УДК 004.056.55

Савчук Д.О.
Шелепало Г.В.

АНАЛІЗ МЕТОДІВ ШИФРУВАННЯ ДЛЯ ЗАХИСТУ ІНФОРМАЦІЇ В МЕСЕНДЖЕРІ TELEGRAM

Вінницький національний технічний університет

Анотація: У даній статті розглянуто аналіз методів шифрування для захисту різного виду інформації в сучасному і популярному месенджері Telegram. Вивчено дане питання, наведено приклади методів шифрування.
Ключові слова: метод, захист, шифрування, сервер, ключ, аналіз, телеграм.

Abstract: This article discusses the analysis of encryption methods to protect different types of information in the modern and popular Telegram messenger. Studies of this issue are presented, examples of encryption methods are given.
Keywords: method, protection, encryption, server, key, analysis, telegram.

Вступ

В теперішній час метод збереження особистої інформації доволі актуальний і важливий, тому що в час розвитку технологій і різних месенджерів знаходяться люди, які залюбки несанкціоновано залізуть у ваші особисті повідомлення, і поширять їх будь-де. На сьогодні важко знайти людину, яка не знає про месенджер відомих російських братів-програмістів Павла та Миколи Дурових – Telegram. Їх месенджер відомий тим, що він багатоплатформовий. Дозволяє обмінюватися повідомленнями і медіафайлами в багатьох форматах. Клієнтські програми Telegram доступні для Android, iOS, Windows Phone, Windows, macOS і GNU / Linux. Користувачі можуть додавати і обмінюватися фотографіями, стікерами, голосовими і відео повідомленнями, файлами будь-якого типу, а також робити аудіо і відеодзвінки.

Додаток прив'язується до номера телефону, приходить для перевірки повідомлення з кодом (на мобільній версії для Android код підтягується автоматично). Спілкуватися можна як з конкретними користувачами, які вже встановили додаток, так і організовувати групові чати і відправляти запрошення повідомленням із закликом встановити собі даний додаток [1].

Найбільше телеграм відомий своїми методами шифрування інформації про які і піде мова в даній роботі.

Дослідження та приклади

Саме захист повідомлень від перехоплення і сторонніх очей став основою популярності месенджера. Після багатьох випадків витоку інформації, які одна за одною відбуваються в цьому році, хочеш-не хочеш три рази подумаєш, чим би таким скористатися, щоб особисті дані не потрапили в мережу інтернет. Тому важливо знати, що листи в Telegram міцно-міцно зашифровані, і можуть самоліквідуватися.

Дані в дата-центрах зберігаються на дисках в зашифрованому вигляді, кожен кластер зашифрований окремим ключем, який зберігається в іншому кластері під іншою юрисдикцією. Тобто навіть якщо хтось руками добереться до цих дисків, їм ще доведеться мозок зламати, щоб ваші повідомлення перечитати. А само-видалені повідомлення не зберігаються ніде. Брати Дурови відносяться по-особливому до даної розробки. Саме тому, щороку влаштовують хакерські конкурси, щоб виявити вразливості в системі. Переможець отримує грошову винагороду, а сервіс удосконалюється та стає все більш захищеним [1].

Шифрування Телеграм на основі MTProto

Протокол призначений для доступу до серверного API з додатків, що працюють на мобільних пристроях. Слід підкреслити, що веб-браузер не є таким додатком.

Протокол розділяється на три практично незалежні компоненти:

– Компонент високого рівня (мова запитів API): визначає метод, за допомогою якого запити та відповіді API перетворюються у двійкові повідомлення.

– Криптографічний (авторизаційний) рівень: визначає метод, за допомогою якого повідомлення шифруються перед передачею через транспортний протокол.

– Транспортний компонент: визначає спосіб передачі клієнтом та сервером повідомлень через деякі інші існуючі мережеві протоколи (наприклад, HTTP, HTTPS, WS (звичайні веб-сокети), WSS(веб-сокети черезHTTPS),TCP,UDP) [4].

Протокол MTProto використовує два шари шифрування – «сервер-сервер» і «клієнт-сервер». Він працює на основі таких алгоритмів:

– AES - симетричний 256-бітний алгоритм, прийнятий урядом США як стандарт.

– RSA - криптографічний алгоритм, в основі якого лежить обчислювальна складність завдання факторизації великих цілих чисел.

– Метод Діффі-Хеллмана - дозволяє отримати двом і більш учасникам секретний ключ по незахищеному від прослуховування, однак захищеному від підміни, каналу зв'язку.

– SHA-1, MD5 - хеш-алгоритми, використовувані в багатьох криптографічних протоколах і додатках для безпечного хешуваня. На відміну від протоколу Double Ratchet, який застосовується WhatsApp і вже встиг отримати схвалення відомих фахівців в області захисту інформації, розробники MTProto не поспішають надавати свій продукт для незалежного аудиту. З одного боку, це робить алгоритм потенційно вразливим для атак, з іншого - на сьогоднішній день не зафіксовано жодної успішної дії, що призвів до розшифрування повідомлень. Розробники месенджера заявляють про гарантії безпеки відповідно до передачі зашифрованих даних [2].

До 2014 року протокол MTProto використовував модифіковану версію схеми обміну ключами за методом Діффі-Хеллмана. Замість генерації ключів за допомогою стандартного протоколу на базі алгоритму Діффі-Хеллмана, сервер відсилав користувачеві ключ, оброблений операцією XOR разом з довільним числом (nonce). Цей факт дозволяє фальшивому серверу використовувати різні nonce-змінні для двох користувачів, у результаті чого буде один і той же ключ, але який буде відомий серверу.

У деяких частинах протоколу при хешуванні замість SHA-256 використовується алгоритм SHA-1, який, як відомо, нестійкий до колізій. Творці Telegram стверджують, що SHA-1 використовується в тих частинах протоколу, де стійкість до колізій не принципова, проте все ж сильніша хеш-функція була б доречніше. Історія не раз доводила, що проломи і невраховані моменти - досить поширене явище [3].

Навіть при використанні секретного чату, мобільна версія Telegram дозволяє третій стороні переглядати інформацію про метаданих. Наприклад, зловмисник може дізнатися, коли користувачі виходять в онлайн і йдуть в оффлайн аж до секунд. Telegram не вимагає угоди від обох сторін для встановлення комунікації, і зловмисник може підключитися і отримати інформацію о метаданих без відома користувача. Крім того, у зловмисника є хороший шанс виявити, чи спілкуються два користувача між собою за допомогою підключення і аналізу метаданих на обох кінцях дроту. Ми назвали цю проблему «витік доступності» [3].

Навіть якщо прийняти як аксіому, що MTProto дійсно має кращі параметри захисту серед сучасних месенджерів, зловмисники все ж мають можливість зламати акаунт користувача. При цьому сам протокол тут абсолютно ні до чого.

У публікації номер два розробники розказують що уразливість полягає в способі авторизації користувача. Для даної процедури використовується реальний номер телефону, на який відправляється СМС-код для підтвердження входу в аккаунт. В основі подібного методу передачі даних лежить технологія SS7 (Signaling System # 7), яка розроблялася 40 років тому і має слабкі параметри безпеки

за сучасними мірками. Теоретично зловмисники можуть перехопити СМС з кодом і зламати акаунт. А оскільки в звичайному режимі Telegram зберігає всі повідомлення на своїх серверах, хакери можуть отримати доступ до всієї листуванні конкретного користувача.

Проблему вирішує спілкування в секретних чатах. В цьому випадку прочитати переписку можна тільки за допомогою реальної крадіжки телефону, так як повідомлення не зберігаються на сервері, а передаються виключно між двома пристроями [2].

ВИСНОВОК

У цьому проекті досліджено месенджер Telegram. За своїм власним спостереженням Telegram має серйозні, і в той же час прості, проблеми в протоколі захисту (наприклад, модифікований і вразливий алгоритм обміну ключами за методом Діффі-Хеллмана).

З усього вищесказаного можна зробити висновок, що Telegram, як і всі інші продукти, має уразливості, про які користувачі повинні знати. Також будь яка система захисту не є ідеальною. Але для цього і треба вивчати їхні проблеми, аналізувати їх, що уникнути взламу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. TELEGRAM. ЧТО ЭТО ТАКОЕ И ПОЧЕМУ ЭТО КРУТО [Електронний ресурс] – Режим доступу до ресурсу: https://keddr.com/2014/11/telegram-chto-eto-takoe-i-pochemu-eto-kruto/.
2. Как осуществляется шифрование Телеграмм и в чем его отличие от других мессенджеров [Електронний ресурс] – Режим доступу до ресурсу: https://ru.telegram-store.com/blog/shifrovanie-telegramm.
3. Анализ безопасности Telegram [Електронний ресурс] – Режим доступу до ресурсу: https://www.securitylab.ru/analytics/490726.php.
4. MTProto Mobile Protocol [Електронний ресурс] – Режим доступу до ресурсу: https://core.telegram.org/mtproto.

Савчук Дар'я Олександрівна - студентка групи КІТС-19б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, Вінниця, e-mail dasha.savchuk.2001@gmail.com

Savchuk Darya Oleksandrivna - student of KITS-19b group, Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia, e-mail dasha.savchuk.2001@gmail.com

Науковий керівник: ***Шелепало Галина Василівна*** – кандидат фізико-математичних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, e-mail hv.shelepalo@vntu.edu.ua

Supervisor: ***Shelepalo Halyna Vasylivna*** - Candidate of Physical and Mathematical Sciences, Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, e-mail hv.shelepalo@vntu.edu.ua