УДК 004.921

МОДЕЛЮВАННЯ СИСТЕМ З БЕЗПАРОЛЬНОЮ АВТЕНТИФІКАЦІЄЮ НА ОСНОВІ ПРОМИСЛОВИХ СТАНДАРТІВ

MODELING SYSTEMS WITH PASSWORDLESS AUTHENTICATION BASED ON INDUSTRY STANDARDS

Юрій Тарнавський, Анна Дяк

Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», просп. Берестейський, 37, Київ, 03056, Україна

Оскільки кіберзагрози продовжують зростати, обмеження та вразливості традиційних систем автентифікації на основі паролів стають все більш очевидними. Багатообіцяючою альтернативою стає безпарольна автентифікація, що пропонує підвищену безпеку та зручність для користувачів.

Традиційна автентифікація значною мірою покладається на паролі, які часто є слабкими, повторно використовуваними та вразливими до фішингу, атак грубої сили та зломів баз даних. На противагу цьому, безпарольна автентифікація усуває потребу в паролях, використовуючи безпечніші методи, такі як біометрія, апаратні токени (YubiKeys) та програмні додатки, які здійснюють автентифікацію за допомогою push-повідомлень або одноразових паролів, прив'язаних до певного часу (TOTP).

Було розроблено кілька галузевих стандартів, які керують впровадженням систем безпарольної автентифікації: FIDO2/WebAuthn, NIST SP 800-63 та OAuth2.0.

FIDO2/WebAuthn забезпечує безпарольну автентифікацію за допомогою криптографії з відкритим ключем. WebAuthn дозволяє веб-програмам використовувати автентифікатори, такі як біометричні дані або апаратні токени. Під час реєстрації автентифікатор створює та зберігає приватний ключ, надсилаючи відкритий ключ на сервер. Для автентифікації він підписує виклик сервера закритим ключем, безпечно перевіряючи користувача.

NIST SP 800-63 містить настанови щодо управління цифровою ідентичністю, зосереджуючись на оцінці ризиків, перевірці ідентичності, рівнях забезпечення автентичності (AAL) та федерації. Стандарт заохочує безпарольну автентифікацію та пропонує рекомендації для процесів автентифікації, адаптованих до різних рівнів ризику.

OAuth 2.0 - це фреймворк авторизації, який дозволяє стороннім додаткам отримувати обмежений доступ до ресурсів користувача без розкриття облікових даних. OpenID Connect базується на OAuth 2.0, забезпечуючи автентифікацію на додаток до авторизації за допомогою веб-токенів JSON (JWT) і підтримуючи безперебійний процес єдиного входу.

Моделювання систем з безпарольною автентифікацією на основі стандартів FIDO2/WebAuthn, NIST SP 800-63 та OAuth 2.0 значно підвищує безпеку і зручність для користувачів. Безпарольні методи усувають вразливості традиційних паролів. Використання цих стандартів дозволяє створювати надійні системи автентифікації, що відповідають сучасним вимогам кібербезпеки.

Бібліографія

1. Blokdyk G. Paswordless Authentication, Second Edition. 5STARCooks, 2021. 80-93 p.
2. Cybersecurity Essentials / C. J. Brooks et al. Hoboken. John Wiley & Sons, 2018. 784 p.