Поліщук С. М., магістрант
Державний університет «Житомирська політехніка»

PASSKEYS – СУЧАСНА ТЕХНОЛОГІЯ АУТЕНТИФІКАЦІЇ БЕЗ ПАРОЛЯ

Passkeys – це нова сучасна технологія аутентифікації без пароля, яка використовує криптографічний ключ замість пароля, а саме криптографію з відкритим ключем, що дозволяє користувачам входити на веб-сайти, у веб або мобільні додатки чи різноманітні хмарні сервіси без необхідності вводити пароль. Натомість користувачі проходять аутентифікацію так само, коли розблоковують свої ноутбуки, телефони чи планшети: за допомогою відбитка пальця, обличчя або інших біометричних даних; за допомогою точкового шаблону; або введення PIN-коду. Для доступу до закритого криптографічного ключа зазвичай обирають біометричну аутентифікацію.

Замість створення звичайного пароля для входу в обліковий запис, користувачі можуть використовувати «аутентифікатор» для генерації ключа доступу, який насправді представляє собою пару закритого та відкритого ключів. Цей аутентифікатор може бути різними засобами, такими як пристрій (наприклад, ноутбук, смартфон чи планшет з відповідним додатком), спеціальна флешка, що генерує ключі доступу, або менеджер паролів, який підтримує технологію Passkeys з використанням стандарту безпарольної авторизації WebAuthn.

Перед створенням ключа доступу аутентифікатор вимагатиме, щоб користувач ідентифікував себе за допомогою PIN-коду, точкового шаблону або біометрії. Потім аутентифікатор відправляє відкритий ключ на сервер для зберігання, а сам аутентифікатор безпечно зберігає закритий ключ локально в зашифрованому сховищі.

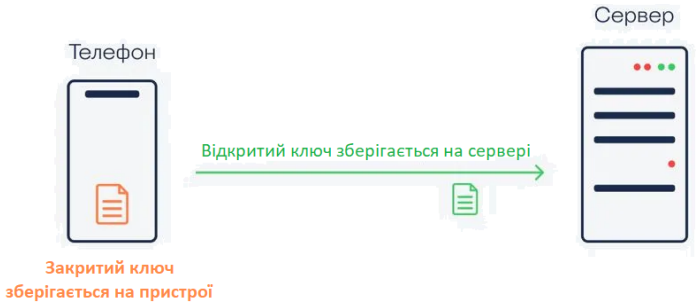

Рис. 1. Створення нового ключа доступу

Принцип роботи Passkeys ґрунтується на застосуванні асиметричного шифрування. Під час створення passkey генеруються два довгих електронних ключі: відкритий, який зберігається на сервері, і закритий, який лишається лише на пристрої користувача і не передається нікуди.

Коли сервер використовує passkey, він висилає на пристрій конкретне повідомлення і запитує про його підпис закритим ключем. Зашифроване повідомлення повертається на сервер, де воно розшифровується його власним відкритим ключем. Якщо розшифрування пройшло успішно, це свідчить про успішну аутентифікацію.

Рис. 2. Приклад проведення аутентифікації
за допомогою технології Passkeys

Використання ключів доступу для аутентифікації за технологією Passkeys безпечніше, ніж використання паролів, з багатьох причин:

1. Якщо сервер облікових записів буде зламаний, зловмисники матимуть доступ лише до відкритих ключів, які не приносять користі без відповідних закритих ключів.
2. Більшість людей використовують надто короткі паролі або паролі, що містять словникові слова чи біографічну інформацію, тому їх легко вгадати. Passkeys завжди дуже складні та унікальні для кожного користувача.
3. Багато людей не захищають свої облікові записи за допомогою двофакторної аутентифікації (2FA), а паролі зберігають на стікерах або у незашифрованих текстових файлах. Passkeys покладаються на 2FA за задумом.
4. Часто однакові паролі використовуються на кількох сайтах. Однак з технологією Passkeys не потрібно пам’ятати всі паролі, достатньо пам’ятати один простий або використовувати біометрію.

5. Ключ доступу не можна зламати, підібравши або перехопивши. Для підтвердження особи потрібно мати фізичний доступ до пристрою. Це робить ключі доступу надійніше двофакторної аутентифікації.

6. На відміну від паролів, ключ доступу не можна вкрасти за допомогою технологій фішингу, тобто через сайти-підробки.

7. Ключі доступу можна використовувати у різних браузерах та операційних системах. Головне, щоб під рукою був пристрій, який може підтвердити особу користувача.

8. Аутентифікація за технологію Passkeys приблизно на 40% швидше, ніж за паролем.

Список використаних джерел

1. Christiaan Brand, Sriram Karra. The beginning of the end of the password. 03 May 2023. URL: https://blog.google/technology/safety-security/the-beginning-of-the-end-of-the-password .

2. Passkeys.dev. URL: https://passkeys.dev/docs/intro/what-are-passkeys/