Агентно-ориентированное моделирование бот-сетей

Коновалов А.М.
Санкт-Петербург, ЗАО “Аркадия”
alexonline@hotbox.ru
Шоров А.В., Котенко И.В.
Лаборатория проблем компьютерной безопасности, СПИИРАН
{ashorov, ivkote}@comsec.spb.ru

В работе рассматривается предложенный общий подход и реализуемая программная среда, предназначенные для моделирования бот-сетей и механизмов защиты от их воздействия. Моделируются жизненный цикл бот-сети, а так же антагонистический, по отношению к нему, процесс сдерживания его развития на основе применения механизмов защиты от воздействия бот-сети. Исследуются сценарии формирования бот-сети, сценарии различных инфраструктурных атак, выполняемых с помощью бот-сетей (в том числе реализации DDoS-атаки), а также сценарии защиты от них. Модели бот-сети и механизмов защиты от воздействия бот-сети задаются в виде модели противоборства команд интеллектуальных агентов атаки и защиты.

С появлением бот-сетей злоумышленники получили доступ к миллионам зараженных компьютеров пользователей, а число киберпреступлений увеличилось в сотни раз. По данным ФБР за октябрь 2009 г., потери из-за бот-сетей составили около $100 млн. Все это говорит об актуальности исследования проблемы защиты от бот-сетей. Одной из важнейших задач таких исследований является исследовательское моделирование бот-сетей и механизмов защиты от них с целью разработки эффективных методов и средств противодействия бот-сетям.

Основой предлагаемого подхода к моделированию бот-сетей и механизмов защиты от их воздействия является агентно-ориентированное моделирование. Модели бот-сети и механизмов защиты от воздействия бот-сети в настоящей работе задаются в виде модели противоборства команд атаки и команд защиты. Каждая команда представляет собой некоторое подмножество узлов вычислительной сети, определенных в виде соответствующих агентов, и имеющих общую коллективную цель. Команда атаки представляется агентами, входящими в состав бот-сети и реализующими действия, направленные на реализацию коллективной цели - обеспечение жизнедеятельности бот-сети. Примером коллективной цели команды атаки является атака типа “распределённый отказ в обслуживании” (DDoS) некоторого заранее идентифицированного ресурса. Аналогичным образом, команда защиты формируется из агентов, выполняющих функции защиты и имеющих коллективную цель противодействовать процессу функционирования бот-сети.

Основной парадигмой используемой в данной работе является представление узлов бот-сети в виде множества интеллектуальных автономных агентов. Алгоритм поведения отдельного агента определяется его целевым назначением. Агенты имеют возможность непосредственно выполнять свою целевую задачу и обмениваться информацией друг с другом, образуя команды, ориентированные на достижение одной общей цели. Множество интеллектуальные агентов, имея простые собственные функции, в процессе своей деятельности могут самоорганизовываться в системы со сложным поведением.

Модель топологии моделируемой глобальной вычислительной сети представляется в виде случайного графа, параметризованного статистическими данными, полученными в результате измерения параметров топологии сети Интернет. Моделирование трафика осуществляется на уровне отдельных сетевых пакетов, и реализуется посредством моделирования поведения сетевых приложений. Поведение сетевых приложений имеет

стохастическую природу и задается рядом статистических параметров, значения которых были получены в результате исследования сетевых приложений сети Интернет. Процессы отправки, получения и прохождения сетевых пакетов по коммуникационным каналам осуществляются посредством системы моделирования дискретных событий.

Для реализации предлагаемого подхода, в качестве основного инструмента необходимо наличие программной среды, обладающей широким спектром возможностей по поддержке различных аспектов имитационного моделирования сетевых процессов. В первую очередь требуется возможность моделирования сетевых систем с произвольной топологией и процессов коммуникации между узлами на уровне дискретных событий. Для моделирования реальных коммуникационных сценариев, наблюдаемых в сети Интернет, необходимо наличие моделей протоколов и моделей сетевых приложений.

Авторами настоящей работы используется и разрабатывается многоуровневая инструментальная среда имитационного моделирования сетевых процессов. Среда представляет собой программный комплекс, включающий в качестве нижнего уровня симулятор дискретных событий, реализованный на языке низкого уровня, а так же ряд компонентов, реализующих сущности более высокого уровня.

Архитектура среды моделирования включает четыре основных компонента: базовую систему имитационного моделирования, модуль имитации сети Интернет, подсистему агентно-ориентированного моделирования и модуль процессов предметной области.

С использованием симулятора OMNeT++, библиотек INET Framework, ReaSE, а так же собственных программных компонент, была реализована архитектура для многоагентного моделирования бот-сетей, атак “распределённый отказ в обслуживании” (DDoS) и механизмов защиты от воздействия бот-сети в виде модели противоборства команд интеллектуальных агентов.

Симулятор OMNeT++ представляет собой систему моделирования дискретных событий, и в предлагаемой модели является компонентом нижнего уровня. Симулятор OMNeT++ обеспечивает процессы обмена сообщениями между компонентами модели, визуализацию хода эксперимента, взаимодействие модели с пользователем, а так же предоставляет отладчик моделей, позволяющий в наглядной форме отлеживать состояния объектов и последовательности модельных событий, что полезно при выявлении и устранении ошибок в процессе построения модели. Дополнительно OMNeT++ предоставляет специальный язык для описания связей между компонентами модели, тем самым описывая сетевую топологию, а так же позволяет определять параметры эксперимента.

Топология сети моделируется на двух уровнях детализации. На первом уровне моделируется топология сети на уровне автономных систем (АС). На втором этапе моделирования, для каждой автономной системы моделируется внутренняя топология (Router-level topology).

Команда атаки представлена узлами следующих типов: узел “хозяин”, узел “командный центр”, узел “цель”, узлы “зомби”. Узел “хозяин” посредством рассылки команд задаёт цели для бот-сети и контролирует поведение сети на самом высоком уровне. Узел “командный центр” осуществляет доставку команд полученных от “хозяина” к узлам “зомби”. Узлы “зомби”, получая команды от “командного центра”, непосредственно осуществляют действия, согласно приказам “хозяина”. В настоящем эксперименте определяется один узел “хозяин”, один узел “командный центр” и множество узлов с уязвимым программным обеспечением, которые потенциально могут превратиться в “зомби”-машины. Для генерации легитимного трафика определяется множество узлов – “сервер”. Узлы – “серверы” в ответ на запрос со стороны клиента генерируют трафик статистически подобный трафику типового веб-сервера. Уязвимые хосты определяются случайным образом.

В соответствии с общим подходом, выделены следующие классы агентов защиты: первичной обработки информации (“сенсоры”); вторичной обработки информации

(“сэмплеры”), обнаружения атаки (“детекторы”); фильтрации (“фильтры”); агенты ограничения трафика; агенты-“расследования”.

В проведенных экспериментах в качестве механизма защиты исследовался метод Source IP address monitoring (SIPM), который, основывается на предположении, что в момент атаки DDoS в проходящем трафике лавинообразно возрастает число новых адресов, с которых идёт обращение к атакуемому ресурсу. Модуль, реализующий механизм защиты, может находиться в одном из двух режимов: в режиме обучения или в режиме фильтрации. В режиме обучения модуль перехватывает трафик и определяет количество различных IP-адресов, участвующих в коммуникации за некоторый промежуток времени (параметр tshift). Данные, полученные в процессе обучения, принимаются за типовые значения трафика в данном узле и в последующем используются в процессе детектирования аномалий. В режиме детектора аномалий модуль вычисляет те же параметры и сравнивает их с типовыми значениями. При существенном превышении наблюдаемых номинальных значений модуль генерирует сигнал об обнаружении аномалии и осуществляет выборочную фильтрацию пакетов с новыми адресами источников.

Проведенные эксперименты показали эффективность предлагаемого подхода к моделированию и возможность его использования для исследования бот-сетей и перспективных механизмов защиты.

Работа выполнена при финансовой поддержке РФФИ (проект № 10-01-00826-а) и программы фундаментальных исследований ОНИТ РАН (проект № 3.2).