УДК 004.056
DOI: 10.31673/2409-7292.2022.040007

**Рабчун Д.І., Найман Г.Г.,
Костирєв Л.В., Іщук М.О.**

ПОТЕНЦІЙНІ УРАЗЛИВОСТІ МЕХАНІЗМУ АУТЕНТИФІКАЦІЇ МЕСЕНДЖЕРІВ WHATSAPP ТА TELEGRAM

У статті розглянуто основні питання безпеки популярних месенджерів WhatsApp та Telegram, досліджено структуру та можливість проникнення до системи на основі використання уразливості протоколу SS7. Зроблено висновок про необхідність застосування двофакторної аутентифікації.

Ключові слова: месенджер, аутентифікація, WhatsApp, Telegram, протокол SS7.

Вступ

В умовах сучасного інформаційного суспільства комп'ютерні технології настільки вкоренилися в нашому житті, що повністю змінили способи обміну інформацією, які ми використовуємо для спілкування з друзями, членами сім'ї і діловими партнерами. Незважаючи на те, що електронна пошта стає все більш мобільною, ділові люди все більше і більше звертаються до тих же самим засобам комунікації, які звичайні користувачі застосовують давно і з величезним успіхом: до миттєвого обміну повідомленнями (Instant Messaging, IM).

Система миттєвого обміну повідомленнями (Месенджер) - це служби для обміну повідомленнями в режимі реального часу. Щоб використовувати подібні сервіси, необхідні лише вихід в інтернет і відповідна клієнтська програма (IM-клієнт). Традиційно в корпоративній системі використовувалася електронна пошта, але з розвитком Instant Messaging вона поступово відійшла на другий план. Різниця між мессенджерами і електронною поштою полягає в тому, що повідомлення передаються миттєво, а також є можливість бачити, чи знаходиться абонент в мережі. Однак, слід врахувати, що месенджер працює не автономно, а в залежності від сервера.

Для початку роботи в месенджері користувачеві необхідно отримати унікальний ідентифікатор (в цій якості може виступати UIN, унікальний код, або адреса його електронної пошти) і завантажити на свій комп'ютер клієнтську програму.

Месенджер WhatsApp

WhatsApp - популярний безкоштовний месенджер для мобільних і інших платформ з підтримкою голосового і відеозв'язку. Дозволяє пересилати текстові повідомлення, зображення, відео, аудіо, електронні документи та навіть програмні установки через Інтернет. WhatsApp Messenger доступний для iPhone, BlackBerry, Windows Phone, Android і Symbian.

Принцип роботи програми полягає в тому, що створюється аккаунт з використанням телефонного номера абонента і додаються ті контакти, які користуються цим сервісом. До зручностей цього додатка можна віднести: відсутність реєстрації та авторизації; немає необхідності шукати друзів. Відкривши вікно чату, можна відзначити ще кілька плюсів: можливість додавати в повідомлення мультимедійні файли, а також геолокацію. Сервіс сповіщає про відправку повідомлення, ставлячи галочку навпроти і другу галочку, якщо повідомлення прочитано. У програму не потрібно спеціально заходити: якщо приходить нове повідомлення, з'являється повідомлення при наявності підключення до Інтернету.

Проблематика безпеки WhatsApp

WhatsApp використовує модифікований протокол Extensible Messaging and Presence Protocol (XMPP, раніше відомий як Jabber). При установці створюється обліковий запис на сервері s.whatsapp.net, який використовує номер телефону в якості імені користувача (Jabber ID: [номер телефону] @ s.whatsapp.net). Версія під Android автоматично використовує в якості пароля MD5-хеш від зміненого ідентифікатора IMEI, а версія під iOS використовує MD5-хеш від MAC-адреси.

Через це алгоритму генерації пароля і відсутності шифрування WhatsApp неодноразово критикувалося. Мультимедіа-повідомлення відправляються шляхом завантаження

зображення, звуку або відео на HTTP-сервер і передачею гіперпосилання на об'єкт разом з закодованим в Base64 зменшеним варіантом зображення.

WhatsApp автоматично синхронізує список контактів з телефонною книгою телефону. Це можливо завдяки тому, що всі користувачі реєструються за своїм телефонним номером. Веб-версія WhatsApp розташована за адресою https://web.whatsapp.com/. Робота веб-версії здійснюється спільно з телефоном і можлива, тільки якщо телефон підключений до мережі Інтернет.

WhatsApp неодноразово був фігурантом гучних скандалів, через велику кількість уразливостей. WhatsApp має закритий код, як серверної так і клієнтьскої частини тому дослідники кіберзпеки не можуть легко перевірити, чи є там бекдори. WhatsApp не тільки не публікує код, вони роблять прямо протилежне: WhatsApp спеціально плутає бінарні файли своїх додатків, щоб ніхто не міг їх ретельно вивчити. Також сервіс довгий час сильно страждав від масових розсилок, - код відкритих проектів широко цьому сприяв. На даний розробники ввели обмеження на кількість повідомлень, що відправляються авторизованим контактам. Такі розсилки зазвичай були фішингові, могли взагалі містили шкідливе програмне забепечення, або бути атаками з використанням соціальної інженерії.

Через коллосальну кількість користувачів, розповсюдження спаму в ньому вже давно стало цілою індустрією зі своїми «корпораціями», які росповсюджують спам. Цілі таких дій можуть бути різні: нав'язливий маркетинг, шахрайські схеми, росповсюдження фішнгових посилань, або шкідливого програмного забезпечення.

Месенджер Telegram

Telegram – кросплатформенне програмне забезпечення, яке дозволяє обмінюватися текстовими, аудіо та відео повідомленнями та файлами, а також безкоштовно телефонувати іншим користувачам програми. Месенджер, який набуває популярності по всьому світу. Telegram сміло можна називати найбільш швидко зростаючим за популярністю месенджером.

Проблематика безпеки Telegram

Як було зазначено вище, для початку роботи з WhatsApp потрібно отримати унікальний ідентифікатор. З Telegram ситуація аналогічна. Але є декілька суттєвих відмностей:

кількість пристроїв телеграм не обмежена одним ПК і одним смартфоном;

за допомогю СМС унікальний ідентифікатор приходить тільки якщо ви не маєте активних пристроїв. В випадку, якщо такі пристрої є то код приходить в спеціальний чат з системними повідомленнями;

клієнт та криптографічний протокол MTProto є зразками відкритого ПЗ;

API більш зручний в використані та має більшу кількість мов програмвання, що підтримуються;

можливість встановити двофакторуну аутифікацію за паролем.

Надалі послідовність дій і принципи аутинтфікації в цих сервісах ідуть за ідентичнми алгоритмом. Ідентифікація користувача Telegram та WhatsApp пов'язана з номером телефону користувача. Користувач вводить номер телефону до якого привязаний аккаунт. Потім сервер WhatsApp, або Telegram надсилає SMS із кодом підтвердження, користувач подає код із отриманого текстового повідомлення та WhatsApp створює, або входить в свій обліковий запис. В Telegram якщо користувач вже має авторизацію на пристрої цей код він може отримати в спеціальний офіційний чат.

Уразливості механізму авторизації месенджерів

З проведеного розгляду виходить, що спосіб взлому вашогу аккаунти тільки один, це SMS-спуфінг.

Уразливість полягає в способі авторизації користувача. Для даної процедури використовується реальний номер телефону, на який відправляється СМС-код для підтвердження входу в аккаунт. В основі подібного методу передачі даних лежить технологія SS7 (Signaling System # 7), яка розроблялася 40 років тому і має слабкі параметрами безпеки за сучасними мірками. Теоретично зловмисники можуть перехопити СМС з кодом і зламати

акаунт. А, оскільки в звичайному режимі Telegram зберігає всі повідомлення на своїх серверах, хакери можуть отримати доступ до всієї листуванні конкретного користувача.

SMS-спуфінг - це технологія, яка використовує службу коротких повідомлень (SMS), доступну для більшості мобільних телефонів та персональних цифрових помічників, щоб встановити, від кого надходить повідомлення, замінивши номер мобільного телефону, що походить (Sender ID), на буквено-цифровий текст. Підробка має як законне використання (встановлення назви компанії, від якої надсилається повідомлення, встановлення власного номера мобільного телефону або назви продукту), так і нелегітимне використання (наприклад, видавання себе за іншу особу, компанію, продукт). Це також може надсилати "таємничі" повідомлення, схожі на те, що вони надходять із законних номерів або контактів.

Найновіші у своїй захищеності, хто користується популярною сьогодні послугою - двофакторна авторизація за допомогою SMS. Такі послуги пропонуються банками, відомими мессенджерами, соціальними мережами, поштовими системами та великою кількістю інших інтернет-ресурсів, вимагаючих реєстрацію. Не просто так цей метод вважається самим безпечним., Ваш мобільний телефон завжди при вас, як гаманець та інші особисті речі, для яких ви пристально стежте. Тому тому він є підтверджувальним фактором аутентифікації (застосовується лише після введення основного пароля). Але такі SMS можна перехватити за допомогою знання алгоритму SS7.

Протокол SS7, також відомий як Сигналізаційна система № 7, відноситься до мереж передачі даних і до низки технічних протоколів або правил, які регулюють обмін данними за ним. Він був розроблений у 1970-х роках для відслідування та підключення визовів у різних мережах операторів зв'язку, а тепер він зазвичай використовується для розсилки біллінгових сотових зв'язків та відправлення текстових повідомлень у доповнення до маршрутизації мобільних та стаціонарних викликів між операторами та регіональними комунікаційними центрами. Також в розглянутих сервісів є можливість додати двофактурну автинфікацию, тобто не тільки за рахунок тимчасового коду, а і за допомогою паролю. Що є додатковою мірую безпеки.

Дослідження уразливостей SS7

Зловмисник підключається до сигнальної мережі SS7 і відправляє службову команду Send Routing Info для SM (SRI4SM) в мережевому каналі, вказуючи номер телефону, атакуваного абонента за вашими параметрами. Домашня абонентська мережа надсилає у відповідь наступну технічну інформацію: IMSI (International Mobile Subscriber Identity) та адресу MSC, за котрою в даний час надає послуги підписника (рис. 1).

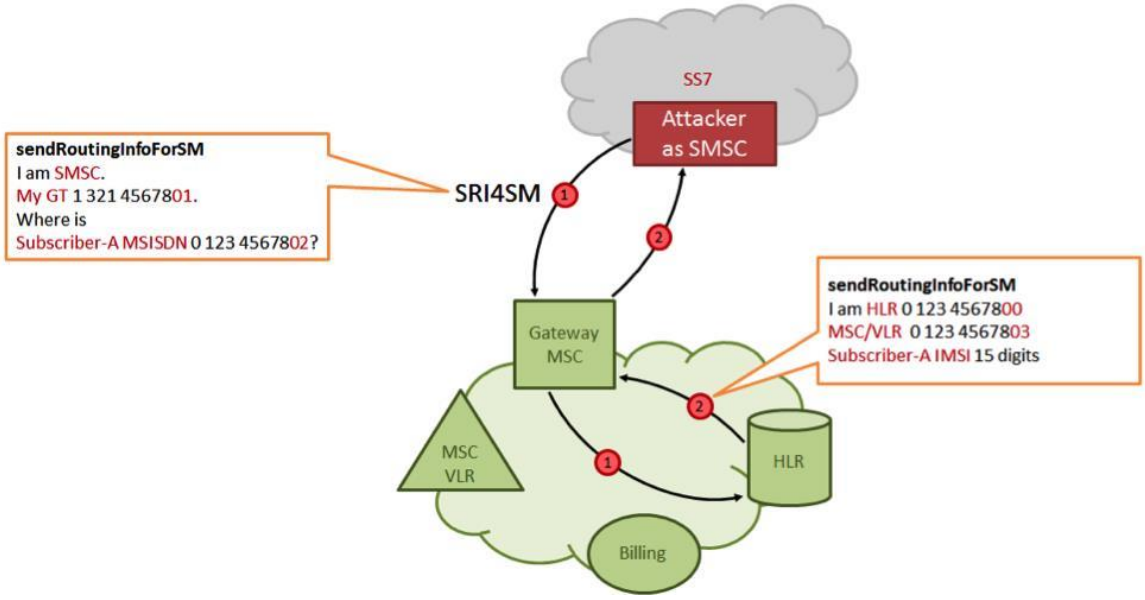

Рис.1. Схема підключення зловмисника

Після цього зловмисник змінює адресу білінгової системи в профілі передплатника на адресу своєї власної псевдобіллінговой системи (наприклад, повідомляє, що абонент прилетів на відпочинок і в роумінгу зареєструвався у новій білінговій системі). 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.

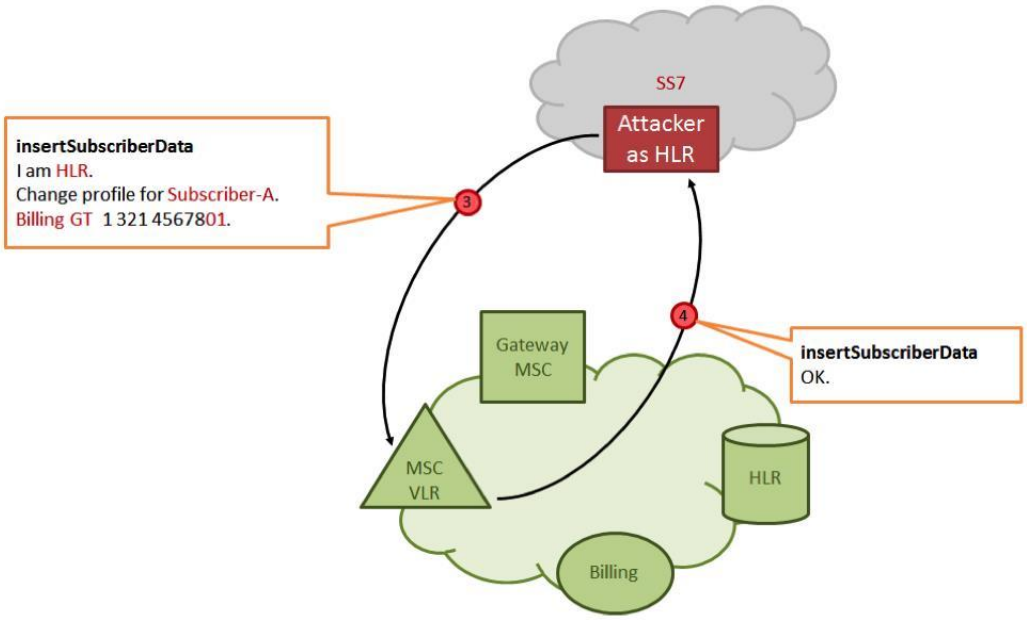

Рис. 2. Виконання запиту

Коли абонент, що атакується, 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. Приклад – на рис. 3.

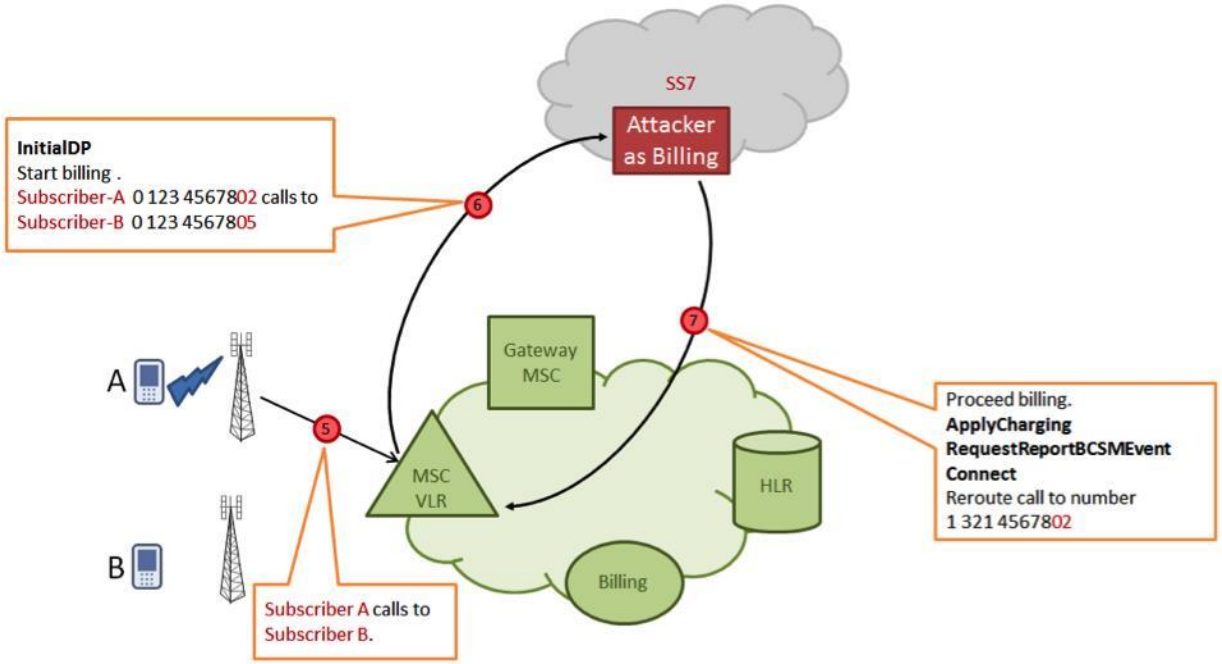

Рис. 3. Відправлення команди на комутатор

У сторонньому місці встановлюється конференц-зв'язок з трьома передплатниками, дві з них є реальними (абонент a і викликається b), а третій вводиться зловмисником незаконно і

здатний прослуховувати і записувати розмову. Відповідним чином отримуємо і SMS атаку. Маючи доступ до псевдобілінгової системи, на яку вже зареєструвався наш абонент, можна отримати будь-яку інформацію, яка приходить або йде з його телефону. Приклад – на рис. 4.

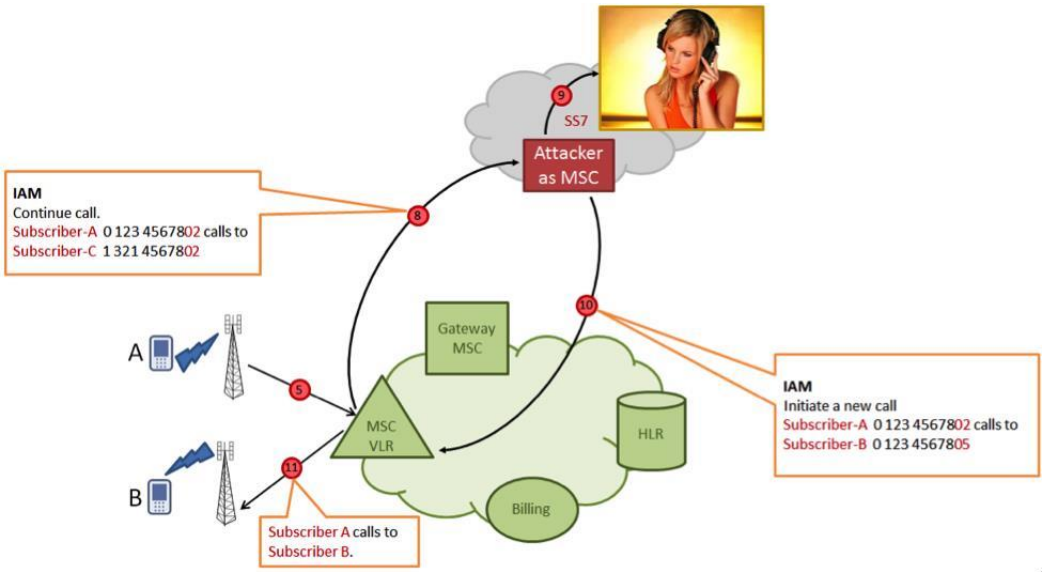

Рис. 4. Приклад підключення конференц-зв’язку

На завершення необхідно розглянути, як оператори стільникового зв'язку дивляться на безпеку SS7. По-перше, вони вважають (і небезпідставно), що неможливо отримати абсолютно нелегальний доступ до мережі SS7. По-друге, між усіма операторами є угоди на пропуск трафіку, і навіть якщо раптом з боку якогось оператора будуть помічені зловмисні дії, то не важко буде провести блокування за адресою джерела. По-третє, не так багато відомо випадків зловживання засобами SS7.

Всі три твердження абсолютно справедливі. Але отримати підключення до SS7 можливо, наприклад, під прикриттям провайдера VAS-послуг. Швидше за все, це не вийде зробити в Україні, проте є країни з більш лояльним законодавством у сфері телекомунікацій. Перш ніж припинити шкідливі дії, їх треба помітити. Вкрай мале число операторів проводить постійний моніторинг мереж SS7 на предмет вторгнень і атак. І навіть якщо атака через мережу SS7 буде помічена і припинена, ніхто не зможе сказати, коли вона почалася і як довго тривала.

Висновки

Проаналізовано проблеми забезпечення безпеки в месенджерах Whatsapp та Telegram, а конкретно спосіб перехвату SMS повідомленнь SS7. Досліджено гіпотетичний спосіб, яким можна через вразливості протоколів SS7, можна заволодіти аккаунтом в Telegram та WhatsApp. Виокремлено, що спосіб працює лише з аккунтами де відсутня двофакторна аунтифікація. Варто зазначити, що на теперішній час використати цю уразливість можуть лише недобросовісні співробітники телеком-послуг.

Перелік посилань

1. Скороход В. Визначення засобів розробки чат-бота «помічник абітурієнта» для сучасних месенджерів. – 2017.

2. Seth Rosenberg. How To Build Bots for Messenger [online]. Fa- cebook; URL: https://developers.facebook.com/blog/post/2016/04/12/bots-for- messenger/.

3. Claudia-bot-builder [online]. Claudiajs; URL: https://github.com/claudiajs/claudia- bot-builder.

4. Developer Survey Results 2017 [online]. StackOverflow; URL: http://stackover-flow.com/insights/survey/2017.

Надійшла: 27.11.2022 Рецензент: д.т.н., доцент Ахрамович В.М.