

ЗАСІБ ДВОСТОРОННЬОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Вінницький національний технічний університет

Анотація

У роботі розглянуто підхід до реалізації засобу двосторонньої автентифікації користувачів у клієнт-серверних застосунках із використанням сучасних криптографічних методів. Запропоновано алгоритм взаємної перевірки автентичності клієнта та сервера на основі симетричного шифрування та генерації випадкових значень. Такий підхід дозволяє знизити ризик атак типу «людина посередині», повторного використання облікових даних та несанкціонованого доступу до інформаційних ресурсів.

Ключові слова: двостороння автентифікація, клієнт-серверні застосунки, криптографія, симетричне шифрування, інформаційна безпека.

Abstract

The paper considers an approach to implementing a mutual authentication mechanism in client-server applications using cryptographic methods. A mutual verification algorithm based on symmetric encryption and random number generation is proposed. This approach reduces the risks of man-in-the-middle attacks, replay attacks, and unauthorized access to information resources.

Keywords: mutual authentication, client-server applications, cryptography, symmetric encryption, information security.

Вступ

У сучасних інформаційних системах клієнт-серверна архітектура є однією з найбільш поширених моделей взаємодії між користувачами та сервісами. При цьому питання захисту інформації та контролю доступу до ресурсів набувають особливої актуальності. Традиційні механізми автентифікації, що базуються лише на використанні логіна та пароля, не забезпечують достатнього рівня безпеки в умовах зростання кількості кіберзагроз.

Однією з найбільш ефективних стратегій підвищення рівня захищеності є застосування двосторонньої автентифікації, за якої перевірка автентичності здійснюється як для клієнта, так і для сервера. Це дозволяє гарантувати, що користувач взаємодіє з легітимним сервером, а сервер — з авторизованим клієнтом.

Метою роботи є розроблення та аналіз засобу двосторонньої автентифікації користувачів у клієнт-серверних застосунках із використанням криптографічних методів.

Результати дослідження

Запропонований засіб двосторонньої автентифікації базується на використанні симетричних криптографічних алгоритмів та механізму обміну випадковими значеннями (nonce). Процес автентифікації складається з таких основних етапів:

1. Клієнт ініціює запит на підключення до сервера.
2. Сервер генерує випадкове число та надсилає його клієнту.
3. Клієнт шифрує отримане значення спільним секретним ключем і повертає результат серверу.
4. Сервер розшифровує повідомлення та перевіряє коректність відповіді клієнта.
5. Аналогічна процедура виконується сервером для підтвердження своєї автентичності перед клієнтом.

Для криптографічного захисту даних може використовуватися симетричний алгоритм шифрування з довжиною ключа не менше 256 біт, що забезпечує достатній рівень стійкості до сучасних атак.

Загальну модель взаємної автентифікації можна описати таким співвідношенням:

$$R = E_k(N)$$

де N – випадкове значення, K – спільний секретний ключ, E_k – операція шифрування, R – результат криптографічного перетворення.

Використання випадкових чисел у кожній сесії унеможливилює повторне використання перехоплених повідомлень зломисником.

Висновки

У результаті дослідження запропоновано засіб двосторонньої автентифікації користувачів у клієнт-серверних застосунках з використанням криптографічних методів. Даний підхід дозволяє суттєво підвищити рівень безпеки системи, зменшити ризик несанкціонованого доступу та забезпечити захист від типових мережесих атак. Запропонований механізм може бути використаний у програмних системах, де критично важливими є конфіденційність і цілісність даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Digital Identity Guidelines: Authentication and Lifecycle Management (SP 800-63B) [Електронний ресурс]. – Gaithersburg : National Institute of Standards and Technology, 2023. – Режим доступу: <https://doi.org/10.6028/NIST.SP.800-63b> (дата звернення: 22.02.2026).
2. The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446) [Електронний ресурс]. – Internet Engineering Task Force, 2023. – Режим доступу: <https://www.rfc-editor.org/rfc/rfc8446> (дата звернення: 22.02.2026).

Денис Олегович Булін — студент групи ІБС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: bulindenis952@gmail.com.

Науковий керівнику: **Віталій Володимирович Лукічов** — доцент кафедри захисту інформації Вінницький національний технічний університет, м. Вінниця.

Denys Olegovich Bulin — student of group 1BS-22b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bulindenis952@gmail.com.

Scientific supervisor: **Vitaliy Volodymyrovych Lukichov** — associate professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia.