Таран Анна Александровна
E-mail: Annie4ka@yandex.ru.
г. Ростов-на-Дону, ул. Добровольского, 36/2, кв. 115.
Тел.: +7515034220; 88632749704.
Студент.

Nesterenko Victor Aleksandrovich
Federal State-Owned Autonomy Educational Establishment of Higher Vocational Education "Southern Federal University".
E-mail: neva@sfedu.ru.
27/30, Tourgenevsky Street, Fl. 32, Rostov-on-Don, 344082, Russia.
Phone: +78632625798.
Senior Lecturer of Chair of Computer Science and Computing Experiment.

Taran Anna Alexandrovna
E-mail: Annie4ka@yandex.ru.
36/2, Dobrovolskogo Street, Russia, Fl. 115, Rostov-on-Don, Russia.
Phone: +79515034220; +78632749704.
Student.

УДК 004.056.5, 004.89

А.В. Никишова

АРХИТЕКТУРА ТИПОВОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ЗАДАЧИ ОБНАРУЖЕНИЯ АТАК

Рассмотрены основные тенденции развития атак. Предложена модель системы обнаружения атак, учитывающая их. Данная система обнаружения атак реализует сбор информации на нескольких уровнях информационной системы и использует для анализа системы искусственного интеллекта (нейронные сети). По результатам анализа ряда информационных систем организаций Волгограда была предложена архитектура типовой информационной системы. На ее основе была сформирован состав многоагентной системы обнаружения атак и деление ее агентов на миры.

Атака; система обнаружения атак; нейронная сеть; интеллектуальный агент; многоагентная система; миры; принятие совместного решения.

A.V. Nikishova

TYPICAL INFORMATION SYSTEM ARCHITECTURE FOR INTRUSION DETECTION PROBLEM

Major trends of attack's development have been considered. Intrusion detection system's model that takes them into consideration has been suggested. This intrusion detection system gathers information in several levels of information system and use artificial intelligence system (neural network) for analysis. According to the analysis of several information systems of Volgograd typical information system architecture was suggested. On its basis multi-agent intrusion detection system's structure and partition its agents into worlds.

Attack; intrusion detection system; neural network; intelligent agent; multi-agent system; worlds; make a joint decision.

В связи с широким распространением сетей общего пользования все большее число компьютеров подвергается атакам. Согласно статистике «Лаборатории Касперского» за 2010 г., количество новых атакующих воздействий держится на уровне 2009 г. и остается высоким (рис. 1), а общее количество инцидентов продолжает увеличиваться. В 2010 г. общее число зафиксированных инцидентов типа атаки через Интернет и локальные инциденты превысило 1,9 млрд.

В настоящее время основными особенностями атак являются:

- постоянное увеличение сложности атакующих воздействий, их технологический уровень значительно вырос даже по сравнению с прошлым годом. Зачастую атаки имеют многошаговый алгоритм действий и распределенный характер;
- большинство атак изначально осуществляется через браузер – при помощи множества уязвимостей и в самих браузерах, и в сторонних приложениях, взаимодействующих с ними. Это приводит к тому, что зачастую одна и та же вредоносная программа может распространяться при помощи десятка различных уязвимостей – что ведет к пропорциональному росту количества разновидностей атак [1].

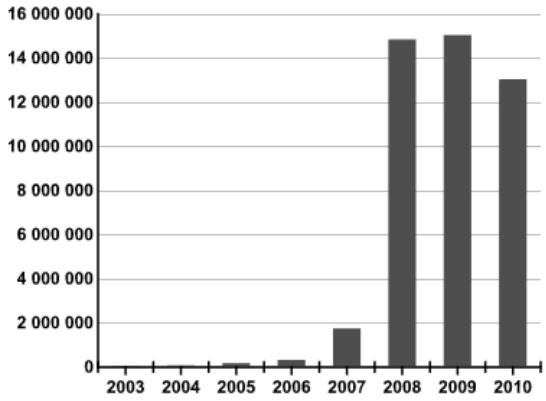

Рис. 1. Число новых атакующих воздействий, обнаруженных «Лабораторией Касперского»

Как показывает анализ современных бесплатных систем обнаружения атак (СОА), их развитие направлено на увеличение количества источников данных для анализа, но при этом в большинстве СОА не учитывается взаимосвязь этих данных. Кроме того, несмотря на то, что осуществляются попытки реализовать возможность СОА адаптироваться к новым видам атакующих воздействий, большинство современных СОА используют методы анализа, не позволяющие реализовать данную возможность.

Предлагается модель СОА. Чтобы учесть распределенный характер атак, также применяется распределенный сбор сведений о событиях, происходящих в информационной системе (ИС). Но, кроме того, СОА объединяет сведения, собранные из нескольких источников данных, и принимает обобщенное решение о возникновении атаки. Применяется метод анализа собранных сведений, позволяющий СОА адаптироваться к новым разновидностям и видам атак, – нейронные сети.

Для реализации идеи распределенного сбора сведений и их объединения для принятия решения о состоянии ИС применяются многоагентные системы. Многоагентные системы состоят из множества взаимодействующих агентов. Агенты в подобных системах характеризуются автономностью, ограниченностью представления и интеллектуальностью.

Свойство интеллектуальности агентов позволит проводить интеллектуальный анализ и учесть вторую особенность атак – существование и появление различных разновидностей атак и новых атакующих воздействий, количество которых велико согласно статистике.

Каждый агент описывается состоянием (P, B, S, G, I), где:

- P – ощущение. Представляет собой информацию об окружающей среде, собираемую агентом, т.е. набор входных данных агента;
- B – убеждения. Множество убеждений, т.е. сведений и знаний об окружающей агента среде. Убеждения агента представляют собой нейронную сеть. На начальном этапе агенты собирают сведения о функционировании информационной системы, и на их основе создается обучающая выборка для нейронной сети;
- S – ситуация. Конкретное состояние среды, т.е. конкретные значения входных данных и результата классификации их нейронной сетью;
- G – цели. Определяется как желаемое состояние среды;
- I – намерения. Множество возможных планов действий агента.

Агенты обладают следующими базовыми функциями:

- порождение и пересмотр убеждений. Данная функция отвечает за сбор сведений для обучения и в случае необходимости переобучения нейронной сети и самообучение;
- оценка ситуации. Получение результатов оценки собранных сведений об информационной системе нейронной сетью;
- активация цели. В зависимости от значения выхода нейронной сети агент выбирает набор элементарных действий, которые необходимо выполнить в данной ситуации;
- назначение. Агент определяет окончательный план действий, определяя последовательность элементарных действий;
- выполнение. Выполнение агентом выбранных элементарных действий [2].

Для выполнения распределенного сбора необходимо выбрать источники сведений о событиях, происходящих в ИС, которые будут подлежать анализу. Был проведен анализ ряда ИС организаций Волгограда и Волгоградской области. На основе этого анализа было проведено обобщение ИС организаций и была предложена архитектура типовой ИС (рис. 2).

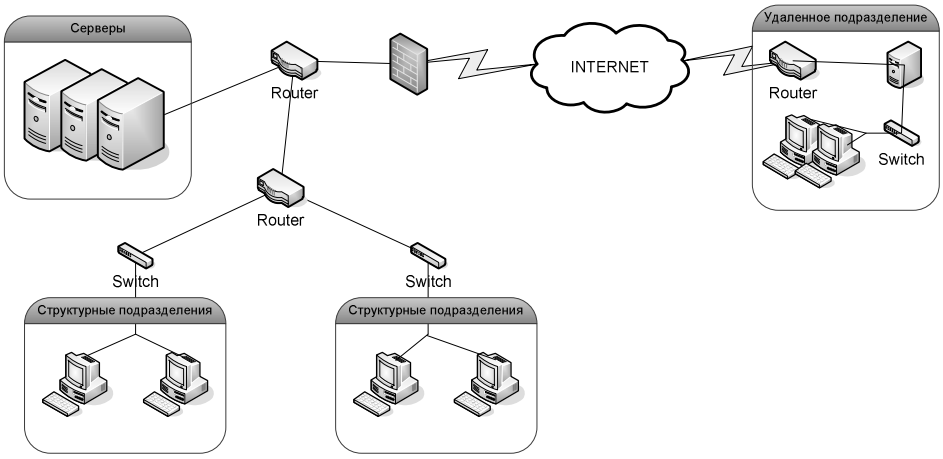

Рис. 2. Архитектура типовой ИС

Элементы данной типовой ИС были взяты за основу при построении многоагентной СОА. Все множество источников о событиях. происходящих в ИС, разбивается между агентами, и каждый агент получает ограниченное представление об ИС. Были выделены следующие источники сведений о событиях, происходящих в ИС, подлежащих анализу для задачи обнаружения атак:

- сведения о событиях операционной системы серверов;
- сведения о событиях маршрутизаторов;
- сведения о сетевых пакетах;
- сведения о событиях операционных систем рабочих станций.

Каждому из этих источников данных соответствует свой тип агента. Множество всех агентов имеет следующий вид:

- агенты рабочей станции. Анализ показал, что большинство рабочих станций функционируют под управлением ОС Windows различных версий (начиная от 98, заканчивая 7 версией). На каждой рабочей станции располагается ряд агентов, которые проводят анализ событий, наиболее критичных с точки зрения безопасности:
  - события, отражающиеся в журнале безопасности. Анализируются такие поля, как тип события, код события, имя пользователя, время возникновения;
  - события, отражающиеся в реестре. Анализируются такие поля, как путь, имя и значение;
  - сведения о процессах, выполняемых на компьютере. Анализируются такие их параметры, как процесс, запрос, источник запроса и результат запроса, и то, как они задействуют ресурсы рабочей станции.
- сетевой агент. Для того чтобы анализировать сведения о пакетах, передаваемых по сети, сетевой агент работает как сниффер, т.е. он получает все пакеты и анализирует их. Однако подобные программы работают только в пределах одного сегмента сети. Поэтому данный агент располагается в каждом сегменте. Анализируются такие сведения, как IP-адреса и порты получателя и отправителя, протокол и время получения пакета;
- агент маршрутизатора. На маршрутизаторах существует возможность ведения журнала событий. Анализ показал, что наиболее распространенным маршрутизатором является Cisco. Данные маршрутизаторы поддерживают возможность пересылать сведения журнала событий для хранения на указанный компьютер. На каждом таком компьютере располагается агент маршрутизатора, производящий анализ сведений данного журнала. Анализируются такие поля, как время, событие, протокол и источник;
- агенты сервера. Анализ показал, что большинство государственных учреждений и некоторые коммерческие организации имеют серверы под управление серверной ОС Windows различных версий (начиная от 2000, до 2008 версии). На каждом сервере располагается ряд агентов (состав зависти от функционального назначения сервера), которые анализируют события, наиболее критичные с точки зрения безопасности.

Так как многоагентная СОА содержит такое большое число агентов, то их взаимодействие каждый с каждым будет иметь существенное влияние на загруженность сети. А потому все пространство ИС разбивается на миры, которые ограничивают функционирование и взаимодействие агентов. Каждый агент может принадлежать нескольким мирам. В результате анализа было сформулировано следующее множество миров:

- миры, включающие в себя агентов рабочей станции. Анализируя события соответствующего источника, агенты рабочей станции принимают совместное решение о состоянии рабочей станции;
- миры, включающие в себя агентов сегмента сети. В этот мир имеют доступ по одному агенту с каждой рабочей станции (он обладает объединенным мнением о состоянии рабочей станции) и сетевой агент соответствующего сегмента сети. Данная группа агентов принимает совместное решение о состоянии сегмента сети;

- миры, включающие в себя агентов подсети. В этот мир имеет доступ агент маршрутизатора и сетевые агенты (они обладают объединенным мнением о состоянии соответствующего сегмента сети), сегмент сети которых соединен с данным маршрутизатором. Данная группа агентов принимает совместное решение о состоянии подсети, ограниченной данным маршрутизатором;
- миры, включающие в себя агентов сервера. Анализируя события соответствующего источника, агенты сервера принимают совместное решение о состоянии сервера;
- мир, в котором принимается окончательное решение о состоянии ИС. Данное решение принимают по одному агенту от каждого сервера (они обладают объединенным мнением о состоянии соответствующего сервера) и агенты маршрутизаторов (они обладают объединенным мнением о состоянии соответствующей подсети). Они принимают совместное решение об общем состоянии ИС.

Как уже отмечалось ранее, агенты проводят интеллектуальный анализ собранных ими данных. Для этого применяются искусственные нейронные сети, которые являются убеждениями агентов, представляя его знания. Недостаток применения систем, подобных нейронным сетям – большое число ложных срабатываний. Необходимость находить совместное решение позволяет нивелировать этот недостаток, уменьшая вероятность ложного срабатывания системы в целом.

Существует подход, интерпретирующий выход нейронной сети как вероятностное значение. В данной СОА принято, что нейронная сеть каждого агента возвращает значение в интервале [a; b]. Для всех событий ИС определяется несколько уровней опасности O_i. Агент относит событие к одному из уровней в зависимости от выхода нейронной сети L согласно разбиению выбранного интервала на соответствующие подынтервалы $[a_i; b_i]$. Каждый агент получает данную оценку. Если событие относится к определенным уровням опасности, то он инициирует принятие совместного решения агентами внутри своего мира.

Для каждого агента определены его предпочтения $O_i \succ O_j$ (например, для трех уровней для каждого агента определена тройка вида $O_i \succ O_j \succ O_k$). Второй в порядке предпочтений уровень определяется согласно алгоритму

Если $L>(a_i+1/2(b_i-a_i))$, *то*
$j=i+1$
иначе
$j=i-1$

То есть следующий уровень в предпочтениях агента определяется как следующий ближайший интервал к значению L и т.д.

Одним из способов принятия совместного решения в подобной ситуации является голосование. Победителем голосования, т.е. совместно принятым уровнем, будет уровень-победитель по Кондорсе, соответственно удовлетворяющий условию $\forall o' \in O, \#(o \succ o') \geq \#(o' \succ o)$. В связи с особенностью выбора порядка уровней в предпочтениях агентов исключен так называемый парадокс Кондорсе, при котором нельзя выявить победителя [4].

Одной из особенностей интеллектуальных агентов является их приспособляемость к внешней среде. Это реализуется за счет пересмотра убеждений агентов в случае необходимости. Чтобы принять решение о необходимости пересмотра убеждений агента, вводится показатель качества убеждений агента. Каждый раз при принятии совместного решения агентами этот показатель меняется в зависи-

мости от того, какое решение принял конкретный агент с учетом совместного решения. Когда такая оценка получена, происходит персонифицированное стимулирование агентов, т.е. уменьшение или увеличение показателя качества.

Когда показатель качества достигает некоторого критического значения, соответствующий агент переобучается на обновленном наборе данных, что позволяет агентам адаптироваться к изменяющимся условиям.

В настоящее время проводятся экспериментальные исследования на разработанном для данной модели программном комплексе.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. http: // www. securelist. com / ru / analysis / 208050677 / Kaspersky_Security_ Bulletin_2010_Razvitie_ugroz_v_2010_godu.
2. *Mluller Jorg P.* The design intelligence agents: a layered approach. Springer 1996 (Lectures notes in computer science. – Vol. 1177: Lectures notes in artifical intelligence) ISBN 3-540-62003-6.
3. *Лукацкий А.В.* Системы обнаружения атак // Сетевой. – 2002. – № 4.
4. *Shoham Y., Leyton-Brown K.* Multiagent systems. Algorithmic, game-theoretic, and logic foundations. – 2009. – С. 256-260.

Статью рекомендовал к опубликованию д.т.н., профессор О.Б. Макаревич.

Никишова Арина Валерьевна
Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Волгоградский государственный университет».
E-mail: arinanv@mail.ru.
400062, г. Волгоград, пр. Университетский, 100.
Тел.: 88442460368.
Старший преподаватель кафедры информационной безопасности.

Nikishova Arina Valerievna
Volgograd State University.
E-mail: arinanv@mail.ru.
100, Universitetsky Pr., Volgograd, 400062, Russia.
Phone: +78442460368.
Senior Lecturer of Department of Informational Security.