Василюк М.Ю. Аутентификация на основе токенов в веб-приложениях // Международный журнал информационных технологий и энергоэффективности. – 2023. –
Т. 8 № 4(30) с. 45–48

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.9

АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ТОКЕНОВ В ВЕБ-ПРИЛОЖЕНИЯХ

Василюк М.Ю.
МИРЭА - Российский технологический университет, Москва, Россия (119454, г. Москва, пр. Вернадского, 78), e-mail: maxim1.480.86@gmail.com

Аутентификация с помощью токенов — на сегодняшний день из самых популярных методов аутентификации пользователей в веб-приложениях. Он подразумевает использование токена, который представляет собой небольшой фрагмент данных, содержащий информацию о пользователе. Токен обычно генерируется сервером и отправляется браузеру пользователя, где он используется для аутентификации пользователя при выполнении последующих запросов. В этой статье будет рассмотрена концепция аутентификации с помощью токенов, ее преимущества и использование ее в веб-приложениях.

Ключевые слова: Стандарты аутентификации, токен, кибербезопасность, веб-приложение.

TOKEN-BASED AUTHENTICATION IN WEB APPLICATIONS

Vasilyuk M.Y.
MIREA - Russian Technological University, Moscow, Russia (119454, Moscow, Vernadskogo Ave., 78), e-mail: maxim1.480.86@gmail.com

Token authentication is by far one of the most popular methods of user authentication in web applications. It implies the use of a token, which is a small piece of data containing information about the user. The token is usually generated by the server and sent to the user's browser, where it is used to authenticate the user when making subsequent requests. This article will discuss the concept of authentication using tokens, its advantages and its use in web applications.

Keywords: authentication standards, token, cybersecurity, web application.

Что такое аутентификация с помощью токенов?

Аутентификация с помощью токенов — это метод аутентификации пользователя, в котором используются токены вместо данных, присущих более традиционным методам, таких как имя пользователя/пароль или идентификатор сессии [1]. Токены обычно генерируются сервером и направляются клиенту, где они и хранятся, а позже отправляются обратно на сервер с каждым последующим запросом. Токены могут использоваться для аутентификации пользователя, предоставления уровней доступа или разрешений на выполнение различного рода операций. Также, они могут быть зашифрованы и подписаны цифровой подписью для предотвращения несанкционированного доступа к текущей сессии.

Преимущества аутентификации с помощью токенов.

У использования аутентификации посредством токенов в веб-приложениях есть ряд преимуществ. Приложения с таким типом аутентификации легко масштабируется [2], поскольку использование токенов не предполагает сохранения состояния на сервере. Это означает, что серверу не нужно отслеживать информацию о сеансе пользователя, что решает проблему масштабируемости при работе с большим количеством пользователей.

Повышенный уровень безопасности. Аутентификация посредством токенов может помочь улучшить безопасность приложения. Например, используя токены для аутентификации пользователей, приложения могут избежать хранения конфиденциальной информации о пользователях на сервере, что снижает риск утечки данных. Кроме того, поскольку токены часто программно ограничены по времени существования, в течение которого они действительны, а также могут быть инвалидированы и отозваны, что может помочь предотвратить несанкционированный доступ к приложению, если токен скомпрометирован.

Кроссплатформенная совместимость. Поскольку аутентификация посредством токенов часто реализуется с помощью готовых стандартов, как например OAuth, такие системы аутентификации могут быть использованы на других платформах и сервисах. Это упрощает пользователям доступ к приложениям, использующих данную систему аутентификации, т.к. позволяет им не создавать несколько учетных записей или вводить свои реквизиты для входа более одного раза.

Улучшение пользовательского опыта. Аутентификация с помощью токена может обеспечить более удобное взаимодействие пользователя с системой, поскольку пользователям не нужно вводить свои учетные данные каждый раз, когда они обращаются к приложению. Вместо этого они могут просто предоставить свой токен, который можно безопасно хранить на своем устройстве или в браузере.

Стандарты аутентификации на основе токенов.

Существует несколько стандартов аутентификации посредством токенов. Самыми ширико используемыми являются OAuth 2.0 и JWT.

OAuth 2.0 — это широко используемый стандарт аутентификации и авторизации на основе токенов [3]. Он позволяет пользователям предоставлять доступ к личной информации сторонним приложениям, не передавая свои данные учетной записи. OAuth 2.0 использует токены доступа (access tokens) для авторизации запросов, и токены обновления (refresh tokens) для поддержания текущего сеанса пользователя, путем обновления access token и refresh token.

JSON Web Tokens (JWT) — еще один популярный стандарт, использующийся для аутентификации посредством токенов. JWT — это, по сути, небольшой JSON-объект, который содержит информацию о пользователе: данные учетной записи, уровень доступа и т.д. JWT запечатан криптографической подписью, которая гарантирует, что токен не будет подделан. Токен может безопасно передаваться по сети в виде стандартного заголовка HTTP или параметра URL-адреса и может использоваться клиентом для аутентификации на сервере и доступа к защищенным ресурсам.

Токен-аутентификация на практике.

Аутентификация с помощью токенов используется в самых разных веб-приложениях, включая социальные сети, приложения электронной коммерции, банковские сервисы и т.д.

Например, социальная сеть Facebook использует аутентификацию с помощью токенов, чтобы пользователи могли входить в сторонние приложения, используя свои учетные данные Facebook. Это позволяет пользователям легко получать доступ к различным сервисам без необходимости создавать и запоминать информацию о разных учетных записях.

В приложениях электронной коммерции аутентификация с помощью токенов часто используется для предоставления доступа к учетным записям пользователей, информации о платежах и истории заказов. Это позволяет пользователям легко и быстро совершать покупки, сохраняя информацию о товарах в корзине покупателя между всеми доступными платформами, а также без необходимости вводить свою платежную информацию каждый раз, когда совершается покупка.

В банковских приложениях аутентификация с помощью токенов используется в первую очередь для защиты учетных записей пользователей и предотвращения несанкционированного доступа. Банки используют токены для аутентификации пользователей, когда они входят в свою учетную запись онлайн-банкинга, а также для авторизации транзакций, таких как денежные переводы или оплата счетов.

Заключение

Аутентификация с помощью токенов — это одновременно мощный и гибкий метод аутентификации пользователей в веб-приложениях. Он обладает существенными преимуществами по сравнению с традиционными методами аутентификации, в число которых входит масштабируемость, безопасность и гибкость. Стандарты аутентификации токенов, такие как OAuth 2.0 и веб-токены JSON (JWT), получили широкое распространение и предлагают разработчикам надежный набор инструментов для создания безопасных и масштабируемых приложений.

Поскольку количество веб-приложений продолжает расти, аутентификация с помощью токенов будет продолжать играть важную роль в обеспечении безопасности и конфиденциальности данных пользователей.

Список литературы

1. A secure Token-based Communication for Authentication and Authorization Servers // ResearchGate URL: https://www.researchgate.net/publication/309365153_A_Secure_Token-Based_Communication_for_Authentication_and_Authorization_Servers (дата обращения: 23.01.2023).
2. What is a Token? What are its Pros and Cons? // loginradius URL: https://www.loginradius.com/blog/identity/pros-cons-token-authentication/ (дата обращения: 02.02.2023).
3. OAuth 2.0 // OAuth 2.0 URL: https://oauth.net/2/ (дата обращения: 04.02.2023).
4. JSON Web Token (JWT) // RFC Editor URL: https://www.rfc-editor.org/rfc/rfc7519 (дата обращения: 05.02.2023).

References

1. A secure Token-based Communication for Authentication and Authorization Servers // ResearchGate URL: https://www.researchgate.net/publication/309365153_A_Secure_Token-

Based_Communication_for_Authentication_and_Authorization_Servers (accessed: 23.01.2023).
2. What is a Token? What are its Pros and Cons? loginradius URL: https://www.loginradius.com/blog/identity/pros-cons-token-authentication/ (accessed: 02.02.2023).
3. OAuth 2.0 // OAuth 2.0 URL: https://oauth.net/2/ (accessed: 04.02.2023).
4. JSON Web Token (JWT) // RFC Editor URL: https://www.rfc-editor.org/rfc/rfc7519 (accessed: 05.02.2023).