УДК 004.4

М.Т. Мусійчук
Л.М. Куперштейн

АВТЕНТИФІКАЦІЯ WEB-ДОДАТКІВ ЗА ДОПОМОГОЮ АПАРАТНОГО ТА ПРОГРАМНОГО ТОКЕНА

Вінницький національний технічний університет

Анотація

Проведено детальний огляд існуючих систем автентифікації, для подальшої розробки та вдосконалення відомих технологій та запропоновано власний програмний засіб.

Ключові слова: Автентифікація, веб-додаток, JWT-токен.

Abstract

A review of existing authentication systems was carried out, for the further development and improvement of known technologies, and own program was proposed.

Keywords: Authentication, web apps, JWTokens.

Вступ

Автентифікація є однією з найважливіших частин веб-додатків, без якої не працювати - жодна система. Однак останнім часом всі розробники хочуть відмовитися від використання cookies і серверної сесії. Найкращим рішенням є використання JSON Web Token (JWT) - це маркер, який зберігає необхідну інформацію для автентифікації та авторизації у зашифрованому вигляді [1]. При цьому не потрібно зберігати дані про користувача в сесії, так як маркер містить її в собі. Розроблений засіб для автентифікації на основі JWT повинен забезпечити віддалений доступ для будь-яких користувачів, який зекономить розробку власного продукту, спростить роботу і забезпечить високй рівень захищеності. Але використання одного методу на основі JWT замало, тому для покращення автентифікації потрібно використовувати програмний токен Bluetooth пристроя. Завдяки цьому покращиться захист автентифікації і унеможливиться проблема викрадання токена.

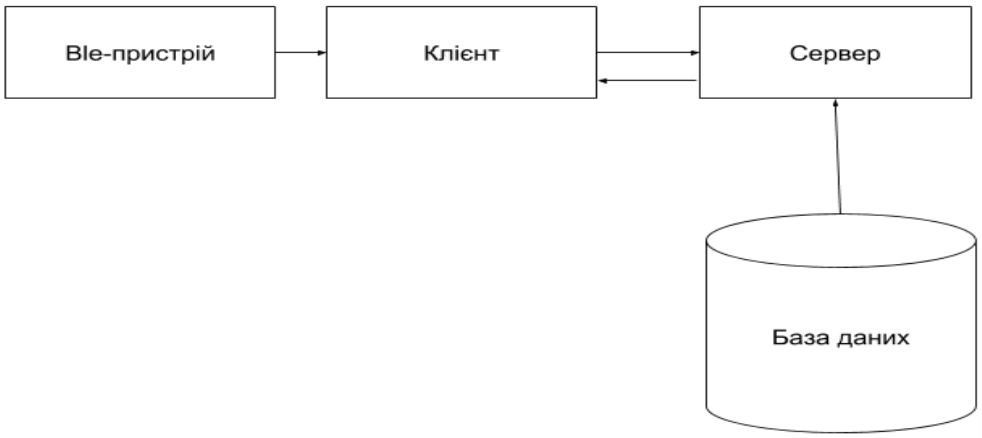
Результати дослідження

Автентифікація за допомогою ble-пристроя відбувається при ввімкненні програмного засобу. Коли користувач заходить в додаток, то з пристрою відправляється широкомовний запит. Коли користувач заходить в додаток з підключенним до смартфону ble-пристроєм, то йому надається можливість увійти до системи та отримати дані, які він зберігає в ній, а якщо ні то користувачу не надаватиметься доступ до тих пір поки не буде під'єднаний потрібний пристрій до смартфону. Коли користувач відкриває додаток і в нього увімкнений Bluetooth, то починається перевірка на підключення ble-пристроїв до смартфону за допомогою їхніх MAC-адрес.

Коли автентифікація за допомогою апаратного токена виконана успішно то користувач має змогу увійти до системи для отримання своїх даних. Користувач, якщо він зареєстрований, вводить свій логін та пароль і при успішному входженні отримує токен, який зберігається на стороні користувача, при наявності якого отримується доступ до захищених даних, а якщо ні то йому надається змога для реєстрації і його дані зберігатимуться в базі даних. Доступ до даних надається при відправлені токена в HTTP запиті в заголовках і при його існуванні у відповідь приходить належна інформація.

Розробка програмного засобу відбувається в два етапи. Спочатку відбується автентифікація користувача за допомогою апаратного токена, а саме MAC-адреси його ble-пристрою. А потім вже відбувається автентифікація користувача на основі jwt-токена, за допомогою якого він здатний отримати приховану інформацію.

Отже, за допомогою автентифікації до смартфону за допомогою апаратного токена та автентифікації до системи на основі jwt-токенів покращить захист власних даних та забезпечить швидкість підключення.



На основі цього засобу система буде максимально захищена, оскільки в інших аналогах використовується інший підхід. А в цьому засобі буде можливість захистити дані в якнайкращому ви- гляді і воно буде доступне для будь-якого початкового бізнесмена або студента.

Висновки

Проведено огляд існуючих технологій автентифікації. Проаналізовано основні аспекти роботи JWT. Запропоновано програмну частину системи автентифікації. Розглянутий спосіб є середньої складності й дозволяє забезпечити безпеку на належному рівні. Також нею можуть користуватися вже існуючі підприємства.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Методичні вказівки до проведення практичних занять та до виконання самостійної й індивідуальної роботи з дисципліни “Основи науково-дослідної роботи/ Укладачі: А. О. Азарова, В. В. Карпінець. – Вінниця: ВНТУ, 2013. – 44с.”
2. Аутентиікація на основі токен. [Електронний ресурс]. – Режим доступу: URL https://php-academy.kiev.ua/uk/blog/token-based-authentication-with-angularjs-nodejs- Назва з екрану
3. JWT [Електронний ресурс]. – Режим доступу: URL https://php-academy.kiev.ua/uk/blog/token-based-authentication-with-angularjs-nodejs
4. JSON Web Tokens [Електронний ресурс]. – Режим доступу: https://jwt.io/– Назва з екрану

Мусійчук Максим Тарасович — студент групи БС-14б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, Україна, e-mail: 1bs14b.musiychuk@gmail.com

Науковий керівник:
Куперштейн Леонід Михайлович — — к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна

Musiichuk M. — Student of Information Technologies and Computer Engineering Department, Vinnytsia National Technical University, Vinnytsia, Ukraine, e-mail: 1bs14b.musiychuk@gmail.com

Kupershtein L. — Phd. Associated Professor of Information Protection Chair, Vinnytsia National Technical University, Vinnytsia, Ukraine.