Оглавление

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.