https://www.sworldjournal.com/index.php/swj/article/view/swj25-00-022
DOI: 10.30888/2663-5712.2024-25-00-022

УДК 004.056.5

REVIEW OF SOLUTIONS FOR IMPROVING AUTHENTICATION AND AUTHORIZATION PROCESSES ON WEB RESOURCES

ОГЛЯД РІШЕНЬ ДЛЯ ПОКРАЩЕННЯ ПРОЦЕСІВ АВТЕНТИФІКАЦІЇ ТА АВТОРИЗАЦІЇ НА ВЕБРЕСУРСАХ

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. *В роботі розглядається аналаіз основних понятть автентифікації та авторизації на вебресурсах, демонструючи їх необхідність та застосування на вебресурсах. Проаналізовано різні методи та засоби захисту, включно із логіном і паролем, біометричними даними, одноразовими паролями та багатофакторною автентифікацією. Також обговорюються потенційні вразливості та загрози, включаючи фішинг, парольні атаки, та соціальну інженерію, з акцентом на стратегії мінімізації ризиків і поліпшення безпеки вебресурсів.*

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

Вступ.

Автентифікація та авторизація – це ключові концепції в сучасних технологіях, які були створені ще до існування вебресурсів для управління доступом і ідентифікації осіб [1-3]. Для входу, скажімо до соціальної мережі, користувач мусить пройти автентифікацію (довести свою ідентичність), використовуючи унікальне ім'я та пароль, або двоетапну аутентифікацію, що може передбачати введення коду, отриманого через СМС або електронну пошту. Після успішної автентифікації, користувач отримує доступ до своєї персональної сторінки, редагувати яку може тільки він. Таким чином, соціальна мережа відображає застосування концепцій автентифікації та авторизації до потреб віртуального простору, де передбачено захист приватності та контроль доступу до персональних даних [4-7].

Точки застосування автентифікації та авторизації на вебресурсах.

Застосування концепції автентифікації та авторизації безпосередньо впливає на безпеку користувачів.

Процес автентифікації, як правило, відбувається одноразово під час входу в систему. В той же час, авторизація яка визначає, які дії користувач може виконувати перевіряється постійно. Проте незважаючи на ці ідеалізовані точки використання, все одно є виключення.

Процес авторизації має бути всюди, проте тільки для користувачів які пройшли автентифікацію можна визначити права доступу для окремого користувача. Тому сторінки входу чи авторизації, або ті які не вимагають автентифікації, не мають використовувати авторизацію.

Ефективне застосування автентифікації та авторизації дозволяє вебресурсам не тільки захищати конфіденційність користувачів та їхні дані, але й надавати персоналізований досвід використання, забезпечуючи доступ відповідно до ролі та прав користувача. Враховуючи широкий спектр вебресурсів та їхніх вимог до безпеки, точки застосування автентифікації та авторизації можуть відрізнятись.

Засоби автентифікації.

Логін і пароль – це введення ідентифікатора користувача (логіну) та пароля для підтвердження ідентичності. Цей засіб є найпоширенішим через його простоту реалізації, мізерний об'єм даних якими користувач ділиться з вебзастосунком, а також за малу відповідальність за особисті дані користувача, оскільки зберігати їх надзвичайно просто та безпечно [4].

Біометрична автентифікація – це використання фізіологічних чи поведінкових характеристик, таких як відбиток пальця, розпізнавання обличчя, розпізнавання ока або голосу. Цей засіб використовувався раніше тільки для спец об’єктів та зараз майже кожен телефон розблоковується за допомогою відбитку пальця або знімком обличчя. Чому ж цей засіб не використовуються частіше, адже від надзвичайно точний, вся справа в відповідальності за зберігання таких даних, не кожен користувач готовий ділитись своїми унікальними біометричними даними. Тому ця інформація зберігається або в державних структурах або безпосередньо в пристрої що розпізнає, і аж ніяк не в хмарних сховищах [6].

Автентифікація на основі ключів – це використання криптографічних ключів (як SSH-ключі, сертифікати) для перевірки ідентичності користувача [2]. Це поширений засіб автентифікації для спеціалізованих задач, таких як підключення до віддаленого сервера або доступу до криптогаманця. Надає високу стійкість завдяки розміру ключів та методам їх перевірки; проте компрометація ключа призведе до компрометації всього з’єднання (рис. 1а).

а) процес обміну ключами для встановлення з’єднання

б) процес генерації одноразового коду (OTP)

Рисунок 1 – Засоби автентифікації

Авторська розробка

Одноразові паролі (OTP) – генерація одноразових паролів для кожної сесії або транзакції, які користувач вводить для автентифікації (рис. 1,б). Цей засіб став доповняльним, оскільки не визначає ідентичність користувача. Механізм генерації одноразового коду постійно змінюється.

Автентифікація з використанням двоетапної або багатофакторної автентифікації – це поєднання декількох методів автентифікації, наприклад, пароль і одноразовий код, для підвищення безпеки. Цей засіб є комбінацією використання логіну та паролю та одноразового пароля (рис. 2) і дає змогу не тільки перевірити правильність облікових даних, а також впевнитись що користувач дійсно є власником облікового запису.

Рисунок 2 – Схема роботи двох етапної автентифікації

Джерело [7]

Дозволяє зберегти облікових запис користувача навіть після компрометації паролю. Недоліком є необхідність доступу до одноразового паролю (код з SMS), який користувач не отримає без телефону.

Засоби авторизації.

Рольова модель – це призначення прав та дозволів користувачам на основі їх ролі в системі. Прикладом буде цього це вхід в ОС Windows. Гість не буде мати можливості змінювати файлову систему та будь-як впливати на ОС, окрім того, як йому це дозволено вже іншими засобами авторизації [2, 7].

Access Control Lists (ACLs) – це інструмент, який визначає права доступу до конкретних ресурсів, таких як файли, папки, мережеві ресурси, або інші об'єкти в інформаційній системі чи на мережі (рис. 3).

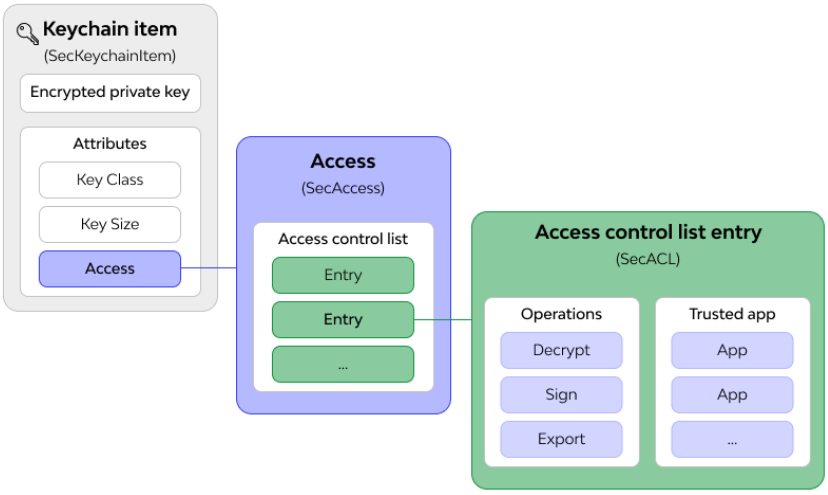
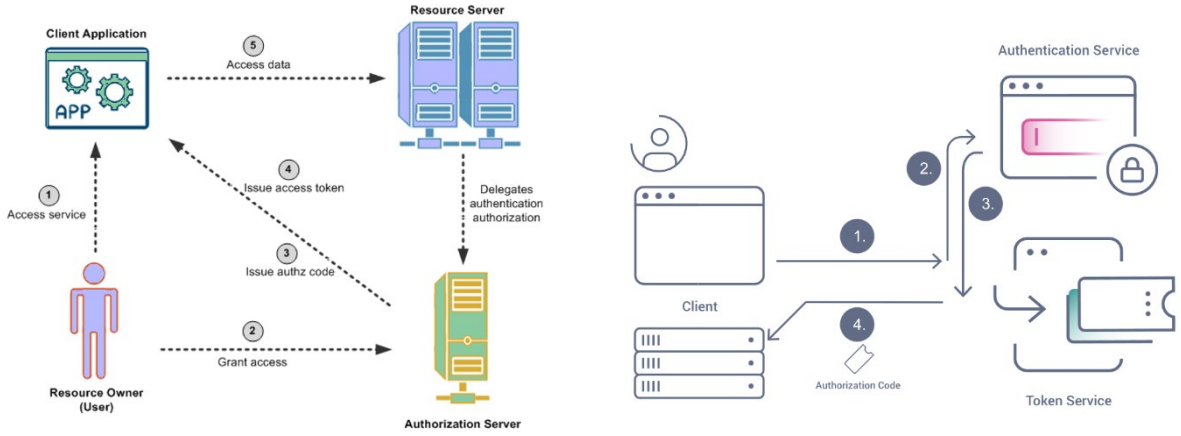


Рисунок 3 – Схема списку контролю доступу

Джерело [7]

ACLs надають системному адміністратору чи власнику ресурсу засіб для точного управління правами користувачів. Кожен запис в ACL визначає, який користувач, група користувачів чи роль має право доступу до ресурсу, а також, які конкретні дозволи вони мають. Приклад схеми списків доступу можна бачити на рис. 3, де показано структуру ключу який має ACL, та структуру кожного окремого доступу до певного ресурсу та відповідні дії над ними.

OAuth (Open Authorization) – це протокол авторизації для забезпечення безпеки та конфіденційності під час взаємодії між додатками та сервісами. Користувачі можуть надавати стороннім додаткам обмежений доступ до своїх ресурсів (наприклад, до облікового запису в соціальній мережі чи електронної пошти) без необхідності розкривати свій пароль. Досягається це за допомогою схеми показаної на рисунку 4, а.



а) OAuth б) OpenID Connect

Рисунок 4 – Схеми роботи протоколів

Авторська розробка

OpenID Connect – протокол аутентифікації, побудований на основі OAuth2.0 і розроблений для спрощення та безпечної ідентифікації користувачів. Основна мета OpenID Connect полягає в тому, щоб користувачі могли використовувати свої існуючі облікові записи на різних онлайн-платформах, таких як Google, Facebook, або інші, для автентифікації на інших вебсайтах без необхідності створення нових паролів або облікових записів (рис. 4, б).

Може здатись що OpenID Connect та OAuth однакові про це не так. Auth 2.0 не займається автентифікацією користувачів, а надає стороннім додаткам обмежений доступ до захищених ресурсів. В той час як OpenID Connect є розширенням OAuth 2.0, яке додає шар автентифікації. OIDC дозволяє клієнтам виконати автентифікацію передавши протоколом OAuth 2.0 дані про обліковий запис від третьої сторони .

Огляд вразливостей під час автентифікації та авторизації на вебресурсах.

Існує досить багато методів автентифікації та авторизації, і кожен має свої вразливості, які інші засоби допомагають частково нівелювати і всі вони розроблені для захисту від найбільш поширених загроз. Наприклад, логін і пароль є зрозумілими у використанні, проте вразливими до компрометації. У разі витоку або викрадення облікових даних, користувач може втратити доступ до

акаунта та конфіденційної інформації. Це вирішується за допомогою використання одноразових паролів, які надсилаються на телефон користувача, забезпечуючи додатковий рівень захисту.

Фішинг. Передбачає використання підроблених повідомлень або вебсайтів для обману людей з метою отримання конфіденційної інформації (паролі, номери кредитних карт тощо). Типи фішингу: фішинг поштою, соціальний фішинг, фішинг в соцмережах, фішинг через вебсайти, спільний фішинг.

Парольні атаки. Парольні атаки є важливим засобом кібератак, де зловмисники намагаються отримати доступ до облікових записів, використовуючи різні методи для вгадування або перебору паролів. Хоча цей тип атаки є менш поширеним через затрати часу на підбір пароля та підвищення обізнаності користувачів у сфері інформаційної безпеки, він все ще залишається значною загрозою. Типи парольних атак: метод грубої сили (Brute Force), атаки з перебору паролів (Dictionary Attacks).

Атаки на токени сесії. Це спроби зловмисників отримати доступ до активної сесії користувача на вебсайті або додатку. Токени сесії використовуються для ідентифікації та авторизації користувачів під час їх візиту на вебсайт. Оскільки після входу у свій обліковий запис не потрібно вводити пароль знову, створюється токен сесії який дає вам змогу певний час використовувати його замість облікових даних. Токени сесії використовуються для зберігання інформації про авторизовану сесію користувача на сервері. Використовуючи схему перехоплення токену зловмисник може отримати доступ без автентифікації. Можливі сценарії атаки на токен сесії: злам токену сесії, перехоплення токенів, збереження токенів на клієнтському боці.

Відповідальні за захист від таких атак є вебресурси, які мають надавати необхідний рівень безпеки, який не дозволить отримати доступ до облікового запису використовуючи тільки токен сесії.

Витоки облікових даних. Зважаючи на вразливості перераховані вище, від цієї загрози нічого не допоможе. Витоки облікових даних відбуваються, коли конфіденційна інформація про користувачів потрапляє в руки злочинців. Такі атаки стаються регулярно, через використання сторонніх ресурсів для збереження даних про користувачів які можуть мати вразливості. Це має серйозні наслідки для безпеки користувачів і компаній. Загрози витоку облікових даних: вразливості безпеки користувачів, вразливості баз даних де зберігаються облікові дані.

Соціальна інженерія. Соціальна інженерія – це один з найефективніших способів атаки через несвідомість людей з доступом до конфіденційної інформації. Цей метод використовує маніпуляцію та переконання для обману користувачів для їхньої інформаційної безпеки чи облікових даних. Найчастіші прийоми соціальної інженерії: маніпуляція, обман, психологічний тиск, підробка особистості.

Пошуки рішень, що стосуються поліпшення процесів автентифікації та авторизації на вебресурсах.

Кожен з процесів автентифікації або авторизації має свої рішення що стосуються поліпшення інформаційної безпеки. Звісно захиститись від всіх

загроз неможливо але мінімізувати загрози можна знаючи та використовуючи методи захисту від найпоширеніших загроз. Розглянемо детальніше про захист кожної з вразливостей (табл. 1).

Таблиця 1 – Рішення щодо поліпшення процесів автентифікації та авторизації

Тип атаки	Рішення
Фішинг	– Освіта користувачів – Використання антифішингових фільтрів – Двофакторна аутентифікація (2FA) – Перевірка URL-адрес
Парольні атаки	– Складність паролів – Зміна паролів – Використання парольних менеджерів – Двофакторна аутентифікація (2FA) – Перевірка паролів на слабкість
Атаки на токени сесії	– Використання протоколу HTTPS – Одноразові токени
Витоки облікових даних	– Різні паролі для різних облікових записів – Перевірка вебресурсів на яких ви реєструєтесь
Соціальна інженерія	– Освіта та навички користувачів – Підвищення свідомості – Підтвердження ідентифікації – Обмеження доступу – Відстеження та аудит

Авторська розробка

Висновки.

В даній роботі виконаний аналіз сучасних методів та засобів авторизації та автентифікації на вебресурсах і запропоновано рішення щодо поліпшення процесів автентифікації та авторизації. Робота є актуальною з огляду на те, що більшість кібератак спрямовані на отримання конфіденційної інформації, використовуючи різноманітні методи. Ці загрози часто вдосконалюються, що стимулює розробку нових систем захисту. Проте, незважаючи на технічні засоби безпеки, абсолютний захист неможливий через людський фактор.

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.

Abstract. *The paper examines the analysis of the key concepts of authentication and authorization on web resources, demonstrating their necessity and application on web platforms. Various methods and means of protection are analyzed, including login and password, biometric data, one-time passwords, and multi-factor authentication. Potential vulnerabilities and threats are also discussed, including phishing, password attacks, and social engineering, with a focus on strategies to minimize risks and improve the security of web resources.*

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

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

Стаття надіслана: 17.05.2024 р.