МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЦЕНТРАЛЬНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ

УДК 004.4

Тези доповідей

VI Міжнародної науково-практичної конференції

"Інформаційна безпека та комп'ютерні технології"

20-21 квітня 2023 року

Кропивницький 2023

УДК 004.4

Матеріали VI Міжнародної науково-практичної конференції "Інформаційна безпека та комп'ютерні технології": тези доповідей, 20-21 квітня 2023 р. – Кропивницький: ЦНТУ, 2023. – 96 с.

Наведені тези пленарних та секційних доповідей за теоретичними та практичними результатами наукових досліджень і розробок. Представлені результати теоретичних досліджень в галузях проектування інформаційних систем, технологій захисту інформації, використання сучасних інформаційних технологій в управлінні системами за різними галузями народного господарства.

Матеріали публікуються в авторській редакції.

За достовірність викладених фактів, цитат та інших відомостей відповідальність несуть автори.

УДК 004.056.523.052(045)

О.В. Салієва[1], І.О. Бондаренко[1], М.О. Берестенко[1]
salieva8257@gmail.com
[1]*Вінницький національний технічний університет, м. Вінниця*

УДОСКОНАЛЕННЯ АЛГОРИТМУ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА НА ОСНОВІ ЕЛЕКТРОННОГО КЛЮЧА ТА ДИНАМІЧНОЇ БІОМЕТРІЇ

Невпинний розвиток інформаційних систем обумовлює гостру потребу забезпечення захищеності даних, що циркулюють в них. Вирішити дану задачу можна різними способами, зокрема шляхом обмеження доступу до конфіденційної, службової, таємної та інших видів інформації за допомогою механізмів автентифікації.

Дослідженню питань щодо удосконалення методів автентифікації користувача присвячено безліч наукових праць, зокрема [1-5].

Особливий інтерес представляє двофакторна автентифікація, що забезпечує ідентифікацію користувача за допомогою двох різних типів автентифікаційних даних. Механізмами для проведення такого типу автентифікації є: знання (інформація, яку знає тільки користувач), володіння (предмет, який є лише у користувача) та невід'ємність (біометричні дані користувача).

Біометричні засоби захисту інформації гарантують високу надійність, підвищений рівень безпеки, неможливість відмови від авторства та зручність для користувачів, враховуючи невід'ємність біометричних характеристик від конкретної особи. Важливе місце серед біометричних факторів займають динамічні, що ґрунтуються на поведінковій характеристиці людини: клавіатурний почерк, рукописний підпис, динаміка роботи комп'ютерної мишки і т. п. При вдалій комбінації біометрії з іншим типом автентифікаційних даних, наприклад із захищеним електронним ключем, система здатна захистити інформацію як від внутрішніх загроз, так і від зовнішніх вторгнень.

Метою роботи є удосконалення алгоритму двофакторної автентифікації користувача на основі захищеного електронного ключа з використанням алгоритму AES та аналізу ентропії рухів мишки.

Об'єктом дослідження є удосконалений алгоритм багатофакторної автентифікації користувача.

Предметом є процес вдосконалення алгоритму для підвищення достовірності автентифікації користувача на основі захищеного електронного ключа та аналізу ентропії рухів мишки.

У результаті дослідження удосконалено алгоритм двофакторної автентифікації на основі розробленого електронного ключа з використанням технології JSON Web Tokens та запропонованого алгоритму аналізу ентропії рухів мишки.

Першим етапом автентифікації користувача є застосування електронного ключа, використання якого можна описати таким чином:

Крок 1. Застосування даних користувача для запиту на формування токену.

Крок 2. Перевірка інформації користувача.

Крок 3. Формування електронного ключа та його шифрування.

Крок 4. Надання ключа користувачеві.

Крок 5 Зберігання користувачем токену та прикріплення його значення до кожного запиту.

Крок 6. Надання доступу користувачеві після перевірки ключа системою.

Крок 7. Можливість відновлення доступу на основі електронного ключа з використанням refresh-токену.

Запропонований алгоритм дозволяє не зберігати інформацію про всі видані токени, як при класичній схемі. У випадку реалізації окремого модуля сервісу аутентифікації за даним алгоритмом стає можливим створення єдиної точки входу в різні сервіси з однаковими обліковими даними.

Додаткове шифрування токену при передаванні користувачеві підвищує рівень захисту переданої послідовності та не викриває структуру даних, що розміщені у файлі. Для шифрування даних токену було використано симетричний ітеративний алгоритм AES, який дозволяє користувачам знайти компроміс між швидкістю та безпекою.

З метою визначення ентропії рухів комп'ютерної мишки було проаналізовано такі показники як:

траєкторія руху комп'ютерної мишки;

відхилення руху комп'ютерної мишки від зафіксованої траєкторії;

швидкість руху комп'ютерної мишки;

прискорення руху комп'ютерної мишки;

нетипові рухи комп'ютерної мишки;

кліки комп'ютерної мишки.

Розроблений алгоритм автентифікації користувача можна представити таким чином:

Крок 1. Запуск виконуваного файлу додатку.

Крок 2. Здійснення процесу автентифікації користувача.

Крок 2.1 Якщо користувач вже має обліковий запис у системі – перехід до кроку 6.

Крок 2.2 Якщо користувачеві необхідно отримати доступ до системи – перехід до кроку 3.

Крок 3. Реєстрація користувача.

Крок 3.1 Заповнення користувачем персональних даних.

Крок 3.2 Здійснення процесу аналізу рухів мишки.

Крок 3.3 Підтвердження процесу реєстрації.

Крок 4. Перевірка форм заповнених користувачем.

Крок 4.1 Якщо всі дані введені вірно та сформовано зразок рухів мишки, то запит на реєстрацію підтверджується.

Крок 4.2 Якщо форма реєстрації заповнена невірно, користувачеві виводиться на екран відповідне сповіщення, а форма реєстрації потребує повторного заповнення.

Крок 5. Підтвердження реєстрації користувача з боку адміністратора.

Крок 5.1 Адміністратор перевіряє нового користувача за його обліковими даними.

Крок 5.2 Якщо такому користувачеві необхідно надати доступ до системи – ставить відповідну відмітку для розмежування доступу.

Крок 5.3 Адміністратор формує електронний ключ, що надсилається користувачеві.

Крок 5.4 Збереження внесених змін.

Крок 6. Здійснення процесу автентифікації користувача.

Крок 6.1 Заповнення користувачем поля для введення логіну.

Крок 6.2 Завантаження електронного ключа.

Крок 6.3 Здійснення процесу аналізу рухів мишки.

Крок 6.4 Підтвердження процесу автентифікації.

Крок 7. Перевірка надання користувачеві доступу до системи.

Крок 7.1 Якщо логін та ключ користувача коректні, зразок ентропії рухів мишки відповідає зареєстрованому – користувач отримує доступ.

Крок 7.2 Якщо один із факторів не відповідає вимогам – користувачеві виводиться на екран сповіщення про невдалу спробу автентифікації.

У випадку, якщо користувач тричі здійснюватиме некоректний вхід, – доступ до облікового запису заблокується, електронний ключ буде недійсним. Для його поновлення потрібно звернутись до адміністратора та отримати новий електронний ключ на основі refresh-токену.

Крок 8. Після успішної автентифікації користувачеві надається доступ до системи.

Тобто, забезпечивши два фактори автентифікації, які залежать виключно від конкретного користувача (оскільки і ключ, і ентропія рухів мишки індивідуальні для кожного), маємо змогу підвищити достовірність автентифікації користувачів при здійсненні функції реєстрації та автентифікації у системі.

Висновки. З активним розвиток інформаційних технологій та систем невпинно зростає можливість зламу алгоритмів автентифікації, які ще донедавна вважалися надійними. Тому дане дослідження було спрямоване на вдосконалення алгоритму двофакторної автентифікації користувача на основі захищеного електронного ключа з використанням алгоритму AES та аналізу ентропії рухів мишки, що є індивідуальною характеристикою для кожної людини.

Для уникнення помилок автентифікації було розроблено електронний ключ з використанням ефективної, гнучкої та безпечної технології JSON Web Tokens. Застосування аналізу ентропії рухів мишки дозволило здійснити автентифікацію користувача на основі біометричних поведінкових характеристик, які є універсальними, унікальними та постійними.

Список літератури

1. В. В. Фесьоха, та Н. О. Фесьоха, «Модель нечіткої автентифікації користувачів інформаційних систем органів військового управління на основі поведінкової біометрії,» Захист інформації, т. 23, № 2, с. 116–123, 2021.

2. О. В. Горбенко, Ю. Л. Горбенко, А. Ю. Горбенко, та О. М. Сівоха, «Захист інформаційних систем за допомогою використання методів автентифікації,» Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського, с. 79-85, 2020.

3. О. Г. Корченко, А. М. Давиденко, та О. О. Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних,» Захист інформації, т. 21, №1, с. 40-51, 2019.

4. P. Jayapriya, R.R. Manimegalai, and R. Kumar Lakshmana, "A Survey on Different Techniques for Biometric Template Protection," Journal of Internet Technology, vol. 21, no. 5, 2020.

5. A. Sarkar and Binod K. Singh, "A Review on Different Biometric Template Protection Methods," Recent Advances in Computer Science and Communications, vol.14, issue 5, pp. 1551–1572, 2021.