Посвящается Клайди и Миранте

СОДЕРЖАНИЕ

Часть II ВЗЛОМ СЕТИ

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. Издательства «ДМК Пресс» и No Starch Press очень серьезно относятся 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.

Об авторах

Фотиос (Фотис) Чанцис (@ithilgore) работает над безопасным и надежным общим искусственным интеллектом (AGI) в OpenAI. Прежде он занимал должность главного инженера по информационной безопасности в Mayo Clinic, где проводил техническую оценку безопасности медицинских устройств, систем клинической поддержки и критически важной инфраструктуры здравоохранения. С 2009 года входил в основную команду разработчиков Nmap, написал Ncrack под руководством Гордона «Федора» Лайона, автора исходной версии Nmap, в ходе инициативной программы Google Summer of Code. Впоследствии выступал наставником в проекте Nmap во время Google Summer of Code 2016 и 2017 года, создал видеокурс по Nmap. Исследование сетевой безопасности Фотиса Чанциса включает использование TCP Persist Timer (вы можете найти его статью по теме, опубликованную в Phrack № 66) и изобретение скрытой атаки со сканированием портов путем злоупотребления протоколом XMPP. Фотис участвовал в различных конференциях по безопасности, включая DEF CON. Основные его работы представлены на его сайте *https://sock-raw.org/*.

Иоаннис Стаис (@Einstais) – старший исследователь в области ИТ-безопасности и руководитель красной команды CENSUS S.A. – компании, предлагающей специализированные услуги в области кибербезопасности клиентам по всему миру. Иоаннис участвовал более чем в 100 проектах по оценке безопасности, включая оценку протоколов связи, сетевых и мобильных банковских услуг, платежных систем NFC, банкоматов и систем точек продаж, критически значимого медицинского оборудования и решений MDM. Получил степень магистра в области компьютерных систем в Афинском университете. В настоящее время исследования Иоанниса сосредоточены на разработке алгоритмов машинного обучения для улучшения анализа уязвимостей, на усовершенствовании фреймворков для исследования уязвимостей методом грубой силы и изучении современных угроз мобильным и веб-приложениям. Иоаннис Стаис представлял свои исследования на конференциях по безопасности, таких как Black Hat Europe, Troopers NGI и Security BSides Athens.

О соавторах

Паулино Кальдерон (@calderpwn) – автор публикаций и международный спикер, более 12 лет работающий в области безопасности сетей и приложений. Он выступает на конференциях по безопасности и вместе со специалистами Websec – фирмы, основанной им в 2011 году – консультирует компании из списка Fortune 500, а свободное от работы время проводит в блаженном отдыхе на пляжах Косумеля (Мексика). Паулино – большой почитатель программного обеспечения с открытым исходным кодом и участвовал во многих проектах, включая Nmap, Metasploit, OWASP Mobile Security Testing Guide (MSTG), OWASP Juice Shop и OWASP IoT Goat.

Евангелос Деирменцоглу (@edeirme) – специалист по информационной безопасности, интересующийся решением масштабных проблем защиты. Руководил работой по обеспечению кибербезопасности финансового технологического стартапа Revolut. Член Сообщества свободно распространяемого ПО с 2015 года; внес вклад в разработку Nmap и Ncrack. В настоящее время пишет диссертацию по кибербезопасности, уделяя особое внимание анализу исходного кода, который он применял в работе со многими крупными поставщиками технологий США, компаниями из списка Fortune 500, финансовыми и медицинскими учреждениями.

Бо Вудс (@beauwoods) – научный сотрудник по инновациям в области кибербезопасности в Атлантическом совете, лидер движения I Am The Cavalry. Основатель и генеральный директор Stratigos Security; входит в правление ряда некоммерческих организаций. В своей работе, которая призвана наладить контакт между сообществами, занимающимися исследованием безопасности, и сообществами публичных политик, он стремится к тому, чтобы любая сетевая технология, способная укрепить безопасность человека, заслуживала доверия. В прошлом сотрудник Управления по санитарному надзору за качеством пищевых продуктов и медикаментов США, главный управляющий консультант Dell SecureWorks. Последние несколько лет проводит консультации в сфере энергетики, здравоохранения, автомобилестроения, авиации, железнодорожного транспорта и интернета вещей; сотрудничает с исследователями кибербезопасности, разработчиками ИТ-политик и Белым домом. Является автором ряда публикаций, часто выступает на публичных мероприятиях.

О техническом обозревателе

Аарон Гусман (Aaron Guzman) – один из авторов «Руководства по тестированию безопасности интернета вещей», технический руководитель группы безопасности Cisco Meraki. В рамках проектов OWASP IoT и Embedded Application Security возглавляет инициативы с открытым исходным кодом, которые повышают осведомленность о стратегиях защиты интернета вещей и тем самым снижают порог входа в отрасль защиты IoT для специалистов. Аарон Гусман – сопредседатель рабочей группы Cloud Security Alliance по IoT и технический рецензент ряда книг по безопасности интернета вещей. Имеет широкий опыт публичных выступлений, проводя презентации на конференциях, тренинги и семинары по всему миру. Следите за исследованиями Аарона в Твиттере: @scriptingxss.

ВСТУПИТЕЛЬНОЕ СЛОВО

Современные программы безопасности предназначены для борьбы с традиционными угрозами на предприятии. Но технологии развиваются с такой скоростью, что выявлять утечку данных организации становится все труднее.

Рождение интернета вещей в одночасье превратило традиционные производственные предприятия в компании по разработке программного обеспечения. Они начали комбинировать интегрированное аппаратное обеспечение и ПО для повышения эффективности своих продуктов, обновлений, простоты использования и ремонтопригодности. Используемые, как правило, в важных инфраструктурах – дома или в корпоративных сетях, – эти устройства предоставили новый ряд функций и приспособлений, облегчающих нашу жизнь.

Однако эти «черные ящики» принесли нам и новые испытания. Созданные специалистами, продумывающими лишь техническую сторону, они почти не интегрируются в систему безопасности. Они подвергли нашу жизнь новым угрозам и предоставили входы в инфраструктуру, которой раньше не было. Такие устройства до сих пор практически не отслеживаются и содержат ряд уязвимостей, так что мы часто не замечаем вторжения в их работу. При выявлении угроз организации подобные устройства не принимаются в расчет – часто их даже не отмечают в списке оборудования, подлежащего внутренней проверке безопасности.

«Практический хакинг интернета вещей» – это не просто очередная книга по безопасности: здесь обсуждается философия тестирования безопасности и показывается, как нам нужно изменить свое отношение к подключению техники у себя дома и на предприятиях, чтобы наилучшим образом себя обезопасить. Многие компании-производители не учитывают вопросов безопасности при разработке, а в результате создаваемые системы очень уязвимы для атак. Такие

устройства можно найти почти в каждой сфере нашей жизни. Интернет вещей влияет на все отрасли и компании, создавая риск, с которым большинство организаций не в состоянии справиться.

Большинство людей не вполне понимает, какие риски таят в себе устройства интернета вещей. Принято считать, что раз они не содержат конфиденциальной информации, то и не критичны для компании. На самом деле злоумышленники используют эти устройства в качестве скрытых каналов в сети, которые остаются незамеченными в течение долгого времени и ведут непосредственно к уязвимым данным. Приведу пример из личной практики. Недавно я участвовал в расследовании инцидента на крупном производственном предприятии. Мы обнаружили, что злоумышленники проникли в организацию через программируемый логический контроллер (ПЛК). Один из заводов-производителей привлекал стороннего подрядчика для изготовления устройств, и злоумышленники получили доступ к системам этого подрядчика. В результате более двух лет они могли распоряжаться всей информацией о клиентах и данными компании, о чем никто не догадывался.

ПЛК был точкой входа в остальную часть сети и в конечном счете открывал прямой доступ ко всем системам исследований и разработок компании, которые содержали большую часть интеллектуальной собственности и уникальных данных. Атака была обнаружена только потому, что один из злоумышленников по небрежности сбросил имена пользователей и пароли контроллера домена, что вызвало случайный сбой системы, потребовавший расследования.

Авторы книги «Практический хакинг интернета вещей» в первую очередь фокусируются на понимании рисков и уязвимостей, моделируя угрозы и описывая эффективную методологию тестирования устройств интернета вещей. Книга повествует о хакинге оборудования, сети, радио и всей инфраструктуры интернета вещей, а также о том, как анализировать выявленные риски путем технической оценки устройств. При описании методов тестирования устройств, входящих в систему интернета вещей, подробно рассказывается, что нужно для создания программы тестирования в организации и как проводить проверку. Эта книга призвана изменить методы оценки безопасности в большинстве организаций и помочь лучше понять риски – тестирование устройств интернета вещей рассматривается как часть этого процесса.

Рекомендую книгу всем техническим специалистам, которые производят устройства интернета вещей, а также всем, кто пользуется таковыми дома или на предприятии. Поскольку безопасность систем и защита информации сегодня важны как никогда, актуальность этой книги очевидна. Я искренне рад ее появлению, учитывая, какая работа за этим стоит, и уверен, что она поспособствует разработке более безопасной инфраструктуры интернета вещей в будущем.

Дэйв Кеннеди,
основатель TrustedSec, Binary Defense

БЛАГОДАРНОСТИ

Мы хотим поблагодарить Фрэнсис Сокс и других сотрудников издательства No Starch Press, которые приняли участие в работе над книгой. Также благодарим Аарона Гусмана за подробный технический обзор содержания. Мы признательны Сальвадору Мендоса за помощь в подготовке главы о RFID. Отдельная благодарность Джорджу Чатзисофронио за освещение ряда концепций в главе о Wi-Fi.

Спасибо Фонду электронных рубежей (EFF) за ценную юридическую консультацию в ходе написании книги. Наконец, мы хотим отметить вклад Харли Гейгера, Дэвида Роджерса, Мари Мо и Джея Рэдклиффа, которые поделились своими соображениями по теме в главе 1, и Дэйва Кеннеди, написавшего вступительное слово.

ПРЕДИСЛОВИЕ

Наша зависимость от технологий растет более быстрыми темпами, чем наша способность защитить их. Технологии, которые, как мы знаем, не застрахованы от вторжения злоумышленников, каждый день везут нас на работу, обслуживают медучреждения, наблюдают за нашими домами… Как доверять этим устройствам, если они не вполне надежны?

Аналитик по кибербезопасности Керен Элазари сказала, что хакеры – это «иммунная система цифровой эры». Нам нужны технически подкованные люди, которые могут выявлять уязвимости и информировать и защищать общество от ущерба, связанного со взломом интернет-систем. Никогда еще эта работа не была настолько актуальна: слишком немногие располагают необходимыми знаниями, навыками и инструментами[1].

Эта книга призвана укрепить иммунную систему общества, чтобы лучше защитить всех нас.

Подход, принятый в книге

Хакинг в сфере интернета вещей – очень широкая тема, и в книге используется практический подход к ней. Мы фокусируемся на концепциях и методах, которые помогут вам быстро приступить к тес-

---

[1] Россия принимает активное участие в развитии международной экосистемы интернета вещей. В феврале 2022 г. официально опубликован первый международный стандарт промышленного интернета вещей, разработка которого велась по инициативе «Ростелекома» на базе технического комитета (ТК) по стандартизации 194 «Кибер-физические системы» Росстандарта при поддержке Минпромторга России. Стандарт станет платформой для развития Национальной технологической инициативы (НТИ) и цифровой экономики. Его утверждение состоялось на уровне ключевых организаций — Международной организации по стандартизации и Международной электротехнической комиссии (ISO/IEC). *https://iotas.ru/media/day_theme/1365/*.

тированию реальных систем, протоколов и устройств интернета вещей. Мы специально выбрали для примера инструменты и уязвимые устройства, широко распространенные и доступные по цене, чтобы вы могли практиковаться самостоятельно.

Мы также подготовили образцы кода и эксплойты, с которыми вы можете поэкспериментировать. Они доступны на веб-сайте книги по адресу *https://nostarch.com/practical-iot-hacking/*. Для удобства изучения некоторые упражнения сопровождаются образами виртуальных машин. В некоторых главах мы ссылаемся на популярные примеры с открытым исходным кодом, которые легко найти в интернете.

Перед вами не руководство по применению средств для взлома интернета вещей – книга не охватывает все аспекты безопасности интернета вещей, поскольку для этого понадобился бы труд куда большего масштаба. Поэтому мы взяли для рассмотрения самые основные методы взлома оборудования, включая взаимодействие с UART, I^2C, SPI, JTAG и SWD. Мы анализируем различные сетевые протоколы интернета вещей, уделяя особое внимание тем, которые не просто важны, но и мало исследовались ранее. Среди них UPnP, *WS-Discovery*, mDNS, DNS-SD, RTSP / RTCP / RTP, LoRa / LoRaWAN, Wi-Fi и Wi-Fi Direct, RFID и NFC, BLE, MQTT, CDP и DICOM. Также мы обсуждаем реальные примеры, с которыми сталкивались в ходе профессионального тестирования.

Для кого предназначена эта книга

Не существует двух людей с одинаковыми воззрениями и опытом. Между тем анализ устройств интернета вещей требует навыков практически во всех областях, потому что эти устройства сочетают в себе вычислительную мощность и возможности подключения в самом разном рабочем окружении. Мы не можем предугадать, какие главы и фрагменты книги читатель сочтет наиболее интересными. Но полагаем, что предоставление этих знаний широким слоям населения обеспечит больший контроль пользователей над стремительно цифровизирующимся миром.

Мы написали книгу для тех, кто профессионально занимается взломом и проникновением в системы (так называемых тестировщиков безопасности), но ожидаем, что она будет полезна и другим людям:

- **исследователь систем безопасности** может использовать книгу как справочник, разбираясь с незнакомыми протоколами, структурами данных, компонентами и концепциями инфраструктуры интернета вещей;
- **системный администратор** предприятия узнает, как лучше защитить рабочую среду и активы своей организации;
- **менеджер по продукции** ознакомится с новыми ожиданиями клиентов в отношении устройств интернета вещей и сможет учесть это при разработке, уменьшив стоимость продукта и сократив время его вывода на рынок;

- **специалист по оценке безопасности** откроет для себя новые навыки, чтобы лучше обслуживать клиентов;
- **любознательный студент** найдет знания, которые помогут ему выстроить карьеру в области, связанной с защитой людей.

Настоящая книга написана в расчете на то, что читатель умеет работать с командной строкой Linux, знаком с сетевыми концепциями TCP/IP и кодированием. При необходимости вы можете обратиться к дополнительным материалам по взлому аппаратного обеспечения, таким как книга *The Hardware Hacking Handbook* (Colin O'Flynn, Jasper van Woudenberg; готовится к выходу в издательстве No Starch Press). Ссылки на дополнительную литературу вы встретите ниже в некоторых главах.

Kali Linux

В большинстве упражнений, представленных в книге, используется Kali Linux – самый популярный дистрибутив Linux для тестирования на взлом. Kali поставляется с различными инструментами командной строки, каждому из которых мы уделим внимание при освещении определенных тем. Если вы не разбираетесь в операционной системе, рекомендуем прочитать книгу OccupyTheWeb. Linus Basics for Hackers (No Starch Press, 2019) и изучить материалы на сайте *https://kali.org/*, а также пройти бесплатный курс *https://kali.training/*.

Чтобы установить Kali, воспользуйтесь инструкциями на сайте *https://www.kali.org/docs/installation/*. Для установки подойдет любая актуальная версия, однако имейте в виду, что большинство упражнений для версий Kali, обновляемых в период с 2019 по 2020 год. Вы можете попробовать старые образы Kali на *http://old.kali.org/kali-images/*, если у вас возникли проблемы с установкой какого-либо инструмента. В новых версиях Kali по умолчанию устанавливаются не все инструменты, но вы можете добавить их с помощью метапакета kali-linux-large. Чтобы установить его, введите в терминале команду:

```
$ sudo apt install kali-linux-large
```

Мы также рекомендуем запускать Kali на виртуальной машине. Подробные инструкции вы найдете на веб-сайте Kali, а на различных онлайн-ресурсах рассказывается, как это сделать с помощью VMware, VirtualBox или других технологий виртуализации.

Структура книги

Книга состоит из 15 глав, которые условно разделены на пять частей. В основе своей главы независимы друг от друга, но в некоторых из них приводятся ссылки на инструменты или концепции, представленные

выше. Поэтому, хотя мы стремились сделать большинство глав автономными, рекомендуем читать книгу последовательно.

Часть I «Угрозы в мире интернета вещей»

Глава 1 «Безопасность интернета вещей» – это своеобразный пролог: здесь рассказывается, почему важна безопасность интернета вещей и каковы особенности хакинга в этой сфере.

Глава 2 «Моделирование угроз» объясняет, как моделировать атаки на системы интернета вещей и какие распространенные угрозы вы можете обнаружить, на примере инфузионной помпы и ее компонентов.

Глава 3 «Методология тестирования безопасности» предоставляет базовые знания для комплексной оценки безопасности вручную на всех уровнях систем интернета вещей.

Часть II «Взлом на уровне сети»

Глава 4 «Оценка сети» показывает, как выполнять переключение VLAN в сетях IoT, идентифицировать устройства IoT в сети и взломать механизм аутентификации MQTT с помощью Ncrack-модуля.

Глава 5 «Анализ сетевых протоколов» посвящена методологии работы с незнакомыми сетевыми протоколами. Рассматривается процесс разработки анализатора Wireshark и модуля Nmap Scripting Engine для протокола *DICOM*.

Глава 6 «Использование сети с нулевой конфигурацией» исследует сетевые протоколы, используемые для автоматизации развертывания и настройки систем IoT. Описываются атаки на UPnP, mDNS, DNS-SD и WS-Discovery.

Часть III «Взлом аппаратной части системы»

Глава 7 «Уязвимости портов UART, JTAG и SWD» посвящена внутренней работе UART и JTAG/SWD. Вы узнаете, как определить на плате контакты UART и JTAG и взломать защиту микроконтроллера STM32F103 с помощью UART и SWD.

Глава 8 «SPI и I^2C» объясняет, как использовать два протокола шины с различными инструментами для атаки на встроенные устройства IoT.

Глава 9 «Взлом прошивки» показывает, как извлечь и проанализировать прошивку для организации доступа через бэкдор, а также изучить распространенные уязвимости в процессе обновления прошивки.

Часть IV «Взлом радиоканалов»

Глава 10 «Радио ближнего действия: взлом rFID»: злоупотребление RFID демонстрирует различные атаки на системы RFID, такие как чтение и клонирование карт доступа.