ВИКОРИСТАННЯ СУЧАСНОГО ТРАНСПОРТУ ДАНИХ У ЗАХИЩЕНИХ СЕРВЕРАХ

Калінін І.М., Власов А.В.
Харківський національний університет радіоелектроніки, Харків, Україна

В сучасному світі постійно підвищуються вимоги щодо обробки великих об'ємів інформації, з формуванням нових підходів щодо зберігання, передачі, сортування та обробки інформації. Використання звичних для користувачів способів передачі файлів, зокрема REST API, стає слабким місцем у побудові захисту сучасних інформаційних систем [1]. Це потребує включення додаткових об'ємів інформації від сервера до клієнта, які не є важливими. Використання нових сучасних транспортів даних дозволяє зменшувати об'єми інформації та трафіку в мережі, використання ресурсів для її обробки. Більшість сучасних транспортів мають вбудовані системи фільтрації та пагінації, які дозволяють використовувати схеми віртуального завантаження даних [2]. Це дозволяє користувачам не зберігати зайві дані на своїх пристроях. Побудова запитів до серверів або хмарних систем зберігання даних на стороні клієнта також дозволяє збільшувати швидкість передачі даних, поліпшувати досвід користувачів. Розробник з використанням побудови запитів на стороні клієнту завжди розраховує на збіжний результат, але при цьому необхідно мати передбачувану модель даних що надсилаються.

В сучасних системах для захисту даних використовують токени, миттєві паролі та двох факторна автентифікація [1, 3]. Використання JWT-токенів під час запитів до захищеного серверу дозволяє перевіряти дані користувачів під час кожного запиту. Але використання токенів з обмеженим терміном дії у REST API потребує від користувачів повторного вводу паролів та даних.

Метою доповіді є розгляд переваг та недоліків під час розробки та використання сучасних систем передачі даних, окремих функцій та концепцій захисту інформації. В доповіді наводяться пропозиції щодо впровадження JWT-токенів з обмеженим терміном дії для підвищення захисту інформації. Це дозволить оновлювати токен користувача з кожним запитом до серверу, уникати його копіювання та розповсюдження серед учасників, поліпшувати моделі даних, змінювати підходи до формування аналітики дій користувачів.

Список літератури

1. Алина Грицай. Використання технології Fingerprint для аутентифікації у вебзастосунках//Наука онлайн: Міжнародний електронний науковий журнал - 2018. - №7. [Електронний ресурс] – Режим доступу до ресурсу: https://nauka-online.com/ua/release/2018/7/

2. Markus Winand We need tool support for keyset pagination. [Електронний ресурс] – Режим доступу до ресурсу: https://use-the-index-luke.com/no-offset

3. Безпека JSON Web Tokens (JWT). [Електронний ресурс] – Режим доступу до ресурсу: https://cyberpolygon.com/ru/materials/security-of-json-web-tokens-jwt/