УДК 378.147

Д. А. Моторнюк

СТЕГАНОГРАФІЧНИЙ МЕТОД ПЕРЕДАВАННЯ ІНФОРМАЦІЇ В ЗАГОЛОВКАХ ПРОТОКОЛЬНИХ БЛОКІВ ДАНИХ

Вінницький національний технічний університет

Анотація

Розглянуто різні методи прихованої передачі даних, а саме передача інформації в службових полях.

Ключові слова: стеганографія, інкапсуляція, передача даних.

Abstract

Different methods of latent data transmission are considered, namely the transfer of information in the field of service.

Keywords: steganography, encapsulation, data transmission.

.

Вступ

У сучасному світі передача інформації в електронному вигляді вже встигла стати повсякденністю. Але цим можуть скористатись зловмисники, які хочуть перехопити інформацію. Тому дуже гостро постає питання захисту даних. І тут можна піти шляхом використання криптографії, тобто, шифрувати інформацію перед передачею. Але в цьому випадку зловмисник може перехопити повідомлення і, можливо, розшифрувати їх. Можна також піти шляхом використання стеганографії. При цьому зловмисник не повинен дізнатись про сам факт передачі повідомлення. Але якщо зловмисник зможе дізнатись про передачу і перехопить повідомлення, більше не буде ніякого захисту. Тому можна сказати, що обидва способи мають свої недоліки. І щоб підвищити рівень безпеки при передачі інформації, потрібно збільшити складність шифрування в криптографічному методі, знайти нові способи передачі інформації в стеганографічному методі або комбінувати їх.

Основна частина

Стеганографія це метод передачі інформації при якому приховується сам факт цієї передачі. Отже розглянемо існуючі методи:

Метод оверлея заключається в тому, що в файлах деяких форматів вказується його межа, і при запуску файлу програма буде зчитувати його лише до цієї межі. А інформація, яка міститься в так званому оверлеї, що знаходиться після мітки межі.

Метод вбудованих повідомлень вбудовує в контейнер повідомлення по певному алгоритму, який відомий обом сторонам при передачі.

LSB-стеганографія – використовує молодші біти контейнерів, для передачі інформації, але при використанні великої кількості біт у оригінальному контейнері з’являються артефакти.

Метод приховування в службових полях – заклечається в передачі даних в полях, які не використовуються на момент передачі.

Для нас цікавий саме останній метод. При передачі даних по мережі існує декілька рівнів інкапсуляції повідомлення, окрім того на кожному з цих рівнів до повідомлення додається заголовок, що містить певну кількість полів. Звісно не всі поля використовуються при передачі і це дає можливість помістити в них повідомлення.

Одним із найпоширеніших типів пакетів, що передаються по мереж. і є ICMP-пакети. Це повідомлення, що виконують службові функції. І при певних значеннях полів, ці пакети пропускаються всіма маршрутизаторами.

Також є можливість використовувати поля IP-пакета. При фрагментації кожному пакету його фрагменту присвоюється ID, яке формується випадково. Оскільки ідентифікатор формується рандомно ми можемо заповнити його частиною повідомлення.

В заголовках на всіх рівнях інкапсуляції повідомлення можна заміняти службові поля, що не використовуються, можна заповнити частинами повідомлення. Також можливе комбінування декількох варіантів або паралельна передача декількох повідомлень.

Висновок

І хоча рівень прихованої передачі даних знаходиться на досить високому рівні, все частіше їх вдається перехоплювати. Тому досить актуальна проблема пошуку нових контейнерів для стеганографії.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Стеганография в IP-пакетах [Електронний ресурс]. – Режим доступу:. https://habr.com/ru/post/413851/ - Назва з екрану.

2. TCP стеганография или как скрыть передачу данных в интернете [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/60726/ - Назва з екрану.

2. Стеганография в современных кибератаках [Електронний ресурс]. – Режим доступу: https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/ - Назва з екрану.

Моторнюк Дмитро Андрійович — студент групи 1КІ – 18м, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 2ki14b.motorniuk@gmail.com;

Науковий керівник: ***Захарченко Сергій Михайлович*** – канд. техн. наук, доцент кафедри ОТ, Вінницький національний технічний університет, м. Вінниця;

Motorniuk Dmytro A. — Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email : 2ki14b.motorniuk@gmail.com;

Supervisor: ***Zaharchenko Sergiy M.*** – Cand. Sc. (Eng.), Assistant Professor of the Chair of CE, Vinnytsia National Technical University, Vinnytsia.