Математические структуры и моделирование
2011, вып. 24, с. 98–101

УДК 004.056.5:005.311.7

ПРОГРАММА, РЕАЛИЗУЮЩАЯ ИГРОВОЙ ПОДХОД ПРИ ВЫБОРЕ ОПТИМАЛЬНОГО НАБОРА СРЕДСТВ ЗАЩИТЫ КОМПЬЮТЕРНОЙ СИСТЕМЫ

Т.В. Вахний, А.К. Гуц, В.В. Константинов

В данной работе представляется программный продукт, предназначенный для поиска наиболее оптимального набора средств защиты компьютерных информационных ресурсов. В основе его работы используется матричная игра двух сторон, одной из которых является система защиты компьютерной информации, а с другой — возможные атаки хакеров.

Введение

Как известно, широкое использование современных информационных технологий сопровождается правонарушениями, связанными с кражей и неправомочным доступом к данным, как передаваемым по линиям связи, так и хранящимся в памяти компьютеров. В настоящее время на рынке представлено большое разнообразие средств защиты компьютерной информации и администратору безопасности приходится принимать субъективные решения о выборе в пользу тех или иных программных продуктов. Применение игровых методов [1–4] позволяет обеспечить оптимизацию выбора существующих программных продуктов для защиты компьютерной информации.

1. Постановка и метод решения задачи

При составлении матрицы игры можно считать, что хакер увлечён желанием нанести как можно больший ущерб атакуемой компьютерной системе. Цель администратора безопасности в матричной игре состоит в том, чтобы позволить хакеру причинить наименьший ущерб при наименьших затратах на программное обеспечение.

В качестве стратегий хакера будем понимать строки x_i $(i = 1, \ldots, n)$ некоторой матрицы, а в качестве стратегий администратора безопасности — её столбцы y_j $(j = 1, \ldots, m)$. К стратегиям хакера можно отнести различные виды компьютерных атак. К стратегиям администратора можно отнести различные средства защиты компьютерной информации.

Омский государственный университет им. Ф.М. Достоевского
E-mail: vahniytv@mail.ru, guts@omsu.ru, v.const.89@gmail.com

Таблица 1. Таблица матричной игры

		y_1	y_1	...	y_m
x_1	$p(x_1)$	a_{11}	a_{12}	...	a_{1m}
x_2	$p(x_2)$	a_{21}	a_{22}	...	a_{2m}
...	...	...	...	...	...
x_n	$p(x_n)$	a_{n1}	a_{n2}	...	a_{nm}

Для проведения на компьютере игры A надо также знать результаты игры при каждой паре стратегий x_i и y_j (например, a_{ij} — причинённый материальный ущерб) и вероятности реализации атак хакеров $p(x_i)$ при выбранной стратегии x_i. Вероятности реализации атак $p(x_i)$ могут быть определены по результатам статистических исследований. Если вероятности атак неизвестны, то предполагается, что все они равновероятны, т. е. $p(x_i) = 1/n$.

В качестве коэффициентов a_{ij} матрицы игры A можно рассматривать, например, годовые потери для всех вариантов комбинаций x_i $(i = 1, \ldots, n)$ и y_i $(j = 1, \ldots, m)$ [4]. Для этого нужно сопоставить каждую атаку с каждым методом защиты и определить ущерб, который может быть при этом нанесён. Покупка, установку и использование средств защиты могут требовать дополнительных затрат, что также нужно вносить в ущерб при расчётах.

Построив игровую матрицу (табл. 1) и проанализировав её, можно заранее оценить затраты каждого решения по защите компьютерной информации и выбрать наиболее эффективные варианты для всего диапазона атак.

Если построена игровая матрица A, в которой результатами игры являются материальные потери от атак, то наилучшей в условиях имеющейся информации об атаках будет стратегия системы защиты компьютерной информации y_j, при которой будут минимальны средние потери, т.е. будет минимальна сумма:

$$\sum_{i=1}^{n} a_{ij} p(x_i).$$

Для выбора наиболее оптимального набора средств защиты компьютерных информационных ресурсов в математической игре следует использовать в качестве стратегий различные сочетания из атак и методов защиты. Прекращение использования или добавление нового средства (атаки или защиты) можно рассматривать как переход от одной стратегии к другой.

2. Определение наиболее вероятных хакерских стратегий

Успешность действий администратора безопасности компьютерной сети зависит от того, насколько правильно он оценивает основные угрозы со стороны хакерских атак, другими словами, насколько знаком он с хакерскими стратегиями x_i и знает, какая хакерская стратегия наиболее вероятна.

Полезно установить систему обнаружения хакерских атак (IDS). Одной из таковых является свободно распространяемая система, известная под названием Honeynet. Honeynet спроектирована таким образом, чтобы контролировать все входящие и исходящие соединения. Её невозможно использовать в качестве плацдарма для сканирования, исследования и атак на большинство других систем.

Первые же эксперименты с запущенной системой Honeynet сильно удивят администратора количеством попыток различного типа установления соединений с компьютерами подведомственной ему сети. Но хорошо освоенная система Honeynet позволяет набрать статистику, с помощью которой можно выявить наиболее распространённые типы атак x_i и вычислить вероятности $p(x_i)$ хакерских стратегий.

3. Описание программного продукта

В данной работе был реализован программный продукт, который по введённым значениям стоимости средств защиты и ущерба от применения всех возможных пар атака-защита вычисляет оптимальный набор из имеющихся в его базе программных продуктов. На рис. 1 представлен её интерфейс.

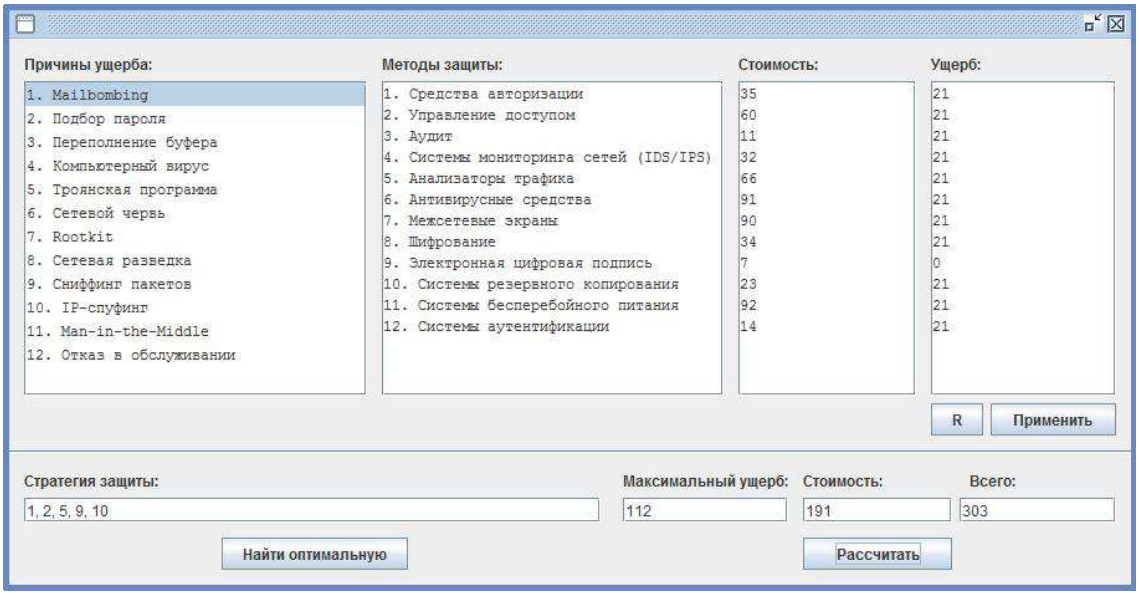

Рис. 1. Интерфейс программного продукта

Для начала работы с данным программным продуктом нужно ввести в его базу данных существующие на рынке программные продукты по защите компьютерной информации и их стоимость. Величину возможного ущерба от атак хакеров можно оценить различными способами, поэтому они изначально имеют нулевые значения, и администратору безопасности потребуется их заполнение на основе установленной системы обнаружения хакерских атак и их статистического анализа. Если нужно протестировать работу программного продукта,

то величину возможного ущерба от применения всех возможных пар атака-защита можно при нажатии кнопки «R» заполнить случайными величинами.

С помощью кнопки «Найти оптимальную» можно получить оптимальный набор методов защиты, позволяющий минимизировать общие затраты (ущерб от атак хакеров и затраты на программные продукты). Номера полученных методов защиты будут показаны в поле «Стратегии защиты». При использовании кнопки «Рассчитать» в поле «Максимальный ущерб» будет выведен максимальный ущерб, который можно получить для данного набора методов защиты.

При выборе из базы данных оптимального набора программных продуктов для защиты компьютерной информации предпочтение отдаётся более дешёвым аналогам. Поэтому для эффективного использования разработанного программного продукта необходимо постоянно пополнять базу данных новинками.

Описанный в данной работе программный продукт позволяет администратору безопасности также проверять свои собственные стратегии. Для этого нужно перечислить через запятую нужные методы защиты в поле «Стратегии защиты» и нажать кнопку «Рассчитать» под полем «Максимальный ущерб», где будет выведен максимально возможный ущерб при применении этой стратегии. Таким образом, администратор безопасности может сначала получить оптимальный набор методов защиты, а потом изменять его, сверяясь с получающейся величиной максимального ущерба.

Заключение

Применение реализованного в данной работе программного продукта даст администратору безопасности возможность оценить эффективность используемого программного обеспечения и выбрать наиболее оптимальный набор средств защиты компьютерной информации.

Литература

1. Воробьев А.А. Методы оценивания и обеспечения гарантированного уровня защиты информации от несанкционированного доступа в вычислительной сети автоматизированной системы управления: Автореф. дис. к-та техн. наук / А.А. Воробьев. СПб., 1997. 15 с.
2. Нестеров С.А. Разработка методов и средств проектирования инфраструктуры обеспечения информационной безопасности автоматизированных систем: Автореф. дис. к-та техн. наук / С.А. Нестеров. СПб., 2002. 18 с.
3. Матричные игры / Под. ред. Н.Н. Воробьева. М : ФМ, 1961. 280 с.
4. Вахний Т.В., Гуц А.К. Теоретико-игровой подход к выбору оптимальных стратегий защиты информационных ресурсов // Математические структуры и моделирование. 2009. №. 19. С. 104-107.