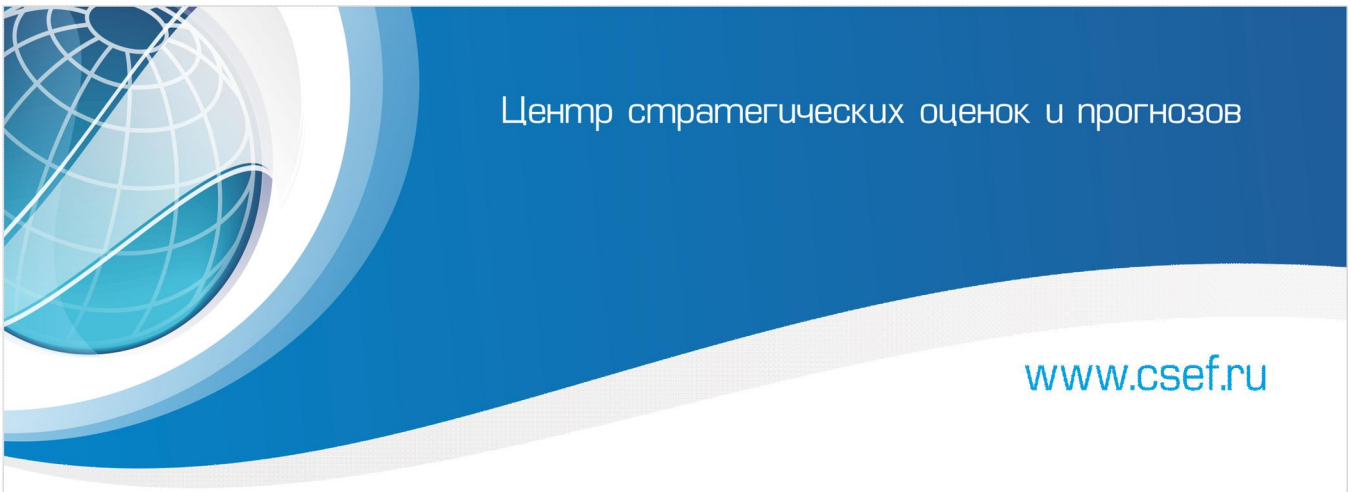

Сергей Гриняев

Системы обнаружения вторжений и реагирования на компьютерные инциденты на основе мобильных программ-агентов

Аналитический доклад

Москва – 2005

Содержание

О ПРОЕКТЕ

Начиная с сентября 1997 в США Национальным институтом стандартов и технологии (NIST), совместно с рядом фирм, при финансовой поддержке Агентства национальной безопасности реализуется проект, призванный оценить перспективу использования технологии мобильных программ-агентов для обеспечения безопасности компьютерных систем.

Целью проекта является исследование способов использования технологии мобильных агентов для улучшения характеристик программного обеспечения информационной безопасности, а также исследование путей, позволяющих обезопасить саму технологию мобильных агентов.

В последнее время работы по проекту сосредоточены на разработке технологии управления привилегиями мобильных агентов на основе цифровой подписи и цифровых сертификатов, что тесно связано с проводимыми NIST работами по формированию национальной инфраструктуры для работы с криптосистемами с открытым ключом (PKI), а также на возможности применения технологии мобильных агентов для улучшения характеристик систем обнаружения вторжения.

1. Введение в проблему

Системы обнаружения вторжения (СОВ) сегодня уже достаточно широко распространены в корпоративных информационных системах и компьютерных сетях. Оценки показывают, что рынок инструментальных средств СОВ достиг в 1998 100 миллионов долларов США. Обнаружение вторжения в компьютерные сети и информационные системы уже далеко не новое направление научных исследований. К тому же достаточно хорошо освоенная коммерческая область с несколькими большими конкурентами типа Cisco и Network Associates. По общему признанию, существующие СОВ выполняют много ложных срабатываний и не обнаруживают все известные атаки на информационные ресурсы компаний. В этом отношении разработка СОВ похожа на недавние тенденции в области антивирусного программного обеспечения. Ранние версии антивирусного программного обеспечения также излишне беспокоили пользователя, каждый раз, когда он создавал новые файлы. Однако в последние несколько лет антивирусное программное обеспечение существенно усовершенствовано. Теперь пользователи практически не обращают внимание на то, что антивирусное программное обеспечение выполняется на их компьютере. При этом большинство из них уверены, что оно обнаружит все известные вирусы.

Концепция создания системы обнаружения вторжения была изначально предложена в 1980 Джеймсом Андерсоном. Однако это научное направление оставалось практически не исследованным до 1987, до тех пор пока Дороти Деннинг опубликовала модель обнаружения вторжения . В 1988 существовало уже, по крайней мере, три прототипа СОВ. В следующие годы число

прототипов постоянно возрастало. Правительства многих стран, понимая, что их компьютерные системы недостаточно защищены, выделили финансирование для исследований в области создания СОВ. Сотни миллионов долларов были потрачены на исследование СОВ за последние десять лет.

В силу того, что обнаружение вторжения стало зрелой технологией и областью промышленных интересов, почти все простейшие проблемы были успешно решены. В последнее время в этой области исследований не было найдено существенных прорывных решений. Вместо этого, разработчики систем подобного рода главным образом совершенствуют существующие методы обнаружения вторжения. В связи с этим, традиционные направления исследования в этой области будут иметь все меньшее значение. Поэтому, будущее исследования обнаружения вторжения, как ожидается, сосредоточатся на относительно неисследованных областях типа:

- механизмы ответа на нападение;
- архитектуры сильно распределенных систем обнаружения вторжения;
- стандарты взаимодействия компонентов системы при обнаружении вторжения;
- новые парадигмы обнаружения вторжения.

2. Технология мобильных агентов

Системы обнаружения вторжения на основе мобильных агентов - одна из новых парадигм создания систем данного класса. Мобильные агенты - специфический тип программного агента, который имеет возможность перемещаться от одного сервера (хоста) до другого. Согласно программный агент может быть определен следующим образом:

« … программный объект, который функционирует непрерывно и автономно в специфической среде … способный выполнять действия гибким и интеллектуальным способом, в ответ на изменения среды … Идеально, если агент, функционирующий непрерывно, …был бы способен учиться на опыте. Кроме того, существуют агенты, которые взаимодействуют с другими агентами и процессами, при этом они способны общаться и сотрудничать с ними, а при необходимости - перемещаться с места на место».

Мобильные агенты были одной из передовых тем исследований в области информационных технологий в течение нескольких последних лет. Однако результаты этих исследований, главным образом, остались в пределах лабораторий и не были достаточно широко внедрены. Вместе с тем, интенсификация работ по созданию Web-приложений имела ключевое значение для взрывного роста заинтересованности к области исследований свойств мобильных агентов, что связано с возможностью создания на их основе распределенных приложений для работы в Интернет. Стала широко применяться процедура запуска на выполнение мобильных агентов через Web-

браузеры для сбора информации и взаимодействия с любым узлом в сети (технология ноуботов). Фирмы IBM и General Magic являются инициаторами этого направления интерактивных систем. Параллельно этим работам в 1994 году Агентство перспективных исследований и разработок Министерства обороны США (ARPA) поддержало программу «Распределение знаний» (Knowledge Sharing). В результате реализации этой программы был разработан язык KQML, который до настоящего времени остается одним из наиболее жизнеспособных языков взаимодействия агентов (Agent Communication Languages, ACLS).

Область исследования мобильных агентов была переформулирована в период 1995-1996 годов, когда Sun Microsystems был выпущен язык программирования Java. Хотя Java - просто новый интерпретируемый машинный язык, он предназначается для организации взаимодействия сетевых приложений и предоставления технологии мобильного, платформнонезависимого кода.

Язык Java обеспечил некоторую независимость системы, в язык были включены конструкции, позволяющие обеспечить приемлемый уровень безопасности. Это не были уникальные механизмы защиты, просто в Java они были реализованы несколько лучше, чем в других языках. В силу этого и ряда других причин язык Java стал весьма популярным. В течение того же периода, были представлены многочисленные предложения по использованию мобильных агентов. Например, система Lava, разработанная в Государственном университете штата Северная Каролина (США). Разработчики этой системы сосредоточились на решении проблема защиты информации, поэтому в системе была реализована простая, но эффективная политика защиты для апплетов Java. Mitre Corporation также проводившая работы в этой области, разработала механизмы аутентификации и определяя таксономии событий в области защиты информации, на базе Java.

Важное наблюдение на основе анализа большинства работ в области мобильного кода в ранний период ее развития, сделанное многими исследователями, касается полной открытости подобных систем. То есть практически все возможные проблемы защиты в полной мере реализовались в системе с полностью открытой архитектурой, что привело к возникновению максимально возможного числа угроз. На основе этого наблюдения некоторые исследователи сделали заключение о том, что использование парадигмы мобильных агентов не является целесообразной там, где всегда имелись угрозы безопасности, которым невозможно противостоять при полностью открытой системе.

Частично из-за этих выводов, частично в силу хорошо разрекламированных нападений хакеров на ряд ранних Java-систем, нерешенные проблемы обеспечения защиты информации препятствовали широкому распространению технологии мобильных агентов. Архитектура

обеспечения защиты информации в этой технологии была определена, но она все еще содержала слишком много риска для большинства приложений.

В одной из последних работ университета г.Тулуза (Франция), например, предлагается использовать мобильные агенты для целей добывания данных (data mining). Такое приложение требует наличие диспетчеров доступа к информации, чтобы сохранить системы открытыми для множества пользователей, большинству из которых источник данных не известен.

Однако относительно немного выполненных работ основываются на использовании архитектуры мобильных агентов для решения задач обеспечения защиты информации, например - для обнаружения вторжения в компьютерные сети. Если структура мобильных агентов предназначена для определенной цели типа администрирования системы или технического обслуживания функции защиты, то оправдано усиление процедур аутентификации, что ведет к снижению остаточного риска.

В то время как мобильные агенты - необычно мощный инструмент, их использованию препятствовали соображения безопасности. Эти соображения особенно чувствительны для систем обнаружения вторжения, так что в итоге большинство исследователей в этой области сконцентрировались на создании структуры, необходимой для обеспечения защиты мобильных агентов.

3. Основные работы

Наиболее интенсивные работы по исследованию свойств мобильных агентов для создания систем обнаружения вторжения на основе мобильных агентов (СОВМА) в компьютерные сети проводятся в настоящее время в нескольких лабораториях США и Японии (университет штата Айдахо, университет штата Нью-Мексика, Армейской научно-исследовательской лабораторией Министерства обороны, Государственный университет штата Айова и Агентство содействия информационной технологии в Японии). Существуют и другие работы в этой области, однако, в большинстве случаев эти исследования испытывают недостаток информации в области мобильных агентов и безопасности информации, необходимой для успешной интеграции этих двух областей исследований. Во многих случаях, такие проекты находятся в предварительной стадии, они непосредственно не решают задачи обнаружения вторжения в компьютерные сети или не используют свойство подвижности агентов.

3.1. Самонастраивающиеся агенты для обнаружения вторжения

Самонастраивающиеся агенты для обнаружения вторжения (САОВ) используются в традиционной системе обнаружения вторжений на основе агентов главным образом как средство для преобразования множества компонентов обнаружения вторжения в совокупность простых программных компонентов, которые могут быть легко реконфигурированы. САОВ используют иерархию агентов. В корне иерархии - мониторы, которые

обеспечивают глобальный контроль и управление. Они же выполняют анализ информации, поступающей от узлов более низких уровней. В листьях иерархии - агенты, которые собирают информацию о событиях. Агенты постоянно находятся во взаимосвязи со специальными базовыми агентами, именуемыми «приемопередатчиками». Приемопередатчики выполняют роль локальных мониторов по контролю и управлению агентами, а также для анализа и обработки потока информации, полученной от этих агентов, с целью его сокращения для передачи агентам-мониторам более высокого уровня. Агенты статические и вводятся в систему путем загрузки с приемопередатчика, однако они могут быть заменены в процессе реконфигурации.

3.2. Hummingbird

В университете штата Айдахо разработан проект Hummingbird. Это - один из наиболее амбициозных проектов распределенной системы обнаружения вторжения из доступных в настоящее время.

Система Hummingbird - это распределенная система для сбора и управления данными о неправильном использовании компьютерных систем. Хотя система использует некоторую агентную технологию, однако, в ней агенты не адаптивные и не мобильные. Распределен только сбор данных, а контроль и управление остается централизованным. Акцент сделан на защищенном распределении данных среди серверов (хостов) сети, имеющих различные уровни защиты. Предполагаются также и инструментальные средства, алгоритмы, методы сжатия данных и технология визуализации информации в системах мобильных агентов.

В Hummingbird не предлагается принципиально новых механизмов защиты, чтобы защитить собственную структуру. Вместо этого в проекте используется система Kerberos.

3.3. Агенты Java для метообучения

В проекте «Агенты Java для метообучения» (JAM) Колумбийского университета (штат Нью-Йорк) метод метообучения применяется для извлечения распределенных данных посредством применения интеллектуальных агентов. Интеллектуальные агенты используют методы искусственного интеллекта для моделирования знаний и рассуждений, также как и поведения в многоагентных сообществах. Проект имеет два ключевых компонента: локальные агенты обнаружения несанкционированных действий, которые изучают, как обнаружить действия такого рода и обеспечить услуги обнаружения вторжения в пределах отдельной информационной системы; и защищенной, интегрированной системы метообучения которая объединяет коллективные знания, приобретенные индивидуальными локальными агентами. Извлечение данных, подобно нейронным сетям и другим приложениям, обучающимся централизованно, не допускает совместного использования знания агентами. Подход на основе метообучения пытается преодолеть это ограничение, интегрируя множество отдельно обученных классификаторов, реализованных как отдаленные агенты.

3.4. Интеллектуальные агенты для обнаружения вторжения

Этот проект, реализуемый в Государственном университете штата Айова, предлагает систему обнаружения вторжений, основанную на технологии интеллектуальных агентов, подобной использованной в проекте JAM. Подвижность агентов позволяет различным типам интеллектуальных агентов (называемых в проекте «уборщики данных»), которые используют алгоритмы классификатора, передвигаться среди точек сбора информации и раскрывать подозрительные действия. Алгоритм агента - стандартные алгоритмы идентификации последовательностей. Структура иерархическая с информационным хранилищем в корне, уборщиками данных в листьях и агентами-классификаторами между ними. Агент-классификатор специализируется на определенной категории вторжения и способен к сотрудничеству с агентами другой категории, чтобы решить, насколько серьезен уровень подозрительных действий. При перемещении вычислительного алгоритма (то есть, агента-классификатора) к каждой точке сбора данных, позволяет избежать дорогостоящего перемещения информации к обобщающему модулю. Результаты работы обеспечивают хороший базис для последующих исследований, так как подход дает возможность определить агентов обнаружения вторжения для индивидуальной системы и подсистемы.

3.5. Программа исследования перспективных телекоммуникаций и распределения информации

Работа, выполняемая вооруженными силами США по программе перспективных телекоммуникаций и распределения информации (the Advanced Telecommunications/Information distribution Research Program, ATIRP), адресована не обнаружению вторжения, а выявлению уязвимых мест в компьютерных систем с использованием мобильных агентов. Однако модули оценки уязвимости могут быть легко заменены модулями обнаружения вторжения, что позволяет создать простую систему обнаружения вторжения. Центральный диспетчер запускает агентов к одному или нескольким целевым узлам, чтобы проверить на известные уязвимости и сообщить обратно результаты проверки. Агенты составляются динамически с использованием генетического алгоритма, который непрерывно пытается максимизировать вероятность обнаружения существующих уязвимостей. Генетический пул, от которого агенты развиваются, состоит из кодовых фрагментов, которые соответствуют методике обнаружения и разработаны таким образом, что способны взаимодействовать с другими фрагментами. Структура имеет определенные возможности защиты, основанные на криптогафических сигнатурах и электронных сертификатах. Идентичные или подобные возможности требуются и для системы обнаружения вторжений. Исходная система должна была бы быть расширена, чтобы управлять системой обнаружения вторжений, так как связь между агентами более чувствительна в обнаружении вторжения, чем при сканировании уязвимостей.

3.6. Система обнаружения вторжения на основе агентов

Агентство содействия информационным технологиям (Information-technology Promotion Agency, IPA) Японии, разрабатывает систему обнаружения вторжений, названную "Система обнаружения вторжения на основе агентов" (Intrusion Detection Agent system, IDA). Система IDA относится к категории многохостовых систем обнаружения вторжений. Вместо анализа действий всех пользователей, IDA наблюдает за определенными событиями, которые могут касаться вторжений, и обозначаемых в системе как "метки, оставленные подозреваемым злоумышленником" (Marks Left by Suspected Intruder, MLSI). Если MLSI найдена, то IDA собирает дополнительную информацию, связанную с этой MLSI, анализирует ее и решает: произошло или нет вторжение.

Система IDA основывается на использовании мобильных агентов, для определения злоумышленников среди множества серверов (хостов), вовлеченных в операцию вторжения и сбора информации. Структура системы иерархическая с центральным менеджером в корне и множеством различных агентов в листьях. Датчиком является агент, который постоянно находится в узле с целью поиска MLSIS. О факте обнаружения такой информации датчик уведомляет менеджера, который посылает агента-инспектора на инспектируемый главный компьютер. Агент-инспектор инициализирует собирающего информацию агента, чтобы собрать дополнительную информацию, связанную с инспектируемым сервером, перед перемещением на любой другой узел сети, идентифицированный как подозреваемый. Менеджер собирает и интегрирует результаты от собирающего информацию агента, которую они направляют. Возможное дублирование, связанное с тем, что несколько датчиков обнаруживают одно и то же событие вторжения, в системе решено через "доску объявлений" в каждом проверенном главном компьютере.

4. Требования к системе обнаружения вторжений

В доступной печати существуют сведения, по крайней мере, об одном из ранее выполненных исследований, в котором определяются характеристики для проектируемой системы обнаружения вторжений. Независимо от механизмов, на которых основана система обнаружения вторжений, она должна делать следующее:

- работать непрерывно без вмешательства человека;
- быть устойчивой к сбоям и живучей;
- противостоять попыткам разрушения системы;
- иметь минимальную избыточность;
- учитывать возможные отклонения от нормального поведения;
- быть легко адаптируемой к определенной сети,

- адаптироваться к изменениям собственной структуры при последующем совершенствовании системы;
- быть устойчивой к дезинформации.

На основе анализа опубликованных результатов исследований, а также исходя из существующих потребностей обеспечения защиты информации в информационных системах, далее представлен набор требований к проектируемой системе обнаружения вторжений по двум направлениям: функциональные требования и требования функционирования.

4.1. Функциональные требования

Так как сложность сетевого пространства непрерывно возрастает, то это должно отразиться на разработке функциональных требований к системе обнаружения вторжения. Общие функциональные требования к системе обнаружения вторжений, предназначенной для оснащения вычислительных систем, которые разворачиваются в настоящее время или будут развернуты в ближайшем будущем (см. Приложение 1) включают следующее:

- СОВ должна непрерывно контролировать ситуацию и сообщать о вторжениях;
- СОВ должна обладать достаточным количеством информации, чтобы восстановить систему, определить степень повреждения и установить ответственность за вторжение;
- СОВ должна быть модульной и с перестраиваемой архитектурой, поскольку каждый сервер и сетевой сегмент будет требовать уникальных тестов на вторжения и эти тесты должны быть модернизируемыми, и, при необходимости, подлежащими замене новыми, более совершенными тестами;
- так как СОВ назначена критическая роль контроля состояния защиты сети, сама СОВ является первичной целью нападения. СОВ должна работать во враждебной вычислительной среде и показывать высокую степень отказоустойчивости, а также учитывать значительную деградацию собственной структуры и функций;
- СОВ должна быть адаптируемой к топологии сети и изменениям конфигурации, поскольку вычислительные элементы динамически добавляются и удаляются из сети;
- системы обнаружения аномалий (как составная часть СОВ) должны иметь очень низкий процент ложных срабатываний. Учитывая прогнозируемое увеличение в сетевой связности и трафике, простое уменьшение процента числа сигналов ложной тревоги от общего числа срабатываний не может быть достаточным, поскольку абсолютное количество сигналов ложной тревоги может продолжать повышаться;

- СОВ должна обучаться на опыте и улучшать возможности обнаружения спустя некоторое время после начала функционирования. Самонастраивающаяся СОВ должна обучаться распознаванию сигналов ложной тревоги сначала при помощи администратора системы, а в дальнейшем и самостоятельно;
- СОВ должна быть легко модифицируемой при частом обновлении сигнатур классификации несанкционированных действий, как только появляются новые положения защиты и исправления в системе защиты, а также в случае обнаружения новых каналов уязвимости информационной системы и появлении новых путей нападения;
- необходимы базовые инструментальные средства для помощи администраторам системы в подготовке ответа на различные нападения. От СОВ будет требоваться не только обнаружить аномальные события, но также и проводить автоматизированные ответные мероприятия;
- СОВ должна проводить интеграцию данных и обрабатывать информацию от множества распределенных источников данных типа межсетевых экранов, маршрутизаторов и коммутаторов. Поскольку требование обнаружения в реальном масштабе времени заставляет в качестве основных решений выбирать перепрограммируемые аппаратные устройства, которые могут загружать новое программное обеспечение в процессе функционирования, СОВ должна быть способной связаться с такими аппаратными устройствами;
- в составе СОВ будут необходимы инструментальные средства сжатия данных для обработки собранной информации. Инструментальные средства извлечения данных будут полезны при реализации методов обнаружения аномалий при статистической обработке собранных данных;
- СОВ должна быть приспособлена к обеспечению автоматизированного ответа на подозрительную деятельность. Быстрые изменения в состоянии сетей и ограниченное время, выделяемое на администрирование сети, делают трудным для администраторов системы процесс диагностирования проблемы и выработки ответных действий с целью минимизировать ущерб, который может быть нанесен злоумышленником;
- наличие способности обнаруживать и реагировать на распределенные и скоординированные по цели, месту и времени нападения станет жизненно необходимой. В скоординированных нападениях против сети будут вовлекаться большие силы, что позволит злоумышленникам реализовывать намного больше число различных нападений против единственной цели. Эти атаки могут

быть комбинацией известных типов атак, быстро развиваться и потребуют незначительных затрат от нападающих;

- распределение вычислительных и диагностических возможностей между агентами, распределенных по сети, добавляет уровень отказоустойчивости системы, но это затрудняет администрирование системы, которое значительно проще, если имеется контроль над СОВ из единого центра управления;
- СОВ должна быть приспособлена к работе с другими коммерческими инструментальными средствами защиты, поскольку никакой комплект инструментальных средств, вероятно, не обеспечивает полную зону обнаружения, диагностирования и ответа на действия злоумышленника. Структура СОВ должна быть способна интегрировать различные средства архивирования данных, основанные на разной аппаратной платформе и сетевых решениях инструментальные средства защиты. Способность к взаимодействию и соответствие стандартам увеличит ценность перспективных СОВ.
- собранные СОВ данные требуют дополнительного анализа для оценки любого нанесенного сети ущерба после того, как вторжение было обнаружено. Несмотря на то, что аномальный случай был обнаружен, это может быть не первая попытка получить неправомочный доступ к сети. Подробный анализ случая необходим, чтобы идентифицировать скомпрометированные машины в сети прежде, чем сеть будет восстановлена в исходное состояние;
- СОВ должна также разрабатываться с учетом мер собственной безопасности. Например, СОВ должна подтвердить подлинность администратора, контролировать действия администратора, взаимно подтверждать подлинность устройств СОВ, защищать собственные данные СОВ и не создавать дополнительные угрозы.

4.2. Требования к функционированию

СОВ, которая является функционально правильной, но обнаруживает нападения слишком медленно, имеет небольшие шансы на использование. Таким образом, необходимы несколько требований к функционированию СОВ.

Подобные требования к СОВ включают:

- аномальные события или нарушения в защите должны быть обнаружены по возможности в реальном масштабе времени и сообщены немедленно, чтобы минимизировать нанесенный ущерб и потерю или искажение важной информации.
- СОВ не должна излишне тяготить пользователей или мешать нормальным действиям, для защиты которых система и была развернута. Это требование делает необходимым агентам быть осведомленным о потреблении сетевых ресурсов, которые они

контролируют. Должно быть установлено соотношение между введением дополнительного уровня защиты и уровнем штрафа за его введение, который будет оплачен другими приложениями.

- СОВ должна быть масштабируемой. Поскольку новые ЭВМ будут добавляться к сети, СОВ должна быть способна обработать дополнительные вычислительные ресурсы и загрузку линий связи.
-

5. Мобильные агенты для обнаружения вторжения

Для того чтобы мобильные агенты были полезными для обнаружения вторжения необходимо, чтобы многие, если не все, главные компьютеры (серверы) и сетевые устройства были оснащены базовой системой мобильных агентов (БСМА). Это - не излишнее и необоснованное требование, потому что базовая система мобильных агентов есть программное обеспечение общего назначения, которое дает возможность осуществить не только реализацию СОВ, но и много других услуг. Если такие услуги станут популярными, каждый новый сервер и рабочая станция может поставляться с предустановленной базовой системой мобильных агентов, также как сегодня большинство персональных компьютеров имеют интерпретатор Java в составе браузера Интернет.

Альтернативой этому может являться схема построения СОВ, в которой предполагается, что базовый комплект СОВ установлен на каждом сервере. Слишком дорого установить частное решение (подобно СОВ, основанной на базовом комплекте) на каждом сервере в сети, но вполне приемлемо установить интерпретатор общего назначения (подобно БСМА и виртуальной машине Java) на каждом сервере.

5.1. Преимущества

Преимущества включают: преодоление задержек в сети, сокращение загрузки сети, выполнение асинхронно и автономно, динамическая адаптация, функционирование в гетерогенных средах, наличие устойчивого и отказоустойчивого поведения.

5.2. Преодоление задержки в сети

Мобильные агенты полезны для приложений, которые должны реагировать в реальном времени на изменения в среде, в силу того, что они могут быть отправлены из центрального контроллера для выполнения действий непосредственно в отдаленной точке сети, представляющей интерес. В дополнение к обнаружению и диагностированию потенциальных сетевых вторжений, СОВ должна обеспечить соответствующий ответ, чтобы защититься и защитить сеть от злонамеренного поведения. В то время как центральный контроллер должен посылать сообщения узлам сети, а также выполнять набор команд по ответу на специфическое состояние или воспринятую угрозу, то реализация такого подхода весьма затруднителен.

Например, центральному контроллеру, вероятно, придется ответить на множество событий повсюду в сети в дополнение к нормальной загрузке и стать критическим узлом или причиной отказа. Если линии связи с этим центральным сервером медленны или ненадежны, то взаимодействие, восприимчивое к недопустимым задержкам, может прекратиться вовсе. Мобильные агенты, так как они распределены повсюду в сети, могут воспользоваться преимуществом обходных направлений вокруг любых перегруженных связей.

Будет всегда быстрее послать сообщение сетевому узлу, чтобы дать команду на выполнение заранее загруженного на нем кода, чем посылать мобильного агента к узлу. Однако, такая структура требует, чтобы весь ответ и действия по реконфигурации были предопределены, клонированы и распределены повсюду в сети. Механизм ответа тогда составляет, в действительности, большую распределенную базу данных, поднимая серьезные проблемы администрирования и управления конфигурацией. Новые приемы ответных мер, по определению, должны быть переданы, по крайней мере, однажды к каждому взаимодействующему узлу при помощи стандартных сетевых средств, последовательности сообщений или мобильным агентом. Из этих вариантов, методика с использованием мобильных агентов предлагает самый быстрый ответ.

5.3. Сокращение загрузки сети

Одна из наиболее неотложных проблем стоящих перед проектируемыми СОВ - обработка огромного объема данных, сгенерированных инструментальными средствами, контролирующими сетевой трафик, и контрольные файлы регистрации событий на серверах. Обычный для СОВ метод - это обработка данных на месте. Однако часто обобщенные формы данных отправляются на другой сетевой узел, где данные далее обобщаются и затем пересылаются к центральному узлу обработки, который оценивает состояние всех узлов в сети. Даже при том, что данные обычно обобщаются, прежде чем поступить на передачу, их количество может значительно загрузить линии связи в сети. Мобильные агенты дают возможность уменьшить сетевую загрузку, устраняя потребность в такой передаче данных.

Мобильные агенты хорошо приспособлены для специального гибкого поиска решения проблем анализа при вовлечении множества распределенных ресурсов, который требует решения специализированных задач, которые не поддержаны сервером данных. Методы поиска и анализа данных, основанные на использовании мобильных агентов, могут помочь уменьшить сетевой трафик, складывающийся из передачи больших количеств данных через всю сеть для локальной обработки. Вместо передачи данных через всю сеть, мобильные агенты могут быть переданы к машине, на которой данные постоянно находятся, по существу перемещая вычисление к данным, вместо перемещения данных к вычислению, таким образом, происходит сокращение сетевой загрузки для подобного сценария. Ясно, что передача агента, который

является меньшим по размеру, чем данные, которые будут переданы, уменьшает сетевую загрузку. Эти выгоды справедливы для случая, когда сравнения сделаны между простыми мобильными агентами и относительно большими данными, которые необходимо передать.

5.4. Асинхронное выполнение и автономность

Архитектуры СОВ, которые скоординированы центральным компьютером, требуют надежных путей связи на сетевые датчики и промежуточное звено обрабатывающих узлов. Критическая роль, которую играет подобный центральный контроллер, делает его вероятной целью нападения. Архитектуры на основе мобильных агентов позволяют СОВ продолжать работу в случае отказа центрального контроллера или связи с ним. В отличие от подпрограмм передачи сообщений или дистанционного вызова процедур (Remote Procedure Call, RPC), как только мобильный агент запущен посредством домашней базовой системы, он может продолжать функционировать автономно, даже если домашняя базовая система, где он был запущен, больше не доступна или не связана с сетью. Координация датчиков СОВ и фильтров может быть защищена от потери сетевых подключений, так как мобильные агенты не требуют управления со стороны другого процесса. Неспособность мобильного агента связываться с центральным контроллером не помешала бы ему в выполнении поставленных задач.

Хотя функционирование при потере связи возможно, это не исключает того, что должно быть адресовано множество экземпляров агентов. Распределение функций центрального контроллера среди распределенных сетевых компонентов - не простая задача. Другая проблема касается методов функционирования собственно мобильных агентов.

Например, основанные на Java мобильные агенты обычно загружают свой файл классов динамически, когда это необходимо, от их домашней базовой системы. Способность динамически загружать классы поднимает вопросы защиты. Если домашняя базовая система не доступна, загрузку этих файлов классов можно обеспечивать локальным сервером или должен быть найден отдаленный доверенный сервер, с которого они могут быть загружены. Загрузка класса от удаленной базовой системы или локального ведущего базового сервера поднимает множество вопросов защиты. Файлы класса, возможно, были изменены таким образом, чтобы изменить функциональные возможности агента или даже осуществлять перехват взаимодействия агентов. Проблема доведения классов также относится к классу проблем, от которых способна избавить система, основанная на мобильных агентах.

5.5. Структура и состав

Применение мобильных агентов является естественным способом структурировать и проектировать СОВ. Например, также как монолитная статическая система, СОВ может быть разделена на поставщиков данных и компоненты анализатора данных, представленных как агенты. Поставщик данных обеспечивает интерфейс к сетям, он перехватывает или контролирует

трафик и формирует следы событий. Множественные анализаторы, каждый ответственный за обнаружение единственного нападения или маленького набора нападений, взаимодействуют с поставщиком, чтобы искать нападения. В такой структуре мобильные агенты могут использоваться множеством поставщиков для создания СОВ. Если компания имеет лучший датчик для нападения X, а другая компания имеет лучший датчик для нападения Y, то мы можем использовать мобильные агенты от обоих продавцов, чтобы обнаружить X и Y. Даже, там где фирмы-изготовители не производят программы, основанные на агентах, можно будет повторно составить программу как агент, через перенос кода или другие методы. В такой среде пользователи могут записывать настроенные агенты, чтобы обнаружить события, специфичные для их среды и слаженно работающие с другими компонентами. Хотя этот подход применяется одинаково также к СОВ, составленной из статических компонентов, ориентация на агенты и соображения подвижности обеспечивают необходимые мотивы для идентификации и расширения функциональных возможностей.

5.6. Динамическая адаптация

Вместе с изменением во времени конфигурации сети, ее топологии и характеристик трафика, должны изменяться типы тестов на обнаружение вторжений. Каждый вычислительный узел в сети будет требовать различных тестов и эти тесты должны изменяться со временем. Некоторые из них могут больше не потребоваться, в то время как новые должны быть добавлены к испытательному набору программ вместе с тем, как новые угрозы развиваются и выявляются. Мобильные агенты обеспечивают универсальную и адаптивную вычислительную парадигму, поскольку от них можно отказаться, отключить выполнение, дублировать или размещать в сети в пассивном "спящем" состоянии в соответствии с тем, как изменяются сетевые условия. Например, как только разработан более совершенный мобильный агент-датчик для обнаружения нападения, он может быть запущен в сеть, чтобы заменить более раннюю версию, либо если агент производит слишком много ложных срабатываний, он может быть отозван или работа его может быть прекращена. Мобильные агенты также имеют способность отслеживать среду выполнения и автономно реагировать на изменения. Например, если вычислительная загрузка ведущей базовой системы слишком высока, и нет возможности обеспечить работу агента, агент и необходимые данные могут переместиться на другую машину, которая может лучше обеспечить вычислительные потребности. Система на основе мобильных агентов может распределять себя среди главных компьютеров в сети таким образом, чтобы обеспечить оптимальную конфигурацию для решения специфической проблемы.

5.7. Функционирование в гетерогенных средах

Большие сети организаций обычно состоят из множества различных вычислительных систем и рабочих станций. Одна из самых существенных выгод от системы на основе мобильных агентов - способность к

взаимодействию на прикладном уровне. Взаимодействие на сетевом или транспортном уровне в виде решений, обеспеченных малым числом поставщиков, требует существенных изменений в операционной среде сервера. Взаимодействие на представительном уровне по типу модели CIDF ограничивает гибкость адаптации системы к новым типам атак. Наоборот, в то время как многоагентные структуры установлены на каждом главном компьютере, системы такого рода обладают свойством независимой настройки. Так как мобильные агенты независимы от сетевого и транспортного уровней и зависят только от их среды выполнения, они обеспечивают подход для гетерогенной интеграции на уровне систем.

Способность системы мобильных агентов работать в гетерогенных вычислительных средах стала возможной в результате размещения виртуальной машиной или интерпретатора на ведущей базовой машине. Задача сбора данных может быть облегчена при наличии мобильных агентов, размещенных на коммутаторах, маршрутизаторах и других элементах сетевой инфраструктуры. Многоагентная система может работать на любом вычислительном узле, который может быть главным компьютером базовой системы агентов. Способность систем такого рода работать в гетерогенных средах обеспечивает возможность простой интеграции сетевых и вычислительных устройств, работающих на различных базовых платформах. Способность к взаимодействию с коммерческими системами облегчена путем использование языка связи агентов (Agent Communication Languages, ASL).

Хотя многоагентная структура позволяет СОВ работать в гетерогенных средах, задачи по обнаружению признаков вторжения, решаемые мобильными агентами - главным образом аппаратнозависимы. Поэтому, если общий интерфейс программирования для функций обнаружения вторжения не доступен, агенты должны или быть ограничены единственным классом главных компьютеров, или быть предназначены для функционирования в гетерогенной среде несколькими способами (например, динамически загружаться или передавать базовому коду зависимый код).

5.8. Устойчивое и отказоустойчивое поведение

Способность мобильных агентов динамически реагировать на неблагоприятные ситуации и события облегчает возможность формирования устойчивых распределенных систем. Например, если главный компьютер отключается, все агенты, выполняющиеся на этой машине предупреждаются всякий раз, когда это возможно, и им предоставляется время, чтобы переместиться и продолжить свою работу с сохраненного состояния на другом главном компьютере в сети. Поддержка ими возможности разъединенного функционирования и распределенная природа многоагентных систем устраняет отдельные причины сбоев, и позволяют мобильным агентам приобрести отказоустойчивые характеристики.

В то время как имеются много особенностей многоагентных систем, которые дают возможность приложениям быть устойчивыми и

отказоустойчивыми, необходимо упомянуть несколько препятствий. Способность мобильных агентов двигаться от одной базовой системы до другой в гетерогенной среде была обеспечена при помощи виртуальных машин и интерпретаторов. Виртуальные машины и интерпретаторы, однако, обладают только ограниченной базой для сохранения и возобновления состояния выполнения в гетерогенных средах из-за отличающихся представлений в используемом оборудовании. Например, полное состояние выполнения объекта не может быть восстановлено в Java. Информация типа состояния счетчика команд и стека цикла - в настоящее время запрещены в программах Java. Обычные методы устранения неисправностей не достаточны для вычислительной парадигмы мобильных агентов. Например, введение контрольных точек до и после потока принятых заявок и после завершения некоторых транзакций или событий может быть необходимо, чтобы гарантировать приемлемый уровень устранения неисправностей.

С каждой процедурой введения контрольных точек и вызовов механизмов предупреждения сбоев, однако, увеличивается ресурсоемкость создаваемой системы, что, в конечном счете, может привести к переполнению доступных вычислительных и сетевых ресурсов. Даже при том, что существует арсенал методов, обеспечивающих защиту и отказоустойчивость, проектировщик должен быть внимательным в выборе механизмов, которые он собирается использовать, и как их воздействие повлияет на работу системы и ее функциональные возможности. Хотя мобильные агенты обладают большой автономностью и хорошо работают в разъединенных условиях, отказ базовой системы или других базовых систем, с которыми агенты взаимодействуют, а также требования безопасности могут серьезно уменьшать их функциональные возможности.

Даже при том, что мобильный агент может стать более отказоустойчивым, перемещаясь в другую машину, уверенность относительно надежной работы и защиты домашней базовой системы или другой базовой системы, ведет к ограничению его функциональных возможностей. Перед проектировщиками систем мобильных агентов стоят проблемы равновесия между проблемами защиты и отказоустойчивостью. Например, чтобы уменьшить риски защиты, связанные с избыточной подвижностью агентов, некоторые структуры были сформированы на централизованных клиент-серверных моделях, требующих от агентов возвратиться к центральному серверу перед переходом к другому серверу. Ясно, что снижение рисков защиты этим способом делает все мобильные агенты уязвимыми к отказу центрального сервера.

5.9. Масштабируемость

Вычислительная загрузка в централизованных СОВ увеличивается с увеличением числа узлов, добавленных к сетям, которые они контролируют. Поскольку технологии построения сетей связи продолжают улучшаться, увеличивается ширина полосы частот и сетевой трафик, что приводит к возрастанию требований на централизованные структуры. Системы

обнаружения вторжений с распределенной многоагентной архитектурой - один из нескольких способов, который позволяет распределить вычислительную нагрузку и диагностические операции во всей сети. Как только число вычислительных элементов в сети увеличится, агенты могут быть клонированы и переданы на новые машины в сети.

6. Недостатки

Очевидный недостаток использования многоагентных систем состоит в том, что они могут внести дополнительные уязвимые компоненты в сеть. Однако, это - не единственный недостаток создания систем обнаружения вторжений на основе мобильных агентов (СОВМА). Решения на основе мобильных агентов не может выполняться достаточно быстро, чтобы выполнить потребности СОВ. Кроме того, многоагентная система может содержать большие количества кода, затрудняющего быстрые перемещение между главными компьютерами. Наконец, ограниченный промышленный опыт и инструментальные средства моделирования для формулировки многоагентных решений вообще и СОВ в частности - также фактор дополнительной сложности разработки приложений на основе агентов, по сравнению с более традиционными формами.

6.1. Защита

Проблемы защиты, связанные с мобильным кодом - одно из основных препятствий широко распространенному использованию этой технологии. Вычислительная парадигма на основе мобильных агентов имеет несколько угроз безопасности, которые не решаются обычными методами защиты. В этом случае стандартные методы защиты должны быть изменены или разработаны новые методы, чтобы решить проблемы, связанные с этими угрозами.

Угрозы защиты могут быть классифицированы в четыре широких категории: "агент агенту", "агент к платформе", "платформа агенту" и "внешний источник - базовая система агента". Категория "агент агенту" представляет набор угроз, в которых враждебные агенты используют слабости защиты других агентов или предпринимают ряд несанкционированных действий против других агентов. Категория "агент к платформе" представляет набор угроз, в которых враждебные агенты используют слабости защиты или предпринимают ряд несанкционированных действий против базовой системы агента. Категория "платформа агенту" представляет набор угроз, в которых базовые системы компрометируют защиту агентов. Категория "внешний источник - базовая система агента" представляет набор угроз, в котором внешние объекты, включая агентов и базовые системы агентов, угрожают защите базовой системы агента.

Возможность СОВ инициализировать автоматизированные ответы облегчает задачу администраторов системы немедленно диагностировать подозрительную деятельность и выполнять оборонительные действия. Однако

эта новая возможность поднимает проблемы защиты на уровень контекста агентов. Многоагентная система может работать и выполнять ответы на несанкционированные действия с привилегиями администратора. Это может нанести серьезный урон защите, если СОВ - злонамеренна, и агенты помещены в систему противником. Процессы, которые работают с административными привилегиями, представляют новые угрозы и подвергают сеть дополнительным рискам. Кроме того, многие случаи, устанавливающие обновления к программам или создающие административные изменения в системе, могут иметь непредвиденный результат на существующие приложения и услуги.

Учитывая, что подобные угрозы существуют, они могут быть смягчены с использованием обычных методов защиты. Если многоагентная система обнаружения вторжений может ограничить обработку только теми агентами, которые подписаны цифровой подписью администратора защиты, это серьезно уменьшает уязвимость защиты, так как нападающий не может изменять код агента, чтобы заставить его быть злонамеренным. Однако противник способен изменить данные мобильного агента и таким образом заставить это исполнять злонамеренные действия. Существуют дополнительные методы, которые могут применяться при решении проблем защиты. Такие методы включают механизмы, управляющие доступом к вычислительным ресурсам, криптографические методы для шифрования обмена информацией, методы идентификации и аутентификации пользователей, агентов, базовых систем и механизмов защиты базовой системы агента.

Большинство ранее разработанных методов обеспечения безопасности мобильного кода главным образом развились по традиционным направлениям. Методы, предложенные для защиты базовой системы агента, включают программную изоляцию ошибки, безопасную интерпретацию кода, оценку состояния, стенограмма пути следования агента и верификация кода. Некоторые методы общего назначения для защиты агента, включающие инкапсуляцию промежуточных результатов, регистрацию маршрута, регистрация маршрута с дублированием и подтверждением, контроль выполнения, генерация открытых ключей, работа с шифрующими функциями и полиморфным кодом. Существующие системы, как правило, включают один или большее количество подобных механизмов.

6.2. Производительность

Одна из наиболее серьезных проблем, стоящих перед СОВ, это повышение скорости с которой они могут идентифицировать злонамеренную деятельность. СОВ не только должна быстро распознавать факт нападения, но также фиксировать и обрабатывать события в системы в реальном времени. Эта задача становится более трудной с увеличением полосы пропускания базовой сети. Мобильное программное обеспечение агента будет скорее препятствовать, чем помогать СОВ быстро осуществить поиск и обработать факт нападения. Мобильные агенты медленно функционируют в том случае, если СОВМА реализована на медленном интерпретируемом языке.

Решение состоит в том, чтобы использовать СОВМА для некоторых функций, но иметь основу СОВ, выполненную в статической форме. Требования к производительности настолько высоки для СОВ, что некоторые компоненты реализуются в аппаратных средствах. Может быть полезным иметь СОВМА, которая непосредственно связывается с более эффективными немобильными компонентам.

Ограничения производительности создания сценариев и интерпретируемых языков в сравнении с компилированным кодом не предлагают перспективное решение этой проблемы, поскольку преимущество гетерогенности, предлагаемого этими языками более ценно, чем повышение скорости исполнения. При учете критерия производительности, вероятно, что СОВ будут сформированы, используя комбинацию мобильных агентов, статических агентов и других технологий.

6.3. Размер кода

СОВ - сложные комплексы программного обеспечения. Агенты, которые выполняют функции в составе СОВ, могут содержать большое количество кода. Если эти агенты, как предполагается, выполняют определенные задачи на различных операционных системах, тогда в этом случае код может стать чрезвычайно большим. Размер кода агента может ограничивать функциональные возможности СОВМА, потому что будет требоваться длительное время, чтобы переместить агент между компьютерами. Кроме того, такое перемещение будет требовать большего вычислительных и сетевых ресурсов. Возможное решение этой проблемы состоит в том, чтобы иметь некоторое число статичных агентов, обладающих стандартным прикладным интерфейсом для агентов, перемещающихся между машинами. Таким образом, большинство базового кода для СОВ остается статичным, в то время как часть - мобильна.

6.4. Недостаток априорного знания

Большие сети составлены из нескольких различных базовых систем, функционирующих под управлением различных операционных систем, имеющие различные конфигурации и выполняющие различные приложения. Это достаточно сложно для мобильных агентов, которым необходимо иметь достаточно априорных знаний относительно того, как система сконфигурирована, как размещаются данные и др. Статические агенты и малое количество мобильных агентов могут лучше справляться с задачей уяснения того, как размещаются и обрабатываются данные в масштабе сети, они способны действовать как посредники между мобильными агентами и базовыми системами. Ограниченные данные могут более эффективно управляться через стандартные API.

6.5. Ограничения изученности многоагентной технологии

Клиент-серверная вычислительная парадигма к настоящему времени хорошо понята и достаточно созрела как технология, но область

распределенного управления системами мобильных агентов - все еще предмет исследования. Предполагаемое самонастраивающееся поведение агента, вовлекающее сотрудничество с другими агентами в различных узлах сети, создает динамическую среду, которая требует новых методологий проектирования и инструментальных средств моделирования, чтобы должным образом формулировать и создать системы на основе агентов. Недостаток отработанных методологий проектирования агентов и инструментальных средств моделирования делает эту задачу трудной.

6.6. Трудности программирования и внедрения

Многоагентные системы, которые установлены в информационных сетях в настоящее время, разрабатывались теми же самыми методами разработки программного обеспечения, что и немобильное программное обеспечение. Этот стандартный процесс проектирования исторически производит код с большим числом ошибок. Возможности многоагентных систем, типа перемещения и клонирования, добавляют большое количество проблем к процессу проектирования. Эти проблемы приведут к тому, что СОВМА будет более склонна к ошибкам, чем их неагентная реализация.

В настоящее время развертывание многоагентных систем сдерживается недостатком методов проектирования многоагентных систем, инструментальных средств управления и др.

7. Новшества в системах обнаружения вторжения

Системы обнаружения вторжения - недостаточно совершенны. Множество недостатков, свойственных СОВ в настоящее время, сгруппированы следующим образом:

- отсутствует универсальная методология проектирования,
- недостаток эффективности;
- недостаток мобильности в контролируемом пространстве;
- ограниченная гибкость (включает универсальность и динамическое реконфигурирование);
- ограниченная возможность обновления методов обнаружения;
- трудности с поддержкой наборов правил функционирования;
- отсутствие тестов производительности и покрытия сети;
- нет приемлемого способа проверять эффективность СОВ.

Многие продолжают решать некоторых из этих недостатков через усовершенствование существующих методов, но некоторые недостатки свойственны основам, на которых созданы СОВ. В то время как мобильные агенты могут помогать улучшать СОВ во многих областях, они не приносят никакую помощь в других. Например, способность СОВ обнаружить нападения

из конкретной точки, путем отслеживания информации от конкретного главного компьютера, конкретного приложения или конкретного сетевого интерфейса, является первичной проблемой, стоящей перед изготовителями СОВ. Мобильная технология не может расширить способность СОВ в области обнаружения единичных атак или уменьшить процент ложных срабатываний.

Кроме того, в большинстве случаев, мобильная технология замедляет работу СОВ при обработке событий, таким образом уменьшая способность обнаружения. Это - неблагоприятное ограничение для СОВ, пытающейся оценить события в реальном времени по информации из одной точки сети.

Вместе с тем, это не означает, что многоагентные системы бесполезны для СОВ. Многоагентная система может решить несколько главных проблем, стоящих перед СОВ, но что более важно - они могут обеспечивать СОВ выгодами производительности и прежде недоступными возможностями. К примеру, подвижность агентов делает их идеально подходящими для схем обнаружения, которые называются «иммунная система».

8. Полезные свойства многоагентных систем

Многоагентные системы имеют много характеристик, которые дают им возможность расширить технологию обнаружения вторжения. Подвижность - очевидно одна из наиболее важных возможностей, и мы можем получить от этого определенную выгоду. Однако, другие возможности агента также применимы для обнаружения вторжения. Агентная технология и приложения на ее основе походит на сообщество самонастраивающихся и интеллектуальных особей. Классы особей имеют специальные цели, и каждый может работать независимо от других. Каждый индивидуум общается и обмениваются информацией с другими.

Эта парадигма остро контрастирует с традиционной парадигмой программирования, где главный логический модуль управляет набором подчиненных модулей. Подчиненные модули не имеют никакой самостоятельности и исполняют только то, что диктует главный логический модуль. Разновидности традиционного подхода включают множественные модули с режимами работы набора и установкой каналов связи. Может не существовать центральный контроллер, а каждый модуль может взаимодействовать с другими модулями, чтобы исполнить задание. Если один модуль прекращает функционировать, другие модули не достаточно интеллектуальны (или не имеют полномочий) чтобы решить проблему.

Эта традиционная распределенная парадигма программирования работает хорошо, когда компоненты отчасти дублируют друг друга по функциональным возможностям. Даже при использовании избыточных компонентов, противник может отключить сравнительно малое число резервных копий функциональных блоков. Проект, основанный на этом принципе, легко осуществляется и предоставляет эффективное решение многих проблем. Агентная технология -

большой контраст этому подходу, так как она пытается дать каждому агенту понимание среды наряду с зоной полномочиями, чтобы независимо принимать решения.

Мобильные агенты по своей природе ***автономные, коллективные, самоорганизующиеся и мобильные***. Эти особенности не отражены в традиционных распределенных программах и дают возможность СОВ реализовать полностью новые подходы для обнаружения вторжения, некоторые из которого основаны ***на аналогиях, найденных в природе и в обществе***.

Представьте совокупность мобильных агентов как колонию пчел. Каждая пчела имеет способность лететь к цветам и подбирать пыльцу точно так же как мобильный агент может двигаться среди главных компьютеров и обрабатывать данные. Пчелы не имеют никакой потребности нести большие цветы домой. Точно так же агент может избегать необходимости передавать данные по факту обнаружения вторжения в центральный архив.

Другая аналогия может представить совокупность мобильных агентов, выполняющих работу в составе СОВ, как колонию муравьев. В случае гибели одного или нескольких сотен рабочих колония продолжает функционировать. Кроме того, муравьи могут двигаться далеко за пределы колонии, когда они видят убывание ноги. Многоагентная система может быть создана с подобным механизмом сопротивления нападению, так как агенты самонастраивающиеся и мобильные, а уничтожение нескольких не влияет на функционирование системы.

Многоагентная система может также рассматриваться как совокупность сторожей. Сотрудники отдела безопасности компании не хотят нести расходы на размещение караульных в каждой комнате офиса. Вместо этого, они делают обход через каждую комнату, периодически проверяя наличие признаков вторжения. Аналогично, многоагентная система дает возможность периодически проверять главные компьютеры с целью выявления проблем защиты без того, чтобы иметь необходимость устанавливать программное обеспечение проверки на каждом главном компьютере. Это исследование описывает перемещающихся агентов.

Это - только несколько примеров того, как сообщества самонастраивающихся мобильных агентов могут приносить пользу технологии обнаружения вторжения. Подвижность - важный аспект, но одно его не достаточно. Многоагентная система должна быть способной использовать автономность и работать во взаимодействии с другими агентами. Эти особенности позволяют предложить новые парадигмы обнаружения вторжения.

9. Области исследования

Из предыдущего обсуждения должно быть ясно, что мобильные агенты не дают существенно новые возможности к факту обнаружения (нераспределенных) нападений или увеличению скорости, с который одни

ведут поиск этих нападений. Имеется, однако, потенциал, чтобы применить преимущества, которыми обладают мобильные агенты, чтобы значительно улучшить путь, которым СОВ разрабатываются, создаются, разворачиваются и используются.

9.1. Многоточечное обнаружение

СОВ осуществляет многоточечное обнаружение, анализируя события в нескольких точках сети, чтобы обнаружить распределенные или организованные нападения. События могут исходить от нескольких главных компьютеров, приложений или сетевые устройств. Многоточечное обнаружение технически труднее осуществить, когда СОВ должна обрабатывать все распределенные события. Однако некоторые СОВ могут зарезервировать себе ширину полосы частот, требуемую для того, чтобы переместить (обычно массивный) файл регистрации распределенных событий к централизованному узлу для обработки. Общее решение, используемое многими поставщиками СОВ, состоит в том, чтобы выполнить фильтрацию и обобщение данных на каждом узле перед объединением событий. Однако этот в дальнейшем усложнит и без того трудную проблему обнаружения распределенных нападений, потому что в этом случае используются сокращенные данные.

Многоточечное обнаружение особенно полезно при обнаружении нападений на сеть, в противоположность нападениям отдельный главный компьютер. То есть цель скоординированного нападения может быть в получении доступа к сетевым ресурсам без обращения на специализированный сервер. Мобильные агенты могут обучаться противодействию этой стратегии нападения путем сопоставления результатов атаки на шлюзы, главные компьютеры, модемы, серверы и другие уязвимые узлы сети со стороны внешних объектов. Централизованные системы определят только то, что дискретные компоненты сети находятся под нападением, однако они не могут размышлять относительно общей стратегии атаки.

В то же время многоагентные системы могут с успехом применяться для реализации многоточечной технологии обнаружения, позволяя большое количество распределенных регистрационных данных оставлять на месте их получения. Блок анализа в мобильном агенте может двигаться среди пулов данных, чтобы исполнить многоточечное обнаружение на оригинальных файлах регистрации. Это - идеальное приложение мобильных агентов, где востребована их способность перемещать вычисления к данным, вместо перемещения данных к блоку вычисления.

Дальнейшие исследования необходимы, чтобы определить, как агент может эффективно собирать и анализировать данные, поскольку он перемещается между различными информационными источниками, для выполнения возложенной задачи по многоточечному анализу. То есть вместо информации, перемещаемой единовременно к центральному узлу обработки и

анализируемой коллективным способом, теперь требуется время на сокращение данных и перемещение кода, при этом эффективно выполняя свои функции.

9.2. Структуры, устойчивые к нападению

СОВ часто использует иерархические структуры по причинам эффективности и простоты централизованного управления (для получения дополнительной информации см. Приложение В). Рассмотрим СОВ, которая использует иерархическую структуру без возможности динамически реконфигурировать зависимости, чтобы компенсировать отказ ключевых компонентов. Обнаружение по одной точке предполагает, что обнаружение происходит в листьях (также как сбор данных для многоточечного обнаружения). Результаты, полученные промежуточными вершинами, передаются по иерархии к внутренним узлам, которые выполняют абстракцию данных (и, возможно, многоточечное обнаружение). Данные непрерывно сокращаются, пока не достигнут узла управления в корне.

Такая реализация СОВ не имеет никаких избыточных линий связи, что приводит к многим отдельным точкам отказа. Нападающий может отрезать поток управления СОВ, нападая на внутренние узлы или отстранять СОВ от выполнения своих функций, атакуя корневой узел. Даже маленькое число избыточных резервных главных компьютеров, созданных для каждого ключевого узла, не помешает хорошо осведомленному и целеустремленному противнику.

В тоже время существует несколько решений этой проблемы, в которых мобильные агенты с готовностью применяются, так как самонастраивающиеся по своей природе мобильные агенты. Взаимоувязанная многоагентная система может быть самоорганизующейся и таким образом адаптивной к нападениям. Некоторые очевидные области для исследования и экспериментирования включают:

· полностью распределенные и децентрализованные структуры СОВ, где не существуют никакие отдельные точки отказа, а существуют многочисленные избыточные информационные трассы;

· стандартная иерархическая СОВ, где мобильные агенты поддерживают каждый узел и восстанавливают любые потерянные функциональные возможности вне поля зрения нападавшего;

· СОВ на основе мобильных агентов, которые перемещаются при обнаружении любой подозрительной деятельности.

9.3. Обобщенные интерфейсы

Отдельные мобильные агенты, вряд ли, выполнят все задачи, порожденные в случае регистрации вторжения, задачи обобщения данных и задачи обнаружения нападения. Таким образом, совокупности самонастраивающихся мобильных агентов должны взаимодействовать друг с другом относительно событий и нападений. Также, мобильные агенты должны связаться со

статически расположенными традиционными генераторами событий. Эти требования связи могут стать препятствием в развивающихся многоагентных системах обнаружения вторжений.

Необходимо определить абстрактные интерфейсы для генераторов событий, произвольных событий и описаний нападения. Несколько альтернативных форм абстракции включают представление как базы информации управления, библиотеки программ или диалога агентов. Информация должна быть достаточно определенная для каждого агента, чтобы исполнить предписанное им вычисление (например, чтобы обнаружить нападение), но обычно достаточного, чтобы избежать дорогостоящих вычислений. Необходима гибкая схема, посредством которой многоагентная система может подписаться на получение определенной информации, в которой она нуждаются. Если слишком много мобильных агентов запрашивают информацию и система становится перезагруженной, необходим алгоритм обработки избыточных запросов.

9.4. Совместное использование знаний

Часто, несколько полностью независимых СОВ развернуто в информационной системе. В идеале эти СОВ должны бы совместно использовать информацию относительно недавних нападений, которая расширит их способность обнаружить будущие нападения. Это не область исследований многоагентных систем обнаружения вторжения, но мобильные агенты допускают совместное использование знаний, легко осуществляя мобильные и самонастраивающиеся компоненты. В то время как может формироваться распределенная и децентрализованная СОВ, использующая мобильные агенты, неясно, как агент может идеально совместно использовать знания относительно событий в сети. Должна быть разработана архитектура, позволяющая совместно использовать знания, для этого надо воспользоваться преимуществом адаптивности и распределенного характера систем на основе мобильных агентов.

В общем случае возможное направление исследований с использованием обмена знаниями между мобильными агентами состоит в том, чтобы попытаться преодолеть недостатки сетевой СОВ на основе мобильных агентов. СОВ на основе сети обычно располагается рядом с сетевым устройством защиты и отслеживает трафик от множества главных компьютеров. В этой ситуации, нецелесообразно для СОВ моделировать стек протокола каждого главного компьютера, который она защищает. В большинстве случаев СОВ не знает то, какие операционные системы выполняются на каждом главном компьютере. Таким образом, СОВ вынуждена фильтровать сетевые пакеты, использующие универсальный сетевой стек протокола. Нападающий может воспользоваться этим преимуществом, посылая специальные ведущие пакеты, которые интерпретируются по-разному СОВ и целевым сервером. Это делается с использованием различной фрагментации, установки порядкового номера и

флажков пакета. Нападающий в этом случае проникает через преграду, в то время как СОВ не обнаружит нападение.

Мобильные агенты могут помочь СОВ в решении этой проблемы, координируя действия между СОВ, контролирующей трафик, и целевым главным компьютером. Если сетевая СОВ способна моделировать множество стеков протоколов, то мобильные агенты могут зондировать главные компьютеры, чтобы выяснить то, какая операционная система и приложения выполняются. В другом случае агенты могут быть направлены на главные компьютеры, чтобы обнаружить нападения, которые используют различия стека протокола. Таким образом, многоагентные системы могут работать как централизованные СОВ совместно с сетевой СОВ, чтобы выявить нападающего, пробующего обмануть сетевую СОВ. Возможно, что развертывание централизованных многоагентных систем обнаружения вторжений может быть в вычислительном отношении достаточно дорогостоящим, так что эта операция может быть выполнена, когда зафиксированы несколько подозрительных образцов данных, которые сами по себе не идентифицируются как нападение.

Имеются много разновидностей, но во всех случаях многоагентная система может работать совместно со статической сетевой СОВ, чтобы предотвратить/обнаружить попытки нападавшего маскировать себя.

9.5. Роуминг агентов

Каждый агент может выполнять определенные действия по контролю трафика (подобно мобильному датчику) и беспорядочно передвигаться по сети. Когда контроль указывает на возможность вторжения, агент может запросить о дополнительном тестировании в узле. Только после того, как уровень подозрений поднимается достаточно высоко, объявляется фактически тревога. Следует обратить внимание, что нападение обнаружено только при выполнении теста, адекватного возможному нападению, а полный набор программ тестирования не должен оставаться резидентом в каждом узле.

Случайная выборка успешно использовалась много лет для контроля качества в производстве. Существенно, если случайная выборка обнаруживает проблему, то должен быть выполнен всесторонний ряд испытаний. Математика этого процесса хорошо понятна и параметры его могут быть с успехом рассчитаны. Например, возможно вычислить средний отрезок времени прежде, чем нападение будет обнаружено, среднее число систем, которые вероятно будет инфицировано, использованная ширина полосы частот и среднее время вычислений в каждом узле.

Мобильные агенты также могут иметь статистические свойства типа некоторой нормы по которой они проверяют узлы, размер их программного обеспечения, разнесение посещенных узлов и т.д. Изменение этих статистических характеристик, может непосредственно указывать на факт нападения. Так как мобильные агенты передвигаются по сети, то они не могут

постоянно находится в узле. Следовательно, узел без резидентского агента уязвим, пока соответствующий агент не прибывает в него.

Эта ситуация, однако, не столь опасна, как это сначала представляется. Очень высок уровень "ложных" сигналов о вторжении так, что возникает некая сигнальная чума в обычных СОВ. В этом случае администраторы игнорируют большинство тревог и редко обнаруживают вторжения во время их первого появления. Информация постепенно накапливается, пока администратор не делает определенное усилие, чтобы объяснить аномалию в работе системы. Поэтому вывод о том, что многоагентная структура случайной выборки будет сильно ухудшать процесс обнаружения не совсем справедлив, результаты зависят от вида нападения и критичности системы. Кроме того, такая система может достаточно хорошо работать вместе с традиционной СОВ.

Передвигающийся агент может использоваться как датчик в СОВ, которая основана на выявлении аномалий. Перемещающиеся агенты-датчики могут генерировать сигналы о событиях от узлов в сети, которые до этого были недоступны для статических датчиков аномалий. Агенты собирают статистику относительно работы сети или главных компьютеров, которые не значимы в индивидуальных узлах, но могут быть значимы при обобщении. Данные должны показать некоторую регулярность в этом случае изменения станут причиной для беспокойства. Сопоставляя события в разных участках сети, появляется возможность обнаружить новые нападения с более низкой вероятностью сигнала ложной тревоги.

9.6. Непредсказуемость

Нападающий может успешно прорваться в главный компьютер, оснащенный обычной централизованной СОВ, и не быть немедленно обнаруженным. Это могло случиться или потому, что алгоритм атаки был слишком сложным для СОВ, или потому, что СОВ только периодически сканирует главный компьютер на предмет наличия факта нападения из-за соображений производительности. В этом случае, нападающий имеет полное господство над системой, чтобы изучить и, при необходимости, изменить СОВ, проделать «люки» и удалить доказательства нападения из файла регистрации.

Решение на основе СОВМА также уязвимо к этому же виду нападения. Однако мобильные агенты дают некоторые выгоды для обнаружения такого вмешательства. Поскольку каждый новый мобильный агент достигает главного компьютера, это запускает новую серию процедур обнаружения вторжения. Некоторые из этих проверок могут дать заключение о том, что базовая система агента неизменна. Например, агент мог бы вычислять контрольную сумму статического системного файла или исполнять подобную проверку целостности на некотором блоке базовой системы и сообщать о результате к направившему его серверу, на котором законность таких изменений может быть определена. Неожиданный результат гарантировал бы действие по восстановлению системы.

Время между двумя последовательными посещениями агентами проверяемого узла, механизм их взаимодействия и точная природа их алгоритма обнаружения может быть сделано непредсказуемым. В зависимости от цели нападения, нападающий может не уничтожить базовую систему агента, поскольку это было бы подозрительно для главного компьютера к внезапному отказу от обслуживания мобильных агентов на этом узле. Вместо этого, нападающий может изменять базовую систему, чтобы селективно блокировать входящих агентов. Степень трудоемкости внесения изменений в базовую систему для селективного блокирования агентов достаточно высока, однако в случае успеха свойства агентов могут изменяться достаточно широко. Однако если существует стандартный интерфейс СОВ, усилия по изменению, могут быть столь же просты как замена соответствующей системной библиотеки. Один путь решения проблемы несанкционированных действий базовой системы состоит в том, чтобы включить базовую систему агента в ядро. Даже при том, что ядро можно вывести из строя, трудность изменения ядра намного выше уровня сложности отключения СОВ. Существуют и аппаратные решения для предотвращения вмешательства к ведущим базовым системам, но они достаточно дороги для широкого использования.

Области для исследования расположены главным образом вокруг применения непредсказуемости как дополнение для других механизмы. Непредсказуемость обычно используется не для борьбы с нападением типа «отказ в обслуживании» или другим малым по длительности, это свойство, прежде всего, для предотвращения тех нападений, которые пытаются использовать пораженный компьютер как основу для дальнейшего выполнения операции и скрытого ухода с уничтожением доказательств. Цель состоит в том, чтобы увеличить вероятность того, что подобное успешное нападение не уклониться от обнаружения.

9.7. Генетическое разнообразие

СОВ созданная на основе мобильных агентов, может рассматриваться как совокупность самонастраивающихся объектов. Однако обычно каждый агент не уникален в смысле наличия отличного набора команд, которые он выполняет. Обычно, создаются классы агентов, и члены одного класса будут иметь различные данные, но те же самые команды. Например, один класс агентов может работать в сети и пытаться обнаружить специфическую уязвимость.

Проблема для стандартных СОВ состоит в том, что испытания, которые выполняются такой системой, являются предсказуемыми. В случае со стандартной СОВ, нападающий может приобрести копию СОВ и выяснять точную сигнатуру, которая используется для обнаружения нападения. Это даст нападающему преимущество при проникновении через сеть.

Что, если агенты, которые обнаруживают однотипное нападение, будут иметь каждый слегка различную сигнатуру обнаружения. Нападавший тогда не смог бы предсказывать точно, какой алгоритм обнаружения собирается использоваться, для обнаружения его нападения. Проблема в том, что,

используя различные сигнатуры обнаружения, каждый агент будет иметь различную вероятность обнаружения и ложного срабатывания. Приходится использовать неоптимальные сигнатуры. Однако эти нормы могут быть привязаны к разумному диапазону, и в этом случае можно воспользоваться преимуществом использования мобильных агентов, когда часть агентов распознает ту же атаку, но несколько по-другому.

Один способ, состоящий в обучении агентов различным способам обнаружения нападения, состоят в том, чтобы дать агенту базовые знания относительно нападения и заставить их автоматически выработать их собственную методику для обнаружения этого вида атаки. На некотором человекоподобном языке проводится описание характеристик атаки. Затем создаются агенты, которые могут читать подобный язык описания событий. Используя разнообразие приемов машинного обучения, агенты могут использовать различные аспекты нападения и формулировать собственную сигнатуру нападения.

Если разместить этих агентов в изолированную сеть и запустить алгоритм атаки то, через контур обратной связи, агенты могут вычислять вероятности их обнаружения или ложной тревоги. Агенты с низкой вероятностью обнаружения могут проводить небольшие модификации к их сгенерированной случайным образом сигнатуре нападения в попытке улучшить вероятность обнаружения.

В результате будет получен большой набор агентов, каждый из которых ведет поиск нападения с различной сигнатурой. Лучшие агенты могут быть развернуты в сети. Таким образом, многоагентная система может автоматически изучать сигнатуры нападения и изучать различные сигнатуры возможных ответов. Это не даст возможность нападающему предсказать точные используемые сигнатуры и таким образом расширит возможности распределенной СОВ.

10. Новые подходы к организации ответа на вторжение

В соответствии с их названием, СОВ традиционно сосредотачиваются на обнаружении нападений. В то время как обнаружение является полезной целью, человечку свойственно анализировать сообщения от СОВ в течение некоторого времени. Это дает нападающему некоторое время, чтобы свободно работать прежде, чем начнется противостояние с администратором системы. В это время, нападающий может захватывать критические данные, устанавливать невидимые люки, использовать захваченный главный компьютер, чтобы напасть на другие узлы сети или скрытно разрушать информацию. В идеале, нападающему нельзя дать время, чтобы продлить его присутствие в сети. В силу этого, многие СОВ начинают оснащаться автоматизированными возможностями ответа на нападение.

СОВ обнаруживает нападение и немедленно отвечает, чтобы выдворить нападающего из сети. Это звучит просто, но практически очень трудно

выполнить. Для безопасности целевого процесса функционирования информационной системы (чтобы не помогать нарушителю), СОВ инициализирует только очень слабые ответы. Ниже представлены пути, которыми многоагентная система может помочь решить эту проблему, однако, сначала исследуем существующие автоматизированные механизмы ответа и вызовы, стоящие перед ними.

10.1. Существующие механизмы ответа

Существующие механизмы ответа в существующих СОВ достаточно слабы, когда проводится сопоставление с целью автоматического изгнания нападающего из сети. Автоматизированные механизмы ответа, существующие в настоящее время, относятся к двум категориям: расширенное уведомление и фильтрация нападающего. Расширенные механизмы уведомления предназначены, для того чтобы сообщить администраторам систем относительно серьезных нападений как можно скорее. Они направлены на уменьшение времени, доступного нападающему, прежде чем в дел вступит человечек-администратор. В случае серьезного нападения, СОВ направляет e-mail сообщение администратору системы, высветятся сообщения уведомления на их мониторах или их Web-странице. Фильтрующее нападение методы активно останавливают нападающего. Одна популярная методика может прервать подключение через TCP между нападающим и целью. СОВ делает это, отслеживая злонамеренное подключение, чтобы определить порядковые номера пакетов и затем, вставляя пакеты сброса, чтобы уничтожить подключение. Другая методика, фильтрующая нападение, состоит в том, чтобы динамически изменить таблицу разрешений маршрутизации в маршрутизаторах и сетевых устройствах защиты. Обычно, СОВ отвергает пакеты от IP-адреса нападающего или подсети от пересекающего маршрутизаторы сети или сетевого устройства защиты. Цель может также быть отключена, используя эту методику, чтобы предотвратить доступ нападающего до целевого главного компьютера. При использовании этого метода, СОВ пытается прерывать доступ нападающего к цели и остановить его попытки посылки злонамеренных пакетов в сеть.

В то время как СОВ подает большие надежды в области автоматизированных ответов, текущие функциональные возможности не достаточны. Существующие механизмы ответа слишком слабы, чтобы остановить искушенных противников. Существующие в настоящее время механизмы ответа не достаточны потому, что они предполагают, что нападение требует времени, чтобы начать его и, что нападающие ограничены использованием единственного IP-адреса или подсети. Однако современные компьютерные нападения обычно начинаются с использованием автоматизированных программ нападения. Эти программы врываются в компьютеры очень быстро с использованием только нескольких пакетов и могут проникать через главный компьютер прежде, чем СОВ обнаруживает и ответит на нападение. Программа нападения может быстро установить люк. Тогда нападающий приближается к скомпрометированной машине от нового

IP-адреса, использует люк, и СОВ не обнаруживает очевидный нормальный вход в главный компьютер.

Другая проблема происходит, когда нападавший запускает нападения отказа в обслуживании. В этом случае каждый пакет может быть направлен с различным IP-адресом, таким образом делающих фильтрацию пакетов нападения невозможной.

10.2. Идеальные механизмы ответа

Предположим, что нападающий проник через сеть и скомпрометировал некоторые главные компьютеры. Алгоритм идеального ответа собирает доказательства деятельности нападающего, удаляет нападающего из сети, восстанавливает повреждения, и реконфигурирует сеть, чтобы сопротивляться данной методике проникновения нападающего. В сегодняшних условиях невозможно автоматизировать подобный идеальный ответ, так как люди будут испытывать большие трудность, выполняя это. Мы не можем автоматизировать то, что мы непосредственно не можем делать. Однако мы можем автоматизировать приближение этого идеального ответа. Такое приближение должно иметь следующие свойства, не существующие в современных средствах автоматизированного ответа:

· способность динамически изменять или отключать цель атаки. Это свойство дает возможность СОВ автоматически удалить злоумышленника из цели, защитить целевой компьютер от дальнейшего повреждения посредством отключения или выполнить расширенный аудит действий нападающего;

· способность динамически изменять или отключать главный компьютер нападения. В случае нападения изнутри сети, это дает возможность СОВ автоматически остановить порождение нападения также как записать доказательства действий нападающего;

· способность определять главный компьютер, который начинает нападение. Когда пакеты нападения перехвачены, они могут быть только прослежены по каналу Ethernet, путем опроса каждого маршрутизатора относительно источника пакетов. Как только правильный Ethernet-адрес найден, каждый из главных компьютеров в сети Ethernet должен быть проанализирован, чтобы определить, который из них является ответственным за запуск нападения. Таким образом, СОВ дает возможность проследить путь нападающего;

· способность контролировать весь сетевой трафик к/от цели. Необходимо записать для доказательства все пакеты, которые нападающий посылает цели. Кроме того, необходимо записать пакеты, исходящие от цели, так как она может быть использована в качестве промежуточной точки для проникновения в другие главные компьютеры;

· способность изменять таблицы маршрутизации и разрешения в Firewall на каждом межсетевом экране и маршрутизаторе. Часто необходимо изолировать нападающего или целевой узел, чтобы предотвратить возможный

дальнейший ущерб. Такая изоляция может ограничивать законный трафик так, что необходимо оптимально разместить фильтры таким образом, чтобы в наибольшей степени сдерживать нападающего, в то время как законный трафик должен проходить беспрепятственно.

Этот список требований, необходимых для реализации приближения к идеальному ответу подразумевает, что службы безопасности установлены на каждом ведущем и сетевом устройстве. Это не означает, однако, что каждый компонент сети должен иметь установленную СОВ, которая знает остальную часть сети. Также это не подразумевает, что службы безопасности должны быть частными решениями. Каждый сетевой компонент должен иметь установленный сервер защиты, который исполняет ограниченный набор поисковых и ответных функций.

Серверы защиты должны иметь стандартный API, который позволил бы им использоваться в распределенной схеме СОВ. Таким образом, каждое сетевое устройство обладает возможностью обнаруживать и отвечать на нападение, но никакая отдельная частная схема не должна быть установлена всюду. Эта точка зрения начала реализовываться на рынке маршрутизаторов, где можно теперь динамически изменять фильтры маршрутизации трафика от отдаленных мест.

Маловероятно, что все сетевые устройства будут скоро установлены с серверами защиты, которые могут управляться с общим API. Было бы очень трудно заставить производителей систем защиты договариваться о принятии такого стандарта, а отсутствие стандарта продвигает частные решения. Однако на ряду с этим мы думаем, что вряд ли компании будут хотеть установить частное решение защиты на каждом ведущем и сетевом устройстве. Стоимость инсталляции и технического обслуживания такой схемы была бы огромной. Поэтому, кажется маловероятно, что инфраструктура безопасности, которая необходима, чтобы приблизиться к осуществлению идеального ответа, может быть создана без мобильных агентов, при приемлемом отношении стоимости и эффективности.

10.3. Автоматизированный ответ на основе мобильных агентов

Технология мобильных агентов может решить проблему установки и поддержки инфраструктуры безопасности, необходимой для осуществления идеального ответа. При использовании многоагентных систем, нет необходимости устанавливать сервер защиты на каждом устройстве, поскольку мобильные агенты могут автоматически путешествовать в сети и устанавливать соответствующее программное обеспечение на соответствующих типах сетевых устройств. Этот путь не ограничивает компании в использовании единственного частного решения, так как деинсталляция одного решения и установка другого может быть почти автоматическая. Мобильные агенты могут обеспечивать серверы безопасности, которые требуются в каждом сетевом устройстве, а также осуществлять функции распределенной СОВ, которая обнаруживает нападения и выполняет ответные мероприятия. Мобильные агенты расширяют способность системы автоматически ответить, потому что

агенты дают возможность рассматривать все сетевые элементы как компоненты той же самой схемы защиты. Ответы могут быть инициализированы в любом месте в сети, что дает возможность системе оптимизировать местоположения, в которых они инициализируют ответы. Кроме того, мобильные агенты расширяют способность СОВ проследить нападавшего через атакованную сеть, ответить на целевом компьютере, ответить на нападающем компьютере и собрать доказательство относительно нападения как в сети, так и на сервере.

10.4. Области исследования

Подобно многим другим областям, мобильные агенты не добавляют принципиально новых возможностей автоматизировать ответ. Однако мобильные агенты могут помочь перенести некоторые идеи автоматизированного ответа от непрактичной и дорогостоящей схемы в решения, которые могут быть осуществлены рентабельным способом. Таким образом, многие из этих областей исследований - определенно не являются областями использования мобильных агентов, но они являются областями, которые нуждаются в применении мобильных агентов, чтобы быть практически реализуемыми. Это области, которые ранее игнорировались в силу их кажущегося непрактичности.

10.5. Автоматизированное отслеживание нападающего

Мы предполагаем, что будущее СОВ будут прослеживать пути нападения в пределах сети, доступной СОВ. Эта особенность полезна по двум причинам. Во-первых, нападающий часто регистрируется в цепочке многих главных компьютеров перед нападением на цель. Таким образом, чтобы найти нападающего нужно назад всю цепочку. Во-вторых, нападающий иногда может изменить исходный адрес. Необходимо определить фактический источник пакетов, составляющих атаку, и способ сделать это состоит в том, чтобы проследить пакеты от одного сегмента сети до другого, пока исходная сеть не будет найдена. Обнаружение фактического главного компьютера, запускающего пакеты требует посещения главных компьютеров в пределах сегмента сети, так как нападающие могут скрывать MAC адреса также как IP-адреса. Много нападений происходят снаружи сети и, таким образом, не могли бы быть прослежены. Однако нападения внутреннего нарушителя являются причиной большего беспокойства, чем нападение от постороннего. СОВ должна определить находится ли злоумышленник внутри или вне сети, и точно определить местоположение нападающего настолько это возможно.

Эффективное отслеживание нападающего от одного сегмента сети до другого требует способности перехватывать трафик в каждом сегменте Ethernet в сети. Обнаружение главного компьютера в сегменте Ethernet, требует анализа каждого главного компьютера в этом сегменте Ethernet. Таким образом, чтобы соответственно проследить нападающего через сеть СОВ нуждается в возможности перехватывать трафик на каждом сегменте Ethernet и анализировать каждый главный компьютер. Обычная инфраструктура, требуемая для реализации этого вида анализа, была бы предельно дорога.

Однако мобильные агенты обеспечивают очень дешевый способ делать это при условии, что базовые системы агентов установлены повсеместно в сети. Имеются несколько устройств, которые система анализа должна адресовать. Если нападающий скомпрометировал главный компьютер, то базовая система агентов не может функционировать.

Таким образом, любая система анализа должна собрать данные из многих мест и сравнить результаты. Кроме того, не все главные компьютеры могут поддерживать мобильные агенты, в этом случае система должна будет понять топологию сети и перехватывать трафик в оптимальных местах, чтобы найти след нападающего.

Наконец, нападающий может посылать полностью различные данные по каждой связи в его цепочке нападений. Например, нападающий мог бы использовать шифрование связи. В этом сценарии, чтобы проследить нападавшего система должна применить сложные методы искусственного интеллекта для принятия решений.

При предположении существования базовых систем агентов, система отслеживания может автоматически развертываться через всю сеть с очень небольшим временем сборки. Основная проблема исследования при формировании этих систем состоит в том, чтобы выявить умного противника.

Автоматизированная система поиска нападающего должна обладать следующими свойствами:

- собирать доказательства следа нападающего с использованием методов искусственного интеллекта;
- работать адаптивно, когда некоторые главные компьютеры не участвуют в схеме поиска (например, не имеющие базовую систему агентов);
- иметь способность искать несколько путей одновременно и в то же время не переполнять сеть агентами.

10.6. Автоматизированный сбор доказательств

В настоящее время, нет практики автоматического сбора доказательств о нападении из многих различных источников. Проблема состоит в том, чтобы определить, что правильное программное обеспечение, выполняется в нужном месте в нужное время. Многоагентные системы предлагают возможность выполнить что-нибудь, где-нибудь в любое удобное время. Поэтому реально, что доказательство может быть собрано от различных аппаратных базовых систем, различных операционных систем и даже различных приложений в сети. Очень просто, проверяя много информации о главном компьютере, переполнить доступные емкости накопителей и пропускные способности сетей связи. Таким образом, администраторы систем не могут записывать все доказательство в сети.

Мобильные агенты могут определять то, какие типы доказательства больше всего необходимы для конкретной сети, для типа исследуемого нападения и в каком месте сети. Это, вероятно, будет хорошо, если доказательство - для внутреннего использования по сравнению с законным использованием. Мобильные агенты тогда могут двигаться в соответствующие местоположения и запускать необходимые тестовые процессы (если им уже не позволяют).

Мобильные агенты, таким образом, могут разумно проверять сеть, динамически реконфигурируя контролирующие последовательности для каждого главного компьютера. Агент может строго контролировать подозрительные или важные сетевые узлы при посредственной проверке других областей. Таким образом, агент может уменьшать количество данных для доказательства, которые должны быть сохранены. Доказательства, собираемое мобильными агентами, должны быть в постоянном контакте с СОВ, которые контролируют эти подозрительными сегменты в сети. С этой совместной методикой, доказательство, собираемое агентом, будет часто способно полностью контролировать ведущий и сетевой трафик, сгенерированный нападающими.

10.7. Операции мобильных агентов на главном компьютере нападающего

В случае нападения, автоматизированные ответы обычно выполняются в сети в маршрутизаторах или сетевых устройствах защиты. Эти элементы обычно пробуют отключить нападающего от цели. Однако, если возможно, было бы выгодно запустить автоматизированные ответы на главном компьютере нападающего. Такое контрнаступление не может преуспеть, поскольку нападающий имеет контроль над его собственным главным компьютером так, что эта методика не заменила бы маршрутизатор или сетевое устройство защиты в качестве основы ответа. Однако, ответ на главном компьютере нападающего дает СОВ намного большую власть по ограничению действий нападающего. Без мобильных агентов маловероятно, что СОВ смогла бы получить достаточно доступа к главному компьютеру нападающего, чтобы инициализировать ответы. Из-за этого, направление организации ответа нападающему на его собственном главном компьютере не исследовалось. Наличие базовых систем агентов, установленных повсюду в сети даст возможность СОВ инициализировать эти виды ответов и таким образом требует этих исследований.

Нет достаточного числа способов ответов, которые могут быть реализованы маршрутизаторами и сетевыми устройствами защиты для прекращения нападения. Ответы состоят из фильтрации некоторых видов связи или разрыва подключения. Вместе с тем, имеется большое число вариантов ответов, которые могли бы быть осуществлены на главном компьютере нападающего. Необходимо исследовать то, какие типы ответов являются наиболее полезными, какие типы ответов работают лучше всего против

нападающего, использующего специфические типы инструментальных средств нападения.

10.8. Операции мобильных агентов на целевом главном компьютере

Когда проходит нападение, очевидно, важно автоматически ответить на него на целевом главном компьютере. Такой ответ позволит не допустить использования нападающим атакованного главного компьютера, чтобы далее компрометировать сеть, а также позволит исправить повреждения, нанесенные противником.

Многое из исследований, определенных для действий агентов на главном компьютере нападающего могут быть перенесены и на эту область. Однако нападающий обычно не будет иметь таких полномочий по управлению компьютером, поскольку он находится не на собственном компьютере, а на главном компьютере нападения. Нападающий может иметь только доступ пользователя, а не администратора на главный компьютер, к тому же нападающий вероятно не разрушил многие из стандартных серверов услуг. Таким образом, если действия СОВ достаточно оперативны, целевой главный компьютер будут функционировать как правильно система, в которой нападающий присутствует как один из пользователей.

Мобильный агент может быть послан СОВ к цели, чтобы привлечь нападающего. Так как агент автоматизирован, он может часто двигаться быстрее. чем ручные действия нападающего. Однако нападающий может использовать автоматизированные инструментальные средства, которые могут действовать быстрее, чем агент. Несмотря на то, что мобильные агенты могут быть потеряны в операции за цель, СОВ все же должна послать агента в надежде на успех.

Мобильный агент должен определить, как нападающий управляет системой. Поскольку нападающий пытается получить привилегию по управлению системой, агент должен противостоять этим попыткам и пытаться удалить нападающего. В этом случае агент вероятно должен будет использовать сведения о нападении, обнаруженном СОВ, чтобы выяснить, как нападающий управляет системой.

В зависимости от типа атакованного главного компьютера, агент может просто остановить главный компьютер или может пробовать восстанавливать жизненно важные для функционирования сервисы в условиях воздействия нападающего, пока администратор системы не сможет оценивать ситуацию.

10.9. Изоляция атакующего или целевого компьютера

Действия по автоматическому ответу на целевом компьютере и компьютере нападающего могут потерпеть неудачу. Жизненно важно, чтобы не скомпрометированные машины отвечали на сетевом уровне с целью ограничить действия нападающего. Три стратегии существуют, чтобы удержать нападающего: изоляция цели, изоляция нападающего и создание набора вырезок между целью и нападающим. Факт, что мобильные агенты могут

путешествовать ко всем элементам сети, чтобы осуществить ответы – это как раз то, что дает возможность им реализовать эти стратегии.

Изоляция цели вовлекает окружающие цель компьютеры в создание барьера так, что подвергшаяся воздействию цель не может предпринять акции наступлений на остальную часть сети. Простой способ устанавливать такой барьер состоит в том, чтобы отключить весь сетевой трафик по периметру целевого компьютера. Могут исследоваться и более сложные фильтры, что позволит предоставлять «безопасные» услуги через периметр. Проблема исследования состоит в том, что барьер вероятно отключит некоторую законную связь. Необходимо брать топологию сети во внимание и окружать цель так, чтобы большинство жизненно важных связей, насколько это возможно, продолжали существовать при окружении цели. Кроме того, некоторые системы, которым мы не можем позволить быть скомпрометированными, должны быть помещены вне круга, в то время как другие системы, которые должны связаться с целью, должны быть помещены внутри круга.

Изоляция нападающего вовлекает ту же самую логическую схему, как и изоляция цели. Каждый хочет создать барьер вокруг нападающего, настолько плотный насколько возможно, такой, что нападающий не может предпринять наступления через него. В этом случае также, некоторые главные компьютеры должны иметь возможность связаться с нападающим и таким образом должны постоянно находиться в пределах круга.

Третья стратегия должна создать набор вырезок между целью и нападавшим. Это просто отделяет два барьера с непроницаемой границей. Они не пытаются останавливать того нападающего или цель от нападения на другие главные компьютеры в сети. Создание набора вырезок полезно, когда каждый, прежде всего, заинтересован относительно нападающего, достигающего цели. Методика вырезок, всегда может быть разработана таким образом, чтобы устранить законную связь не более чем, методика изоляции нападающего или изоляция цели.

10.10. Операции мобильных агентов в подсети нападающего и целевой подсети

Выше было описано использование многоагентных систем для ответа на нападение на центральном компьютере нападающего и целевом компьютере, где в силу гибкости, мобильные агенты будут использоваться для инициализизации ответов. Однако проблема состоит в том, что агенты будут терпеть неудачу перед лицом искушенного противника. Также были описаны приемы изоляции атакующего и целевого компьютеров в маршрутизаторах и сетевых устройствах защиты так, чтобы нападающий не мог бы сорвать ответ, но эти приемы наряду с трафиком злоумышленника отсекают и законный трафик. Третья альтернатива ответа, которая может быть осуществлена с использованием мобильных агентов, состоит в том, чтобы отправить агента на нескомпрометированный главный компьютер в подсети цели или нападающего.

С этой позиции мобильный агент может предпринять ряд действий против нападающего или целевого главного компьютера, чтобы отключить его. Агент может использовать известные уязвимость или просто перегружать нападающий и целевой главный компьютер пакетами с пустыми полями данных, чтобы вызвать их переполнение. Учитывая, что мобильный агент может переходить на разные главные компьютеры, он может проводить выявление достаточных сетевых ресурсов, необходимых, чтобы вызвать перегрузку любой атакованной машины. В этом случае мобильный агент сохранит функционирование целевого компьютера, а нападающий не сможет продолжить выполнение задуманного плана до тех пор, пока администратор системы не оценит ситуацию.

Заключение

На первый взгляд, технология мобильных агентов предлагает много интересного в деле обнаружения вторжений в компьютерные сети. Идея относительно мобильных и самонастраивающихся компонентов интуитивно кажется полезной в обнаружении вторжения и многих других приложениях. Однако достаточно трудно реализовать выгоды от технологии мобильных агентов практически. Несмотря на эти трудности, технология обеспечивает ценные дополнения к текущим возможностям. Хотя препятствия на пути создания практических систем на основе мобильных агентов достаточно высоки, способность перемещать программу выполнения от одной аппаратной базовой системы до другого – весьма ценное свойство. В конечном счете когда проблемы, связанные с обеспечением защиты, производительности, безопасной технологий функционирования и барьеры стандартов, которые подавляют это развитие технологии мобильных агентов, будут решены, технологии на основе агентов ждет широкое применение.

Мобильные агенты не только полезны вообще, но они весьма полезны для перспективных СОВ. Мобильные агенты могут расширять характеристики СОВ и даже предлагают им новые возможности. Однако получить эти выгоды не просто и будет требоваться существенные затраты ресурсов на исследования.

Имеются три основных области исследования для изучения возможности использования мобильных агентов при решении задачи обнаружения вторжения: повышение производительности, усовершенствования архитектуры СОВ и усовершенствование методологии ответа. Усовершенствование архитектуры проектируемых СОВ могут вестись по трем направлениям исследований: новые парадигмы обнаружения, новые парадигмы структуры и усовершенствования в существующих проектах.

Ниже выделены три области и оценена важность каждой области исследования. Каждая определенная область исследования отражает направление исследования, обсуждавшуюся выше. Важность для каждой области оценена как высокая, средняя или низко. Важность - субъективные 3 мера, объединяющая случай успешного исследования с возможным

воздействием на поле обнаружения вторжения. Это - наша надежда, что эти оценки помогут вести будущее исследование к более плодотворным областям в использовании мобильных агентов, чтобы исполнить обнаружение вторжения.

ПРИЛОЖЕНИЕ. - Архитектурные решения

Первое поколение систем обнаружения вторжения строилось по простой двухуровневой архитектуре: компонент сбора данных и компонент анализа данных. Компонент сбора данных получает информацию из контрольных файлов регистрации в главном компьютере или от контроля пакетов в атакованных сетях. Эта информация затем поступает в централизованный компонент анализа, который использует одни или более различных методов обнаружения. Два логических компонента могут располагаться в одном главном компьютере или быть физически распределенными в сети. Подобная структура эффективна для небольшого множества компьютеров, требующих контроля, централизованный анализ ограничивает способность к масштабированию. Последующие поколения СОВ стремятся к достижению универсальности главным образом, путем введения промежуточных блоков между множеством компонент сбора и компонентами анализа информации, формируя некоторую иерархию взаимодействия. Данное приложение дает краткий обзор иерархической и сетевой архитектур, их достоинства и недостатки, а также возможность использования мобильных агентов при реализации одной из них.

Иерархическая организация

Иерархическая конструкция исходит из древовидной структурой с компонентами системы управления наверху, информационные модули агрегирования данных во внутренних узлах и операционных единицах в вершинах. Операционные единицы могут быть как компонентами сетевой СОВ, централизованной СОВ, антивирусным программным обеспечением и компонентами системы формирования ответа на вторжение.

Сбор информации происходит в листьях. Далее, информация передается во внутренние узлы, которые агрегируют информацию от множественных листьев. После агрегирования и сжатия, данные поступают во все более высокие внутренние узлы, пока не достигают корень иерархии. Корень - система управления, которая оценивает ситуацию с нападением и планирует ответные меры. Корень обычно имеет интерфейс с консолью администратора, который может вручную оценить ситуацию и спланировать ответ.

Ключевое свойство иерархических структур состоит в эффективности связи посредством информационных фильтров для передаваемой вверх в иерархии информации и управлении вниз к листьям структуры. Структура наиболее привлекательна для создания масштабируемой распределенной СОВ с центральным пунктом администрации. Системы с иерархической архитектурой обладают высокой эффективностью связей между компонентами, но недостаточно гибки в области функционирования.

Сетевая организация

В отличие от иерархической структуры, сетевая архитектура разрешает поток информации от любого узла до любого другого узла. Поэтому, структуры

с сетевой архитектурой имеют тенденцию страдать от неэффективности в связи из-за беспрепятственного потока информации. Они, однако, компенсируют неэффективность связи гибкостью в функционировании. По крайней мере, одна из существующих СОВ, Cooperating Security Managers, использует эту структуру, объединяя функции сбора, агрегирования и управления в единственный компонент, постоянно находящийся на каждой проверенной системе. Любые значащие события, встречающиеся в одной системе, которая основа от подключения, возникающего в другого, сообщены назад системному программисту исходящей системы руководителем службы безопасности в системе, где случай произошел. В ситуациях, где исходящая система подключения - промежуточный узел в цепочке связей, системный программист обязан сообщить вперед следующему системному программисту в цепочке.

Неявно компоненты СОВ имеют тенденцию к иерархии, однако, тенденция не строга, так как связь может происходить, вообще, между любым типом компонент и не строго на принципе «один-с-одним» или «ведущий-ведомый». Например, модуль сбора данных может сообщить о важном инциденте непосредственно управляющему устройству, гораздо быстрее, чем через промежуточные узлы. Кроме того, равные по положению управляющие компоненты, являются соответствующими точками администрирования и управления частями сети предприятий или выделенных и удаленных сегментов сети.

Как путь объединения лучших характеристик иерархических и сетевых архитектур, может использоваться гибридная модель. Гибридная модель исходит из сетевой архитектуры. Не имея явного корневого узла, система все же сохраняет полную иерархическую структуру и позволяет компонентам гибко связываться вне строгой иерархии там, где это полезно.

При использовании мобильных агентов узлы сбора данных, узлы агрегирования и узлы управления не должны постоянно находиться на конкретной машине. То есть мобильный агент может функционировать как узел абстракции данных и двигаться в любой физический сегмент в сети для улучшения конечного результата. Фактически, архитектура на основе мобильных агентов предлагает дополнительное усовершенствование этой идеи, - различные агенты могут быть предназначены для различных функций. Например, может иметься иерархия мобильных агентов, специализированных для обнаружения и ответа на вирусные атаки. Узлы агрегирования и управления, необходимые для обнаружения вирусов, могут быть совершенно другими мобильными агентами чем, те которые требовались для аудита внутренних атак. Таким образом, много иерархий агентов могут существовать одновременно, каждая из которых настроена на различные виды нападения и функционирующая каждая наиболее приемлемым способом.

Архитектура для обнаружения вторжения

Общая структура обнаружения вторжения обеспечивает полезную перспективу для понимания и обсуждения особенностей и составляющих,

существующих в любой СОВ. CIDF определяет следующие универсальные типы компонентов:

- генераторы события - контролирующие фильтры данных, системы охранной сигнализации или другие датчики, необходимые для обнаружения события в вычислительной среды;
- анализаторы - компоненты типа генератора событий, датчика сигнатуры нападения, статистического анализатора или коррелятора, используемого для получения информации об обнаружении вторжения, от других компонентов, ее анализа и получения новой информации о событии. Информация о событии включает описание самого события, которое произошло в системе, анализ этих событий, описание действий, которые были выполнены, а также делает запрос относительно данного события;
- базы данных - компоненты, которые не выполняют обработку или изменения информации, которую они хранят, а просто представляют собой хранилище информации о событии;
- модули ответа - компоненты, которые выполняют «предписания» по локализации вторжения от других компонентов. «Предписания» - запросы, типа уничтожения процессов или разрыва соединения, направляемые другими компонентами, но выполняемые модулем ответа;
- модули-представители - компоненты, которые обеспечивают конфигурацию и директивные услуги по связи компонентов друг с другом. Представитель позволяет компонентам разыскивать взаимодействующие компоненты либо по названию, либо по предоставляемому сервису.

Компоненты могут быть организованы в иерархических, сетевых или гибридных структурах. Компоненты могут также поддерживать разные типы интерфейса. Некоторые компоненты могут быть далее расчленены. Например, анализатор может быть реализован двумя различными компонентами: агент выявления, который выявляет вторжение и агента планирования ответа, который формулирует ответы. Точно так же один или несколько компонентов могут быть объединены вместе в том же самом узле. Однако, начальные типы определенных компонентов адекватны фиксированным характеристикам СОВ. Любой из CIDF компонентов может быть представлен как мобильный агент.

Однако, некоторые компоненты лучше функционируют, если они остаются статическими и могут быть обозначены как статические агенты. Вряд ли, что полная подвижность всех компонентов была бы эффективна. Далее описаны некоторые из преимуществ и препятствий использования мобильных агентов для общих компонентов СОВ.

- ***сетевые датчики трафика***: не отстающий увеличивающийся трафик сети, кажется, становится заданием ядерных или специальных аппаратных средств цели. Датчик трафика подвижной сети связи, если это когда-либо могло бы не отставать от сетевого

трафика, будет терять информацию, когда это упаковывает и идет на другую машину. Мобильный агент плохо подошел бы непосредственно для мониторинга трафика сети, но только данные, обеспеченные сетевым датчиком на анализаторы данных.

- ***главный компьютер базирования датчика***: Мобильные агенты могли бы идти на главные компьютеры (например, автоматизированные рабочие места, сетевые устройства защиты, маршрутизаторы, и т.д.) собирать(забирать) информацию, которая не доступна на проводе. Где они идут, может быть в ответ на анализ контрольных фильтров данных или времени запуска сетевых проводов поездки.
- ***анализаторы***: агенты Анализатора обрабатывают контрольные файлы регистрации, сопоставляют данные от мониторов трафика цепи с распределенными параметрами и обрабатывают данные собранными сетевыми датчиками. Поскольку новые нападения признаны, или новые образцы подозрительной деятельности признаны, анализаторы должны быть модернизированы, в то время как другие удалили, поскольку они больше не полезны. Агенты Анализатора могут исполнять специализированные исследования данных, которые не поддержаны ведущей базовой системой, на которой данные постоянно находятся.
- ***ответчики***: Мобильные агенты хорошо подходящие, чтобы служить в емкости(пропускной способности) агентов ответчика. Эти агенты могут путешествовать через сеть, чтобы реконфигурировать сеть, особенно полезную для тонких клиентов, которые не обладают функциональными возможностями, требуемыми, чтобы принимать решения и выполнить административные изменения(замены).
- ***координаторы***: Агенты со способностью анализировать(расчленять) и решить проблемы совместным способом были разработаны успешно интеллектуальным семейством агента для множества доменов(областей). Агенты наблюдают(соблюдают), рассуждают, взаимодействуют с другими агентами, и выполняют действия одновременно с другими агентами. Взаимодействия могут передавать факты или веры через язык связей агентов и могут зависеть от онтологии, чтобы достигнуть общего(обычного) понимания.

Различные сценарии поднимают вопрос, как эти различные характеристики могут быть интегрированы под единственной(отдельной) структурой MAIDS или проектом? Этот вопрос будет должен быть адресован, или неявно или явно, из-за значения, такая перспектива имеет в построении любого выполнения MAIDS.