

УДК 004.738.5  
ББК 32.372  
Ч18

*Спасибо за помощь в подготовке книги  
Юрию Владимировичу Потапову,  
техническому директору ООО «Евроинтех»*

**Чанцис Ф., Стаис И., Кальдерон П., Деирменцоглу Е., Вудс Б.**  
Ч18 Практический хакинг интернета вещей / пер. с англ. Л. Н. Акулич. – М.: ДМК Пресс, 2022. – 480 с.: ил.

**ISBN 978-5-97060-974-3**

Устройств, управляемых через интернет, с каждым годом становится больше, но не все грамотно оценивают сопутствующие риски. Из этой книги читатель узнает, каким образом подключать умную технику у себя дома и на предприятиях, чтобы наилучшим образом себя обезопасить. Авторы подробно описывают уязвимости в сфере интернета вещей (IoT), моделируют угрозы и представляют эффективную методологию тестирования умных устройств – от инфузионной помпы до беговой дорожки. Практические упражнения научат вовремя распознавать угрозы и предотвращать атаки злоумышленников.

Издание будет полезно тестировщикам безопасности, системным администраторам, а также разработчикам и пользователям IoT-систем.

УДК 004.738.5  
ББК 32.372

Copyright © 2021 by Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, Beau Woods. Title of English-language original: *Practical IoT Hacking: The Definitive Guide to Attacking the Internet of Things*, ISBN 9781718500907, published by No Starch Press Inc. 245 8th Street, San Francisco, California United States 94103. The Russian-Language 1st edition Copyright © 2022 by DMK Press Publishing under license by No Starch Press Inc. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-7185-0090-7 (англ.)

ISBN 978-5-97060-974-3 (рус.)

© Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods, 2021  
© Перевод, издание, оформление, ДМК Пресс, 2022

# СОДЕРЖАНИЕ

<i>От издательства</i> .....	14
<i>Об авторах</i> .....	15
<i>О соавторах</i> .....	16
<i>О техническом обозревателе</i> .....	17
<i>Вступительное слово</i> .....	18
<i>Благодарности</i> .....	20
<i>Предисловие</i> .....	21

## Часть I УГРОЗЫ В МИРЕ ИНТЕРНЕТА ВЕЩЕЙ

<b>1. Безопасность интернета вещей</b> .....	27
Почему важна защита интернета вещей? .....	28
Чем защита интернета вещей отличается от традиционной ИТ-защиты?.....	30
В чем особенность взлома интернета вещей?.....	31
Методики, стандарты и инструкции.....	32
Пример: обнаружение проблемы безопасности, связанной с интернетом вещей, составление отчета и информирование .....	36
Мнения экспертов: навигация в среде интернета вещей .....	38
Законы хакинга интернета вещей.....	38
Роль правительства в безопасности интернета вещей .....	40
Взгляд пациентов на безопасность медицинских устройств .....	41
Заключение.....	43
<b>2. Моделирование угроз</b> .....	44
Моделирование угроз для интернета вещей.....	44
Схема моделирования угроз.....	45
Определение архитектуры .....	46
Разбивка архитектуры на компоненты.....	47
Выявление угроз .....	49
Использование деревьев атак для обнаружения угроз .....	57

Оценка угроз с помощью схемы классификации DREAD .....	58
Другие типы моделирования угроз, структуры и инструменты.....	59
Распространенные угрозы интернета вещей.....	60
Атаки с подавлением сигнала .....	60
Атаки с воспроизведением .....	60
Атаки со взломом настроек.....	61
Атаки на целостность оборудования .....	61
Клонирование узла.....	61
Нарушения безопасности и конфиденциальности .....	62
Осведомленность пользователей о безопасности.....	62
Заключение .....	62

### **3. Методология тестирования безопасности .....** 63

Пассивная разведка .....	65
Физический или аппаратный уровень.....	68
Периферийные интерфейсы.....	68
Среда загрузки.....	69
Блокировки .....	70
Предотвращение и обнаружение несанкционированного доступа.....	70
Прошивка.....	70
Интерфейсы отладки .....	71
Физическая устойчивость.....	71
Сетевой уровень .....	72
Разведка .....	72
Атаки на сетевой протокол и службы .....	75
Тестирование беспроводного протокола.....	77
Оценка веб-приложений .....	77
Картирование приложений.....	78
Элементы управления на стороне клиента.....	79
Аутентификация .....	79
Управление сеансом.....	80
Контроль доступа и авторизация.....	80
Проверка ввода .....	80
Логические ошибки.....	81
Сервер приложений .....	81
Исследование конфигурации хоста .....	81
Учетные записи пользователей .....	81
Надежность пароля .....	82
Привилегии учетной записи.....	82
Уровни патчей.....	83
Удаленное обслуживание.....	84
Управление доступом к файловой системе .....	84
Шифрование данных .....	85
Неверная конфигурация сервера.....	85
Мобильное приложение и облачное тестирование .....	85
Заключение .....	86

## Часть II ВЗЛОМ СЕТИ

<b>4. Оценка сети</b> .....	89
Переход в сеть IoT .....	89
VLAN и сетевые коммутаторы .....	90
Спуфинг коммутатора .....	91
Двойное тегирование .....	94
Имитация устройств VoIP .....	95
Идентификация устройств IoT в сети .....	98
Обнаружение паролей службами снятия отпечатков .....	98
Написание новых инструментов зондирования служб Nmap .....	103
Атаки MQTT .....	105
Настройка тестовой среды .....	106
Написание модуля MQTT Authentication-Cracking в Ncrack .....	109
Тестирование модуля Ncrack на соответствие MQTT .....	119
Заключение .....	120
 <b>5. Анализ сетевых протоколов</b> .....	121
Проверка сетевых протоколов .....	122
Сбор информации .....	122
Анализ .....	124
Создание прототипов и разработка инструментов .....	125
Проведение оценки безопасности .....	126
Разработка диссектора Wireshark для протокола DICOM на языке Lua .....	127
Работа с Lua .....	128
Общие сведения о протоколе DICOM .....	128
Генерация трафика DICOM .....	129
Включение Lua в Wireshark .....	130
Определение диссектора .....	131
Определение основной функции диссектора .....	132
Завершение диссектора .....	133
Создание диссектора C-ECHO .....	134
Извлечение строковых значений заголовков объектов приложения .....	135
Начальная загрузка данных функции диссектора .....	135
Анализ полей переменной длины .....	136
Тестирование диссектора .....	137
Разработка сканера служб DICOM для механизма сценариев Nmap .....	138
Написание библиотеки сценариев Nmap для DICOM .....	138
Коды и константы DICOM .....	139
Написание функций создания и уничтожения сокетов .....	140
Определение функций для отправки и получения пакетов DICOM .....	141
Создание заголовков пакетов DICOM .....	142
Написание запросов контекстов сообщений A-ASSOCIATE .....	143
Чтение аргументов скрипта в движке сценариев Nmap .....	145
Определение структуры запроса A-ASSOCIATE .....	146
Анализ ответов A-ASSOCIATE .....	147
Создание окончательного сценария .....	148

Заключение .....	149
<b>6. Использование сети с нулевой конфигурацией .....</b>	<b>150</b>
Использование UPnP .....	151
Стек UPnP .....	152
Распространенные уязвимости UPnP .....	154
Проникаем сквозь лазейки в файрволе .....	155
Злоупотребление UPnP через интерфейсы WAN .....	161
Другие атаки UPnP .....	165
Использование mDNS и DNS-SD .....	166
Как работает mDNS .....	167
Как работает DNS-SD .....	167
Проведение разведки с помощью mDNS и DNS-SD .....	168
Злоупотребление на этапе проверки mDNS .....	170
Атаки «человек посередине» на mDNS и DNS-SD .....	171
Использование WS-Discovery .....	181
Как работает WS-Discovery .....	181
Подделка камер в вашей сети .....	183
Создание атак WS-Discovery .....	189
Заключение .....	190

## Часть III ВЗЛОМ АППАРАТНОЙ ЧАСТИ СИСТЕМЫ

<b>7. Уязвимости портов UART, JTAG и SWD .....</b>	<b>192</b>
UART .....	193
Аппаратные средства для связи с UART .....	194
Как найти порты UART .....	194
Определение скорости передачи UART .....	198
JTAG и SWD .....	199
JTAG .....	199
Как работает SWD .....	200
Аппаратные средства для взаимодействия с JTAG и SWD .....	201
Идентификация контактов JTAG .....	201
Взлом устройства с помощью UART и SWD .....	203
Целевое устройство STM32F103C8T6 (Black Pill) .....	205
Настройка среды отладки .....	205
Кодирование целевой программы на Arduino .....	208
Запись и запуск программы Arduino .....	210
Отладка целевого устройства .....	218
Заключение .....	226
<b>8. SPI и I<sup>2</sup>C .....</b>	<b>227</b>
Оборудование для связи с SPI и I2C .....	228
SPI .....	229
Как работает SPI .....	229
Извлечение содержимого микросхем флеш-памяти EEPROM с SPI .....	230

I <sup>2</sup> C .....	235
Как работает I <sup>2</sup> C.....	235
Настройка архитектуры шины I <sup>2</sup> C типа «контроллер–периферия» .....	236
Атака на I <sup>2</sup> C с помощью Bus Pirate.....	241
Заключение.....	244

## 9. Взлом прошивки.....245

Прошивка и операционные системы .....	245
Получение доступа к микропрограмме.....	246
Взлом маршрутизатора Wi-Fi.....	250
Извлечение файловой системы .....	251
Статический анализ содержимого файловой системы .....	252
Эмуляция прошивки .....	255
Динамический анализ .....	261
Внедрение бэкдора в прошивку .....	264
Нацеливание на механизмы обновления микропрограмм .....	269
Компиляция и установка .....	270
Код клиента .....	270
Запуск службы обновления .....	274
Уязвимости служб обновления микропрограмм.....	274
Заключение.....	277

## Часть IV ВЗЛОМ РАДИОКАНАЛОВ

### 10. Радио ближнего действия: взлом rFID .....279

Как работает RFID.....	280
Радиочастотные диапазоны.....	280
Пассивные и активные технологии RFID .....	281
Структура меток RFID.....	282
Низкочастотные метки RFID.....	284
Высокочастотные RFID-метки.....	285
Атака на RFID-системы с помощью Proxmark3.....	286
Настройка Proxmark3.....	286
Обновление Proxmark3.....	287
Определение низко- и высокочастотных карт .....	289
Клонирование низкочастотных меток.....	290
Клонирование высокочастотных меток.....	291
Имитация RFID-метки.....	296
Изменение содержимого RFID-меток .....	297
Атака на MIFARE с помощью приложения для Android .....	298
Команды RAW для небрендируемых или некоммерческих RFID-тегов .....	299
Подслушивание обмена данными между меткой и считывателем .....	303
Извлечение ключа сектора из перехваченного трафика .....	304
Атака путем подделки RFID .....	305
Автоматизация RFID-атак с помощью механизма скриптов Proxmark3.....	306

Пользовательские сценарии использования RFID-фаззинга .....	307
Закключение .....	312
<b>11. Bluetooth Low Energy (BLE)</b> .....	313
Как работает BLE .....	314
Общий профиль доступа и общий профиль атрибутов .....	316
Работа с BLE .....	317
Необходимое оборудование BLE .....	317
BlueZ .....	318
Настройка интерфейсов BLE .....	318
Обнаружение устройств и перечисление характеристик .....	319
GATTTool .....	319
Bettercap .....	320
Получение перечня характеристик, служб и дескрипторов .....	321
Чтение и запись характеристик .....	322
Взлом BLE .....	323
Настройка BLE CTF Infinity .....	324
Приступаем к работе .....	324
Флаг 1. Исследование характеристик и дескрипторов .....	326
Флаг 2. Аутентификация .....	328
Флаг 3. Подмена вашего MAC-адреса .....	329
Закключение .....	331
<b>12. Радиоканалы средней дальности: взлом Wi-Fi</b> .....	332
Как работает Wi-Fi .....	332
Оборудование для оценки безопасности Wi-Fi .....	333
Атаки Wi-Fi на беспроводные клиенты .....	334
Деаутентификация и атаки «отказ в обслуживании» .....	334
Атаки на Wi-Fi путем подключения .....	337
Wi-Fi Direct .....	342
Атаки на точки доступа Wi-Fi .....	345
Взлом WPA/WPA2 .....	346
Взлом WPA/WPA2 Enterprise для сбора учетных данных .....	352
Методология тестирования .....	353
Закключение .....	354
<b>13. Радио дальнего действия: LPWAN</b> .....	355
LPWAN, LoRa и LoRaWAN .....	356
Захват трафика LoRa .....	357
Настройка платы разработки Heltec LoRa 32 .....	358
Настройка LoStik .....	363
Превращаем USB-устройство CatWAN в sniffер LoRa .....	367
Декодирование протокола LoRaWAN .....	372
Формат пакета LoRaWAN .....	372
Присоединение к сетям LoRaWAN .....	374

Атаки на LoRaWAN .....	377
Атаки с заменой битов .....	377
Генерация ключей и управление ими .....	380
Атаки воспроизведения .....	381
Подслушивание .....	382
Подмена ACK .....	382
Атаки, специфичные для приложений .....	382
Заключение .....	382

## Часть V АТАКИ НА ЭКОСИСТЕМУ IoT

<b>14. Взлом мобильных приложений .....</b>	<b>385</b>
Угрозы в мобильных приложениях интернета вещей .....	386
Разбивка архитектуры на компоненты .....	386
Выявление угроз .....	386
Средства управления безопасностью Android и iOS .....	389
Защита данных и зашифрованная файловая система .....	390
Тестовая среда приложения, безопасный IPC и службы .....	390
Подписи приложений .....	391
Аутентификация пользователя .....	391
Управление изолированными аппаратными компонентами и ключами .....	391
Проверенная и безопасная загрузка .....	392
Анализ приложений iOS .....	392
Подготовка среды тестирования .....	393
Извлечение и повторная подпись IPA .....	394
Статический анализ .....	395
Динамический анализ .....	398
Атаки путем инъекции .....	406
Хранилище связки ключей .....	407
Реверс-инжиниринг двоичного кода .....	408
Перехват и изучение сетевого трафика .....	410
Обход механизма обнаружения джейлбрейка с помощью динамического патча .....	411
Как обойти обнаружение джейлбрейка с помощью статического патча .....	412
Анализ приложений Android .....	414
Подготовка тестовой среды .....	414
Извлечение файла APK .....	415
Статический анализ .....	416
Обратная конвертация двоичных исполняемых файлов .....	417
Динамический анализ .....	418
Перехват и анализ сетевого трафика .....	423
Утечки по побочным каналам .....	423
Обход защиты от root-доступа с помощью статического патча .....	424
Обход защиты от root-доступа с помощью динамического патча .....	426
Заключение .....	426



<b>15. Взлом умного дома</b>	428
Физический доступ в здание	429
Клонирование RFID-метки умного дверного замка	429
Глушение беспроводной сигнализации	432
Воспроизведение потока с IP-камеры	437
Общие сведения о протоколах потоковой передачи	437
Анализ сетевого трафика IP-камеры	438
Извлечение видеопотока	439
Атака на умную беговую дорожку	443
Умные беговые дорожки и операционная система Android	444
Перехват управления интеллектуальной беговой дорожкой на базе Android	446
Заключение	460
<i>Инструменты для взлома интернета вещей</i>	461
<i>Предметный указатель</i>	476