СТЕГАНОГРАФИЧЕСКОЕ СКРЫТИЕ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ДАННЫХ

Шишонок А.А.
Кафедра систем управления
Научный руководитель: Сорока Н.И., доцент кафедры СУ, канд. техн. наук, доцент
e-mail: weron3004@mail.ru

***Аннотация* — В последнее десятилетие, в связи с широким распространением информационных технологии и необходимостью защиты важной информации, появился интерес к стеганографическим методам защиты информации. В данной статье описаны основные понятия и принципы построения стеганографических систем, а также рассматривается применение стеганографических методов в сетевых протоколах передачи данных.**

Ключевые слова: стеганография, сокрытие информации, стегосистема, контейнер, сетевой протокол

Введение

Информация является одним из ценнейших предметов современной жизни. Получение доступа к ней с появлением глобальных компьютерных сетей стало невероятно простым. Легкость и скорость такого доступа значительно повысили угрозу нарушения безопасности данных при отсутствии мер относительно их защиты.

Задачей стеганографии является скрытие факта существования секретной информации при ее передаче, обработке или хранении. Методы стеганографии позволяют не только скрыто передавать данные, но и позволяют решать проблемы помехоустойчивой аутентификации, защиты информации от несанкционированного копирования, отслеживания распространения информации через сети, поиска информации в базах данных [1].

Основные понятия и принципы построения стеганографических систем.

Стеганографическое сокрытие информации осуществляется различными способами, однако общей чертой всех методов является то, что скрываемое сообщение встраивается в некий непривлекающий внимания объект, который затем открыто пересылается адресату.

На рис. 1 приведена структурная схема типичной стеганографической системы (стегосистемы) [2].

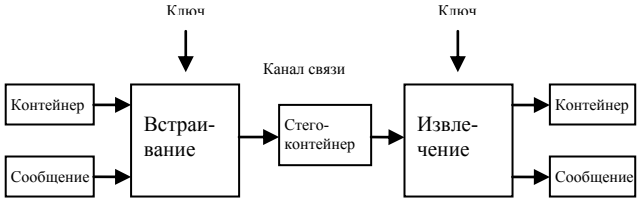

Рис. 1. Структурная схема типичной стеганосистемы

Основными стеганографическими понятиями являются сообщение и контейнер. Сообщение — это секретная информация, наличие которой необходимо скрыть. Контейнером называется несекретная информация, которую можно использовать для скрытия сообщения. Основной задачей построения стегосистемы – является корректный выбор контейнера.

Применение стеганографических методов в протоколах передачи данных

В настоящее время большое внимание уделяется применению стеганографии для скрытия данных в сетевом трафике [3]. Сокрытие информации основывается на использовании, так называемых, скрытых каналов протоколов передачи данных. Выделяют два направления: в первом используются временные параметры сетевого протокола [4], во втором используются структура сетевого протокола.

Рассмотрим возможность применения стеганографии в сетевом протоколе TCP/IP. В качестве контейнера используется заголовок пакета протокола IP. Его структура приведена на рис. 2 [5].

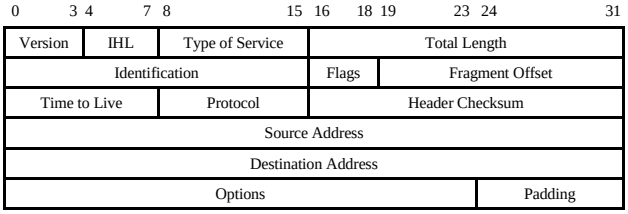

Рис. 2. Структура заголовка IP-датаграммы

В соответствии со спецификацией протокола IP [5], поле Identification содержит уникальный идентификатор пакета, который используется для сборки фрагментированных датаграмм. Значение этого поля не зависит от значений других полей заголовка и сохраняется при фрагментации. Таким образом алфавит передаваемого сообщения может быть закодирован с помощью данного поля.

[1] Конахович, Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А. Ю. Пузыренко. – К.: МК-Пресс, 2006. – 288 с, ил.

[2] Грибунин, В. Г. Цифровая стегано-графия / В. Г.Грибунин, И. Н. Оков, И. В. Туринцев. – М.: Солон-Пресс, 2002. — 272 с., ил.

[3] Handel, T., Sandford, M.: Hiding Data in the OSI Network Model, Proc. 1st International Workshop. Information Hiding, 1996 pp. 23–38.

[4] S. Cabuk, C. E. Brodley, and C. Shields. IP covert timing channels: design and detection. In CCS ’04: Proceedings of the 11th ACM conference on Computer and communications security, pages 178–187, New York, NY, USA, 2004. ACM Press.

[5] Снейдер, И. Эффективное программирование TCP/IP / И. Снейдер. Библиотека программиста. – СПб: Питер, 2001.- 320 с.

[6] Murdoch, S.J., Lewis, S., Embedding Covert Channels into TCP/IP, Information Hiding (2005), pp. 247-262.