**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ**

**“КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО”**

**Фізико-технічний інститут**

**«Проектування, розробка і реалізація криптографічних систем»**

**Лабораторна робота №4**

**Тема: «Дослідження систем захисту захищених месенжерів типу Skype, Viber, WhatsApp, Signal».**

**Мета роботи: «Дослідження особливостей реалізації криптографічних механізмів протоколів захисту мультимедійної інформації типу SIP».**

**Виконав: студент групи ФІ-42мн**

**Сергеєв Станіслав**

**Хід роботи**

Група 1. 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.

**Аналіз**

Розпочну з опису криптографічних механізмів та їх особливостей для кожного месенджера по черзі.

1. *Viber*

Було проаналізовано, яку надає Viber відкрито у вигляді документації на своєму веб-сайті.

Для захищеної комунікації між двома зареєстрованими девайсами ***створюється сесія***, як тільки вона створилась, користувачі можуть обмінюватись безлімітною кількістю повідомлень в будь-якому напрямку.

Спочатку Аліса створює дві 256-бітні пари ключів еліптичної кривої Curve-25519, з допомогою них генеруються RootKey з використання алгоритму Діффі-Гелмана та SHA-256. RootKey, в свою чергу вже використовується для створення сесійного ключа з використання HMAC_SHA256.

Боб, отримавши від Аліси її ключі, за процедурою Діффі-Гелмана відновлює сесійний ключ, таким чином роблячи його спільним.

***Обмін повідомленнями.*** Надіслані повідомлення зашифровуються ARX-шифром Salsa20. Сесійні ключі також оновлюються кожного разу при зміні напрямку розмови з використанням алгоритму Діффі-Гелмана.

***Зашифровані дзвінки.*** Кожна сторона ефемерну 256-бітову ключову пару еліптичної кривої Curve-25519. Публічна частина підписується з використанням приватного ID-ключа девайсу і обмінюється між двома девайсами протягом фази налаштування дзвінка. Інша частина автентифікує запит, використовуючи публічний ID-ключ співрозмовника. Кожен девайс верифікує підпис та генерує одноразовий сесійний ключ (з допомогою Діффі-Гелмана). RTP потік аудіо чи аудіо/відео зашифровується алгоритмом Salsa20.

***Надсилання файлів, фото та відео.*** При надсиланні клієнт генерує ефемерний ключ Salsa20 та зашифровує файл. Зашифрований файл, разом з HMAC підписом завантажується на сервер Viber, де на зашифровані дані накладається додатковий MD5 підпис. Потім відправник надсилає отримувачу повідомлення з ID файлу та ключ зашифрування. Отримувач тепер має посилання на завантаження файлу з цього ID, завантажує файл та розшифровує його з отриманим ключем.

***Про рівень захищеності.*** Водночас, Viber містив деякі вразивлості, які були виявлені та описані (в 2019 році) на сайті NIST в розділі National Vulnerability Database, де зазначається, що не весь трафік, що проходив, до версії 11.7.0.5 шифрувався, певні пакети, а саме модель девайсу, ОС, IMSI та udid не зашифровувались, що дозволяло нападнику отримати доступ до

акаунту жертви. Втім, зараз ця вразливість вже виправлена. Шукаючи на сайті NIST по новим вразливостям, остання з них стосується десктопної версії Viber 25.6.0 – про вразливість до HTML-ін'єкційй через текстовий параметр інтерфейсу створення та пересилання повідомлень.

2. *WhatsApp*

WhatsApp має доволі детальну документацію "WhatsApp Encryption Overview", де описано всі криптографічні механізми та де вони використовуються.

Для захищеної комунікації між двома зареєстрованими девайсами ***створюється сесія.*** Для генерації спільного ключа також використовуються ефемерні ключі Curve-25519 та алгоритм Діффі-Гелмана на еліптичних кривих.

***Обмін повідомленнями.*** Повідомлення шифруються алгоритмом AES-256 в режимі CBC, а HMAC-SHA256 використовується для автентифікації.

***Надсилання файлів, фото та відео.*** Відправник шифрує файли також AES256 в режимі CBC, а потім додається MAC шифртексту з використанням HMAC-SHA256 та завантажує їх до "blob store". Отримувач завантажує звідти зашифрований blob, верифікує його геш SHA256 та дешифрує файли.

***Зашифровані дзвінки.*** Відео- та аудіо-дзвінки є "end-to-end" зашифрованими. Це стосується як дзвінків між двома абонентами, так і групових дзвінків. В першому випадку ключи генеруються один раз на весь дзвінок, в другому – кожен раз, коли хтось приєднується чи покидає дзвінок. Дзвінки шифруються з допомогою SRTP.

***Про рівень захищеності.*** З огляду на архітектуру безпеки я вважаю, що WhatsApp є доволі захищеним месенджером, який використовує сильні алгоритми шифрування даних. Документація викладена доволі детально описано, по ній можна покроково розібратись, що і як працює. На практиці вразливості все одно існують, останні з них стосуються проблем месенджера на iOS-пристроях, наприклад месенджер міг дозволити непов'язаному користувачеві запускати обробку контенту з довільної URL-адреси на пристрої цільової програми, що дає можливість для атаки на певних цільових користувачів.

WhatsApp, на відміну від Viber, використовує Signal Protocol, що є сильною перевагою в бік захищеності та надійності.

3. *Telegram*

Телеграм також наводить документацію з криптографічними механізмами. Кастомна версія MTProto 2.0 використовується для цього, який вважається закритим протоколом.

Ключі генеруються з використання ДХ на еліптичних кривих .

***Обмін повідомленнями.*** AES-256 в режимі IGE використовується для зашифрування повідомлень. В секретних чатах створені сеансові ключі періодично оновлюються. Для гешування використовується SHA-256. Для звичайних чатів ключі шифрування зберігаються на серверах телеграм, тому це не вважається наскрізним шифруванням. У випадку секретних чатів реалізовано наскрізне шифрування.

***Надсилання файлів, фото та відео.*** Для надсилання файлів використовується одноразовий ключ, який не пов'язаний з сесійним ключем. Файли шифруються AES-256 в режимі IGE та завантажуються на сервер.

***Зашифровані дзвінки.*** Відео- та аудіо-дзвінки є “end-to-end” зашифрованими. Хоч і не вдалось знайти повну специфікаю для алгоритмів, але те, що відомо – ключі генеруються з допомогою ДХ, а самі дзвінки – з допомогою AES, при тому ключі зберігаються на пристроях абонентів.

***Про рівень захищеності.*** На мою думку, найбільш спірний момент в реалізації Телеграм – це те, що ключі шифрування зберігаються на серверах для випадку звичайних чатів, а також те, що використовується досить рідкісний режим AES-256 IGE. Тому з рекомендацій можу дати використовувати секретні чати для важливих повідомлень або ж дзвінки, які є більш захищеними. Як більш глобальна альтернатива – використання іншого більш захищеного месенджера, наприклад WhatsApp.

4. *Skype*

На офіційних джерелах від Microsoft знайдено досить небагато технічної документації щодо криптографічних алгоритмів в Skype.

На етапі ***логіну та аутентифікації*** застосовуються RSA-сертифікати (1536- або 2048-бітні) для сертифікації публічних ключів.

Коли встановлено з’єднання***, створюється сесійний ключ***, який використовується для шифрування медіа/даних під час сесії.

Skype традиційно використовував шифрування: для передачі між клієнтом і сервером — через TLS, а для передач між клієнтами (коли це можливо) — AES-256.

Від 2018 року Skype додав ***можливість «приватних розмов»*** (Private Conversations), які використовують Signal Protocol. У приватних розмовах шифруються текстові повідомлення, файли, голосові повідомлення, медіа, а також — голосові дзвінки Skype-to-Skype. E2EE покриває лише «приватні розмови» між двома користувачами на одному пристрої; в групових чатах / дзвінках E2EE не гарантується.

***Про рівень захищеності.*** Скайп захищений, але недостатньо добре в порівнянні з месенджерами, які мають повністю наскрізне шифрування. Найбільш захищений спосіб спілкування – це приватні розмови.

**Висновок.** На мою думку, серед розглянутих месенджерів найбезпечнішим з точки зору криптографічних механізмів є WhatsApp, оскільки він реалізує повністю наскрізне шифрування, при якому ключі зберігаються на пристроях користувачів. Інші месенджери реалізують дану концепцію лише частково, для деяких типів комунікації, як-от Телеграм з приватними розмовами та дзвінками, чи Скайп для приватних розмов. У Viber раніше спостерігались досить серйозні вразливості, коли не весь трафік шифрувався