УДК 004.056
DOI: 10.31673/2409-7292.2021.021314

Ірза К.С., Гай Д.О.

ТЕХНОЛОГІЯ ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В СОЦІАЛЬНИХ МЕРЕЖАХ

В роботі наведені основні функції соціальних мереж та дані, що містяться в них. Розглянуті спектри атак та контрзаходи. Досліджено загрози та технології захисту інформації і розроблено варіант технології захисту персональної та конфіденційної інформації у соціальних мережах. Представлено перший прототип месенджеру P2P, написаний на Java, який може виконуватися в декількох операційних системах, таких як Windows, Linux та MacOS.

Ключові слова: соціальна мережа, конфіденційність, доступність, цілісність, цифрове стеження, централізовані мережі, децентралізовані мережі, механізми захисту.

Послуги соціальних мереж, такі як Facebook, LinkedIn або Twitter, є переважним фактором Інтернету. Обслуговуючи дуже велику кількість користувачів із величезною різницею в соціальному, освітньому та національному походженнях, вони дозволяють навіть користувачам з обмеженими технічними навичками публікувати особисту інформацію та легко спілкуватися. Однак популярність і широке визнання послуг соціальних мереж як платформ для обміну повідомленнями та спілкування приваблює не лише вірних користувачів, які намагаються додати цінності для спільноти, але і партій із досить несприятливими інтересами, будь то комерційні чи зловмисні [1].

Основною програмою, яку використовують користувачі Online Social Network OSN, є створення та ведення їхніх списків контактів за допомогою Social Networking Service SNS. Завдяки автоматичному інформуванню користувачів про зміни профілів своїх контактів, SNS, таким чином, допомагає користувачам бути в курсі новин про їх контакти, і дуже часто популярність користувачів вимірюється кількістю контактів, на які вони посилаються [2].

Аналіз робіт

Аналізуючи OSN щодо їх властивостей безпеки та конфіденційності користувачів, загрози стають очевидними. Як правило, велика кількість персональних даних про учасників зберігається у провайдерів, особливо у випадку, коли OSN націлена на непрофесійні цілі. Ці дані є або видимими для загального користування, або, якщо користувач знає про проблеми конфіденційності та може користуватися налаштуваннями відповідної SNS [3].

Різні дослідження показали, що учасники однозначно представляють слабку ланку безпеки в OSN і що вони вразливі до декількох типів атак соціальної інженерії. Це частково спричинено недостатньою обізнаністю щодо наслідків простих і, мабуть, приватних дій, таких як прийняття запитів на контакт або позначення зображень, а також комунікаційних операцій, таких як коментування профілів або розміщення на стінах. Низька ступінь зручності управління конфіденційністю, що здійснюється SNS [4].

Аналізуючи проблеми конфіденційності в поточній OSN [5–7], стає очевидним, що навіть якщо всі учасники були обізнані про викриття та компетентні у використанні SNS, і навіть якщо б застосовувався стислий набір заходів щодо конфіденційності, OSN все одно піддавався б потенційному конфіденційності порушення з боку всезнаючого провайдера послуг: дані, прямо чи опосередковано надані всіма учасниками, збираються та постійно зберігаються в базах даних постачальника послуг, який потенційно може використовувати ці дані багатьма способами, які можуть порушити конфіденційність окремих користувачів або груп користувачів. У зв'язку з цим забезпечення інформаційної безпеки при використанні соціальних мереж є *актуальною* задачею.

Метою даної роботи є розроблення варіанту технології захисту персональної та конфіденційної інформації в соціальних мережах.

Функціонал соціальних мереж та їх політики конфіденційності

Обслуговування і доступ до OSN та їх послуг надаються комерційними постачальниками соціальних мереж (SNP), такими як Facebook, LinkedIn, Twitter, XING та подібні. Загалом, велика кількість PII, що надається користувачами, зберігається в базах даних, що перебувають під контролем цих провайдерів, особливо у випадку, коли OSN націлена на непрофесійні цілі. Ці дані є загальнодоступними, або якщо користувач знає про проблеми конфіденційності та може користуватися налаштуваннями відповідного SNS, вони доступні вибраній групі інших користувачів. Оскільки профілі приписуються імовірно відомим особам із реального світу, вони неявно оцінюються з такою ж довірою, як і передбачуваний власник профілю. Крім того, будь-які дії та взаємодії, пов'язані з профілем, також знову приписуються передбачуваному власнику цього профілю [8].

SNP може разом зі своїм SNS також пропонувати інтерфейс прикладного програмування (API), що дозволяє зацікавленим користувачам програмувати додаток соціальної мережі (SNA), розширюючи функціональний спектр послуги (рис. 1) [9].

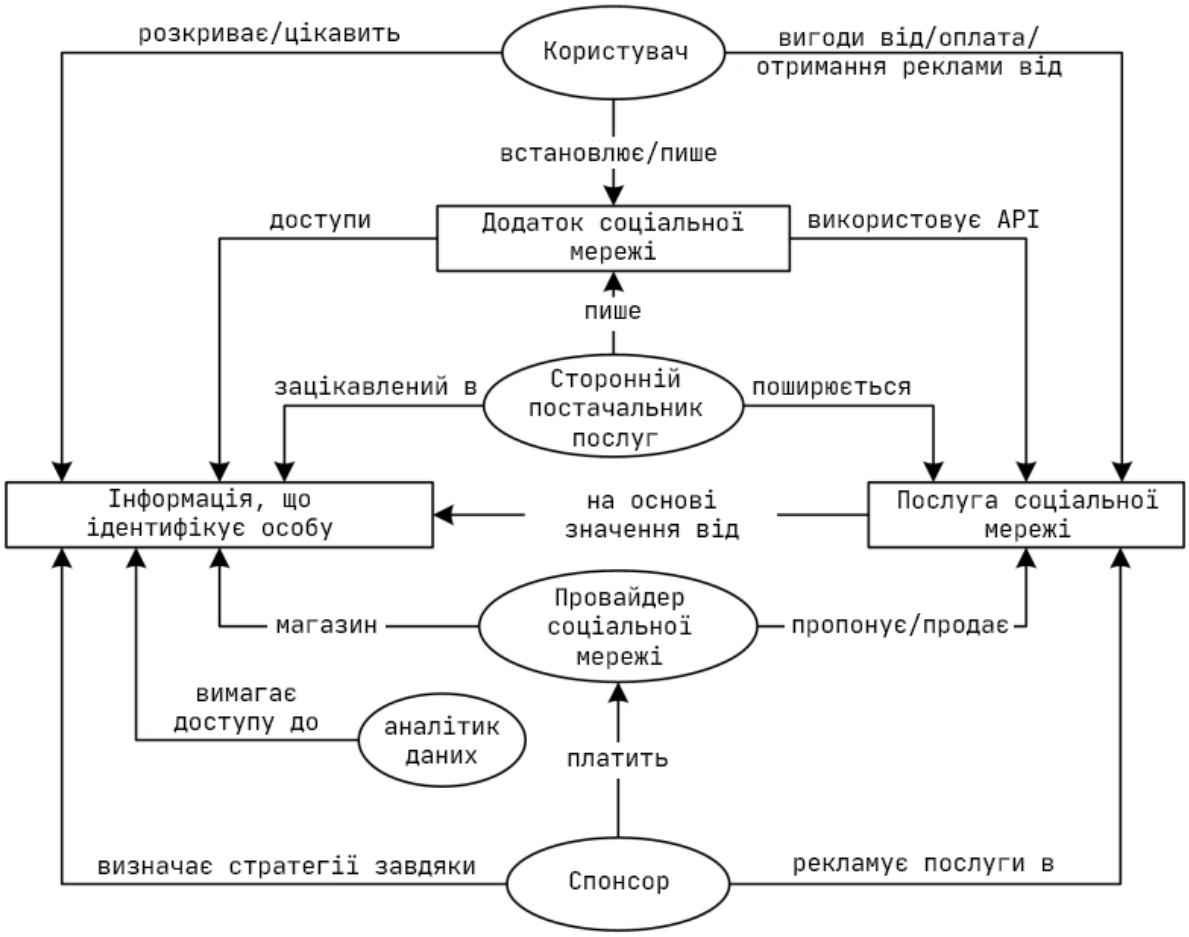

Рис. 1. Клієнти OSN і їхні стосунки до персональних даних та SNS

Рисунок ілюструє та узагальнює різноманітність клієнтів OSN та відображає їхнє відношення до функціональних можливостей SNS та можливий доступ до особистої інформації користувачів OSN.

Дані, що містяться в соціальних мережах

Основну інформацію, що зберігається в OSN, власні дані, що генеруються та підтримуються користувачами та їхніми профілями, можна класифікувати на наступні типи:

– особисті контактні дані, що описують особу користувача;
– підключення, що представляє зв’язки на графіку соціальної мережі;

– інтереси користувача;
– інформація про автобіографію користувача;
– спілкування, включаючи всі взаємодії з іншими користувачами OSN.

Ці типи складають особисту інформацію, яка надається безпосередньо користувачем OSN. Додаткова інформація про користувача OSN часто генерується іншими користувачами.

Будь-яка форма цифрового вмісту, створеного користувачами, може також спричинити розголошення інформації третьою стороною. Наприклад, деякі OSN намагаються заважати користувачам публікувати фотографії, на яких зображені люди у їхніх профілях, якщо власник профілю там не зображений. Однак це не заважає користувачам публікувати фотографії, на яких вони зображені разом з іншими. Крім того, багато OSN платформ пропонують теги зображених користувачів, чиї профілі зазвичай безпосередньо пов'язані з цією картинкою. Ці теги можуть містити додаткові коментарі, додані користувачем, який завантажує зображення.

Загрози конфіденційній інформації у соціальних мережах

Порушення конфіденційності та цілісності наданого користувачем вмісту може призвести до економічної шкоди для користувачів, спричинити незручні ситуації, а також заплямувати їх репутацію (навіть у реальному світі), відсутність доступності вмісту або послуг може також зменшити рівень привабливість фактичної платформи OSN та шкодить її провайдеру. Впоратися з усіма цими цілями надзвичайно важко одночасно. Особливо конфіденційність користувачів OSN є складною, оскільки обсяг особистої інформації величезний, і ця інформація може бути доступна не тільки на певній платформі OSN, але і в Інтернеті [10].

Далі представляється та обговорюється вплив серії атак OSN на вищезазначені цілі безпеки.

Таблиця 1.

Атаки проти цілей безпеки в інтернет-соціальних мережах

Атаки	Конфіденційність	Цілісність	Доступність
Звичайне уособлення	x	x	
Клонування профілю	x	x	
Викрадення профілю	x	x	
Портування профілю	x	x	
Викрадення ID	x	x	x
Профілювання	x		
Вторинний збір даних	x		
Підроблені запити	x		
Сканування та збирання	x		
Виявлення та аналіз зображень	x		
Відстеження спілкування	x		
Атака фейковими профілями та Sybil		x	
Груповий метаморфоз		x	
Виборчі бюлетені та наклеп		x	
Цензура		x	x
Атаки змови	x	x	x

Варіант технології захисту персональної та конфіденційної інформації у соціальних мережах

У літературі про мережі P2P [11–13] вже було розглянуто проблему анонімного спілкування та запропоновано рішення, які підходять для спільного використання, але виявляються недостатніми в контексті DOSN. Як приклад, добре відома техніка Onion Routing, коли вузол відправника рекурсивно шифрує секретний вміст за допомогою відкритого ключа вузлів, що складають шлях, яким повинен йти цей вміст, коли він приймається в мережі Friend-to-Friend (F2F), коли peer співпрацюють завдяки своїй дружбі, потрібно, щоб відправник знав топологію графіків соціальних мереж, тобто інформацію, яку

DOSN має на меті захистити. З іншого боку, коли мережа P2P не є мережею F2F, необхідні відповідні механізми стимулювання для співпраці між peer.

У цій роботі пропонується кардинально нова архітектура P2P для безпечної, збереженої конфіденційності, розподіленої OSN для належного націлювання на безпеку та конфіденційність користувача в OSN. Подібне рішення вирішує питання конфіденційності, уникає проблем цифрового стеження та гарантує співпрацю між peers.

Реалізація власного P2P месенджера на мові програмування Java

Для досягнення головної мети конфіденційності розподілене зберігання даних для OSN може бути досягнуте або за допомогою підходу клієнт-сервер (або хмари), коли користувачі не беруть участі в службі зберігання, а збережені дані завжди доступні або за допомогою рівноправного підходу, коли користувачі беруть участь у службі зберігання, і збережені дані можуть бути не завжди доступними.

Підхід P2P за своєю суттю піддається розробці архітектури з основною метою уникнення контролю з боку однієї сторони, такої як організація чи компанія. Тому було вирішено вибрати P2P-підхід, враховуючи додаткові його переваги, такі як масштабованість та відмовостійкість.

В якості першого принципу проектування розглядається система P2P і покладається на вузли однорангового рівня для виконання основних операцій OSN, таких як:

– зберігання даних користувача;
– пошук даних користувача;
– спілкування між користувачами.

Тим не менше, система P2P серйозно страждає від головної проблеми, а саме відсутності співпраці між одноранговими вузлами. Відсутність апріорної довіри, що характеризує будь-яку систему P2P, підвищує внутрішню віддаленість вузлів, які часто беруть участь у вільному спілкуванні [13] і намагаються споживати якомога більше ресурсів, не роблячи внеску в послуги мережі. Отже, примусове співробітництво є обов'язковою вимогою до ефективної настройки розподіленої P2P OSN.

Тим не менш, у конкретному контексті OSN, довіра між користувачами в реальному житті може служити набагато більше, ніж проста співпраця: вона може бути використана для побудови самої соціальної мережі у Інтернеті. Отже, OSN допомагає користувачеві встановити стосунки з друзями, а вузли друзів надають основні послуги зберігання даних, пошуку та зв'язку, а отже, і побудови OSN.

Інтерфейс та функціонал месенджера

Інтерфейс користувача був реалізований як додаток, використовуючи технологію Java Swing. Користувач запускає програму і у його просить ввести бажане ім'я та порт. Довжина можливого імені обмежена, мінімальна кількість 2 символи, а максимальне 16. Порт буде використовуватися для подальшого об'єднання з іншими користувачами, його максимальне значення може бути 65535.

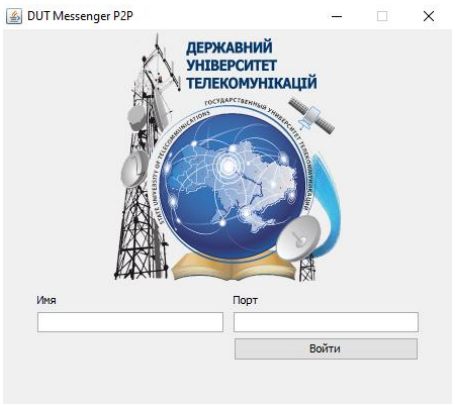

Рис. 2. Вікно входу до месенджеру P2P

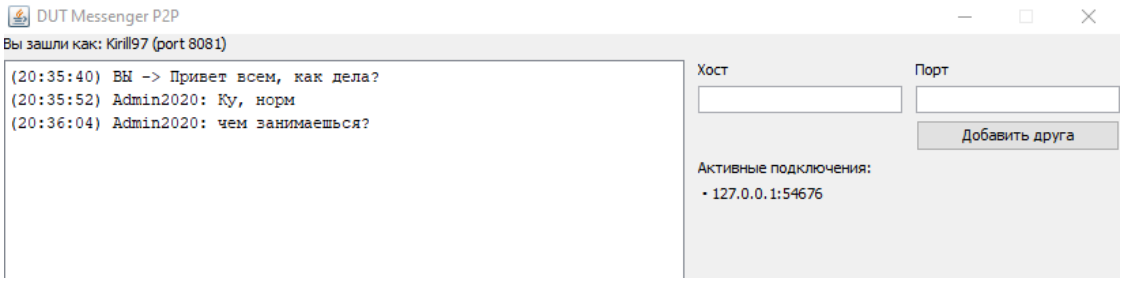

Рис. 3. Вікно з чатом в месенджері P2P

Після входу в месенджер з'являється вікно з чатом, поле для введення повідомлення і кнопка виходу. Для початку спілкування необхідно додати друга, щоб це зробити, треба в полях хост і порт ввести дані свого майбутнього співрозмовника. В активних підключеннях буде відображатися список адрес, які знаходяться в чаті [14–16].

У чаті одночасно може перебувати необмежена кількість користувачів, таким чином люди всередині месенджера можуть об'єднуватися в локальні групи і ділитися інформацією лише з тими користувачами, яким довіряють.

Технічна реалізація месенджера

Для реалізації децентралізованої мережі необхідно створити два обробника, перший буде називатися ClientThread і буде відповідати за підключення до інших серверів користувачів і читанням вхідних пакетів.

```java
package ua.dut.messenger;

import ua.dut.messenger.frame.ChatFrame;

import java.io.BufferedReader;
import java.io.IOException;
import java.io.InputStreamReader;
import java.net.Socket;

public class ClientThread extends Thread {

    private final ChatFrame frame;

    private final Socket socket;
    private final BufferedReader reader;

    public ClientThread(ChatFrame frame, String host, int port) throws IOException {
        this.frame = frame;

        socket = new Socket(host, port);
        reader = new BufferedReader(new InputStreamReader(socket.getInputStream()));
    }

    @Override
    public void run() {
        while (true) {
            try {
                frame.addMessage(reader.readLine());
            } catch (Exception ex) {
                ex.printStackTrace();
                break;
            }
        }
    }

}
```

Рис. 4. Реалізація ClientThread обробника

У той час, як обробник ServerThread відповідатиме за створення сервера, очікування підключення інших клієнтів та відправлення пакетів усім підключеним користувачам [17,18].

Основний протокол додатку реалізовано, залишилось створити інтерфейс входу в месенджер і в обробник натискання кнопки додати перевірки введених значень в поле імені та порту.

```
package ua.dut.messenger.frame;

import javax.swing.*;
import java.awt.*;
import java.io.IOException;
import java.util.concurrent.Executors;
import java.util.concurrent.ScheduledExecutorService;
import java.util.concurrent.TimeUnit;

public class JoinFrame extends JFrame {

    private final ScheduledExecutorService scheduler = Executors.newSingleThreadScheduledExecutor();

    private JPanel panel;

    private JLabel logoLabel;

    private JTextField nameField;
    private JTextField portField;

    private JLabel messageLabel;
    private JButton button;

    private JoinFrame(String title) throws HeadlessException {
        super(title);

        setContentPane(panel);

        logoLabel.setIcon(new ImageIcon(getClass().getResource( name: "/images/dut_logo.png")));
        messageLabel.setForeground(Color.RED);

        button.addActionListener(event -> {
            String nameText = nameField.getText();
            String portText = portField.getText();

            if (nameText == null || nameText.isEmpty()) {
                showMessage("Введите свое имя");
                return;
            }

            int length = nameText.length();
            if (length < 2 || length > 16) {
                showMessage("Неправильный размер имени");
                return;
            }

            if (portText == null || portText.isEmpty()) {
                showMessage("Введите свой порт");
                return;
            }

```

Рис. 5. Реалізація інтерфейсу входу в месенджер

У класі ChatFrame створюється область чату, обов'язково додається можливість підключення друзів, виведення активних користувачів та поле для відправлення повідомлень. Все це за допомогою слухачів підключається до ServerThread обробника.

І нарешті додається клас запуску всієї програми, який буде створювати об'єкт JoinFrame і показувати це вікно користувачеві.

Висновки

Клієнт-серверні (або хмарні) підходи вимагають придбання або розгортання конфіденційних даних користувачів, що розміщують веб-простір, і не завжди уникають потенційного контролю однієї сторони, як, наприклад, компанії або організації, за такими даними. Для того, щоб гарантувати повну доступність даних, вони часто вимагають, щоб користувач OSN платив за послугу зберігання або за обслуговування власної інфраструктури.

З іншого боку, сучасні однорангові підходи послаблюють вимоги щодо доступності даних та надають найкращі послуги. Хоча такі підходи не підпадають під контроль однієї сторони, вони піддають користувачів потенційному відстеженню зв'язку з боку зловмисників. У контексті OSN такі сліди спілкування можуть розкривати подробиці про структуру графіку соціальної мережі.

У цій роботі був представлений перший прототип месенджеру P2P, написаний на Java, який може виконуватися в декількох операційних системах, таких як Windows, Linux та MacOS. Вказано на централізовану архітектуру існуючих онлайн соціальних мереж як ключове питання конфіденційності та запропоновано рішення, яке спрямоване на уникнення будь-якого централізованого контролю. Це месенджер P2P, створений на одноранговій архітектурі. Завдяки своїй повністю розподіленій природі уникає централізованого контролю з боку будь-якого потенційно шкідливого постачальника послуг.

Перелік посилань

1. Сторінки фанатів Facebook потребують оновлення безпеки, каже жертва. /https://gadgetwise.blogs.nytimes.com/2010/03/18/fake-facebook-fan-pages/ // 2010.
2. Злом Facebook розкриває тенденцію орієнтування на соціальні мережі. /https://fraudwar.blogspot.com/2009/05/facebook-hack-reveals-trend-in.html // 2009.
3. Заява про права та обов'язки у Facebook. /https://www.facebook.com/legal/terms
4. Користувачі Facebook націлені на масовий спам. /https://www.pcworld.com/article/191847/article.html // 2010.
5. Користувачі Facebook мимоволі поширюють черв'яка koobface. /http://content.usatoday.com/communities/technologylive/post/2009/12/koobface-compels-facebook-victims-to-help-spread-worm-/1 // 2009.
6. Facebook реагує на масштабну схему фішингу. /https://scitech.blogs.cnn.com/2010/03/19/facebook-responds-to-massive-phishing-scheme/ // 2010.
7. Угода користувача LinkedIn. /https://www.linkedin.com/legal/user-agreement
8. Статистичні дані Twitter. /https://www.oberlo.com/blog/twitter-statistics // 2020.
9. Статистичні дані LinkedIn. /https://www.oberlo.com/blog/linkedin-statistics // 2020.
10. Статистичні дані Facebook. /https://www.oberlo.com/blog/facebook-statistics // 2020.
11. Блог у Twitter: Понеділок вранці божевільний. /https://blog.twitter.com/official/en_us/a/2009/monday-morning-madness.html // 2009.
12. Умови використання Twitter. /https://twitter.com/tos
13. Eytan Adar and Bernardo A. Huberman, Free riding on Gnutella, First Monday, 2000.
14. Algirdas Avizienis, Jean-Claude Laprie, Brian Randell, and Carl Landwehr, Basic concepts and taxonomy of dependable and secure computing, IEEE Transactions on Dependable and Secure Computing, 2004.
15. Lars Backstrom, Cynthia Dwork, and Jon Kleinberg. Wherefore art thou r3579x?: anonymized social networks, hidden patterns, and structural steganography. In Proceedings of the 16th international conference on World Wide Web, 2007.
16. Randolph Baden, Adam Bender, Daniel Starin, Neil Spring, and Bobby Bhattacharjee. Persona: An online social network with user-defined privacy. In ACM SIGCOMM, Barcelona, Spain, August 2009.
17. Marco Balduzzi, Christian Platzer, Thorsten Holz, Engin Kirda, Davide Balzarotti, and Christopher Kruegel. Abusing Social Networks for Automated User Profiling. Research Report RR-10-233, EURECOM, 2010.
18. Leyla Bilge, Thorsten Strufe, Davide Balzarotti, and Engin Kirda. All your contacts are belong to us: automated identity theft attacks on social networks. In Proceedings of the 18th international conference on World wide web, Madrid, Spain, 2009.

Надійшла: 16.04.2021 Рецензент: д.т.н., доцент Ахрамович В.М.