УДК 004.056.5

М.С. Ратушняк

АНАЛІЗ СТЕГАНОГРАФІЧНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ У СОЦІАЛЬНИХ МЕРЕЖАХ

Вінницький національний технічний університет

Анотація

У доповіді розглянуто можливість використання основних стеганографічних методів передавання секретних повідомлень через соціальні мережі. Здійснено огляд каналів зв'язку у соціальних мережах.

Ключові слова: соціальні мережі, стеганографія, вбудовування, контейнер.

Abstract

The report discusses the possibility of using different steganographic algorithms to transmit hidden messages through the social networks. Examined channels of communication through the social networks.

Key words: social networks, steganography, embedding, container.

Вступ

Соціальні мережі вже перестали бути тільки розважальним ресурсом або засобом індивідуального спілкування. На даний момент соціальні мережі є одним з найкращих маркетингових інструментів з багатомільярдним оборотом. Також соціальні мережі активно використовуються в корпоративному секторі для підбору персоналу, пошуку клієнтів, отримання репутаційної інформації про людей і організації. У зв'язку з цим багато фірм відмовилися від жорсткого обмеження на використання соціальних мереж з робочих місць. З'явився попит на менеджерів по роботі з соціальними мережами (SocialMediaManager). Таким чином, для співробітників компанії соціальні мережі залишаються доступним каналом зв'язку з людьми поза фірмою, в тому числі, з потенційними конкурентами і іншими супротивниками компанії [1].

Раніше витоки інформації були пов'язані з передачею даних у відкритому вигляді, і основну небезпеку представляла міграція даних з однієї соціальної мережі в іншу. Однак, такі факти передачі можна було відстежити (безпосередньо з аккаунта користувача або через сервер соціальної мережі). Зараз передачу конфіденційної інформації намагаються захистити різними методами, наприклад, із застосуванням криптографічних або стеганографічних засобів. Однак, слід зауважити, що в більшості країн, застосування криптографічних засобів регламентується законодавчими актами різного рівня і відстежується відповідними органами. Тому застосування криптографії для передачі комерційної конфіденційної інформації порушує не тільки інтереси фірми, а й закони держави. Застосування стеганографії ніяк не регламентується сучасним законодавством. Комп'ютерна стеганографія взагалі дуже молода галузь науки, але вона активно розвивається, і її методи швидко набирають популярність. [2].

У зв'язку з цим, використання сервісів соціальних мереж для обміну секретними повідомленням має широке застосування, так як важко прослідкувати за великими потоками інформації, що циркулюють.

Результати дослідження

В даний час вже відомі і ще розробляються стеганографічні методи, які в якості контейнера (файлу або пакета даних, в який вбудовується приховувана інформація) використовують не тільки файли, але і особливості мережевих протоколів (мережева стеганографія). Тож, у доповіді було розглянуто найбільш популярні методи приховування інформації:

1. Вбудовування в графічні файли:
   - приховування в просторової області (наприклад, використання молодших бітів, заміна палітри);
   - приховування в частотній області (наприклад, модифікація дискретного косинусного перетворення);
2. Вбудовування в аудіофайли

– приховування в часовій області (наприклад, заміна молодших бітів, розширення спектра);
– приховування в частотної області (наприклад, фазове кодування);
– використання луна-сигналу. [3]

Тож, на основі проведеного аналізу, визначено наступні закономірності, щодо використання соціальних мереж для передачі секретних повідомлень:

– аватар непридатний для передачі даних (сильне стиснення зображення);
– більшість соціальних мереж конвертують формат зображень в листуванні, тому стегоповідомлення не вдається витягти;
– фотоальбоми і аудіоальбоми передають приховане зображення без спотворень;
– будь-які посилання на зовнішні файли передають повідомлення без спотворень і не фіксуються соціальною мережею;
– мобільні додатки вносять спотворення і в зображення з фотоальбомів, тому що дані стискаються для передачі по мобільним мережам.

Висновки

Проведено аналіз стеганографічних методів захисту інформації у соціальних мереж, виявлено, що найпопулярнішими та найефективнішими методами є вбудовування секретних повідомлень у графічні та аудіофайли. Проте через особливості завантаження та зберігання файлів у соціальних мережах, вбудоване повідомлення не завжди може бути виявлено отримувачем.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Карпінець В. В., Яремчук Ю. Є. Аналіз рівня спотворень векторних зображень внаслідок вбудовування цифрових водяних знаків / В.В. Карпінець, Ю.Є. Яремчук // Сучасний захист інформації. – 2011. – №2. – С.94 – 99
2. V. Karpinets, Ju. Yaremchuk, M. Prokofjev. Матеріали конференції, Technical University of Gabrovo. International scientific conference UNITECH'12. / V. Karpinets, Ju. Yaremchuk, M. Prokofjev. // Proceedings. Volume I, 16–17 November 2012, Gabrovo. – Pp. 348 – 352.
3. Кувшинов, Станислав Сергеевич. Методы и алгоритмы сокрытия больших объемов данных на основе стеганографии : диссертация кандидата технических наук : 05.13.19 / Кувшинов Станислав Сергеевич; [Место защиты: С.-Петерб. гос. ун-т информац. технологий, механики и оптики].- Санкт-Петербург, 2010.- 26 с.

Ратушняк Марія Сергіївна – студентка групи УБ-12, факультет менеджменту, кафедра менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, Вінниця, e-mail: ratushnyak95@outlook.com;

Науковий керівник: ***Василь Васильович Карпінець*** – к.т.н., доцент кафедри менеджменту та безпеки інформаційних систем, Вінницький національний технічний університет, м. Вінниця.

Maria S Ratushnyak - Department of Management and Information Systems Security, Vinnytsia National Technical University, Vinnytsia, email: ratushnyak95@outlook.com;

Supervisor: ***Vasyl V Karpinets*** – Cand. Sci. (Eng.), Docent of Department of Management and Information Systems Protection, Vinnytsia National Technical University, Vinnytsia.