УДК 004.056.5

А.М. Луцків канд.техн.наук; доц., А.М. Калинюк
Тернопільський національний технічний університет імені Івана Пулюя, Україна

ІНТЕГРАЦІЯ ПІДСИСТЕМ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ У ВЕБ-СЕРВІСІВ

A.M. Lutskiv Ph.D., Assoc. Prof., A.M. Kalyniuk

BIOMETRIC AUTHENTICATION INTEGRATION INTO WEB-SERVICES

На сьогодні для аутентифікації користувачів веб-сервісів використовуються різні методи аутентифікації. Зокрема, до найпопулярніших належать наступні: OAuth 1.0[1], OAuth 2.0[2], Digest Auth[3], Bearer Token[4], Microsoft NTLM[5], AWS IAM v4[6], Netrc[7] та низка інших.

Важливою задачею, яку розв'язують при організації веб-серсвісів є надання користувачеві можливості для аутентифікації з урахуванням фактору зручності (usability). До одного із найпопулярніших на сьогодні видів аутентифікації належить біометрична аутентифікація особи. Серед наведених вище технологій найкраще підходять наступні методи аутентифікаці: OAuth 1.0[1], OAuth 2.0[2], Bearer Token[4], оскільки, вони дають змогу інтегрувати біометричний ключ в е-токен, на основі якого відбувається аутентифікація.

Для розв'язання задачі аутентифікації користувача на web-сервісі пропонується низка підходів:

– Simple Web Token (SWT) – найбільш простий формат, який передбачає набір довільних пар ім'я/значення в форматі кодування HTML form.

– JSON Web Token (JWT) – містить три блоки, які розділені крапками: заголовок, набір полів, і підпис;

– Security Assertion Markup Language (SAML) – визначає токени (SAML assertions) в XML-форматі, включає інформацію про елемент, про суб'єкт, необхідні умови для перевірки токену, набір додаткових тверджень (statements) про користувача.

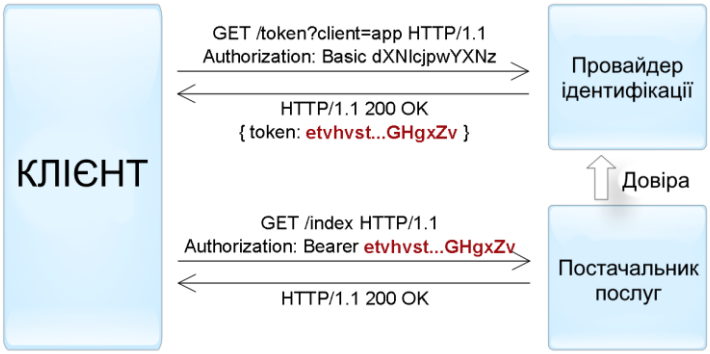

Рисунок 1. Приклад аутентифікації клієнта за допомогою токена переданого за допомогою Bearer схеми

Реалізація цього способу полягає в тому, що провайдер ідентифікації надає достовірні відомості про користувача в вигляді токена, а постачальник послуг (додаток) використовує цей токен для ідентифікації, аутентифікації і авторизації користувача.

Загалом, весь процес аутентифікації виглядає наступним чином:

– клієнт аутентифікується у провайдера ідентифікації одним із способів, специфічним для нього (пароль, ключ доступу, сертифікат, Kerberos, і т.д.);

– клієнт просить провайдера ідентифікації надати йому токен для конкретного постачальника послуг (Додатка). Провайдер ідентифікації генерує токен і відправляє його клієнту.

– Клієнт аутентифікується в Постачальнику послуг (Додатку) за допомогою цього токена.

JWT[8] є одним із найоптимальніших методів аутентифікації за критеріями:

– розміру токену;

– підтримки в мовах/технологіях програмування (Java, NodeJS, Python та інших);

– простотою інтеграції (в URL, параметр POST-запиту, в HTTP-заголовок).

Використання наведеної схеми може бути використано при доступі до веб-сервісу клієнтів, які працюють через веб-переглядач на робочих станціях, а також з мобільних додатків на мобільних терміналах (телефонах, планшетах, тощо). При цьому робочі станції та мобільні телефони повинні бути обладнані апаратними засобами для отримання біометричних ключів. У даному контексті, актуальною задачею є інтеграція біометричних ключів в запит аутентифікації від користувача до провайдера ідентифікації.

Задача інтеграції біометричної аутентифікації у веб-сервіси є реалізована в низці проектів. Ключовою проблемою даних сервісів є проблема уніфікованості методів генерування цих ключів. Для створення даних сервісів використовуються різні бібліотеки [9], зокрема й низка відкритих та безкоштовних, які підтримують протокол BioAPI.

Для генерування JWT-токена на основі динамічного біометричного ключа необхідно, запропонувати механізм однозначного формування криптографічного хешу на основі даного біометричного ключа засобами клієнтського програмного забезпечення. Даний хеш буде записуватись у відповідне поле JWT-токену й використовуватись аналогічно до звичайно отриманого хеша на основі секретних даних користувача.

Література

1. RFC 5849 - The OAuth 1.0 Protocol - IETF Tools [Електронний ресурс] - Режим доступу до ресурсу: https://tools.ietf.org/html/rfc5849.
2. RFC 6749 - The OAuth 2.0 Authorization Framework - IETF Tools [Електронний ресурс] - Режим доступу до ресурсу: https://tools.ietf.org/html/rfc6749.
3. RFC 7616 - HTTP Digest Access Authentication - IETF Tools [Електронний ресурс] - Режим доступу до ресурсу: https://tools.ietf.org/html/rfc7616.
4. RFC 6750 - The OAuth 2.0 Authorization Framework: Bearer Token Usage [Електронний ресурс] - Режим доступу до ресурсу : https://datatracker.ietf.org/doc/rfc6750.
5. RFC 4559 – SPNEGO - based Kerberos and NTLM HTTP Authentication in Microsoft Windows [Електронний ресурс] - Режим доступу до ресурсу: https://tools.ietf.org/html/rfc4559.
6. RFC: 3986 - Uniform Resource Identifier (URI): Generic Syntax [Електронний ресурс] - Режим доступу до ресурсу: https://tools.ietf.org/html/rfc3986.
7. RFC 959 - FILE TRANSFER PROTOCOL (FTP) [Електронний ресурс] - Режим доступу до ресурсу: https://tools.ietf.org/html/rfc959.
8. RFC 7519 - JSON Web Token (JWT) [Електронний ресурс]- Режим доступу до ресурсу: https://tools.ietf.org/html/rfc7519 .
9. Засоби динамічної біометрії у веб-сервісах [Електронний ресурс] – Режим доступу до ресурсу: https://www.tutorialspoint.com/assets/white-papers/126.pdf.