Математические структуры и моделирование
2009, вып. 19, с. 104–107

УДК 004.056.5:005.311.7

ТЕОРЕТИКО-ИГРОВОЙ ПОДХОД К ВЫБОРУ ОПТИМАЛЬНЫХ СТРАТЕГИЙ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Т.В. Вахний, А.К. Гуц

В данной работе для поиска наиболее оптимальных стратегий защиты информационных ресурсов используется математическая игра двух сторон, одной из которых является система защиты компьютерной информации, а с другой – атаки азартных хакеров. Применение игровых методов дает преимущества администратору безопасности перед субъективными случайными решениями и обеспечивает оптимизацию стратегий защиты компьютерной информации. Учет психологии азартного хакера позволяет направлять его активность в ложном направлении.

Введение

В настоящее время, учитывая широкое распространение информационных систем, интегрированных в глобальные информационно-вычислительные сети, приходится опасаться удаленных атак хакеров. Одной из существенных особенностей обеспечения защиты информационных ресурсов является недостаточность информации о возможных атаках, времени их проведения и их последствиях. Поэтому задачи обеспечения защиты информационных ресурсов следует относить к «задачам о выборе решений в условиях неопределенности».

В данной работе для поиска наиболее оптимальных стратегий защиты информационных ресурсов используется математическая игра двух сторон, одной из которых является система защиты компьютерной информации, а с другой – возможные атаки азартных хакеров. При составлении матрицы игры можно считать, что хакер увлечен желанием нанести как можно больший ущерб атакуемой компьютерной системе. Цель администратора безопасности в матричной игре состоит в том, чтобы позволить хакеру причинить наименьший ущерб.

Идея использования теоретико-игрового подхода в теории защиты информационных ресурсов не является новой [1-3], но соответствующие работы малодоступны. Поэтому имеет смысл уточнить постановку задачи и ход ее решения.

Омский государственный университет.
E-mail: vahniytv@mail.ru

В результате математического моделирования игры можно оценить эффективность стратегий администратора безопасности по защите информационных ресурсов и выбрать из них наиболее эффективные.

Постановка и решение задачи

Будем понимать стратегии хакера как строки x_i $(i = 1, 2, ..., n)$ некоторой матрицы, а стратегии администратора информационных ресурсов – как ее столбцы y_j $(j = 1, 2, ..., m)$. К стратегиям хакера можно отнести различные виды компьютерных атак. Например, это может быть удаленное или локальное проникновение в компьютер, удаленное или локальное блокирование компьютера, применение сетевых сканеров для сбора информации о компьютерах сети и программах, потенциально уязвимых к атакам, использование сканеров уязвимых мест программ в поисках компьютеров, уязвимых к тому или иному конкретному виду атаки, применение вскрывателей паролей, применение сетевых анализаторов (снифферов) и др.

К стратегиям администратора можно отнести различные варианты использования методов и средств защиты информации. Например, применение и регулярное обновление антивирусных программ, шифрование, использование межсетевых экранов и средств обнаружения атак, оперативная установка от производителей исправлений для программ (чтобы ликвидировать неблагоприятные последствия ошибок в них), применение вскрывателей паролей и сканеров уязвимых мест и др.

Для проведения на компьютере игры A надо также знать результаты игры a_{ij} при каждой паре стратегий x_i и y_j (например, a_{ij} – причиненный материальный ущерб) и вероятности реализации атак хакеров $p(x_i)$ при выбранной стратегии x_i. Построив игровую матрицу (см. табл. 1) и проанализировав ее, можно заранее оценить затраты каждого решения по защите компьютерной информации и рекомендовать наиболее эффективные варианты для всего диапазона атак.

Таблица 1.

		y_1	y_2	...	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}

Если построена игровая матрица (a_{ij}), 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 [1–3]:

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

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. $p(x_i) = 1/n$.

Азартный хакер увлечён желанием нанести как можно больший ущерб атакуемой компьютерной системе. В силу своей психологии он преувеличивает свои выигрыши и преуменьшает свои неудачи в предыдущих попытках атак на систему, воспринимая игру A как матричную игру $f(A)$ с матрицей $(f(a_{ij}))$, где f — так называемая функция полезности. В случае азартного нарушителя эта функция задается непрерывной выпуклой (вниз) вещественной функцией $f : \mathbb{R} \to \mathbb{R}$ [3, с. 222]. На рис. 1 приводится вид функции полезности азартного хакера. Такой функцией может являться, например, функция $f(a) = e^a - 1$.

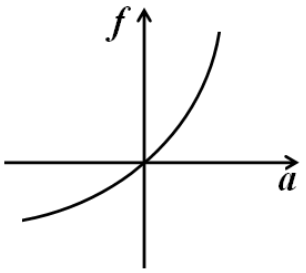

Рис. 1. Вид функции полезности азартного игрока [3, с. 222]

Обозначим через $val(A)$ значение матричной игры A с матрицей (a_{ij}). В случае азартной функции полезности имеют место утверждения [3]:

1) из $val(A) = 0$ следует $val(f(A)) \geq 0$, т. е. нарушитель может видеть победу там, где её нет;

2) из $val(A) > 0$ следует $val(f(A)) \geq val(A)$, т. е. азартный нарушитель преувеличивает размер успеха;

3) при любом опыте l предыдущих вторжений существует такая игра A_0, что $val(A_0) < 0$ (реальный проигрыш, неудачная атака) и $val(A_0 + lE) > f(l)$, где E — матрица, состоящая из единиц, т. е. азартный нарушитель всегда будет повторять некоторые проигрышные атаки (игру A_0).

Учет психологии азартного хакера и моделирование его поведения позволяет строить ловушки либо для его идентификации, либо для направления его активности по ложному пути.

Оценка материальных потерь

Построение игровых матриц и выбор наиболее приемлемых решений при использовании игровых моделей требует оценки результатов функционирования систем защиты компьютерной информации в целом при различных возможных вариантах решений. Опишем один из способов определения коэффициентов a_{ij} матрицы игры A.

Единичные потери P_{ij}^1 при взломе j-ой рабочей станции в случае однократ-

ной реализации угрозы x_i, можно оценить следующим образом:

$$P_{ij}^1 = R_j k_i,$$

где R_j – стоимость ресурса «рабочая станция пользователя» при использования j-ой комбинации методов и средств защиты; k_i – процент потерь в случае реализации угрозы x_i на данном ресурсе. Стоимость ресурса R_j обычно включает стоимость сопровождения и восстановления, прямые затраты на покупку и обновление соответствующего оборудования и программного обеспечения, расходы на поддержание информационной системы, административные расходы, затраты на обучение пользователей и убытки от вынужденных простоев.

Годовая оценка инцидента N_i, т. е. число, отражающее частоту проявления угрозы x_i в год, может быть рассчитана так:

$$N_i = s\nu_i,$$

где s – число подверженных атаке рабочих станций и ν_i – частота реализации угрозы x_i в год (может быть найдена на основе собственного опыта или усредненной статистической информации).

Годовые потери P_{ij} j-ой рабочей станции в результате реализации угрозы x_i можно оценить следующим образом:

$$P_{ij} = P_{ij}^1 N_i.$$

В качестве коэффициентов a_{ij} матрицы игры A можно рассматривать годовые потери P_{ij} для всех вариантов комбинаций x_i $(i = 1, 2, ..., n)$ и y_j $(j = 1, 2, ..., m)$.

Заключение

Таким образом, применение игровых методов дает преимущества администратору безопасности перед субъективными случайными решениями и обеспечивает оптимизацию стратегий защиты компьютерной информации. Организация проигрышных атак и подробное исследование матричной игры A_0 сводится к изучению психологии азартного нарушителя.

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. Воробьёв. — 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: Государственное издательство физико-математической литературы, 1961. – 280 с.