Котенко И. В.

“СЕТЕВЫЕ КОШКИ-МЫШКИ”: ВОЙНЫ АДАПТИВНЫХ ПРОГРАММНЫХ АГЕНТОВ

Санкт-Петербург, СПИИРАН
ivkote@comsec.spb.ru

Текущее состояние противодействия систем нападения злоумышленников и систем защиты хакеры характеризуют как “игру в сетевые кошки-мышки” (a game of Network Cat and Mouse) – кто кого обманет [1].

Злоумышленники - профессионалы для достижения своих целей способны реализовать развитые стратегии осуществления различных угроз безопасности [2]. Эти стратегии могут включать комплекс различных действий: сбор информации о системе, обнаружение уязвимостей, моделирование способов преодоления защиты, подавление, обход или обман средств защиты, использование уязвимостей и получение доступа к ресурсам, повышение полномочий, реализацию своей цели, скрытие следов своей деятельности и создание “черных ходов” для использования их для последующего вторжения.

Поэтому обеспечение информационной безопасности в современных условиях требует выполнения в реальном времени непрерывного комплекса разнообразных мероприятий: реализация механизмов защиты, соответствующих установленной политике безопасности (в том числе проактивное предупреждение атак и препятствование их выполнению, дезинформация злоумышленника, сокрытие и камуфляж важных ресурсов и процессов), сбор информации о состоянии информационной системы и анализ обстановки за счет механизмов обработки информации из различных источников, обнаружение аномальной активности, нелегитимных действий, атак и вторжений, предсказание намерений и возможных действий злоумышленников, непосредственное реагирование на вторжения, в том числе введение злоумышленника в заблуждение, заманивание злоумышленника с использованием ложных компонентов с целью раскрытия и уточнения его целей, рефлексивное управление поведением злоумышленника, усиление критических механизмов защиты, устранение последствий вторжения, выявленных уязвимостей и адаптация системы обеспечения информационной безопасности к последующим вторжениям.

Чтобы реализовать свои цели как системы нападения злоумышленников, так и системы защиты должны быть адаптивными и динамически эволюционировать и изменять реализуемые механизмы поведения при изменении условий функционирования. При этом изменение условий подразумевается в широком смысле [3]: с одной стороны, оно связано с изменением бизнес-процессов; а, с другой стороны, задается изменением среды, которое включает эволюцию внешнего окружения, изменение стратегий и тактики действий противоборствующей стороны и т.д. Средства нападения злоумышленников эволюционирует посредством генерации новых экземпляров и типов атак, а также сценариев их реализации с целью преодоления подсистемы защиты. Системы защиты адаптируются к действиям злоумышленников путем изменения исполняемой политики безопасности, формирования новых экземпляров механизмов и профилей защиты.

Чтобы реализовать эти возможности в перспективных системах защиты, необходимо обеспечить динамическое адаптивное поведение, автономность и адаптацию отдельных компонентов, использовать методы, основанные на переговорах и кооперации, которые лежат в основе многоагентных систем и (или) автономных вычислений.

В данной работе, на примере защиты от компьютерных атак “Распределенный отказ в обслуживании” в сети Интернет, предлагается *подход к исследованию адаптивных и кооперативных механизмов функционирования команд интеллектуальных агентов.*

Предлагаемый подход основан на представлении сетевых систем в виде комплекса команд взаимодействующих агентов, которые могут быть в состоянии антагонистического

противостояния, безразличия или кооперации. Агрегированное поведение системы выражается в локальных взаимодействиях агентов.

Задача многоагентного моделирования процессов кибернетического противоборства представляется как моделирование антагонистического взаимодействия команды агентов-злоумышленников и агентов защиты.

Цель команды агентов-злоумышленников заключается в определении уязвимостей компьютерной сети и системы защиты и реализации заданного перечня угроз информационной безопасности посредством выполнения распределенных скоординированных атак. Цель команды агентов защиты состоит в защите сети и собственных компонентов от атак. Агенты различных команд соперничают для достижения противоположных намерений. Агенты одной команды сотрудничают для осуществления общего намерения (по реализации угрозы или по защите компьютерной сети).

Выбор сценария поведения каждой из команд зависит, прежде всего, от выбранной ею цели, а конкретная реализация сценария определяется, в первую очередь, непосредственной реакцией противоположной команды. Поэтому выбор каждого очередного шага поведения каждой из команд должен определяться динамически в зависимости от действий противоположной команды и состояния среды.

Поскольку каждая команда действует в условиях ограниченной информации, а каждый член команды может обладать различной информацией о действиях других членов команды, то модель поведения агентов должна быть в состоянии отражать свойство неполноты информации и возможность возникновения случайных факторов, а само поведение должно зависеть от информации, которой владеет команда, и от ее распределения на множестве членов команды.

Поведение антагонистических команд основано на использовании некоторого *критерия адаптации*. В соответствии с этим критерием, антагонистические команды (системы атаки и защиты) настраивают свою конфигурацию и поведение в соответствии с условиями сети и поведением соперничающей команды, например, в зависимости от серьезности (мощности) атаки и защиты.

В докладе рассматриваются методы организации командной работы агентов, структуры команд агентов нападения и защиты, механизмы их взаимодействия и планы действий, реализованный стенд (среда) моделирования противоборства агентов и различные примеры реализованных сценариев моделирования.

Проведенные эксперименты показали возможность использования предложенного подхода для моделирования механизмов защиты и для анализа проектируемых сетей. Они продемонстрировали также, что использование кооперации нескольких команд и комбинированного адаптивного применения различных механизмов функционирования ведет к существенному повышению эффективности защиты.

Работа выполнена при финансовой поддержке РФФИ (проект №07-01-00547) и программы фундаментальных исследований ОНИТ РАН.

Литература

1. Nomad Mobile Research Centre. http://www.nmrc.org

1. Котенко И.В. Интеллектуальные механизмы управления кибербезопасностью // Управление рисками и безопасностью. Труды Института системного анализа Российской академии наук (ИСА РАН). Москва, URSS, 2008.

2. Котенко И.В., Уланов А.В. Моделирование адаптации противоборствующих команд интеллектуальных агентов // КИИ-2008. XI Национальная конференция по искусственному интеллекту с международным участием. Труды конференции. Том 1. М.: URSS, 2008.