УДК 004.056.5

Б. Г. Гончарук
І. Р. Арсенюк

ЗАХИСТ ВЕБ-ДОДАТКІВ ТА ВЕБ-СЛУЖБ ЗА ДОПОМОГОЮ БАГАТОЕТАПНОЇ ВЕРИФІКАЦІЇ З ВИКОРИСТАННЯМ ПОТОКУ АВТОРИЗАЦІЇ ЧЕРЕЗ ВЕБ-СЕРВЕР

Вінницький національний технічний університет

Анотація

Запропоновано рішення для реалізації алгоритмів автентифікації та авторизації веб-сервісів та веб-служб із використанням потоку авторизації через веб-сервер.

Ключові слова: автентифікація, авторизація, захист даних, веб-сервіс, веб-служба, веб-додаток, конфіденційність, персональні дані.

Abstract

An approach is proposed on using authorization web-server flow to implement web-service authentication and authorization.

Keywords: authentication, authorization, data protection, web-service, web-application, privacy, personal data.

Проблема використання, поширення та захисту персональних даних є глобальною та однією з найважливіших у сфері технологічного простору. Інформація – найцінніший ресурс яким володіє людина, це стосується також і конфіденційної інформації, тому, очевидно, захист та обмеження доступу – це класичні проблеми, рішення яких еволюціонують разом із тим як вдосконалюються інформаційні технології. Втрата даних може мати непередбачувані наслідки як для сторони, що володіє даними так і для сторони, що зацікавлена у наданні послуг обробки та захисту цих даних. Одним із надійних шляхів захисту є застосування алгоритму так званого потоку авторизації через веб сервер “Authorization Web Server Flow” із використанням коду авторизації та токена доступу [1 – 3].

Для захисту веб-додатку або веб-служби за допомогою алгоритму наведеного вище, потрібно реалізувати програмну інфраструктуру, що буде містити такі компоненти:

- Юзер – суб’єкт (клієнт або аплікація), що володіє даними на захищеному ресурсі.
- Юзер-агент – аплікація, за допомогою якої реалізується взаємодія клієнта та веб-додатку.
- Веб-служба або веб-додаток – ресурс, який здійснює первинну ідентифікацію, автентифікацію та авторизацію та надає доступ до запитуваної юзер-агентом інформації.
- Сервер авторизації – сервер, що містить два незалежні ендпоінти: для генерації, видачі програмного токена та здійснення авторизації, видачі авторизаційного коду.
- Ресурс сервер – це ресурс, що містить дані.

Основний процес взаємодії юзера та веб-додатку наведено нижче.

Під час первинного запиту юзера, веб-додаток перенаправляє користувача на сервер авторизації, який відповідає за генерацію відповідного інтерфейсу для первинної ідентифікації та авторизації користувача.

Юзер вводить необхідні дані (логін, пароль тощо) та надсилає на сервер авторизації.

Сервер авторизації проводить валідацію даних, генерує код авторизації та надсилає на юзер-агент інструкцію переадресації на веб-сервер із використанням коду авторизації.

Юзер-агент надсилає код авторизації на веб-сервер.

Веб-сервер надсилає код авторизації на сервер авторизації.

Сервер авторизації здійснює валідацію, генерує токен доступу та надає його веб-серверу.

Веб-сервер здійснює запит до ресурс серверу із наданням токена доступу.

Ресурс-сервер здійснює валідацію токена доступу та повертає (або не повертає) відповідні дані на веб-сервер.

Даний процес наведено на рис. 1.

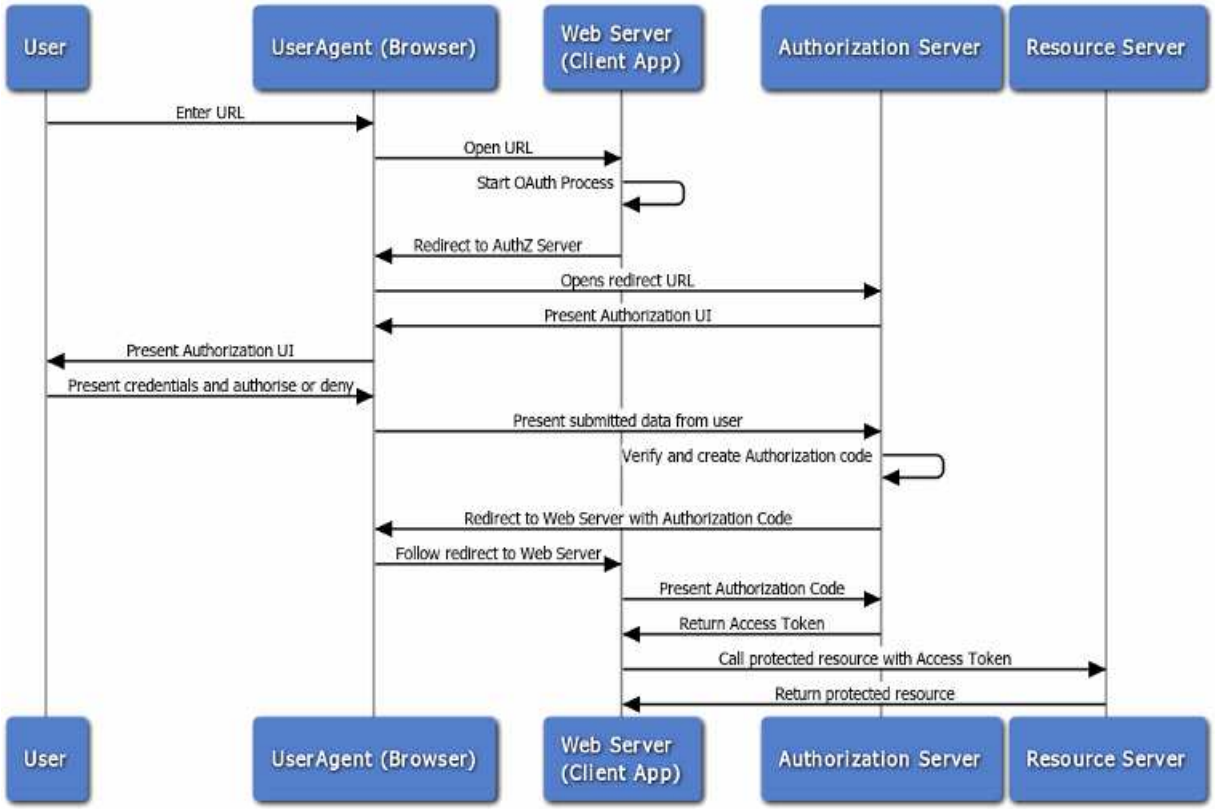

Рис. 1. Процес взаємодії юзера та веб-додатку

Висновки

Запропонований алгоритм авторизації, автентифікації, аналізу та передачі персональних даних з використанням потоку авторизації через веб-сервер дає можливість захистити дані на кожній ітерації взаємодії. Варто також зазначити незалежну багатоетапну перевірку та відстеження актуальності даних клієнта, який надсилає запити до веб-додатку.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. OAuth [Електронний ресурс] – Режим доступу: https://docs.oracle.com/cd/E39820_01/doc.11121/gateway_docs/content/part_oauth.html

2. Microsoft identity platform and OAuth 2.0 authorization code flow – [Електронний ресурс] – Режим доступу: https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth2-auth-code-flow

3. Authorization code grant flow [Електронний ресурс] – Режим доступу: https://docs.axway.com/bundle/APIGateway_762_OAuthUserGuide_allOS_en_HTML5/page/Content/OAuthGuideTopics/oauth_flows_auth_code.htm

Гончарук Богдан Ігорович – студент групи 1КН-16Б, факультету інформаційних технологій та комп'ютерної інженерії, Вінницького національного технічного університету, м. Вінниця, e-mail: universalshon@gmail.com

Арсенюк Ігор Ростиславович – доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, м. Вінниця

Honcharuk Bohdan I. – Student, Department of information technology and computer engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: universalshon@gmail.com

Ihor Arseniuk R. – Cand. Sc. (Eng), Assistant Professor of the Chair of Computer Science, Vinnytsia National Technical University, Vinnytsia