Перспективи застосування стеганографічних систем в XXI столітті

Пшец С.О.
студент 5 курсу
ПНПУ імені В.Г. Короленка

Стеганографія – це метод організації зв'язку, який власне приховує саму наявність зв'язку. На відміну від криптографії, де ворог точно може визначити чи є передане повідомлення зашифрованим текстом, методи стеганографії дозволяють вбудовувати секретні повідомлення в нешкідливі послання так, щоб неможливо було запідозрити існування вбудованого таємного послання.

Слово «стеганографія» в перекладі з грецької буквально означає «тайнопис» (steganos – секрет, таємниця; graphy – запис). До неї відноситься величезна кількість секретних засобів зв'язку, таких як невидимі чорнила, мікрофотознімкі, умовне розташування знаків, таємні канали та засоби зв'язку на плаваючих частотах і т. д.

Стеганографія займає свою нішу в забезпеченні безпеки: вона не замінює, а доповнює криптографію. Приховування повідомлення методами стеганографії значно знижує ймовірність виявлення самого факту передачі повідомлення. А якщо це повідомлення до того ж зашифровано, то воно має ще один, додатковий, рівень захисту.

На даний час у зв'язку з бурхливим розвитком обчислювальної техніки і нових каналів передачі інформації з'явилися нові стеганографічні методи, в основі яких лежать особливості подання інформації в комп'ютерних файлах, обчислювальних мережах і т. п. Це дає нам можливість говорити про становлення нового напрямку – комп'ютерної стеганографії.

При побудові стегосистеми повинні враховуватися наступні положення:

- противник має повне представлення про стеганографічну систему і деталі її реалізації. Єдиною інформацією, яка залишається невідомою потенційному противнику, є ключ, за допомогою якого тільки його власник може встановити факт присутності і зміст прихованого повідомлення;
- якщо противник якимось чином дізнається про факт існування прихованого повідомлення, це не повинно дозволити йому витягти подібні повідомлення в інших даних до тих пір, поки ключ зберігається в таємниці;

– потенційний противник повинен бути позбавлений будь-яких технічних та інших переваг в розпізнаванні або розкритті змісту таємних повідомлень.

Сучасна стеганографія має три цілі.

1. *Цифрові відбитки* (ЦВ, Digital Fingerprint). Даний вид стеганографії має на увазі наявність різних стеганографічних міток-повідомлень, для кожної копії контейнера. Як приклад ЦВ можна навести продаж електронних книг (наприклад у форматі *.PDF). При оплаті книги і відправки її одержувачу можна в *.pdf впроваджувати інформацію про e-mail; IP; дані, введені користувачем і т.д.

2. *Стеганографічні водяні знаки* (СВЗ, Stego Watermarking). На відміну від ЦВ, СВЗ передбачають наявність однакових міток для кожної копії контейнера. Зокрема СВЗ можна використовувати для підтвердження авторського права. Наприклад, при записі на відеокамеру можна в кожен кадр вбудовувати інформацію про час запису, моделі відеокамери та / або імені оператора відеокамери. У разі якщо відзнятий матеріал потрапить в руки конкуруючої компанії, можна спробувати використовувати СВЗ для підтвердження авторства запису. Якщо ключ тримати в секреті від власника камери, то за допомогою СВЗ можна підтверджувати справжність фото та / або відео знімків.

3. *Прихована передача даних* (ППД). Це «класична» мета стеганографії, відома з часів Енея Тактика. Завдання – передати дані так, щоб противник не здогадався про сам факт появи повідомлення.

Для кожної з цих трьох цілей слід розробляти свої власні критерії стійкості стеганографічної системи і формальні інформаційно-теоретичні моделі для їх досягнення, тому сенс застосування стеганографії різний.

Розглянувши цілі, перейдемо до практичних застосувань. Пропонуємо 15 сучасних завдань, для яких може бути актуальна стеганографія.

1. Непомітна передача інформації (ППД).

2. Приховане збереження інформації (ППД). Очевидно, що дана задача реалізується на носіях даних, але не в каналах зв'язку. Причому надмірність на багатьох носіях може бути неймовірно великою. Наприклад загальний об'єм даних (з урахуванням кодів RLL), які можна записати на CD диск складають 1828 Мб даних.

3. Недекларованe збереження інформації (ППД). Багато інформаційних ресурсів дозволяють зберігати дані тільки певного виду. Наприклад портал YouTube дозволяє зберігати тільки відеоінформацію у форматах MOV, MPEG4, AVI, WMV, MPEG-PS, FLV, 3GPP, WebM. Однак можна використовувати стеганографії для зберігання даних в інших форматах.

4. Захист виключного права (ЦВ). В якості можливого застосування можна навести голографічний багатоцільовий диск (Holographic Versatile

Disc, HVD). Ці технології передбачають використовувати компаніями теле- і радіомовлення для зберігання відео і аудіо інформації. Наявність ЦВ всередині коригувальних кодів цих дисків може використовуватися в якості основного або додаткового засобу для захисту ліцензійного права. В якості іншого прикладу можна навести інтернет-продаж інформаційних ресурсів. Це можуть бути книги, фільми, музика і т.д. Кожна копія повинна містити ЦВ для ідентифікації особи або спеціальну мітку для перевірки ліцензії.

5. Захист авторського права (ЦВЗ). В даному випадку одним знаком захищається кожна копія контенту.

6. Захист оригінальності документа (ЦВЗ).

7. Індивідуальний відбиток в системі електронного документообігу (ЦВ). В системі електронного документообігу (СЕДО) можна використовувати індивідуальний відбиток всередині * .odt, * .docx та інших документах при роботі з ними користувачем.

8. Водяний знак в DLPсистемах (СВЗ). Стеганографія може бути застосовна для запобігання витоків інформації (Data Leak Prevention, DLP). На відміну від індивідуального відбитку в СЕДО, в даному застосуванні стеганографії при створенні документа, що містить конфіденційний характер, вбудовується певна мітка. При цьому мітка не змінюється, незалежно від кількості копій та / або ревізій документа.

9. Прихована передача керуючого сигналу (ППД). Припустимо, що одержувачем є яка-небудь система (наприклад супутник); а відправником є оператор. В даному випадку стеганографія може бути застосовна для доставки будь-якого керуючого сигналу системі.

10. Стеганографічні botnet-мережі (ППД).

11. Підтвердження достовірності переданої інформації (ЦВ). Стего-повідомлення в даному випадку містить дані, що підтверджують коректність переданих даних контейнера. Як приклад це може бути контрольна сума або хеш-функція (дайджест).

12. Funkspiel «радіогра» (ППД). Стего-повідомлення в даному випадку містить дані, що повідомляють про те, чи варто сприймати інформацію контейнера всерйоз. Якщо стего-повідомлення не пройшло перевірку, то контейнер повинен бути проігнорований одержувачем, незалежно від його вмісту. В даному випадку стеганографія може бути використана для дезінформації противника.

Це далеко не повний перелік можливих застосувань стеганографічних систем в сучасних умовах та найближчих перспективах.

Список використаних джерел

1.Zollner J., Federrath H.,Klimant H., Pfitzmann A., Piotraschke R., Westfeld A., Wicke G., Wolf G. Modeling the security of steganographic system, Proc. 2nd International Workshop on Information Hiding, 1998, LNCS, v.1525, 344-354.