Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Вразливості системи захисту інформації в сучасних мессенджерах
(тема)

Виконала: Арчакова А.І.
(прізвище, ініціали)
студент 2 курсу, групи БДІРм-18-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)

Керівник д.т.н., проф. Северінов О.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові *Арчакової Альоні Ігорівні*
(прізвище, ім'я, по батькові)

1. Тема роботи *Вразливості системи захисту інформації в сучасних месенджерах*
затверджена наказом по університету від "04" листопада 2019 р. № 1648Ст
2. Термін подання студентом роботи до екзаменаційної комісії _____
3. Вихідні дані до роботи *Теоретчні дані про мессенджери*
4. Перелік питань, що потрібно опрацювати в роботі
1. Функції безпеки у мессенджерах
2. Огляд популярних мессенджерів в Україні та світі
3. Стандарти SS7 та Diameter
4. Методика пошуку захищенного мессенджеру
5. Результати досліджень
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Презентаційний матеріал у вигляді слайдів*

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	*Отримання завдання*	*01.09.19*	
2	*Пошук літератури*	*31.09.19-01.12.18*	
3	*Практичні випробування*	*10.02.19-20.06.19*	
4	*Збір даних за час випробувань*	*15.06.19-31.08.19*	
5	*Аналіз отриманих результатів*	*01.09.19-03.11.19*	
6	*Оформлення пояснювальної записки*	*04.11.19-20.12.19*	

Дата видачі завдання __01____вересня___2019 р.

Студент _____
(підпис)

Керівник роботи (проекту) _____ __к.т.н., проф. Сєвєрінов О.В.____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка атестаційної роботи: 73 сторінки, 38 посилань, 13 рисунків.

МЕССЕНДЖЕРИ, VIBER, WHATSAPP, TELEGRAM, ДВОХФАКТОРНА АВТЕНТИФІКАЦІЯ, НАСКРІЗНЕ ШИФРУВАННЯ, SIGNALING SYSTEM 7, DIAMETER, MTPROTO

Об'єкт дослідження: функції щодо забезпечення безпеки в сучасних мессенджерах.

Мета роботи: пошук вразливостей в системах сучасних месенджерів.

В спеціальній частині розглянуто особливості сучасних мессенджерів, їх функції забезпечення конфіденційності користувачів, проведення аналізу з безпеки функцій для захисту мессенджерів, аналіз на тему захищеності сучасних мессенджерів, методика пошуку захищених сучасних мессенджерів.В роботі проаналізовані сучасні телекомунікаційні протоколи, засоби захисту конфіденційної інформації у мессенджерах.

Практичне значення роботи полягає в підвищенні ефективності функцій захисту у сучасних мессенджерах та в сучасних телекомуникаційних протоколах Signaling System 7 та Diameter.

Наукова новизна роботи полягає у визначенні особливостей та виборі методики пошуку захищенного мессенджеру у сучасному світі.

ABSTRACT

Explanatory note of the performance appraisal: 73 pages, 38 references, 13 drawings.

MESSANGERS, VIBER, WHATSAPP, TELEGRAM, TWO-FACTOR AUTHENTIFICATION, THROUGH ENCRYPTION, SIGNALING SYSTEM 7, DIAMETER, MTPROTO

Object of study: security features in modern messengers.

Purpose: search for vulnerabilities in the systems of modern messengers.

The special part deals with the features of modern messengers, their functions of ensuring the confidentiality of users, carrying out security analysis of functions for the protection of messengers, analysis on the security of modern messengers, the method of searching for protected modern messengers.

The practical importance of the work is to increase the efficiency of security features in modern messengers and in modern telecommunication protocols Signaling System 7 and Diameter.

The scientific novelty of the work is to identify the features and choice of methods for finding a secure messenger in the modern world.

ПЕРЕЛІК СКОРОЧЕНЬ

SS7 – Signaling System 7

EE2E – End-to-end encryption

MIM – Man in the middle

CAP – Camel

HLR - Home Location Register

VLR - Реєстр розташування відвідувачів

ВСТУП

У сучасному світі досить складно уявити людину без смартфона і мобільного зв'язку. Кожен день величезна кількість користується мобільними телефонами для зв'язку з друзями, родичами і колегами за допомогою мобільних додатків для миттєвого обміну повідомленнями, здійснення голосових дзвінків.

Через величезної кількості інформації, що передається, деякі користувачі замислюються про безпеку використовуваних додатків. Розробники таких додатків пропонують безліч функцій для захисту конфіденційної інформації - паролі, спеціальне шифрування, секретні чати і багато іншого.

Через інтернету - здійснення покупок в інтернет-магазинах, платежі в банках - в наше життя міцно увійшли SMS з одноразовими кодами для підтвердження особи в різних операціях.

Signaling System 7 - це стандарт, який розроблявся в 1970-х роках і використовується для обміну службовою інформацією між мережевими пристроями в телекомунікаційних мережах. У той час, коли він створювався, розробники не замислювалися про безпеку, так як доступ до мережі мали лише оператори. У наш час відсутність будь-яких засобів захисту у Signaling System 7 є великою проблемою, так як зловмисник, тим або іншим способом отримав доступ до неї доступ, може перехоплювати SMS користувачів для підтвердження особи, викрадаючи конфіденційну інформацію і викрадаючи гроші з особистих, прослуховувати голосові дзвінки і навіть впливати на функціонування мобільної мережі.

У 2015 році запустили мережу нового покоління 5G, в якій вже повинні були використовувати новий стандарт Diameter. За результатами досліджень, проблеми безпеки Signaling System 7 залишатимуться ще досить довго, так як оператори зв'язку все ще повинні забезпечувати підтримку стандартів 2G / 3G і взаємодія між мережами різних поколінь. Більш того, дослідження доводять, що протокол Diameter схильний тим же загрозам, що і SS7.

Об'єктом дослідження є функції щодо забезпечення безпеки в сучасних месенджерах.

Предметом дослідження є методи підвищення безпеки в сучасних месенджерах, пошук захищеного месенджера з існуючих альтернатив.

Метою даної магістерської роботи є пошук вразливостей в системах сучасних месенджерів.

Завданнями даної роботи є:

– провести огляд літературних джерел і проаналізувати існуючі аналоги месенджерів;

– проаналізувати можливі функції з безпеки і уразливості в сучасних месенджерах;

– обґрунтувати можливі функції з безпеки та вразлівості в сучасних месенджерах;

– провести оцінку існуючим функціям безпеки в месенджерах.

1. АНАЛІЗ СУЧАСНИХ МЕССЕНДЖЕРІВ

1.1 Історія створення додатків для миттєвого обміну повідомленнями

Спочатку, концепція для спілкування між людьми за допомогою електронних пристроїв йде в 1960-і роки. Перша подібна система з'явилася в Массачусетському технологічному інституті (MIT) в 1961 році. В ході експерименту одночасно в мережі могло перебувати до тридцяти користувачів, обмінюючись при цьому текстовими повідомленнями. Трохи пізніше, даний проект став досить популярний як внутрішній спосіб спілкування між співробітниками в MIT [1].

Найперше додаток для обміну повідомленнями, приблизно схоже на те, яким ми звикли його бачити зараз, з'явилося вже в 1990-х роках.

Месенджер (Instant messaging, IM) - це мобільний додаток або веб-сервіс, що дозволяє миттєво обмінюватися повідомленнями. У 1996 році два ізраїльських студента заснували компанію Mirablis і запустили перший месенджер ICQ. Це було одне з перших програм, що дозволяють в режимі реального часу обмінюватися повідомленнями на великих відстанях [2]. Доступна ICQ була тільки на персональних комп'ютерах, с інноваційними, на той момент, можливостями - передача файлів, відображення статусу "в мережі", пошук потрібних користувачів по самому месенджер і рядом інших переваг, яких раніше не було.

Через два роки компанію Mirablis набуває AOL - найбільший, на той момент, американський інтернет-провайдер, а потім в 2010 році перепродує її Digital Sky Technologies.

У 2003 році велика частина користувачів ICQ переходить на Jimm - її мобільний аналог.

З 2009 року популярність ICQ стала стрімко падати через появу WhatsApp. З появою останнього, аудиторія користувачів ICQ впала на 35%, що в підсумку склало близько 17 мільйонів чоловік.

Творцями WhatsApp були український емігрант Ян Кум і колишній інженер Yahoo Брайон Актон [3].

Мобільний сервіс WhatsApp спочатку був сервісом, який показував який з контактів в записнику на мобільному телефоні знаходиться в мережі, хто розмовляє по телефону, а хто зайнятий. Також управляти статусом можна було вручну. Запам'ятався месенджер тим, що перший в історії мав можливість прив'язки до мобільного номеру, що на той момент було фішкою виключно користувачів BlackBerry, але вона працювала тільки з телефонами цієї ж марки. У 2014 році компанія Facebook викупила WhatsApp.

Величезна популярність месенджерів почалася в 2010 році [4]. Розробники месенджерів намагаються якомога сильніше виділити свій продукт на тлі інших, додаючи різноманітні унікальні функціональні властивості - можливість дзвінків, обмін аудіо- та відеофайлами, текстовими матеріалами та багатьом іншим. Кожен новий мессенджер, щоб бути конкурентно спроможним, був зобов'язаний надати унікальні функціональні новинки. Як приклад можна розглянути Viber.

Viber був представлений користувачам в кінці 2010 року [5], ставши першим месенджером, що дозволяє здійснювати безкоштовні дзвінки при наявності мобільного інтернету. Згодом цю функцію додали в свої месенджери і другими компанії.

Технічні особливості подібних додатків не стояли на місці в той час. Наприклад, месенджер WeChat [6], що належить китайській компанії, додав можливість здійснювати відеодзвінки.

У наш час месенджери - це те, без чого важко уявити свій звичайний день. За допомогою месенджерів зараз передаються відео, музика, голосові повідомлення, документи за лічені секунди незалежно від їх географічного положення. Також однією з зручних і популярних функцій в більшості

месенджерів є можливість створення "груп" або "бесід" для великої кількості користувачів, об'єднуючи їх за інтересами або загальним цілям.

1.2 Загальна структура месенджерів

Сучасний месенджер - це клієнтський сервіс, що дозволяє передавати текст в режимі онлайн через сервери компанії-виробника. Тобто текст, відео та картинки йдуть не напряму одержувачу, а спочатку проходять через централізовану систему.

Далі йде криптографічний протокол - це своєрідний комутатор для всього месенджера. Їх існує багато, і саме вони визначають, як саме необхідно надіслати лист - через сервер, хмару, через які конкретно адреси, хто отримає доступ до певного каналу, в стислому чи вигляді файл дійде до адресата або в оригінальному і так далі. Серед них є протоколи безпеки, які як раз створені для приватності особистого листування - їх сенс в тому, щоб не дати нікому, крім учасників чату, отримати до нього доступ.

Важливі параметри при виборі захищеного месенджера:

1) FLOSS, або FOSS - Free / Libre and Open-Source Software (Вільне програмне забезпечення з загальнодоступними (відкритими) вихідними кодами) - категорія програмного забезпечення, яка включає в себе як вільне, так і відкрите програмне забезпечення;

2) Ступінь централізації [7]:

– централізований - вимагає сервера, можливо заблокувати. Приклади: WhatsApp, Telegram, Viber;

– децентралізований - кожен клієнт є одночасно і сервером.

3) Тип ліцензії:

  – федеративний - мережа з серверів, які спілкуються один з одним. Приклади: Jabber, Riot Matrix;
  – пропріетарний - приватний сервер або сервера;

4) Можливість анонімної реєстрації та використання.

Є месенджери, які дозволяють реєструватися з використанням поштової скриньки або облікового запису в соціальній мережі. Є й такі, де можна створити обліковий запис в самому месенджере без прив'язки до чогось;

5) Наявність End-to-End Encryption (E2EE) [8]

Деякі месенджери мають функцію наскрізного шифрування за умовчанням, в інших її можна включити, але є й ті, де наскрізного шифрування просто немає;

6) Чати з наскрізним шифруванням для великої кількості користувачів і їх синхронізація

Ця функція зустрічається досить рідко, але є дуже важливим параметром безпеки спілкування;

7) Повідомлення про необхідність перевірки відбитків E2EE

На початку використання чатів з наскрізним шифруванням, деякі месенджери пропонують перевірити відбитки співрозмовників;

8) Повідомлення про необхідність перевірки відбитків E2EE в групових чатах

При додаванні нового співрозмовника, з яким не звірені відбитки, в секретний груповий чат не всі месенджери пропонують перевірити його відбитки. Через такого упущення втрачається сенс секретних чатів;

9) Захист соціального графа

Деякі месенджери збирають інформацію про контакти користувача та інші метадані, наприклад кому дзвонив користувач, як довго розмовляв.

1.3 Аналіз популярних месенджерів в Україні та у світі

За статистикою на 2019 рік (рис 1.1), найпопулярнішим месенджером в Україні є Viber. За ним йде Facebook Messenger, Telegram і лише в самому кінці можна спостерігати WhatsApp [9] [10].

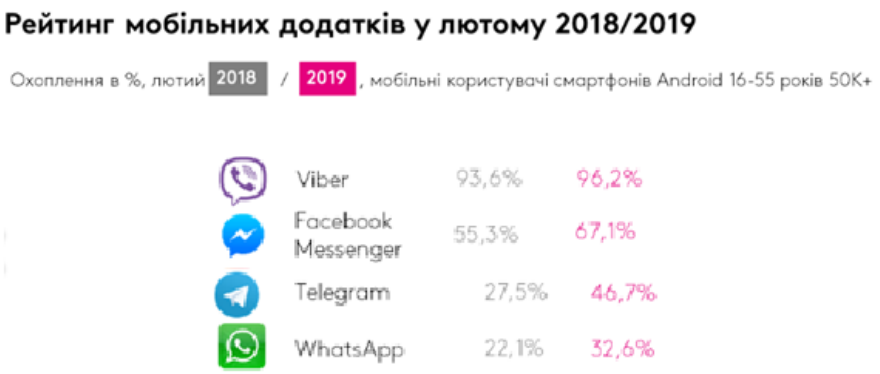

Рисунок 1.1 - Рейтинг популярних месенджерів в Украйні

Більшість користувачів додатків для швидкого обміну повідомленнями навіть не замислюються над їх безпекою та збереженням власної конфіденційної інформації при листуванні. Переважно використовують те що вже встановлене у родичів, друзів або колег.

Давайте розглянемо чому саме Viber став самим використовуваним мессенджеров серед користувачів в Україні [11]. На ринок додатків по швидкому обміну повідомленнями Viber потрапив в 2010 році. Тоді вже був досить популярно інший аналогічний додаток - WhatsApp. Перевагою ж Viber виявилася більш швидше випущена версія програми під операційну систему Android, а ще через три роки розробники першими випускають комп'ютерну версію програми.

За даними компанії Viber, операційну систему Android використовують 84,23% користувачів Viber в Україні, 15% віддають перевагу IOS, 1,79% використовують десктоп [12].

Також в компанії повідомили, що їх програма встановлена на 97% смартфонів українських користувачів. Таким чином, дев'ять з десяти українців користується додатком Viber, а кожен другий український користувач відправляє десять і більше повідомлень в день у месенджері.

Статистика популярності месенджерів у світі значно різниться від української, її можна побачити на рисунку 1.2, де цифри вказані в мільйонах [13].

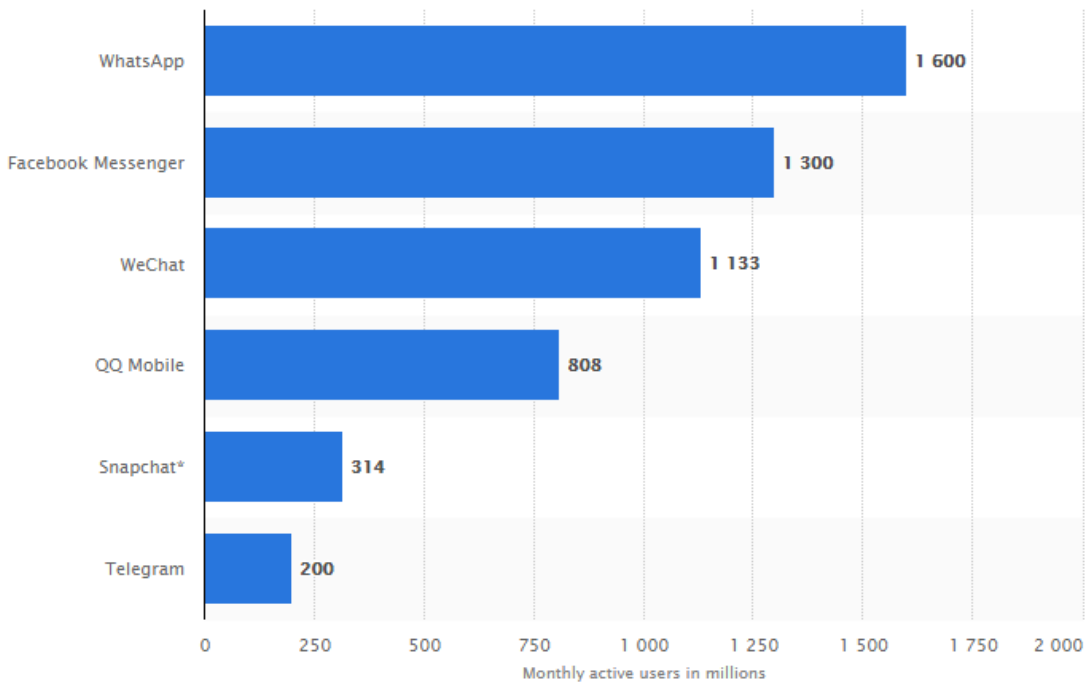

Рисунок 1.2 - Рейтинг популярних мессенджерів у світі

Найпопулярніші глобальні додатки для мобільних листувань станом на жовтень 2019 року значно відрізняються від тих, що використовують в Україні. WhatsApp використується великою популярністю в Індії, Бразилії та США. Facebook Messenger та Snapchat є самим популярним мессенджером у США. На третьому та четвертомі місці йдуть найпопулярніші мессенджери у Китаї. Telegram є дуже популярним по всієї Європі.

1.4 Viber

Ідея та первинна розробка програми належала ізраїльтянину Тальмону Марко та росіянину Ігорю Магазінніку [6].

2 грудня 2010 року Viber був запущений спочатку тільки на операційній системі iOS. Перша версія для Android вийшла в травні 2011 року, але мала обмеження, тільки для 50 тис. користувачів; останній випуск відбувся 19 липня 2012 року. Viber був випущений для BlackBerry, Bada і Windows Phone 8 травня

2012 року. 7 травня 2013 року вийшло оновлення програми для iOS до версії 3.0, де передбачена доступність Viber Desktop для Windows і OS X.

У 2014 року японська компанія Rakuten придбала Viber за 900 млн доларів.

Офіс технічної розробки програми і підтримки її користувачів знаходиться в Мінську та Бересті. Viber є резидентом Білоруського парку високих технологій.

29 листопада 2015 року з'явилась можливість видаляти надіслані повідомлення у отримувача. Функція працює на iOS та Android. Також є додатки для розумних годинників на базі Android та Apple Watch, вони мають базовий функціонал для перегляду повідомлень і відповіді на них.

Зараз Viber є найпопулярнішим месенджером серед українців. За даними українського представництва компанії, месенджером користуються більше 20 млн осіб, тобто половина населення країни.

Месенджер є централізованим, із наскрізним шифруванням за замовчуванням, без перевірки про необхідність порівняння відбитків та без захисту соціального графу.

Він має секретні чати, закриті чати та повідомлення, які знищуються через певний час.

Але, не завжди подібні міри захисту можуть гарантувати безпеку конфіденційних даних. Дуже важливо вчасно обновляти додаток, тому що це знижує можливість зловмисників скористуватись деякими помилками та недоробітками мессенджера. Наприклад, у Viber був випадок, коли один із користувачів виявив вразливість, за допомогою якої співрозмовник мав можливість підслуховувати розмову користувача [14].

Коли два абонента розмовляють між собою через Viber, назвемо їх А і Б, під час розмови, абоненту А надходить виклик, але не через Viber, а через мобільну мережу. Абонент А відповідає на виклик, тим самим абонент Б виявляється на утриманні.

Абонент Б перебуваючи на утриманні, наживає на кнопку «Утримання» двічі, тим самим поставивши і знявши режим утримання зі свого боку, дана опція

доступна при розмові по мобільному телефону або з планшета, в стаціонарному клієнта я такий кнопки не знайшов.

Проробивши дані дії абонент Б чує розмову абонента А, правда без можливості брати участь в ньому. Абонент А ніяк не розуміє, що його в цей момент вже «підслуховують» і коли закінчує розмову по мобільній мережі - повертається в Viber для продовження діалогу з абонентом Б.

Цю вразливість виправили майже через рік і до кінця не видомо чи на всіх операційних системах, або ні.

1.5 Facebook Messenger

Додаток для обміну миттєвими повідомленнями, створений Facebook. Він інтегрований з системою обміну повідомленнями на основному сайті Facebook і побудований на базі відкритого протоколу MQTT. За даними на квітень 2017 року місячна аудиторія месенджера становила 1 млрд. осіб.

Facebook Messenger є централізованим, із наскрізним шифруванням, але не за замовчуванням, без перевірки про необхідність порівняння відбитків із наскрізним шифруванням та без захисту соціального графу.

Однак слід пам'ятати, що Facebook збирає дуже багато інформації про користувача (наприклад, ваші дії, дії інших людей і яку ви надаєте інформація, яку ви їм надаєте; різну інформацію з пристроїв: операційна система, дії на пристрої, дані з налаштувань пристрою та много чего ще).

З 2015 року користувачам «Messenger» більше не обов'язково бути зареєстрованим в «Facebook». Після останнього оновлення для входу в додаток досить вказати номер телефону, що ще більше зближує його з іншими подібними сервісами.

1.6 Telegram

Telegram – мессенджер неоднозначний. З одного боку його вважають одним із найзахищеніших мессенджерів у всьому світі, з другого – мессенджером із вдалою рекламою. Telegram не дає доступу до вихідного коду сервера, тільки клієнта. Основні чати не мають наскрізного шифрування за замовчуванням, така функція є тільки у секретних чатах. Також відсутній захист соціального графу, його сервери є централізованими.

Щоб забезпечити безпеку даних, які не мають наскрізного шифрування, Telegram використовує розподілену інфраструктуру. Інформація з звичайних чатів зберігається в дата-центрах по всій земній кулі і знаходиться під різними юрисдикціями. Ключі дешифрування розбиті на частини і ніколи не зберігаються в тому ж місці, де і дані, які цими ключами зашифровані. У підсумку, щоб примусити Telegram видати будь-яку інформацію, необхідно отримати кілька судових приписів з різних юрисдикцій.

Також експерти з безпеки ставлять під питання існування протоколу MTProto [15], тому що сам вихідний код є закритим та його закритість для незалежного аудиту робить його потенційно вразливим для майбутніх атак.

Разом з цим спосіб наскрізного шифрування WhatsApp і Viber схвалений з боку експертів в області безпеки. Про MTProto можна сказати лише те, що на даний момент не зафіксовано успішних атак, які б привели до розшифровки повідомлень Telegram.

Зараз Telegram програє WhatsApp або Viber, які запровадили наскрізне шифрування за замовчуванням.

Для месенджера був створений протокол MTProto, що передбачає використання декількох протоколів шифрування.

В останніх версіях Telegram з'явилася функція «Сховати свій номер телефону». Ідентифікатор користувача – його нікнейм. Інші популярні месенджери не мають такої опції - завжди йде прив'язка до номера телефону, а номер телефону - це слабке місце будь-якого мессенджера. Це можливість

отримати несанкціонований доступ до цього додатка - за допомогою знайомих у мобільного оператора, які працюють там, або за допомогою вразливості в протоколі SS7.

1.7 WhatsApp

Месенджер WhatsApp відомий тим, що досить часто з'являється в новинах через чергову уразливості, яку знайшли і використовували зловмисники, або ж від чергової атаки.

У жовтні 2018 року знайши вразливість, яка дозволяла хакерам захоплювати користувальницькі додатки, коли вони відповідали на вхідний відеодзвінок [16].

У травні 2019 зловмисники скористалися вразливістю для установки технології спостереження, телефонуючи користувачеві через WhatsApp і в результаті отримуючи повний доступ до місця розташування користувача і його особистим повідомленнями [17].

Трохи пізніше, в цьому ж місяці, Facebook підтвердив у своєму блозі, опублікованому репортером з кібербезпеки Брайаном Кребсом, що протягом багатьох років Facebook зберігає «сотні мільйонів» паролів від облікових записів своїх користувачів у відкритому вигляді [18].

Відкриття було зроблено в січні, сказав Педро Канахуаті з Facebook, в рамках звичайної перевірки безпеки. Жоден з паролів не був видний нікому за межами Facebook, сказав він. Facebook визнав помилку безпеки через місяці після того, як Кребс сказав, що журнали були доступні приблизно 2000 інженерам і розробникам. Кребс сказав, що помилка датується 2012 роком.

Розробники запевняють, що вони на постійній основі взаємодіють з дослідниками безпеки по всьому світу, щоб забезпечити безпеку і надійність WhatsApp.

Також Facebook, компанія, якій належить WhatsApp, активно збирає всі можливі метадані користувачів [19]:

– час, частоту і тривалість активності в вікні з вкладкою соцмережі, включаючи інформацію про те, відкрито воно або перебуває у фоновому режимі);

– покупки, здійснені на сторонніх сайтах;

– плагіни в браузері користувача;

– руху курсора на пристрої;

– використання камери, вбудованої в додаток Facebook;

– метадані фотографій (включаючи час і місце зйомки);

– встановлені додатки;

– назви та типи файлів на пристрої користувача;

– ідентифікатори додатків;

– кількість вільного місця на пристрої;

– контакти з довідника користувача;

– журнал дзвінків і історію SMS Android-пристроїв;

– найближчі точки доступу Wi-Fi і стільникового зв'язку;

– інформацію мобільних і стаціонарних провайдерів через комп'ютери, телефони, зв'язані телевізори та інші пристрої в мережі;

– заряд акумулятора пристрою;

– налаштування та дозволу на пристрої;

– інформацію та фотографії інших користувачів, а також частоту взаємодія і спілкування з ними.

На початку 2019 року месенджер WhatsApp зробили доступним для кнопкових телефонів, повідомляє портал The Verge. Це стало можливим завдяки виходу версії WhatsApp для операційної системи KaiOS [20].

Завантажити додаток можна з магазину KaiStore на пристрої, що мають 256 або 512 МБ оперативної пам'яті.

Передбачається, що з третього кварталу 2019 року можна буде попередньо встановити месенджер на нові пристрої з KaiOS. Зараз на ринку більше 100 млн

телефонів з цією операційною системою, найвідоміша модель серед них - Nokia 8110.

Відомо, що версія WhatsApp для кнопкових телефонів відрізняється від тієї, яка працює на операційних системах iOS і Android. Зокрема, недоступна функція відеодзвінків через відсутність на таких пристроях фронтальної камери.

Всі інші базові функції присутні: користувачі можуть надсилати приватні повідомлення і писати в групових чатах, а також ділитися фотографіями, відеозаписами, документами і аудіофайлами.

WhatsApp належить Facebook. І якщо для вас проблема, що компанія читає повідомлення, то, напевно, теж не варто користуватися цим месенджером.

Додаток зберігає повідомлення на телефоні, а також на хмарному сервері iCLoud, з використанням протоколу підтримки шифрованих групових чатів. При цьому зміст розмов не зберігається, але номера, на які ви дзвонили, модель телефону, IP-адреса і версія ОС залишаються в базі.

1.8 Аналіз менших за популярністю захищених месенджерів

1.8.1 Signal

Месенджер активно рекомендується для використання фахівцями з безпеки зі всього світу. За словами розробників, всі повідомлення зберігаються виключно на мобільному пристрої користувача і шифруються локально перед відправкою. Але, на відміну від інших месенджерів, Signal не проводить аудити безпеки власного додатка на предмет вразливостей.

При цьому важливо, що даний месенджер, спрямований на захист листування, при реєстрації запитує мобільний номер. При спілкуванні у користувача є можливість створювати само знищується повідомлення. Щоб переконатися, що на тому боці знаходиться саме потрібний нам співрозмовник, в Signal додали функцію під назвою «Safety Number».

З боку користувача можна зробити кілька простих дій для захисту листування в Signal. По-перше, на запуск програми можна встановити парольний

фразу, яка буде запитуватися через певні періоди бездіяльності. Можна включити заборону зняття скріншотів. При включенні парольної фрази все листування починає шифруватися локально на пристрої. Важливо відзначити, що парольні фрази недоступні користувачам iOS, а значить, локальне шифрування листування не працюватиме при спілкуванні на Android - iOS.

Повідомлення в Signal зашифровані за допомогою наскрізного шифрування і можуть бути прочитані тільки одержувачем. За допомогою Safety Number користувач може бути впевнений, що на тому боці знаходиться саме потрібний співрозмовник. Всі повідомлення і дзвінки зберігаються локально на пристрої і піддаються локальному шифрування за допомогою парольної фрази (якщо вона включена) перед відправкою на сервер.

Розробник не має ніякого доступу до відправлені повідомленнями. Щоб користувачі могли переконатися у відсутності вразливостей програмного забезпечення для прослуховування, код месенджера і сервера опубліковані на GitHub, де будь-який бажаючий може його вивчити.

Але навіть у визнаних по безпеці месенджерів можуть існувати небезпечні вразливості.

Восини 2019 року була знайдена вразливість, яка дозволяла зловмисникам слідкувати за користувачами мессенджеру під час дзвінків [21].

А за допомогою вразливості в Signal зловмисник міг ініціювати виклик і отримати доступ до мікрофона на пристрої жертви, після чого прослуховувати розмови, навіть якщо дзвінок залишився без відповіді.

Дана проблема була виявлена в Signal для Android. Вона поширювалася тільки на голосові виклики, не зачіпаючи відеодзвінки. Виявлена уразливість фактично могла використовуватися для підслуховування користувачів пристроїв без їх відома.

Проблему виявила фахівець Google Project Zero Наталі Сільванович. За її словами, зловмисники могли використовувати модифіковану версію програми Signal, ініціювати виклик, а потім натиснути на власну кнопку "Mute" (відключення звуку), "щоб примусово підключити викликається пристрій".

Якщо зловмисник встигав швидко натиснути на кнопку відключення звуку, жертва могла не помітити атаку.

"За допомогою модифікованого клієнта можна відправити повідомлення" з'єднати "на викликається пристрій під час дзвінка, але до того, як користувач його прийняв. Таким чином виклик буде прийнятий навіть без участі користувача ", - зазначила Сільванович.

Уразливість спрацювала тільки при аудіозвонках, оскільки для відеодзвінків в додатку Signal користувачам потрібно вручну включити камеру.

За словами Сільванович, в зоні ризику знаходилися тільки користувачі Android-версії, оскільки в iOS-клієнті відбувався збій виклику через помилки в інтерфейсі.

На сьогодні вразливість вже усунена.

1.8.2 Threema

Даний месенджер користується популярністю серед європейських користувачів, хоча і має початковий одноразовий внесок у розмірі трьох євро. У Threema розробники приділяють велику увагу параметрам безпечності та захисту даних. Для того, щоб почати користуватися системою, користувачеві спочатку треба активувати особистий ідентифікатор [21].

Користувачеві буде необхідно створити кілька ключів - відкритий і закритий. Паролів також можна створити кілька, і додати кодове слово.

Особливістю Threema є його повна приватність. Навіть після реєстрації у користувача не буде можливості зареєструватися за допомогою номера телефону, електронної пошти або соціальних мереж.

Використання Threema має генерувати якомога менше даних на серверах - це частина концепції месенджера. З цієї причини такі дані, як, наприклад, контакти або групові чати зберігаються децентралізовано на призначених для користувача пристроях, а не на сервері Threema. Сервера месенджера приймають на себе роль комутатора. Повідомлення та дані пересилаються, але не зберігаються постійно. Там, де немає даних, немає доступу або неправильного

використання. Однак без будь-якого тимчасового зберігання даних не може бути ніякої асинхронного зв'язку.

Як тільки повідомлення було успішно доставлено користувачеві, воно негайно видаляється з сервера. Всі повідомлення і мультимедіа передаються наскрізним зашифрованим в Threema. Це означає, що навіть якщо хтось перехопить повідомлення, воно буде абсолютно некорисним. Тільки передбачуваний одержувач може розшифрувати і прочитати повідомлення.

При синхронізації контактів списки контактів не зберігаються. Адреси електронної пошти і номери телефонів з адресної книги анонімізуються (хешується) до того, як вони потрапляють на сервер. Після завершення порівняння вони відразу видаляються з сервера.

Компанія стверджує, що закритий ключ їм ніколи не відомий, і тому вони не можуть розшифрувати вміст повідомлень користувачів.

Ключ, використовуваний для цього шифрування, генерується випадковим чином при першому запуску Threema і може бути додатково захищений шляхом установки ключової фрази головного ключа у параметрах додатку.

Блокування за допомогою PIN-коду, яке можна включити незалежно від ключової фрази головного ключа, не викликає додаткового шифрування, це є однією з функцій блокування призначеного для користувача інтерфейсу.

На новіших моделях iOS також використовуються апаратні функції для шифрування, тому навіть простий чотиризначний PIN-код забезпечує певний захист. Для максимального захисту від атак методом перебору, користувач повинен зробити складний код доступу.

На Windows Phone Threema використовує ізольоване сховище, до якого має доступ тільки самі розробники. Крім того, для захисту файлів мультимедіа, ідентифікатора, особистого ключа та повідомлень також використовується спеціальне шифрування на основі AES-256. Ключ, використовуваний цим методом шифрування, генерується при першому використанні і може бути додатково захищений парольним словом, яке настійно радять використовувати розробники Threema для більшої безпеки.

Також Threema стверджує, що ні за яких умов не може розшифрувати вміст листувань користувачів, так як у них немає секретних ключів, які існують виключно на пристроях самих користувачів. Серверів необхідно знати хто кому відправляє повідомлення, щоб вони могли направити його правильному одержувачу, але вони не реєструють цю інформацію і не можуть розшифрувати зміст повідомлення.

1.8.3 Briar

Briar - не дуже популярний месенджер, однак він вважається одним з кращих по безпеці. Він заснований на технології децентралізованих мереж, може працювати по Bluetooth або Wi-Fi або через інтернет, але в такому випадку він підключиться через Tor [22].

Вихідний код Briar відкритий, є можливість анонімної реєстрації та використання, а чати шифруються за умовчанням. Переписка не зберігається на серверах Briar - тільки на телефоні самого користувача в зашифрованому вигляді. Є захист соціального графа, групові чати з наскрізним шифруванням, але немає синхронізації таких чатів між пристроями, оскільки немає можливості використовувати одну і ту ж обліковий запис на різних пристроях.

З недоліків Briar можна виділити відсутність версії для iPhone, немає можливості голосових дзвінків. Якщо відсутність дзвінків ще можна опустити, то без версії для однієї з великих платформ коло спілкування виявиться ще більш вузьким.

1.8.4 Wire

Wire - один з найбільш анонімних месенджерів [23]. В його основі - протокол Wire Swiss, заснований на Signal. У нього є можливість анонімної реєстрації, також за замовчуванням підтримується наскрізне шифрування з можливістю синхронізації зашифрованих чатів. Є захист соціального графа, підтримуються групові зашифровані чати і безпечні розраховані на багато користувачів дзвінки. Подібні функції є в Briar, але у Wire перевага в більшій

кількості підтримуваних платформах, таких як: Android, iOS, Windows, macOS, Linux.

Ім'я профілю не є загальнодоступним і не буде доступний широкому ні в яких загальнодоступних пошукових системах. Ім'я профілю користувача з'являється тільки при пошуку іншими учасниками Wire.

Повідомлення можна отримувати тільки від користувачів, яким дали на це дозвіл.

Месенджер платний і коштує шість євро в місяць (чотири при оплаті за рік). Розробники стверджують, що це плюс: подібна бізнес-модель - це хоч якась гарантія того, що на даних користувачів не спробують заробити. З іншого боку, грошові транзакції погано ладнають з анонімністю.

1.8.5 Confide

Додаток було розроблено зі своєю особливістю - текст на екрані одержувача не відображаються у вигляді тексту, а лише у вигляді прямокутників (рис. 1.3). Щоб прочитати слово, заховане під прямокутником, потрібно навести на нього палець[24]. Таким способом автори Confide захистять повідомлення не тільки від перехоплення, але і від ситуації, коли текст Вашого повідомлення прочитає хтось стоїть у вас за спиною. Всі повідомлення видаляються без можливості їх відновлення [25].

Розробники на постійній основі проводять аудити безпеки і викладають звіти в загальний доступ.

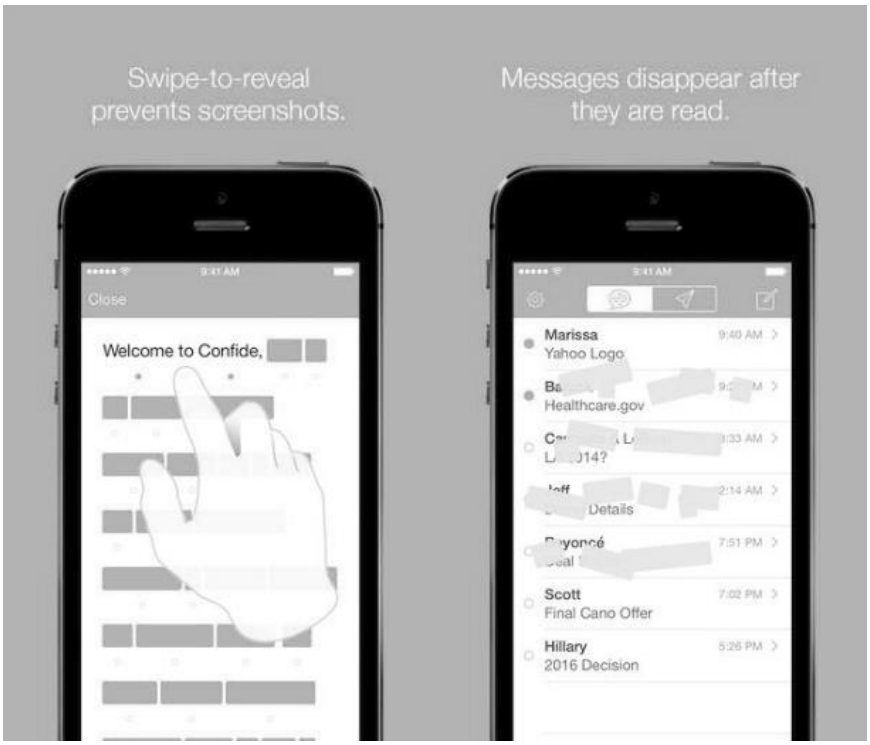

Рисунок 1.3 – Схема роботи месенджеру Confide

Отримавши повідомлення, користувач може побачити на екрані набір смужок, де кожне окреме слово - одна смужка. Щоб прочитати повідомлення, потрібно провести пальцем зверху вниз по рядках. Ім'я абонента при цьому з екрану зникає. Рядки будуть відкриватися по одному, таким чином побачити відразу весь текст одночасно неможливо. Поки користувач не натиснув кнопку повернення до переписки, повідомлення можна переглядати без обмеження за часом. Якщо була відправлена картинка, то переглянути її теж можна тільки по частинах.

Після того, як користувач прочитав повідомлення і натискає кнопку "повернутися", воно повністю знищується. Немає ніяких історій листування, лог-файлів або резервних копій. Повідомлення зникає повністю, не залишаючи після себе нічого. Є функція залишати останнім відправлене повідомлення, , але ця опція відключається.

Якщо спробувати обдурити месенджер, зробивши скріншот екрану, як і раніше навівши палець на повідомлення - месенджер відкине назад до списку

контактів. Співрозмовник побачить повідомлення, якщо раптом буде спроба зберігти фрагмент листування, а виділене повідомлення буде видалено.

1.9 Висновки аналізу мессенджерів

Сьогодні для користувачів представлено більше тридцяти мессенджерів із різною ступеню популярності. Майже усі вони впровадили функції для надання безпечного користування додатками та і для збереження конфіденційної інформації користувачів. Але на ділі, у самих популярних з них спостерігаються деякі проблеми з безпекою.

Такі мессенджери, як WhatsApp, Facebook Messenger та Telegram, не можуть бути безпечними з різних причин. У перших двух постійни проблеми із вразливостями – стабільно 3-4 рази за рік можно побачити нову статтю з черговою знайденої проблемою. Ще й сама компанія дуже зацікавлена у збори практично усіх можливих метаданніх своїх користувачів в випущених додатках.

У Telegram хоч і існують секретні чати, але це не змінює того, що звичайні чати не мають протоколу шифрування повідомлень за замовчуванням, ще й зберігаються на серверах.

Усі популярни мессенджери мають закритий вихідний код, що робить їх неможливим до аудиту по безпеці спеціалістами. Більшість із них зберігає листування своїх користувачів на власних серверах та має прив'язку аканта до номерів їх мобільних телефонів.

2. АНАЛІЗ ЗАГРОЗ У СУЧАСНИХ МЕССЕНДЖЕРАХ

2.1 Стандарт Signaling System 7 у телекомунікаційних системах

Протокол SS7 та пов'язане з ним накладення поза мережевою сигнальною мережею було розроблено на початку 1980-х, головне розгортання розпочалося в середині 1980-х [26]. За цей час в усьому світі існувала обмежена кількість операторів мережі, і відносини між операторами були одними з довіри. Мережі, як правило, були провідними, а доступ до SS7 здійснювався через фізичну підключення, створюючи підгороджений садовий підхід до безпеки. SS7 став основною міжвідомчою методологією сигналізації між операторами, що забезпечує налаштування та виклик викликів, а також розширені послуги, такі як безкоштовний дзвінок та Advanced Intelligent [27].

В кінці 1980-х рр. були визначені нові верхні рівні протоколів для підтримки мобільних телекомунікацій. Ці шари були Мобільною програмою (MAP) та додатком CAMEL (CAP).

Через обмеження зв'язку та пропускної здатності SS7, в середині 2000-х було введено транспорт сигналів (SigTran). Шари адаптації SigTran використовували протокол передачі управління потоком (SCTP) спільно з протоколом Internet (IP) в якості транспортних механізмів.Дослідники завжди попереджали, що лазівки в SS7 дозволяють зловмисникам красти гроші з банків, маніпулювати дзвінками і повідомленнями.

Так, наприклад, на початку 2019 року Metro Bank виявив, що якийсь зловмисник отримав повний доступ до конфіденційної інформації про клієнтів [28]. Вторгнення відбувається в той момент, коли клієнт отримує на свій мобільний телефон спеціальний код для виконання будь-якої операції (наприклад, код безпеки для входу в онлайн-банк або підтвердження виконання фінансової операції).

Частина 1, 2, 3 транспорту повідомлень (MTP1, MTP 2, MTP3) - транспортні рівні для SS7. Частина користувача ISDN (ISUP) використовується для налаштування та припинення викликів у середовищі з комутацією ланцюгів.

Частина управління з'єднанням сигналів (SCCP) містить вихідні та цільові адреси для повідомлень TCAP / MAP / CAP. SCCP також забезпечує можливості глобального перекладу заголовків.

Частина мобільних додатків (MAP) забезпечує спеціальну сигналізацію для мобільних пристроїв.

спілкування, включаючи аутентифікацію, авторизацію, роумінг, SMS та інші.

Частина програми CAMEL забезпечує спеціальну сигналізацію для мобільного зв'язку, включаючи передплачену та інші.

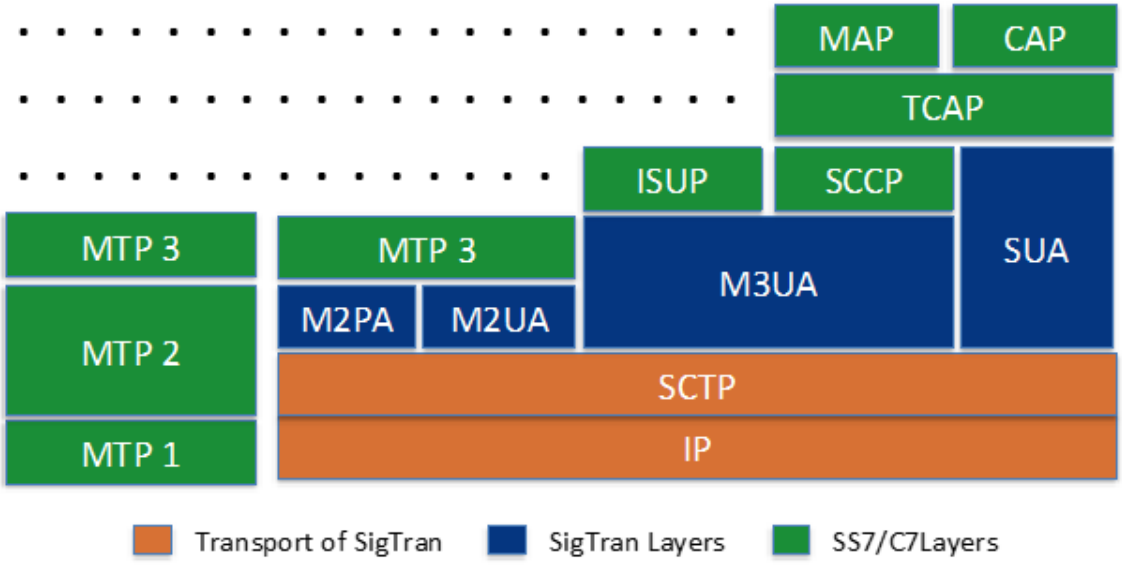

Рисунок 2.1 - Стек протоколу SS7

Metro Bank виявив, що саме в цей момент відбувалося потенційне порушення даних, коли код міг потрапити в руки зловмисника, що призводило до реальної небезпеки і проблем в інформаційній безпеці клієнтів банку. Банк погодився з наявністю вразливості, але заявив, що це не одиничній випадок.

Фактично, це вже не перша фінансова організація, яка зіткнулася із даною вразливістю. Але це перший банк, який визнав її.

У травні минулого року сенатор США Рон Уайден стверджував, що великий телекомунікаційний оператор піддався дуже схожою кібер-атаці. В результаті даної атаки конфіденційні дані клієнтів і користувачів стали доступні зловмисникам, якім навіть не були потрібні величезні знання і досвід в даній області, щоб отримати в свої руки цю інформацію. Таким чином, ця вразливість є досить поширеною, причому її не так складно використовувати.

Однак постачальники стільникових мереж ігнорували ці проблеми, так як вважали, що атаки SS7 здійснюються тільки висококваліфікованими зловмисниками, і для них потрібно значний обсяг інвестицій. Однак деякі професійні зловмисники довели відсутність безпеки в стільникових мережах, і вони успішно експлуатують мережі і, отже, просочується гроші з банківських рахунків. Таким чином, хакери можуть зламати телефон за допомогою ss7 і можуть читати ваші дзвінки та повідомлення.

2.1.1 Атака на SS7. Типи атак SS7, викликані вразливостями в мобільних мережах

При проведенні атаки на SS7 зловмисник має приєднатися до SS7, відправити службову команду Send Routing Info для SM (SRI4SM) в мережевий канал, вказав номер телефону користувача, якого він атакує в якості параметра . Домашня абонентська мережа відправляє у відповідь таку технічну інформацію: IMSI (International Mobile Subscriber Identity) і адреса MSC, за яким в даний час надає послуги передплатнику (рис. 2.2) .

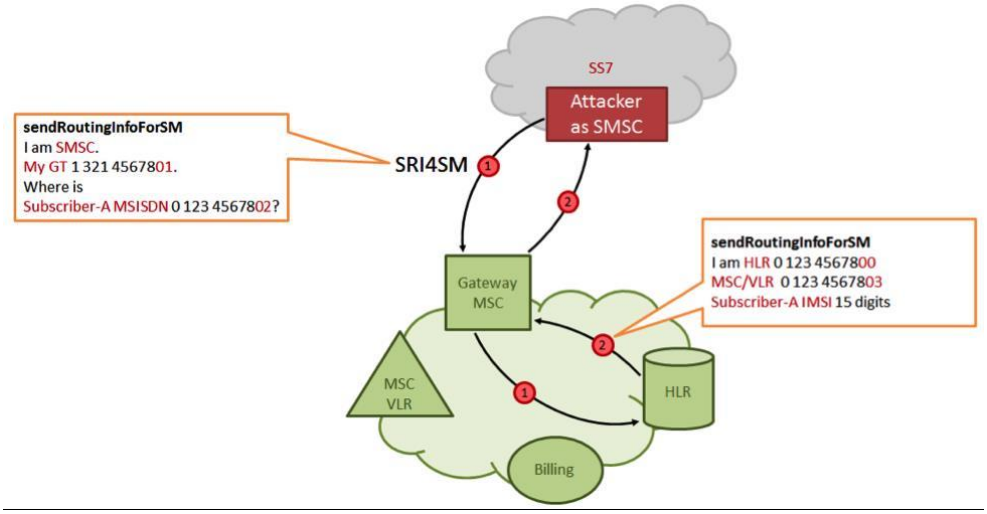

Рисунок 2.2 - Підключення зловмисника до SS7 та відправлення команди SendRoutingInfo

Після цього зловмисник має змінити адресу білінгової системи в профілі передплатника на адресу своєї власної псевдобіллінговой системи (наприклад, повідомляє, що абонент прилетів на відпочинок і в роумінгу зареєструвався на новій білінгової системи). Як відомо, ніяку перевірку така процедура не проходить.

Далі атакуючий вводить оновлений профіль в базу даних VLR через повідомлення «Insert Subscriber Data» (ISD) (рис 2.3).

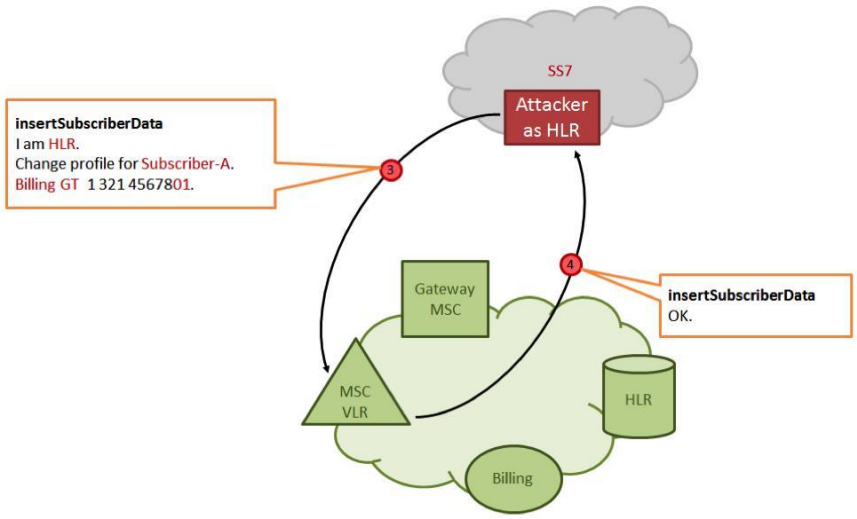

Рисунок 2.3 - Звернення комутатора до системи зловмисника

Коли атакує мий абонент здійснює вихідний дзвінок, його комутатор звертається до системи зловмисника замість фактичної білінгової системи. Система зловмисника відправляє комутатору команду, що дозволяє перенаправити виклик третій стороні, контрольованої зловмисником (рис.2.4).

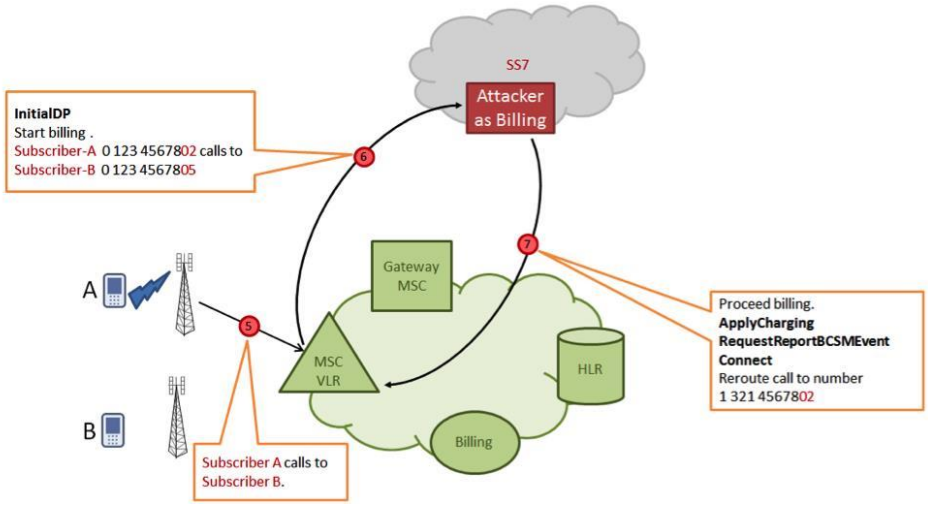

Рисунок 2.4 - Встановлений зв’язок між абонентами та зловмисником

У сторонньому місці встановлюється конференц-зв'язок з трьома передплатниками, дві з них є реальними (абонент А і викликається В), а третій вводиться зловмисником незаконно і здатний прослуховувати і записувати розмову (рис 2.5).

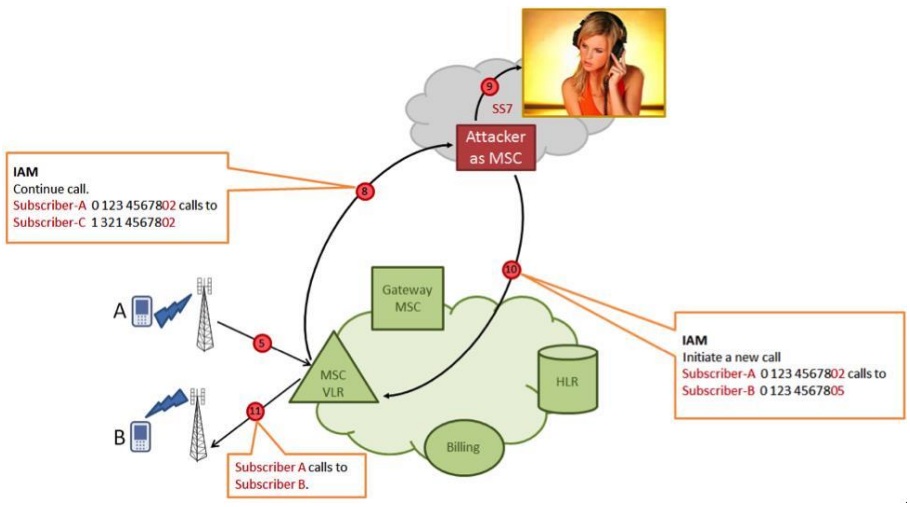

Рисунок 2.5 - Отримання SMS абонента, якого атакують

Відповідним чином отримуємо і SMS користувача, якого атакуємо. Маючи доступ до псевдобіллінговой системі, на яку вже зареєструвався наш абонент, можна отримати будь-яку інформацію, яка приходить або йде з його телефону.

Доступ до SS7 продають у даркнеті, а при бажанні можна знайти і безкоштовно. Така доступність обумовлена тим, що в мало розвинутих державах отримати статус оператора дуже просто, відповідно і отримати доступ до SS7. Так само присутні і недобросовісні працівники у операторів.

Як і в багатьох застарілих протоколах, SS7 був спроектований з мінімальною безпекою. Такі поняття, як аутентифікація і авторизація, майже не були присутні і не обговорювалися. Безпека SS7 була заснована виключно на довірі. Елементи базової мережі були побудовані відповідно з невеликими, засобами захисту від зловживання функціональністю SS7. Будучи розцінена як закрита мережа, дуже мало досліджень безпеки було зроблено для оцінки безпеки SS7. Дослідники безпеки не мали доступу до мереж SS7, і постачальники послуг мало цікавилися цією темою.

Але мережа SS7 більше не закрита. Мережеві провайдери відкривають свої Мережі SS7 для третіх осіб в рамках їх комерційних пропозицій. Мережеві елементи такі як фемтосоти виходять із закритих кордонів операторів і засновані на ненадійні місцях. Зловмисники можуть знайти свої шляхи в мережі мобільних операторів, і також можна згадати, що деякі оператори можуть бути під контролем національних держав зі зловмисними намірами зловживати такими незахищеними мережами.

Зловживання безпекою SS7 може мати серйозні наслідки - характер протоколу дозволяє отримати доступ до такої інформації, як місце розташування користувача і деталі виклику / SMS. Фінансови послуги і системи аутентифікації були побудовані на основі довіри послуг, що надаються за такими протоколами. Атаки типу «відмова в обслуговуванні», які зловживають цими ненадійними системами, можуть мати руйнівні наслідки до телекомунікаційної інфраструктури націй.

– атака відмови в обслуговуванні: зловмисник може відключити мобільні сервіси для конкретного абонента, групи абонентів, випадкових абонентів або, в деяких випадках, для всієї мережі;

– геолокація: зловмисник може виявити мобільний телефон абонента, знаючи тільки його номер телефону, з точністю до кількох метрів;

– перехоплення викликів: зловмисник може перехоплювати і записувати виклики від абонента без відома абонента або оператора;

– шахрайство за платні послуги: зловмисник може придбати роздрібні у оператора умови і здійснювати вихідні платні дзвінки, не стягуючи плату за ці дзвінки. Це може привести до значних втрат для оператора протягом короткого проміжку часу, коли націлені преміальні номера;

– шахрайство з використанням оптових СМС: зловмисник може використовувати мережу мобільного оператора для припинення або ретрансляції великої кількості оптових СМС-повідомлень. Ця практика може тривати роками непоміченими. Оператори благими намірами розгорнули брандмауери SMS, але деякі зловмисники першого покоління можуть бути обійдені зловмисниками;

– постійно з'являються додаткові зловживання, уявні все більш і більш творчими зловмисниками, які використовують такі методи, як підміна або розмиття.

2.2 Двухфакторна автентифікація

Двухфакторная аутентифікація - це додатковий рівень захисту облікового запису. Крім введення пароля, потрібно також ввести одноразовий код, який приходить на пошту або телефон; або відбиток пальця. Цим користувач підтверджує свою особистість. Коли користувач активує цю опцію, крім пароля злоумилшленніку потрібно також ввести код, щоб зайти в аккаунт користувача. Користувач також отримає повідомлення, якщо хтось спробує отримати доступ до його облікового запису.

Одноразовий код діє пару хвилин або годин, після чого він самознищується. Таким чином, завдяки двофакторної аутентифікації ваші онлайн-акаунти стають більш захищеними від кіберзлочинців.

Телефонні сигнали надходять на базові станції сусідніми вежами і передаються в мережу SS7 на несучої A. Кожна мережу SS7 має такі компоненти, як:

1) HLR (Home Location Register): містить базу даних з інформацією про абонента, такий як номер телефону, попередньо оплачений контракт, дозволу на виклик / текстові дані;

2) VLR (реєстр розташування відвідувачів): містить базу даних географічного розташування, яке близьке до місця розташування абонента.

Ці мережеві пристрої SS7 обмінюються даними від оператора A до B і навпаки, і, нарешті, вони успішно досягають іншого кінця абонента.

Але цей протокол (SS7), який використовується більше 800 глобальними телекомунікаційними компаніями, небезпечний і може бути легко зламаний хакерами.

Не існує встановленої системи безпеки, яка розгорнута в мережевому протоколі SS7. Як тільки хакер отримує доступ до мережі SS7, він / вона може:

- слухати і записувати ваші телефонні дзвінки;
- читати SMS-повідомлення, які відправлені і отримані;
- відстежувати географічне положення.

Вони також можуть легко обійти двухфакторную аутентифікацію, яка зазвичай відправляється користувачеві за допомогою SMS. Хакер, який слухає конкретну мережу, може перехопити це SMS-повідомлення і використовувати надану інформацію.

2.3 Стандарт у телекомунікаційних системах нового покоління Diameter

Мережі нового покоління 4G повсюдно набирають популярність, забезпечуючи абонентам високу якість зв'язку, а також захист переданих даних [31].

У мережах 4G на заміну SS7 прийшов протокол Diameter, за допомогою якого виконується більшість службових завдань. Проте, протокол Diameter аж ніяк не є повністю захищеним. Теоретично шахрайство, перехоплення SMS, відмова в обслуговуванні і інші загрози все ще залишаються актуальними. Більш того, абоненти мереж 4G так чи інакше залишаються абонентами мереж попередніх поколінь, оскільки більшість мобільних операторів на поточний момент використовують 4G тільки для надання доступу в інтернет, а передача SMS або голосові виклики здійснюються в режимі 3G.

Всі досліджені мережі містять критично небезпечні уразливості, що дозволяють відстежити місце розташування абонентів і викликати відмову в обслуговуванні. До ризику шахрайства відносно оператора схильна кожна третя мережу. Абоненти мереж 4G схильні до тих же загрозам, що і абоненти мереж попередніх поколінь. У мережах на основі протоколу Diameter можливі атаки, спрямовані на відмову в обслуговуванні, розкриття інформації про абонентів і мережі оператора, а також шахрайство відносно оператора. Хоча спектр атак обмежений в порівнянні з мережами попередніх поколінь, зловмисник може примусово перевести пристрій абонента в режим 3G - і проводити подальші атаки вже на менш захищену систему SS7: прослуховувати голосові виклики, перехоплювати SMS і здійснювати шахрайські схеми щодо абонентів. Для забезпечення захисту мережі необхідний комплексний підхід до безпеки. Більшість недоліків пов'язані не тільки з некоректним настроюванням або уразливими мережевого обладнання, але також з фундаментальними проблемами протоколу Diameter, для вирішення яких потрібні додаткові засоби захисту. Вкрай важливо, щоб всі заходи щодо забезпечення безпеки приймалися в комплексі і включали в себе регулярний аналіз захищеності мережі, підтримка

параметрів безпеки в актуальному стані, постійний моніторинг і аналіз сигнального трафіку, своєчасне виявлення нелегітимною активності і реагування на виникаючі загрози на ранніх стадіях (таблиця 2.1) [32].

Таблиця 2.1 – Розподіл абонентської бази операторів

Місце	Оператор	Кількість клієнтів, млн	Частка ринку, %
1	Київстар	26,5	46, 21
2	Vodafone	20,3	35,40
3	lifecell	8	13,95

2.2.1 Огляд загроз у мережах Diameter

Загальна статистика

Відносно мереж на основі сигнального протоколу Diameter зловмисник може проводити атаки с метою:

– розкриття інформації про абонента;
– розкриття інформації про мережу оператора;
– перехоплення абонентського трафіку;
– шахрайства;
– відмови в обслуговуванні.

До розкриття інформації про абонента відносяться ті атаки, які дозволяють відстежити місце розташування абонента, дізнатися деталі його профілю і визначити IMSI - унікальний ідентифікатор абонента, що потребується для проведення подальших атак. Також зловмиснику може знадобитися і інформація про мережу оператора - адреси пристроїв, конфігурація мережі.

Перехоплення абонентського трафіку (що входять SMS) в мережах 4G теоретично можливий, однак на практиці його реалізація утруднена, оскільки передача SMS часто здійснюється через мережі попередніх поколінь або із

застосуванням технологій, які не використовують протокол Diameter. Установка з'єднання при голосові дзвінки також здійснюється за допомогою інших протоколів. Зловмисник може проводити атаки з метою шахрайства для отримання безкоштовного доступу до послуг зв'язку, що означає прямі фінансові втрати для мобільного оператора.

В рамках аналізу захищеності лише невелика частина операторів зв'язку проводить тестування свого обладнання на можливість відмови в обслуговуванні, оскільки це потенційно може привести до перебоїв в роботі мобільної мережі.

Порівняємо, наскільки мережі 4G, в яких використовується сигнальний протокол Diameter, безпечніше мереж попередніх поколінь, і розглянемо частки успішних атак щодо мереж різних поколінь у таблиці 2.2.

Таблиця 2.2 - Частки вразливих мереж за типами загроз

Загроза	Мережі SS7	Мережі Diameter
Розкриття інформації про абонента	100%	100%
Розкриття інформації о мережі оператора	63%	75%
Перехоплення абонентського трафіку	89%	-
Шахрайство	78%	33%
Відмова в обслуговуванні абонентів	100%	100%

Передача SMS з використанням Diameter не провадилась. Для встановлення голосових викликів в мережах 4G використовується протокол SIP.

Як і в мережах на основі SS7, у всіх мережах, де застосовується протокол Diameter, можливі розкриття інформації про абонента і відмова в обслуговуванні абонентів. При цьому частка успішних атак, спрямованих на відмову в обслуговуванні абонентів, трохи вище. Можливо, такі результати пов'язані з тим, що оператори обізнані про існуючі проблеми безпеки в мережах SS7 і не вживають ніяких заходів для захисту.

У 75% мереж виявилося можливим розкриття інформації про мережу оператора, що дещо гірше показників для мереж попередніх поколінь. Це пояснюється тим, що серед сигнальних повідомлень протоколу Diameter, що дозволяють отримати дані про мережі оператора, вище частка тих повідомлень, які вимагають додаткових перевірок для здійснення коректної фільтрації. Ці повідомлення можуть бути отримані від будь-якого вузла, а єдиний спосіб виявити підробку - звіряти поточне повідомлення з попередніми, беручи до уваги місце розташування користувача і часовий проміжок між повідомленнями.

Поточне обладнання в більшості мереж Diameter не готове до цього - воно не дозволяє гнучко налаштувати правила фільтрації та здійснювати моніторинг відповідної активності. Оператори не бачать цих атак і, отже, не знають про те, що від них потрібно захищатися. Удвічі менше мереж виявилися схильні до ризику шахрайства. Втім, причина такого зниження частково полягає в тому, що на поточний момент відомо лише мале число атак, спрямованих на проведення шахрайських операцій в мережах Diameter, в той час як для мереж SS7 добре вивчені різні варіації таких атак (нелегітимна переадресація викликів, експлуатація USSD- запитів, маніпулювання SMS, зміна профілю абонента). Як показують дослідження, в мережах 4G існує можливість перехоплення SMS абонентів. Однак у всіх мережах, для яких проводився аналіз захищеності, при передачі SMS пристрої абонентів або переключалися в режим 3G (де використовується сигнальна система SS7), і відповідно, провести тестування нової технології було неможливо, або використовувалися методи передачі SMS, що не дозволяють здійснити перехоплення повідомлень .

Надалі, з впровадженням IMS (і, відповідно, технологій VoLTE / VoWiFi), передача SMS може здійснюватися з використанням протоколу SIP замість протоколу Diameter, тому атаки, спрямовані на перехоплення трафіку абонентів, потенційно можуть бути ускладнені. В процесі встановлення голосових викликів пристрою абонентів також перемикаються в режим 3G, рідше застосовується протокол SIP. Витік інформації про абонента Приватність абонентів залишається під загрозою навіть в мережах Diameter. Відстежити місце розташування

абонента вдавалося в 38% випадків. Для мереж SS7 цей показник становив 33%. Успішними були й переважна більшість спроб розкрити деталі профілю абонента.

У той же час дізнатися IMSI абонента вдавалося набагато рідше - всього в 7% випадків, і це пов'язано з більш безпечної конфігурацією досліджуваних мереж: невикористовувані в роумінгу інтерфейси не були доступні з зовнішньої IPX-мережі. Цей показник дуже важливий з точки зору безпеки; IMSI потрібно для проведення інших видів атак, тому зниження ймовірності розкриття ідентифікаторів впливає і на можливість реалізації інших загроз. Проте варто враховувати, що отримати IMSI абонента можливо і іншими способами, наприклад шляхом експлуатації вразливостей мережі SS7, за допомогою підроблених базових станцій і навіть використовуючи спеціальні сервіси в інтернеті. У всіх випадках розкрити IMSI виходило за допомогою повідомлення Sh UDR (User-Data-Request), яке використовується сервером додатків для запиту різних даних про абонента з HSS. Інший потенційний метод атаки - за допомогою повідомлення S6c SRR (Send-Routing-Info-for-SM-Request), призначеного для отримання інформації, необхідної для маршрутизації вхідних повідомлень - не був успішний в жодній дослідженій мережі. Некоректна настройка мережевого обладнання і, в окремих випадках, недостатньо ефективна фільтрація сигнальних повідомлень дозволяли відстежити місце розташування користувачів за допомогою методів Sh UDR і S6a IDR (InsertSubscriber-Data-Request). Повідомлення S6a IDR призначене для отримання HSS поточної інформації про місцезнаходження абонента з MME. Зловмисник може сфабрикувати підроблені повідомлення, видавши себе за легітимне обладнання роумінг-партнера. Повідомлення SLg PLR (Provide-Location-Request), яке використовується GMLC для запиту інформації про місцезнаходження абонента з MME, було заблоковано мережею оператора в кожному випадку і не дозволило отримати потрібні дані.

Витік інформації про оператора Інформація про мережу оператора - структура мережі, адреси та функціональність мережевих пристроїв - також служить вихідними даними для проведення інших атак з метою шахрайства,

перехоплення трафіку, відмови в обслуговуванні абонентів або обладнання. У зв'язку з тим, що вкрай складно відрізнити фальшиве повідомлення S6a AIR від легітимного, за допомогою цього методу необхідну інформацію вдавалося отримати в 88% випадків. Метод SLh RIR (LCS-Routing-Info-Request), навпаки, не приводив до потрібних результатів: всі повідомлення були заблоковані завдяки корректно налаштованою фільтрації. Шахрайство У мережах Diameter можливе проведення атак, що дозволяють безкоштовно користуватися послугами зв'язку. Існують два різновиди таких атак, кожна з яких заснована на зміні профілю абонента.

Перший варіант - модифікація параметрів тарифікації, що зберігаються в профілі абонента, - досить складно реалізуємо на практиці, оскільки вимагає від зловмисника знань про пристрій мережі оператора. Значення цих параметрів не стандартизовані і залежать від конкретного оператора, а отримати їх з профілю абонента не вдавалося ні в одній досліджуваній мережі. Інший варіант атаки - використання сервісів в обхід встановлених обмежень, яке завдає оператору прямий фінансовий збиток. Інформація про профіль абонента і обмеженнях передається в MME за допомогою повідомлення S6a IDR. Видаючи себе за HSS, зловмисник може відправити спеціально сформований повідомлення, яке дозволить зняти встановлені заборони на надання послуг. В результаті зловмисник отримає можливість необмежено користуватися послугами, не передбаченими його тарифним планом, і не залишиться без зв'язку навіть в тому випадку, якщо у нього закінчилися гроші на рахунку і оператор відключив його від мережі. Такі атаки були успішні в 20% випадків. Зловмисник може не тільки самостійно користуватися такою можливістю, але і продавати подібні послуги третім особам.

На даний момент оператори зв'язку приймають лише мінімальні заходи захисту щодо сигнальних мереж Diameter. Можливо це відбувається через те, що оператори не в повній мірі усвідомлюють існуючі проблеми безпеки і пов'язані з ними ризики в мережах нового покоління, вони впевнені в тому, що протокол Diameter досить захищений від атак на відміну від застарілої системи SS7.

Спеціальне обладнання, призначене для моніторингу сигнального трафіку, яке дозволило б помітити атаки, просто відсутня в досліджуваних мережах. Роблячи тільки окремі кроки щодо захисту, оператори не мають повного уявлення про ситуацію і вважають, що їх мережа являє собою безпечне середовище, вважаючи установку дорогого додаткового обладнання зайвою.

Для забезпечення захисту від розглянутих в даному звіті атак необхідний комплексний підхід до безпеки, що також відображено в рекомендаціях GSMA в документі FS.19 Diameter Interconnect Security. В першу чергу, слід регулярно проводити аналіз захищеності мобільної мережі для виявлення вразливостей, оцінки поточного рівня захищеності і потенційних ризиків, вироблення захисних заходів і перевірки їх ефективності. Важливо підтримувати параметри безпеки в актуальному стані і проводити аналіз захищеності при будь-яких змінах в мережі, наприклад при зміні конфігурації або впровадженні нового обладнання.

Крім того, необхідний постійний моніторинг і аналіз сигнальних повідомлень, що перетинають кордони мережі, для своєчасного виявлення нелегітимною активності і реагування на виникаючі загрози безпеки на самій ранній стадії. Спеціальні системи виявлення атак дозволяють виконувати аналіз сигнального трафіку в режимі реального часу і проводити блокування небажаних повідомлень без ризику порушення доступності абонентів - або передавати інформацію про інциденти безпеки додатковим системам захисту.

Незважаючи на всі механізми захисту, закладені в протокол Diameter, в досліджених мережах виявилися можливими атаки щодо абонентів і самого оператора. Зловмисник може простежити місце розташування абонента, викликати відмову в обслуговуванні, залишивши тисячі користувачів без зв'язку, або перевести пристрій абонента в режим роботи 3G, щоб скористатися численними уразливостями SS7.

Таким чином, абоненти мереж 4G мають ті ж уязвимості, що і абоненти мереж попередніх поколінь. Чи не захищені і оператори: зловмисники можуть отримувати безкоштовний доступ до послуг зв'язку, що веде до серйозних фінансових втрат.

Виявлені уразливості пов'язані як з недоліками настройки мережевого обладнання та механізмів фільтрації, які усуваються відносно легко, так і з фундаментальними проблемами протоколу Diameter, для вирішення яких необхідне спеціальне додаткове обладнання. При цьому обізнаність операторів про існуючі загрози поки невисока, а значить, приймаються лише мінімальні заходи захисту, які є недостатніми для забезпечення безпечної та безперебійної роботи мобільної мережі.

2.4 Перехоплення SMS-повідомлень у стандарті Diameter

Дана атака дуже небезпечна для абонентів в контексті двофакторної аутентифікації, в основі якої лежить підтвердження операцій через SMS, в тому числі при роботі з інтернет-банкінгом. Скориставшись даною вразливістю, зловмисник зможе вкрасти гроші користувача з рахунку, при цьому для банку це буде виглядати як легітимне дію клієнта з використанням двофакторної авторизації. Користувачеві в такому випадку практично неможливо оскаржити транзакцію.

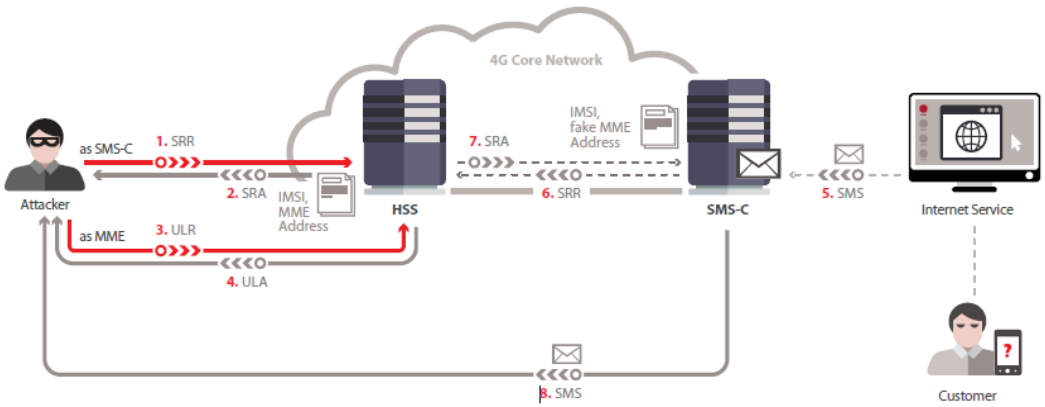

Рисунок 2.6 – Схема перехоплення SMS зловмисником

В основі атаки з перехоплення SMS-повідомлень в мережі на основі Diameter лежить ідея аналогічної атаки, проведеної в мережах на базі SS7.

Зловмисник, заздалегідь знаючи номер абонента MSISDN і діючи як SMS-центр, надсилає запит SRR на HSS, у відповідь на який отримає інформацію, в якій містяться IMSI абонента і відомості про MME, який в даний момент обслуговує атакується користувача.

Потім, виступаючи в ролі MME, атакуючий посилає запит ULR (Update-Location-Request) на HSS і в разі успіху отримує відповідну відповідь ULA (Update-Location-Answer).

Тоді в HSS буде зберігатися оновлена інформація, що атакується користувач обслуговується на підставну MME і пов'язаний з SMS-центром зловмисника.

Варто відзначити одну важливу особливість протоколу Diameter, серед іншого сприяє реалізації цієї атаки. Відповідь на запит завжди повертається тому вузлу, який його послав, незалежно від того, яка інформація була вказана в парі ОРИГИН-Host.

Далі атакуючий може спровокувати відправку SMS для відновлення пароля в будь-якому сервісі (соціальна мережа, месенджер і т. П.) Або для підтвердження грошового переказу через систему ДБО.

SMS-центр оператора запитує у HSS інформацію про MME, який обслуговує

атакується користувача. HSS відповідає інформацією про те, що користувача обслуговують підставні MME і SMS-центр. Потім SMS-повідомлення з конфіденційними даними

користувача відправляється на підставний SMS-центр, підконтрольний зловмисникові.

Використовуючи код підтвердження з отриманого SMS-повідомлення, атакуючий в одному випадку може отримати повний доступ до даних профілю користувача в соціальній мережі

і особистому листуванні, провести зміну пароля для входу, а також розмістити від імені користувача інформацію, яка може завдати шкоди його репутації. В іншому випадку зловмисник через систему ДБО може отримати

доступ до управління банківським рахунком користувача і зробити розкрадання наявних на ньому коштів.

Факт перехоплення SMS-повідомлень абонент може визначити тільки за непрямими ознаками. Зокрема, якщо на нього виробляється подібна атака, він не буде отримувати ніяких вхідних SMS-повідомлень.

2.5 Вразливості наскрізного шифрування

2.5.1 Атака «людина посередині»

Наскрізне шифрування передбачає, що контроль за листуванням здійснюється безпосередньо користувачами. Одним з варіантів обходу наскрізного шифрування для зловмисника є захоплення під свій контроль каналу зв'язку між кінцевими точками, після цього він може спробувати видати себе за одержувача повідомлення, щоб, наприклад, підмінити відкритий ключ. Щоб не дати себе виявити, зловмисник після дешифрування повідомлення може зашифрувати його ключем, який він розділяє з фактичним одержувачем, або його відкритим ключем (у разі асиметричних систем) і знову відправити повідомлення. Атаки такого типу прийнято називати атаками «людина посередині» [35].

Для запобігання MITM-атак більшість криптографічних протоколів використовують аутентифікацію. Для цього можуть використовуватися, наприклад, центри сертифікації. Альтернативним методом є створення відбитків відкритого ключа на основі загальнодоступних відкритих ключів користувачів або загальних секретних ключів. Перш ніж почати розмову, сторони порівнюють свої відбитки відкритих ключів з використанням зовнішнього каналу зв'язку, який гарантує цілісність і автентичність зв'язку, при цьому він не обов'язково повинен бути секретним. Якщо відбитки ключів збігаються, значить атака «людина посередині» не була проведена.

2.5.2 Безпека кінцевих точок

Іншим способом обходу наскрізного шифрування є атака безпосередньо на кінцеві точки доступу [8]. Кожен пристрій користувача може бути зламано, з метою вкрасти криптографічний ключ (для створення атаки «людина посередині») або просто прочитати дешифровані повідомлення користувачів. Для уникнення такого роду спроб злому, необхідно забезпечити відповідний захист призначених для користувача пристроїв за допомогою програмних або інших методів. Основними спробами підвищити безпеку кінцевих точок були виділення ключових операцій генерації, зберігання та криптографії на смарт-карту, наприклад, в Project Vault Google. Проте, так як введення і виведення відкритого тексту видно в системі, то ці підходи не здатні захистити від клавіатурних шпигунів і шкідливого програмного забезпечення, яке може відстежувати розмови в режимі реального часу. Більш надійний підхід полягає у фізичній ізоляції пристрої

2.5.3 Вразливості програмного забезпечення

Компанії можуть також (самостійно або з примусу) впроваджувати в своє програмне забезпечення бекдори, які допомагають порушити узгодження ключа або обійти шифрування. Згідно з інформацією, розкритою Едвардом Сноуденом в 2013 році, Skype містив бекдор, який дозволяв Microsoft передавати в АНБ повідомлення користувачів, незважаючи на те, що офіційно ці повідомлення піддавалися наскрізного шифрування [8].

2.6 Вразливості десктопніх версій мессенджерів

Signal - це мессенджер, який гарантує усім користувачам повне шифрування їх переписок, але не може забезпечити необхідний захист під час оновлення свого розширення для браузеру Chrome на десктопній версії, оскільки

експортує повідомлення користувача у вигляді незашифрованих текстових файлів [35] . При експорті діалогів на диск Signal формує окремі папки, іменовані по імені і телефонним номером контактів. Весь вміст діалогів зберігається в форматі JSON відкритим текстом (рис 2.6). Ніяких попереджень про те, що інформація розшифровується і зберігається на диск, програма не виводить. Цей момент і є ключовим для загрози витоку конфіденційних даних.

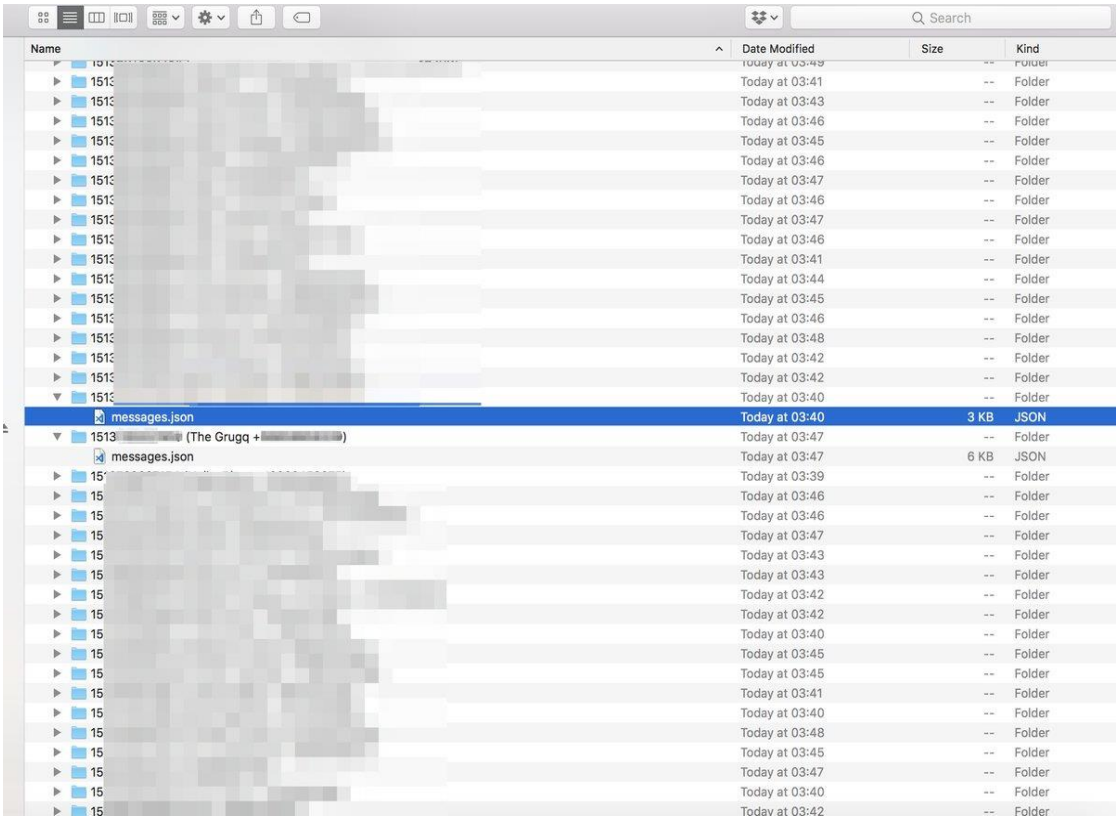

Рисунок 2.6 – Демонстрація можливості читання переписки через файлову систему для браузеру Chrome на десктопній версії macOS.

Метью Сюіш знайшов проблему на macOS, коли отримав сповіщення про оновлення розширення Signal для Chrome. У тестах BleepingComputer робився на Linux Mint з кількома тестовими обліковими записами, ми спостерігали однакову поведінку [36].

Під час тестування Метью Сюіш не бачив жодного попередження про збереження даних у незашифрованому вигляді. Також інформація зберігається на диску навіть після того, як оновлення завершиться, і новий Signal імпортує

його. Користувачі повинні видалити папки вручну, щоб знизити ризик витоку їх приватних розмов.

Найгірше ж у цій ситуації - незашифровані повідомлення залишаються на диску навіть після завершення апгрейда, і видаляти їх доведеться вручну. Метью Сюіш виявив цей небезпечний баг при роботі в macOS.

Подібна ситуація також була помічена у десктопній версії мессенджеру Telegram у кінці 2018 року. Натаніэль Сачі знайшов вразливість на десктопній версії Telegram [37].

Сачі отримав доступ до власних повідомлень та картинок, вивчаючи бази даних, які зберігаються на диску комп'ютера. Інформація виявилася важкою для читання, але не зашифрованою. Також він видмітив, що доступ до неї можна отримати навіть якщо був поставлений пароль встановлений пароль.

Довірені дані Сачі також знайшли іменів і номерів телефонів учасників переписок, які можна встановити.

2.7 Втрата або тривале невикористання SIM-карти

У більшості популярних мессенджерів реєстрація у її додатку їде виключно через мобільний номер (WhatsApp, Telegram, Viber та інші). Але є невеликий нюанс у тому, що якщо користувач перестане поповнювати свій мобільний рахунок, або втратить телефон разом із SIM-картою, оператор через деякий час поверне мобільний номер до себе да зможе перепродати його іншому користувачу.

Таким чином, новий власник цієї SIM-карти зможе при установці мессенджерів потрапити до аккаунтів старого користувача, якщо він не робив переноса своїх даних на новий номер телефону.

Таким чином, якщо подібні SIM-карти зможуть потрапити до рук зловмисника, він може вкрасти усі конфіденційні дані минулого користувача та використати їх у своїх інтересах.

2.8 Висновки по аналізу сучасних загроз у мессенджерах

Хоч у майже кожному сучасному мессенджері є коритсні функції з безпеки, такі як наскрізне шифрування та секретні чати, від проблем із існуючим протоколом Sighaling System 7, навмисно залишеними вразливостями програмного забезпечення самими компаніями це не врятує.

Нажаль, проблема із протоколом SS7 повністю обертає функцію двухфакторної автентифікація проти самого користувача мессенджеру та любих інших додатків.

Самою великою загрозою для безпеки користувачів, крім самих компаній-розробників, є саме протокол по передачі кодів для двухфакторної автентифікації для користувачів.

Доки його не буде змінено, або покращено, всі популярні месенджери і інші додатки будуть під загрозою, так як перехопити дане повідомлення може будь-який зловмисник з мінімальною підготовленістю.

3. МЕТОДИ ЗАХИСТУ У СУЧАСНИХ МЕССЕНДЖЕРАХ

3.1 Актуальність функцій безпеки у мессенджерах

Вимоги до рівня захисту інформації почали зростати зі збільшенням кількост атак від зловмисників не тільки на великі технологічні компанії, але і на рядових користувачів. Після викриття Сноуденом фактів прослуховування спецслужбами пересічних громадян США все, хто користуються мобільними мессенджерами, відразу стали приділяти увагу особистій безпеці даних і захисту інформації. Саме тому на ринку з'явився ряд месенджерів, які використовують повне або часткове шифрування повідомлень, файлів, фотографій або відео, які ви пересилаєте іншим людям.

Крім власне шифрування, також з'явилася опція самознищення повідомлень і цілих чатів і навіть блокування можливостей для скріншотів. Месенджери Wickr, Wiper і ряд аналогів пропонують саме такі суперможливості.

3.2 Двухфакторна автентифікація

Багатофакторна автентифікація (БФА, multi-factor authentication,) - розширена автентифікація, метод контролю доступу до комп'ютера, в якому корістувачеві для Отримання доступу до информации необходимо пред'явити более одного «доказу механізму автентифікації» [38].

Відповідно до думки експертів, багатофакторна автентифікація різко зніжує можлівість крадіжкі особістом Даних.

Тім не менше, багатофакторні підході автентифікації залішаються уразливостей для атак «фішінгу», «людина-в-браузері», «людина посередіні».

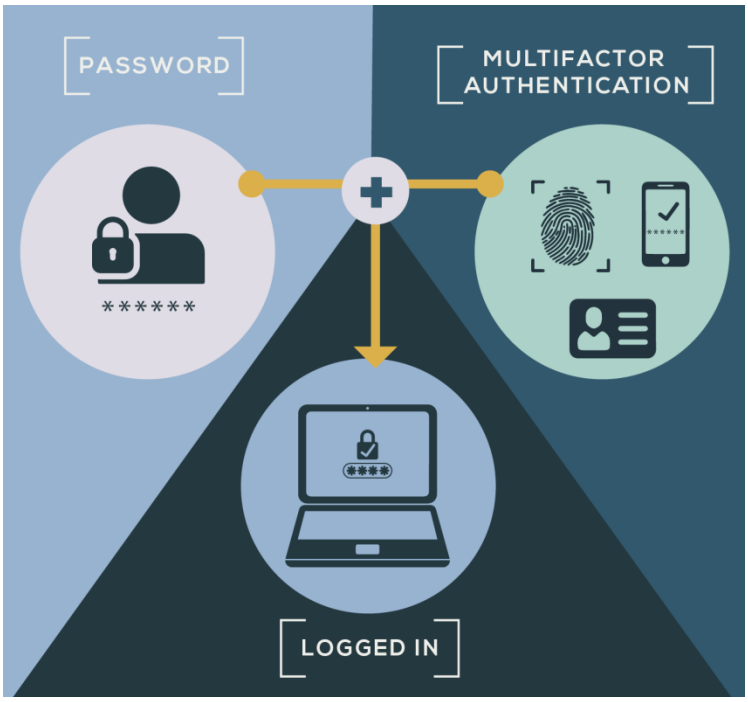

Рисунок 3.1 – Схема роботи двухфактороной автентифікації

Методам захисту, Заснований на методиках багатофакторної автентифікації, сегодня довіряє велика Кількість зарубіжніх компаний, среди якіх организации IT, фінансового и страхового секторів Сайти Вся, Великі банківські установи та підприємства держсектора, незалежні експертні организации, Дослідницькі фірми.

Метод контролю доступу, що вимагає одночасної наявності двох компонентів з боку користувача. Крім традиційних логіна і пароля, принцип двухфакторную передбачає підтвердження особи користувача за допомогою того, що у нього є. Це може бути: смарт-карта, токен, OTP-брелоки, біометричні датчики і так далі. Найчастіше для другого етапу ідентифікації використовується мобільний телефон, на який надсилається одноразовий код доступу.

Також в якості другого ідентифікатора можуть бути використані біометричні дані людини: відбиток пальця, райдужна оболонка ока і т.п. У системах контролю доступу для цього використовуються комбіновані (мультиформатні) зчитувачі, які працюють і з різного роду картами, і з біометричними параметрами користувачів.

3.3 Наскрізне шифрування (end-to-end encryption)

Наскрізне шифрування (також кінцеве шифрування; англ. End-to-end encryption) - спосіб передачі даних, в якому тільки користувачі, які беруть участь в спілкуванні, мають доступ до повідомлень. Таким чином, використання наскрізного шифрування не дозволяє отримати доступ до криптографічних ключів з боку третіх осіб [8].

Для обміну ключами можуть бути застосовані симетричний і асиметричний алгоритми. Наскрізне шифрування передбачає, що ключі шифрування відомі тільки спілкується між собою сторонам. Для реалізації даної умови може бути використана схема з попередніми поділом секрету або, наприклад, протокол Діффі-Хелмана, який використовується в месенджерах WhatsApp і Telegram.

Наскрізне шифрування гарантує, що доступ до вихідного тексту повідомлення є тільки у відправника і одержувача. Це означає, що призначена для користувача інформація стає недоступною навіть серверів, передає дані (рис 2.7).

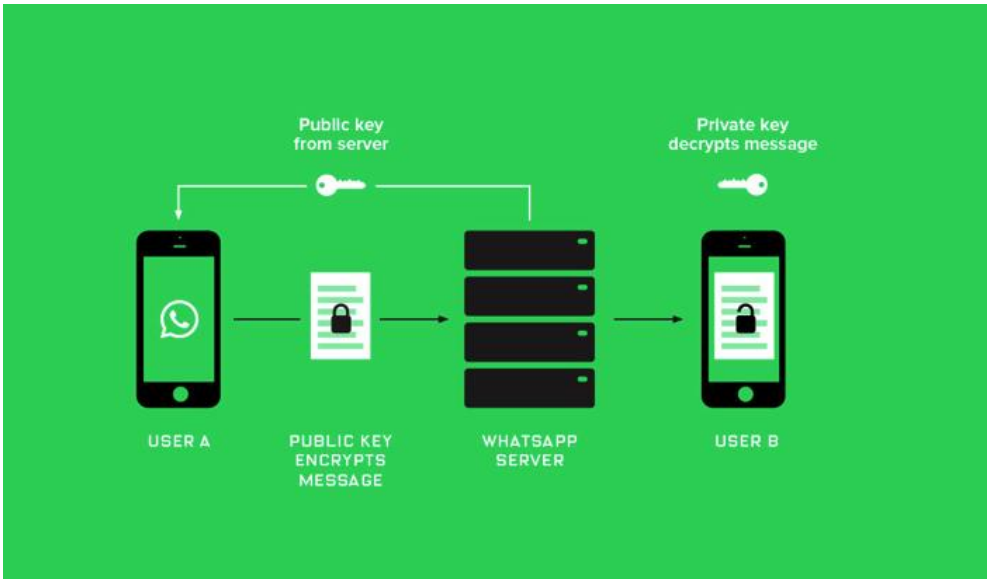

Рисунок 2.7 – Схема роботи наскрізного шифрування

Шифрування і дешифрування відбувається на кінцевих пристроях користувачів. Крім того, дані залишаються зашифрованими, поки не будуть доставлені до місця призначення. Тому часто наскрізне шифрування також називають «нульовий доступ» або «шифрування на стороні клієнта». Однак, слід розрізняти кінцеве шифрування при передачі даних і шифрування на стороні клієнта при зберіганні даних.

3.4 Протокол MTProto у мессенджері Telegram

Протокол призначений для доступу до серверного API з додатків, запущених на мобільних пристроях. Підкреслимо, що інтернет-браузер не вважається таким додатком [15].

Протокол розбитий на три майже незалежні частини(рис 2.8):

– Високорівнева частина (мова запитів до API) - визначає, яким чином запити до API і відповіді на ці запити перетворюються в двійкові повідомлення.

– Криптографічна (авторизаційної) прошарок - визначає, яким чином повідомлення шифруються перед передачею через транспортний протокол.

– Транспортна частина - визначає, яким чином передаються повідомлення між клієнтом і сервером поверх будь-якого іншого існуючого мережевого протоколу (наприклад, http, https, tcp, udp).

Кожне текстове повідомлення, яке потрібно зашифрувати через MTProto, завжди містить такі дані, які перевіряються розшифровкою, щоб зробити систему стійкою проти відомих проблем з компонентами:server salt (64-битная)

– session id
– message sequence number
– message length
– time

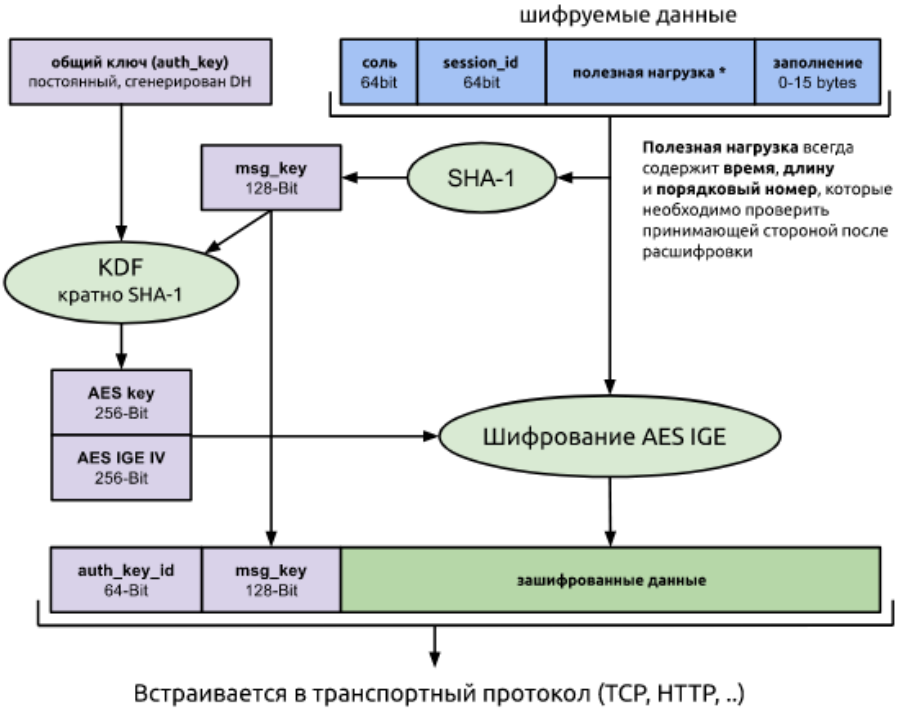

Рисунок 2.8 – Шифрування у протоколі MTProto

3.4.1 Короткий огляд компонентів

Високорівнева частина (мова RPC-запитів / API)

З точки зору високорівневою частини, клієнт і сервер обмінюються повідомленнями в рамках деякої сесії. Сесія прив'язана до клієнтського пристрою (вірніше, з додатком), але не до конкретного http / https / tcp-з'єднанню. Крім того, кожна сесія прив'язана до ідентифікатора користувача ключа, за яким фактично проводиться авторизація.

Може бути відкрито декілька з'єднань до сервера; повідомлення в ту чи іншу сторону можуть йти з будь-якого з них (відповідь на запит не зобов'язаний прийти по тому ж з'єднанню, за яким був відправлений сам запит, хоча найчастіше це так, а проте ні в якому разі повідомлення не може бути повернуто в з'єднанні, що належить іншій сесії). При використанні UDP-протоколу може статися, що відповідь на запит приходить не з того IP, на який був відправлений запит.

Повідомлення бувають декількох типів:

– RPC-виклики (від клієнта до сервера) - звернення до методів API

– RPC-результати (від сервера до клієнта) - результати RPC-викликів

– Підтвердження прийому повідомлень (вірніше, повідомлення про стан набору повідомлень)

– Запит стану повідомлень

– Складені повідомлення або контейнер (контейнер, що містить кілька повідомлень, чи потрібен, наприклад, щоб по HTTP-з'єднання можна було відправити кілька RPC-викликів відразу; крім того, контейнер може підтримувати gzip).

– З точки зору протоколів більш низького рівня, повідомлення - це потік двійкових даних, вирівняний по межі 4 або 16 байтів. Перші кілька полів повідомлення фіксовані і використовуються системою криптографії / авторизації.

– Кожне повідомлення, окреме або всередині контейнера, складається з ідентифікатора повідомлення (64 біта; див. Нижче), порядкового номера повідомлення в сесії (32 біта), довжини (тіла в байтах; 32 біта) і тіла (будь-який розмір, кратний 4 байтам). Крім того, при відправці контейнера або одиночного повідомлення, в його початок дописується внутрішній заголовок (див. Нижче), після чого все це шифрується, і в початок зашифрованого повідомлення додається зовнішній заголовок (64-бітний ідентифікатор ключа і 128-бітний ключ повідомлення).

Зокрема, кожної RPC-функції відповідає свій тип повідомлення. Більш детально читайте в статті про двійкову серіалізацію даних і службові повідомлення.

Всі числа записуються як little-endian. Однак дуже великі числа (2048-бітові), які використовуються в RSA і DH, записуються як big-endian, тому що так робить бібліотека OpenSSL.

Перед передачею повідомлень (або складових повідомлень) по мережі за допомогою транспортного протоколу вони шифруються певним чином; при цьому перед повідомленням приписується зовнішній заголовок: 64-бітний ідентифікатор ключа (однозначно визначає авторизаційний ключ для сервера, а

також користувача) і 128-бітний ключ повідомлення. Призначений для користувача ключ разом з ключем повідомлення визначають реальний 256-бітний ключ, яким і зашифровано повідомлення за допомогою шифру AES-256. Початок тіла незашифрованого повідомлення містить деякі дані (сесію, ідентифікатор повідомлення, порядковий номер повідомлення в сесії, серверну сіль); ключ повідомлення повинен збігатися з молодшими 128 бітами SHA1 від тіла повідомлення (включаючи сесію, ідентифікатор повідомлення і т.п.). Складові повідомлення шифруються як єдине ціле.

Основний недолік протоколу - в тому, що зловмисник, пасивно перехоплює повідомлення, а потім якимось чином залучив авторизаційний ключ (наприклад, вкравши пристрій) отримає можливість розшифрувати всі перехоплені повідомлення post factum. Ймовірно, це не дуже серйозно (вкравши пристрій, можна отримати і всю закешировалася на ньому інформацію, нічого не розшифровуючи), однак для подолання цих проблем можна зробити наступне:

Сесійні ключі, які генеруються по протоколу Діффі-Хелмана, і використовуються спільно з авторизаційним ключем і ключем повідомлення для вибору параметрів AES. Для їх створення клієнт повинен першим дією після створення нової сесії відправити сервера спеціальний RPC-запит («згенерувати сесійний ключ»), сервер відповість на нього, після чого всі наступні повідомлення сесії шифруються з урахуванням і сесійного ключа.

Захищати ключ, що зберігається на клієнтському пристроєм, (текстовим) паролем; цей пароль ніколи не зберігається в пам'яті і вводиться користувачем під час запуску програми або частіше (в залежності від налаштувань програми).

Дані, що зберігаються (кешувального) на призначеному для користувача пристрої, можна також захищати, шифруючи за допомогою авторизационного ключа, який, в свою чергу, треба захистити паролем. Тоді без введення пароля неможливо буде отримати доступ навіть до цих даних.

Якщо час на клієнті сильно відрізняється від часу на сервері, може так статися, що сервер почне ігнорувати повідомлення клієнта, або навпаки, через некоректне значення ідентифікатора повідомлення (яке тісно пов'язане з часом

створення). У таких ситуаціях сервер шле клієнту спеціальне повідомлення з правильним часом, містять, крім нього, якусь 128-бітну сіль (або явно надіслану клієнтом в спеціальному RPC-запиті синхронізації, або рівну ключу останнього повідомлення, отриманого від клієнта в рамках даної сесії). Таке повідомлення може бути першим в контейнері, що містить і інші повідомлення (якщо рассинхронизация істотна, але ще не призводить до ігнорування клієнтських повідомлень).

При отриманні такого повідомлення (або містить його контейнера) клієнт спочатку виконує синхронізацію часу (фактично всього лише запам'ятовує різницю свого і серверного часу, щоб вміти надалі обчислювати «правильне» час), а потім перевіряє ідентифікатори повідомлень на коректність.

У запущених випадках клієнту доведеться згенерувати нову сесію, щоб забезпечити монотонність ідентифікаторів повідомлень.

Дозволяє доставляти вже зашифровані контейнери разом із зовнішнім заголовком (надалі - корисне навантаження) від клієнта до сервера і навпаки. Є три типи транспорту:

- HTTP
- TCP
- UDP

Реалізується поверх HTTP , запущеного поверх класичного TCP-порту 80. HTTPS не використовується; використовується криптографічний схема, пояснена вище.

HTTP-з'єднання прив'язується до сесії (вірніше, сесії + ідентифікатором ключа), зазначеної в останньому прийшов запиті; зазвичай у всіх запитах сесія однакова, однак хитрі HTTP-проксі можуть це зіпсувати. Сервер може повернути повідомлення в HTTP-з'єднання тільки в тому випадку, якщо воно належить тій же сесії, і якщо зараз чергу сервера (був отриманий HTTP-запит від клієнта, на який ще не був відправлений відповіді).

Загальна схема така. Клієнт відкриває одне або кілька keepalive HTTP-з'єднань до сервера. При необхідності відправлення одного або декількох

повідомлень з них складається корисне навантаження, після чого робиться POST-запит на URL / api, як даних якого і передається корисне навантаження. Крім того, допускаються HTTP-заголовки Content-Length, Keepalive, Host.

Після отримання запиту сервер може або почекати трохи (якщо запит на увазі відповідь після невеликого очікування), або відразу повернути фіктивний відповідь (що повідомляє лише про те, що контейнер був отриманий). У будь-якому випадку у відповіді може виявитися скільки завгодно повідомлень - сервер має право заодно відправити будь-які накопичилися у нього повідомлення для цієї сесії.

Крім того, є спеціальний longpoll RPC-запит (дійсний тільки для http-з'єднань), в якому передається максимальний час очікування T. Якщо у сервера є повідомлення для цієї сесії, вони повертаються відразу ж; в іншому випадку відбувається очікування до тих пір, поки у серверу не з'явиться повідомлення для клієнта, або не пройде T секунд. Якщо за T секунд не відбулося ніяких подій, повертається фіктивний відповідь (спеціальне повідомлення).

Якщо серверу треба відправити повідомлення клієнту, він перевіряє, чи немає HTTP-з'єднання, що належить потрібної сесії, і що знаходиться в стані «виконання HTTP-запиту» (включаючи long poll), після чого повідомлення додається в контейнер відповіді цього з'єднання і відправляється користувачеві. У типовому випадку відбувається невелике додаткове очікування (50 мілісекунд), на той випадок, якщо у сервера незабаром з'являться ще повідомлення для цієї сесії.

Якщо жодного підходящого HTTP-з'єднання немає, повідомлення ставляться в чергу відправки для даної сесії. Втім, вони туди потрапляють в будь-якому випадку, поки явно або опосередковано не підтверджено отримання клієнтом. Для http-протоколу неявним підтвердженням вважається відправка наступного запиту за тим же HTTP-з'єднання (вже немає - і для HTTP-протоколу необхідно надсилати явні підтвердження); в інших випадках клієнт повинен надіслати явне підтвердження за розумний час (його можна додати в контейнер для наступного запиту).

Важливо: якщо підтвердження вчасно не прийшло, повідомлення може бути перепослано (можливо, в складі іншого контейнера). Сторони повинні бути морально готові до цього і зберігати ідентифікатори останніх отриманих повідомлень (і ігнорувати такі дублі, а не повторювати дію). Для того, щоб не зберігати ідентифікатори вічно, є спеціальні повідомлення збірки сміття, які експлуатують монотонність ідентифікаторів повідомлень.

Якщо чергу відправки переповнюється, або повідомлення чекають в ній більше 10 хвилин, то сервер їх забуває (або відправляє в своп - дурне діло нехитре). Це може статися і швидше, якщо у сервера закінчуються буфери (наприклад, через серйозних проблем в мережі, що призвели до розриву великої кількості з'єднань).

Дуже схожий на HTTP-транспорт, може бути реалізований теж на порт 80 (щоб проходити всі фаєрволи) і навіть на ті ж ip-адреси серверів. У цьому випадку сервер розуміє, чи потрібно використовувати HTTP або TCP-протокол для даного з'єднання по перших чотирьох прийшли байтам (для HTTP це буде POST).

При створенні TCP-з'єднання воно приписується сесії (і авторизаційному ключу), переданому в першому повідомленні користувача, і потім використовується виключно для даної сесії (схеми мультиплексування не допускаються).

Повною і в скороченій версії протоколу є підтримка швидких підтверджень. У цьому випадку клієнт встановлює старший біт довжини в пакеті із запитом, а сервер відсилає у відповідь спеціальні 4 байта, що представляють собою самостійний пакет. Вони являють собою старші 32 біта SHA1 від зашифрованої частини пакета, з встановленим старшим бітом, щоб було зрозуміло, що це не довжина звичайного пакета з відповіддю сервера; якщо використовується скорочена версія, то до цих чотирьох байтів застосовується bswap.

Неявних підтверджень для TCP-транспорту не буває: всі повідомлення повинні бути явно підтверджені. Найчастіше підтвердження поміщаються в

контейнер разом з наступним запитом або відповіддю, якщо він відправляється незабаром. Наприклад, це майже завжди так для повідомлень від клієнта, що містять RPC-запити: підтвердження зазвичай приходить разом з RPC-відповіддю.

У разі виникнення помилки сервер може надіслати пакет, корисне навантаження якого складається з 4 байтів - коду помилки. Наприклад, код помилки -403 відповідає ситуацій, в яких через HTTP-протокол повернулася б відповідна HTTP-помилка.

4. МЕТОДИКА ПОШУКУ ЗАХИЩЕННОГО МЕССЕНДЖЕРУ

4.1 Аналіз існуючих мессенджерів із функціями безпеки

У ході виконання роботи було розглянуто більш десятка різних за популярністю мессенджерів із різним набіром функцій по забезпеченню безпеки конфіденційної інформаціх користувачів.

У усіх із них є наскрізне шифрування, у багатьох є функція секретнів чатів. Але тількі у мессенджерів із меншою популярністю самий цікавий набір функцій для збереження особистості та конфіденційної інформації своїх користувачів.

4.2 Метод пошуку найзахищенішого мессенджеру

У ході аналізу буде обрано шість мессенджерів популярних за різними показниками та провірени на більше двух десятків питань, з отвітів на які можно будет винести рішення який із мессенджерів можно вважати найбільш захищеним для користування та збереження конфіденційної інформації.

Для пошуку будуть використані статті та звіти з безпеки у період з 2017 по 2019 роки.

4.3 Мессенджери

Для порівняння було обрано шість популярних месенджерів, які можна розділити на дві категорії:

1) Найзахищеніши серед популярних у всьому світі:
   - WhatsApp
   - Viber
   - Telegram

2) Найзахищеніши серед менш популярних:

– Signal

– Threema

– Wickr

Останні три вважаються достатньо захищеними на думку фахівців из захисту інформації та компаній, які займаються аудитом із пошуку вразливостей у подібних додатках.

4.4 Таблиця порівнянь месенджерів по критеріям

Таблиця 4.1- Порівняння месенджерів за критеріями

Критерії	WhatsApp	Viber	Telegram	Signal	Threema	Wickr
Чи захищає додаток повідомлення та медіа?	Ні	Ні	Ні	Так	Так	Ні
Юрисдикція компанії	США	Люксем-бург та Японія	США Британія Беліз	США	Швейцарія	США
Спрямоване надання даних клієнтів розвідувальним агенціям?	Так	Ні	Ні	Ні	Ні	Ні
Можливість спостереження вбудована в додаток?	Ні	Ні	Ні	Ні	Ні	Ні

Продовження таблиці 4.1

Критерії	WhatsApp	Viber	Telegram	Signal	Threema	Wickr
Чи надає компанія звіт про прозорість?	Так	Ні	Ні	Так	Так	Так
Загальна позиція компанії щодо конфіденційності клієнтів	Ні	Ні	Ні	Так	Так	Так
Фінансування	Facebook	Rakuten	Павло Дуров	Фонд "Свобода преси", "Найт" та інші	Користувач платить	Гілман Луї, Juniper Networks та інші
Компанія збирає дані клієнтів?	Так	Так	Так	Ні	Ні	Ні
Чи шифрування ввімкнено за замовчуванням?	Так	Так	Ні	Так	Так	Так
Додаток та сервер повністю відкриті?	Ні	Ні	Ні	Так	Ні	Ні
Чи є анонімна реєстрація?	Ні	Ні	Ні	Ні	Так	Так
Чи можна додати контакт, не довіряючи серверу каталогів?	Ні	Так	Ні	Ні	Так	Ні

Продовження таблиці 4.1

Критерії	WhatsApp	Viber	Telegram	Signal	Threema	Wickr
Чи можна вручну перевірити відбитки пальців контактів?	Так	Так	Ні	Так	Так	Так
Служба каталогів може бути змінена, щоб організувати MITM-атаку?	Так	Так	Так	Так	Так	Так
Чи отримуєте повідомлення, якщо відбиток від контакту змінився?	Ні	Так	Ні	Так	Так	Ні
Чи хешована особиста інформація (номер мобільного телефону, список контактів тощо)?	Ні	Ні	Ні	Майже уся	Так	Так

Продовження таблиці 4.1

Критерії	WhatsApp	Viber	Telegram	Signal	Threema	Wickr
Чи може компанія читати повідомлення?	Ні	Ні	Так	Ні	Ні	Ні
Чи є у додатку двухфакторна автентифікація?	Так	Ні	Так	Ні	Так	Так
Коли проводився аудит коду та незалежний аналіз безпеки?	Ні	Ні	Так (листопад 2015 р.)	Так (жовтень 2014 р.)	Так (березень 2019 р.)	Так (серпень, 2014 р.)
Чи додаток містить саморуйнівні повідомлення?	Ні	Так	Так	Так	Ні	Так
Чи шифрує додаток метадані?	Ні	-	Ні	Так	Так	Так

Із проведенного аналізу шляхом порівняння у таблиці різних мессенджерів, можна зробити висновок, що одним із самих захищених є Threema.

Threema має достатньо переваг серед інших додатків по обміну миттевими повідомленнями, так як у більший часті критерієв вона майже завжди мала переваги.

Одна із вагомих переваг Threema це те, що вона є платною, має можливість анонімної реєстрації та нещодавно успішно пройшла аудит із пошуку вразливостей у додатку.

ВИСНОВКИ

Більшість сучасних популярних додатків для обміну повідомленнями використовують end-to-end encryption за замовчуванням, але у ході досліджень було з’ясовано, що це не гарантує того, що конфіденційна інформація користувачів знаходиться у безпеці і не може бути вкраденою.

Однією з найбільшоих проблем є протокол SS7. Про існуючі вразливості знають зловмисники і це є великою небезпекою для усіх користувачів мессенджерів незалежно від статусу і становища. Оператори обізнані про існуючі проблеми, але закривають бреши в протоколі достатньо повільно. Вони почали поступово впроваджувати додаткові засоби захисту для закриття вразливостей, однак ці системи не можуть повністю вирішити проблеми, пов'язані з архітектурою мереж SS7.

Також були розглянуті загрози безпеки абонентів в мережі на основі Diameter, пов'язані з тим, що будь-який підготовлений зловмисник, спеціальна група або іноземні розвідувальні органи можуть з легкістю отримати інформацію про поточне місцезнаходження абонента, а потім використовувати її при негласної стеження, шпигунство або для публічного розголошення відомостей про переміщення абонента. Проблеми зі зміною обладнання та сервісів можуть призводити до реалізації загрози перехоплення призначених для користувача даних, в тому числі SMS-повідомлень. Цю можливість зловмисник може використовувати для отримання доступу до системи ДБО, в якій для підтвердження входу користувача використовуються тимчасові паролі, що надсилаються

SMS. Перехопивши тимчасовий пароль, атакуючий отримає повний доступ до системи ДБО користувача і може викрасти всі грошові кошти, якими той володіє. при

цьому користувачеві під час крадіжки коштів з банківського рахунку може бути заблокований доступ до мережі зв'язку, таким чином він не буде отримувати повідомлення ні через

SMS-повідомлення, ні по електронній пошті - в зв'язку з блокуванням послуг, що надають доступ до мобільного Інтернету. Більш того, користувач не зможе зв'язатися з банком, щоб зробити блокування рахунку, оскільки обладнання оператора буде «рахувати», що він знаходиться в іншому регіоні, і постійно відключати його від мережі.

Для усунення загроз і підтримки налаштувань безпеки мережі в актуальному стані необхідно здійснювати постійний моніторинг, аналіз і фільтрацію повідомлень, що перетинають кордони мережі. З подібними завданнями дозволяють впоратися спеціалізовані системи виявлення атак і обладнання, що підтримує функціональність міжмережевого екранування сигнальних повідомлень.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Історія мессенджерів [Електронний ресурс]. – Режим доступу: https://itcrumbs.ru/istoriya-evolyutsiya-messendzherov_23557 (дата звернення 27.11.2019)

2. Історія мессенджерів [Електронний ресурс]. – Режим доступу: https://www.astrosoft.ru/articles/unified-communications/istoriya-messendzherov-pervaya-volna/ (дата звернення 27.11.2019)

3. Мессенджер WhatsApp [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/WhatsApp (дата звернення 26.10.2019)

4. Популярність WhatsApp [Електронний ресурс]. – Режим доступу: https://vc.ru/flood/5924-whatsapp-growth (дата звернення 26.10.2019)

5. Viber [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Viber

6. https://www.wechat.com/ru/ (дата звернення 26.10.2019)

7. Цетралізація [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Централізація (дата звернення 7.12.2019)

8. Наскрізне шифрування [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Наскрізне_шифрування (дата звернення 12.06.2019)

9. Популярні мессенджери за лютий 2019 [Електронний ресурс]. – Режим доступу: https://tns-ua.com/news/top-15-mobilnih-dodatkiv-za-lyutiy-2019 (дата звернення 11.06.2019)

10. Популярні мессенджери у 2019 р. [Електронний ресурс]. – Режим доступу: https://www.epravda.com.ua/rus/news/2019/11/14/653717/ (дата звернення 07.09.2019)

11. Популярність Viber [Електронний ресурс]. – Режим доступу: https://gagadget.com/business/48781-vojna-messendzherov-pochemu-v-ukraine-pobedil-viber/#! (дата звернення 20.10.2019)

12. Кількість користувачів різних мобільних операційних систем [Електронний ресурс]. – Режим доступу: https://tech.liga.net/technology/novosti/skolko-polzovateley-ukrainy-ispolzuyut-android-a-skolko-ios (дата звернення 22.10.2019)

13. Найпопулярніші мессенджери у світі [Електронний ресурс]. – Режим доступу: https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (дата звернення 22.10.2019)

14. Вразливість Viber, що дозволяє прослуховувати чужу розмову [електронний ресурс]. – Режим доступу: https://habr.com/ru/post/319360/ (дата звернення 11.06.2019)

15. Протокол MTProto [Електронний ресурс]. – Режим доступу: https://tlgrm.ru/docs/mtproto (дата звернення 11.06.2019)

16. Вразливість WhatsApp [Електронний ресурс]. – Режим доступу: https://securitytoday.com/articles/2018/10/12/whatsapp-bug-allowed-hackers-to-hijack-accounts.aspx (дата звернення 12.09.2019)

17. Вразливість WhatsApp [Електронний ресурс]. – Режим доступу: https://www.businessinsider.com/whatsapp-hacked-attackers-installed-spyware-2019-5?r=US&IR=T (дата звернення 12.09.2019)

18. Facebook зберігає паролі користувачів у відкритому виді [Електронний ресурс]. – Режим доступу: https://www.pravda.com.ua/rus/news/2019/03/22/7209902/ (дата звернення 08.12.2019)

19. Facebook приватність [Електронний ресурс]. – Режим доступу: https://www.facebook.com/about/privacy/update/?ref=email&locale=ru_ru

20. WhatsApp на кнопочних телефонах [Електронний ресурс]. – Режим доступу: https://tech.liga.net/technology/novosti/whatsapp-sdelali-dostupnym-dlya-knopochnyh-telefonov (дата звернення 08.12.2019)

21. Threema [Електронний ресурс]. – Режим доступу: https://threema.ch/en/faq (дата звернення 08.12.2019)

22. Briar [Електронний ресурс]. – Режим доступу: https://briarproject.org (дата звернення 08.12.2019)

23. Wire [Електронний ресурс]. – Режим доступу: https://wire.com/en/ (дата звернення 08.12.2019)

24. Confide [Електронний ресурс]. – Режим доступу: https://getconfide.com (дата звернення 08.12.2019)

25. Захищені непопулярні мессенджери [Електронний ресурс]. – Режим доступу: https://medium.com/@Emisare/top-4-messendjera-paranoika-2ea512775833 (дата звернення 08.12.2019)

26. Протокол Signaling System 7[Електронний ресурс]. – Режим доступу: https://elibrary.ru/item.asp?id=37165133 (дата звернення 12.06.2019)

27. Атака на протокол SS7 [Електронний ресурс]. – Режим доступу: https://networkguru.ru/ataka-na-protokol-ss7/ (дата звернення 12.06.2019)

28. Ататка на протокол SS7 [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/blog/company/PandaSecurityRus/346138.php (дата звернення 12.06.2019)

29. Ататка на протокол SS7 [Електронний ресурс]. – Режим доступу: https://networkguru.ru/ataka-na-protokol-ss7/ (дата звернення 12.06.2019)

30. Багатофакторна_автентифікація [Електронний ресурс]. – Режим доступу: https://ssl.com.ua/blog/what-is-2fa/ (дата звернення 07.06.2019)

31. Стандарт Diameter Електронний ресурс]. – Режим доступу: https://www.ptsecurity.com/ru-ru/research/analytics/diameter-2018/ (дата звернення 18.12.2019)

32. Мобільні оператори в Україні [Електронний ресурс]. – Режим доступу: https://fastcredit.money/poleznoe/vybor-mobilnogo-operatora-v-ukraine/ (дата звернення 18.12.2019)

33. Дослідження стандарту Diameter [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/news/493921.php (дата звернення 18.12.2019)

34. Атака “Атака людина посередині” [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Атака_людина_посередині (дата звернення 08.06.2019)

35. Вразливість у настільній версії Signal [Електронний ресурс]. – Режим доступу: https://www.bleepingcomputer.com/news/security/signal-upgrade-process-leaves-unencrypted-messages-on-disk/ (дата звернення 18.12.2019)

36. Вразливість у настільній версії Signal [Електронний ресурс]. – Режим доступу: https://bykvu.com/ru/bukvy/u-signal-vijavili-vrazlivist-jaka-dozvoljala-pidsluhovuvati-koristuvachiv/ (дата звернення 18.12.2019)

37. Вразливість у настільній версії Telegram [Електронний ресурс]. – Режим доступу: https://tjournal.ru/tech/79153-student-iz-ssha-obnaruzhil-chto-telegram-na-desktope-hranit-soobshcheniya-v-otkrytom-vide-durov-ne-uvidel-v-etom-uyazvimosti (дата звернення 18.12.2019)

38. Багатофакторна автентифікація [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Багатофакторна_автентифікація (дата звернення 08.06.2019)