УДК 004

УДОСКОНАЛЕННЯ СИСТЕМИ АВТОРИЗАЦІЇ ЗА ДОПОМОГОЮ PASSKEY АУТЕНТІФІКАЦІЇ В ВЕБ ЗАСТОСУНКАХ

Плехова А.А. Окушко О.М..

Харківський національний автомобільно-дорожній університет, Харків

Постановка проблеми : У сучасному цифровому віці, коли веб-застосунки визначають не лише наші щоденні розваги, але й взаємодію з ключовими аспектами нашого життя, починаючи від електронної комерції та закінчуючи взаємодією з банківськими сервісами та зберіганням особистих даних, необхідність надійної системи авторизації виходить на перший план. Це стає ключовим аспектом для забезпечення не лише безпеки в інтернет-просторі, але й конфіденційності особистої інформації та зручності використання веб-ресурсів. Завдяки поширенню різноманітних веб-сервісів і онлайн-платформ, стає очевидним, що існують виклики, які необхідно вирішувати для подальшого вдосконалення систем авторизації в цьому динамічному середовищі.

Однією з основних проблем є забезпечення високого рівня безпеки систем авторизації. Суттєвий ріст кількості кіберзагроз і атак змушує зосередитися на розробці та впровадженні надійних методів ідентифікації та аутентифікації користувачів, а саме passkeys аутентифікації.

Окрім того, зручність та користувацький досвід беруть на себе не менш важливу роль у розвитку сучасних систем авторизації. Процес входу в систему повинен бути не лише безпечним, але й інтуїтивно зрозумілим для кінцевого користувача, максимально уникати зайвих труднощів та покращити загальний враження від використання веб-ресурсів.

Мета дослідження: Удосконалення системи авторизації за допомогою фізичного ключа в веб-застосунках.

Основний матеріал: Passkeys представляють собою більш безпечну та просту альтернативу звичайним паролям. Використовуючи паролі, користувачі можуть увійти

в додатки та веб-сайти, використовуючи біометричні дані (наприклад, відбиток пальця або розпізнавання обличчя), PIN-код або графічний ключ, при цьому звільняючись від необхідності запам'ятовувати паролі та управляти ними.[1]

Паролі є джерелом неприязності як для розробників, так і для користувачів: вони погіршують користувацький досвід, додають тертя при конвертації [2] та створюють відповідальність за безпеку.

Ключ доступу відрізняється від пароля. Пароль - це рядок символів, який вводиться для входу на вебсайт або в застосунок. Існують вимоги до паролів які рекомендують NIST, такі як мінімум вісім символів, використання різних символів, обмеження на повторення символів, використання контексту та уникання часто використовуваних слів.[3]

Passkey - це технологія автентифікації, яка дозволяє користувачам входити на вебсайти і додатки без пароля. Це можна зробити за допомогою біометрії (відбитка пальця, обличчя), точкового шаблону або PIN-коду. Замість створення пароля, користувачі генерують ключ доступу, що складається з відкритого і закритого ключа. Аутентифікатор (наприклад, смартфон або менеджер паролів) вимагає ідентифікацію користувача, потім відправляє відкритий ключ на сервер зберігання, а закритий ключ зберігається локально. Закритий ключ може бути збережений у зв'язці ключів пристрою або в зашифрованому сховищі менеджера паролів.

Google Password Manager в Android і Chrome спрощує процес завдяки автоматичному заповненню. Для розробників, які прагнуть подальшого поліпшення конверсії та безпеки, ключі та федерація ідентичностей є сучасними стратегіями в даній галузі [4].

Passkey може відповідати вимогам багатофакторної автентифікації в один етап, замінюючи як пароль, так і одноразовий код (наприклад, 6-значний SMS-код). Це забезпечує надійний захист від фішингових атак і уникнення проблем, пов'язаних з користувацьким інтерфейсом, які виникають при використанні одноразових паролів на основі SMS або додатків. Оскільки реалізація ключів-паролів стандартизована [5], вони гарантують безпарольний доступ на всіх пристроях користувачів, у різних браузерах та операційних системах.

Рисунок 2 - Авторизація за допомогою passkeys

Passkeys мають вищий рівень безпеки. Розробники зберігають лише публічний ключ на сервері, замість пароля. Це означає, що для зламання серверів зловмисникам стає набагато складніше, і навіть у випадку порушення безпеки, зусилля для відновлення значно зменшуються.

Passkeys ефективно захищають від фішингових атак. Оскільки паролі працюють лише на зареєстрованих веб-сайтах і додатках, користувач не може бути обманутим для автентифікації на підробленому сайті. Важливо відзначити, що перевірку проводить сам браузер або операційна система.

Порівняно з паролями, Passkeys зменшують витрати на відправлення SMS, що робить їх безпечнішим та економічно вигіднішим засобом двофакторної автентифікації.

Passkeys є більш простими у використанні. Користувачам не потрібно вводити ім'я користувача, оскільки вони можуть просто обрати обліковий запис для входу.

Автентифікація користувачів може відбуватися шляхом блокування екрану пристрою, такого як застосування відбитка пальця, розпізнавання обличчя або введення PIN-коду.

Після створення та реєстрації пароля користувач може легко переходити на новий пристрій і відразу ж починати його використання без необхідності повторної реєстрації, відмінності від традиційного підходу до біометричної автентифікації, яка вимагає налаштувань на кожному новому пристрої.

Анатомія системи доступу складається з кількох компонентів. Початкова сторона, що перевіряє (RP), відповідає за видачу ключа доступу та автентифікацію. Ця сторона управляє клієнтом (веб-сайтом або додатком), який створює або перевіряє ключі

доступу, а також сервером, який зберігає та перевіряє облікові дані. Мобільний застосунок, що використовує ключ доступу, повинен бути прив'язаний до домену RP-сервера за допомогою механізму асоціації, наприклад, Digital Asset Links. Аутентифікатор, такий як мобільний телефон або комп'ютер, здатен створювати та перевіряти ключі доступу за допомогою функції блокування екрана.

Менеджер паролів, такий як Google Менеджер паролів, є програмним забезпеченням, яке обслуговує, зберігає і синхронізує ключі доступу на пристроях кінцевого користувача.

Процес реєстрації передбачає використання API WebAuthn на веб-сайті або бібліотеки Credential Manager у застосунку Android. Щоб створити новий ключ доступу, потрібно вказати ідентифікатор сторони, що перевіряє, відомості про користувача та облікові дані, що виключаються. Крім того, необхідно визначити тип ключа доступу: автентифікатор платформи або кросплатформний/роумінговий автентифікатор. Зареєстрований ключ доступу повертається на сервер для майбутньої автентифікації.

Аутентифікація за допомогою ключа доступу складається з кількох компонентів: вимагає вказання ідентифікатора сторони, що перевіряє, а також завдання, що запобігають атакам повторного відтворення. Після підтвердження користувачем за допомогою розблокування екрана, облікові дані відкритого ключа відправляються на сервер для перевірки підпису за допомогою збереженого відкритого ключа.

Загалом, система доступу включає RP-сторону, аутентифікатор та менеджер паролів. Процес реєстрації та аутентифікації вимагає вказання ключових компонентів та перевірки облікових даних. Ця система допомагає гарантувати безпеку при доступі до веб-сайтів та додатків.[6]

Висновок; У висновку слід відзначити, що Passkeys, як безпечна та зручна альтернатива звичайним паролям, вносять значні покращення в сферу автентифікації. Використання біометричних даних, PIN-кодів та графічних ключів робить процес входу не лише безпечнішим, але й зручнішим для користувачів. Пасивне зберігання лише публічного ключа на сервері робить систему стійкішою до зламу, а ефективний

захист від фішингових атак та зменшення витрат на SMS-повідомлення роблять Passkeys важливим інструментом для безпечної двофакторної автентифікації.

Зокрема, в подальших дослідженнях та розвитку систем авторизації важливо звертати увагу на переваги Passkeys у порівнянні з традиційними паролями, підкреслюючи їхню зручність для користувачів та високий рівень безпеки. Розробники мають можливість вдосконалювати та впроваджувати Passkeys, щоб покращити конверсію та забезпечити найвищий рівень безпеки в цифровому просторі.

Література:

1. Carly P. Google makes passkeys the default sign-in method for all users [Електронний ресурс] / Page Carly // Join TechCrunch+. – 2023. – Режим доступу до ресурсу: https://techcrunch.com/2023/10/10/google-makes-passkeys-the-default-sign-in-method-for-all-users/?guce_referrer=aHR0cHM6Ly9kb3UudWEv&guce_referrer_sig=AQAAAEJ0f3SLi0ZdtLBNe11bqz6WDQxMu2q5pXEsU1KC8UdjCyjPe49NOsdj9eQ4dH1Q1Vlsz0hJMJh6H4sLT8gqGONKS-HVWIQQrlVEdaZkc7ZjN4EVwyGjWdnUB3yM2DhndY-dJzQqYUSZtOzvh5hK2AgbIBf_1vFZDI-KFbOXLc_8&guccounter=
2. Chaudhary, Sunil & Schafeitel-Tähtinen, Tiina & Helenius, Marko & Berki, Eleni. (2019). Usability, security and trust in password managers: A quest for user-centric properties and features. Computer Science Review. 33. 69-90. 10.1016/j.cosrev.2019.03.002.
3. Bergsma C. NIST Password Best Practices: 2022/2023 [Електронний ресурс] / Caitlin Bergsma // PSM. – 2022. – Режим доступу до ресурсу: https://www.psmpartners.com/blog/nist-password-best-practices/#:~:text=The%20NIST%20advises%20a%20password,only%20be%20sixty%2Dfour%20characters.
4. Sign in your user with Credential Manager [Електронний ресурс] // Google for Developers. – 2023. – Режим доступу до ресурсу: https://developer.android.com/training/sign-in/passkeys.

5. Passkey support on Android and Chrome [Електронний ресурс] // Google. – 2023. – Режим доступу до ресурсу: https://developers.google.com/identity/passkeys/supported-environments#google-password-manager.
6. Passkeys developer guide for relying parties [Електронний ресурс] // Google. – 2023. – Режим доступу до ресурсу: https://developers.google.com/identity/passkeys/developer-guide.