НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
"КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО"
НАВЧАЛЬНО-НАУКОВИЙ ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Проектування і розробка криптографічних систем

Лабораторна робота №4

Дослідження систем захисту захищених месенжерів типу Skype, Viber, WhatsApp, Signal

Виконали:
Молдован Дмитро ФІ-42мн
Сковрон Роман ФІ-42мн
Волинець Сергій ФІ-42мн

Київ – 2025

1 Мета роботи

Дослідження особливостей реалізації криптографічних механізмів протоколів захисту мультимедійної інформації типу SIP.

2 Постановка задачі

Проаналізувати існуючу інформацію про системи Viber, WhatsApp, Skype, Telegram та їх криптографічні механізми. Детально розібрати опис усіх механізмів протоколу, структуру пакетів та характеристики систем. Довести теоретично можливість існування в системі виявлених протоколів та зробити огляд відомих аналізів захищеності вказаних протоколів, включаючи вже виправлені помилки. Зробити порівняльний аналіз можливостей вказаних систем, їх криптографічних механізмів та рівня захищеності (обґрунтований). Дати рекомендації користувачам щодо безпечного використання таких систем. Всю зібрану інформацію оформити у вигляді детального звіту з власним аналізом рівня захищеності та обраних криптографічних механізмів.

3 Теоретичний аналіз та опис дослідження

3.1 Viber

Viber – це популярний крос-платформний месенджер компанії Rakuten, який використовують понад мільярд людей. Він поєднує функції голосових і відеодзвінків, обміну повідомленнями, групових чатів, стікерів, каналів і секретних чатів. Під час пандемії сервіс навіть використовували вчителі для комунікації з учнями, що підкреслило його поширеність і зручність.

У 2016 році Viber увімкнув наскрізне шифрування за замовчуванням, але воно працює не для всіх типів розмов. E2E застосовується до приватних чатів, приватних дзвінків і груп, проте не діє в спільнотах, каналах, чатах із ботами, групових дзвінках і сервісі Viber Out. Кожен пристрій генерує власну пару ключів Curve25519 (ID Key), а також PreKey для ініціації сесії. Коли один користувач хоче почати чат із іншим, він отримує з сервера його ID Key та PreKey, генерує додаткові ключі для рукостискання. Після цього він надсилає повідомлення про початок сесії. Інший пристрій може відтворити ті самі ключі через ту саму процедуру Диффі-Геллмана.

$$\text{RootKey} = \text{SHA256}(\text{DH}(\text{ID}_{\text{Allice}}, \text{HS}_{\text{Bob}})||\text{DH}(\text{HS}_{\text{Allice}}, \text{ID}_{\text{Bob}})||\text{DH}(\text{HS}_{\text{Allice}}, \text{HS}_{\text{Bob}}))$$
$$\text{TempKey} = \text{HMAC\_SHA256}(\text{RootKey}, \text{DH}(\text{Ratchet}_{\text{Alice}}, \text{Ratchet}_{\text{Bob}}))$$
$$\text{NewRootKey} = \text{HMAC\_SHA256}(\text{TempKey}, \text{"root"})$$
$$\text{SessionKey} = \text{HMAC\_SHA256}(\text{TempKey}, \text{"mesg"})$$

Повідомлення у Viber шифруються за допомогою одноразового симетричного 128-бітного ключа, який використовується разом із алгоритмом Salsa20. Сам одноразовий ключ потім шифрується сеансовим ключем кожного отримувача. Сервер лише розподіляє зашифровані частини повідомлення, не маючи доступу до його змісту. Основу безпеки складає подвійний храповий механізм (Double Ratchet), який забезпечує пряму та зворотну секретність: навіть у разі компрометації одного ключа минулі та майбутні повідомлення залишаються захищеними. Окрім цього, ланцюжок ключів прив'язаний до початкових ID Key, що забезпечує автентичність пристроїв.

Viber є надзвичайно популярним в Україні – приблизно дев'ять мільйонів користувачів. Хоча месенджер загалом вважається надійним і підтримує Україну, Сили оборони не користуються ним через підвищені вимоги до безпеки. Крім того, були гучні випадки витоків даних, зокрема масивний злам на сотні гігабайтів. Документація сервісу подає загальну структуру протоколів, але не дає достатньо глибоких технічних деталей, що ускладнює повноцінну оцінку безпеки.

3.2 WatsApp

WhatsApp – це популярний месенджер від Meta, який дозволяє обмінюватися текстовими, голосовими та відеоповідомленнями, здійснювати дзвінки, а також надсилати фото, документи й геолокацію. Реєстрація відбувається за номером телефону. Окрім основної версії, існує WhatsApp Business – окремий застосунок, створений для компаній та підприємців, що дає розширені можливості взаємодії з клієнтами.

Сервіс заснували Ян Кум і Браян Ектон, які понад двадцять років працювали в Yahoo. У 2014 році WhatsApp став частиною Facebook, але продовжує функціонувати як окремий продукт.

Щодо безпеки, WhatsApp використовує протоколи Signal – одні з найнадійніших на сьогодні, що пройшли аналіз багатьох дослідників. Повноцінне наскрізне шифрування було впроваджено у 2016 році. Месенджер має окремі схеми роботи для звичайних користувачів і бізнесів: у першому випадку трафік проходить через сервери WhatsApp, а у випадку WhatsApp Business організації можуть використовувати власний локальний API-сервер. Канал між бізнесом і WhatsApp у такому сценарії також вважається наскрізно зашифрованим.

Як було сказано раніше, WhatsApp використовує Signal Protocol, який поєднує два основні механізми: X3DH для встановлення початкового захищеного каналу та Double Ratchet для постійного оновлення ключів під час переписки. Коли користувачі вперше починають спілкування, їхні пристрої обмінюються відкритими ключами через сервер, але таким чином, що реальний секрет формують лише самі пристрої. Завдяки кільком обмінам Diffie–Hellman кожна сторона незалежно отримує однаковий спільний ключ, до якого не має доступу ні сервер, ні будь-хто інший. Після цього початкового встановлення сеансу включається Double Ratchet – механізм, який автоматично змінює ключі при кожному отриманому або надісланому повідомленні. Він оновлює їх як через симетричні перерахунки, так і через періодичну заміну Diffie–Hellman компонентів, тому кожне повідомлення має свій унікальний ключ. Навіть у випадку перехоплення одного з них зловмисник не зможе відновити ні попередні, ні наступні повідомлення.

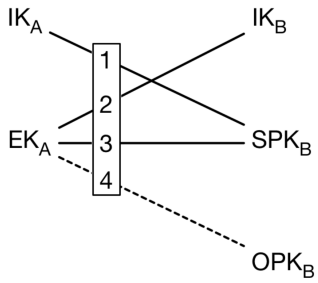

Рис. 1: X3DH Schema

У реалізації протоколу використовуються сучасні криптографічні алгоритми, серед яких Curve25519 для обміну ключами, AES-256 для шифрування та HMAC-SHA256 для

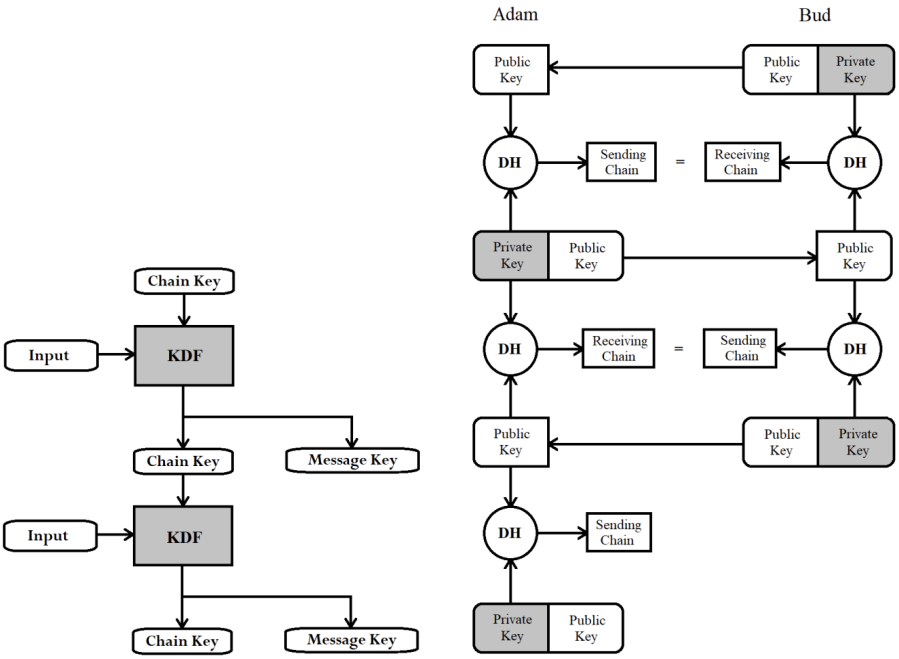

Рис. 2: Symetric and Diffie-Hellman Ratchet

контролю цілісності. Це забезпечує високий рівень захисту змісту листування, хоча WhatsApp усе ще збирає метадані, такі як інформацію про те, хто, коли і з ким спілкується. Цей рівень даних залишається вразливим, оскільки структура WhatsApp не дозволяє повністю приховати такі взаємодії, хоча самі повідомлення залишаються недоступними навіть для компанії.

Існує багато досліджень безпеки протоколів WhatsApp: від аналізу використаних алгоритмів і порівняння з іншими месенджерами до вивчення слабких місць у реєстрації пристроїв чи резервному копіюванні.

У підсумку WhatsApp є досить надійним месенджером як для особистого, так і для бізнес-спілкування. При цьому ватро звернути увагу на те, що Meta збирає метадані, такі як номери телефонів та контакти, метадані повідомлень (зміст шифрований, але час відправки, частота та інше відкриті), технічні данні пристрою, тощо.

3.3 Skype

Skype – це один із найстаріших і найвідоміших сервісів для онлайн-спілкування, який дозволяє здійснювати голосові та відео дзвінки, обмінюватися текстовими повідомленнями, надсилати файли та організовувати групові конференції. Спочатку Skype став популярним завдяки можливості дешево дзвонити на мобільні й стаціонарні телефони по всьому світу.

Сервіс створили Ніклас Зеннстрьом та Янус Фріс у 2003 році, а згодом у 2011 році Skype придбала компанія Microsoft. Після цього він був інтегрований у глобальну екосистему Microsoft і став частиною її бізнес-рішень.

У частині безпеки Skype використовує власні криптографічні механізми для шифрування дзвінків і повідомлень. Хоча сервіс шифрує трафік між клієнтом і сервером, тривалий час йому закидали відсутність повноцінного наскрізного шифрування, на відміну від сучасних месенджерів. У відповідь Microsoft поступово додала “Приватні розмови” – режим, що використовує протокол Signal, але він доступний не для всіх функцій і не є стандартним

за замовчуванням.

Архітектура Skype історично побудована на серверно-клієнтській моделі, де частина трафіку проходить через інфраструктуру Microsoft. Це забезпечує стабільність дзвінків і масштабованість, але водночас означає певну залежність від серверів компанії.

Попри це, існує багато досліджень, які підтверджують захищеність основних механізмів Skype: шифрування трафіку, захист від перехоплення дзвінків та певний рівень конфіденційності. Однак у порівнянні з сучасними месенджерами, орієнтованими на повне E2E-шифрування, Skype зазвичай розглядають як менш приватний, але стабільний та надійний інструмент для бізнесу й особистих дзвінків.

У підсумку Skype залишається функціональним і перевіреним сервісом для спілкування, особливо популярним у корпоративному середовищі. Основний недолік – менший рівень приватності порівняно з месенджерами, які використовують наскрізне шифрування за замовчуванням.

3.4 Telegram

Telegram позиціонує себе як швидкий, хмарний та кросплатформений месенджер, орієнтований на масштабування: канали з необмеженою кількістю підписників, великі групи до двохсот тисяч учасників, можливість синхронізації між усіма власними пристроями та зберігання повідомлень у хмарі. Саме завдяки хмарній архітектурі Telegram отримав значну популярність, адже користувач може миттєво відновити історію листування на будь-якому пристрої. Водночас саме така архітектура пояснює, чому месенджер не використовує наскрізне шифрування за замовчуванням: повідомлення хмарних чатів зберігаються на серверах компанії й можуть бути теоретично доступні для аналізу або відновлення.

Telegram має два принципово різні типи приватних чатів: звичайні чати та секретні чати, які не синхронізуються між пристроями і використовують повноцінне наскрізне шифрування. Окремо реалізовані приватні аудіо- та відеодзвінки, що будуються на тих самих криптографічних принципах, що й секретні чати, але з додатковою взаємною автентифікацією у момент встановлення з'єднання.

Першою технологічною основою месенджера був протокол MTProto v1, який компанія розробила самостійно. Ідея Telegram полягала в поєднанні мобільної ефективності і криптографічної гнучкості, однак саме через "власноручність" реалізації цей протокол зазнав критики. Дослідники продемонстрували, що MTProto v1 не забезпечує доказової стійкості щодо певних типів атак, зокрема IND-CCA, а структура побудови повідомлень давала можливість виконувати окремі маніпуляції з трафіком без розкриття ключів. Telegram з часом визнав недоліки першої версії й повністю відмовився від неї, перейшовши на MTProto 2.0.

Сучасний протокол MTProto v2 складається з кількох окремих механізмів: початкової автентифікації, встановлення довгострокового авторизаційного ключа між клієнтом і сервером, створення короткоживучих ключів сеансів, криптографічного захисту звичних хмарних чатів та встановлення спільного сеансового секрету для секретних чатів. Архітектурно протокол поділяється на прикладний рівень, рівень авторизації й криптографії та транспортний рівень. На початковому етапі клієнт і сервер виконують модифікований обмін Діффі-Геллмана для формування довготривалого ключа авторизації, що зберігається лише локально та використовується для шифрування всіх подальших взаємодій із сервером. Для секретних чатів клієнти додатково проводять між собою обмін ключами через сервер, але сервер не отримує значення спільного секрету. Саме цей ключ і забезпечує наскрізне шифрування.

На відміну від першої версії протоколу, MTProto v2 має формальний аналіз безпеки,

включаючи перевірку таких властивостей, як автентичність, цілісність, ідеальна пряма секретність і правильність механізмів повторної ротації ключів. Ця формалізація зменшила кількість зауважень щодо криптографічної строгості протоколу, хоча критика підходу "власного криптографічного дизайну" з боку спільноти залишається актуальною.

Хмарна архітектура Telegram безпосередньо впливає на питання приватності. Повідомлення звичайних чатів зберігаються на серверах у зашифрованому (але не наскрізно шифрованому) вигляді, що дозволяє Telegram здійснювати автоматизований аналіз на спам, боротьбу з шахрайством або виконувати юридично обґрунтовані запити державних структур. Метадані, такі як IP-адреси, інформація про пристрої, історія зміни імен користувачів, також можуть зберігатися до року згідно з політикою конфіденційності. Це забезпечує функціональність синхронізації, але створює криптографічно неминучу асиметрію між секретними та стандартними чатами.

Для аудіо- й відеодзвінків Telegram повторно використовує криптографічні елементи MTProto 2.0. Трафік дзвінків шифрується симетричними ключами, одержаними з результатів дифі-геллманівського обміну, а передача здійснюється через оптимізовану мультимедійну транспортну систему Telegram.

4 Порівняння

За можливостями всі чотири платформи покривають базові сценарії: особисті та групові чати, голосові й відеодзвінки, обмін файлами. Telegram виділяється хмарною моделлю з широкими каналами і синхронізацією між пристроями, що робить його дуже зручним для масових трансляцій і роботи з історією, але це й визначає його архітектурні компроміси в приватності. Viber і WhatsApp позиціонують себе як універсальні месенджери з багатими мультимедійними функціями. Viber додає суспільні канали й деякі соціальні можливості, коли WhatsApp інтегрується з бізнес-сервісами. Skype є насамперед інструментом дзвінків і конференцій, використовується у корпоративному середовищі, і відрізняється великою інфраструктурною інтеграцією з Microsoft.

Криптографічно WhatsApp спирається на Signal Protocol (X3DH, Double Ratchet, сучасні примітиви Curve25519, AES-256, HMAC-SHA256 та HKDF), що дає йому високий рівень стійкості для контенту повідомлень. Viber застосовує подібну до Signal ідеологію: Curve25519, Double Ratchet і одноразові PreKeys, із шифруванням тіла повідомлення. Telegram використовує власний стек MTProto. у секретних чатах застосовується E2E на основі MTProto v2 з DH-обмінами і ефемерними ключами, тоді як хмарні чати шифруються клієнт–сервер і дозволяють зберігання на серверах Telegram. Skype у загальному режимі шифрує трафік, але наскрізне шифрування не є стандартом для всіх функцій. Microsoft додала режим "Приватні розмови" з використанням протоколів Signal для окремих випадків, але це не охоплює весь функціонал сервісу за замовчуванням.

Щодо практичної безпеки змісту повідомлень, найбільш сильними з криптографічної точки зору підходами є ті, що використовують перевірені, формально проаналізовані протоколи з мінімальною залежністю від серверної інфраструктури. WhatsApp забезпечує найвищий рівень конфіденційності в сенсі криптографічної стійкості. Viber технічно близький за моделлю захисту, але обмежена публічна документація та менша кількість незалежних аудитів роблять оцінку менш однозначною. Telegram у режимі секретних чатів має прийнятний криптографічний захист, але його хмарна модель для звичайних чатів створює принципову слабкість, адже сервер може теоретично отримати доступ до вмісту повідомлень. Skype як комплексний сервіс пропонує добрий практичний захист для дзвінків, але загалом поступається у приватності через відсутність E2E для всіх сценаріїв та має менш прозору реалізацію.

Важливі не лише алгоритми, а архітектура й політика: збір метаданих, хмарне зберігання і ступінь відкритості коду визначають реальний рівень приватності. WhatsApp і Viber, навіть при сильних E2E-алгоритмах для вмісту, зберігають метадані про контакти, час та частоту зв'язків. WhatsApp як частина Meta має додаткові ризики політики обробки даних. Telegram централізовано зберігає великі обсяги повідомлень у хмарі, що робить архітектуру зручною, але менш приватною без використання секретних чатів. Skype інтегровано в екосистему Microsoft, де корпоративні політики й інтеграції можуть вимагати доступу у певних випадках.

Для максимального захисту вмісту корисно використовувати месенджери з відкритими, формально перевіреними протоколами. Практично це означає віддавати перевагу Signal або, при неможливості, використовувати WhatsApp. Коли потрібно зручно синхронізувати історію між пристроями або працювати з великими каналами, Telegram дає функціональність – але слід уникати передачі дуже чутливої інформації в хмарні чати і користуватися секретними чатами для конфіденційних розмов. Для Viber корисно переконатися, що функції E2E увімкнені для необхідних типів діалогів, регулярно оновлювати додаток і відключати резервні копії в хмарі, якщо вони не шифруються локально. Skype можна використовувати для бізнес-дзвінків із розумінням, що повна наскрізна та мультифункціональна приватність може бути недоступна.

5 Висновки

У ході дослідження месенджерів Viber, Telegram, WhatsApp та Skype було встановлено, що кожний із них має різний рівень безпеки та власні підходи до шифрування. Найвищі гарантії конфіденційності забезпечують WhatsApp та Viber що використовують протоколи розроблені Signal. Вони використовують наскрізне шифрування за замовчуванням та сучасні криптографічні механізми. Telegram демонструє гібридний підхід. "Хмарні чати" покладаються на серверну інфраструктуру й не мають E2EE за замовчуванням, тоді як "секретні чати" забезпечують повну приватність, але використовуються не всіма користувачами. Skype що є більш орієнтованим на інфраструктуру Microsoft не надає рівня захисту, порівняного з сучасними месенджерами.

Загалом можна зробити висновок, що найбільш безпечними та орієнтованими на приватність залишаються месенджери з повним наскрізним шифруванням і відкритою криптографією, тоді як сервіси зі змішаним або частковим шифруванням залежать від довіри до центрального провайдера. Попри різницю в підходах, усі досліджувані платформи забезпечують прийнятний рівень захисту для повсякденного спілкування.