Оценка пропускной способности стеганографических каналов передачи информации и возможности их обнаружения методом статистического анализа

Бусыгин А.Г.
busygin@neo-bit.ru

Классификация стеганографических каналов передачи информации

Генерация собственного трафика

- Активные
- Пассивные

Наличие шума в стеганографическом канале

- Зашумлённые
- Незашумлённые

Способ кодирования передаваемой информации

- Временные
- Туннелирующие
- Основанные на событиях

Оценка пропускной способности стеганографических каналов

Сеганографический канал	Класс	Оценка пропускной способности, Кбит/с
Поля заголовков IP и TCP	• Активный • Туннелирующий	2
«NUSHU»	• Пассивный • Туннелирующий	0,03
«RSTEG»	• Активный • Туннелирующий	1
Поля заголовков HTTP	• **Активный** • **Туннелирующий**	**256**
«Infranet»	• **Активный** • **Осн. на событиях**	**256**
DNS TTL	• Активный • Туннелирующий	0,9
«SkypeMorph»	• Активный • Туннелирующий	40

Противодействие стеганографическим каналам

Стеганографический канал	Способы противодействия
Поля заголовков IP и TCP	• Обнаружение аномалий в распределении длин пакетов, размеров окон и проч. • Нормализация заголовков.
«NUSHU»	• Обнаружение с помощью нейронной сети Элмана (не обнаруживается статистическими методами в силу случайности значений ISN).
«RSTEG»	• Обнаружение аномалий в частоте возникновения повторных передач.
Поля заголовков HTTP	• Нормализация заголовков. • Запрет нестандартных заголовков. • Проверка соответствия заголовков Set-Cookie/Cookie.
«Infranet»	• **(Не предложено общего подхода к обнаружению).**
DNS TTL	• Обнаружение аномалий в распределении значений поля TTL.
«SkypeMorph»	• Возможна полная блокировка трафика Skype (не обнаруживается статистическими методами, поскольку мимикрирует под видео-трафик Skype).

Представление стеганографического канала основанного на событиях

Алфавит исходных (скрываемых) сообщений:

$$\mathbb{X} = \{x_1, x_2, \dots, x_{\#\mathbb{X}}\}, \#\mathbb{X} \geq 2.$$

Множество исходных сообщений длины s:

$$\mathbb{X}^s.$$

Множество событий несущего протокола:

$$\mathbb{C} = \{c_1, c_2, \dots, c_{\#\mathbb{C}}\}, \#\mathbb{C} \geq \#\mathbb{X}^s.$$

Алфавит несущего протокола:

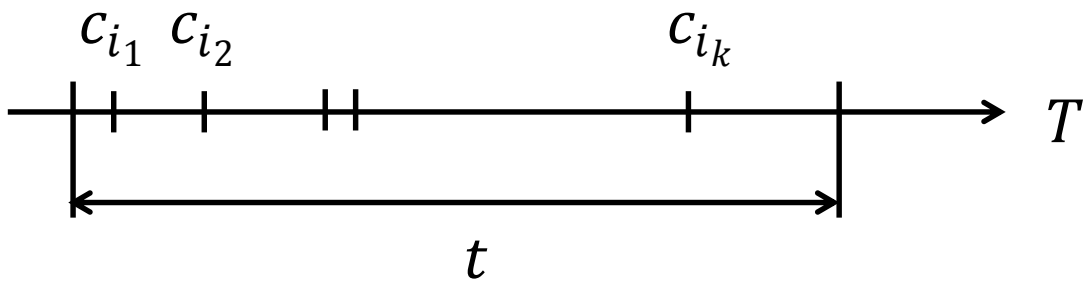
$$\mathbb{Y} = \{y_1, y_2, \dots, y_{\#\mathbb{Y}}\}.$$

Кодирование исходных сообщений:

$$\psi\varphi, \qquad \varphi: \mathbb{X}^s \to \mathbb{C}, \qquad \psi: \mathbb{C} \to \mathbb{Y}^*.$$

Метод противодействия (1)

Рассматривается временной интервал длинны t, в течение которого произошло k событий несущего протокола:



Вычисляется частота возникновения событий и средняя длина сообщения, используемого для представления события несущего протокола:

$$(\omega_{\mathbb{C}}, l): \qquad \omega_{\mathbb{C}} = \frac{k}{t}, \qquad l = \frac{\sum_{j=1}^{k} \mathrm{len}\left(c_{i_j}\right)}{k}.$$

Метод противодействия (2)

Задаётся минимальная пропускная способность поведенческого стеганографического канала:

$$\omega_{\mathbb{X}_{\min}}$$

Определяется максимально допустимая частота возникновения событий несущего протокола:

$$\omega_{\mathbb{C}_{\max}}$$

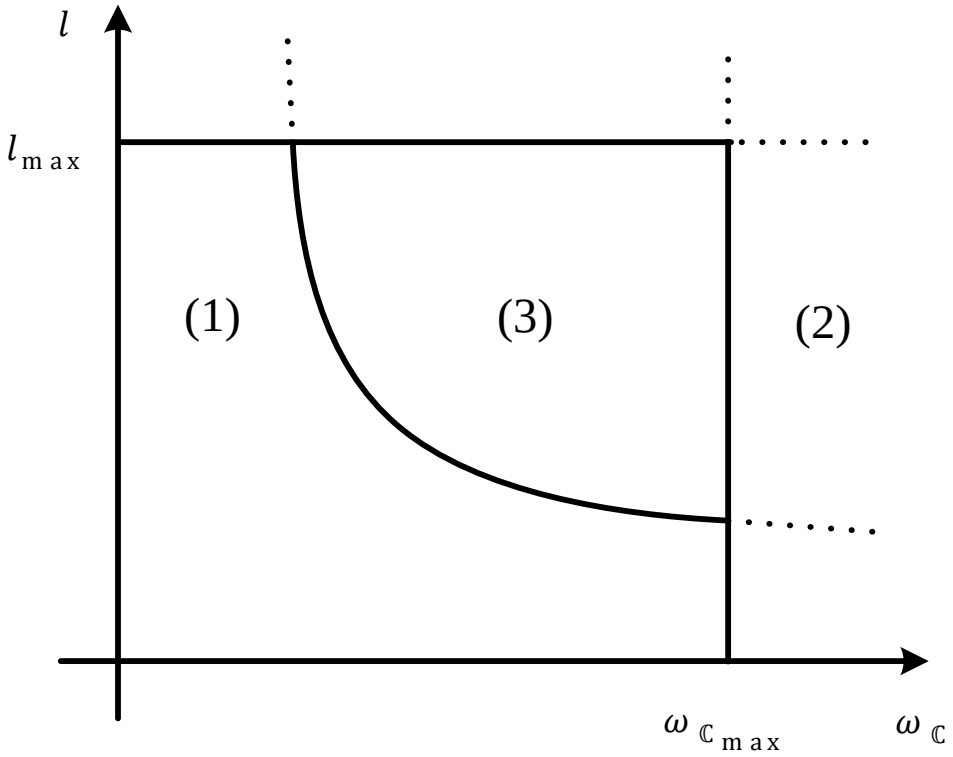
Определяется максимально допустимая длина сообщения несущего протокола:

$$l_{\max}$$

Определяется принадлежность пары $(\omega_{\mathbb{C}}, l)$ к одному из трёх множеств, определяемых следующей системой неравенств:

$$\begin{cases} l \geq \dfrac{\omega_{\mathbb{X}_{\min}}}{\omega_{\mathbb{C}} \log_{\#\mathbb{X}} \#\mathbb{Y}} \\ l \leq l_{\max} \\ \omega_C \leq \omega_{\mathbb{C}_{\max}} \end{cases}.$$

Графическое представление предложенного критерия обнаружения поведенческих стеганографических каналов



(1) Стеганографический канал отсутствует.

(2) Стеганографический канал существует.

(3) Стеганографический канал не обнаруживается данным методом.

Результаты

- Выявлен класс стеганографических каналов передачи информации, обладающих высокой пропускной способностью и сложностью обнаружения.

- Предложен метод противодействия данному классу стеганографических каналов передачи информации.


НОВЫЕ БЕЗОПАСНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
НЕОБИТ