МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ АТАК С ПОМОЩЬЮ СКРЫТЫХ КАНАЛОВ И ВРЕДОНОСНОГО КОДА

А.А. Грушо, Н.А. Грушо, Е.Е. Тимонина

Российский государственный гуманитарный университет
Кировоградская 25, г. Москва, Россия
телефон: + 7(495) 2506699; e-mail: grusho@yandex.ru

В работе рассматривается новая парадигма построения защиты в распределенных компьютерных системах в предположениях, что в ее компонентах могут присутствовать враждебные программно-аппаратные агенты нарушителя безопасности, связанные с помощью скрытых каналов. Защищенность достигается обеспечением «невидимости» объектов защиты для враждебного кода. Рассматриваются методы обеспечения «невидимости» процессов, данных и программ.

Работа выполнена при поддержке РФФИ, грант № 07-07-00236, грант № 07-01-00484.

Ключевые слова – безопасность распределенных компьютерных систем, враждебный код, искусственный интеллект.

Специфика России состоит в том, что в решении задачи защиты информации в распределенных системах приходится иметь дело с импортной техникой, оснащенной иностранным программным обеспечением, которое может содержать средства скрытого информационного воздействия и разрушения. В системах связи используются протоколы, надежность которых нигде не доказана. Распределенные системы опираются на открытые сети, например Интернет. Поэтому проблема построения надежной защиты, опирающейся на ненадежные аппаратную и программную составляющие, использующей ненадежные глобальные сети и открытые протоколы, является для России актуальной научной проблемой [9].

Мы рассматриваем угрозы информационным ресурсам (ИР) и информационным технологиям (ИТ) в информационных системах, связанные с внедрением вредоносного кода (ВК) в компьютерные системы. ВК может представлять собой автономно действующего агента или совокупность агентов (многоагентную систему), выполняющих различные функции, связанные с нанесением ущерба ИТ и ИР. Программный агент – это некоторая вычислительная сущность, способная к автономному поведению, то есть программный агент может делать выбор из некоторого набора действий, когда сталкивается с задачей принятия решений, относящейся к его области действий. Помимо этого такая сущность рассматривается как часть сообщества подобных сущностей, которые спроектированы, чтобы взаимодействовать друг с другом для достижения общих целей. Агенты должны иметь возможность взаимодействовать друг с другом. ВК может располагаться как в аппаратной платформе (процессорах и контроллерах компьютерной системы), может находиться в памяти компьютерной системы и относиться к операционной системе или приложениям. Мы предполагаем, что проблема построения надежной защиты распределенных систем из ненадежных с точки зрения безопасности элементов состоит, в первую очередь, в противодействии угрозам, связанным с ВК.

Для описания методов ограничения возможностей ВК по нанесению ущерба приведем основные определения и рассмотрим некоторые аспекты вредоносного воздействия ВК [9].

Атака – это совокупность взаимосвязанных действий нарушителя безопасности по нанесению ущерба активам в автоматизированной системе.

Атака условно состоит из двух этапов. Первый этап (более длительный) заключается в разведке атакуемой автоматизированной системы, определении активов, способов воздействия на них и выявление уязвимостей системы, через которые может быть нанесен ущерб. Первый этап заканчивается подготовкой организационных и технических средств для нанесения ущерба. Второй этап – этап активных действий по нанесению ущерба. Он состоит, как правило, из трех шагов. Первый шаг – использование уязвимостей с целью реализации условий по нанесению ущерба (доступ к защищаемым ресурсам или к средствам воздействия на защищаемые ресурсы). Второй шаг – собственно нанесение ущерба активам. Третий шаг – маскировка действий нарушителя безопасности, для того чтобы избежать ответственности за нанесенный ущерб.

ВК может использоваться как на этапе разведки, так и в период активной фазы атаки по нанесению ущерба.

В работе отражены результаты исследований по анализу враждебных многоагентных систем (ВМА) и ВК в распределенныых компьютерных системах. В связи с анализом угроз со стороны ВМА возникают следующие задачи.

1. Содание ВМА.
2. Взаимодействие агентов между собой.
3. Защита одних агентов с помощью других от средств защиты.
4. Взаимодействие враждебной многоагентной системы с внешней средой.
5. Разведка компьютерной среды и поиск целей атаки.
6. Развитие враждебной многоагентной системы.
7. Реставрация враждебной многоагентной системы при сбоях и разрушениях.

8. Нанесение ущерба.
9. Защита от ВМА.

В качестве прообраза ВМА взята Open Agent Architecture, разработанная SRI [11]. Данная архитектура позволяет придать ВМА интеллектуальные функции, позволяющие объяснить, как решаются перечисленные выше задачи.

Пусть сеть враждебных агентов «невидима» для средств защиты. Выделяются три типа агентов:
1. агенты-посредники;
2. мета-агенты;
3. агенты интерфейса с внешними сетями.

Первый тип агента – агент посредник. Агент посредник представляет собой специализированного служебного агента, который отвечает за координацию взаимодействия агентов, их связь и кооперацию. В некоторых случаях посредник обеспечивает хранение данных для других типов агентов, то есть предоставляет им функции «black board» для их взаимодействия. Посредники должны быть связаны между собой в некоторый кластер. В частном случае это может быть иерархическая структура.

Следующим типом агентов являются мета-агенты. Этот тип агента ориентирован на реализацию конкретного набора функций в ВМА. Функции агента этого типа связаны с предметно-ориентированной информацией, либо с заданным видом приложений, либо с заданным видом деятельности.

Особо необходимо выделить агентов, реализующих функции интерфейсов. Эти агенты не являются посредниками, они реализуют интерфейсы с глобальными сетями, между узлами локальных сетей и т.д. Особенностью этих агентов является то, что данные агенты реализуют функции скрытых каналов, использующие открытые коммуникации [2, 4, 5, 6].

Всех агентов, которые не являются посредниками, будем называть агентами-клиентами. Каждый клиент соединен, по крайней мере, с одним посредником, который мы будем называть посредником-родителем для данного клиента.

Посредник получает запросы от клиента, отвечает ему или контролирует статус клиента. Для реализации запроса посредник задействует связь с другими посредниками и мета-агентами. Для создания агентов используются специальные библиотеки агентов. С помощью этих библиотек создаются, настраиваются новые агенты, осуществляется уничтожение агентов. Коды агентов могут поступать извне через агентов интерфейса и коммуникационную сеть посредников.

Рассмотрим некоторые сценарии функционирования ВМА. Предположим, что задачей агента-нарушителя безопасности является выборочное взаимодействие с ИР. Например, кража определенных данных или кража данных определенного формата, модификация определенных программ или данных, изменение определенных настроек программного обеспечения и т.д. Тогда ВМА должны уметь решать простейшие задачи искусственного интеллекта:
- распознавание форматов данных;
- распознавание данных в рамках данного формата;
- распознавание программ;
- распознавание начала и конца вычислений заданного вида.

При решении этих задач агенты должны следовать следующей логике, которая, вообще говоря, является обязательной для решения любой задачи:
1. Запуск задач.
2. Сбор исходных данных (в соответствии с некоторой схемой сбора данных).
3. Предоставление исходных данных для обработки.
4. Обработка данных по некоторому алгоритму.
5. Формирование результата.
6. Распределение данных в соответствии с некоторой схемой распределения данных.
7. Закрытие задачи.

При этом решение сложных задач осуществляется благодаря суперпозиции задач.

Основные идеи ВМА состоят в следующем [7].
1. Новый агент устанавливает связь с посредником, осуществляет поиск в окружающей среде информации по заданным признакам, создает образ среды и передает посреднику информацию об окружающей среде и о тех действиях, которые он может реализовать в этой среде. Данная информация через посредника передается мета-агентам, которые из фрагментов составляют некоторую общую картину компьютерной среды, определяют возможные действия в этой среде, определяют структуру защиты и организуют через посредников и прикладных агентов нейтрализацию функций защиты, в частности, «невидимость» ВМА для системы защиты. Особую роль играют агенты, обнаруживающие в окружающей среде каналы во внешнюю среду. Мета-агенты обеспечивают таких агентов информацией, позволяющую установить связь с другими агентами через найденные каналы во внешнюю среду. При установлении связи с внешними приложениями агент становится агентом интерфейса.
2. Интерпретация и выполнение заданий для ВМА является распределенным процессом.
3. Запрос одного агента может породить кооперацию и взаимодействие среди многих агентов ВМА.

Кооперация среди агентов ВМА достигается через передачу сообщений на общем языке, доступном пониманию агентами. Обычная процедура кооперации состоит из 2-х шагов.
1. Агенты через посредника снабжают мета-агента информацией о доступных сервисах.
2. Запросы на сервисы поступают от мета-агентов через посредников.

Посредники координируют действия агента при достижении заданной цели (например, взять информацию, передать ее через посредников агенту, имеющему связь с внешним нарушителем безопасности).

Структура языка взаимодействия агентов основана на понятии события. Активность всех агентов, а также и коммуникаций между агентами строится вокруг передачи и обработки информации о событиях. При коммуникаци-

ях события составляют содержание сообщений между агентами. События являются целями для действий агентов. Каждое событие имеет тип, множество параметров и содержание. Допустимые содержания и значения параметров могут различаться в зависимости от типа события.

Рассмотрим потенциально возможную схему создания ВМА в компьютерной или распределенной компьютерной системе.

1. Должен существовать сигнал активизации агента посредника. Этот сигнал может представлять собой «логическую бомбу» или сигнал извне, полученный по каналам связи из внешней среды. Посредник может быть заложен производителем в процессоре компьютерной системы. Однако возможны другие возможности скрытого от защиты местоположения посредника.
2. Активизированный посредник по шинам или другим каналам в системе передает запросы или сигналы активизации другим посредникам, которые могут присутствовать в системе. При получении ответа создается распределенная сеть посредников. В случае выполнения условия невлияния для каждого посредника и скрытых каналов взаимодействия между ними полученная распределенная сеть посредников будет удовлетворять условиям невлияния, то есть будет «невидима» для средств защиты.
3. Одновременно посредник (сеть посредников) должен создать хотя бы одного мета-агента.
4. Сеть посредников ищет канал во внешнюю среду и при наличии такого канала использует один из языков, заложенных в данные мета-агентов, для связи с внешней средой.
5. Для исследования окружающей среды с помощью мета-агентов и посредников создается сеть агентов.

Основная идея нашего подхода к защите информации при наличии ВК (ВМА) состоит в использовании ограничений интеллектуальных возможностей ВК и ограничение возможностей общения ВК с нарушителем безопасности с помощью скрытых каналов.

Предположим сначала, что нет скрытых каналов для интерактивного взаимодействия ВК с нарушителем безопасности, обладающим большим интеллектуальным потенциалом. Тогда функционирование ВК определяется возможностями программ и теми данными, которые удалось внедрить в атакуемый компьютер. Поскольку эти данные ограничены, то всегда существуют структуры данных, которые программа не может распознать как объект своего поиска. Например, программе могут быть недоступны некоторые эвристические методы поиска. Программа, ограниченная рамками своего искусственного интеллекта «не видит» недоступные ей структуры данных. При этом не исключаются взаимодействия ВК с искомыми объектами. В этом наша концепция отличается от известных концепций невлияния и ограничений на информационные потоки.

Рассмотрим, каким образом «невидимость» может быть использована при построении защиты от ВК [3, 9].

Для того чтобы нанести ущерб, ВК должен распознать место вредоносного воздействия и после этого реализовывать само воздействие. На этапе разведки ВК должен собрать информацию об используемых структурах данных и передать их в интеллектуальный центр для разработки атаки. Во всех случаях ВК должен осуществлять сканирование данных и анализировать взаимодействие с другими процессами в компьютерной системе. Однако если нужных данных нет, то ВК не может нанести ущерб, а отсутствие скрытого канала не позволяет ему привлечь высокий интеллектуальный потенциал для разработки атаки.

При разработке концепции мы использовали следующие слабые стороны ВК:

- интеллектуальная ограниченность ВК;
- присутствие и действие ВК могут быть замечены, и работа ВК может быть заблокирована;
- скрытые каналы взаимодействия ВК с интеллектуальным противником вне защищаемой системы могут быть ограничены.

В перечисленных предположениях можно эффективно использовать методы, затрудняющие ВК распознавать необходимую информацию. Применение данных методов не отменяет и не ограничивает применение системы ограничения доступов [1, 10].

Результат исследований можно сформулировать следующим образом. ВК может быть организован в распределенную интеллектуальную невидимую для средств защиты многоагентную систему. Однако для эффективного функционирования в серьезных приложениях интеллекта ВМА может казаться недостаточно. Тогда для реализации атак необходимо взаимодействие с интеллектуальной системой внешнего нарушителя безопасности. Для такого взаимодействия необходимы скрытые каналы. Если предотвратить функционирование скрытых каналов и обеспечить невозможность для ВК распознавать искомые программы и данные, то можно защитить информационные активы даже в присутствии ВК.

ЛИТЕРАТУРА

[1] Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. Изд-во Агентства «Яхтсмен», Москва, 1996.

[2] Грушо А.А., Тимонина Е.Е. Использование скрытых статистических каналов для атак и защиты информационных технологий, Тезисы докладов конференции «Методы и технические средства обеспечения безопасности информации», 27-29 октября, С.-Петербург, 1998.

[3] Грушо А.А., Тимонина Е.Е. Безопасность в многоагентной системе, Труды международной конференции «Информационные технологии в науке, образовании, телекоммуникации, бизнесе (осенняя сессия)», Украина, Крым, Ялта-Гурзуф, 20-30 сентября 2001, 129-130.

[4] Грушо А.А., Володин А.В., Тимонина Е.Е. Безопасный интерфейс с глобальной сетью из ненадежных в смысле безопасности элементов, Труды международной конференции «Информационные технологии в науке, образовании, телекоммуникации, бизнесе», Украина, Крым, Ялта-Гурзуф, 20-29 мая 2001 г.

[5] Тимонина Е.Е. Скрытые каналы (обзор), Jet Info, вып. 14(114), изд-во компании «Джет Инфо Паблишен», 2002, 2-11.

[6] Грушо А.А., Тимонина Е.Е. Роль скрытых каналов при построении защиты в распределенных компьютерных системах, В сб. Математика и безопасность информационных технологий. Материалы конференции в МГУ 23-24 октября 2003 г.
– М.: МЦНМО, 2004.

[7] Грушо А.А., Тимонина Е.Е. Враждебные многоагентные системы, В сб. Математика и безопасность информационных технологий. Материалы конференции в МГУ 28-29 октября 2004 г., М.: МГУ, 2005.

[8] Грушо А.А., Тимонина Е.Е. Распределенные атаки на распределенные системы, Jet Info, 2006.

[9] Грушо А.А., Грушо Н.А., Тимонина Е.Е. Методы защиты информации от атак с помощью скрытых каналов и враждебных программно-аппаратных агентов в распределенных системах // Вестник РГГУ: Серия «Информатика. Защита информации. Математика». – М.: Изд. Центр РГГУ, 2009. – с.33-45.

[10] Теоретические основы компьютерной безопасности: учеб. пособие для студентов высш. учеб. заведений / А.А. Грушо, Э.А. Применко, Е.Е. Тимонина, – М.: Изд. Центр «Академия», 2009. – 272 с.

[11] Martin D.L., Cheyer A.J., Moran D.B. The Open Agent Architecture: A Framework for Building Distributed Software Systems.