УДК 681.3

МОДЕЛИРОВАНИЕ ПРОЦЕССА АТАКИ ПЕРСПЕКТИВНЫМИ СРЕДСТВАМИ СЪЕМА ИНФОРМАЦИИ: МОДЕЛИ ПЕРЕХВАТА ТРАФИКА

А.Е. Киселев, А.С. Пахомова, А.В. Бабурин, И.В. Шевченко

В данной работе рассматривается моделирование процесса атаки перспективными средствами съема информации на основе сетей Петри-Маркова. Дальнейшее описание модели перехвата трафика позволяет получить вид функции ущерба и сопоставить ее со статистическими данными

Ключевые слова: атака, средства негласного съема информации, ущерб, трафик

По данным WASC Threat Classification [1] выделяют три основных вида сниффинга:

- сниффинг во время обновления программного обеспечения;
- сниффинг во время первоначальной установки программного обеспечения;
- сниффинг во время установки патчей.

Но не стоит забывать что сниффинг пакетов по различным протоколам (*Telnet, FTP, SMTP, POP3 и т.д.*) реализуется при любом обмене пакетами между двумя хостами по wi-fi каналу связи.

Смоделируем атаку, направленную на съем критически важной информации, в распределенных вычислительных системах с помощью сети Петри-Маркова. Для этого рассмотрим сниффинг-атаку с использованием перспективных средств мониторинга сети и съема информации [2].

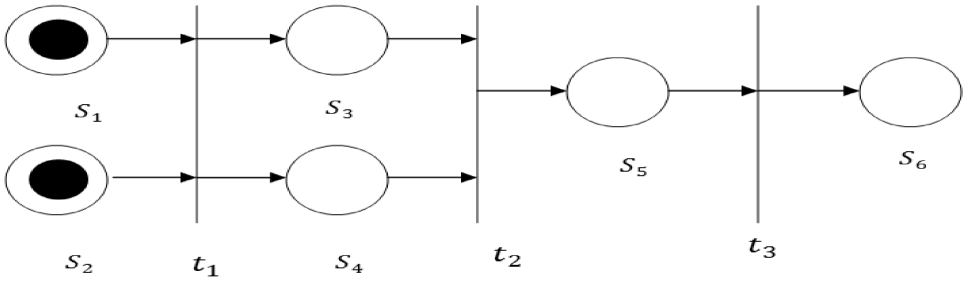


Рис. 1. Вид сети Петри-Маркова для общего вида сниффинг - атаки с использованием перспективных средств съема информации

S_1 – обработка данных на одном из элементов распределенной вычислительной сети

S_2 – злоумышленник настроил сниффер

t_1 – сетевая разведка

S_3 – прием/передача данных по wi-fi каналам

S_4 – злоумышленник готов к перехвату

t_2 – перехват данных

S_5 – информация получена злоумышленником

S_6 – анализ перехваченной информации

Запишем элементы матрицы, которые определяют логические функции срабатывания сети (без учета направленности дуг графа)

Киселев Антон Евгеньевич – ВГТУ, студент, e-mail: manc@comch.ru
Пахомова Анна Степановна – ВГТУ, канд. техн. наук, ст. науч. сотрудник, e-mail: manc@comch.ru
Бабурин Александр Вильямович – ВГТУ, д-р. техн наук, глав. науч. сотрудник, e-mail: manc@comch.ru
Шевченко Игорь Викторович – ВГТУ, студент, e-mail: mnac@comch.ru

$V_{S_1 t_2} =$

	t_1	t_2	t_3
S_1	1	0	0
S_2	1	0	0
S_3	0	1	0
S_4	0	1	0
S_5	0	$S_1 t_1 \cap S_2 t_1$	1
S_6	0	0	1

Построим для данной сети Петри-Маркова систему интегрально-дифференциальных уравнений.

$$\Phi_{S_1 t_1}(t) = \lambda_{11} \int_0^t f_{S_1 t_1}(\tau) d\tau,$$

$$\Phi_{S_2 t_1}(t) = \lambda_{21} \int_0^t f_{S_2 t_1}(\tau) d\tau,$$

$$\Phi_{S_3 t_2}(t) = \lambda_{32} \int_0^t f_{S_3 t_2}(\tau) d\tau,$$

$$\Phi_{S_4 t_2}(t) = \lambda_{42} \int_0^t f_{S_4 t_2}(\tau) d\tau,$$

$$\Phi_{S_5 t_3}(t) = \lambda_{32} \int_0^t f_{S_5 t_2}(\tau) \Phi_1(t-\tau) d\tau, \quad (1)$$

$$\Phi_{S_6 t_3}(t) = \lambda_{43} \int_0^t f_{S_6 t_3}(\tau) \Phi_1(t-\tau) d\tau,$$

$$\Phi_1(t) = \int_0^t f_{S_1 t_1}(\tau)\, \Phi_{S_2 t_1}(\tau) + f_{S_2 t_1}(\tau) \Phi_{S_1 t_1}(\tau) + f_{S_3 t_2}(\tau) \Phi_{S_4 t_2}(\tau) +$$

$$+ f_{S_4 t_2}(\tau) \Phi_{S_3 t_2}(\tau) d\tau.$$

Полагаем, что плотности распределения вероятностей являются экспоненциальными зависимостями и имеют вид:

$$f_{S_i t_j} = \beta_{ij} e^{-\beta_{ij} t}, \quad (2)$$

где $\beta = \frac{1}{\tau_{ij}}$ при $i = 1,\ldots,6$; $j = 1,\ldots,3$.

Применяя пуассоновское приближение, получаем среднее время перемещения по

сети Петри-Маркова из начальной позиции до конечного перехода и вероятность этого перемещения:

$$\tau_1 = \frac{\tau_{11}^2+\tau_{11}\tau_{21}+\tau_{21}^2}{\tau_{11}+\tau_{21}},$$

$$\tau_2 = \frac{\tau_{12}^2+\tau_{12}\tau_{22}+\tau_{22}^2}{\tau_{12}+\tau_{22}},$$

$$\tau_3 = \tau_1 + \tau_2 + \tau_{32},$$

$$\tau_4 = \tau_1 + \tau_2 + \tau_{32} + \tau_{42},$$

$$\tau = \frac{\tau_{11}^2 + \tau_{11}\tau_{21} + \tau_{21}^2}{\tau_{11} + \tau_{21}} + \frac{\tau_{12}^2 + \tau_{12}\tau_{22} + \tau_{22}^2}{\tau_{12} + \tau_{22}} + \tau_{32} + \tau_{42},$$

$$P(t) = 1 - e^{-\frac{1}{\tau}t}.$$

где:

τ_{11} =5с – среднее время работы хоста в сети необходимое для мониторинга сети

τ_{21}=20с - среднее время настройки программы для реализации сетевой разведки

τ_{12} = 0,5с - среднее время передачи количества пакетов по сети достаточного для анализа

τ_{22} – 0,1с - среднее время подготовки к перехвату

τ_{32} – 0,1с среднее время перехвата пакетов

τ_{42} – 0,5 с среднее время анализа пакетов

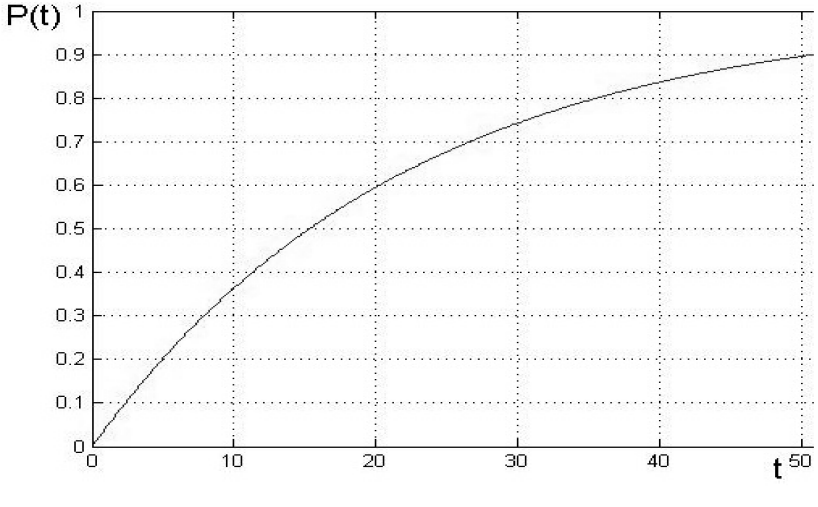


Рис. 2. Зависимость вероятности реализации сниффинг-атак с помощью перспективных средств съема информации от времени

Представленная с помощью сетей-Петри Маркова модель, является обобщенной моделью атаки с помощью перспективных средств съема информации. По приведенной ранее классификации средств съема информации можно смоделировать любую сниффинг - атаку для каждого класса средств в отдельности. Так как схема реализации атаки практически одинакова для всех классов, то данные модели будут отличаться лишь используемым программным обеспечением.

В упрощенном виде модель перехвата трафика предполагает наличие хоста работающего в сети и хоста злоумышленника, встраивающегося в сеть по wi-fi каналу. Проведя сетевую разведку.

Хост злоумышленника начинает мониторинг сети с сохранением следующих данных:

- пакеты с информацией о времени получения пакета, MAC-адресах отправителя и получателя, IP-адресах отправителя и получателя, протоколе передачи, портах источника и получателя пакетов, размер TCP-окна, номер последовательности пакета и номер подтверждения этого пакета
- декодированная информация об отдельных полях пакета;
- содержимое самого пакета [3].

Пусть произвольный хост сети, состоящей из постоянного количества M хостов, может находиться в двух состояниях– уязвимом (S) и прослушиваемом (J), т.е. S +J = M. Положим что сниффинг wi-fi трафика происходит с постоянной скоростью ξ. В простейшем случае ξ будет определяться следующим соотношением

$$\xi = V_{scan}\frac{M}{M_o}, \qquad (3)$$

где V_{scan} – скорость сканирования сети;

M_o - число перехваченных злоумышленником пакетов.

Для описания динамики сканирования сети введем переменные $j = J/M$ и $s = S/M$. Уравнение динамики перехвата трафика по wi-fi сети имеет следующий вид:

$$\frac{dj}{dt} = \xi j. \qquad (4)$$

Данное уравнение имеет следующее аналитическое решение

$$u(t) = 1 + (-1)\cdot e^{-\xi t}. \qquad (5)$$

Применительно к сниффинг-атаке распределение функции ущерба можно записать следующим образом:

$$u(t) = 1 - e^{-\xi(t-t_0)^2}. \qquad (6)$$

где

ξ - интенсивность атаки

t_0 - время начала атаки.

Введем дополнительный весовой аргумент характеризующий скорость работы процессора злоумышленника. Соответственно время необходимое для реализации сниффинг-атаки, (дешифрования сообщений, зашифрованных 64-х битным ключом) будет существенно сокращаться при использовании более современных ЭВМ. Соответственно весовая функция ущерба примет вид

$$u(t) = 1 - e^{-\xi\cdot\frac{V}{k}\cdot(t-t_0)^2}, \qquad (7)$$

где

V – тактовая частота процессора;

t - время реализации атаки;

k- коэффициент, определяемый экспертным методом с учетом значимости каждого эксперта

Таблица 1

Статистические данные распространение ущерба в результате реализации сниффинг-атаки во времени

Время (t), с	Ущерб (U(t))
0	0,0001
10	0,00031
20	0,0015
35	0,0055
50	0,055
68	0,252
79	0,391
95	0,599
108	0,8
120	0,89
140	1

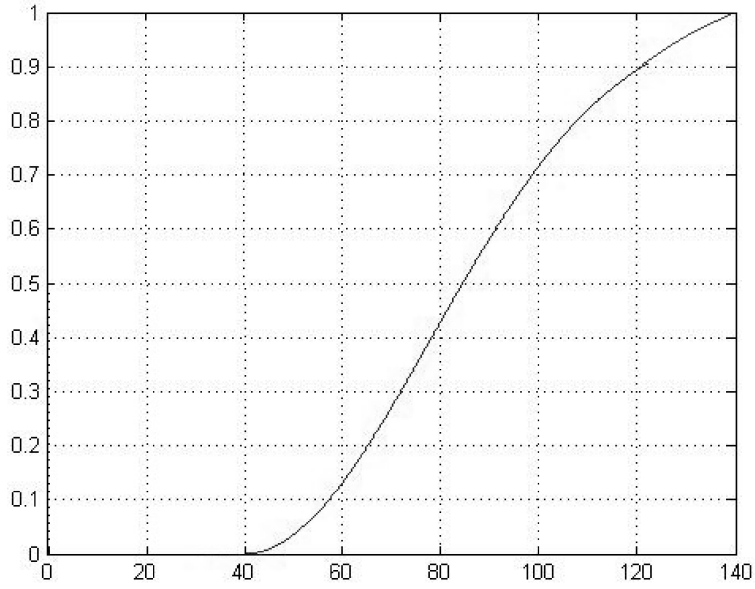


Рис. 3. Графическое (статистическое) представление ущерба

Для доказательства соответствия теоретической и статистической функции воспользуемся аппроксимацией функции с помощью глобальной интерполяции. Построим полином Лагранжа [2].

Предположим, что для $k = 1,2,\dots,n+1$ функции $\Phi_n(x)$ являются полиномами степени n, которые обладают следующим свойством:

$$\Phi_k(x_j) = \begin{cases} 1, & k = j \\ 0, & k \neq j \end{cases}. \qquad (8)$$

Тогда полином $L_n(x)$ будет как раз тем, который нам и нужен, поскольку это полином степени не выше n и $L_n(x_k) = y_k$ для всех $k = 1,2,\dots,n+1$.

$$L_n(x) = \sum_{k=1}^{n+1} y_k \Phi_k(x). \qquad (9)$$

Построим функции $\Phi_n(x)$.

$$(x - x_1)(x - x_2) \cdot \dots \cdot (x - x_{k-1})(x - x_{k+1}) \cdot \dots \cdot (x - x_n)(x - x_{n+1}). \qquad (10)$$

Данная функция является полиномом степени n, который обращается в ноль для всех x_j не равных x_k. В точке x_k она принимает значение:

$$(x_k - x_1)(x_k - x_2) \cdot \dots \cdot (x_k - x_{k-1})(x_k - x_{k+1}) \cdot \dots \cdot (x_k - x_n)(x_k - x_{n+1}). \qquad (11)$$

Тогда:

$$\Phi_k(x) = \frac{(x - x_1)(x - x_2) \cdot \dots \cdot (x - x_{k-1})(x - x_{k+1}) \cdot \dots \cdot (x - x_n)(x - x_{n+1})}{(x_k - x_1)(x_k - x_2) \cdot \dots \cdot (x_k - x_{k-1})(x_k - x_{k+1}) \cdot \dots \cdot (x_k - x_n)(x_k - x_{n+1})}.$$

$$\Phi_k(x) = \prod_{\substack{j=1,2,\dots,n+1 \\ j \neq k}} \frac{x - x_j}{x_k - x_j}. \qquad (12)$$

Построим полином Лагранжа применительно к снифинг-атаке реализуемой перспективными средствами съема информации, который будет выглядеть следующим образом:

$$\Phi_0(z) = \frac{(z-10)(z-20)(z-35)(z-50)(z-68)(z-79)(z-95)(z-108)\cdot}{(0-10)(0-20)(0-35)(0-50)(0-68)(0-79)(0-95)(0-108)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(0-120)(0-100)},$$

$$\Phi_1(z) = \frac{(z-0)(z-20)(z-35)(z-50)(z-68)(z-79)(z-95)(z-108)\cdot}{(10-0)(10-20)(10-35)(10-50)(10-68)(10-79)(10-95)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(10-108)(10-120)(10-100)},$$

$$\Phi_2(z) = \frac{(z-0)(z-10)(z-35)(z-50)(z-68)(z-79)(z-95)(z-108)\cdot}{(20-0)(20-10)(20-35)(20-50)(20-68)(20-79)(20-95)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(20-108)(20-120)(20-100)},$$

$$\Phi_3(z) = \frac{(z-0)(z-10)(z-20)(z-50)(z-68)(z-79)(z-95)(z-108)\cdot}{(35-0)(35-10)(35-20)(35-50)(35-68)(35-79)(35-95)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(35-108)(35-120)(35-100)},$$

$$\Phi_4(z) = \frac{(z-0)(z-10)(z-20)(z-35)(z-68)(z-79)(z-95)(z-108)\cdot}{(50-0)(50-10)(50-20)(50-35)(50-68)(50-79)(50-95)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(50-108)(50-120)(50-100)},$$

$$\Phi_5(z) = \frac{(z-0)(z-10)(z-20)(z-35)(z-50)(z-79)(z-95)(z-108)\cdot}{(68-0)(68-10)(68-20)(68-35)(68-50)(68-79)(68-95)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(68-108)(68-120)(68-100)},$$

$$\Phi_6(z) = \frac{(z-0)(z-10)(z-20)(z-35)(z-50)(z-68)(z-95)(z-108)\cdot}{(79-0)(79-10)(79-20)(79-35)(79-50)(79-68)(79-95)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(79-108)(79-120)(79-100)},$$

$$\Phi_7(z) = \frac{(z-0)(z-10)(z-20)(z-35)(z-50)(z-68)(z-79)(z-108)\cdot}{(95-0)(95-10)(95-20)(95-35)(95-50)(95-68)(95-79)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(95-108)(95-120)(95-100)},$$

$$\Phi_8(z) = \frac{(z-0)(z-10)(z-20)(z-35)(z-50)(z-68)(z-79)(z-95)\cdot}{(108-0)(108-10)(108-20)(108-35)(108-50)(108-68)\cdot \atop \cdot(z-120)(z-100)} \over \cdot(108-79)(108-95)(108-120)(108-100)},$$

$$\Phi_9(z) = \frac{(z-0)(z-10)(z-20)(z-35)(z-50)(z-68)(z-79)(z-95)\cdot}{(120-0)(120-10)(120-20)(120-35)(120-50)(120-68)\cdot \cdot(z-108)(z-100)} \frac{}{\cdot(120-79)(120-95)(120-108)(120-100)},$$

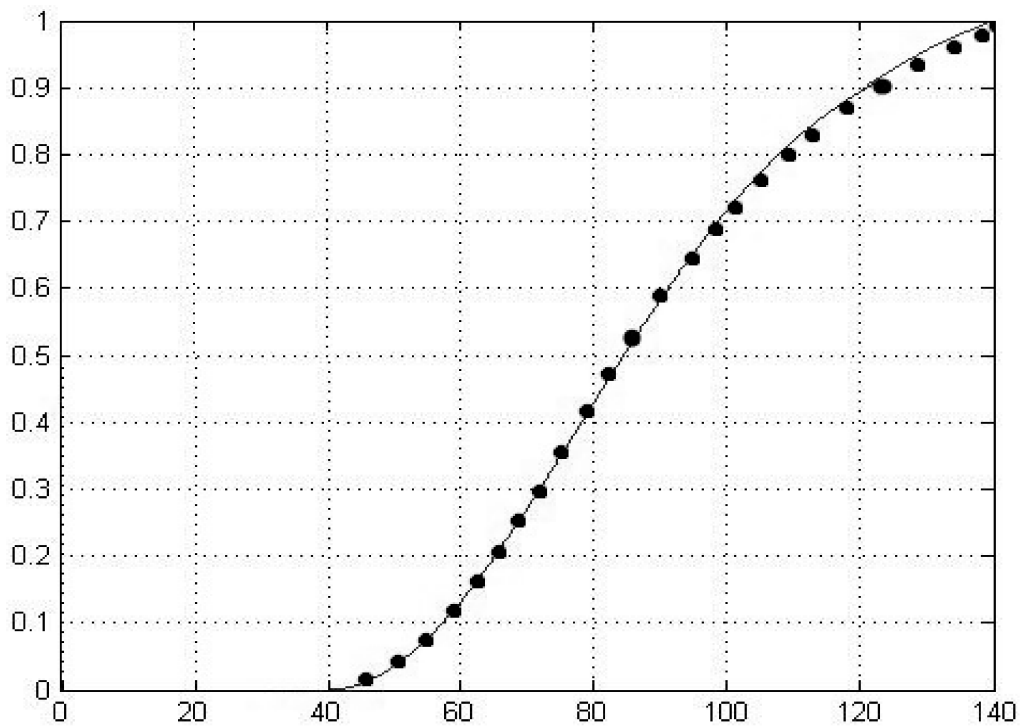
$$\Phi_{10}(z) = \frac{(z-0)(z-10)(z-20)(z-35)(z-50)(z-68)(z-79)(z-95)\cdot}{(100-0)(100-10)(100-20)(100-35)(100-50)(100-68)\cdot \cdot(z-108)(z-120)} \frac{}{\cdot(100-79)(100-95)(100-108)(100-120)}.$$

Общий вид аппроксимированной функции примет следующий вид:

$$fU(z) = 0{,}0001 \cdot \Phi_0(z) + 0{,}00033 \cdot \Phi_1(z) + 0{,}0017 \cdot \Phi_2(z) + 0{,}0055 \cdot \Phi_3(z) + +0{,}055 \cdot \Phi_4(z) + 0{,}252 \cdot \Phi_5(z) + 0{,}391 \cdot \Phi_6(z) + 0{,}58 \cdot \Phi_7(z) + 0{,}765 \cdot \Phi_8(z) + 0{,}79 \cdot \Phi_9(z) + 1 \cdot \Phi_{10}(z). \quad (13)$$

Для сравнения функций ущерба (статистической и теоретической), построим теоретическую функцию (по формуле модели перехвата траффика), используя теже параметры, которые были использованы ранее в статистической модели и сопоставим ее с графиком статистической функции ущерба

$$u(t) = 1 - e^{-\xi \cdot \frac{V}{k} \cdot (t-t_0)^2} \quad . \quad (14)$$



$u(t)$

$fu(t)$

Рис. 4 Графическое представление сравнения теоретического и практического ущерба модели перехвата трафика

Таблица 2

Теоретические данные распространение ущерба в результате реализации сниффинг-атаки во времени

Время (t), с	Ущерб (U(t))
0	0,0001
10	0,00033
20	0,0017
35	0,0055
50	0,055
68	0,252
79	0,391
95	0,58
108	0,765
120	0,79
140	1

На основе данного сравнения можно утверждать, что для описания процесса реализации сниффинг-атаки возможно использование модели перехвата трафика.

На основе функции ущерба (7) получим функцию полезности

$$U(t) = 1 - e^{-\xi \cdot \frac{V}{k} \cdot (t)^2} . \quad (15)$$

Оценим вероятность наступления ущерба вероятность наступления ущерба:

$$P(t) = 1 - e^{-\frac{(t-\tau_a)}{\tau}}, \quad (16)$$

где

$t - \tau_a = t_0$ – время начала атаки;

τ_a – время действия атаки;

τ – время для подготовки сниффинг-атаки перспективными средствами съема информации, полученное при моделировании сетей Петри – Маркова в предыдущем разделе.

В дальнейшем полученные результаты могут быть использованы для обоснования выбора аналитического выражения риска.

Литература

1. WASC Threat Classification. Version 2.0/ WEB APPLICATION SECURITY CONSORTIUM http://www.webappsec.org.

2. Радько Н.М., Скобелев И.О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. - М: РадиоСофт. 2010 . 230 С.

3. Hansman, S., Hunt R., “A taxonomy of network and computer attacks”. Computer and security (2005).

Воронежский государственный технический университет
Voronezh State Technical University

MODELLING THE PROCESS OF ATTACK BY STEALING PERSPECTIVE MEANS OF INFORMATION: MODEL OF INTERCEPTION OF TRAFFIC

A.E. Kiselyov, A.S. Pakhomova, A.V. Baburin, I.V. Shevchenko

In this work modeling of process of attack by perspective means съема information on the basis of Petri-Markov's networks is considered. The further description of model of interception of a traffic allows to receive a type of function of damage and to compare it with statistical data

Key words: attack, means secret съема information, damage, traffic