
Оглавление

Предисловие от издательства	13
Предисловие	14
Об авторах	16
Колофон	17
Вступление	18
Почему мы написали эту книгу	19
Кому адресована эта книга	19
Что вы узнаете	20
Облачные среды.....	20
Чем эта книга не является.....	21
Использование примеров кода.....	21
Терминология	23
Структура книги	23
Соглашения	24
Благодарности.....	25
ЧАСТЬ I. ВВЕДЕНИЕ В ОБЛАЧНЫЙ OAUTH.....	27
Глава 1. Зачем нужен OAuth?	28
Безопасность на основе API	29
Что такое OAuth 2.0?.....	29
Безопасность с нулевым доверием	31
API с защитой периметра	31
API с защитой инфраструктуры	32
API с защитой на основе токенов	33
Нулевое доверие к клиентам	35
Нулевое доверие к пользователям	35
Компоненты поддержки API.....	36
Облачные платформы	38
Итоги	39
Глава 2. Основы OAuth 2.0.....	41
Роли	41
Абстрактный поток	42
Токен доступа.....	43

Возможности клиентов	44
Публичные и конфиденциальные клиенты	45
Поток кода.....	45
Многоэтапный подход	45
HTTP-сообщения в потоке кода	48
Ключ подтверждения для обмена кодами.....	50
Поток устройства.....	51
Поток учетных данных клиента	52
Поток токена обновления	53
Устаревшие потоки.....	55
Поток пароля.....	55
Неявный поток	56
OpenID Connect.....	57
Гибридный поток.....	58
Информация о пользователе	59
Эволюция OAuth	60
Сеансы и жизненный цикл	61
Поток отзыва.....	61
Завершение сеанса SSO.....	62
Итоги	62
Глава 3. Архитектура безопасности	63
Функции в архитектуре безопасности API	64
Управление идентификацией	64
Управление API.....	65
Управление разрешениями	65
Роль клиента	66
Роль токена доступа.....	66
Какие компоненты безопасности нужны?	67
Роль сервера авторизации	69
Роль шлюза API	71
Роль механизма политик	72
Сфера ответственности API	73
Сфера ответственности клиента	74
Компоненты безопасности	75
Расширение OAuth	77
Итоги	78
Глава 4. Организация данных для интеграции с OAuth	79
Данные сервера авторизации.....	79
Параметры конфигурации OAuth.....	81
Организация учетных записей пользователей	83
Персональные данные	83
Атрибуты пользователя, связанные с бизнесом	85
Идентификаторы пользователей API.....	86
Операции по идентификации	88
API управления пользователями.....	89
Мультирегиональность	91

Мультиарендность	92
Пример миграции учетных записей пользователя	93
Итоги	96

ЧАСТЬ II. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ API С ПОМОЩЬЮ ТОКЕНОВ 99

Глава 5. Разработка защищенных API 100

Унифицированная защита API с помощью токенов доступа JWT	100
Проверка токенов доступа JWT	103
Веб-ключи JSON	103
Ротация ключей для подписи токенов	104
Стандартные утверждения JWT	105
Основные приемы проверки JWT	105
Реализация проверки JWT	106
Логика авторизации API	109
Использование областей действия для упрощенной авторизации	109
Использование утверждений для детальной авторизации	110
Проектирование гибкости	112
Обработка истечения срока действия токена	113
Тестирование API с нулевым доверием	116
Пример кода API	117
Итоги	119

Глава 6. Проектирование токенов доступа 120

Токен доступа как контракт	120
Публикация контракта	121
Версии контракта	122
Область действия токена	122
Области действия в OpenID Connect	125
Области доступа с высокими привилегиями	126
Утверждения в токенах	127
Что должно включать хорошее утверждение?	128
Связь утверждений и областей действия	129
Утверждение об аудитории	130
Источники данных для утверждений	131
Получение согласия пользователя	134
Управление токенами доступа в масштабе	136
Масштабирование областей действия	137
Масштабирование утверждений	139
Проектирование совместного использования токенов	141
Обмен токенов	141
Встраивание токенов в токены	142
Интеграция API	143
Токены в асинхронных взаимодействиях	144
Итоги	146

Глава 7. Безопасность токенов доступа 147

Требования к безопасности токенов доступа	147
Форматы токенов доступа	148
Токены доступа JWT	149
Зашифрованные токены доступа JWT	149
Непрозрачные токены доступа	150
Упакованные непрозрачные токены доступа	151
Доставка токенов доступа	153
Интроспекция	153
Паттерн фантомного токена	155
Паттерн разделенного токена	156
Укрепление безопасности токенов доступа	158
Выбор алгоритма подписи JWT	158
Использование доказательства владения	159
Укрепление безопасности учетных данных в браузерах	161
Ограничение привилегий токенов доступа	162
Ограничение срока действия токена доступа	162
Отзыв токенов	163
Следуйте безопасным методам разработки	165
Итоги	165

Глава 8. Прокси, шлюзы и контейнеры-расширения 166

HTTP-прокси, передача входящего и исходящего трафика	166
Роль шлюза API	168
Представление доступа к API в Kubernetes	169
Настройка сети	170
Развертывание шлюза API	171
Организация доступа к API с использованием ресурса Ingress	173
Организация доступа к API с использованием Gateway API	174
Выбор расширяемого шлюза	176
Проксирование токенов	177
Проксирование непрозрачных токенов	177
Проксирование файлов cookie	179
Проксирование именных токенов	179
Шлюз API и нулевое доверие	180
Роль сервисной сетки	181
Пример расширения возможностей шлюза API	183
Создание кластера	184
Развертывание шлюза API	185
Развертывание сервера авторизации	186
Развертывание примера API	187
Запуск клиента OAuth	187
Использование плагина шлюза API	188
Итоги	189

Глава 9. Привилегии191

Модели управления доступом	191
Управление доступом на основе ролей.....	192
Управление доступом на основе отношений	193
Управление доступом на основе атрибутов	195
Принцип наименьших привилегий	196
Роль авторизации на основе токенов.....	197
Преимущества системы управления привилегиями	197
Гибкость.....	198
Контролируемость	198
Гибкое управление безопасностью	199
Поддержка высокого качества с помощью политик как кода	199
Масштабируемая авторизация	200
Политики	202
Точка администрирования политик	202
Точка извлечения политик	202
Точка принятия решения	203
Точка реализации политики.....	203
Точка получения информации о политике	204
Агент открытой политики	204
Написание политик для OPA	205
Загрузка внешних данных	206
Авторизация на основе утверждений	207
Результаты решения.....	209
Аудит решений об авторизации	210
Извлечение политик в OPA.....	210
Пример развертывания.....	211
Итоги	214

ЧАСТЬ III. РАБОТА OAUTH В ОБЛАЧНОЙ СРЕДЕ 217**Глава 10. Идентификаторы рабочей нагрузки.....219**

Выпуск идентификатора рабочей нагрузки	220
Реализация конфиденциальности запроса	223
Ограничение доступа к рабочим нагрузкам.....	225
Укрепление безопасности учетных данных	225
Использование в качестве учетных данных токенов JWT, выпущенных платформой	227
Использование X.509 SVID в качестве учетных данных.....	228
Укрепление безопасности токенов на предъявителя	230
Ограничения идентификаторов рабочей нагрузки	232
Пример реализации идентификаторов рабочей нагрузки.....	233
Основная конфигурация.....	234
Прозрачное использование идентификаторов рабочей нагрузки	236
Использование идентификаторов рабочей нагрузки JWT	237
Использование идентификаторов рабочей нагрузки X.509.....	238
Итоги	239

Глава 11. Управление облачным сервером авторизации 241

Хостинг	242
Компоненты	243
Кластеризация	244
Адресация	245
URL-адреса рабочих нагрузок среды выполнения	247
URL-адреса рабочих нагрузок администрирования	247
Внутренние URL-адреса	248
Развертывание	249
Процесс сборки	250
Конфигурация среды	251
Процесс развертывания	253
Обновления	255
Операции с данными	256
Обновление учетных записей пользователей	256
Обновление конфигурации	257
Надежность	259
Высокая доступность	259
Быстрое решение проблем	261
Аудит безопасности	264
Итоги	265

ЧАСТЬ IV. БЕЗОПАСНОСТЬ КЛИЕНТОВ API..... 267**Глава 12. OAuth для нативных приложений 268**

Поток кода	268
Реализация клиентов OAuth	270
OAuth для настольных приложений	270
OAuth для мобильных приложений	273
Безопасное хранение данных на устройстве	275
Укрепление безопасности	276
Протокол динамической регистрации клиента	276
Уникальный ключ для каждого устройства	278
Аттестация приложения	279
Аутентификация пользователя без браузера	281
Примеры кода	283
Консольное приложение	284
Настольное приложение	285
Мобильные приложения	287
Итоги	289

Глава 13. OAuth для браузерных приложений 290

Основы веб-приложений	290
Веб-сайты и веб-приложения	291
Архитектура веб-приложений	291
Браузерные приложения	293

Угрозы безопасности в браузерах	294
Кликджекинг	294
Подделка межсайтовых запросов	295
Межсайтовый скриптинг	296
Механизмы веб-безопасности	297
Политика единого источника	297
Политика безопасности контента	298
Настройки безопасности файлов cookie	300
Совместное использование ресурсов разными источниками	302
Реализация OAuth с использованием JavaScript	305
Получение токенов	305
Публичные клиенты	305
Скрытая аутентификация	306
Токены обновления	306
Ротация токенов обновления	307
Именные токены обновления	308
Хранение токенов	308
Web Storage API	308
Хранилище в памяти	309
Файлы cookie JavaScript	309
Безопасное хранение токенов	309
Реализация OAuth с использованием BFF	310
Клиент BFF OAuth	311
Маршрутизатор BFF API	312
Реализация на основе API	313
Интерфейс BFF API	315
Опыт веб-разработчика	316
Укрепление безопасности OAuth	317
Использование файлов cookie в запросах API	318
Варианты развертывания	319
Масштабирование развертываний	321
Выбор реализации BFF	322
Пример кода браузерного приложения	323
OAuth Agent	324
Маршруты шлюза API	324
OAuth Proxy	325
Браузерное приложение	325
Итоги	326
Глава 14. Аутентификация пользователей	328
Современные потоки аутентификации	329
Методы аутентификации пользователей	331
Пароли	332
Внешние поставщики идентификационной информации	333
Одноразовые пароли	335
Аутентификация без пароля	336
Проверка личности	338
Нестандартная аутентификация пользователя	339

Технологии аутентификации пользователя	340
Многофакторная аутентификация.....	341
Поэтапная аутентификация	342
Единый вход	342
Смена методов аутентификации	344
Связывание учетных записей.....	345
Действия аутентификации	347
Выбор аутентификации	347
Жизненный цикл аутентификации пользователя	348
Настройка пользовательских форм.....	349
Регистрация пользователей.....	349
Восстановление учетной записи	352
Запрет доступа	352
Удаление учетной записи пользователя	353
Пример аутентификации пользователей	
с соблюдением принципа нулевого доверия.....	354
Итоги	355
Предметный указатель	357

Предисловие 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 – возможно, ошибку в основном тексте или программном коде, – мы будем очень благодарны, если вы сообщите нам о ней. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Если вы найдете какие-либо ошибки в коде, пожалуйста, сообщите о них главному редактору по адресу dmkpress@gmail.com, и мы исправим это в следующих тиражах.

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 dmkpress@gmail.com.

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

Предисловие

Наша команда успешно реализовала продвинутый сервер OAuth и OpenID Connect, поддерживающий сложные стандарты безопасности, описанные в этой книге. При этом мы получили глубокое понимание этих стандартов и эффективных способов их использования. За годы работы мы поняли, что все наши труды будут напрасными, если мы не поможем другим понять, как наш продукт вписывается в цифровую идентификацию и безопасность API.

По мере расширения цифровизации организациям неизбежно придется предоставлять данные в виде веб-сервисов. Эти API используются мобильными приложениями, одностраничными приложениями и традиционными веб-сайтами. По сути, эти API становятся платформами для новых цифровых процессов и бизнес-моделей. Переход к цифровым технологиям требует от организаций аутентификации пользователей и авторизации доступа к API данных. Для решения этих сложных проблем и были разработаны спецификации OAuth и OpenID Connect. И очень важно, чтобы те, кто осуществляет цифровизацию бизнеса, приняли и внедрили эти стандарты у себя.

Чтобы объяснить, как это сделать, нам нужно было добавить в нашу команду людей, которые не только освоили эти технологии, но и начали обучать других. Эти люди должны были быть умелыми ораторами, увлеченными преподавателями и опытными писателями. Мы обнаружили эти качества в Гэри, Джудит и Михале и сразу же прониклись их желанием поделиться знаниями. Все трое страстно желали рассказывать о сложном простым языком, понятным обычным командам разработчиков программного обеспечения.

Работая вместе, члены новой команды часто использовали собственные облачные технологии для демонстрации стандартов OAuth и подкрепления теории. Мы поняли, что появилось еще одно слияние технологий, о котором тоже нужно рассказывать. Учебные пособия, написанные ими, объясняли, как связаны цифровая идентификация и API, а также показывали, как эти технологии могут использоваться в облачных вычислениях в качестве нативных компонентов. Защищая данные, представленные в сетках микросервисов, они выявили повторяющиеся шаблоны вариантов использования. По мере того как мы узнавали от них новые методы, мы все больше утверждались в своем мнении, что эти критически важные знания тоже необходимо распространять.

Когда авторы предложили написать книгу на эти темы в рамках своей повседневной работы, мы согласились без колебаний, потому что главная цель компании Curity заключается в том, чтобы внести свой вклад в повышение безопасности интернета, в том числе путем распространения знаний по вопросам идентификации. Поскольку мы работаем в Curity, нам выпала уникальная возможность читать главы по мере их написания авторами. В каждой из них мы видели, как они пропагандируют паттерны проектирования, передовой опыт и четко излагают суть протоколов без излишней рекламы продуктов.

В главах, которые вам предстоит прочитать, авторы собрали все свои знания и не только объясняют, как пересекаются цифровая идентификация и безопасность API, но и как развертывать соответствующие решения в облачных окружениях. Если раньше вам не доводилось заниматься таким развертыванием, то эта книга поможет вам понять суть подхода и как работать с несколькими компонентами и конечными точками, чтобы устанавливаемые вами решения были безопасными, современными и простыми в эксплуатации.

OAuth и облачные технологии описываются в книге в манере независимости от конкретного поставщика. Представляемые инструменты и методы останутся актуальными даже для тех, кто не использует облачные окружения. В конце концов, речь идет о наилучших приемах обслуживания API, который, в свою очередь, служит интересам вашего бизнеса и пользователей. Во многих организациях для внедрения OAuth необходимо учитывать нормативные ограничения, многооблачные стратегии и сложности миграции с устаревшей инфраструктурой идентификации. Облачные технологии могут помочь вам в достижении этих целей. Как показывает опыт авторов, интеграция OAuth и облачных технологий не так сложна, как кажется, и имеет много преимуществ.

С учетом вышесказанного мы рекомендуем вам эту книгу и передаем вас в руки авторов.

– *Трэвис Спенсер (Travis Spencer) и Джейкоб Идеског (Jacob Ideskog),*
соучредители Curity.

Об авторах

Гэри Арчер (Gary Archer) работал ведущим разработчиком и архитектором в течение 20 лет и занимался созданием инвестиционно-банковских решений. Его работа включала проектирование миграций на OAuth, разработку простого для понимания кода, а также обучение инженеров, занимающихся безопасностью распределенных архитектур. Имеет богатый опыт поддержки сложных бизнес-систем. Последние несколько лет Гэри работает в Curity, занимаясь обучением сквозным потокам безопасности, включая веб-, мобильные и API-компоненты, а также их интеграции с компонентами безопасности.

Джудит Карер (Judith Kahrer) начала интересоваться вопросами безопасности и идентификации еще в старшей школе. Она считала, что безопасность является важнейшим элементом будущего IT, и продолжает придерживаться этого убеждения по сей день. На протяжении всей своей карьеры она работала на разных технических должностях и приобрела опыт в различных аспектах безопасности, от высокоуровневых протоколов до низкоуровневых политик. Благодаря этому разнообразному опыту она прекрасно справляется с объяснением технических деталей, связанных с OAuth и OpenID Connect, и не только.

Михал Трояновски (Michał Trojanowski) в Curity занимается инженерными изысканиями, написанием документации и преподаванием – всем тем, к чему он сам стремился в предыдущие годы работы разработчиком. Обычная работа разработчика всегда дополнялась публичными выступлениями, обучением стажеров и новых сотрудников, чтением лекций в университетах, наставничеством на хакатонах и ответами на вопросы в сообществе Stack Overflow. Его недавнее внимание к технологиям разработки API и их безопасности привело к OAuth, OpenID Connect, JWT и некоторым новым решениям аутентификации, таким как ключи доступа и децентрализованное хранение идентификационной информации.

Колофон

На обложке «Защита данных в облаке с OAuth» изображен чилийский голубой орел, более известный как черногрудый канюк (*Geranoaetus melanoleucus*).

Эти хищные птицы обитают в основном в Чили, но также встречаются в некоторых других странах Южной Америки. В основном они питаются млекопитающими, но не слишком разборчивы в выборе добычи, довольствуясь тем, что попадется.

Самец и самка вместе заботятся о яйцах (от одного до трех в кладке). Примерно через 50 дней после вылупления птенцы отправляются в самостоятельную жизнь, сначала располагаясь поблизости от родителей. Однако вообще эти птицы ведут одиночный образ жизни, и их можно увидеть летающими в одиночку или вместе со своей парой.

Многие животные на обложках O'Reilly находятся под угрозой исчезновения; все они важны для мира.

Рисунок для обложки выполнила Карен Монтгомери, взяв за основу старинную гравюру из энциклопедии «Zoological Gardens Birds». Дизайн серии разработали Эди Фридман, Элли Фолькхаузен и Карен Монтгомери. Текст на обложке набран шрифтами Gilroy Semibold и Guardian Sans. Текст книги набран шрифтом Adobe Minion Pro; текст заголовков – шрифтом Adobe Myriad Condensed; а фрагменты программного кода – шрифтом Ubuntu Mono, созданным Далтоном Магом (Dalton Maag).

Вступление

При использовании цифровых решений ваши пользователи запускают приложения, получающие доступ к данным через интернет. Эти приложения могут работать в браузерах, на мобильных устройствах, серверах или любой другой платформе. Однако у них есть одна общая черта: они являются клиентами API, и это означает, что для доступа к данным они обращаются к API, а API должны обеспечить безопасность, потому что данные, которые они предоставляют, могут содержать интеллектуальную собственность, персональные сведения, принадлежащие гражданам или пользователям, или информацию, принадлежащую деловым партнерам. Чтобы защитить данные и доступ к ним, необходимо обеспечить безопасность и API, и приложений, извлекающих данные. Такие требования безопасности могут исходить из инициатив по соблюдению нормативно-правовых требований. Одним из примеров является «Общий регламент ЕС по защите данных» (European Union's General Data Protection Regulation, GDPR), который регулирует конфиденциальность и согласие пользователей.

Управление безопасностью и конфиденциальностью данных в API и в клиентах API – сложная задача, которая должна решаться на уровне архитектуры. API должны правильно обрабатывать данные, идентифицирующие пользователей, чтобы каждый пользователь получал доступ только к дозволенным ресурсам API. Для этого в API необходимо использовать бизнес-авторизацию. Точные правила авторизации зависят от конкретных требований бизнеса. В идеале каждый запрос, посылаемый клиентом в API, должен включать не поддающиеся подделке учетные данные с минимально необходимыми привилегиями. Эти учетные данные определяют бизнес-разрешения. Сначала вы должны проверить учетные данные в API и лишь потом применить свои конкретные правила. Защищая подобным образом каждый запрос к API, вы получаете архитектуру API с нулевым доверием.

Мы предполагаем, что при реализации безопасности API вам потребуются определенные архитектурные качества, включая надежность, масштабируемость и продуктивность. Архитектура должна удовлетворять всем этим нефункциональным требованиям, помимо безопасности. Мы покажем вам, как построить такую архитектуру, используя надежные решения. Также мы продемонстрируем подход разделения интересов для выделения сложных областей из кода вашего приложения. Например, с помощью такого подхода можно размещать компоненты безопасности на собственной облачной платформе с поддержкой кластеризации и эластичности для удовлетворения требований к высокой доступности. Аналогичным образом можно управлять криптографией и другими компонентами безопасности, используя специальные конечные точки и библиотеки. Ваш выбор должен учитывать возможность дальнейшего развития в будущем и масштабирования для поддержки многих приложений, API и команд.

ПОЧЕМУ МЫ НАПИСАЛИ ЭТУ КНИГУ

Мы (авторы) все работаем в Curity – компании, специализирующейся на управлении идентификацией и доступом к API. В своей повседневной работе мы обучаем использованию OAuth и других связанных технологий. Некоторые из наших онлайн-материалов основаны на применении Curity Identity Server, однако большая их часть не привязана к конкретному продукту и объясняет архитектуру на основе стандартов. Наша работа предполагает создание презентаций, видеоуроков, онлайн-статей и примеров кода, а также проведение исследований и изысканий в области безопасной аутентификации и доступа к API. Облачные технологии являются передовыми в области развертывания API, но мы заметили, что ресурсы, посвященные облачной безопасности, в основном сосредоточены на инфраструктуре. Мы подтверждаем, что защита на уровне инфраструктуры, например шифрование, играет важную роль в безопасности данных, но не менее важны процедуры, нормы и правила, к которым относится и авторизация – область, где мы являемся экспертами.

Мы написали эту книгу, потому что считаем, что OAuth несет значительные архитектурные преимущества для приложений и API, но понимают эту технологию очень немногие. Это мешает организациям сделать правильный выбор и реализовать все преимущества. В частности, мы считаем, что токены доступа часто используются неоптимально. Правильно спроектированное использование токенов доступа позволяет устанавливать границы безопасности и контролировать авторизацию доступа к защищенным бизнес-ресурсам так, что это становится выгодно всем видам организаций – от малых до очень крупных. Объединив централизованный источник токенов с интеллектуальными методами авторизации, вы сможете контролировать, проверять и управлять доступом к ресурсам в любом масштабе.

Мы объясним основные требования безопасности к API и клиентам API в отношении авторизации и покажем, как OAuth помогает их соблюдать. Часть II является ядром книги, и мы рекомендуем уделить ей особое внимание. Мы думаем, что если с нашей помощью вы поймете, как работают вместе идентификация и бизнес-компоненты, то сможете сделать правильный выбор и в полной мере воспользоваться преимуществами OAuth, чтобы получить защищенное и масштабируемое решение. Мы объясним последовательность действий с точки зрения разработчиков и организаций, создающих цифровые решения, и наряду с теорией представим практические примеры, подкрепляющие ее.

КОМУ АДРЕСОВАНА ЭТА КНИГА

Эта книга предназначена для разработчиков, архитекторов или инженеров по надежности информационных систем, интересующихся защитой API. Возможно, вы уже работаете с API, имеющими некоторую базовую защиту, но хотите узнать, как обновиться до архитектуры нулевого доверия. Желательно, чтобы у вас были знания API и защиты API на среднем уровне.

Для представления примеров реализации защиты мы используем Docker и Kubernetes. Поэтому знакомство с контейнерами поможет вам получить бо-

лее полный практический опыт. Однако описанные в книге концепции в равной мере применимы к любой облачной платформе.

Книга местами содержит много технических деталей, поэтому будьте готовы встретиться со значительным объемом информации по темам идентификации и принять подход к разработке программного обеспечения, основанный на принципе разделения ответственности.

Что вы узнаете

Вы узнаете, как защитить API и клиентов с помощью фреймворка авторизации OAuth 2.0. Мы представим проекты, паттерны и рекомендации, которые помогут вам обеспечить соблюдение бизнес-разрешений в API. В этой книге вы узнаете, как:

- проектировать токены доступа с минимальными привилегиями;
- управлять сервером авторизации;
- выдавать токены доступа клиентам API, а затем направлять их в API;
- проверять токены доступа в API, а затем авторизовать доступ к бизнес-данным;
- реализовать поддержку множества способов аутентификации в клиентах;
- управлять конфиденциальностью токенов для интернет-клиентов;
- следовать рекомендациям для веб-приложений, чтобы ограничить ущерб в случае использования уязвимости межсайтового скриптинга (XSS);
- реализовать поддержку OAuth 2.0 в настольных и мобильных приложениях;
- управлять различиями в безопасности, характерными для клиентов, в шлюзе API;
- объединить OAuth 2.0 с системой безопасности инфраструктуры;
- сохранить код приложения переносимым и основанным на стандартах;
- устранять ошибки и обеспечить надежную сквозную защиту.

Облачные среды

Мы решили разместить эту книгу в облачной среде, поскольку считаем, что такая среда обеспечивает оптимальные возможности для управления защищенными API.

Нативные облачные (Cloud native) технологии позволяют организациям создавать и запускать масштабируемые приложения в современных динамических средах, таких как публичные, частные и гибридные облака. Контейнеры, сервисные сетки (service meshes), микросервисы, неизменяемая инфраструктура и декларативные API являются примером такого подхода.

– CNCF Cloud Native Definition v1.0.

В контексте этой книги соответствующими технологиями для архитектуры безопасности, а также для запуска примеров кода являются контейнеры, сервисные сетки и микросервисы. Мы не делаем никаких предположений о том, какое облако вы используете – публичное, частное или гибридное.

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru