XXIX Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч.IV: С.16
, 2001.

УДК 681.222.

А.В. Маленкова (асп., каф. "Прикладная математика"),
Н.О. Вильчевский, д.т.н, проф., В.Е. Клавдиев, к.т.н, доц.

РАЗРАБОТКА СРЕДСТВ ОБНАРУЖЕНИЯ И ЗАЩИТЫ ОТ УДАЛЕННЫХ АТАК НА УЗЛЫ ГЛОБАЛЬНОЙ КОМПЬЮТЕРНОЙ СЕТИ

Данная работа посвящена рассмотрению возможности обнаружения атак хакеров на удаленные узлы глобальных компьютерных сетей, в частности Internet, и принципам построения защиты от подобного рода атак.

Детальное рассмотрение схемы удаленной атаки "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)" позволило построить ее математическую модель. При этом для определения времени задержки пакетов в сети использовался экспоненциальный закон распределения вероятностей, что позволило установить зависимость вероятности удачной атаки по приведенной в работе схеме от статистических параметров сети.

Рассмотрим пример удаленной атаки "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)". Схема данной атаки приведена на рис. 1.

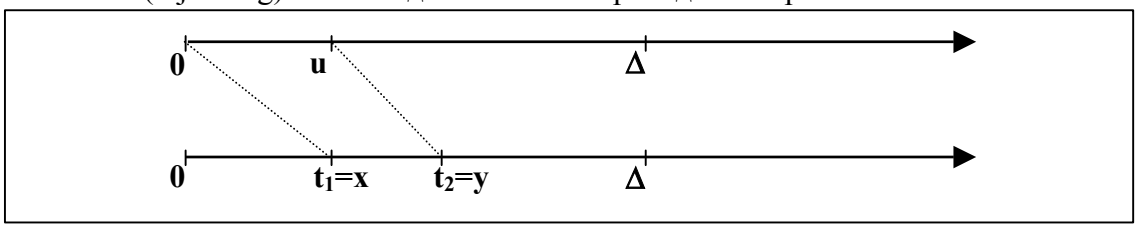

Рис. 1. Схема удаленной атаки "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)"

На данном рисунке: u — интервал времени между отправкой первой и второй серий пакетов; $t_1=x$ — момент приема первой серии пакетов; $t_2=y$ — момент приема второй серии пакетов; Δ — общее время атаки.

Обозначим: $F(t)$ — вероятность того, что задержка в сети (время доставки пакета от отправителя до получателя) не более t; P_n — вероятность того, что пакет с нужным идентификационным номером n содержится в посылаемой серии пакетов. Тогда вероятность успешной атаки можно выразить с помощью формулы:

$$P = \int_0^{\Delta}\int_x^{\Delta} P_n\, dF(x)dF(y-u) = P_n[F(\Delta)F(\Delta-u) - \int_u^{\Delta} F(x-u)dF(x)]$$

Найдем зависимость вероятности удачной атаки по приведенной схеме от параметра u, которым может манипулировать хакер. При этом воспользуемся экспоненциальным законом распределения вероятности $F(t)$ и получим:

$$F(\tau) = 1 - e^{-\lambda\tau},\ \tau \ge 0,\ \lambda = \frac{1}{t_{cp}} \qquad P = P_n[1 - e^{-\lambda(\Delta-u)} + \frac{1}{2}e^{-\lambda(2\Delta-u)} - \frac{1}{2}e^{-\lambda u}]$$

Для уточнения этой формулы может быть введено минимальное время запаздывания пакетов в сети: u^*.

Полученные в данной работе результаты могут быть применены для анализа возможности атаки по схеме "Подмена одного из субъектов TCP-соединения в сети Internet (hijacking)" на какой-либо определенный узел компьютерной сети.