Математические структуры и моделирование
2005, вып. 15, с. 116–124

УДК
004.056.53+004.49+004.891

ВОЗМОЖНЫЕ ВАРИАНТЫ ПОСТРОЕНИЯ ИНТЕЛЛЕКТУАЛЬНОЙ СИСТЕМЫ ОБНАРУЖЕНИЯ НЕСАНКЦИОНИРОВАННОЙ РАБОТЫ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Е.Н. Дудоров

Представлен анализ основных методов обнаружения несанкционированной работы программного обеспечения. Рассмотрен возможный подход к построению интеллектуальной системы выявления подозрительной активности исполняемого кода.

В настоящее время большое внимание уделяется вопросам обеспечения информационной безопасности автоматизированных систем обработки информации, предназначенных для управления жизненно важными объектами страны. К таким объектам можно отнести системы телекоммуникаций, атомные станции, системы управления воздушным и наземным транспортом, банковские системы, системы обработки и хранения секретной и конфиденциальной информации и т.д.

Указанные автоматизированные системы также называются критическими, так как любое искажение, несанкционированное использование, потеря циркулирующей в них информации может привести к неисправимым последствиям. В целях предупреждения таких ситуаций необходимо постоянно совершенствовать методы и средства обеспечения безопасности подобных компьютерных систем. Любая явная или скрытная угроза направлена на нарушение целостности вычислительных процессов, происходящих в автоматизированной системе. В качестве возможного подхода к обеспечению стабильной работы предлагается внедрить в компьютерную систему интеллектуальную среду, позволяющую анализировать и контролировать процессы, сопутствующие запуску и работе программного обеспечения.

Стремительное развитие информационных технологий привело к появлению бесчисленного множества программных средств скрытого информационного воздействия. При создании нового программного продукта в большинстве случаев используются уже готовые программные решения, порой содержащие в себе заимствованные ошибки программирования, а также дополнительные программные модули, способные нанести существенный вред при обработке информации. Данное обстоятельство приводит к необходимости создания гибкого

аппарата принятия решений о несанкционированном поведении внедряемого программного обеспечения.

Для решения данной задачи предлагается использовать наработки таких направлений искусственного интеллекта, как теория распознавания образов, нечеткая логика и искусственные нейронные сети.

Рассмотрим наиболее распространенные подходы к выявлению подозрительной активности программного обеспечения.

1. Сигнатурный метод анализа

Метод основан на том, что большинство вредоносных воздействий на систему известны и развиваются по схожим сценариям. В данном подходе сигнатуры подозрительной активности определяют характерные особенности, условия, устройство и взаимосвязь событий, которые ведут к попыткам нарушения безопасности системы или способствуют им. Простейшим методом реализации сигнатурного анализа является поддержание системой безопасности базы данных сигнатур вторжений. Последовательность действий, выполняемая пользователем или программой во время выполнения, сравнивается с известными сигнатурами.

Необходимо отметить, что непосредственное сравнение сигнатуры вторжения с регистрируемой активностью малоэффективно в связи с тем, что регистрируемые данные, относящиеся к атаке, часто бывают зашумлены вследствие вариаций действий нарушителя во время атаки или мутаций сценария.

2. Контроль работы программ по профилям

Наиболее характерными особенностями автоматизированных систем обработки информации (АС) является наличие большого количества разнородных компонентов, сложных взаимно переплетающихся связей, развитой системы математического обеспечения, предназначенной для обработки огромных информационных потоков. Любая АС характеризуются множеством состояний. В компьютерных системах для описания поведения субъектов по отношению к объектам используют понятие «профили».

Профиль представляет собой образ, который создается на базе множества состояний протекающих процессов в АС. Иначе, профили — это набор статистических характеристик (частоты встречаемости событий, временные интервалы работы CPU и т.д.), вычисленных по наблюдениям за действиями субъекта по отношению к объекту, а также некоторой статистической моделью такого поведения.

Структура профиля может быть представлена в следующем виде: имя переменной; отражаемые действия; имеющиеся исключения; данные использования ресурсов; период измерений; порог допустимых значений; субъект; объект; значение последнего наблюдения модели и т.д. Статистические сведения о программах можно получить лишь путем мониторинга за его работой в конкретной среде и на конкретной платформе.

Любое отклонение используемого профиля от эталонного, рассматривается как проявление подозрительной активности программы. Недостатком данного метода является: во-первых, факт того, что «статистические» системы могут быть с течением времени «обучены» нарушителями так, чтобы подозрительные действия рассматривались как нормальные. Во-вторых, «статистические» системы не чувствительны к порядку следования событий. В-третьих, очень трудно задать граничные (пороговые) значения характеристик, отслеживаемых системой обнаружения аномалий, чтобы адекватно идентифицировать подозрительную деятельность.

3. Использование прогнозируемых шаблонов

Этот способ позволяет «предсказывать» будущие события на основе уже происшедших. Данный метод имеет несколько преимуществ. Во-первых, правила, базирующиеся на последовательности шаблонов, могут определять подозрительную активность, которую трудно идентифицировать традиционными методами. Во-вторых, системы, построенные на этой модели, очень хорошо приспособлены к изменениям. Это связано с тем, что редкие шаблоны непрерывно удаляются, оставляя наиболее часто используемые шаблоны. В третьих, подозрительные действия могут быть обнаружены в течение нескольких секунд после генерации события.

Недостаток данного метода состоит в том, что если в базе знаний не описаны некоторые сценарии осуществления несанкционированной деятельности, то такие действия не будут определены как подозрительные.

4. Метод обнаружения опасных комбинаций безопасных событий

Подразумевается распознавание последовательности, на первый взгляд, «безобидных» действий, суммарным результатом которых является нарушение целостности вычислительного процесса и доведение системы до неработоспособного состояния. Сложность распознавания таких событий заключается в большом количестве комбинаций опасных событий.

5. Анализ перехода системы из состояния в состояние

В данном подходе подозрительная активность представляется как последовательность переходов контролируемой системы из состояния в состояние. Состояние шаблона атаки соответствует состоянию системы и связано с утверждениями, которые должны быть удовлетворены для последующего перехода из состояния в состояние. Возможные состояния связаны дугами, представляющими события, необходимые для перехода из состояния в состояние. Типы допустимых событий встроены в модель. Данная модель может определить только атаку, состоящую из последовательных событий, не позволяя выразить

атаки с более сложной структурой. Более того, не существует общего целевого механизма в случае частичного распознавания атак.

6. Нечеткие сети Петри

Метод, использующий формализм сетей Петри для обнаружения нарушителей, является развитием метода анализа изменений состояний. Сети Петри представляют собой математическую модель для представления структуры и анализа динамики функционирования систем в терминах «условие-событие». К настоящему времени известно большое количество разновидностей сетей Петри, к которым, в первую очередь, следует отнести временные СП, СП с разноцветными маркерами и дугами, алгебраические СП, Е-сети. Данные классы моделей позволяют представить структуру и динамику функционирования исследуемых систем в условиях отсутствия влияния различных факторов неопределенности [7]. Указанный метод позволяет получить более точные результаты в области обнаружения нарушителя, однако требует значительных вычислений.

7. Контроль превышения пороговой величины частоты событий

Метод наиболее часто используется для распознавания атак типа «отказ в обслуживании». Для анализа частоты событий и установления для них пороговых величин системе распознавания требуются сведения о нормальном, рабочем состоянии АС, которые для каждой системы уникальны. Использование данного подхода требует глубокого анализа всех параметров АС, а также составление алгоритма действий на случай превышения пороговых величин.

8. Статистический анализ последовательности системных вызовов

Для обнаружения несанкционированной деятельности исследуется применимость различных моделей анализа данных к последовательностям системных вызовов, сгенерированных исследуемой программой во время исполнения. Эти данные могут рассматриваться как стационарные (отсутствие корреляции между различными запусками программ), но не независимыми (часто имеются различные распределения последовательностей вызовов в начале выполнения программы, в ее конце и на определенных участках) [5]. Наиболее часто используются следующие методы анализа данных.

– Простая нумерация последовательностей. Метод заключается в нумерации последовательностей системных вызовов, обнаруженных в трасе программы при нормальном исполнении и вторжении.

– Относительная частота последовательностей. Метод основан на частотном распределении последовательности системных вызовов. Каждая последовательность характеризуется значением, определяемым на основе того, как часто она встречается в нормальном поведении. Таким образом, каждое выполнение

программы может быть представлено гистограммой последовательностей вызовов. Каждая гистограмма определяет точку в многомерном пространстве. Множество нормальных выполнений программы образует центроиды, относительно расстояния до которых можно делать заключения о правильности текущего выполнения.

– Информационный анализ. Метод состоит в выделении особенностей больших наборов данных, т.е. необходимо определить наиболее компактное описание нормального поведения на основе перебора максимально возможных шаблонов, отражающих нормальное поведение пользователя. На основе определенных особенностей необходимо сделать обобщение для определения нормальных шаблонов, пропущенных в тренировочных данных.

– Машина конечных состояний (скрытая модель Маркова). Подход заключается в разработке машины конечных состояний для распознавания «языка» – трасы программы. Для решения данной задачи существует много техник, основанных на использовании как детерминистских, так и вероятностных автоматов. Обычно определяется частота, с которой появляются отдельные символы (системные вызовы) в зависимости от некоторого числа предыдущих символов. Состояния соответствуют истории системы, а переходы показывают вероятность появления следующего символа. При этом алгоритмы базируются на стационарности данных.

Одной из основных моделей построения таких систем является Скрытая Модель Маркова (СММ). Состояния СММ представляют некоторые ненаблюдаемые условия моделируемой системы. В каждом состоянии существует вероятность некоторого наблюдаемого вывода системы и отдельная вероятность, определяющая следующее состояние. Наличие в модели отдельного распределения вероятности вывода для каждого состояния и возможности изменений состояний во времени позволяет представить в модели нестационарные последовательности. Модель является очень мощной, но требует большого объема вычислений.

9. Продукционные /экспертные системы

Продукционные /экспертные системы обнаружения вторжений представляют собой специализированные автоматы обработки знаний для интерактивного и кооперативного решения проблем распознавания на естественном профессиональном языке со способностями приобретения, хранения и представления знаний в форме алгоритмических программ с одной стороны и неалгоритмических фактов и правил – с другой стороны [1].

Основное преимущество данных систем состоит в том, что они не отвергают и не заменяют традиционного подхода к программированию. Они отличаются от традиционных программ тем, что ориентированы на решение неформализованных задач и обладают следующими особенностями:

– алгоритм решений не известен заранее, а строится самой экспертной системой с помощью символических рассуждений, базирующихся на эвристических приемах;

– ясность полученных решений, то есть система «осознает» в терминах пользователя, как она получила решение;

– способность анализа и объяснения своих действий и знаний;

– способность приобретения новых знаний от пользователя-эксперта, не знающего программирования, и изменения в соответствии с ними своего поведения.

Таким образом, экспертная система состоит из набора правил, которые охватывают знание человека-эксперта. На основе анализа данных, получаемых от модулей слежения, экспертная система может предоставлять заключение об аномальной работе программного обеспечения. Экспертные системы допускают объединение огромного опыта, накопленного человеком, в компьютерном приложении, которое затем использует эти знания для идентификации деятельности, соответствующей несанкционированному поведению программ. Наряду с достоинствами есть и недостатки. Наличие базы знаний требует высокой квалификации для ее постоянного обновления для того, чтобы оставаться актуальной. [2]

Системы на основе фиксированных правил страдают от неспособности обнаруживать сценарии несанкционированной деятельности, которые имеют место в течение продолжительного времени. Одним из путей устранения названной проблемы является использование нейронных сетей.

10. Нечеткая логика

Нечеткая логика (fuzzy logic) позволяет описывать правила в незавершенном, «размытом» режиме, в котором правила основываются на знаниях и весах событий, позволяющих предположить вероятность атаки. Использование аппарата нечеткой логики при составлении правил экспертной системы позволяет ввести нечеткость в определение вредоносных воздействий и сетевых вторжений. Ввиду новизны и сложности технологии на сегодняшний день известно ограниченное число специализированных приложений.

11. Нейронные сети

В отличие от экспертных систем, которые могут дать пользователю определенный ответ, соответствуют или нет рассматриваемые характеристики характеристикам, заложенным в базе данных правил, нейросеть проводит анализ информации и предоставляет возможность оценить, согласуются ли данные с характеристиками, которые она научена распознавать. Наиболее важное преимущество нейросетей при обнаружении подозрительной активности программы заключается в способности «изучать» характеристики несанкционированной деятельности и идентифицировать процессы, которые не похожи на те, что наблюдались в системе прежде.

Общая идея использования нейронных сетей заключается в следующем [10,11]: искусственная нейросеть состоит из набора элементарных элементов, которые взаимосвязаны друг с другом и трансформируют набор входных данных к набору желаемых выходных данных. Результат преобразования определяется

характеристиками элементов и весами, соответствующими взаимосвязям между ними. Путем видоизменения соединений между узлами сети можно адаптироваться к желательным выходным результатам. Обучение сети включает многократную подачу примеров на ее входы. Сеть отгадывает выход, сравнивает его с предложенным правильным и выполняет внутреннюю коррекцию сети, если выход был неправильным. Этот процесс повторяется для каждого примера. Для оценки выхода сети необходим критерий, определяющий достаточность соответствия. Обычно считается достаточным, если сеть дает правильный ответ в 90 случаев.

Искусственные нейросети представляют значительный потенциал для решения задач, связанных с обнаружением злоупотреблений, внешних атак, направленных против сетевых ресурсов. Но до сих пор остаются неразрешенными следующие проблемы:

– если для обучения используется небольшое множество примеров, результаты обнаружения являются приемлемыми; большое множество примеров значительно расширяет пространство решений, что приводит к неприемлемому уровню ошибок в распознавании;

– нейросети не позволяют увидеть логику принятия решения;

– нейросети требуют четкой настройки топологии и параметров сети, что требует от специалиста высокой квалификации в данной области.

В настоящее время большинство из перечисленных методов применяются в системах выявления атак (Intrusion Detection System IDS). Эти системы решают задачу мониторинга информационной системы на сетевом, системном и прикладном уровнях с целью выявления нарушений безопасности и оперативного реагирования на них. Наиболее известные продукты: RealSecure, Snort NetRanger, NIDES. Однако стоит отметить, что подобные системы, как правило, ориентированы на отслеживание состояния сетевого взаимодействия отдельных хостов или сегментов сети. Разработка и создание интеллектуальных систем распознавания подозрительной активности программного обеспечения является отдельным, перспективным направлением в организации комплексной защиты АС.

В этой связи предлагается в качестве возможного подхода при построении систем выявления подозрительной активности ПО использовать наработки таких направлений искусственного интеллекта, как нейронные сети и аппарат нечеткой логики на базе экспертной системы. Данный подход позволит за счет нейросети фильтровать большой объем вычислительных процессов, выделять подозрительные признаки деятельности и передавать данные экспертной системе для последующего принятия решения о нештатной работе программы. Структура возможной системы обнаружения подозрительной активности ПО представлена на рис.1.

В составе интеллектуальной системы присутствуют следующие компоненты:

– сенсоры слежения – обеспечивают сбор данных из контролируемого пространства;

– подсистема обнаружения подозрительной активности – непосредственно занимается обнаружением подозрительной активности исполняемого кода, ос-

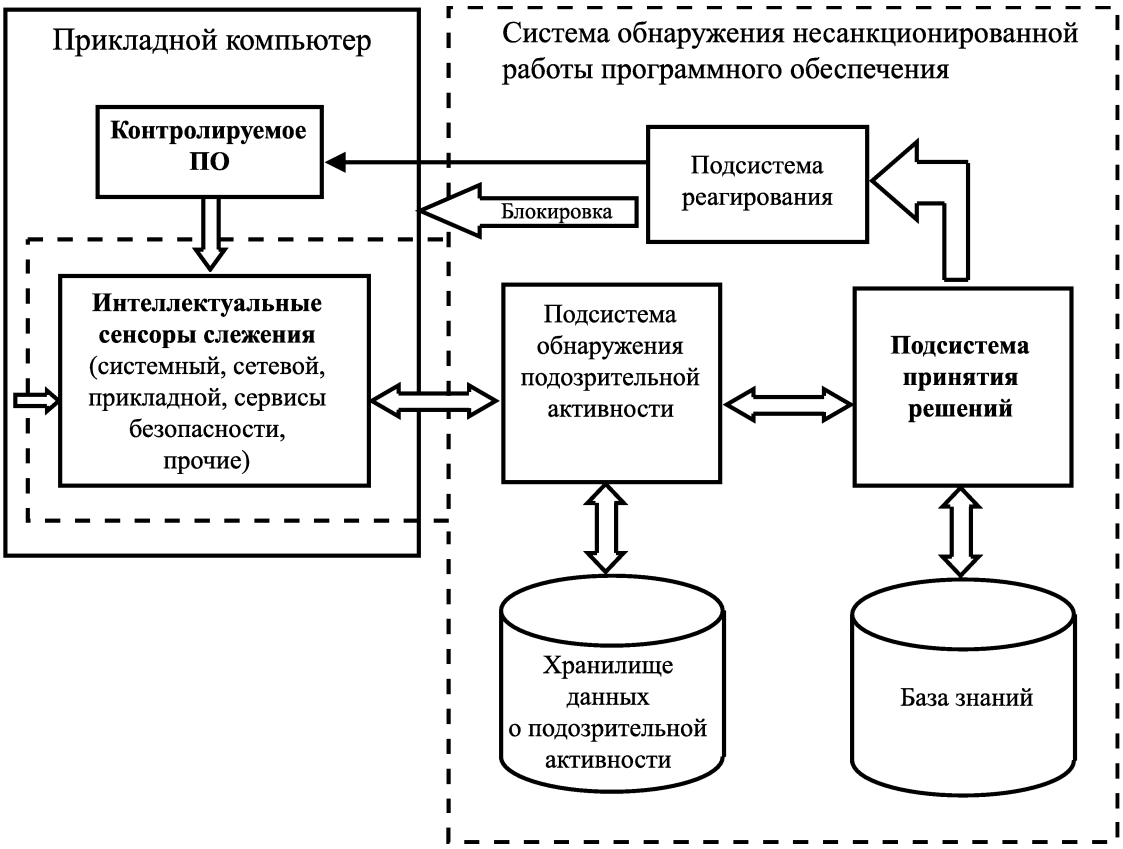

Рис. 1. Основные элементы системы обнаружения подозрительной активности ПО.

новываясь на критериях обнаружения;

– база знаний – в зависимости от методов, используемых в системе, может содержать профили вычислительной системы, сигнатуры атак, сценарии осуществления несанкционированной деятельности и т.д.;

– подсистема принятия решений – контролирует все компоненты системы обнаружения, хранит конфигурацию и инициирует сенсоры и подсистему обнаружения подозрительной активности, обеспечивает их критериями обнаружения, принимает решение о блокировании опасных процессов;

– хранилище данных о подозрительной активности – обеспечивает хранение данных, собранных в процессе функционирования подсистемы обнаружения подозрительной активности;

– подсистема реагирования – система, осуществляющая реагирование на обнаруженные несанкционированной деятельности программы.

Теоретическая правомерность использования нейросетей для идентификации подозрительной активности программ подтверждается результатами, полученными в ходе проведенных исследований при построении интеллектуальных систем обнаружения компьютерных вирусов [9, 10]. Предлагаемая сеть была предназначена для изучения характеристик деятельности обычной системы и идентификации статистических отклонений от нормы, что позволяло говорить о наличии вируса.

Таким образом, предложенный подход может быть реализован при построении систем выявления подозрительной активности программ.

Литература

1. Белов В.И. *Теория фазовых измерительных систем* / Под. ред. проф. Г.Н. Глазова. Томск: ТГАСУР, 1994.
2. Белозерский Л.А. Конспект лекций по курсу «Основы построения систем распознавания образов». Донецкий государственный институт искусственного интеллекта, 1997.
3. Дж. Кеннеди. Нейросетевые технологии в диагностике аномальной сетевой активности (перевод А.В. Лукацкого, Ю.Ю. Цаплева, В.П. Сахорова)// Сборник статей НИП «Информзащита», 2000.
4. Корнеев В.В. Использование нейросетей для аутентификации классов пользователей, операторов, идентификации управляющих воздействий и технологических процессов в компьютерах // Сб. докл. Республиканской научно-технической конференции «Методы и технические средства обеспечения безопасности информации» 17-19 окт. 1995, с. 95-97.
5. Корнеев В.В., Масалович А.И., Савельева Е.В., Шашаев А.Е.. Распознавание программных модулей и обнаружение несанкционированных действий с применением аппарата нейросетей. http://banana.stack.net:16000/db/msg/23820.html
6. Корт С.С. Теоретические основы защиты информации. Учебное пособие. М.: Гелиос АРВ, 2004. 240 с.
7. Круглов В.В., Борисов В.В. Искусственные нейронные сети. Теория и практика. М.: Горячая линия - Телеком, 2001. 382 с.: ил.
8. Черноруцкий И.Г. Методы принятия решений. СПб.: БХВ-Петербург, 2005. 416 с.: ил.
9. Минаев Ю.Н., Филимонова О.Ю., Бенамеур Лиес. Методы и алгоритмы решения задач идентификации и прогнозирования в условиях неопределенности в нейросетевом логическом базисе. М.: Горячая линия - Телеком, 2003. 205 с.: ил.
10. Denault, M., Gritzalis, D., Karagiannis, D., and Spirakis, P. (1994). Intrusion Detection: Approach and Performance Issues of the SECURENET System. In Computers and Security Vol. 13, No. 6, pp. 495-507
11. Fox, Kevin L., Henning, Rhonda R., and Reed, Jonathan H. (1990). A Neural Network Approach Towards Intrusion Detection. In Proceedings of the 13th National Computer Security Conference.
12. Hampshir J., Perlmutter B. A. . Equivalence Proofs for Multy-Layer Perceptron Classifiers and the Bayesian Discriminant Function. Carnegie Mellon University, Pittsburg, 1997.
13. Сайт с ПО SNORT. http://www.snort.org.
14. Сайт с ПО NIDS. http://www.bgnett.no/ giva .