Модели и методы построения и поддержки функционирования интеллектуальных адаптивных систем защиты информации

Котенко И. В.
ivkote@iias.spb.su
Санкт-Петербург, Институт информатики и автоматизации РАН

Используемым в настоящее время подходам к защите информации в распределенных компьютерных системах присущ целый ряд недостатков, и системы защиты информации (СЗИ) оказываются не в состоянии эффективно решать задачу управления защищенностью в режиме реального времени. Эти недостатки обусловлены, главным образом, узкой специализацией отдельных средств обеспечения безопасности, неразвитыми механизмами верификации защиты на этапах создания и поддержки, неадекватными механизмами определения уязвимостей, анализа рисков и определения уровня защищенности, мониторинга состояния сетей и адаптации к изменению условий функционирования [1]. В докладе предлагается подход к разработке и использованию СЗИ, основанный на использовании интеллектуальной надстройки над традиционными механизмами защиты и построении единой унифицированной среды для создания и поддержки функционирования систем защиты.

Интеллектуализация механизмов защиты

В соответствии с современными представлениями перспективная СЗИ распределенных компьютерных систем должна представлять собой взаимоувязанную, многоэшелонированную и непрерывно контролируемую систему защиты используемых информационных, программных и аппаратных ресурсов, способную оперативно реагировать на удаленные и локальные компьютерные атаки и несанкционированные действия (НСД), накапливать знания о способах противодействия, обнаружения и реагирования на атаки и НСД и использовать их для усиления защиты.

Такая СЗИ должна предоставлять, по крайней мере, три уровня защиты. Первый уровень защиты составляют «традиционные» средства защиты, реализующие функции идентификации и аутентификации, криптографической защиты, разграничения доступа, контроля целостности, регистрации и учета, межсетевого экранирования. Второй уровень включает в себя средства проактивной защиты, обеспечивающие сбор необходимой информации, анализ защищенности, мониторинг состояния сети, обнаружение атак, противодействие их реализации, введение злоумышленника в заблуждение, и т. п. Третий уровень соответствует средствам управления защитой, которые осуществляют интегральную оценку со-

стояния сети, управление защитой и адаптацию политик безопасности и компонентов СЗИ.

Первый уровень достаточно широко представлен в существующих исследованиях. Разработка механизмов защиты, относящихся ко второму и особенно третьему уровню, реализующих по существу интеллектуальную надстройку над традиционными механизмами защиты, составляет в настоящее время приоритетную задачу в области теоретических и прикладных исследований по построению информационно-безопасных распределенных вычислительных систем.

В рамках решения этой задачи в работе предлагается комплекс формальных методов, моделей, алгоритмов и построенных на их основе программных прототипов, реализующих следующие интеллектуальные механизмы защиты [1]:

1) сбор информации о состоянии информационной системы и ее анализ за счет механизмов обработки и слияния информации из различных источников;
2) проактивное предупреждение атак и препятствование их выполнению;
3) обнаружение аномальной активности и явных атак, а также нелегитимных действий и отклонений работы пользователей от политики безопасности, предсказание намерений и возможных действий нарушителей;
4) активное реагирование на попытки реализации действий нарушителей путем автоматической реконфигурации компонентов защиты для отражения действий нарушителей в реальном масштабе времени;
5) дезинформацию злоумышленника, сокрытие и камуфляж важных ресурсов и процессов, «заманивание» злоумышленника на ложные (обманные) компоненты с целью раскрытия и уточнения его целей, рефлексивное управление поведением злоумышленника;
6) мониторинг функционирования сети и контроль корректности текущей политики безопасности и конфигурации сети;
7) поддержку принятия решений по управлению политиками безопасности, в том числе по адаптации к последующим вторжениям и усилению критических механизмов защиты.

Поддержка жизненного цикла систем защиты

В процессе использования различных механизмов защиты необходимо осуществлять поддержку защищенной информационной среды на различных этапах жизненного цикла, включая этапы их проектирования, конфигурирования, развертывания, функционирования и модификации.

Поэтому, кроме создания отдельных перспективных механизмов защиты, необходимо решать задачу разработки моделей и методов построения единой унифицированной системы (среды), осуществляющей поддержку всего жизненного цикла СЗИ, включая адаптивное управление политиками безопасности [1].

В работе предлагается подход к осуществлению непрерывной цепочки различных этапов жизненного цикла распределенных защищенных компьютерных систем (с множеством прямых и обратных связей от одного этапа к другому). Данный подход предполагает реализацию следующих механизмов:

1) спецификацию политик безопасности и архитектуры (или конфигурации) защищаемой системы;
2) трансформацию политик безопасности с целью их уточнения (детализации) с учетом описания защищаемой системы;
3) верификацию политик безопасности (проверку правильности и устранение конфликтов);
4) определение уровня безопасности и анализ рисков;
5) моделирование поведения системы защиты в различных условиях функционирования;
6) изменение политик в соответствии с требуемым уровнем безопасности и возможностями по использованию различных ресурсов и выделению финансовых средств и на защиту информации;
7) реализацию политик безопасности в системе, в том числе трансляции сформированных правил безопасности в параметры конфигурации и настройки программно-аппаратного обеспечения;
8) проактивный мониторинг выполнения политик безопасности, в том числе обнаружение отклонений работы пользователей от политики безопасности, обнаружение вторжений и анализ уязвимостей;
9) адаптацию поведения распределенных защищенных компьютерных систем и реализованных политик безопасности в соответствии с условиями функционирования.

В докладе приводятся примеры задач классификации, прогнозирования и анализа данных, используемые в предлагаемых механизмах защиты (в частности, при сборе информации о состоянии и ее анализе, обнаружении аномальной активности, дезинформации злоумышленника и мониторинге сети) и механизмах поддержки различных этапов жизненного цикла системы защиты, в том числе при адаптации ее поведения.

Заключение

В работе предложен подход к разработке и использованию интеллектуальных адаптивных систем защиты информации распределенных компьютерных систем. Подход основан на реализации интеллектуальных механизмов управления защитой и построении единой унифицированной среды для создания и поддержки функционирования систем защиты на всем их жизненном цикле, включая адаптивное управление политиками безопасности.

Работа выполняется при поддержке РФФИ (проект № 07-01-00547), программы фундаментальных исследований ОИТВС РАН (контракт № 3.2/03) и Фонда содействия отечественной науке.

Литература

[1] *Котенко И. В., Юсупов Р. М.* Технологии компьютерной безопасности // Вестник РАН. — 2007. — Т. 77. — № 4.