https://www.proconference.org/index.php/usc/article/view/usc24-00-010
DOI: 10.30888/2709-2267.2024-20-00-010

УДК 004.056.5

AUTHENTICATION AND AUTHORIZATION INVOLVING THIRD PARTIES: MODERN APPROACHES AND SOLUTIONS

АВТЕНТИФІКАЦІЯ ТА АВТОРИЗАЦІЯ ІЗ ЗАЛУЧЕННЯМ ТРЕТІХ СТОРІН: СУЧАСНІ ПІДХОДИ ТА РІШЕННЯ

Korobeinikova T.I. / Коробейнікова Т.І.
c.t.s., as.prof. / к.т.н., доц.
ORCID: 0000-0003-2487-8742
Matviichuk A.A. / Матвійчук А.А.
студент / student
Lviv Polytechnic National University, S. Bandera St. 12, Lviv, 79013
Національний університет «Львівська політехніка», Львів, Бандери, 12, 79013
Nepyivoda M.V./ Непийвода М.В.
викладач спецдисциплін / teacher of special disciplines
ORCID: 0000-0002-9383-7752
Vinnytsia Technical Vocational College, st. 91/2 Khmelnytske highway, Vinnytsia, 21021
Вінницький технічний фаховий коледж, вул. Хмельницьке шосе, 91/2, м. Вінниця, 21021

Анотація. *У роботі досліджується базова автентифікація на вебресурсах, розглядаються стандарти автентифікації та авторизації із залученням третіх сторін: OAuth 2.0 та OpenID Connect. Запропоновано альтернативний механізм автентифікації та авторизації, що використовує окремий вебресурс для захисту персональних даних. Такий механізм замінює стандартні сторінки входу та реєстрації на сторінки, створені вебресурсами, і не вимагає додаткових дій від користувача. Вебресурс отримує токен доступу та ідентифікаційний токен з інформацією про користувача.*

Ключові слова: *ризики мережевої безпеки, загрози безпеці, вразливості, процеси автентифікації та авторизації.*

Abstract. *The work explores basic authentication on web resources and discusses authentication and authorization standards involving third parties: OAuth 2.0 and OpenID Connect. An alternative authentication and authorization mechanism is proposed, utilizing a separate web resource for safeguarding personal data. This mechanism replaces standard login and registration pages with those created by the web resources, requiring no additional actions from the user. The web resource obtains an access token and an identity token containing user information.*

Key words: *network security risks, security threats, vulnerabilities, authentication and authorization processes.*

Вступ.

Базова автентифікація – це метод автентифікації на вебресурсах, тут вебклієнт передає логін та пароль на сервер в заголовку HTTP-запиту [1]. Ця інформація передається у відкритому вигляді, але кодується за Base64 [2] і його легко декодувати, тому базова автентифікація вважається небезпечною, якщо використовувати її без захищеного з'єднання, наприклад, через HTTPS. RFC

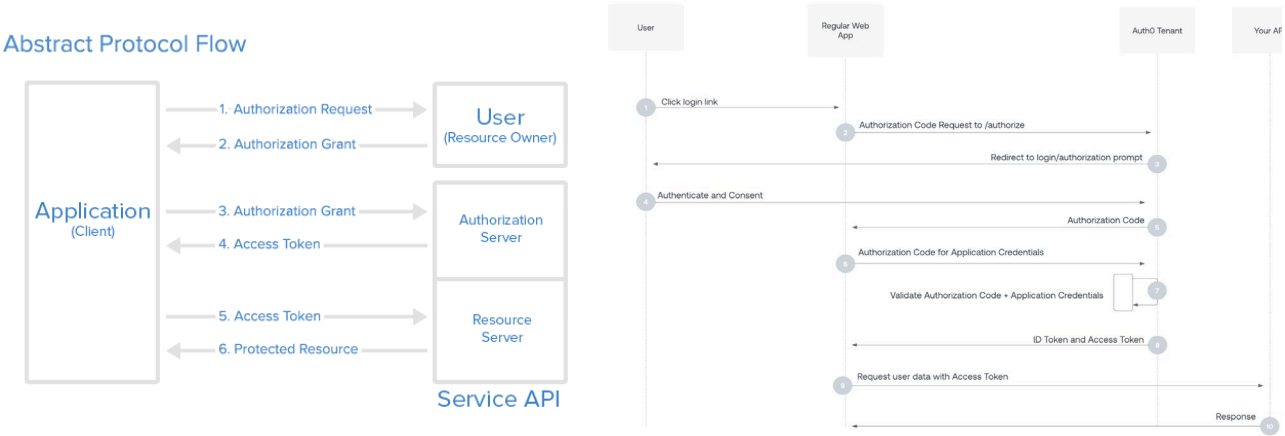
7235 [3] визначає структуру автентифікації HTTP, яка може використовуватися сервером для авторизації запиту клієнта, а клієнтом для надання інформації автентифікації [4-5].

Автентифікація та авторизація із залученням третіх сторін передбачає обидва ці процеси, проте використовує для цього 2 різні стандарти: OAuth 2.0 для авторизації та OpenID Connect для автентифікації [5-7].

Автентифікація та авторизація із залученням третіх сторін.

Оскільки OpenID Connect є надбудовую над OAuth 2.0 то перш розглянемо стандарт авторизації.

OAuth 2.0 – це протокол авторизації, що дозволяє видати одному сервісу права на доступ до ресурсів на іншому сервісі. Позбавляє необхідності довіряти додатку логін і пароль, і надає обмежений набір прав. Опис механізму роботи описано в RFC 6749. OAuth визначає 4 компоненти: власника ресурсу, клієнта, сервера ресурсів та сервера авторизації. З точки зору розробника, API сервісу OAuth виконує роль сервера ресурсів і сервера авторизації. Ми будемо називати обидві ці ролі разом роллю API сервіс. Стандарт RFC 6749, описує декілька механізмів авторизації, загальна діаграму взаємодії сервісів відповідно своєї ролі є на рис. 1, а та за авторизаційним кодом (рис. 1, б).



а) діаграма взаємодії сервісів б) взаємодія за авторизаційним кодом

Рисунок 1 Механізми авторизації за OAuth 2.0

Джерела [4-5]

Загальний механізм має такі етапи:

1. Додаток запитує у користувача доступ до ресурсів сервісу;
2. Якщо користувач авторизував запит, програма отримує дозвіл на авторизацію;
3. Додаток запитує токен доступу від сервера авторизації (API), надає автентифікацію своєї власної особистості та тип доступу;
4. Якщо ID програми автентифікований і тип доступу є дійсним, API видає токен доступу до програми. Авторизація завершена;
5. Програма запитує ресурс із API і дає токен для автентифікації;
6. Якщо токен доступу дійсний, API надає ресурс програмі.

OpenID Connect (OIDC) – це протокол автентифікації користувачів під час входу для доступу до цифрових служб. Організації можуть використовувати безпечну систему керування ідентифікацією та доступом (IAM), як Microsoft Entra ID (раніше Azure Active Directory), як основний засіб автентифікації ідентифікаторів, а далі використовувати OIDC для передачі цієї автентифікації третій стороні.

Автентифікація та авторизація із залученням третіх сторін: запропоноване рішення.

Авторами пропонується замість авторизаційного серверу впровадити створення окремого вебресурсу який спеціалізується на захисті персональних даних, наданням автентифікації та авторизації користувачам і ресурсам, створенням можливості перекласти відповідальність за цей процес, що є одним з рішенням обробки ризику відповідно стандарту ISO 27005.

Звичайний підхід до автентифікації користувачів передбачає використання сторінки входу або сторінки реєстрації вебресурсу, до якого ви бажаєте отримати доступ. У цій моделі механізм автентифікації та безпека збереження даних забезпечуються самим вебресурсом. В нашому випадку ці сторінки будуть надані запропонованим сервісом, тобто сам вебресурс немає ніякого відношення до механізму автентифікації. Це досягається засобами протоколу OIDC, та типом авторизації за авторизаційним кодом.

Механізм складається з 10 етапів та майже повністю повторює вхід за авторизаційним кодом який використовує OAuth 2.0. Відмінністю є те, що авторизаційним провайдером є не сторонній вебресурс а запропонований сторонній сервіс. На рис. 2 можна бачити 4 основних компонента: користувач, вебресурс, запропонований сервіс авторизації, сторінка входу.

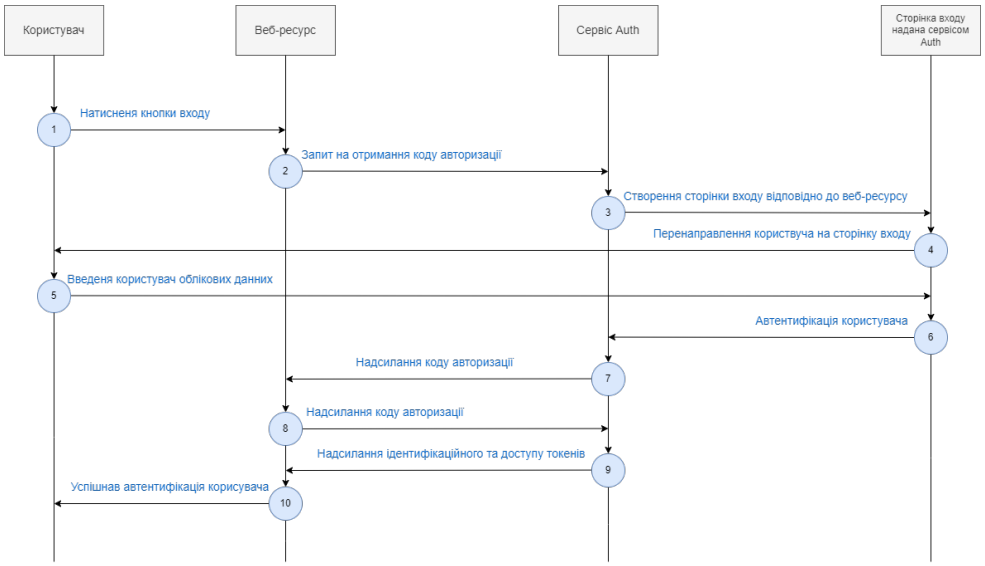


Рисунок 2 – Механізм входу та реєстрація запропонованого сервісу

Авторська розробка

Схема вище описує крок за кроком механізм автентифікації та реєстрації користувача використовуючи запропонований сервіс:

1. Натиснення кнопки входу – користувач на вебресурсі хоче до нього увійти і натискає кнопку входу;
2. Запит на отримання коду авторизації – вебресурс запитує в сервісу авторизації дозвіл на проведення автентифікації користувача;
3. Створення сторінки входу до вебресурсу – сторінка входу для кожного вебресурсу буде визначена самим вебресурсом.
4. Перенаправлення користувача на сторінку входу;
5. Введення користувачем облікових даних;
6. Автентифікація користувача – сервіс авторизації перевіряє облікові дані;

7. Надання коду авторизації – сервіс авторизації після успішної автентифікації користувача надсилає код до вебресурсу відповідно до протоколу OAuth 2.0;
8. Надання коду авторизації – вебресурс обмінює раніше наданий авторизаційний код на необхідні йому токени;
9. Надання токенів – сервіс авторизації надає необхідні токени які обов'язково включать ідентифікаційний токен та токен доступу, та в деяких випадках токен оновлення;
10. Успішна автентифікація користувача – після введення облікових даних користувач успішно ввійде до вебресурсу.

Висновки.

В даній роботі запропоновано альтернативний механізм надання автентифікації та авторизації користувачам і ресурсам. Запропонований механізм на відміну від існуючих має можливість замінити стандартну сторінку входу та реєстрації на сторінки створені вебресурсами які відповідають старому дизайну. Також від користувача не очікується додаткових дій на противагу до базового методу автентифікації. В кінці роботи механізму вебресурс отримав токен доступу, з яким він може отримувати додаткову інформацію про користувача, а також змінювати інформацію про нього, і ідентифікаційний токен який зберігає в собі базову інформацію про користувача.

Література:

1. De Soete M. Two-Factor Authentication. Encyclopedia of Cryptography and Security. Boston, MA, 2011. P. 1341.

2. Landrock P. Two-Factor Authentication. Encyclopedia of Cryptography and Security. P. 638.

3. Security Analysis and Improvements of Two-Factor Mutual Authentication with Key Agreement in Wireless Sensor Network sensors ISSN 1424-8220

4. Holmes S. Getting MEAN with Mongo, Express, Angular, and Node. Manning Publications, 2015. 440 p.

5. Audio Fingerprinting. An Introduction to Audio Content Analysis. Hoboken, NJ, USA, 2012. P. 163–167.

6. Biometrics: Personal Identification in Networked Society. Springer, 2005. 411 p.

7. Трояновська Т. І. Побудова захищених мереж на базі обладнання компанії Cisco. // Захарченко С.М., Трояновська Т. І., Бойко О.В. Навчальний посібник. Вінниця : ВНТУ, 2017. – 133 с.

Науковий керівник: к.т.н., доц. Коробейнікова Т.І.

Стаття надіслана: 17.05.2024 р.