ВИКОРИСТАННЯ ГІБРИДНОГО ШИФРУВАННЯ У СИСТЕМАХ ОБМІНУ ПОВІДОМЛЕННЯМИ (МЕСЕНДЖЕРАХ)

Цариценко І.К., Балагура Д.С.
Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні системи обміну повідомленнями (месенджери) є невід'ємною частиною цифрової комунікації користувачів та активно використовуються як у побутовій, так і в професійній діяльності. Вони забезпечують обмін текстовими повідомленнями, мультимедійним контентом, файлами, а також підтримують голосові та відеодзвінки. Зростання обсягів переданої інформації та зростаючі вимоги до конфіденційності даних зумовлюють необхідність використання ефективних криптографічних механізмів захисту інформації під час її передачі каналами зв'язку.

Особливої актуальності набуває питання забезпечення такого рівня захисту, щоб навіть сервери, через які передаються повідомлення, не мали можливості отримати доступ до їхнього вмісту. Така модель безпеки відома як наскрізне шифрування (end-to-end encryption) і є стандартом для сучасних захищених комунікаційних платформ. Сучасні месенджери, такі як Signal, WhatsApp та Telegram, використовують гібридний підхід до шифрування для вирішення цієї проблеми, який поєднує переваги симетричних та асиметричних криптографічних алгоритмів. Такий підхід дозволяє забезпечити високу швидкість обробки даних разом із надійним механізмом розподілу криптографічних ключів між абонентами, а також зменшити обчислювальне навантаження на клієнтські пристрої.[1]

Метою доповіді є дослідження принципів застосування гібридного шифрування в системах обміну повідомленнями та формування рекомендацій щодо підвищення рівня їх криптографічного захисту. Зокрема, розглядається використання асиметричного алгоритму RSA [2] для обміну ключами та симетричного алгоритму AES [3] для шифрування даних як базового підходу до забезпечення конфіденційності.

Така комбінація дозволяє вирішити проблему безпечної доставки ключа симетричного шифру, який використовується для безпосереднього шифрування повідомлень. Додатково враховується необхідність захисту цілісності та автентичності повідомлень, що може реалізовуватися шляхом використання криптографічних геш-функцій та механізмів аутентифікації повідомлень (MAC).

Разом з тим, більшість існуючих підходів гібридного шифрування в месенджерах, що базуються на використанні RSA для обміну ключами та AES для шифрування даних, мають суттєвий недолік — відсутність або недостатню реалізацію властивості perfect forward secrecy (PFS) [5].

Це означає, що безпека попередніх сесій залежить від збереження конфіденційності довгострокових ключів.

У разі компрометації довгострокового приватного ключа користувача зловмисник отримує можливість розшифрувати раніше перехоплені

повідомлення, що створює значні ризики для конфіденційності історичних даних. Така загроза є особливо критичною в умовах тривалого зберігання зашифрованого трафіку з метою його подальшого аналізу.

Для усунення зазначеного недоліку запропоновано удосконалений підхід до організації гібридного шифрування. Він передбачає використання RSA виключно для початкового обміну ключовим матеріалом у поєднанні з генерацією ефемерних (тимчасових) сесійних ключів AES для кожного сеансу зв'язку.

Додатково пропонується механізм динамічної ротації ключів після кожного повідомлення, що забезпечує реалізацію PFS та унеможливлює розшифрування попередніх повідомлень навіть у разі компрометації довгострокових ключів, зберігаючи при цьому високу продуктивність. Такий підхід також сприяє мінімізації обсягу даних, які можуть бути скомпрометовані внаслідок однієї атаки, та підвищує загальну стійкість системи до криптографічного аналізу.

У доповіді також розглядаються загальні принципи побудови клієнт-серверної архітектури захищених месенджерів та підходи до встановлення безпечного сеансу зв'язку між клієнтами.

Моделювання запропонованого підходу доводить, що навіть за умови повного контролю над серверною інфраструктурою зловмисник не має можливості отримати доступ до вмісту переданих повідомлень без володіння закритими ключами користувачів.

Отримані результати підтверджують доцільність застосування вдосконалених підходів гібридного шифрування та можуть бути використані при формуванні рекомендацій щодо підвищення безпеки сучасних систем обміну повідомленнями [4].

Список літератури

1. Paar C., Pelzl J. Understanding Cryptography. Springer, 2010. https://gnanavelrec.wordpress.com/wp-content/uploads/2019/06/2.understanding-cryptography-by-christof-paar-.pdf

2. Zehao Tuo. A comparative Analysis of AES and RSA algorithms and their integrated application. DOI: https://doi.org/10.54254/2753-8818/25/20240893

3. Rahoul Ganesh, Burhan Ul Islam Khan,· Abdul Raouf Khan, Amirrudin Bin Kamsin A panoramic survey of the advanced encryption standard: from architecture to security analysis, key management, real-world applications, and post-quantum challenges. https://link.springer.com/article/10.1007/s10207-025-01116-x

4. Гібридне шифрування. https://www.vpnunlimited.com/ua/help/cybersecurity/hybrid-encryption

5. Colin Boyd, Kai Gellert, A Modern View on Forward Security. *The Computer Journal*, Volume 64, Issue 4, April 2021, Pages 639–652 DOI: https://doi.org/10.1093/comjnl/bxaa104

Ігор Костянтинович Цариценко, бакалавр, +380999710223, ihor.tsarytsenko@nure.ua