Використання JWT маркерів для аутентифікації та авторизації користувачів у web- додатках

Ганна Олійник[1], Сергій Грибков[2]

1. Кафедра інформаційних систем, Національний університет харчових технологій, УКРАЇНА, м. Київ, вул. Володимирська, 68, E-mail: anna.oliinyk@ukr.net

2. Кафедра інформаційних систем, Національний університет харчових технологій, УКРАЇНА, м. Київ, вул. Володимирська, 68, E-mail: sergio_nuft@ukr.net

The problems of implementing of authentication and authorization mechanisms in web-oriented systems were considered. Analysis and comparison of users' authentication and authorization approaches were performed. Features of using of JWT tokens were examined and their advantages were proved.

Ключові слова – аутентифікації та авторизації, web-орієнтовані системи, JWT маркери.

Вступ

Сучасний стрімкий розвиток інформаційних технологій спонукає до все більшого поширення web-орієнтованих інформаційних систем, які дають набагато більше переваг у порівнянні з традиційними. Авторами ведеться розробка web-орієнтованої системи підтримки прийняття рішень при плануванні виконання договорів, яка повинна забезпечувати можливість розв'язання основних задач прийняття рішень, а також їх підтримку необхідною інформацією у будь якому місці, де є доступ до мережі Інтернет. Проте, особливо важливо відмітити наявність цілої низки проблем, пов'язаних з організацією захисту даних, централізованим управлінням інформаційними ресурсами, розмежуванням доступу до таких ресурсів, управлінням сеансами доступу тощо.

Саме тому виникла задача обрання способу реалізації механізму аутентифікації та авторизації користувачів для web-орієнтованої системи підтримки прийняття рішень при плануванні виконання договорів.

Особливості аутентифікації та авторизації користувачів у web-додатках

Основним методом аутентифікації в сучасних web-додатках є використання файлів cookie, що вміщують ідентифікатор сесії на сервері. При цьому сесія має термін дії, який автоматично збільшується при зверненні користувача на сервер.

Аутентифікація на основі серверної сесії та cookie відноситься до групи підходів, які зберігають стан взаємодії між клієнтом і сервером, а також дані, які між ними передаються. При використанні такого підходу дані про сесію зберігаються як на клієнтській, так і на серверній частині. Перелік активних сесій зберігається на сервері (наприклад, у базі даних), а на клієнтській частині створюється файл cookie, що містить ідентифікатор активної сесії.

Алгоритм взаємодії зареєстрованого користувача з web-додатком при використанні традиційного підходу складається з трьох основних кроків, а саме:

1. Після введенням користувачем свого імені та паролю відбувається їх відправлення на сервер, де здійснюється перевірка та, у разі успішного її проходження, створюється сесія. Дані про створену сесію зберігається на сервері у вигляді, наприклад, окремої таблиці з полями ідентифікатор сесії, термін її дії та відповідний ідентифікатор користувача. У браузері клієнта зберігається файл cookie з ідентифікатором створеної на сервері сесії.

2. При усіх наступних запитах користувача ідентифікатор сесії з файлу cookie звіряється з ідентифікатором, збереженим на сервері, і, за умови їх відповідності, відбувається обробка запитів.

3. Після закінчення користувачем роботи з web-додатком дані про сесію видаляються на серверній і клієнтській частинах.

Важливо зазначити, що останнім часом, зважаючи на цілий ряд причин, все актуальнішою стає потреба у відмові від використання файлів cookie та серверної сесії. До основних причин відносять наступні:

1. Все частіше розробники реалізують взаємодію з серверною частиною за допомогою запитів через окремий інтерфейс, яким визначені усі функціональні можливості системи. Цей самий інтерфейс використовують для мобільних додатків. Уніфікація підходу до аутентифікації користувачів при використанні традиційного підходу є доволі складною задачею, оскільки використання однакових файлів cookie у настільних додатках та на мобільних платформах є досить проблематичним.

2. Необхідність у постійному зверненні до репозиторію даних при кожному запиті для пошуку даних про користувача за отриманим ідентифікатором сесії, що негативним чином впливає на продуктивність та швидкодію системи.

3. У випадку горизонтального масштабування web-додатку виникає проблема синхронізації стану сесій між серверами з метою підтримки актуального стану даних. Для вирішення цієї проблеми існують окремі підходи, проте створення додатку, який не потребує використання сесії взагалі, є значно простішим для його підтримки в майбутньому, а також значним чином дозволяє скоротити обсяг робіт при вдосконаленні та розширенні.

З урахуванням усього вищезазначеного, актуальною задачею є дослідження альтернативних підходів реалізації аутентифікації та авторизації з усуненням зазначених недоліків.

Одним із сучасних підходів при реалізації механізмів аутентифікації та авторизації користувача є використання спеціальних web-маркерів – JWT (JSON Web Token). JWT маркер представляє собою текстовий рядок, що містить у зашифрованому вигляді необхідні для аутентифікації та авторизації користувача дані.

Особливості використання JWT маркеру

JWT маркер у текстовому вигляді складається з трьох частин, розділених між собою крапкою, а саме: заголовку (header), інформаційної частини (payload) та підпису (signature). Таким чином, маркер має вигляд «header.payload.signature». Кожна частина маркеру кодується за допомогою методу кодування Base64. Сформований JWT маркер представлений на наступному прикладі:

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikhhbm5hIE9saWlueWsiLCJhdXRoIjo0LCJleHAiOjE0OTI4ODMzNDF9.qDVQJxJLtVSNEZ3CGi4mzzNjIDQ1lOCvSBZd7dhNquU

Заголовок містить тип маркера та назву алгоритму шифрування (наприклад, HS256). Типовий заголовок у форматі обміну даних JSON (JavaScript Object Notation) має вигляд:

```
{
  "typ":"JWT",
   "alg":"HS256"
}
```

Інформаційна частина складається з наборів пар ключ-значення (JWT Claims Set), що в загальному випадку містять мінімально необхідні для аутентифікації та авторизації в системі дані про користувача, якому даний маркер належить. Інформаційна частина з чотирьох полів, що містять певні значення, має наведений на прикладі вигляд:

```
{
 "sub": "1234567890",
 "name": "Hanna Oliinyk",
 "auth": 4,
 "exp": 1492883341
}
```

Інформаційна частина може включати як стандартні поля, описані у специфікації (RFC 7519), так і довільні користувацькі поля. У наведеному прикладі використані стандартні поля: sub – ідентифікатор користувача, name – ім’я користувача, exp – час закінчення дії токена. Крім цього, використано додаткове поле auth, значення якого у числовому вигляді відповідає рівню доступу користувача у системі.

Підпис створюється з використанням секретного коду, заголовку та інформаційної частини. Він призначений для верифікації маркеру, а також унеможливлює підробку маркера та його формування сторонніми системами.

Формування підпису можна описати за допомогою наступного псевдокоду:

data = base64urlEncode(header) + “.” + base64urlEncode(payload);

signature = hash(data, secret).

Використання JWT маркеру визначає наступний порядок взаємодії зареєстрованого користувача з web-додатком:

1. На серверній частині відбувається перевірка логіну та паролю користувача. У разі успіху формується та надсилається у відповідь JWT маркер, до інформаційної частини якого вносяться усі необхідні дані (ідентифікатор користувача, роль у системі тощо). Іншими словами, маркер включає дані про користувача та його можливості у системі.

2. При кожному наступному запиті користувача отриманий маркер включається до заголовку авторизації (Authorization header) у форматі: Authorization: Bearer {маркер}. На сервері відбувається перевірка коректності та дійсності маркеру, а також його підпису. Успішне проходження перевірки дозволяє подальшу обробку запиту.

Основною перевагою використання JWT маркерів є відсутність необхідності зберігання будь-яких даних про маркери чи самі маркери на сервері. Кожен маркер включає всі необхідні дані для перевірки його достовірності, а також дає можливість передавати довільний набір даних. Серверна частина забезпечує формування, підпис та видачу JWT маркерів, перевірку дійсності маркерів у вхідних запитах.

Недоліком використання маркерів є необхідність обмеження довжини заголовку у запиті для деяких серверів. У таких випадках у інформаційну частину маркеру варто включати лише мінімально необхідні дані. Крім цього, маркер містить у собі термін дії, який відповідно до вимог безпеки повинен бути не дуже тривалим, а після його закінчення необхідно формувати новий маркер.

Висновок

У результаті проведених досліджень та аналізу особливостей використання JWT маркерів для аутентифікації та авторизації користувачів було прийняте рішення про використання такого підходу при створенні web-орієнтованої системи підтримки прийняття рішень при плануванні виконання договорів, що забезпечить підвищення рівня захисту інформації при роботі з web-орієнтованими системами та зменшить час обробки запитів.

Література

[1] Jones. M. JSON Web Token (JWT) [Електронний ресурс] / M. Jones, J. Bradley, N. Sakimura // Internet Engineering Task Force. – 2015. – Режим доступу до ресурсу: https://tools.ietf.org/html/rfc7519[2]

[2] Ado Kukic. Cookies vs Tokens: The Definitive Guide [Електронний ресурс] / Ado Kukic // auth0.com. – 2016. – Режим доступу до ресурсу: https://auth0.com/blog/cookies-vs-tokens-definitive-guide/

[3] Mikey Stecky-Efantis. 5 Easy Steps to Understanding JSON Web Tokens (JWT) [Електронний ресурс] / Mikey Stecky-Efantis // vandium software. – 2016. – Режим доступу до ресурсу: https://medium.com/vandium-software/5-easy-steps-to-understanding-json-web-tokens-jwt-1164c0adfcec.