УДК 004.056.5

А. В. Кришина
В. В. Лукічов

ЗАСІБ ТРИФАКТОРНОЇ АВТЕНТИФІКАЦІЇ

Вінницький національний технічний університет;

Анотація

Дослідження розглядає засіб трифакторної автентифікації, що забезпечує підвищений рівень безпеки за рахунок використання трьох різних факторів підтвердження особи, що забезпечують вищий рівень безпеки, оскільки використовує комбінацію різних факторів, таких як паролі, токени безпеки та біометричні дані. Це ускладнює роботу зловмисників і знижує ризик несанкціонованого доступу.

Ключові слова: трифакторна автентифікація, токен, біометричні дані, пароль

Abstract

The study looks at a three-factor authentication tool that provides an increased level of security through the use of three different identity verification factors that provide a higher level of security because it uses a combination of different factors such as passwords, security tokens, and biometrics. This makes it more difficult for attackers to work and reduces the risk of unauthorized access.

Keywords: Three-factor authentication, token, biometrics, password

Вступ

З кожним роком зростає кількість кібератак і спроб несанкціонованого доступу до конфіденційної інформації, що вимагає постійного вдосконалення методів захисту.

Традиційні методи автентифікації, такі як паролі та PIN-коди, виявилися недостатньо ефективними для вирішення нових викликів кібербезпеці.

Тому потрібен був більш надійний метод перевірки особи.

Одним із цих методів є трифакторна автентифікація, яка використовує три різні фактори автентифікації: знання, активи та біометричні дані для забезпечення високого рівня захисту.

Цей метод вимагає трьох незалежних перевірок для успішної автентифікації, що значно зменшує можливість несанкціонованого доступу.

Результати досліджень

Процес автентифікації — це процес перевірки ідентичності сутності на основі одиного або кілька факторів.[1]

Існує кілька методів аутентифікації, автентифікація на основі пароля - це найпоширеніший метод автентифікації, коли користувачі вказують ім'я користувача та пароль для доступу до системи чи програми.

Багатофакторна автентифікація (MFA) цей метод вимагає від користувачів надання двох або більше форм ідентифікації, таких як пароль і відбиток пальця або одноразовий код, надісланий на їхній мобільний пристрій.

Автентифікація на основі токена, цей метод використовує токен, наприклад веб-токен JSON (JWT), для автентифікації[2]

Дослідження трифакторної аутентифікації показало, що ця технологія має великий потенціал для підвищення рівня безпеки інформаційних систем.

Експерименти та аналізи проводилися в різних галузях промисловості, щоб оцінити ефективність, надійність і простоту використання.

Дослідження підтвердили, що трифакторна автентифікація значно знижує ймовірність несанкціонованого доступу до системи. Використання трьох незалежних факторів таких як знання, володіння та біометрія, підвищує надійність процесу автентифікації порівняно з однофакторним методом.

Зокрема, систему три факторної автентифікації майже неможливо зламати, якщо немає фізичного доступу до всіх трьох елементів. Трифакторна автентифікація успішно використовується в банківському секторі для захисту онлайн-банкінгу та транзакцій.

Дослідження показують, що впровадження такої автентифікації зменшує шахрайство на 70-80%.

Державні установи використовують для захисту державних інформаційних систем і баз даних.

Дослідження показують, що кібератаки на державні ресурси значно зменшилися після впровадження трифакторної аутентифікації.

Хоча така автентифікація забезпечує високий рівень безпеки, дослідження показали, що його впровадження може викликати деякі труднощі з точки зору взаємодії з користувачем.

Користувачі часто стикаються з незручністю використання кількох пристроїв або проходження біометричних перевірок.

Проте з розвитком технологій, особливо мобільних додатків і більш досконалих біометричних датчиків, ці недоліки поступово зменшуються.

Основними технічними проблемами є інтеграція трифакторної автентифікації в існуючі системи, забезпечення сумісності між різними пристроями та платформами та захист біометричних даних від компрометації.

Проте з розвитком технологій штучного інтелекту та машинного навчання можливості постійно розширюються, що робить цей метод все більш ефективним та зручним для користувачів.

Таким чином, результати дослідження демонструють високу ефективність трифакторної автентифікації в захисті інформаційних систем, водночас підкреслюючи необхідність подальшого вдосконалення технології для покращення досвіду користувача .

Висновки

Трифакторна автентифікація значно підвищує рівень безпеки інформаційних систем, поєднуючи три незалежні фактори підтвердження особи: знання, володіння та біометрію. Цей багатошаровий підхід суттєво знижує ризик несанкціонованого доступу та забезпечує надійний захист від кібератак і витоків даних. Незважаючи на високий рівень безпеки, може створювати деякі незручності для користувачів, пов'язані з необхідністю використання кількох факторів автентифікації. Однак, нові технології, такі як мобільні додатки та удосконалені біометричні системи, допомагають зменшити ці незручності, роблячи процес автентифікації більш зручним та швидким.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Smith, Richard E. Authentication: From Passwords to Public Keys. New York: McGraw-Hill, 2002.
2. Zhang, David. Biometric Authentication: A Machine Learning Approach. London: Springer, 2014.Kaufman, Charlie, Radia Perlman, and Mike Speciner. Network Security: Private Communication in a Public World. New York: Prentice Hall, 2002.
3. Anderson, Ross. Security Engineering: A Guide to Building Dependable Distributed Systems. New York: Wiley, 2008.
4. Jurjens, Jan. Designing Usable and Secure Software with IRIS and UML. Berlin: Springer, 2013.
5. Stanislav, Mark, and Joseph Zachary. Authentication. New York: Wiley, 2016.

Кришина Адріана Віталіївна — студентка групи 1БС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, email: adriana.krush@gmail.com

Лукічов Віталій Володимирович — доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, email: lukichov.vitalyi@vntu.edu.ua

Kryshyna Adriana— student of group 1БС-20б, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: adriana.krush@gmail.com

Lukichov Vitalii — Associate Professor of the Department of Information Security, Vinnytsia National Technical University, Vinnytsia, email: lukichov.vitalyi@vntu.edu.ua