УДК 343.98

Филипов Эдуард Олегович, магистрант кафедры защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций имени профессора М. А. Бонч-Бруевича, г. Санкт-Петербург

Косов Никита Алексеевич, старший преподаватель кафедры защищенных систем связи, Санкт-Петербургский государственный университет телекоммуникаций имени профессора М.А. Бонч-Бруевича, г. Санкт-Петербург

ИСПОЛЬЗОВАНИЕ JSON WEB TOKEN (JWT) ДЛЯ БЕЗОПАСНОЙ АУТЕНТИФИКАЦИИ И АВТОРИЗАЦИИ

Аннотация. Современные распределённые системы, облачные платформы и микросервисные архитектуры предъявляют особые требования к безопасности процессов аутентификации и авторизации. В условиях децентрализации вычислений и множественности точек доступа к данным возрастает необходимость в эффективных механизмах управления доступом. Одним из таких решений стал JSON Web Token (JWT) — открытый стандарт для безопасного обмена информацией между сторонами. В статье рассмотрены принципы работы JWT, его структура, а также преимущества и потенциальные уязвимости. Проведено сравнение JWT с традиционными методами управления сессиями и рассмотрены практики безопасного внедрения в современных веб-приложениях.

Annotation. Modern distributed systems, cloud platforms, and micro-service architectures place special demands on the security of authentication and authorization processes. With the decentralization of computing and the multiplicity of data access points, the need for effective access control mechanisms is increasing. One of these solutions was the JSON Web Token (JWT), an open standard for the secure exchange of information between the parties. The article discusses the principles of JWT, its structure, as well as advantages and potential vulnerabilities.

JWT is compared with traditional session management methods and the practices of secure implementation in modern web applications are considered.

Ключевые слова: JSON Web Token, аутентификация, авторизация, безопасность, токен

Keywords: JSON Web Token, authentication, authorization, security, token

Введение

В условиях цифровизации и активного развития веб-технологий вопросы аутентификации и авторизации пользователей приобретают ключевое значение. Многие популярные способы управления доступом на основе сессий, при которых данные об авторизованном пользователе хранились на сервере, становятся менее эффективными в условиях, где сетевое взаимодействие осуществляется между большим количеством клиентов и компонентов.

JSON Web Token (JWT) представляет собой альтернативу традиционной модели сессионного хранения данных. Этот инструмент позволяет реализовать stateless-аутентификацию, когда данные о пользователе и правах доступа встраивается в токен, передаваемый между участниками сетевого взаимодействия, что позволяет исключить необходимость постоянного обращения к серверу авторизации. Цель данной статьи — рассмотреть основные принципы работы JWT, обозначить его достоинства и недостатки, а также определить главные критерии, влияющие на безопасность при его использовании.

Основная часть

JWT (от англ. JSON Web Token) — это компактный и самодостаточный формат токена для передачи утверждений между сторонами. Токен состоит из трёх частей: заголовка (header), полезной нагрузки (payload) и электронной подписи (signature). Все три части кодируются в Base64Url. Такой подход делает JWT легким для отправки по HTTP заголовкам или через URL.

Преимущества JWT:

- Независимость от серверного хранения сессий;

- Простота масштабирования;
- Отсутствие необходимости постоянного обращения к базе данных снижает нагрузку на сервер.

Вместе с тем существуют и некоторые уязвимости:

- Перехват токена при недостаточно защищенном соединении;
- Атаки при простом ключе или подписи;
- Угроза XSS-атак при хранении токенов в localStorage;
- Отсутствие механизма отзыва токена без внедрения дополнительных решений.

Рекомендации по безопасной реализации JWT:

- Использование HTTPS — все запросы должны осуществляться через защищённый протокол HTTPS для предотвращения MITM-атак.
- Надёжные алгоритмы подписи — необходимо использовать алгоритмы с симметричными или асимметричными ключами (например, HS256, RS256). Следует избегать алгоритма "none".
- Минимизация данных в payload — в нагрузке не должны содержаться чувствительные данные, так как она не зашифрована.
- Установка сроков действия токена — установка короткого срока жизни access-токенов с возможностью обновления через refresh-токен повышает уровень безопасности.
- Защищённое хранение токенов — предпочтительно хранение токенов в httpOnly cookies для снижения риска XSS-атак.
- Механизмы отзыва — для поддержки отзыва токенов можно внедрить чёрные списки (blacklist) или базы отозванных идентификаторов.

На практике JWT реализуется следующим образом. После успешной аутентификации пользователь получает от сервера токен, который в дальнейшем передаётся в заголовке Authorization при каждом запросе:

Authorization: Bearer <token>

На стороне сервера выполняется верификация подписи токена, а затем извлекается полезная нагрузка с данными пользователя. На основании этих данных сервер может принимать решение об авторизации.

Сравнение JWT с альтернативными механизмами реализации безопасной аутентификации и авторизации рассматривается в таблице 1.

Таблица 1.

Таблица сравнения JWT с альтернативными механизмами реализации безопасной аутентификации и авторизации

Реализуемый метод	JWT	Sessions	OAuth 2.0 (без JWT)
Хранение	Stateless	Server-side	Зависит от реализации
Масштабируемость	Высокая	Ограниченная	Средняя
Безопасность	Зависит от реализации	Зависит от реализации	Высокая
Расширяемость	Гибкая структура	Ограниченная	Широкая

Заключение

JWT представляет собой мощный инструмент для реализации безопасной, масштабируемой и эффективной схемы аутентификации и авторизации в современных веб-приложениях. Однако, его использование требует строгого соблюдения рекомендаций по безопасности, так как ошибки в реализации могут привести к серьёзным уязвимостям. При грамотной интеграции JWT позволяет существенно упростить архитектуру распределённых систем, снижая нагрузку на сервер и повышая отказоустойчивость сервисов.

Таким образом, использование JWT — это не только тренд в области веб-разработки, но и обоснованное техническое решение для построения надёжной системы идентификации пользователей.

Литература

1. Макаров, Д. А. Механизм авторизации с использованием технологии JWT / Д. А. Макаров // Теория и практика современной науки. – 2020. – № 1(55). – С. 474-476. – EDN YJULBN.
2. Козлов, С. В. Реализация аутентификации пользователя в web-приложении с использованием стандарта JWT / С. В. Козлов, М. С. Воробьев // Системы компьютерной математики и их приложения. – 2022. – № 23. – С. 362-366. – EDN EILXZE.
3. Ананченко, И. В. Процесс аутентификаци с использованием токенов доступа, формируемых на основе стандарта RFC 7519 (JWT Token) / И. В. Ананченко, И. Д. Грязных // ЛУЧШАЯ ИССЛЕДОВАТЕЛЬСКАЯ СТАТЬЯ 2023 : сборник статей II Международного научно-исследовательского конкурса, Пенза, 15 марта 2023 года. – Пенза: Наука и Просвещение (ИП Гуляев Г.Ю.), 2023. – С. 6-9. – EDN TUJQAA.
4. Временная атака на JWT и способы ее устранения / Д. А. Макаров, Ю. Ю. Ваняшкин, Д. А. Калугина [и др.] // Естественные и технические науки. – 2019. – № 5(131). – С. 200-203. – EDN ZPYXQO.
5. Филатов, К. Ю. Использование токенов на примере JWT в spring boot rest API приложении / К. Ю. Филатов // Информационные технологии моделирования и управления. – 2022. – Т. 128, № 2. – С. 153-157. – EDN IPDNXO.

Literature

1. Makarov, D. A. Authorization mechanism using JWT technology / D. A. Makarov // Theory and practice of modern science. – 2020. – № 1(55). – Pp. 474-476. – EDN YJULBN.
2. Kozlov, S. V. Implementation of user authentication in a web application using the JWT standard / S. V. Kozlov, M. S. Vorobyov // Computer mathematics systems and their applications. – 2022. – No. 23. – PP. 362-366. – EDN EILXZE.
3. Ananchenko, I. V. The authentication process using access tokens generated on the basis of the RFC 7519 (JWT Token) standard / I. V. Ananchenko, I. D. Gryaznykh // The BEST RESEARCH ARTICLE 2023 : collection of articles of the II International Scientific Research Competition, Penza, March 15, 2023. Penza: Science and Education (IP Gulyaev G.Yu.), 2023. pp. 6-9. – EDN TUJQAA.
4. Temporary attack on JWT and ways to eliminate it / D. A. Makarov, Yu. Yu. Vanyashkin, D. A. Kalugina [et al.] // Natural and Technical Sciences. – 2019. – № 5(131). – Pp. 200-203. – EDN ZPYXQO.
5. Filatov, K. Y. The use of tokens using the example of JWT in the spring boot rest API application / K. Y. Filatov // Information technologies of modeling and management. – 2022. – Vol. 128, No. 2. – pp. 153-157. – EDN IPDNXO.