УДК 004.422.83

В. Левицький, канд. тех. наук, А. Станько, А.А. Микитишин
Тернопільський національний технічний університет імені Івана Пулюя, Україна

АНАЛІЗ ТЕХНОЛОГІЇ БЕЗПАРОЛЬНОЇ АУТЕНТИФІКАЦІЇ ЯК МЕТОД ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

V. Levytskyi , Ph.D., A. Stanko, A. Mykytyshyn

ANALYSIS OF SAFETY AUTHENTICATION TECHNOLOGY AS A METHOD OF INFORM SAFETY

Аутентифікація без паролів – сучасний напрямок розробників і кібербезпеки. В індустрії відомі різні способи обходу прямого введення паролю: за допомогою біометрії та біхевіоральних даних для підтвердження особистості. Але всі ці спроби не дали бажаного результату. Новою частиною розроблюваних технологій став стандарт під назвою WebAuthn. Стандарт передбачає що, єдиний відбиток пальця або пристрій-ідентифікатор дозволятиме проходити аутентифікацію в усі необхідні ресурси. WebAuthn — результат спільної роботи Консорціума Всесвітньої павутини та альянсу FIDO (Fast Identity Online).

Нова технологія повинна стати продовженням існуючих специфікацій FIDO — U2F та UAF. Зараз вони використовуються для так званої двохфакторної аутентифікації. Під час неї користувач, крім вводу паролю, також повинен вказати другий, тимчасовий код для отримання доступу до аккаунта. Часто аутентифікація без паролю стає другорядною опцією, а за допомогою WebAuthn браузери будуть підтримувати її нативно. Для єдиного логіна у всіх браузерах та онлайн-екаунтах з’явиться дві опції. Перша – універсальний USB-донгл з підтримкою нового протоколу FIDO. Приклад такого – Yubikey від компанії yubico. Друга опція – використання біометричного ідентифікатора (наприклад, за допомогою відбитку пальця).

У процесі аутентифікації беруть участь три елементи. Перший - це WebAuthn Relying Party. Він являє собою сайт, на який хоче зайти користувач.

Другий елемент - WebAuth API. В його основі лежать два базових методи, що відповідають за реєстрацію і вхід в систему: navigator.credentials.create () і navigator.credentials.get (). Один створює реквізити доступу при реєстрації нового аккаунта і пов'язує пару ключів з уже існуючим. Інший - використовує відомі дані для авторизації на сайті. Обидва методи застосовують захищене з'єднання для передачі інформації (наприклад, HTTPS).

Третій елемент - це аутентифікатор. Він керує ідентифікаційними даними користувачів і відповідає за генерацію публічних ключів облікових записів.

У такому випадку процедура авторизації може виглядати наступним чином:

1. Користувач заходить на сайт і вибирає опцію беспарольної аутентифікації (наприклад, за допомогою телефону).
2. Сайт направляє клієнту WebAuthn (браузеру) відповідний JavaScript-запит.
3. Браузер звертається до аутентифікатору (смартфону), щоб той згенерував ключі і направив їх перевіряючій стороні.
4. Сервер перевіряє дані для входу.
5. Якщо все в порядку, то користувач авторизується на сайті.

Впровадження таких нововведеннь в браузерах дозволять підвищити захист від фішингу, атак посередника (MITM) і атак повторного відтворення.

Література

1. A demo of the WebAuthn specification. [Електронний ресурс] – Режим доступу: https://webauthn.io.