УДК 004.056

Шамарін В.В., Вінковська І.С.

Національний університет «Одеська політехніка»

БЕЗПЕЧНИЙ ОБМІН ДАНИМИ В ДЕЦЕНТРАЛІЗОВАНИХ P2P-СИСТЕМАХ

Вступ. Сучасні інтернет-комунікації активно використовуються для обміну конфіденційною інформацією, тому питання захисту даних стає критично важливим. Централізовані моделі обміну повідомленнями, які базуються на клієнт-серверній архітектурі, мають суттєві недоліки – залежність від одного сервера, ризик перехоплення даних, цензурування та можливість компрометації інформації.

У зв'язку з цим актуальною є створення децентралізованих систем обміну повідомленнями, які базуються на архітектурі peer-to-peer (P2P) та забезпечують наскрізне шифрування.

Мета: Проаналізувати проблеми захисту інформації в сучасних месенджерах і обґрунтувати архітектурні підходи для побудови безпечного P2P-месенджера з інтегрованими криптографічними засобами.

1. Проблематика захисту інформації у сучасних месенджерах

Ключові проблеми більшості популярних месенджерів полягають у централізованій архітектурі, де вся комунікація та метадані користувачів проходять через сервери компаній – власників. Це призводить до таких ризиків:

– несанкціонований доступ до серверів – навіть за наявності наскрізного шифрування, метадані часто залишаються незахищеними;

– витік ключів шифрування – у деяких системах резервні копії чатів або ключі можуть зберігатися на хмарних сервісах, створюючи «єдину точку відмови»;

– недостатній контроль автентичності – існує ризик підміни відправника або повідомлення, якщо не застосовуються надійні механізми цифрового підпису.

Вирішенням цих проблем є перехід до децентралізованої (P2P) моделі, де дані передаються безпосередньо між користувачами, а всі криптографічні операції виконуються локально [1].

2. Застосування криптографічних методів у P2P-архітектурі

Криптографічні методи є основою безпечного P2P-месенджера, що гарантує конфіденційність, цілісність та автентичність переданих даних.

Конфіденційність забезпечується гібридним підходом, який поєднує асиметричне шифрування (ECC, RSA) для безпечного обміну ключами та симетричне шифрування (AES-256, ChaCha20) для швидкої та ефективної передачі великих обсягів даних.

Цілісність та автентичність гарантуються за допомогою цифрових підписів (Ed25519, RSA) та хеш-функцій (SHA-256), що підтверджують справжність відправника та незмінені повідомлення [2].

Для підвищення стійкості до атак типу «людина посередині» (MitM) доцільно впровадити протоколи обміну ключами з властивістю forward secrecy,

наприклад X3DH або Double Ratchet, як це реалізовано в Signal-протоколах [3].

Планується створення програмного засобу, який реалізує комбінований підхід до захисту, інтегруючи зазначені механізми безпосередньо в P2P-протокол.

3. Аналіз проблем та ризиків при побудові P2P-месенджера

Під час створення безпечного P2P-месенджера виникають ключові проблеми, які необхідно враховувати:

– складність управління ключами – безпечний обмін, зберігання та оновлення ключів без центрального сервера є технічно складним завданням;

– проблема ідентифікації – у P2P-мережі складніше забезпечити автентифікацію користувачів і гарантувати унікальність ідентифікаторів;

– людський фактор – помилки користувачів при керуванні ключами або налаштуванні параметрів безпеки можуть послабити ефективність технічних засобів захисту;

– продуктивність – криптографічні операції, особливо асиметричне шифрування, можуть уповільнювати передачу даних, тому необхідна оптимізація алгоритмів.

Також важливим аспектом є захист метаданих (часу, адреси комунікації), адже навіть при повному шифруванні вони можуть розкривати структуру взаємодії користувачів [4].

Висновок. Аналіз сучасних комунікаційних систем підтверджує, що створення безпечного P2P-месенджера з інтегрованими криптографічними механізмами є актуальним завданням кібербезпеки. Основними викликами залишаються управління ключами, автентифікація користувачів та мінімізація впливу людського фактора.

Подальша робота буде зосереджена на формуванні архітектури месенджера, що поєднує гібридне шифрування та цифрові підписи, а також на розробленні прототипу системи з автоматизованими процесами шифрування й перевірки автентичності. Очікуванні результати включають підвищення рівня конфіденційності комунікацій і демонстрацію практичної реалізації безпечних децентралізованих обмінів повідомленнями.

Перелік використаних джерел

1. CyberLab.ua «Загрози месенджера Telegram: що потрібно знати про ризики користування улюбленим месенджером?». 2023. – URL: https://cyberlab.ua/archives/5413

2. Яремчук Ю.Є., Салієва О.В., Бондаренко І.О. Основи криптографічного захисту інформації. Вінниця. 2024. – URL: https://pdf.lib.vntu.edu.ua/books/2024/Yaremchuk_2024_139.pdf

3. MoxieMarlinspike, TrevorPerrin. Signal. The X3DH Key Agreement Protocol. 2016. URL: https://signal.org/docs/specifications/x3dh/

4. Матвій О.В., Мельник В.С., Черевко І.М. Основи комп'ютерних мереж. Чернівці. Навчальний посібник. 2024. – URL: https://archer.chnu.edu.ua/bitstream/handle/123456789/10326/Основи%20комп%27ютерних%20мереж_%20навчальний%20посібник.pdf?sequence=1