УДК 004.056.523

ДОСЛІДЖЕННЯ МЕТОДІВ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Кутовий Д.О.
Науковий керівник – проф. Філатов В.О.
Харківський національний університет радіоелектроніки, каф. ШІ
м. Харків, Україна
тел.: +38(050) 237-74-94, e-mail: danylo.kutovyi@nure.ua

Cybersecurity is a constant battle between those who possess information worth protecting and those who want to obtain it. With the development of technology, security is increasing exponentially. Passwords are one of the methods used to protect vulnerabilities. However, as technology evolves, passwords can be guessed or decrypted, leading to increased demands for longer, more complex passwords. Two-factor authentication (2FA), a subset of MFA, was proposed as a possible solution to combat weak user passwords but also has its own set of problems.

This article discusses some of the vulnerabilities of different password protection methods and the challenges of implementing effective cybersecurity measures.

Кібербезпека – це постійна боротьба між тими, хто володіє інформацією, яку варто захистити, і тими, хто хоче отримати цю інформацію. З розвитком технологій безпека зростає в експоненціальній швидкості. Ранні комп’ютери спричинили зміну дизайну безпеки: від незначного захисту шляхом обмеження фізичного доступу до безпеки для кількох користувачів і багаторівневого застосування. У епоху Інтернету будь-який підключений пристрій є потенційно вразливим. Один із методів захистити вразливості входу — це паролі.

У сфері технологій паролі реалізуються комп’ютерами, причому комп’ютер пропонує завдання, на яке потрібно правильно відповісти в текстовому форматі. Комп’ютер може лише проаналізувати введений текст і порівняти його з точною правильною відповіддю, тобто правильну текстову відповідь на виклик користувач має точно запам’ятати. Оскільки технологія продовжує розвиватися, паролі можна вгадувати, розшифровувати або використовувати грубим методом, що призводить до підвищення вимог до паролів, включаючи довжину, використання символів і відмінності в регістрі літер.

Двофакторна аутентифікація (2FA), підмножина MFA, була запропонована як можливе рішення для боротьби зі слабкими паролями користувачів, але вона породжує власний набір проблем. Джовер виявив, що одноразові паролі (OTP) служби коротких повідомлень (SMS) вразливі до викрадення під час передачі незахищеними лініями стільникового зв’язку та заміною SIM-карт. Коган та ін. у своїй пропозиції щодо T/Key

обговорюють, як одноразовий пароль на основі часу (TOTP) вимагає, щоб секретне початкове число зберігалося у відкритому вигляді на сервері та може бути відкритим у разі атаки на всьому сервері. Дрю повідомляє про успішний злам мережі LockheedMartin, підрядника національної оборони, після того, як секретні коди LockheedMartin були викрадені з їхніх серверів. Сассе та ін. пояснюють, що якщо користувачі вважають політику безпеки або пароль надто складною або не повністю розуміють політику, вони, швидше за все, обійдуть її.

Наразі паролі є стандартним методом аутентифікації користувачів. Оскільки апаратне забезпечення продовжує розвиватися, зламати ці паролі стає легше. Традиційним рішенням цієї проблеми є постійно зростаюча складність пароля та двофакторна аутентифікація.

Однак користувачі стають напруженими через надто складні системи входу і часто обходять їх. Двофакторна аутентифікація також додає цю складність, і багато форм двофакторної аутентифікації за своєю суттю є небезпечними. У відповідь на ці проблеми цей проект пропонує безпарольну багатофакторну систему аутентифікації, яка використовує випробувані й перевірені існуючі технології, асиметричну криптографію, цифрові підписи та біометричну аутентифікацію.

Метою досліджень є визначення ефективності та надійності різних методів аутентифікації користувачів в інформаційних системах з метою поліпшення захисту конфіденційної інформації та забезпечення безпеки користувачів. В доповіді наводяться такі методи дослідження:

- експериментальні дослідження ефективності різних методів аутентифікації користувачів в інформаційних системах, включаючи тестування на реальних користувачах та оцінку швидкості та точності роботи;
- застосування методів статистичного аналізу та інші методи обробки даних для оцінки результатів дослідження;
- вивчення сучасних тенденцій та розробка нових методів аутентифікації користувачів в інформаційних системах.

Список використаних джерел:

1. J. Foti, «Guideline for the use of advanced authentication technology alternatives» National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST Special Publication (SP) 800-32 Rev 1 (Final), 1994.

2. G. A. Miller, «The magical number seven, plus or minus two: some limits on our capacity for processing information» Psychological review, vol. 63, no. 2, p. 81, 1956.

3. D. of Defense, «Dod instruction 8520.03, identity authentication for information systems» Department of Defense, Tech. Rep., May 2011.