Частота оновлення маркерів доступу при використанні OAuth 2.0 технології

УДК 004.9

Микола Герцюк[1], Дмитро Новостройний[2]

Державний університет інформаційно-комунікаційних технологій,
gertsiuk@gmail.com[1], digitaldut2022@gmail.com[2]

Одним з найкращих протоколу для аутентифікації користувача до системи є протокол OAuth 2.0. Таке судження може бути зроблене виходячи з аналізу логіки роботи та популярності використання даного протоколу. Зокрема, даний протокол забезпечує можливість проведення валідації сесії, використовуючи маркери доступу(далі токени), які мають визначений час валідації, та час від часу мають бути перегенеровані. Такий підхід робить низькою можливість перехоплення та використання токену зловмисниками. Однак, налаштування часу життя такого маркеру є доволі важливою складовою, оскільки впливає на рівень безпеки інформаційної системи. Аналіз різних інформаційних систем, як Google[1], Facebook[2], Azure[3] та інших систем, що використовує OAuth 2.0 показав, що токени мають наступний час життя:

- короткі: мають час життя від 5 хвилин до 1 години;
- довгі: від 8 годин до 30 днів.

Короткі токени мають наступні переваги для інформаційної системи:

- низький ризик витоку інформації. Токени, що мають короткий час життя дозволяють зменшити ризик в разі, якщо потраплять до рук зловмисників. Очевидно, якщо токен дійсний лише обмежений час, зловмисники матимуть менше часу на його використання в своїх цілях перед тим, як строк їхньої дії буде недоступний;
- менеджмент доступу. Короткий час життя токенів сприяє кращому контролю за доступом користувача до інформаційної системи. Такий підхід дозволить змусити користувачів отримувати токени частіше. Таким чином, адміністратори систем зможуть більш динамічно реагувати на зміну прав доступу та актуалізувати дані користувачів в сесіях.

Водночас, короткі токени мають деякі недоліки, що негативно впливають на функціонування системи:

- збільшене навантаження на сервери авторизації. Короткий час життя токену означає часте оновлення їх. У випадку з великою кількістю користувачів, навантаження на сервер авторизації зростає. Оскільки сервер авторизації є ключовим в будь-якій інформаційній системі, що має функціонал авторизації, продуктивність всієї системи погіршується;
- складність управління сеансами користувачів. Оскільки короткий час життя токенів означає часте їх оновлення, розробники повинні описувати більш складну логіку управління сеансами користувачів. Таким підхід, наприклад, змусить їх створювати окремі таймери в клієнтських складових системи для оновлення, і відмовитись від більш простої логіки оновлення «за запитом»;

– підвищений обсяг трафіку мережі. Часте оновлення токенів означає велику кількість запитів, що можуть призводити до неминучого збільшення трафіку в мережі і викликати проблеми навантаження мережі.

Аналізуючи переваги та недоліки, можна зробити висновок, що короткі токени є більш безпечними, однак вони негативно впливають на продуктивність системи.

Довгий час життя токенів має наступні переваги:

– невисоке навантаження на сервери. Невелика частота оновлення токенів не призводить високого навантаження на сервер авторизації;
– невисоке навантаження на трафік. Низька частота запитів на оновлення токенів не перевантажує сервер авторизації великою кількістю запитів. Відповідно, не спричиняє високе навантаження на трафік.

Однак, існують і недоліки такого підходу:

– збільшений ризик безпеки. В разі заволодіння токеном зловмисниками такий токен стає компрометованим на довгий час. Таким чином існує ризик втрати великої кількості даних;
– складніше управління правами доступу. Довгий час життя токену вимагає в системних адміністраторів враховувати дану характеристику при змінах прав доступу, або інших метаданих, що робить управління користувачами ускладненим та більш статичним процесом.

Аналіз довгих токенів показав, що хоча продуктивність інформаційної системи покращується, безпека даних погіршується.

Існує, також варіант використовувати середній час життя токенів, що має значення від 1 до 8 годин. Такий варіант є прийнятним, як «золота середина» між безпекою та навантаженням на інформаційні системи.

Врахувавши вищеописані переваги та недоліки різних часів життя токенів можна дійти таких висновків:

– якщо безпека інформаційної системи є пріоритетною, потрібно використовувати якнайкоротший час життя токену. Однак, потрібно обов'язково враховувати це при розробці та розгортанні інформаційної системи;
– якщо продуктивність системи повинна бути на першому місці і безпека не є важливою, довгий час життя є найсприятливішим вибором.
– якщо продуктивність системи та безпека є однаково важливими факторами, варто обирати середній час життя токену.

Більш точні значення для різних градацій токенів, зазвичай, обираються індивідуально для кожної інформаційної системи, та мають враховувати велику кількість факторів самої системи.

1. Google for Developers - from AI and Cloud to Mobile and Web. URL: https://developers.google.com/ (дата звернення: 16.04.2024).
2. Meta Developer Documentation | Meta APIs, SDKs Guides. URL: https://developers.facebook.com/docs?locale=en_US (дата звернення: 15.04.2024).
3. Authorize access to REST APIs with OAuth 2.0 - Azure DevOps | Microsoft Learn. URL: https://learn.microsoft.com/en-us/azure/devops/integrate/get-started/authentication/oauth?view=azure-devops (дата звернення: 17.04.2024).

4. Access Tokens - OAuth 2.0 Simplified. URL: https://www.oauth.com/oauth2-servers/access-tokens/ (дата звернення: 17.04.2024).

Кібербезпека колісних транспортних засобів: регламенти ООН

УДК 004.056

Віктор Горицький, Анна Дорошенко

Державне підприємство «Державний автотранспортний науково-дослідний і проектний інститут», gorytski@ukr.net, ad990820@gmail.com

Автомобільна промисловість останні роки стикається з радикальною зміною парадигми в частині інтелектуалізації автомобілів: зі швидкими темпами інтелектуалізації та підключеності колісних транспортних засобів (КТЗ), які підвищують загальну безпеку КТЗ, спостерігається і зростаюча залежність від електроніки, підключеності, насиченості інформаційно-комунікаційними технологіями (ІКТ), що породжує іншу небезпеку – кібернетичну, що породжує проблему кібербезпеки автомобіля.

Ця проблема, як і інші подібні у сфері захисту інформації, вирішується шляхом регламентації, стандартизації, оцінки відповідності (сертифікації), акредитації органів з оцінки відповідності, їх нотифікації (призначення) тощо.

В статті досліджено поточний стан та подальший розвиток зазначеного комплексу міжнародного регулювання в сфері кібербезпеки автомобіля.

Сьогодні у світі формується декілька стандартів та регламентів, які регулюють кібербезпеку автомобіля, що додатково сприяє розгортанню рішень щодо кібербезпеки у всіх, зокрема і підключених автомобілях.

ООН 24 червня 2020 року ухвалила документ WP.29 ЄЕК, який регулює питання кібербезпеки. WP.29 діє у 54 країнах, у тому числі ЄС.

Регламенти ООН юридично забезпечені. Якщо країна або регіон приймає регламент WP.29, то всім виробникам комплектуючих, що діють у ній, потрібен доказ відповідності для проходження обов'язкової сертифікації та подальшого права роботи на ринку. У Європі проходження обов'язкової сертифікації потребує взаємного визнання відповідності нормам на рівні всього автомобіля. Якщо виробник отримує сертифікат на автомобіль певного типу в одній країні ЄС, може продавати таку модель у всіх країнах ЄС без подальших перевірок.

Регламент WP.29 складається з двох основних директив з кібербезпеки автомобілів. Докладніше про них далі.

Перший документ норми ООН щодо кібербезпеки, у рамках документа WP.29 – UN Regulation No. 155. У документі основна увага приділяється кібербезпеці та системам управління кібербезпекою (CSMS).

Визначення WP.29 CSMS: під CSMS розуміється систематичний підхід на основі оцінки ризиків, який визначає організаційні процеси, зони відповідальності та управління для правильного трактування ризиків, пов'язаних з кіберзагрозами транспортних засобів та із захистом транспортних засобів від кібератак.

У документі CSMS добре розглянуті загрози, пов'язані з кібербезпекою, наведено великий перелік уразливостей та методів атаки. Додаток 5 містить 10 сторінок з описом уразливостей, розподілених по безлічі категорій. У першій з