

Аудит

Ми взяли кожне твердження з цього сайту й з App Store і звірили його з кодом, який це твердження виконує. Нижче - що тримається, що ми полагодили того ж дня і чого ми не робимо.

Аудит внутрішній. Зовнішнього аудиту в «Тиші» не було жодного разу, і ми пишемо це першим рядком, а не дрібним шрифтом унизу. Внутрішня перевірка коштує довіри менше, ніж зовнішня - але сказати «пройшли аудит», не назвавши аудитора, коштувало б усієї.

Навіщо це взагалі

Месенджер продає довіру, а довіру не можна показати знімком екрана. Єдиний чесний спосіб - назвати обіцянку, показати місце, де вона виконується, і сказати, як перевірити це без нас. Там, де перевірити без нас не можна, ми пишемо про це прямо - і не робимо вигляд, що там теж усе перевірювано.

442

перевірки в застосунку

140

перевірок на сервері

2

сторонні складові - усього

3

аудити з 12 вересня

Обіцянка проти коду

Три можливих результати, і жодного четвертого: **тримається** - обіцянка виконується; **уточнено** - формулювання було сильнішим за правду, і ми його змінили; **полагоджено** - обіцянка не виконувалася, помилку виправлено.

Листування й дзвінки шифруються на телефонах

тримається

Шифрує libsignal - той самий рушій, що в Signal, прикріплений тегом і контрольною сумою. Код клієнта даємо за запитом: подивіться самі.

Постквантове установлення ключів

тримається

ML-KEM-1024 стоїть у кожній гілці знайомства, обійти його нічим. Перевірка міряє справжній розмір ключа - заглушку вона б спіймала.

Ключі не покидають телефон

тримається

Лежать у Keychain із позначкою «тільки цей пристрій»: у копію iCloud не їдуть і на новий телефон не переносяться. Досі це не охоронялося нічим - тепер охороняє перевірка.

Листування не потрапляє в резервну копію

тримається

Каталоги застосунку виключені з копії. Теж не мало перевірки - тепер має.

Ні сторонньої аналітики, ні стеження

тримається

У застосунку рівно дві сторонні складові: libsignal і збірка WebRTC. Жодного хоста, крім нашого сервера й ретранслятора.

Пуш не містить нічого з листування

тримається

Сервер не має тексту й не може його вкласти. Текст підставляє ваш телефон, розшифрувавши сам.

Пошуку людей немає

тримається

Запиту «дай ключі за іменем» на сервері не існує - і його відсутність закріплена окремими перевірками, щоб він не з'явився непомітно.

Дзвінок за замовчуванням ховає вашу адресу

з обмовкою

Ide через ретранслятор, і той не бачить змісту. Але якщо ретранслятора немає, дзвінок піде прямо - і тоді адресу побачить співрозмовник. Екран дзвінка про це каже.

Адреса черги нічого про вас не каже

полагоджено

Раніше вона рахувалася з вашого імені - отже таблиця конвертів на сервері вказувала на людей, і перевірити це міг будь-хто зі словником. Тепер адреса випадкова й приїжджає до співрозмовника всередині запрошення.

Сервер не знає, хто кому пише

неправда, виправлено

15.09 ми пом'якшили це до «бачить, але не зберігає». Audit 29.09 показав, що й це сильніше за правду: сервер годину тримає, на які черги писав акаунт, а перший конверт розмови несе ключ відправника. Тепер сторінка приватності каже прямо: сервер знає, хто кому пише. Сховати відправника (Sealed Sender) - у плані.

12 слів повертають акаунт

виправлено

Раніше тут стояло «і листування» - неправда. Копія повертає співрозмовників, групи й налаштування; текст розмов лишається тільки на тому телефоні, де був.

«Видалити чат» видаляє

полагоджено

Фотографії й відео лишалися на диску: видалення шукало файл не під тим іменем. Виправлено, і перевірка тепер падає, якщо помилка повернеться.

«Один перегляд» зникає назавжди

полагоджено

Зникав рядок, а файл лишався в пам'яті телефона. Тепер зникає файл.

Видалення акаунта забирає все

полагоджено

Вкладення переживали видалення й чекали своїх чотирнадцяти днів. Тепер ідуть разом з акаунтом.

Чого ми не робимо

Цей список довший за попередній навмисно. Те, чого немає, зазвичай дізнаються пізніше й від когось іншого.

- **Зовнішнього аудиту не було.** Це найбільша відкрита позиція, і закрити її можна тільки грошима й чужим ім'ям на звіт.

- **Метадані ми маємо.** Ім'я користувача лежить відкритим, час і розмір кожного конверта видно. Повідомлення в групу йде окремим конвертом кожному - отже розмір групи видно з кількості. Адреса черги тепер випадкова, але сам сервер тримає її поруч з іменем в одному рядку: від нього вона не ховається й не могла б, поки доставка йде через нього.
- **Код входу замикає застосунок, а не листування.** Листування зашифроване ключем зі сховища iPhone - він прив'язаний до цього телефона й доступний, лише поки телефон розблоковано. З вашого коду цей ключ не виводиться, і ось чому це видно неозброєним оком: текст нового повідомлення з'являється у сповіщенні ще до того, як ви ввели код. Отже код і Face ID закривають екрани «Тиші», а не самі байти.
- **Знімок екрана ми не забороняємо.** iOS цього не вміє. Ми лише повідомляємо - і взаємно: вимкнувши повідомлення в себе, ви перестаєте їх і отримувати.
- **Вкладення на диску лежать під захистом iOS,** а не під нашим ключем - на відміну від самого листування.
- **Сервер закритий.** Код клієнта даємо за запитом (він під AGPL); усе серверне перевіряється на слово - або підняттям свого сервера, який ми ставимо за запитом.
- **Хостинг бачить те саме, що наш сервер** (він завершує захищене з'єднання), а Apple бачить час кожного сповіщення. Це ціна хостингу й ціна iOS, і обійти її ми не можемо.
- **Скарга - єдине місце, де текст потрапляє на сервер відкритим.** Ті повідомлення, які ви самі вибрали, і на 90 днів.

Як перевірити це без нас

- **Попросіть код застосунку.** Ми даємо його за запитом - разом із перевірками, про які тут написано. Він під AGPL; напишіть у підтримку, і ми його надішлемо.
- **Звірте код безпеки.** 60 цифр або QR у картці співрозмовника: якщо вони збігаються, між вами немає нікого третього. Змінився ключ - застосунок скаже.

- **Подивіться «Діагностику».** Хід дзвінка показує, яким шляхом іде звук і чи справді йдуть байти.
- **Підніміть свій сервер.** Команді чи організації ставимо «Тишу» на вашому залізі - тоді на слово не доведеться вірити взагалі.

Попередні перевірки: 12 вересня 2026 (25 знахідок, 19 закрито того ж дня), 13 вересня 2026 (перевірка власних правок), 15 вересня 2026 - цей звіт.