УДК 004.056

Д.А. Хорьков

О возможности использования математического аппарата сетей Петри для моделирования компьютерных атак

Предложена новая модель компьютерной атаки, предназначенная для синтеза сетевого трафика атакующего воздействия в задаче тестирования сетевых систем обнаружения атак. Модель базируется на математическом аппарате модифицированных сетей Петри, представляющих собой обобщенные стохастические сети Петри с задержками специального вида, сдерживающими дугами и взвешенными переходами.
Ключевые слова: атака, система обнаружения атак, модель, моделирование, трафик.

Одним из перспективных способов тестирования сетевых систем обнаружения атак (СОА) является воспроизведение предварительно записанного трафика компьютерных атак на специальном стенде, к которому подключена тестируемая СОА. Преимуществом этого подхода является возможность обеспечения многократной повторяемости условий эксперимента при условии, что трафик компьютерных атак каждый раз будет воспроизводиться идентичным образом. Отсутствие в составе стенда реальных атакуемых систем устраняет проблему восстановления состояния отдельных его элементов после проведения атак. Вместе с тем рассматриваемый способ тестирования не позволяет варьировать параметры атак (например, кодировки HTTP-запросов и используемый эксплоитом shell-код) в процессе тестирования, поскольку это требует серьезной модификации уже сформированных пакетов сетевого трафика. Предварительная запись *всех* возможных вариантов реализации каждой атаки является чрезвычайно трудоемкой задачей, поэтому большой интерес представляет возможность управляемого *синтеза сетевого трафика* компьютерных атак с использованием математической модели атакующего воздействия и соответствующего программного обеспечения.

Сетевой трафик состоит из двух составляющих: статической и динамической. Статической составляющей трафика является передаваемая информация, т.е. *последовательность* пакетов и содержащиеся в них *данные*. Динамическая составляющая трафика – это последовательность *временных интервалов*, соответствующих моментам передачи пакетов и состоянию ожидания линии связи. Адекватная модель компьютерной атаки, которую можно применять для синтеза сетевого трафика атакующего воздействия, должна отражать как статическую, так и динамическую составляющие сетевого трафика.

Разрабатываемая модель компьютерной атаки должна удовлетворять следующему минимальному набору требований, целью которых является, во-первых, максимальный охват атак различного типа, в том числе многоэтапных, и, во-вторых, обеспечение реалистичности получаемого в результате трафика:

1) случайный характер синтезируемых задержек;
2) логичность действий злоумышленника;
3) многоальтернативность сценария атаки.

Существующие модели на основе графов атак хорошо подходят для описания последовательности действий злоумышленника, однако не содержат механизмов для организации управляемого ветвления и моделирования динамической составляющей атаки. Аналогичным недостатком обладают модели на основе формальных языков и онтологий. Детерминированные модели, такие как конечные автоматы, для решения поставленной задачи непригодны, поскольку не позволяют моделировать случайные задержки и осуществлять выбор одной из равноценных альтернатив развития атаки. Стохастические модели, например вероятностные автоматы и цепи Маркова, напротив, неудобно использовать для систем, функционирующих в соответствии с определенным алгоритмом.

Разумным компромиссом, сочетающим наглядность с возможностью описания как детерминированных, так и стохастических систем, являются модели на базе обобщенных стохастических сетей Петри (англ. Generalized Stochastic Petri Nets), наделенные дополнительной функциональностью. Содержимое и порядок следования сетевых пакетов, генерируемых в ходе реализации атаки, определяются, с одной стороны, действиями злоумышленника и, с другой стороны, алгоритмом работы сетевых программ, которые реализуют протокол обмена. Сети Петри традиционно использовались для моделирования работы алгоритмов и программного обеспечения, поэтому подходят для решения этой

задачи как нельзя лучше. Введение понятия *задержанного перехода* расширяет область практического применения сетей Петри и делает возможным не только проследить *порядок* событий, происходящих в системе, но и попытаться смоделировать их *динамику*. Выделим подлежащие моделированию виды задержек:

1. *Межконцевая задержка распространения пакетов* – время передачи пакета из одной точки компьютерной сети в другую. Может быть описана суммой детерминированной величины и случайной величины с гамма-распределением.

2. *Время выполнения запроса сервером* – детерминированная величина, определяемая алгоритмом работы серверного ПО.

3. *Программная задержка* – детерминированная величина, которая определяется алгоритмом работы клиентской программы.

4. *Задержка ввода команды* – случайная задержка, определяемая временем, необходимым атакующему или пользователю для ввода очередной команды или запроса. Будем считать величину задержки нормальной случайной величиной с математическим ожиданием и дисперсией, зависящими от длины вводимой команды и средней скорости набора текста пользователем (атакующим).

5. *Задержка оценки результата* – случайная задержка, связанная, во-первых, с количеством текста, который следует прочитать или просмотреть пользователю или атакующему, и, во-вторых, с необходимостью производить какие-либо вычисления. Примем эту задержку распределенной по нормальному закону.

Таким образом, необходимо моделировать пять различных видов задержек, три из которых являются случайными величинами. Можно заметить, что все они могут быть представлены линейной комбинацией нормальной случайной величины и случайной величины с гамма-распределением:

$$T = k_1 T_{\text{норм}} + k_2 T_{\Gamma} . \qquad (1)$$

Для представления детерминированных величин можно обнулить коэффициент k_2 при гамма-распределенной случайной величине и устремить дисперсию нормальной случайной величины к нулю.

В качестве модели компьютерной атаки используем обобщенную стохастическую сеть Петри с задержками вида (1), сдерживающими дугами и взвешенными переходами. *Пространство состояний* модели определяется множеством позиций и, кроме того, множеством переменных состояния. В частности, эти переменные содержат значения IP-адресов, номеров TCP- и UDP-портов, имена и пароли пользователей, а также другую информацию, которая используется при реализации атаки. *Текущее состояние* модели, т.е. фаза атаки, описывается расстановкой фишек в позициях сети и конкретными значениями переменных состояния. С переходами рассматриваемой сети Петри свяжем два типа событий: изменение состояния модели и генерацию очередного Ethernet-кадра атакующего воздействия. Содержимое генерируемого кадра определяется текущим состоянием модели.

Предлагаемая модель обладает следующими преимуществами:

1) содержит механизмы, необходимые для описания алгоритма действий злоумышленника, включая случайный выбор одной из равноценных альтернатив;

2) позволяет описывать динамическую составляющую сетевого трафика атакующего воздействия в виде детерминированных и случайных задержек.

Дальнейшей работой в направлении синтеза сетевого трафика атакующего воздействия является создание программного обеспечения, реализующего предложенную модель. Выходными данными программы должны стать массив сетевого трафика и файл протокола атаки, содержащий подробную информацию об атаке в целом и отдельных ее этапах, а также временные отметки, необходимые для ее однозначной идентификации. Указанные файлы затем используются при тестировании СОА в качестве тестового воздействия.

Хорьков Дмитрий Алексеевич
ГОУ ВПО «Уральский государственный технический университет» – УПИ им. Б.Н. Ельцина
аспирант каф. теоретических основ радиотехники Радиотехнического института (РТФ)
Эл. адрес: dimkhor@planet-a.ru

D.A. Khorkov

On the using of Petri nets for computer attack modeling

This paper presents a novel method of computer attack modeling for testing network-based intrusion detection systems using network traffic. The model is based on generalized stochastic Petri nets with special delays, inhibitor arcs, and weighted transitions.

Key words: attack, system of attacks detection, model, modeling, traffic.