УДК 004.725.7

Балакин С.В.

ОПТИМИЗАЦИЯ ДИАГНОСТИРОВАНИЯ НЕСАНКЦИОНИРОВАННЫХ ДЕЙСТВИЙ В КОМПЬЮТЕРНОЙ СЕТИ

Національний авіаційний університет
bpys@i.ua

Введение

Технологии глобальных компьютерных сетей стремительно развиваются, формируют в информационной области новую систему отношений, которая отражает реалии технического уровня современного человечества. Интенсивность изменений в значительной степени диктуется тем огромным значением, которое приобретает информация в постиндустриальном обществе, становясь главным ресурсом и инструментом одновременно.

Проведена оптимизация диагностики вредоносных программ в компьютерной сети и предложены новые решения имеющихся проблем.

Разрешимой проблемой выступает оптимизация метода диагностирования вредоносных программ в компьютерной сети. Главной задачей является корректное диагностирование вторжений в компьютерной сети, без обновления сигнатур. Данная модель основана на работе с симптомами вторжений, которые посредством использования операторов Теории Демпстера-Шафера (ТДШ) формируют соответствующее движение о наличии или отсутствии несанкционированных действий (НД) в системе.

Исследования в данной сфере

При выполнении поставленного задания использовались результаты предыдущих исследований, которые описывали диагностирования НД и показывали корректность их работы.

Исследования базируются на использовании ТДШ разработанной Гленном Шафером и Артуром Демпстер, которая описана в работах [1, 2]. Теория развивалась и в последующих работах. ТДШ также может быть использована в системах обнаружения вторжений для структурирования полученных в ходе постоянного мониторинга и анализа функций системы данных [3]. ТДШ может объединить отдельные части доказательств для получения конечного результата и установления вывода о наличии или отсутствии вторжений. ТДШ обладает всеми свойствами, которые могут помочь выявлять вторжения и НД в компьютерной сети.

Цель исследования

Цель исследования заключается в предоставлении необходимой теоретической базы для использования приведенных концепций и теорий, которые могут комбинироваться с современными решениями для повышения эффективности обнаружения вторжений в компьютерной сети. Рассмотрены основные алгоритмы обнаружения изменения, потому что они будут использоваться при диагностике для контроля временных фрагментов и формирования данных для определения симптомов и сигнатур вторжений [3].

Цель диагностирования - определить полностью наблюдаемую систему и дерево диагностики, которое классифицирует все состояния, чтобы определить, является эффективным диагноз в любой момент времени.

Результаты исследования

Для решения задачи распознавания НД методом диагностики предлагается, основываясь на работе операторов ТДШ, использовать следующую модель обнаружения вторжений (рис.1).

На основе наблюдений и собранных доказательств строятся симптомы, которые после процесса отбора дают возможность относить определенные

типы активностей в сети до вторжений или обычных действий системы [3].

Обзор процесса диагностирования сведен к следующему виду:

DRT=(Obs,Symp,Sel)=[Present(Obs) → Check(Symp) →Sel(Symp) →

Get (SymptA,SymptP)]→Diagn.

где, Obs – наблюдаемые;

Symp – симптомы;

Sel – критерий отбора.

При работе выполняются следующие операторы:

Present (Obs) - оператор представления наблюдаемых (O);

Check (Symp) - проверка наблюдаемых на наличие в них симптомов, которые будут служить для диагностики состояния системы;

Sel (Symp) - отбор симптомов из набо-ра наблюдаемых;

Get (SymptA, SymptP) - после операции отбора получаем на выходе информацию о наличии симптома (SymptP) или его отсутствие (SymptA);

Diagn - вынесение диагноза на основе совокупности полученных симптомов из набора наблюдаемых.

Рис.1. Модель диагностирования несанкционированных действий

На основе наблюдений и собранных доказательств, главной целью ТДШ является определение вероятности того, насколько данное состояние SRTi является фактическим состоянием процесса [1, 2]. Диагноз формируется на основе доказательств ТДШ. При наличии доказательства о предоставлении информации о текущем состоянии процесса, то он должен либо поддерживать группировки возможных состояний, или не допускать их, если не достигнуто определенной степени уверенности в этих доказательствах.

ТДШ формирует доказательства по достижении уровня уверенности в них, и такой результат называется основным убеждением (ОУ). Формально ОУ является функцией fsrt, где SRT представляет собой связанную структуру проникновения. fsrt отражает любую подмножество структуры проникновения для реального значения, fsrt: P(SRT) → R. Значение области представляет собой набор поддерживаемых состояний, а соответствующее значение диапазона представляет силу этой поддержки. Значение в диапазоне обозначается как масса убеждения (или просто масса).

Все массы убеждения ограничены значениями 0 и 1 включительно, $\forall x \in P(STR), 0 \leq fsrt(x) \leq 1$. Масса убеждению 0 представляет собой полное отсутствие поддержки соответствующего набора состояний (то есть не содержит фактического состояния). Масса убеждения 1 означает, что текущее состояние входит в данного набора. ОУ делит ровно 1 единицу массы убеждения на все возможные наборы состояний. Разделение достигается уравнением. Масса убеждения никогда не должна распределяться на пустые состояния fsrt (∅)=0. Получается, что ОУ - это совокупность всех возможных «претензий», которые могут возникнуть в процессе в рамках конкретной структуры проникновения. Любой набор состояний, которому присваивается ненулевая масса, свидетельствует, что процесс может быть в одном из этих состояний. Присвоение нулевой массы означает, что процесс отсутствует.

Можно назначить массу убеждения против набора состояний A, через

структуру проницательности SRT. Это делается путем построения нового набора состояний B, содержит все элементы в структуре проницательности не в A, B = SRT / A, и присвоении ей массы убеждения. Масса убеждения в пустых множествах равна нулю. Это происходит потому, что масса в пустом наборе доказывает, что ни одно состояние из структуры проницательности не описывает текущее состояние процесса, а это противоречит тому, что структура проницательности охватывает все возможные состояния процесса, в которых может быть система. В ОУ масса может быть приписана к его структуре проницательности.

Данный набор имеет особое значение, поскольку любая присвоенная к нему масса не знает ничего об истинном положении процесса (он обеспечивает равную поддержку для всех состояний, не оказывая полезной информации о них). ОУ со всей своей массой, предназначенной в структуру различия, будет полностью пустой.

Все симптомы будут двоичными (BS) - то есть иметь только два значения - наличие или отсутствие вторжения.

Пусть BST обозначает «массив истинных верований» и будет BST*(∧) (BST)>0, то есть будет одним фокальным элементом, а не структурой проникновения. Пусть BSF обозначать «массив ложных верований» и будет определяться BSF ⊂ ∧ (BSF) > 0, то есть одним координационным элементом, а не структурой проникновения . Значение достоверности можно настроить так, чтобы регулировать количество масс, выделяемых на любой элемент ОУ. Этот принцип применим к двум отдельным значений достоверности, регулирующих достоверность в *STa* и в *STp* .

Обозначим "текущее состояние" S как CS. Оказывается, что корректировка значений доверия stx и sty не затрагивают результаты диагноза CS из-за того, что:

1. Все симптомы - бинарные.

2. Каждый симптом на выходе имеет массив симптомов BST или BSF, содержащий текущее состояние S, CS. Каждый симптом правильно предусматривает CS из массива симптомов, содержит CS. Следует отметить, что по определению бинарного симптома CS содержаться в BST, BSF или BST и BSF таким образом, симптом всегда способен сделать правильный прогноз.

3. Каждое состояние в структуре проникновения должено иметь уникальную сигнатуру или набор сигнатур.

Процесс выявления симптомов громоздкий и часто выдает много ошибок. Чтобы избежать погрешностей при присвоении доверий BST и BSF, в состояниях бинарного симптома при прогнозировании актуализируется CS. Как правило, если симптом st правильно определен при прогнозировании состояния BS (где BS будет симптомом, а BST или BSF множеством состояний), ему должно быть назначено больше массы доверия (BS) ≈ 1, а если симптом st некорректен, то ему будет назначен меньшую массу веры (BS) ≈ 0. Чем больше масса доверия представлена в BS, тем больше она будет учитываться при слиянии, а чем меньше масса - тем меньше она будет учитываться.

Система может быть построена для назначения масс вероятности к набору симптомов. Если есть | ST | бинарные симптомы, каждый из которых имеет состояния BST и BSF, то будет два | ST | состояния, которым нужно назначить массы вероятности. Сначала все массы будут установлены в определенное начальное значение. Затем система начнет работать под наблюдением оператора. Если система предусмотрела CS неправильно, например, c ∈ , а оператор идентифицирует несоответствие и устанавливает настоящий CS в состояние d ∈ , то можно отслеживать каждое состояние с z, выпускающее симптом с ST, и занизить массу вероятности неправильных определений c ε z ∧ d ε z. Если система не смогла правильно предсказать CS-за того, что множества состояний были назначены после сравнений достоверности, а оператор не заметил ошибку, то со временем система сама по себе за-

высит массу правильных и занизит массу неправильных состояний.

Недостатком такого метода является то, что даже обученная таким образом система может выводить неправильный результат. Корректность зависит от количества симптомов, содержащихся в ST. Можно даже научить систему так, чтобы она всегда выдавала ложные значения CS. Но если возможность выявления правильного диагноза работает корректно, то со временем система сможет перейти в правильный режим обнаружения несанкционированных действий путем перераспределения масс важности среди своих состояний.

Как было рассмотрено выше, хоть листья дерева диагностики и могут определить точный набор состояний, другие узлы аппроксимируются как объединение множеств состояний их производных. Когда система переходит в состояние, содержащиеся в состоянии набора узла, но не в его приближенном состоянии, диагностика будет возвращать узел, предшествующий настоящему узлу в дереве диагностики. Единственный способ обеспечить то, чтобы конкретный узел всегда получал наиболее точный диагноз, это полностью обеспечить объяснение набора состояний объединением множеств состояний его предыдущими узлами. Это приведет к увеличению размера и количества вершин писем, увеличит структуру проникновения, которая будет требовать большего количества симптомов для правильного выполнения диагностики.

Повышение достоверности, утраченной в результате установления состояний приближения, требует дополнительных вычислительных ресурсов из-за сложности конечной модели. Среди огромного количества возможных состояний, в которых система может быть, получение абсолютно точного диагноза практически недостижимо.

Дополнительным преимуществом обучения масс есть информация, которую оно предоставляет о качестве симптомов. Если симптом имеет низкую массу вероятности на обоих своих состояниях, то он будет автоматически заменен другим, более точным симптомом.

Выводы

Представлена модель выявления НД, которая базируется на диагностике вторжений в компьютерной сети, без обновления сигнатур. Данная модель основана на работе с симптомами вторжений, которые посредством использования операторов ТДШ формируют соответствующее движение о наличии или отсутствии НД в системе.

Для обнаружения вторжений описаны характеристики НД, которые лучше всего характеризуют действия злоумышленника или атаки.

Было описано всю необходимую информацию для организации диагностирования. Определены состояния, в которых находится система, а также требования к этим состояниям. Для обеспечения функционирования и организации состояний системы на различных уровнях детализации ведено дерево спецификаций, которое используется для построения дерева диагностики и моделирует аномальное поведение системы.

Дано объяснение наблюдаемости и того, как формируются и используются симптомы для диагностики системы. Показано как несколько симптомов могут быть объединены вместе для обеспечения более точного диагноза. Показано, что диагностирование будет работать корректно как в лабораторных, так и в реальных условиях, с помощью функции настройки массы симптомов.

Проведенные исследования показывают целесообразность используемых инструментов оптимизации диагностики. Данный подход эффективен при выявлении и предотвращении НД в компьютерной сети.

Литература

1. Yang B-S. Application of Dempster-Shafer theory in fault diagnosis of induction motors using vibration and current signals. / Yang B-S., Kim K. J // Mechanical Systems and Signal Processing. – 2006. Vol. 20 (2). – P. 403-420.

2. Prioritizing intrusion analysis using Dempster-Shafer theory: proceedings of the 4th ACM workshop on Security and articial intelligence. / ACM. October 2011. – P. 59-70.

3. Пат. 123634 Україна МПК G06F 12/14. Спосіб діагностування несанкціонованих дій в комп'ютерній мережі / Жуков І. А., Балакін С. В. – №201702719; заявл. 23.03.17; опубл. 12.03.18, Бюл. №5. 4 с.

Балакін С.В.

ОПТИМІЗАЦІЯ ДІАГНОСТУВАННЯ НЕСАНКЦІОНОВАНИХ ДІЙ В КОМП'ЮТЕРНІЙ МЕРЕЖІ

Проаналізовано проблему діагностування несанкціонованих дій в комп'ютерних мережах з метою оптимізації протоколів їх роботи і підвищення працездатності. Розглянуто можливості по обробці діагнозів вторгнень через бінарні симптоми. Введено масу переконання, що дозволить більш точно регулювати відбір необхідних симптомів для формування точних діагнозів. Наведено рівняння моделі діагностування вторгнень. Запропоновано шляхи оптимізації підвищення виявлення шкідливих програм і атак в комп'ютерній мережі. Сформульовано необхідні критерії і вимоги для забезпечення своєчасного виявлення вторгнень в комп'ютерні мережі. Сформовано шляхи оптимізації діагностики та можливості автономного виявлення несанкціонованих дій (без використання і звернення до сигнатурних баз даних). Запропоновано описувати набори станів необхідними структурами проникнення, що дадуть можливість групувати необхідні дії і прискорити їх обробку. Введена можливість класифікації якості симптомів, дозволить автоматично замінювати слабкі симптоми найсильнішими.

Ключові слова: комп'ютерна мережа, діагностування, дослідження, симптом, оптимізація, несанкціоновані дії, виявлення вторгнень.

Balakin S. V.

OPTIMIZATION OF DIAGNOSIS OF UNAUTHORIZED ACTIONS IN A COMPUTER NETWORK

The problem of diagnosing unauthorized actions in computer networks is analyzed in order to optimize the protocols of their work and increase efficiency. Considered possibilities of processing the diagnosis of intrusions through binary symptoms. Introduced Mass of Conviction that will accurately regulate the selection of the necessary symptoms for the formation of diagnoses. Equations of the model for diagnosing intrusions are given. Ways to optimize the improvement of malware detection and attacks on a computer network are proposed. The necessary criteria and requirements are formulated to ensure timely detection of intrusions into computer networks. The ways of optimizing diagnostics and the possibility of autonomous detection of unauthorized actions (without using and accessing signature databases) have been formed. It is proposed to describe sets of states by predefined structures, that will make it possible to group the necessary actions and speed up their processing. Introduced ability to classify the quality of symptoms, that will automatically replace weak symptoms with strong ones.

Keywords: computer network, diagnostics, research, symptom, optimization, unauthorized actions, intrusion detection.