УДК 004.056

Олійник В. О.
Маліновський В. І.

АНАЛІЗ ВІДОМИХ ТЕХНОЛОГІЙ І ЗАСОБІВ ЗАХИСТУ ДАНИХ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Вінницький національний технічний університет

Анотація

У роботі проведено аналіз сучасних технологій і засобів захисту даних автентифікації в інформаційних системах. Розглянуто основні підходи до автентифікації користувачів, зокрема парольну, багатофакторну та токен-орієнтовану автентифікацію. Проаналізовано сучасні методи захисту облікових даних, включаючи криптографічне хешування, використання солі та одноразових паролів. Окрему увагу приділено практичним аспектам реалізації систем автентифікації. Визначено, що ефективний захист досягається за рахунок комплексного поєднання декількох технологій.

Ключові слова: автентифікація, інформаційна безпека, MFA, хешування, JWT, OTP, захист даних

Abstract

The paper analyzes modern technologies and tools for protecting authentication data in information systems. The main approaches to user authentication are considered, in particular password, multi-factor, and token-oriented authentication. Modern methods of protecting credentials, including cryptographic hashing, the use of salts, and one-time passwords, are analyzed. Special attention is paid to the practical aspects of implementing authentication systems. It is determined that effective protection is achieved through a comprehensive combination of several technologies.

Keywords: authentication, information security, MFA, hashing, JWT, OTP, data protection.

Вступ

У сучасному світі інформаційні системи відіграють ключову роль у функціонуванні бізнесу, державних установ і повсякденному житті користувачів . У зв’язку з цим питання забезпечення інформаційної безпеки набуває особливої актуальності, зокрема з точки зору захисту даних автентифікації [1, 2]. Механізми автентифікації є першою лінією захисту від несанкціонованого доступу до інформаційних ресурсів.

Зі збільшенням кількості кіберзагроз, таких як фішинг, збір даних і викрадення облікових даних, традиційні методи автентифікації поступово втрачають свою ефективність. Це зумовлює необхідність дослідження сучасних технологій захисту даних автентифікації, а також пошуку більш надійних і стійких до атак рішень [3-5].

Метою цієї роботи є аналіз існуючих технологій і засобів захисту даних автентифікації в інформаційних системах, визначення їх ефективності, переваг і недоліків, а також формулювання рекомендацій для підвищення рівня безпеки.

Постановка проблеми захисту даних автентифікації в інформаційних

Автентифікація в інформаційних системах — це процес встановлення достовірності суб’єкта доступу на основі наданих ним ідентифікаційних даних . Відповідно до підходів, визначених Національним інститутом стандартів і технологій, механізми автентифікації класифікуються за трьома основними факторами: фактор знання, фактор володіння та фактор спадковості [6]. Ця класифікація є основою для побудови сучасних систем контролю доступу.

Найбільш поширеним підходом є парольна автентифікація, яка передбачає перевірку секретного рядка, відомого лише користувачу. Однак, як показано в дослідженні Джозефа Бонно, більшість користувачів використовують слабкі або передбачувані паролі, що суттєво знижує ефективність цього методу [7]. Крім того, згідно з рекомендаціями OWASP Foundation [4], парольні системи є вразливими до атак перебору, словникових атак типу credential stuffing [4]. Це зумовлює необхідність використання додаткових механізмів захисту.

Для підвищення рівня безпеки застосовується багатофакторна автентифікація (MFA) [8], яка передбачає поєднання кількох незалежних факторів. Використання MFA значно знижує ймовірність компрометації облікового запису навіть у разі витоку пароля. Практична реалізація MFA передбачає,

наприклад, використання пароля разом із одноразовим кодом, згенерованим мобільним застосунком або надісланим через SMS [8].

З точки зору захисту даних автентифікації критично важливим є спосіб їх зберігання. У сучасних системах паролі не зберігаються у відкритому вигляді, а обробляються за допомогою криптографічних хеш-функцій. Алгоритми bcrypt, scrypt та Argon2 реалізують принципи адаптивного хешування, що передбачає підвищення обчислювальної складності процесу з метою ускладнення атак перебору. Використання механізму «солі» дозволяє уникнути однакових хешів для однакових паролів і запобігає застосуванню попередньо обчислених таблиць [3, 5].

Практична реалізація захисту паролів може бути представлена таким алгоритмом: під час реєстрації користувача пароль хешується з випадковою «сіллю», після чого в базі даних зберігається лише отриманий хеш. Під час автентифікації введений пароль обробляється аналогічним чином, і результат порівнюється зі збереженим значенням. Такий підхід забезпечує захист навіть у разі компрометації бази даних.

Окрему увагу слід приділити методам автентифікації на основі токенів, які широко застосовуються у вебзастосунках. Зокрема, стандарт JSON Web Token (JWT) [9] дозволяє реалізувати механізм керування сесіями без збереження стану (stateless). Після успішної автентифікації сервер генерує токен, який підписується криптографічним ключем і передається клієнту. У подальших запитах цей токен використовується для підтвердження прав доступу без необхідності повторної перевірки пароля [9].

Ще одним практичним механізмом є використання одноразових паролів (OTP), які генеруються на основі часу або подій [8]. Відповідно до стандарту TOTP, код змінюється через певний проміжок часу, що значно ускладнює його перехоплення та повторне використання. Такий підхід широко застосовується в банківських системах і сервісах із підвищеними вимогами до безпеки.

Висновок

Сучасні інформаційні системи функціонують в умовах постійного зростання кількості кіберзагроз, що обумовлює підвищені вимоги до захисту даних автентифікації. У цьому контексті ефективна організація процесів автентифікації стає одним із ключових факторів забезпечення надійності та безпеки інформаційних ресурсів.

Аналіз існуючих підходів показує, що використання лише одного методу автентифікації не дозволяє досягти необхідного рівня захисту. Саме тому сучасні рішення орієнтуються на комбінування декількох технологій, що дозволяє враховувати як технічні аспекти безпеки, так і поведінкові особливості користувачів.

Застосування багатофакторної автентифікації, сучасних алгоритмів хешування та токен-орієнтованих механізмів створює основу для побудови гнучких та масштабованих систем захисту. Такі системи здатні адаптуватися до нових викликів та забезпечувати стабільну роботу навіть в умовах підвищеного навантаження та активних спроб несанкціонованого доступу.

Загалом, розвиток технологій автентифікації відкриває нові можливості для підвищення рівня інформаційної безпеки, що робить їх важливим напрямом подальших досліджень і практичних розробок у сфері інформаційних систем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Конахович Г. Ф. Захист інформації в комп'ютерних системах : навч. посіб. / Г. Ф. Конахович, В. П. Климчук. – К. : Видавництво «Ліра-К», 2019. – 320 с.
2. Хорошко В. О. Основи інформаційної безпеки : навч. посіб. / В. О. Хорошко, О. Д. Азаров. – Вінниця : ВНТУ, 2015. – 216 с.
3. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 7th ed. – Pearson, 2017. – 768 p.
4. Authentication Cheat Sheet [Електронний ресурс] / OWASP Foundation. – 2023. – Mode of access: https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html.
5. Menezes A. Handbook of Applied Cryptography / A. Menezes, P. van Oorschot, S. Vanstone. – CRC Press, 2018. – 816 p.
6. Digital Identity Guidelines / National Institute of Standards and Technology. – Gaithersburg : NIST, 2020. – 128 p.
7. Bonneau J. The Science of Guessing: Analyzing an Anonymized Corpus of Passwords / J. Bonneau // IEEE Symposium on Security and Privacy. – 2012. – P. 538–552.
8. M'Raihi D. TOTP: Time-Based One-Time Password Algorithm : RFC 6238 / D. M'Raihi. – IETF, 2011. – 16 p.
9. Jones M. JSON Web Token (JWT) : RFC 7519 / M. Jones, J. Bradley, N. Sakimura. – IETF, 2015. – 30 p.

Олійник Володимир Олегович – студент групи 2 БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: vovaolinik4@gmail.com.

Науковий керівник: Маліновський Вадим Ігоревич – доцент кафедри захисту інформації , Вінницький національний технічний університет, Вінниця, email: v.malinovskyi@vntu.edu.ua.

Oliinyk Volodymyr O. – student, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: vovaolinik4@gmail.com.

Scientific supervisor: Malinovskyi Vadym I. – Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, email: v.malinovskyi@vntu.edu.ua.