УДК 004.051

Ю.В. Алейнов

Метод повышения эффективности обнаружения сетевых атак неизвестного типа путем внедрения ложных целей в состав сети

Рассмотрен метод повышения эффективности обнаружения вторжений неизвестного типа, основанный на внедрении в сеть ложных целей. Предложена модель, позволяющая в каждый момент времени связать вероятность атаки на ложную цель с параметрами ложных целей, защищаемой сети и внешней среды. Описан обобщенный метод получения оптимальной конфигурации ложных целей в сети в условиях меняющихся со временем входных параметров.
Ключевые слова: обнаружение вторжений, ложные цели, повышение эффективности.

Одним из важнейших направлений исследований в области информационной безопасности является обнаружение вторжений. В настоящее время существует много способов выявления фактов компьютерных атак разных типов. Среди них всегда особо выделялись те способы, которые позволяют обнаруживать атаки ранее неизвестного вида. Для обнаружения таких атак применяется, как правило, подход, основанный на идентификации аномального поведения в сети. Часто предлагается использовать различные эвристики для выявления заведомо отличного от нормального поведения [1, 2]. В частности, можно предложить эвристику, основанную на предположении о том, что легальный пользователь не будет обращаться к неизвестному для него объекту в сети. Для использования этой эвристики необходимо разместить в сети системы, не участвующие в других производственных процессах и не анонсируемые как работающие сетевые сервисы – так называемые ложные цели (ЛЦ). Любая сетевая активность такой ложной цели является подозрительной и должна рассматриваться как злонамеренная [3, 4]. В данной статье рассмотрена модель, позволяющая оценивать эффективность применения описанной эвристики в зависимости от параметров сети и ложных целей внутри нее, а также метод расчета параметров ложных целей в сети.

Модель сети, содержащей ложные цели. Отличительной особенностью рассматриваемой эвристики является то, что ее эффективность зависит от доли общего числа атак, приходящейся на ложные цели. В свою очередь, она определяется соотношением числа ложных и реальных целей в сети и другими их параметрами. Рассмотрим подробнее модель, позволяющую связать искомую эффективность с параметрами ложных и реальных целей.

Основным понятием рассматриваемой модели является понятие цели. Под целью будем понимать работающий на хосте в сети процесс, выполняющий определенный программный код. Так как очень часто сетевые атаки направлены на эксплуатацию уязвимостей в прикладном программном обеспечении, такое понимание цели можно считать обоснованным [5]. Атакой в рамках рассматриваемой модели будем называть следующую последовательность шагов, выполняемую атакующей стороной:

1) выбор по некоторому правилу цели для очередной атаки;
2) проверка наличия у цели подходящей уязвимости;
3) попытка эксплуатации уязвимости.

Как правило, любая атака ориентирована на некоторый набор уязвимостей программного кода. Таким образом, имеет смысл группировать цели в классы по признаку его совпадения (C_j на рис. 1). Каждый такой класс будет содержать как реальные, так и ложные цели.

Будем считать, что атакующая сторона представлена множеством копий вредоносного программного обеспечения, каждая из которых циклически осуществляет попытки атаки на сеть. Попытки атак совершаются в дискретные моменты времени. Можно предположить наличие большого количества независимых источников атак в каждый момент времени. Следовательно, можно рассматривать суммарный поток атак от этих источников, считая его простейшим. Очевидно, в условиях изменяющихся характеристик внешней среды будут меняться и параметры регистрируемого потока атак, но будем считать, что всегда можно выбрать такой промежуток времени, в течение

которого этот поток можно считать простейшим. В этом случае достаточно рассматривать состояние внешней среды в дискретные моменты времени, соответствующие промежуткам стационарности параметров регистрируемых потоков атак. При этом само состояние будет определяться параметрами этих потоков, а воздействие на защищаемую сеть атакующей стороны можно описать множеством независимых потоков атак, по одному на каждый класс целей (рис. 1).

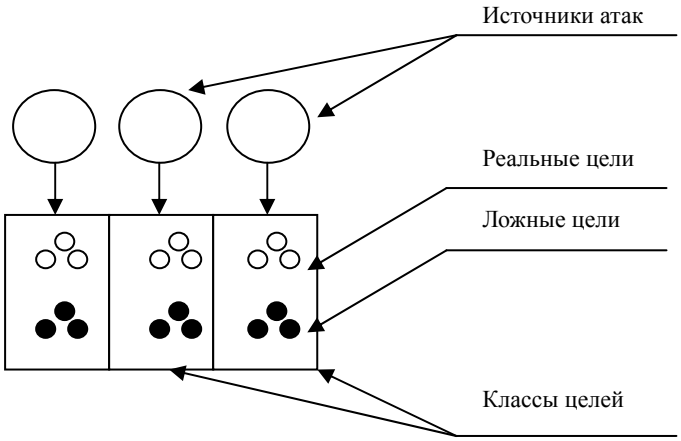

Рис. 1. Схема взаимодействия компонентов модели

Рассмотрим вероятность атаки на какую-либо ложную цель в сети на каждом промежутке стационарности параметров потоков атак. В силу введенных определений и предположений, эта вероятность равна сумме таких вероятностей по всем классам целей. Справедливо следующее выражение для указанной вероятности:

$$P = \sum_{i=1}^{k} P\{t \in C_i\} \frac{f_i}{f_i + r_i}, \qquad (1)$$

где $P\{t \in C_i\}$ – вероятность выбора на следующем шаге цели из класса C_i; f_i и r_i – количество ЛЦ и РЦ соответственно в классе C_i, а k – число классов целей.

Вероятность выбора цели из определенного класса на практике можно определить как отношение среднего числа атак на цели этого класса к общему количеству атак на все цели сети. Эти средние значения можно определить с помощью понятия интенсивности (I) потока атак. Наилучшей в смысле предложенной модели будет являться такая конфигурация параметров ЛЦ в сети, которая обеспечит максимальное значение P при заданных ограничениях на количество ЛЦ в каждом классе. Это справедливо для фиксированного момента времени.

Пусть теперь интенсивность атакующих воздействий для каждого класса целей меняется со временем. Если вычислять оптимальную конфигурацию ЛЦ на каждом шаге без учета внесенных ранее изменений, то есть опасность того, что некоторые ЛЦ, внедренные в сеть малое время назад, будут удалены на следующем шаге. Очевидно, это не даст им исполнить свою функцию и потенциально может привести к их раскрытию. Таким образом, рассматривая модель в динамике, необходимо учитывать такой значимый параметр цели, как время, прошедшее с момента ее появления, или время доступности. Каждый класс можно охарактеризовать распределением времени доступности целей этого класса. Можно сформулировать следующее ограничение: распределение времени доступности ЛЦ не должно отличаться от распределения времени доступности РЦ в этом же классе. Данное ограничение прямо следует из основного принципа внедрения ложных объектов в сеть: для того чтобы атакующий не смог раскрыть факт его дезинформации, ложный объект должен как можно меньше отличаться от реального.

Еще одно ограничение, связанное с этим же принципом, заключается в необходимости сохранять устойчивые наборы сервисов, находящихся на одном хосте при внедрении ложных целей. Кроме того, обычно присутствует ограничение на максимальное число хостов – «носителей» ложных целей.

Итак, можно перечислить следующие параметры целей, влияющие с точки зрения принятой модели на эффективность эвристики:

1) принадлежность цели к определенному классу с точки зрения совпадения исполняемого кода;

2) принадлежность цели к классу реальных или ложных целей;

3) момент времени, когда цель стала доступной в сети;

4) хост, на котором расположена цель.

Для сети в целом вычисляются такие параметры, как:

1) количество классов целей по признаку совпадения исполняемого кода;

2) распределение времени доступности цели в каждом классе;

3) множество комбинаций реальных целей, размещенных на каждом хосте;

4) количество реальных и ложных целей в каждом классе, а также максимально возможное число хостов, несущих ложные цели.

Формально модель можно записать следующим образом, учитывая (1):

$$\begin{cases} P = \sum\limits_{j=1}^{k} \dfrac{I_j}{I} \dfrac{f_j}{f_j + r_j} = \max, \\ \sum\limits_{i=1}^{k} \alpha_i x_i \le N, \\ P\left(\tau_j^F < \tau\right) = P\left(\tau_j^R < \tau\right), \end{cases} \quad (2)$$

где k – число классов целей в сети; I_j – интенсивность атак на цели класса C_j; I – интенсивность атак на цели всех классов; $x_j \in X$ – фиксированный набор типов целей (конфигурация хоста) из множества всех имеющихся конфигураций в сети; α_j – число хостов с ложными целями, соответствующих конфигурации x_j; N – максимальное число хостов с ложными целями; τ_j^F и τ_j^R – время доступности ложной и реальной целей соответственно (в классе целей C_j).

Метод определения оптимальных параметров ложных целей. В обобщенном виде метод заключается в итеративном выполнении следующих действий:

1. Получение входных параметров модели и исходной конфигурации ЛЦ.

2. Вычисление оптимальной конфигурации ЛЦ с помощью решения задачи оптимизации, задаваемой моделью (2).

3. На каждом шаге определение возможных управляющих воздействий для приближения текущей конфигурации ЛЦ к вычисленной на предыдущем шаге. При этом следует проводить оценку схожести распределений времени доступности РЦ и ЛЦ.

4. Среди возможных управляющих воздействий выбираются такие, которые обеспечивают максимальный рост вероятности выбора атакующим ЛЦ.

5. При изменении параметров модели оптимальная конфигурация должна быть вычислена вновь.

Данный метод позволяет поддерживать такую конфигурацию ложных целей в защищаемой сети, которая обеспечит максимальный поток атак на детекторы системы обнаружения вторжений (внедренные ложные цели) с учетом изменения характера внешнего воздействия на защищаемую сеть, а также с учетом изменения ее параметров.

Заключение. В данной статье предложена модель, описывающая работу системы обнаружения вторжений, использующей ложные цели, внедренные в адресное пространство защищаемой сети для повышения эффективности детектирования атак неизвестного типа. Предложен метод определения необходимых параметров ложных целей, обеспечивающий наибольший поток атак на ложные цели, что является условием максимальной эффективности применения данной эвристики. Отличительной особенностью предложенного метода является использование в качестве входных данных наиболее простых параметров сети, таких как размер адресного пространства, интенсивность потоков атак, количество ложных и реальных целей. В качестве основного направления дальнейших исследования в этой области можно назвать экспериментальную проверку предложенного метода и соотнесение результатов с расчетными.

Литература

1. Allen J. State of Practice of intrusion detection technologies : Technical Report / J. Allen, A. Christie, W. Fithen et al. – Pittsburgh: Carnegie Mellon Software Engineering Institute, 2000. – 242 с.

2. Милославская Н.Г. Интрасети: обнаружение вторжений: учеб/ пособие для вузов / Н.Г. Милославская, А.И. Толстой. – М.: Юнити-Дана, 2001. – 592 с.

3. Котенко И.В. Обманные системы для защиты информационных ресурсов в компьютерных сетях / И.В. Котенко, М.В. Степашкин // Труды СПИИРАН. – 2004. – Вып. 2, т. 1. – С. 211–230.

4. Правиков Д.И. Использование виртуальных ловушек для обнаружения телекоммуникационных атак / Д.И. Правиков, П.В. Закляков // Проблемы управления безопасностью сложных систем: труды междунар. конф. – М., 2002. – Ч. 1. – С. 310–314.

5. Боршевников А.Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы междунар. науч. конф., г. Уфа, октябрь 2011 г. – Уфа, 2011. – С. 8–13.

Алейнов Юрий Викторович
Аспирант каф. безопасности информационных систем Самарского государственного университета
Тел.: 8 (917) 812-9568
Эл. почта: aleinov@gmail.com

Aleinov Y.V.

The method for increasing the efficiency of unknown type intrusion detection by introducing false targets in the network

A method of increasing the efficiency of unknown type intrusion detection, based on using of decoys in the network, is suggested. A model that allows to tie likelihood of an attack on a decoy for each time with parameters of decoys, network and the external environment is described. A generalized method for obtaining the optimal configuration of decoys in the network in a time-varying input parameters is shown.
Keywords: intrusion detection, decoys, increasing efficiency.
