УДК 004.056

І. В. Миронець, *к.т.н., доцент,*
доцент кафедри інформаційної безпеки та комп'ютерної інженерії,
e-mail: irenmir30@gmail.com
В. О. Кобрін, *магістрант,*
e-mail: vitaliy.kobrin@gmail.com
Черкаський державний технологічний університет,
бульв. Шевченка, 460, м. Черкаси, 18006, Україна

АНАЛІЗ МЕТОДІВ РЕАЛІЗАЦІЇ АУТЕНТИФІКАЦІЇ НА ОСНОВІ МАРКЕРІВ ДОСТУПУ ДЛЯ КОРПОРАТИВНОЇ СИСТЕМИ ЗБЕРЕЖЕННЯ ТА ОБМІНУ ДАНИМИ

Стаття присвячена аналізу методів аутентифікації користувача в інформаційній системі, а саме аутентифікації на основі маркерів доступу. В процесі дослідження проаналізовано принцип роботи методу аутентифікації, його ключові особливості, сферу застосування та стандарт, що його описує. Також досліджено переваги даного методу у порівнянні з іншими методами аутентифікації.

В інформаційній системі для ідентифікації користувач надає свої особисті електронні дані для перевірки з метою отримання доступу до певного ресурсу. На етапі аутентифікації особисті електронні дані користувача перевіряються за допомогою певних протоколів. На кінцевому етапі, в результаті успішної перевірки електронних даних користувача на достовірність, користувач отримує права доступу до запитуваного ресурсу. Електронні системи передачі інформації мають і складніші методи аутентифікації та авторизації, такі як багатофакторна аутентифікація або аутентифікація з одноразовими паролями.

Дослідивши переваги та недоліки розглянутого протоколу аутентифікації користувача в інформаційних системах, було визначено основні проблеми, що виникають в процесі розробки додатку на його основі. Запропоновані рішення проблем розширюють функціональні можливості аутентифікації на основі маркерів доступу та підвищують ступінь захисту системи від несанкціонованого доступу.

Ключові слова: *ідентифікація, аутентифікація, маркер доступу, інформаційні системи, конфіденційні дані, захист інформації, несанкціонований доступ.*

Постановка проблеми. В продовж останніх років спостерігається стрімке зростання популярності односторінкових веб-додатків, мобільних програм та веб-сервісів. Як результат, істотно змінюється підхід до створення таких додатків. За допомогою сучасних технологій та фреймворків на розробку веб-додатку витрачається набагато менше часу, а якість та продуктивність додатків зростає. Відповідно, приділяється більше уваги до побудови серверної частини додатку, створення більш потужного та продуктивного API. Зона відповідальності серверної частини додатку обмежується опрацюванням бізнес-логіки та реалізацією рівня доступу до даних, а логіка відображення є винятково відповідальністю веб або мобільного додатку. Ці зміни призвели до нових шляхів впровадження аутентифікації в сучасних додатках.

Аутентифікація – це одна з найважливіших частин будь-якого веб-додатку. Досить тривалий час найпростішим та найпопулярнішим вирішенням проблеми аутентифікації були файли cookie та аутентифікація на базі серверів. Проте, обробка аутентифікації в сучасних додатках для мобільних пристроїв та односторінкових додатків може бути складнішою та вимагати іншого підходу. Одне з найбільш відомих рішень для реалізації аутентифікації для веб-сервісів – аутентифікація на основі маркерів доступу.

Для корпоративної системи збереження та обміну даними захист від несанкціонованого доступу є винятково важливим атрибутом, що, наряду з іншими найбільш важливими компонентами системи (оптимізовані алгоритми обробки великих об'ємів даних, файлова система, реалізація розмежування прав доступу до ресурсів та ін.), забезпечує надання інформаційною системою високоякісних послуг.

Будь-яка система збереження даних, крім документів користувачів, може також

зберігати базу даних особистої інформації користувачів: фізичні адреси, телефонні номери, адреси електронної пошти, приватні повідомлення. Зловмисники є зацікавленими у заволодінні такими інформаційними ресурсами.

Корпоративна система збереження даних може використовуватися для збереження інтелектуальної власності, результатів діяльності компанії, електронних версій юридичних документів тощо. Цінність таких даних істотно перевищує цінність звичайних документів, відповідно збільшуються і вимоги до системи захисту.

Аналіз останніх досліджень та публікацій. Аналіз науково-технічної літератури [1-10] доводить актуальність досліджень методів і протоколів аутентифікації та зростання зацікавленості відомих корпорацій у пошуку новітніх рішень для реалізації аутентифікації. У публікаціях останніх років описано постійно зростаючу інтенсивність удосконалення засобів злому інформаційних систем з метою заволодіння інформаційними ресурсами. У зв'язку з цим удосконалюються і методи захисту інформації від несанкціонованого доступу. В процесі функціонування інформаційної системи здійснюється постійна обробка даних, їх передача в мережі та зберігання. Захист інформації повинен забезпечувати надійність виконання всіх операцій з даними.

Науковцем Дасгупта Д. розглянуто процес перевірки автентичності, а також типи механізмів аутентифікації та їх особливостей. В його книзі [2] розглянуто використання цих механізмів в експлуатаційному середовищі, що змінюється у часі, включаючи такі сторонні фактори, як пристрої, засоби масової інформації та навколишнє середовище.

Малюком А.А. [9] розглянуто проблеми вразливості інформації в системах обробки даних, описано принципи роботи протоколів аутентифікації, а також їх взаємодія з веб-серверами та веб-додатками.

Чапмен Н. [1] надав опис способів вирішення проблеми видачі інформаційною системою дозволу на виконання операції над даними на вимогу від певного користувача або програми.

За результатами проведеного аналізу публікацій було визначено основні існуючі протоколи та засоби аутентифікації.

Мета даної роботи полягає у дослідженні методів реалізації аутентифікації на основі маркерів доступу для корпоративної системи збереження та обміну даними, їх доцільності використання, а також переваг та недоліків.

Виклад основного матеріалу. Існує два основні типи аутентифікації користувача в інформаційній системі:

- аутентифікація на основі файлів cookie;
- аутентифікація на основі маркерів доступу.

Аутентифікація на основі файлів cookie на даний час є застарілою у зв'язку з недосконалістю реалізації механізму аутентифікації користувача. Такий тип аутентифікації передбачає, що сесія користувача повинна зберігатися як на сервері, так і на стороні клієнта. Сервер повинен відстежувати активні сесії в базі даних, тоді як на стороні клієнта створюється файл cookie, який містить ідентифікатор сеансу, тобто аутентифікацію на основі файлу cookie.

Аутентифікація на основі маркерів доступу навпаки не передбачає збереження сесії користувача. Немає необхідності реалізовувати на сервері механізм обліку користувачів, що авторизуються у системі. В такому випадку кожен запит на сервер супроводжується маркером доступу, який сервер використовує для перевірки автентичності запиту.

Маркер (токен) доступу – це фрагмент даних, що містить облікові дані для сеансу входу та ідентифікує користувача, групи користувачів, привілеї користувача та, у деяких випадках, певну програму. Маркер доступу може використовуватись клієнтською частиною додатку для доступу до прикладного програмного інтерфейсу (Application programming interface (англ.) або API) сервера. Мета маркера доступу полягає в інформуванні API про те, що носій цього маркера отримав дозвіл на доступ до API та виконання певних дій (в межах наданого доступу).

Функція аутентифікації на основі маркерів доступу забезпечує, що кожен запит на сервер супроводжується підписаним маркером, який сервер перевіряє на достовірність, а потім відповідає на запит в залежності від результатів перевірки.

Маркер доступу створюється на етапі аутентифікації користувача у системі у разі її успішного завершення.

Розглянемо процес створення та використання маркера доступу (рис. 1):

• користувач вводить свої реєстраційні дані;

• сервер перевіряє правильність облікових даних і повертає підписаний маркер;

• отриманий від сервера маркер зберігається на стороні клієнта, найчастіше в локальному сховищі браузера, але також може зберігатися в пам'яті або файлі cookie;

• наступні запити на сервер містять цей маркер як додатковий заголовок (Authorization) запиту, також додатково може бути відправлений в тілі запиту POST або як параметр запиту;

• сервер здійснює валідацію маркера і в разі, якщо він дійсний, здійснює обробку запиту, інакше – повертає відповідь з помилкою;

• коли користувач виходить з системи, маркер знищується на стороні клієнта, взаємодія з сервером не потрібна.

Аутентифікація на основі маркерів доступу має наступні переваги:

- відсутність механізму керування сесіями;
- кросдоменність;
- збереження даних в маркері;
- біль висока продуктивність;
- адаптація для використання у мобільних додатках;
- стандартизованість.

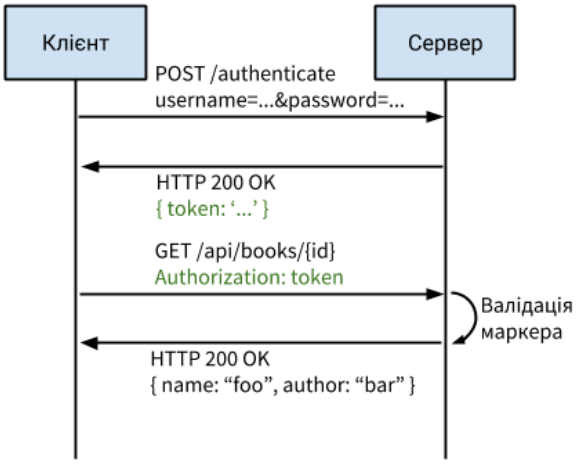

Рис. 1. Послідовність отримання та використання маркера доступу

Розглянемо ці пункти детальніше.

Перевагою використання маркерів у порівнянні з файлами cookie є те, що при використанні маркерів немає необхідності у збереженні сесії користувача на стороні сервера. Кожен маркер є самостійною одиницею, що містить всі дані, необхідні для перевірки його дійсності, а також передачі інформації про користувача.

В такому випадку робота сервера полягає у підписуванні маркерів у випадку успішного виконання запиту на авторизацію користувача і перевірці правильності вхідних маркерів. Використовуючи сторонні сервіси для підпису маркерів, задачею сервера є лише підтвердження валідності маркера.

Аутентифікація на основі cookies працює коректно з сингулярними доменами та субдоменами. У випадках необхідності керування файлами cookie в різних доменах, процес реалізації аутентифікації стає набагато складнішим. Аутентифікація на основі маркерів доступу не вимагає додаткових налаштувань, оскільки маркер доступу перевіряється з кожним запитом на стороні сервера.

Використовуючи підхід, заснований на файлі cookie, передбачає збереження ідентифікатора сесії користувача у цьому файлі. Підхід на основі маркерів доступу дозволяє зберігати будь-який тип метаданих безпосередньо у маркері, якщо дані можуть бути представлені у форматі JSON.

Під час використання аутентифікації на основі файлів cookie є необхідність у виконанні пошукових запитів до бази даних для вилучення даних про сесію користувача. В залежності від типу СУБД, що використовується, такі запити можуть бути більш тривалими, ніж процес декодування маркера.

Наприклад, якщо є ресурс, що доступний за запитом на адресу /api/books, але доступ для перегляду даних за цією адресою мають лише користувачі з роллю «адміністратор». При використанні файлів cookie, під час виконання запиту буде здійснено принаймні три запити до бази даних:

1. перевірка, що сесія є дійсна;
2. пошук даних користувача та перевірка, що користувач має роль адміністратора;
3. пошук запитуваних даних.

За допомогою підходу на основі маркерів доступу роль користувача може бути збережена всередині маркера. Тому після валідації маркера і підтвердження, що користувач має роль адміністратора, буде виконано один запит до бази даних з метою отримання запитуваних даних.

В ролі клієнта по відношенню до сервера може виступати як браузер так і мобільний додаток. Мобільні платформи не мають підтримки файлів cookie. Також існує ряд обмежень щодо використання файлів cookie на мобільних платформах пов’язані з вразливістю системи захисту даних користувача. Для реалізації аутентифікації на основі маркерів доступу не потрібно мати підтримки на рівні платформи. Даний підхід повністю придатний для реалізації на платформах iOS та Android.

Існує стандарт JSON Web Token (RFC 7519), що описує структуру маркера доступу, способи його використання, процедури кодування та підпису тощо. Існує підтримка стандарту для більшості популярних платформ програмування (.NET, Ruby, Java, Python, PHP, NodeJS та ін.). Стандарт використовується багатьма сервісами наряду із стандартами OAuth та OAuth 2.0.

Стандарт JSON Web Token (JWT) визначає компактний та автономний спосіб безпечного передавання інформації між сторонами як об'єкт у форматі JSON. Цю інформацію можна перевірити на достовірність, оскільки вона підписана цифровим способом. JWT можна підписати, використовуючи секрет (з алгоритмом HMAC) або пару публічний/приватний ключ з асинхронними алгоритмами шифрування.

JWT передбачає компактність маркера, оскільки він надсилається через HTTP-запити. Крім того, менший розмір означає більшу швидкість передачі.

Автономність означає, що маркер містить у собі всю необхідну інформацію про користувача.

JWT складаються з трьох частин, розділених крапками:

- заголовок (header),
- вміст (payload),
- підпис (signature).

Заголовок, як правило, складається з двох атрибутів: «typ» (тип маркера, в даному випадку JWT), та «alg» (алгоритм хешування, що використовується, наприклад HMAC SHA256 або RSA).

Друга частина маркера містить набір тверджень (claims). Твердження – це інформація про суб'єкт (як правило, користувача) та додаткові метадані. Всього використовується три типи тверджень:

- Зареєстровані твердження – це набір попередньо визначених тверджень, які не є обов'язковими, але рекомендовані для включення їх до набору тверджень (див. табл. 1).
- Публічні твердження – твердження, які можна визначити за бажанням тих, хто використовує JWT. Щоб уникнути колізій, вони повинні бути визначені в реєстрі IANA JSON Web Token або бути визначеними як URI, що містить конфліктну зону імен.
- Приватні твердження – це спеціальні вимоги, створені для обміну інформацією між сторонами, які погоджуються на їх використання.

Звернімо увагу, що назви тверджень, як правило, складаються лише з трьох символів, оскільки одна із вимог до побудови JWT – забезпечення його компактності.

Таблиця 1

Зареєстровані твердження вмісту JWT

Поле	*Назва*	*Значення*
iss	Issuer	Ідентифікатор сервісу, що видав маркер
sub	Subject	Ідентифікатор суб'єкта, якого стосуються твердження.
exp	Expiration Time	Час закінчення терміну дії маркера в форматі Unix.
iat	Issued At	Час, коли маркер був виданий (в форматі Unix)

Заголовок та вміст маркера кодуються у форматі Base64Url, що дозволяє перетворити набір даних в компактну послідовність символів і утворити маркер.

Підпис є результатом криптографічного перетворення перших двох частини маркера (заголовку та вмісту у форматі Base64Url та розділених крапкою). Шифрування відбувається за алгоритмом, вказаним у заголовку. Отримана в результаті перетворення послідовність символів (хеш) додається до перших двох частин та відокремлюється крапкою.

Наприклад, підписаний алгоритмом HMAC SHA256 маркер, може мати наступний вигляд: eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RMHrHDcEfxjoYZgeFONFh7Hg.

Підпис призначений для ідентифікації джерела маркера та підтвердження цілісності даних, які він містить.

Під час валідації маркера здійснюється операція, подібна до операції підпису маркера: створюється хеш на основі перших двох частин маркера та порівнюється із третьою частиною маркера. Якщо обидва хеши співпадають, маркер вважається валідним. В протилежному випадку система генерує помилку і подальша обробка маркера припиняється.

Одним із найпопулярніших способів отримання хешу для JWT є використання механізму HMAC (Hash-based message authentication code (англ.) або хеш-код аутентифікації повідомлень).

HMAC – це група алгоритмів, які забезпечують спосіб підписування повідомлень за допомогою спільного ключа. У випадку HMAC використовується криптографічна хеш-функція (наприклад, SHA256). Потужність залежить від алгоритму хешування, що використовується.

Основним завданням при проектуванні алгоритму було досягти можливість комбінувати ключ з повідомленням, одночасно надаючи гарантії проти несанкціонованого втручання і модифікації повідомлення. Спеціальні рішення (наприклад, додавання ключа до повідомлення, а потім хешування результату) мають математичні недоліки, які дозволяють потенційним зловмисникам підробляти підпис. Алгоритм HMAC розроблений з урахуванням цих недоліків.

HMAC використовується з JWT, коли є необхідним простий спосіб для створення та валідації JWT в різних компонентах інформаційної системи. Будь-який компонент системи, якому відомий ключ, може створювати нові JWT. Іншими словами, перехопивши ключ, зловмисник може видати себе за іншого: JWT на основі HMAC не надає гарантій щодо сторони, на якій було створено JWT. Для запобігання цього доцільніше використовувати асиметричні алгоритми для побудови хешу, а саме RSA.

RSA – асиметричний алгоритм шифрування та цифрового підпису. Даний алгоритм надає можливість перевірки або дешифрування повідомлення без можливості створення нового. Сторона, яка видає маркер, використовує приватний ключ для підписання JWT. Сторона, що отримує маркер, використовує відкритий ключ, що поширюється відкритим джерелом. Приймаючі сторони не можуть створювати нові JWT за допомогою відкритого ключа відправника.

Алгоритм RSA є більш складним у реалізації, ніж HMAC. Але використання цього алгоритму істотно зменшує шанс підробки маркера доступу.

Наступним важливим кроком у валідації маркера доступу після ідентифікації автора маркера та підтвердження його цілісності – це перевірка терміну його дії.

Як зазначалось раніше, одним із рекомендованих тверджень вмісту маркера є exp (Expiration Time), що містить дату та час завершення дії маркера. За реалізації аутентифікації на основі маркерів доступу відсутній механізм контролю сесій користувачів. В даному випадку доцільним є перевірка терміну дії маркера.

Термін дії маркера – термін закінчення дії умовної сесії користувача, тобто час, протягом якого користувач може взаємодіяти із системою без необхідності виконання повторної процедури авторизації у системі.

Існують рекомендації щодо терміну підтримки сесій користувачів активними (від 10 годин до 1 доби), недотримання яких може призвести до поганого впливу на досвід користування системою.

Оскільки механізм контролю сесій користувачів відсутній, є неможливим відстеження та анулювання маркерів, що були видані. Якщо став відомий факт перехоплення маркера доступу користувача та його несанкціонованого використання, система не в змозі виявити даний маркер та заборонити доступ до системи стороні, що його використовує, навіть якщо користувач здійснить вихід із системи. Збереження у базі даних будь-яких міток або реєстру маркерів суперечить принципам реалізації аутентифікації на основі маркерів доступу та нівелює існуючі переваги такого підходу.

Вирішенням даної проблеми є використання маркера оновлення (refresh token). Даний підхід вимагає впровадження додаткових кроків в процеси авторизації та аутентифікації користувачів, але дозволяє підвищити контроль над використанням існуючих маркерів.

Використання маркерів оновлення дозволяє генерувати маркери доступу з короткотривалим терміном дії (до 1 год.). Маркер оновлення – JWT, з терміном дії, що еквівале-

нтний терміну дії сесії користувача в системі та з відображенням у базі даних.

Розглянемо процес аутентифікації з використанням маркера оновлення (рис. 2):

- користувач вводить свої реєстраційні дані;
- сервер перевіряє правильність облікових даних і повертає підписані маркери доступу та оновлення;
- отримані від сервера маркери зберігаються на стороні клієнта;
- наступні запити на сервер містять маркер доступу;
- сервер здійснює валідацію маркера доступу і в разі, якщо він дійсний, здійснює обробку запиту, інакше – повертає відповідь з помилкою;
- якщо отримано помилку від сервера, надсилається запит на оновлення маркера доступу, відповідно запит містить маркер оновлення;
- сервер здійснює валідацію маркера оновлення і в разі, якщо він дійсний, повертає новий маркер доступу;
- коли користувач виходить з системи, маркери знищується на стороні клієнта, сервер повідомляється про завершення сесії.

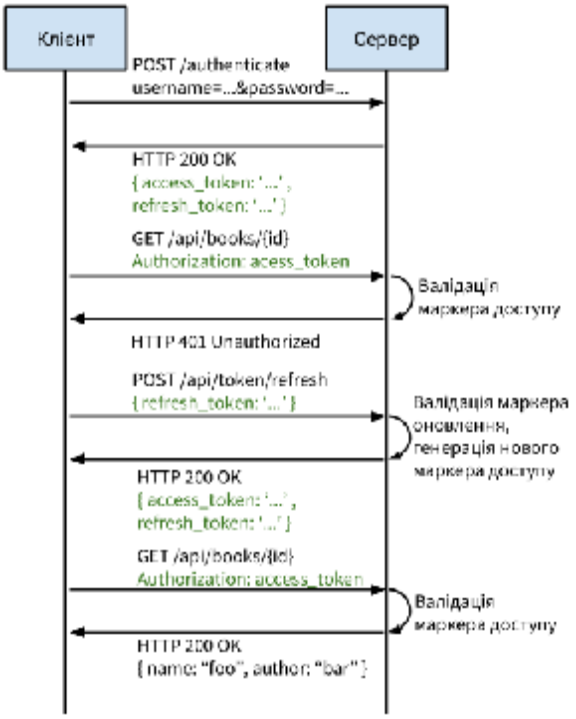

Рис. 2. Процес аутентифікації користувача з використанням маркера оновлення

Якщо маркер оновлення є невалідним або термін його дії закінчився, новий маркер доступу не буде виданий.

Як видно, даний процес аутентифікації передбачає виконання додаткових запитів до бази даних, але лише у разі запиту на оновлення маркера.

Якщо користувач здійснив вихід із системи або його сесія була автоматично завершена у випадку виявлення факту несанкціонованого використання маркера доступу, сесія фактично буде активною до завершення терміну дії маркера доступу. Новий маркер доступу не буде виданий навіть у випадку перехоплення маркера оновлення.

Даний підхід не гарантує абсолютного захисту від несанкціонованого доступу, але є значно надійнішим у порівнянні з підходом без використання маркера оновлення.

Також даний підхід дозволяє вирішити іншу проблему, пов'язану з неможливістю анулювати маркер доступу. Якщо в системі передбачено механізм управління правами доступу користувачів до певних даних, може виникнути ситуація, коли адміністратором інформаційної системи буде вирішено заблокувати або частково обмежити конкретному користувачеві доступ до певного ресурсу. З використанням лише маркера доступу, даний користувач буде мати доступ до забороненого для нього ресурсу протягом терміну дії сесії. Проте, під час валідації маркера оновлення можливо здійснити додаткову перевірку на можливі зміни у права доступу користувача та запобігти його доступ до захищеного ресурсу.

Як вже зазначалось, заголовок JWT містить параметр, що вказує алгоритм, що використовувався для підпису маркера. Крім назви алгоритму, даний параметр може містити нульове значення (none). Нульове значення використовується в ситуаціях, коли цілісність маркера вже підтверджена.

В разі використання сторонніх реалізацій механізмів валідації JWT необхідно передбачити додатковий ступінь перевірки маркера на назву алгоритму, що міститься в заголовку маркера. Така процедура є необхідною, оскільки в сторонніх реалізаціях може бути відсутнім механізм валідації для маркерів, які містять в заголовку нульовий алгоритм. Це надає зловмисникам можливість підміни маркера доступу на будь-який інший та отримати несанкціонований доступ до захищених ресурсів.

Також однією із проблем використання JWT є Формат Base64, що передбачає лише кодування вмісту маркера. Дані, що містяться в маркері, не є захищеними та можуть бути розкодованими третіми особами. В інформаційних системах, вимогою до яких є передача в маркері інформації, недоступної для третіх осіб, використання JWT не є прийнятним рішенням. Замість цього можна використовувати модифікацію JWT – JWE (JSON Web Encryption). JWE, на відміну від JWT, містить зашифровані дані. JWE має структуру, відмінну від структури JWT, і має більш складні процеси генерації та валідації.

Використання JWE замість JWT потребує додаткового аналізу для виявлення відповідно переваг та недоліків аутентифікації на основі JWE.

Висновки. В процесі даного дослідження було розглянуто основні методи реалізації аутентифікації, виявлено переваги та недоліки аутентифікації на основі маркерів доступу. Здійснено покроковий аналіз можливих алгоритмів роботи системи аутентифікації.

Проведено дослідження особливостей використання маркерів доступу, проблеми, пов'язані з їх використанням, та способи їх вирішення. Розглянуто один із стандартів побудови маркерів доступу, внутрішню структуру маркерів, особливості передачі даних в середині маркерів. Також проаналізовано способи шифрування вмісту маркерів та створення цифрового підпису, що дозволяє ідентифікувати джерело маркера та підтвердження цілісності даних, які він містить.

Список літератури

1. Chapman N., Chapman J. Authentication and Authorization on the Web. MacAvon Media. 2012. 236 с.
2. Dasgupta D., Arunava R., Nag A. Advances in User Authentication. Springer International Publishing AG. 2017. 233 с.
3. Topol B. Nash H., Martinelli S. Identity, Authentication, and Access Management in OpenStack. O'Reilly Media, Inc. 2015. 130 с.
4. Афанасьев А. А, Веденьев Л. Т., Воронцов А. А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. 2-е изд. Москва: Горячая линия-Телеком, 2012. 570 с.
5. Барабанов А.В., Дорофеев А. В., Марков А. С., Цирлов В. Л. Семь безопасных информационных технологий. Москва: ДМК Пресс, 2017. 224 с.
6. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. Учеб. пособ. 3-е изд., перераб. и доп. Москва: Инфра-М, 2017. 324 с.
7. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. 3-е изд. Москва: Горячая линия-Телеком, 2017. 176 с.
8. Горбатов В. Г., Полянская О. Ю. Основы технологии PKI. Москва: Горячая линия-Телеком, 2004. 248 с.
9. Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах. Москва: Горячая линия-Телеком, 2001. 148 с.
10. Малюк А. А., Горбатов В. С., Королев В. И. Введение в информационную безопасность. Москва: Горячая линия-Телеком, 2011. 288 с.

References

1. Chapman, N. Chapman, J. (2012) Authentication and Authorization on the Web. MacAvon Media, 236 p.
2. Dasgupta, D., Arunava, R., Nag, A. (2017) Advances in User Authentication. Springer International Publishing AG, 233 p.
3. Topol, B., Nash, H., Martinelli, S. (2015) Identity, Authentication, and Access Management in OpenStack. O'Reilly Media, 130 p.
4. Afanas'ev, A. A., Veden'ev, L. T., Voroncov, A. A. (2012) Authentication. The theory and practice of research of secure access to the information resources. Moscow: Goryachaya liniya-Telekom [in Russian].
5. Barabanov, A. V., Dorofeev, A. V., Markov, A. S., Cirlov, V. L (2017) Seven secured information technologies. Moscow: DMK Press [in Russian].
6. Baranova, E. K., Babash, A. V. (2017) Information security and protection. Moscow: Infa-M [in Russian].
7. Barichev, S. G., Goncharov, V. V., Serov, R. E. (2017) Basics of modern cryptography. Moscow: Goryachaya liniya-Telekom [in Russian].

8. Gorbatov, V. G., Polyanskaya, O. YU. (2004) Basics of PKI technology. Moscow: Goryachaya liniya-Telekom [in Russian].
9. Malyuk, A. A., Pazizin, S. V., Pogozhin, N. S. (2001) Introduction into information protection in automated systems. Moscow: Goryachaya liniya-Telekom [in Russian].
10. Malyuk, A. A., Gorbatov, V. S., Korolev, V. I. (2011) Introduction into information security. Moscow: Goryachaya liniya-Telekom [in Russian].

I. V. Myronets, *Ph.D., associate professor,*
associate professor of information security and computer engineering chair,
e-mail: irenmir30@gmail.com,
V. O. Kobrin, *master,*
e-mail: vitaliy.kobrin@gmail.com,
Cherkasy State Technological University,
Shevchenko blvd., 460, Cherkasy, 18006, Ukraine

ANALYSIS OF METHODS FOR AUTHENTICATION IMPLEMENTATION BASED ON TOKENS OF ACCESS FOR CORPORATE SYSTEM OF DATA STORAGE AND SHARING

In recent years, the population of single page applications, mobile applications and web services is growing rapidly. As a result, the approaches to developing such applications are changing significantly. Usage of new approaches brings new implementation methods of authentication in modern applications. The objectives of this research are implementation methods of token based authentication for corporate system of data storage and sharing, investigation of such method usage expediency, research for existing solutions and analyzing their advantages and disadvantages. A protection from unauthorized access is the most important attribute for corporate system of data storing and sharing. This is the one of the most important components which guarantees providing high quality service. The intensity of improvements of ways to hack information systems are growing significantly. So, the information security system should provide reliable performing of data processing, transferring and storing. The results of the research on the use of the token based authentication system are presented in this article. This type of authentication was compared with cookie based authentication. The main advantages and disadvantages of this approach were described.

Access token is a fragment of a data contained user claims. Token allows server to identify the user, group of the users and/or application. Token is used by client side application as a key to the API. The main goal of the access token is to inform that the bearer of this token has access to the API. Function of a token based authentication is to provide every request to the server with signed access token. This token is checked by server on authenticity. After that the server responds to request depending on the results of the checking. There is a JSON Web Token (JWT) standard that describes access token structure, ways of it usage and caching procedures.

This article contains the detailed description of the JWT usage scenarios. There is a description of the authentication process based on refresh token usage that brings more control over user sessions. The ways to sign the token described as well.

The result of this research is defined implementation methods of authentication. Advantages and disadvantages of token based authentication were defined. Step-by-step analysis of possible working algorithms of authentication system was performed.

Keywords: *identification, authentication, access token, information system, confidential data, information security, unauthorized access.*

Рецензенти: С. В. Голуб, д.т.н., професор,
Т. О. Прокопенко, д.т.н., доцент.