечении, включая недавно обнаруженные уязвимости Meltdown и Spectre в различных микропроцессорах, представленных на рынке. Появление новых областей применения в режиме интернета вещей создает новые поверхности для атак и новые требования к аппаратному обеспечению для поддержки безопасных и надежных системных операций. Кроме того, разработка, производство и распространение интегральных схем (ИС), печатных плат (ПП, PCB), а также других компонентов электронного оборудования (пассивных или активных) становятся все более сложными и глобально распределенными, в которых участвует множество недоверенных организаций. Эта горизонтальная, но очень сложная цепочка поставок порождает огромное количество проблем с безопасностью аппаратного обеспечения, включая злонамеренные изменения, утечку информации, атаки по побочным каналам, контрафакт, реверс-инжиниринг и пиратство. Сокращение сроков выпуска на рынок систем на кристалле (СнК), которые служат основой многих современных вычислительных систем, еще больше усугубляет проблему, поскольку в конструкции остаются непреднамеренные уязвимости, которые могут быть использованы злоумышленниками после того, как микросхемы поступят в продажу.

Тема безопасности аппаратного обеспечения включает в себя широкий спектр вопросов, касающихся обеспечения безопасности и доверия; эти вопросы охватывают весь жизненный цикл электронной аппаратуры и все уровни абстракции (микросхемы, печатные платы, системы, а также системы систем). С увеличением числа вопросов, связанных с безопасностью, роль аппаратуры как якоря доверия вычислительных систем постоянно подвергается новым испытаниям. Поэтому крайне важно организовать эффективное и всестороннее образование в области безопасности аппаратного обеспечения на всех уровнях, включая студентов, аспирантов, а также специалистов, занимающихся проектированием и развертыванием вычислительных систем. Мы видим, что на рынке труда растет спрос на хорошо подготовленных специалистов в области безопасности аппаратного обеспечения. Насколько нам известно, учебные программы в колледжах и университетах не дают адекватного понимания полного спектра угроз аппаратуре и подходов к за-

щите от них. Как правило, существующие курсы не в состоянии обеспечить: (а) целостное обучение безопасности аппаратного обеспечения, которое охватывает безопасность на всех уровнях абстракции; (б) практический подход к обучению, который, по нашему мнению, имеет решающее значение для понимания уязвимостей сложной системы и соответствующих механизмов защиты. Чтобы удовлетворить эту растущую потребность в подготовке специалистов, мы взялись за создание первого в мире учебника, посвященного безопасности аппаратного обеспечения и доверию.

Цель этой книги – предоставить студентам старших курсов инженерных факультетов целостную подготовку и образование в области безопасности аппаратного обеспечения. Хотя книга ориентирована в первую очередь на студентов, она может послужить полезным справочником для аспирантов, исследователей и практиков в области безопасности, а также для профессионалов отрасли, включая инженеров-проектировщиков, инженеров по безопасности, системных архитекторов и руководителей служб безопасности. Книга содержит материал о предыстории современных вычислительных систем, за которым следует описание проблем безопасности и механизмов защиты. В книге также содержится набор хорошо спланированных экспериментов, которые можно провести в любой адекватно оборудованной лаборатории для изучения различных аспектов аппаратной безопасности, включающих в себя уязвимости, атаки и механизмы защиты. Чтобы помочь студентам понять компоненты современных систем до более глубокого погружения в конкретную предметную область безопасности, в справочных главах рассматриваются основы вычислительной техники, теория схем, активные и пассивные электронные компоненты, проектирование микросхем / печатных плат и организация испытаний.

Книга содержит описание уникального сопутствующего материала: аппаратной платформы, называемой платформой аппаратного взлома (HaHa – *Hardware Hacking*), с помощью которой легко смоделировать аппаратно-программную систему и корректно «взломать» ее, чтобы изучить различные проблемы аппаратной безопасности и меры противодействия. Все практические эксперименты, представленные в данной книге, могут быть реализованы на этой платформе, хотя для выполнения некоторых экспериментов также можно использовать альтернативные аппаратные модули, например отладочные платы с программируемыми логическими интегральными схемами (ПЛИС/FPGA)[1]. Всестороннее освещение концепций аппаратной безопасности вкупе со справочными материалами, а также практический подход к обучению являются ключевыми отличительными особенностями этого учебника, которые, по нашему мнению, необходимы для подготовки студентов к решению современных проблем аппаратной безопасности.

---

[1] FPGA – ППВМ (программируемая пользователем вентильная матрица), наряду с CPLD и проч. одна из разновидностей ПЛИС (PLD, programmable logic device); поскольку вопросы аппаратной безопасности, поднятые авторами книги, касаются не только ППВМ, здесь и далее был выбран более расширительный перевод. – *Прим. перев.*

Уникальные особенности этого учебника

В нем представлен подробный обзор компьютерного оборудования, включая основы вычислительных систем и связанные с ними риски безопасности, исследования известных методологий атак и контрмер, а также тематические исследования. Ожидается, что на этой основе читатели получат глубокое понимание ключевых концепций, которые облегчат для них распознавание и противодействие угрозам безопасности аппаратуры в реальных продуктах и системных архитектурах.

Каждая важная тема в области аппаратной безопасности (уязвимости, атаки и подходящие механизмы защиты) излагается подробно и сопровождается хорошо продуманным практическим экспериментом.

В книгу включено описание специальной электронной аппаратной платформы НаНа, созданной авторами книги для выполнения вышеупомянутых лабораторных упражнений. Этот аппаратный модуль специально разработан для иллюстрации различных ключевых концепций на одной платформе. Описания экспериментов предоставляются в качестве сопроводительного материала, который включает пошаговые описания процесса экспериментирования, наблюдений, формата отчетов и дополнительных параметров.

Каждая глава также сопровождается набором упражнений, разделенных на три группы по уровню сложности. Эти задачи помогут читателю эффективно понять концепции, обсуждаемые в главе.

Организация книги

Основываясь на десятилетнем опыте преподавания аппаратной безопасности, авторы составили темы так, чтобы наиболее эффективно передать соответствующие концепции. Глава 1 представляет собой введение в тему аппаратной безопасности. В ней обсуждаются предварительные и базовые концепции по основным темам, например векторы аппаратных атак, поверхности атак, модель противника, причины аппаратных атак и их влияние на экономические и бизнес-модели, цепочка поставок оборудования, а также связь между безопасностью и доверием. В этой главе также описана краткая история аппаратной безопасности, дан обзор литературы и лабораторных исследований.

Остальной материал книги поделен на 4 части:

- часть I «Базовые сведения в области электронной аппаратуры»;
- часть II «Атаки на аппаратуру: анализ, примеры и модели угроз»;
- часть III «Контрмеры: предотвращение атак на аппаратуру»;
- часть IV «Новые тенденции в атаках на аппаратуру и методах защиты».

Часть I «Базовые сведения в области электронной аппаратуры» состоит из трех глав. Глава 2 посвящена основам цифровой логики, теории схем, встроенных систем, интегральных схем (ИС), специализированных ИС (ASIC), ПЛИС (FPGA), печатных плат, встроенного программного обеспечения, взаимодействия аппаратного, встроенного программного и программного обеспечения, а также роли аппаратного обеспечения в системной

Конец ознакомительного фрагмента.
Приобрести книгу можно
в интернет-магазине
«Электронный универс»
e-Univers.ru