АРХІТЕКТУРА ТА ЗАСОБИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНОГО МЕНЕДЖЕРА ПАРОЛІВ ІЗ НАСКРІЗНИМ ШИФРУВАННЯМ

Федюшин О.І., Міллер К.З.
Харківський національний університет радіоелектроніки, Харків, Україна

Швидке зростання кількості веб-сервісів та хмарних платформ призводить до використання користувачами десятків паролів. На практиці це часто завершується використанням слабких або повторюваних даних, що значно підвищує ризик компрометації облікових записів. Хмарні менеджери паролів дозволяють централізовано зберігати та синхронізувати облікові дані між пристроями, проте у традиційних рішеннях питання безпеки часто обмежуються лише використанням TLS-шифрування каналу та базовим хешуванням паролів на сервері. Компрометація серверної інфраструктури або внутрішні зловмисники в таких моделях можуть призвести до витоку конфіденційної інформації. Одним із сучасних підходів до мінімізації довіри до сервера є застосування концепції наскрізного шифрування (end-to-end encryption, E2EE). У цій моделі всі критично важливі криптографічні операції виконуються виключно на стороні клієнта, а на сервер передаються та зберігаються лише зашифровані дані. Сервер виступає транспортним рівнем та сховищем і не має доступу до відкритого вмісту сховища паролів. Додатково використовується принцип «zero-knowledge»: постачальник сервісу не володіє інформацією, яка дозволила б відновити ключі шифрування користувача.

Метою доповіді є розробка та дослідження архітектури безпечного хмарного менеджера паролів із наскрізним шифруванням та автентифікацією користувача, у якому серверна частина не має доступу до відкритих облікових даних, а компрометація сервера не призводить до розкриття вмісту сховища. Для досягнення цієї мети запропоновано поєднання криптографічних механізмів на стороні клієнта з захищеною серверною інфраструктурою, яка відповідає за автентифікацію, авторизацію та синхронізацію. **Об'єктом дослідження** є процес зберігання та синхронізації облікових даних користувачів у хмарному середовищі. **Предметом дослідження** є методи організації наскрізного шифрування, керування ключами та автентифікації користувача в архітектурі хмарного менеджера паролів [1]. У запропонованій архітектурі користувацькі секрети (логіни, паролі, нотатки, дані двофакторної автентифікації) [2] зберігаються у вигляді зашифрованого сховища, ключ до якого генерується локально з майстер-пароля. Для формування криптографічних ключів використовується стійка функція похідних від пароля, наприклад Argon2id або PBKDF2 з індивідуальною сіллю та високою обчислювальною складністю. Отриманий ключ розділяється на принаймні два логічні компоненти: ключ шифрування сховища та ключ автентифікації, що знижує ризики у разі часткової компрометації.

Для симетричного шифрування вмісту сховища доцільно застосовувати сучасні режими автентифікованого шифрування, такі як AES-GCM [3], які

одночасно забезпечують конфіденційність і цілісність даних. Кожен запис у сховищі має власний унікальний вектор ініціалізації (IV/nonce), а метадані (мітки часу, тип запису, ідентифікатор запису) включаються до додаткових автентифікованих даних (AAD). Це ускладнює маніпуляції з зашифрованим вмістом без знання ключа.

Автентифікація користувача на сервері відділяється від механізму шифрування сховища. Додатково може використовуватися двофакторна автентифікація, що зменшує ризик захоплення облікового запису при витоку пароля [4, 5]. Серверна частина реалізує REST- або GraphQL-API для роботи з зашифрованими сховищами, а також механізм черги змін для синхронізації між кількома пристроями.

У роботі проведено формалізацію моделі загроз для хмарного менеджера паролів та аналіз основних сценаріїв атак: компрометація серверної БД, пасивне перехоплення трафіку, атаки грубої сили на майстер-пароль, спроби підміни клієнтського застосунку. Показано, що у разі компрометації серверного сховища зловмисник отримує доступ лише до зашифрованих даних; їхнє успішне розшифрування потребує підбору майстер-пароля з урахуванням параметрів KDF, що при правильному виборі параметрів робить атаку економічно невигідною. На основі запропонованої архітектури розроблено прототип хмарного менеджера паролів, у якому криптографічні операції на клієнті реалізовано із застосуванням стандартних засобів платформи, а серверна частина побудована як веб-служба з використанням сучасного фреймворку та реляційної бази даних. Проведені експериментальні дослідження показали, що вибрані параметри KDF забезпечують прийнятний час обробки на користувацьких пристроях при значному підвищенні стійкості до атак перебору. Отримані результати демонструють, що застосування наскрізного шифрування, розділення ключів та посилених механізмів автентифікації дозволяє суттєво підвищити рівень безпеки хмарних менеджерів паролів без критичного погіршення зручності користування. Подальші дослідження можуть бути спрямовані на інтеграцію апаратних модулів безпеки, побудову формальних доказів стійкості окремих компонентів системи та впровадження додаткових механізмів захисту від фішингових атак і компрометації клієнтських пристроїв.

Список літератури

1. Bonneau J., Herley C., Van Oorschot P., Stajano F. The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes // 2012 IEEE Symposium on Security and Privacy. – 2012. – P. 553–567.

2. Biryukov A., Dinu D., Khovratovich D. Argon2: The Memory-Hard Function for Password Hashing and Other Applications // Proc. of IEEE EuroS&P. – 2016. – P. 289–302.

3. Dworkin M. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC. NIST Special Publication 800-38D. – 2007.

4. Grassi P. et al. Digital Identity Guidelines. NIST Special Publication 800-63B. – 2017.

5. FIDO Alliance. FIDO2: Client to Authenticator Protocol (CTAP) and Web Authentication (WebAuthn). Technical Specifications. – 2019.