УДК 004.056.53
Зайко Т.А.[1], Сидорський В.С.[2]
[1] канд. техн. наук, доц. НУ «Запорізька політехніка»
[2] студ. гр. КНТ-228 НУ «Запорізька політехніка»

МЕТОДИ МЕРЕЖЕВОЇ СТЕГАНОГРАФІЇ

Інформація має велике значення в усіх сферах людської діяльності, тому способам її передавання також приділяється багато уваги. У певних ситуаціях важливо приховати факт переміщення даних, щоб зменшити ймовірність перехоплення повідомлення. Для цього протягом усієї історії людства розроблювались різноманітні способи приховання інформації, серед яких в реаліях розвитку кіберпростору виділяються методи мережевої стеганографії.

Мережева стеганографія – це спосіб передачі інформації серед звичайних користувацьких даних через «приховані канали» протоколів моделі взаємодії відкритих систем (OSI). Приховані канали можуть існувати у будь-якому відкритому каналі, якому притаманна надмірність [1, с. 2].

Основними параметрами методів такого роду вважається пропускна здатність прихованого каналу, ймовірність виявлення прихованої інформації (стеганограми) та обсяг змін до носія прихованих даних [1, с. 2].

На сьогоднішній день існує значна кількість методів мережевої стеганографії, серед яких до розгляду було обрано такі методи: RSTEG, LACK, TranSteg і передавання інформації через заголовки протоколів TCP/IP та SCTP.

Метод передання інформації через TCP/IP базується на заміні даних необов'язкових чи обов'язкових полів заголовків, наприклад: «Identification», «Initial Sequence Number». Цей метод легко реалізувати, він не порушує функціонал пакета і має невисоку пропускну здатність. Однак існує обмеження при роботі з IP-заголовком: необхідно знати й не перевищувати MTU мережі, щоб поле «Ідентифікатор» не використовувалось [1, с. 3].

Метод на основі протоколу SCTP використовує дві його особливості.

Перша особливість полягає у структурі пакета: він поділений на шматки (chunks), кожен з яких містить власні обов'язкові та необов'язкові поля. Таким чином можна модифікувати дані подібно тому, як дані модифікуються у методі приховання інформації у заголовках TCP/IP.

Друга особливість полягає в тому, що відправник може не надсилати усі дані та проінформувати про це отримувача. В такому випадку втрачені пакети не будуть автоматично надсилатися ще раз. Завдяки цьому можливо затримати певну кількість пакетів, замінивши їх зміст стеганограмою [1, с. 4].

Метод RSTEG (Retransmission STEGanography) використовує механізм повторного надіслання пакетів у разі відсутності підтвердження отримання. Відправник надсилає пакети звичайним чином,однак при одержанні певного пакета отримувач навмисно не надсилає пакет-відповідь, після чого відправник має автоматично наново надіслати пакет, який спеціально змінюється так, щоб містити стеганограму. Отримувач одержує пакет, читає інформацію та знову не відповідає, а відправник знову надсилає нібито той самий пакет, який більше не містить прихованого повідомлення, після чого отримувач підтверджує отримання [1, с. 5].

Метод LACK (Lost Audio PaCKets steganography) засновано на затримці звукових пакетів при використанні голосового зв'язку за протоколом IP (VoIP). Затримані пакети не використовуються у процесі зв'язку і містять приховану інформацію. Якщо отримувач знає про передачу, він може зчитати дані, в іншому випадку пакети автоматично видаляються [1, с. 5].

Метод TranSteg (Transcoding Steganography) використовує перекодування звукових пакетів для зменшення їх розміру до мінімально допустимого, після чого отримана різниця між звичайними та стиснутими даними заповнюється прихованою інформацією [1, с. 4].

Методи редагування заголовків найлегші для реалізації, вони мають найменшу пропускну здатність, складність виявлення та обсяг змін до носія інформації. Засновані на редагуванні пакетів VoIP методи дозволяють передавати значні обсяги інформації, але для цього необхідно, щоб дзвінок продовжувався певний час. Ці методи складно реалізувати, в певних випадках навіть неможливо. При цьому також необхідно вносити значні зміни до складу пакетів даних, однак в результаті виявити передачу прихованих даних досить складно. Прості методи можуть бути модифіковані для ускладнення процедури виявлення і підвищення пропускної здатності. Прикладом є гібридний метод RSTEG та методи використання особливостей протоколу SCTP [1].

Окремо слід зазначити, що експлуатація прихованих каналів мережевих протоколів може використовуватися не тільки для нешкідливого приховання інформації, а і для зловмисних дій, що в умовах сучасного розвитку інтернет-технологій становить значну загрозу. Тому дослідження цієї теми є важливим

для запобігання мережевим атакам і витоку конфіденційних, секретних, технічних даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Пескова О.Ю. Применение сетевой стеганографии для скрытия данных, передаваемых по каналам связи [Электронный ресурс] / О.Ю. Пескова, Ю.Г. Халабурда // Научная электронная библиотека «КиберЛенинка». – Режим доступа : https://cyberleninka.ru/article/n/primenenie-setevoy-steganografii-dlya-skrytiya-dannyh-peredavaemyh-po-kanalam-svyazi/pdf