Вероятностно-временные характеристики компьютерной атаки типа «Анализ сетевого трафика»

Probability and time characteristics of computer attack like «Network traffic analysis»

Ключевые слова: компьютерные атаки – computer attacks; вероятностно-временные характеристики – probability and time characteristics; профильная модель – profile model; математическая модель – mathematical model; информационно-телекоммуникационная сеть – information and telecommunication network.

В статье описывается профильная модель компьютерной атаки типа «Анализ сетевого трафика», представленная в виде стохастической сети. На основе предлагаемой модели, авторы, используя метод топологического преобразования стохастических сетей, обосновали вероятностно-временные характеристики указанной компьютерной атаки. Представленный подход позволяет обосновать направления по защите информационно-телекоммуникационной сети.

This paper describes the profile model of computer attack like «Network traffic analysis», presented in the form of a stochastic network. On the basis of the proposed model, the authors, using the method of the topological transformation of stochastic networks substantiated probability and time characteristics of this computer attack. The presented approach allows to justify the directions for protection of information and telecommunications network.

КОЦЫНЯК / KOTSINYAK M.
Михаил Антонович
Профессор, доктор технических наук,
Военная Академия Связи,
Санкт-Петербург

ЛАУТА / LAUTA O.
Олег Сергеевич
(Laos-82@yandex.ru)
адъюнкт,
Военная Академия Связи,
Санкт-Петербург

ОСАДЧИЙ / OSADCHIY S.
Сергей Александрович
(spb.sos@hotmail.com)
ведущий инженер,
Санкт-Петербургский филиал «Ленинградское отделение центрального научно-исследовательского института связи»,
Санкт-Петербург

Основная цель любой компьютерной атаки — получить несанкционированный доступ к информации. Существуют две принципиальные возможности доступа к информации — перехват и искажение. Перехват информации обеспечивает доступ к информации. Он нарушает ее конфиденциальность и является первым шагом к модификации (искажению) информации. Примером перехвата информации может служить анализ сетевого трафика. В этом случае имеется несанкционированный доступ к информации без возможности ее искажения [2].

Анализ сетевого трафика позволяет, во-первых, изучить логику работы информационно-телекоммуникационной сети (ИТКС), то есть определить соответствие событий, происходящих в системе, и команд, что достигается путем перехвата и анализа пакетов сообщений на канальном уровне. Во-вторых, анализ сетевого трафика позволяет злоумышленнику получить доступ к семантической составляющей трафика ИТКС.

Компьютерные атаки обладают вероятностно-временными характеристиками (ВВХ), определение которых позволяет оценить степень их опасности, выбрать и реализовать меры защиты.

Для исследования и определения ВВХ компьютерных атак необходима разработка их моделей (профильных, математических).

Профильная модель атаки. Задана ИТКС. При реализации компьютерной атаки «Анализ сетевого трафика» злоумышленник осуществляет запуск аппаратно-программного комплекса (сетевого сканера) за среднее время $\overline{t_{зап.}}$ с функцией распределения времени $W(t)$, задает параметры,

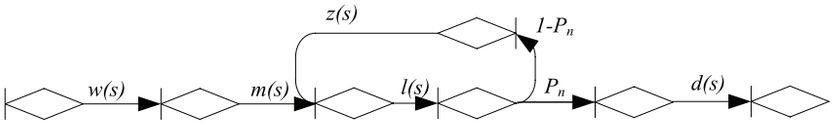

Рис. 1. Стохастическая сеть компьютерной атаки типа «Анализ сетевого трафика»

определяющие перехват информации за среднее время $\overline{t_{\text{инф.}}}$ с функцией распределения времени $M(t)$ и осуществляет ее перехват с вероятностью Pn за среднее время $\overline{t_{\text{пер.}}}$, с функцией распределения времени $L(t)$. После перехвата сетевой сканер осуществляет статистический анализ и подготовку отчета за среднее время $\overline{t_{\text{стат.анализ}}}$ с функцией распределения времени $D(t)$. Если информация не перехвачена, то с вероятностью (1-Pn) сетевой сканер запускается повторно за среднее время $\overline{t_{\text{повт.}}}$ и функцией распределения времени $Z(t)$.

Требуется определить интегральную функцию распределения вероятности $F(t)$ и среднее время $\overline{T}$ реализации компьютерной атаки типа «Анализ сетевого трафика».

Математическая модель атаки. Описанный выше процесс реализации компьютерной атаки представим в виде стохастической сети (рис. 1).

Используя уравнение Мейсона, преобразование Лапласа, разложение Хевисайда и метод топологического преобразования стохастических сетей [1], функцию распределения вероятности времени реализации компьютерной атаки можно определить следующим образом

$$F(t) = \sum_{k=1}^{5} \frac{w \cdot m \cdot l \cdot P_n \cdot d \cdot (z + s_k)}{\varphi} \cdot \frac{1 - \exp[s_k t]}{-s_k}, \quad (1)$$

а среднее время $\overline{T}$, затрачиваемое на реализацию компьютерной атаки определяется так

$$\overline{T} = \sum_{k=1}^{5} \frac{w \cdot m \cdot l \cdot P_n \cdot d \cdot (z + s_k)}{\varphi'} \cdot \frac{1 - \exp\,[s_k t]}{-s_k}, \quad (2)$$

где:

$w(s) = \int_0^\infty \exp(-st)\, d[W(t)] = \frac{w}{w+s}$ – преобразование Лапласа функции распределения времени запуска сетевого сканера;

$m(s) = \int_0^\infty \exp(-st)\, d[M(t)] = \frac{m}{m+s}$ – преобразование Лапласа функции распределения времени ввода параметров, определяющих перехват информации;

$l(s) = \int_0^\infty \exp(-st)\, d[L(t)] = \frac{l}{l+s}$ – преобразование Лапласа функции распределения времени перехвата информации;

$d(s) = \int_0^\infty \exp(-st)\, d[D(t)] = \frac{d}{d+s}$ – преобразование Лапласа функции распределения времени анализа перехваченной информации и подготовки отчета;

$z(s) = \int_0^\infty \exp(-st)\, d[Z(t)] = \frac{z}{z+s}$ – преобразование Лапласа функции распределения времени повторного запуска сетевого сканера;

$W(t) = 1 - \exp[-wt]$ – функция распределения времени запуска сетевого сканера;

$M(t) = 1 - \exp[-mt]$ – функция распределения времени ввода параметров, определяющих перехват информации;

$L(t) = 1 - \exp[-lt]$ – функция распределения времени перехвата информации;

$D(t) = 1 - \exp[-dt]$ – функция распределения времени анализа перехваченной информации и подготовки отчета;

$Z(t) = 1 - \exp[-zt]$ – функция распределения времени повторного запуска сетевого сканера;

$$w = \frac{1}{t_{\text{зап}}};\ m = \frac{1}{t_{\text{инф}}};\ l = \frac{1}{t_{\text{пер}}};$$

$$d = \frac{1}{t_{\text{стат.анализ}}};\ z = \frac{1}{t_{\text{повт}}}$$

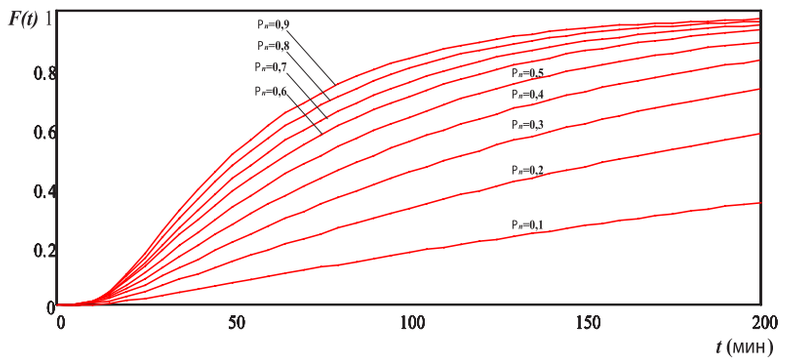

Рис. 1. а) зависимость интегральной функции распределения вероятности от времени реализации компьютерной атаки

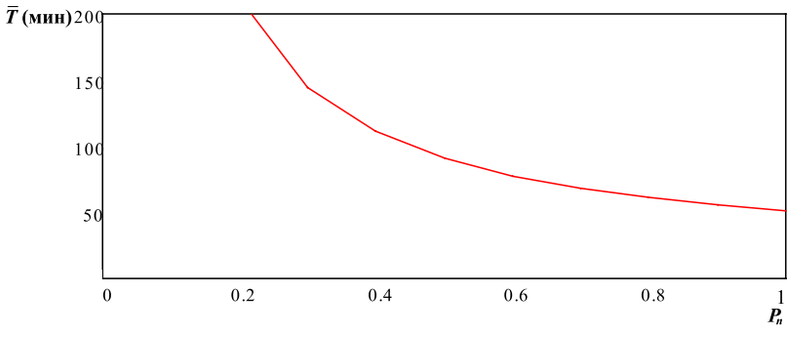

Рис. 2. б) зависимость среднего времени реализации компьютерной атаки от вероятности перехвата информации сетевым сканером
Вероятностно-временные характеристики компьютерной атаки типа «Анализ сетевого трафика»

$\overline{t_{зап}}$, $\overline{t_{инф}}$, $\overline{t_{пер}}$, $\overline{t_{стат.анализ}}$, $\overline{t_{повт}}$ – среднее время каждого процесса компьютерной атаки;

$\varphi'(s_k)$-значение производной многочлена знаменателя в точке s_k.

Результаты расчетов $F(t)$ и $\overline{T}$ представлены в виде зависимостей на рисунке 2. В качестве исходных данных используются следующие значения времени и вероятности, соответствующие профильной модели компьютерной атаки:

$$\overline{t_{зап}} = 7_{мин}, \overline{t_{инф}} = 5_{мин}, \overline{t_{пер}} = 38_{мин}, \overline{t_{стат.анализ}} = 5_{мин}, \overline{t_{повт}} = 4_{мин}, P_n = 0{,}1 \ldots 0{,}9.$$

Анализ полученных результатов позволяет сделать выводы:

– среднее время реализации компьютерной атаки типа «Анализ сетевого трафика» с вероятностью 0,8 составляет 60 мин;

– полученные зависимости позволяют оценить влияние времени перехвата информации на показатель эффективности реализации компьютерной атаки «Анализ сетевого трафика». Видно, что увеличение вероятности перехвата информации Pn уменьшает среднее время реализации компьютерной атаки «анализ сетевого трафика».

– результаты моделирования могут быть использованы при обосновании направлений разработки системы защиты ИТКС, целью которой является предотвращение (затруднение) реализации компьютерной атаки;

– адекватность разработанной модели подтверждается её соответствием статистическим данным по атакам.

Литература

1. Привалов А.А. Метод топологического преобразования стохастических сетей и его использование для анализа систем связи ВМФ. – СПб: ВМА, 2000 г.

2. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. – Москва, РадиоСофт, 2011 г., 229 с.