УДК 004.056.55

Ю.В. Баришев[1]
Д.А. Сокол[2]

ЗАСІБ ЗАХИЩЕНОГО АУДІО ТА ВІДЕО ЗВ'ЯЗКУ

Вінницький національний технічний університет

Анотація. *У даній роботі проаналізовано різні реалізації програмних засобів захищеного аудіо та відео зв'язку для операційних систем Android та iOS. Запропоновано та розроблено власний варіант засобу для встановлення захищеного аудіо та відео зв'язку. Користувацький інтерфейс реалізований мовою програмування Dart з використанням фреймворку Flutter, криптографічний протокол з використанням бібліотеки pointycastle для використання геш-функції SHA3-256, а автентифікація користувачів за допомоги JWT-токенів.*

Ключові слова: *захищений аудіо та відео зв'язок, методи автентифікації, алгоритми захисту даних, Dart.*

Abstract. *This paper analyzes various software implementations of secure audio and video communication for Android and iOS operating systems. We proposed and developed our own version of the tool for establishing secure audio and video communication. The user interface is implemented in the Dart programming language using the Flutter framework, a cryptographic protocol using the pointycastle library to use the SHA3-256 hash function, and user authentication using JWT-tokens.*

Keywords: *secure audio and video communication, authentication methods, data protection algorithms, Dart.*

Вступ

В двадцять першому столітті, через різноманітні перепони та загрози більшість людей змінила звичний формат живого спілкування на використання засобів інтернет-телефонії, ці засоби щоденно використовуються великою кількістю людей по всьому світу, оскільки вони мають набагато ширший ряд функціоналу, в порівнянні зі звичайним зв'язком шляхом телефонії тим більше з форматом живого спілкування, якому перешкоджають певні сучасні проблеми. За значним поширенням та розвитком, даних засобів, з'явились і проблеми забезпечення безпеки конфіденційних даних, що циркулюють в таких засобах.

Популярні, засоби інтернет-телефонії належним чином не достатньо піклуються про забезпечення конфіденційності даних, як на етапах автентифікації, так і при наступному їх зберіганні та передаванні. Це можна пояснити нагальною потребою в таких засобах і поспіхом розробників вийти на ринок з продуктом якомога раніше. Відповідно питання безпеки не було в їх фокусі в гонитві за першістю в заповненні ринку, який неочікувано стрімко виріс через пандемію, тому питання кібербезпеки розглядались як другорядні [1]. Також варто відзначити, неодноразові докази того, що компанії збирають через такі засоби велику кількість конфіденційних даних, від номерів телефонів до біометричних особливостей користувача, таких як відбитки пальців, і всі ці дані збираються через використання сумнівних методів автентифікації. Саме тому актуально розробити засіб, який би не використовував конфіденційні дані користувачів такі як біометрію та номери телефону під час автентифікації користувачів.

Метою даної роботи є покращення методів забезпечення конфіденційності інформації в програмних засобах для встановлення захищеного аудіо та відео зв'язку, шляхом розробки засобу, що зменшує вірогідність витоку даних через вищевказану проблему, через використання власних ідентифікаторів. Завдяки даному рішенню, не потрібно передавати в відкритому вигляді чи взагалі використовувати конфіденційні дані як номер телефону та біометрію.

Результати дослідження

У сучасному світі існує чимало розроблених та реалізованих аналогів програмного засобу захищеного аудіо та відео зв'язку. Відомі рішення можна розглянути в залежності від методів захисту, методів автентифікації, технологій, що в них використовуються та реалізації аудіо та відео зв'язку. Для аналізу відомих реалізацій було прийнято рішення розглянути декілька популярних варіантів із таким набором функціональних можливостей: створення захищеного з'єднання між користувачами із можливістю передачі відео потоку та аудіо потоку даних.

Поміж цих засобів попри однакові функціональні можливості використовуються різні методи автентифікації та підходи до захисту даних. Для початку розглянемо певно найрозповсюджений програмний засіб захищеного аудіо та відео зв'язку під назвою WhatsApp від компанії Meta [2].Даний програмний засіб є найстаршим серед приведених нижче аналогів, що обумовило його високу популярність попри те що він має доволі стандартний набір функціональних можливостей. Цей засіб дозволяє: надсилати текстові, відео, аудіо повідомлення, встановлювати аудіо та відео зв'язок, створювати групові чати та канали. WhatsApp використовує наскрізне шифрування для всіх розмов, що захищає повідомлення від перехоплення третіми сторонами під час передачі. WhatsApp забезпечує двоетапну перевірку для додаткової безпеки. З квітня 2016 з виходом оновлення версії 2.16.12 WhatsApp включив наскрізне шифрування (end-to-end) для всіх користувачів на базі розробок протоколу Signal [3]. Цей протокол використовує комбінацію протоколу узгодження ключів X3DH [6], алгоритму Double Ratchet [7] для безпечного керування ключами та 256-бітного симетричного шифрування AES разом із обміном ключами за протоколом Діффі-Геллмана на основі еліптичних кривих (ECDH) [8] для шифрування повідомлень. Шифрування поширюється на всі типи повідомлень: текст, фото, відео та голосові повідомлення. Шифрування також доступне у групових чатах.

Основні види автентифікації, які використовуються в WhatsApp, включають:

– Геш-код - після реєстрації WhatsApp генерує геш-код на основі номера телефону користувача та інших даних. Цей геш-код використовується для автентифікації користувача при кожному вході в застосунок. Геш-код зберігається на пристрої користувача та використовується для перевірки його ідентичності.

– Номер телефону - WhatsApp прив'язаний до номера мобільного телефону користувача. При реєстрації в WhatsApp користувач повинен підтвердити свій номер телефону шляхом отримання SMS-повідомлення або використання автоматичного дзвінка з унікальним кодом підтвердження. Це дозволяє підтвердити, що користувач має доступ до вказаного номера телефону.

– QR-код - WhatsApp також підтримує автентифікацію за допомогою QR-кодів. Користувач може сканувати QR-код на пристрої, що вже автентифікований в WhatsApp, для з'єднання свого облікового запису з цим пристроєм. Це забезпечує зручність та швидкість процесу автентифікації.

– Біометричні дані - WhatsApp підтримує використання біометричних даних, таких як сканування відбитка пальця або розпізнавання обличчя, для автентифікації та розблокування доступу до програми. Це додатковий рівень безпеки, який забезпечує, що лише власник пристрою має доступ до облікового запису WhatsApp.

– Використання декількох факторів автентифікації - WhatsApp підтримує можливість використання двофакторної автентифікації (2FA). Користувачі можуть налаштувати додатковий пароль або PIN-код, який потрібно буде ввести під час першого входу на новий пристрій або після тривалої неактивності. Це додає додатковий шар захисту для облікового запису користувача. До недоліків можна віднести те, що WhatsApp - підтримує політику обміну даними з материнською компанією Facebook, що може призвести до використання даних користувачів для цільової реклами та інших цілей. Також WhatsApp не має традиційної функції «вийти», що означає, що користувачі завжди перебувають в обліковому записі застосунку, що ускладнює певним чином користування.

Наступним варіантом аналогу для аналізу можна розглянути програмний засіб Skype від компанії розробника Microsoft[4]. Skype використовує протокол, що передбачає шифрування трафіку, TLS (Transport Layer Security)[9] для захисту приватності та конфіденційності даних, переданих під час розмови. TLS забезпечує криптографічний захист шляхом шифрування даних, що передаються між клієнтами Skype і серверами компанії Microsoft[4]. Це допомагає унеможливити прослуховування та підслуховування комунікації третіми особами, також використовується 256-розрядний AES над 128-розрядними блоками, який. Skype використовує алгоритми гешування, наприклад, SHA-256 (Secure Hash Algorithm 256-bit), для створення гешів інформації, таких як паролі або контрольні суми. Гешування допомагає забезпечити цілісність та перевірку даних під час передачі.

Щодо автентифікації, Skype використовує різні методи автентифікації для перевірки та підтвердження ідентичності користувачів. Основними видами автентифікації, що використовуються в Skype, є такі [4]:

– Парольна - користувачі мають створювати облікові записи з унікальними ідентифікаторами (ім'я користувача або електронна пошта) та паролями. Цей метод є найпоширенішим і забезпечує перевірку ідентичності на основі збігу введених та еталонних логіну та пароля.

– Багатофакторна автентифікація - Skype підтримує функцію двоетапної перевірки (2FA). Це дозволяє користувачам налаштувати додатковий шар безпеки, запитуючи додатковий код підтвердження після введення основного пароля. Код може бути надісланий через SMS або генеруватися додатком автентифікації.

– Прив’язка до облікового запису Microsoft - Skype пов'язаний з обліковим записом Microsoft, що дозволяє використовувати його як фактора автентифікації. Це може включати використання Windows Hello або інших біометричних методів, таких як відбиток пальця або розпізнавання обличчя.

– Біометрична - також підтримується використання відбитка пальця або розпізнавання обличчя для автентифікації користувача.

Ще одним аналогом є Signal від розробника Signal Foundation [3]. Даний аналог має такі самі функціональні можливості, як і два попередніх, однак, саме даний програмний засіб найбільше зосередився на конфіденційності даних користувача, а саме: сигнал не зберігає ніяких даних про користувача, лише час останнього візиту у форматі UNIX-часу та час створення аккаунту користувача, також у форматі UNIX-часу. На відміну від раніше переглянутих аналогів, Signal розроблений таким чином, щоб не зберігати ніякої інформації користувача на серверах, це реалізовано за допомогою того, що використовується наскрізне шифрування не тільки для повідомлень і даних що надсилаються, але і до всіх інших даних користувача, таких як: контакти, соціальний граф, групові дані, інформація про стан груп, ім’я профілю, аватар профілю, данні про місцеположення, історію пошуку та інше.

Методи автентифікації, що використовуються в Signal:

– Номер телефону - Signal використовує номер телефону користувача як основний ідентифікатор. При реєстрації в Signal, користувач повинен підтвердити свій номер телефону, а також створити і підтвердити код реєстрації, що надсилається через SMS.

– Багатофакторна автентифікація - Signal підтримує можливість включення двофакторної автентифікації для додаткового рівня безпеки. При цьому користувач повинен налаштувати додатковий пароль, який буде використовуватися під час входу в додаток або відновлення облікового запису.

– Сертифікація ключів - Signal дозволяє користувачам перевіряти “відбиток” ключа для підтвердження ідентичності особи під час обміну повідомленнями.

В результаті проведення попереднього аналізу засобів інтернет-телефонії, далі було порівняно та проаналізовано вищевказані засоби інтернет-телефонії, в рамках таблиці 1.1 за такими характеристикам: підтримка апаратних засобів, мультиплатформеність (Операційні Системи), шифрування, анонімність, збереження даних, інтеграція з іншими сервісами. Окремо було наведено порівняння використовуваних методів автентифікації в таблиці 1.2.

Таблиця 1.1 – Порівняльний аналіз проаналізованих засобів

Характеристика	Signal	WhatsApp	Skype
Підтримка апаратних засобів	Немає	Немає	Фізичний ключ YubiKey
Мультиплатформеність(Операційні Системи)	iOS, Android, Microsoft Windows, Linux, macOS	Android, iOS, Microsoft Windows macOS, S40, Tizen, KaiOS	Microsoft Windows, macOS, Android, iOS, Symbian OS, Windows Phone, Linux, BlackBerry OS, webOS
Шифрування	Шифрування на стороні користувача, застосовується E2E шифрування	Шифрування на стороні користувача, застосовується E2E шифрування	Шифрування на стороні користувача але E2E шифрування не застосовується для всіх типів повідомлень
Анонімність	Анонімний	Не анонімний, потрібен номер телефону	Не анонімний, потрібен, обліковий запис Microsoft
Збереження даних	Зберігаються на серверах, після доставки повідомлення вони видаляються з сервера, не зберігає метадані	Зберігаються на серверах, можливе видалення повідомлень з обох сторін	Зберігаються на серверах, можливе видалення повідомлень з обох сторін
Інтеграція з іншими сервісами	Обмін файлами, можливість інтеграції з деякими сервісами	Обмін файлами інтеграція з різними сервісами, такими як iCloud	Обмін файлами, інтеграція з різними сервісами, такими як OneDrive

Таблиця 1.2 – Порівняльний аналіз використання методів автентифікації в засобах

Методи автентифікації	Signal	WhatsApp	Skype
Парольна	+	+	+
2FA	+	+	+
Біометрична	-	+	+
Одноразові паролі(OTP)	+	+	+
OpenID Connect	-	-	+

Після проведеного аналізу відомих програмних засобів для захищеного аудіо та відео зв’язку, можна навести певні недоліки кожного з них:

Skype:

Відмінна якість зв'язку: У деяких випадках якість зв'язку у Skype може бути нестабільною, залежно від якості Інтернет-з'єднання, швидкості Інтернету та загальної мережевої пропускної здатності. Це може призвести до проблем з аудіо та відео під час розмови.

Висока споживання ресурсів: Skype відомий своєю високою споживанням ресурсів комп'ютера або мобільного пристрою. Він може використовувати значну кількість оперативної пам'яті та процесорного часу, що може призвести до зниження продуктивності системи.

Відсутність приватності: Skype був звинувачений у збереженні та передачі користувальницьких даних третім сторонам, включаючи правоохоронні органи та розвідувальні агентства. Це підкопує приватність користувачів та може викликати побоювання щодо конфіденційності особистих даних.

Відсутність функціональності безкоштовного виклику на мобільні телефони: Хоча Skype надає можливість безкоштовних викликів між користувачами Skype, він вимагає платних планів абонентського обслуговування для здійснення викликів на мобільні телефони та стаціонарні телефони.

Відсутність енд-ту-енд шифрування: За замовчуванням Skype використовує шифрування даних, але воно не забезпечує енд-ту-енд шифрування для всіх видів комунікації. Це означає, що компанія може мати доступ до розмов, повідомлень та файлів, що зберігаються на серверах Skype.

Обмежені можливості конференц-зв'язку: Skype має обмежені можливості для багатокористувацьких конференц-викликів. Безплатна версія Skype дозволяє проводити конференц-виклики до 50 учасників, але для більшої кількості учасників потрібно придбати платний план.

Signal:

Обмежені функції: Signal не має стільки функцій налаштувань, як інші застосунки, такі як WhatsApp, також він не має функції групового дзвінка.

Покладення на номер телефону: Signal вимагає від користувачів реєструватися за допомогою свого номера телефону, що деяким людям може бути незручно.

Централізація: хоч Signal і більше зосереджений на конфіденційності, ніж інші застосунки захищеного аудіо та відео зв’язку, він покладається на централізовані сервери, які потенційно можуть бути зламані, скомпрометовані.

WhatsApp:

Обмін даними: WhatsApp підтримує політику обміну даними з материнською компанією Facebook, що може призвести до використання даних користувачів для цільової реклами та інших цілей.

Неможливість вийти: WhatsApp не має традиційної функції «вийти», що означає, що користувачі завжди входять у програму, якщо вони не видалять її або не перейдуть на інший номер телефону.

Загальною ж проблемою застосунків є:

Залежність від номера телефону: WhatsApp, Telegram та Signal вимагає від користувачів реєстрації за номером телефону, проблема полягає в тому, що при втраті телефону користувач втрачає абсолютно всі дані та аккаунт як такий(за умови, що аккаунт не поширено на інші пристрої).

Реалізація програмного засобу має такі функціональні можливості: двофакторна автентифікація клієнта перед сервером за допомогою JWT-token[5] та двостороння автентифікація за допомогою

криптографічного протоколу, створення захищеного зв’язку між двома користувачами із підтримкою аудіо та відео зв’язку, створення окремої кімнати для проведення мітингів для багатьох учасників.

Основною перевагою розробленого засобу є те, що прив’язка до номеру телефону відсутня, реалізована прив’язка до певного ID, який буде назначатись кожному користувачу окремо та індивідуально, також, використання власного криптографічного протоколу автентифікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Cohen R. A random woman joined the wrong Zoom meeting while it was live on The BBC. Insider. URL: https://www.insider.com/woman-joined-wrong-zoom-meeting-live-on-bbc-news-2022-6 (accessed: 14.06.2023).
2. WhatsApp. WhatsApp.com. URL: https://www.whatsapp.com/?lang=en (accessed: 14.06.2023).
3. Documentation. Signal Messenger. URL: https://www.signal.org/docs/ (accessed: 14.06.2023).
4. Skype | Stay connected with free video calls worldwide. Skype | Stay connected with free video calls worldwide. URL: https://www.skype.com/en/ (accessed: 15.06.2023).
5. JWT.IO - JSON Web Tokens Introduction. JSON Web Tokens - jwt.io. URL: https://jwt.io/introduction#:~:text=What%20is%20JSON%20Web%20Token,because%20it%20is%20digitally%20signed (accessed: 14.06.2023).
6. Specifications >> The X3DH Key Agreement Protocol. Signal Messenger. URL: https://signal.org/docs/specifications/x3dh/ (accessed: 15.06.2023).
7. Specifications >> The Double Ratchet Algorithm. Signal Messenger. URL: https://signal.org/docs/specifications/doubleratchet/ (accessed: 15.06.2023).
8. Specifications >> The XEdDSA and VXEdDSA Signature Schemes. Signal Messenger. URL: https://signal.org/docs/specifications/xeddsa/ (accessed: 15.06.2023).
9. Introduction to WebRTC protocols - Web APIs | MDN. MDN Web Docs. URL: https://developer.mozilla.org/en-US/docs/Web/API/WebRTC_API/Protocols (accessed: 15.06.2023).

Баришев Юрій Володимирович — : к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, Україна.

Baryshev Yuryi Volodymyrovych —: Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Сокол Дмитро Анатолійович— студент групи 1БС-19Б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: dimafolkman@gmial.com.

Dmytro Anatoliyovych Sokol — student of group 1BS-19B, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: dimafolkman@gmial.com