Є. Є. Стасюк

ВДОСКОНАЛЕНИЙ МЕТОД АУТЕНТИФІКАЦІЇ ШЛЯХОМ ДОДАТКОВОГО ШИФРУВАННЯ МАРКЕРУ ДОСТУПУ

Вінницький національний технічний університет

Анотація

Проведено аналіз існуючих методів аутентифікації, що дозволило дослідити їхні переваги та недоліки. На основі цього аналізу розроблено концепцію вдосконаленого методу аутентифікації, що підвищить безпеку та секретність користувачів у мережі інтернет.

***Ключові слова**: аутентифікація, шифрування, маркер доступу.*

Abstract

An analysis of existing authentication methods was conducted, which allowed us to explore their advantages and disadvantages. Based on this analysis, a concept of an improved authentication method was developed, which will increase the security and privacy of users on the Internet.

***Keywords**: authentication, encryption, access token..*

Вступ

Аутентифікація користувача це важлива складова в сучасній веб розробці. Кожен вебсайт, комп'ютерна програма чи телефонний застосунок мають різні методи для ідентифікації користувача після його авторизації. Це важлива складова таких проектів завдяки якій користувач не має вводити свої облікові дані при кожному запиту на сервер, достатньо, щоб клієнт запам'ятав маркер доступу та відправляв його з кожним авторизованим запитом.

В сучасному світі маркери доступу містять в собі не один ідентифікатор користувача з бази даних чи логін. В залежності від величини серверного додатку та його логіки у цьому маркері може бути багато різних даних користувача які, як правило, не використовують додаткового шифрування. Інформація, що міститься у цих маркерах доступу не дасть стороннім отримати доступ до профілів інших користувачів, але розкриє певні конфіденційні дані користувача.

У даній статті ми розглянемо як можна вдосконалити існуючі методи аутентифікації на прикладі JWT.

Основна частина

JSON Web Token – це відкритий стандарт маркеру доступу, який дозволяє передавати дані для аутентифікації між різними частинами застосунку. Зашифрований рядок поділяється на три частини. У першій частині закодовано алгоритм шифрування JWT. У наступній дані користувача. Остання частина являється підписом, який валідується, щоб підтвердити справжність маркеру, це єдина частина яка справді кодується таким чином, щоб не бути розшифрованою за межами застосунку. JWT зазвичай зашифровується за допомогою приватного ключа, в той час як публічний ключ лише дає змогу перевірити валідність маркеру доступу.

Вдосконаленням цього методу може слугувати додаткове шифрування маркеру перетворюючи його в рядок, що не можна швидко розшифрувати на відмінну від звичайного JWT. Для цього добре підходить алгоритм AES-256, який зашифровує та розшифровує масиви символів використовуючи ключ у форматі Base64.

При такій аутентифікації сервер буде виконувати додатковий крок для розшифрування маркеру доступу з звичайний JWT. Схематичну роботу серверу при аутентифікації зображено на рисунку 1. Як тільки запит з bearer token потрапляє на сервер, він намагається його розшифрувати. При невдалій спробі сервер повертає помилку до клієнта. В разі успіху сервер валідує JWT перевіряючи його час закінчення терміну дії та підпис. У разі виникнення помилок чи закінчення терміну дії маркеру сервер повертає відповідну помилку на клієнт. Якщо помилок не виникає, то сервер аутентифікує користувача за полем sub та продовжує виконувати запит.

Рисунок 1 – Схема роботи сервера при аутентифікації

Цей метод підходить для різних серверних застосунків і підвищить безпеку даних користувачів за допомогою шифрування конфіденційних даних та зберігання в секреті технологій аутентифікації, а саме JWT в цьому випадку.

Висновок

У цій статті було розглянуто вдосконалення популярних методі аутентифікації на основі JWT та алгоритму шифрування AES-256. Наведена схема роботи сервера при аутентифікації та описано головні принципи цього методу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Що таке автентифікація? [Електронний ресурс] // Microsoft – Режим доступу до ресурсу: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-authentication.
2. Garfinkel S. Web Security, Privacy & Commerce / S. Garfinkel, G. Spafford., 2001. – (O\'Reilly Media, Inc.).
3. Authentication [Електронний ресурс] // TechTarget – Режим доступу до ресурсу: https://www.techtarget.com/searchsecurity/definition/authentication.
4. Алгрен М. Що таке шифрування AES-256 і як воно працює? [Електронний ресурс] / Метт Алгрен // WebSiteRating – Режим доступу до ресурсу: https://www.websiterating.com/uk/blog/cloud-storage/what-is-aes-256-encryption/.

Стасюк Євгеній Є. – студент групи 1КІ-23м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: stasyuk5656@gmai.com.

Войцеховська Олена В. – кандидат технічних наук, доцент, доцент кафедри обчислювальної техніки., Вінницький національний технічний університет, м. Вінниця, e-mail: vojcexovska.o.v@vntu.edu.ua.

Stasiuk Yevhenii Y. - student of group 1CI-23m, faculty of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail:.stasyuk5656@gmai.com

Voitsekhovska Olena V. — Cand. Sc. (Eng.), Assistant Professor of the Computer Techniques Chair, Vinnytsia National Technical University, Vinnytsia, e-mail: vojcexovska.o.v@vntu.edu.ua