XXIX Неделя науки СПбГТУ. Материалы межвузовской научной конференции. Ч.V: С.106-107, 2001.

УДК 50.41.00

М.О. Калинин (асп., каф. ИБКС), Д.П. Зегжда, доц., к.т.н.

ЛАБОРАТОРНОЕ МОДЕЛИРОВАНИЕ И ИССЛЕДОВАНИЕ ПОЛИТИК БЕЗОПАСНОСТИ

Существующие в настоящее время модели безопасности используют различные подходы к решению задачи управления доступом. До сих пор не появились универсальные модели, эффективные во всех случаях. Поэтому актуальной является проблема создания таких систем защиты, которые могли бы обеспечить реализацию нескольких политик безопасности. Наибольший уровень универсальности можно получить, если отделить политику от механизмов ее реализации. Наиболее простое решение состоит в спецификации правил доступа посредством универсального языка описания политик безопасности и в разработке машины логического вывода, обрабатывающей спецификации системы. Это позволит построить модельную среду для описания и исследования защищенных систем.

В докладе рассматривается универсальный язык описания политик безопасности. Каждому объекту и субъекту поставлен в соответствие набор атрибутов безопасности, которые характеризуют его содержание (уровень безопасности, группу и т.д.) и используются для определения правил политики. Над значениями атрибутов возможны операции сравнения. Введены предикаты, используемые для описания моделируемой системы (субъектов, объектов и их атрибутов), а также предикаты для описания правил доступа. Определяя множества субъектов, объектов, атрибутов и задавая правила обработки предикатов, можно моделировать системы, подчиняющиеся той или иной политике безопасности. Разработанный универсальный язык описания положен в основу создания программной среды для моделирования и исследования политик безопасности.

Главная цель разработки состоит в создании программного продукта, позволяющего описать модель безопасности и провести практическое исследование ее механизмов защиты. Результатом этой работы является лабораторный стенд, который реализован в среде Windows и представляет собой интегрированную среду, применяя которую пользователь получает возможность моделировать политики безопасности, проверять выполнимость ее требований и контролировать процесс обработки правил доступа.

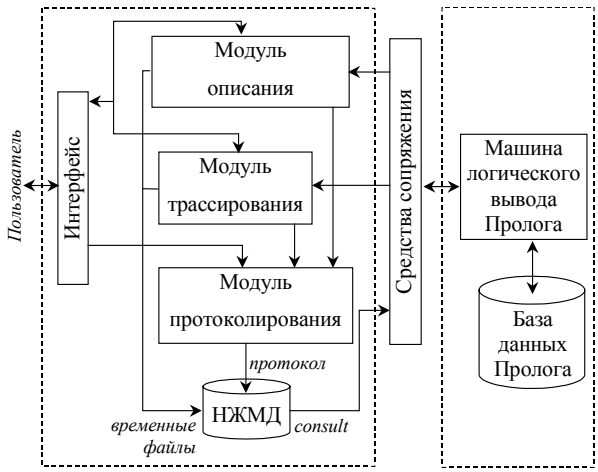

Рис. 1. Архитектура автоматизированного лабораторного

Функция моделирования политик безопасности заключается в предоставлении пользователю средства описания — языка описания политик безопасности. Механизм

моделирования, реализованный в исследовательской системе, основан на применении концепции логического программирования. Ситуации описываются при помощи формул логики предикатов I порядка, а для выполнения выводов из этих формул применяется автоматическая машина вывода. В качестве системы логического программирования выбран SWI-Prolog, имеющий возможность сопряжения с Си-программой.

Разработанная система включает пользовательский интерфейс, модули описания, трассирования и протоколирования (на языке Си), а также средства описания и механизм отладки (на языке Пролог) (рис. 1).

Исследовательская система используется для изучения студентами теории классических политик безопасности, анализа их достоинств, недостатков и реакций на попытки нарушения доступа. В ходе работы приобретаются навыки в решении проблем моделирования поведения систем в зависимости от политики; анализа ситуации и выбора соответствующей модели; поиска противоречий в состояниях информационной системы; синтеза новых средств защиты.

Исследование политик безопасности осуществляется в следующей последовательности:

1. В ходе работы проводится проверка на доступ к объектам. Модель обеспечивает надежную защиту, например, по чтению и записи, что подтверждается протоколом работы стенда.

2. Затем моделируется поведение троянского коня, который эквивалентен получению неавторизованным субъектом доступа на чтение секретного объекта.

3. Многократное повторение операций создания, удаления сущностей, смены их атрибутов переводит систему в новое состояние. Предлагается убедиться в безопасности этого состояния. Для этого необходимо исследовать систему на предмет прежней корректности правил доступа и выяснить, не получили ли субъекты возможность доступа к объектам, которой они раньше не имели.

Кроме того, исследовательские средства системы могут быть применены в процессе проектирования новых моделей, поскольку позволяют тестировать свойства создаваемой модели и подбирать правила политики безопасности. Наконец, язык описания и разработанный инструментарий могут быть использованы при построении адаптивных защитных механизмов, инвариантных к политикам безопасности.

Разработанный лабораторный стенд проходит апробацию как обеспечение лабораторных занятий по курсам информационной безопасности, читаемых на кафедре информационной безопасности компьютерных систем СПбГТУ.