МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ЮЖНО-РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
(НОВОЧЕРКАССКИЙ ПОЛИТЕХНИЧЕСКИЙ ИНСТИТУТ)

КОМПЬЮТЕРНЫЕ ТЕХНОЛОГИИ В НАУКЕ, ПРОИЗВОДСТВЕ, СОЦИАЛЬНЫХ И ЭКОНОМИЧЕСКИХ ПРОЦЕССАХ

Материалы
IV Международной научно-практической конференции

Часть 1

14 ноября
г. Новочеркасск

Новочеркасск 2003

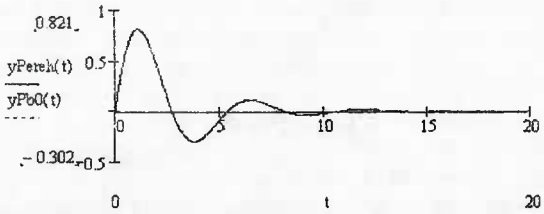

Рис.5. Совпадающие графики переходного процесса (yPereh(t)) и реакции системы (yPb0(t)) на нулевое входное воздействие ($x(t)$=0)

Из графиков можно заметить, что кривая переходного процесса не зависит от входного воздействия и совпадает с реакцией системы на нулевое входное воздействие ($x(t)$=0) (на рисунке 5 выведены графики переходного процесса и реакции системы на нулевое входное воздействие).

Литература

1. Левин А.И. Математическое моделирование в исследованиях и проектировании станков. – М.: Машиностроение, 1978.
2. Вержбицкий В.М. Численные методы. Математический анализ и обыкновенные дифференциальные уравнения. – М.: Высшая школа, 2001.
3. Корн Г., Корн Т. Справочник по математике для научных работников и инженеров. – М.: Наука, 1974.
4. Бендат Дж., Пирсол А.Д. Применения корреляционного и спектрального анализа. – М.: Мир, 1983.
5. Волков Н.В. Функциональные ряды в задачах динамики автоматизированных систем. – М.: Янус-К., 2001.
6. Образцов И.Н. Разработка математического и программного обеспечения для изучения технических систем в частотной области на основе применения нелинейных моделей в виде функциональных рядов. – М.: 2001.

111555, г. Москва, ул. Сталеваров, д. 18, корп. 2, кв. 151, т. (095) 303-22-38,
e-mail: dows@mail.ru.

УДК 004.056

О МОДЕЛЯХ КОНТРОЛЯ ДОСТУПА ВО ВЗАИМОУВЯЗАННЫХ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ ПРОСТРАНСТВАХ

Рамиз Гусейн оглы Шыхалиев
Институт информационных технологий
национальной академии наук Азербайджана

Рассматриваются модели контроля доступа во взаимоувязанных корпоративных информационных пространствах.

Сегодня практически ни одно предприятие не может добиться успеха в обработке принадлежащей ей информации в рамках одной локальной сети. Это связано с необходимостью обмена информацией между тер-

риториально разнесенными пользователями предприятий, а также с внешним миром. Объединение территориально удаленных локальных сетей через частные и публичные сети, а также возможность обеспечения доступа клиентов этих сетей к ресурсам Internet во многом определяет успех в деятельности государственных и коммерческих организаций. Поэтому создаются корпоративные сети (КС), осуществляющие обмен информацией как в рамках одного предприятия, так и для сотрудничества с другими предприятиями. Однако при этом усиливаются угрозы несанкционированного доступа (НСД) к ресурсам КС.

Как организация может противостоять НСД и защитить свои ресурсы и информацию? Контроль доступа – фундаментальный элемент любой политики безопасности, непосредственно ориентированный на решение этой задачи. Для этого необходимо построить систему согласованного безопасного информационного взаимодействия в КС предприятия и между КС других предприятий, обеспечивающий защиту от НСД, базирующейся на применении технологии экранирования. При этом контроль доступа в КС предприятия и между КС других предприятий осуществляется посредством межсетевых экранов.

Как правило, для контроля доступа используются следующие модели: дискреционный контроль доступа, мандатный контроль доступа.

Модель дискреционного доступа описывается матрицей доступа субъектов системы к объектам, в ячейках которой указаны права доступа субъектов системы к объектам [1, 2]. Язык политики безопасности позволяет непосредственно специфицировать модель дискреционного доступа.

Противоречивость правил доступа субъектов системы к объектам является одной из проблем моделей дискреционного доступа. Эта противоречивость может быть вызвана ошибками при задании матрицы доступа субъектов системы к объектам. В результате обнаружения противоречивости спецификаций могут быть обнаружены такие проблемы, как: отсутствие требования авторизации для процесса в системе; существование неидентифицированных ресурсов системы; утечка прав доступа (проблема, описанная в модели Харрисона - Руззо - Ульмана [1, 2, 3]) и т.д .

В отличие от моделей дискреционного доступа, модели мандатного доступа накладывают ограничения на передачу информации от одного пользователя к другому.

Классической моделью, лежащей в основе построения многих систем мандатного доступа и породившей остальные модели мандатного доступа, является модель Белла и Лападулла [1, 2]. Модель Лападулла – это модель, в которой определены два правила:

- NoReadUp – запрет на чтение объекта субъектом более низкого уровня;
- NoWriteDown – запрет на запись в объект субъектом более высокого уровня.

Несмотря на все достоинства, при использовании модели Белла и Лападулла в контексте практического проектирования и разработки реальных компьютерных систем возникает ряд технических вопросов. Данные вопросы являются логическим следствием достоинства модели Белла и Лападулла – ее простоты. Проблемы возникают при рассмотрении вопросов построения политики безопасности для конкретных типов систем, т.е. менее абстрактном уровне рассмотрения. При данном рассмотрении системный компонент модели усложняется, что может привести к неадекватности модели Белла и Лападулла в ее классической форме. Как следствие, в мире компьютерной безопасности ведется широкая полемика по поводу применимости модели Белла и Лападулла для построения безопасных систем.

В реальной жизни компьютерные системы обычно имеют администратора, который управляет системой, добавляя и удаляя пользователей, восстанавливает функционирование после сбоев, устанавливает специальное программное обеспечение, устраняет ошибки в операционной системе или приложениях и т.п. Очевидно, что такие процессы не могут управляться правилами модели Белла и Лападулла или каких-либо других моделей, не позволяющих им выполнить функции администрирования.

При практической реализации вышеуказанных моделей контроля доступа, для организации защиты информации в реально функционирующих КС, в силу их инертности появляется проблема реализации динамики изменения политики безопасности, происходящих в защищаемой КС.

Обычно контроль доступа осуществляется на базе субъектов и объектов. Субъектами могут быть пользователи или процессы, которые выполняются от имени пользователей. Объектами могут служить данные или ресурсы системы, например – объектами могут быть файлы. Обычно процессом могут быть приложения, выполняемые от имени пользователя, которые являются самым хорошим разделяемым на части субъектом, по отношению с которым со стороны операционной системы осуществляется контроль доступа.

Деятельность любой организации представляет собой систему процессов, в которую вовлечены финансовые, материальные, кадровые, информационные и прочие виды ресурсов.

Так как в организациях, участвующих в информационном обмене, невозможно создать гомогенные вычислительные среды, то обычно в межорганизационных совместных вычислительных средах преобладают разнородность в технологии на базе Internet [4, 5]. Одной из технологий, на основе которой обеспечивается разделение данных и координация работы в глобальном масштабе, является workflow (workflow – «поток работ») [6, 7].

В взаимоувязанных корпоративных информационных пространствах workflow осуществляется в крупных масштабах и может состоять из

множества задач, которые могут быть нитями в пределах процесса. Следовательно, обычные методы контроля доступа могут быть слишком грубыми для workflow вообще и не позволить должным образом обеспечивать информационную безопасность КС. Поэтому необходим детальный контроль доступа, который базируется на рабочем контексте пользователя. Задачи workflow обусловливают рабочий контекст пользователей [8]. Даже один и тот же пользователь может иметь различные потребности и требования доступа к данным в зависимости от задач, над которыми работает пользователь.

Рассмотрим workflow, который состоит из четырех задач. Предположим, что все четыре задачи находятся в одном процессе, и для каждой задачи имеется соответствующее разрешение. При использовании традиционного метода контроля доступа, пользователь получит все разрешения, даже если он нуждается только в одном разрешении, чтобы выполнить соответствующую задачу, потому что обычные механизмы контроля доступа не могут различить задачи в пределах процесса.

Для применения детального контроля доступа в workflow вводятся модули контроля доступа, ориентированные на конкретные задачи (task-specific access control modules (TACM)) [8]. Цель TACM состоит в том, чтобы обеспечить детальный контроль доступа как для субъекта, так и для объекта.

Литература

1. Теория и практика обеспечения информационной безопасности / Под ред. П.Д. Зегжды. – М.: Яхтсмен, 1996.
2. Хоффман Дж. Современные методы защиты информации. – М.: Сов. Радио, 1980.
3. M. Harrison, W. Ruzzo «Monotonic protection systems», Foundation of secure computation, 1978.
4. Аббасов А.М., Алгулиев Р.М., Касумов В.А. Методы защиты данных от несанкционированного доступа // Известия Академии наук Азербайджана. Сер. физ.-техн. и мат. наук. – 1994. – № 5-6. – С. 79-84.
5. Алгулиев Р.М. Концептуальная модель управления глобальным состоянием безопасности корпоративной сети. // Труды XIV Междунар. симп. «Управление большими системами» CONTROL'2000. – Тбилиси, 30-31 окт. 2000 г. – С. 184-189.
6. .D.L. Long, J. Baker and F. Fung «A Prototype Secure Workflow Server», In Proceedings of 15 th Annual Computer Security Applications Conference, Phoenix, Arizona, December 1999.
7. M.H. Kang, B.J. Eppinger, and J.N. Froscher, «Tools to Support Secure Enterprise Computting», In Proceedings of 15 th Annual Computer Security Applications Conference, Phoenix, Arizona, December 1999.
8. R.K. Thomas and R.S. Sandhu, «Task-based Authorization Controls (TBAC): A Family of Models for Active and Enterprise-oriented Authorization Management», In Proceedings of the IFIP WG11.3 Workshop on Database Security, August 1997.

Az1141, г. Баку, Азербайджанская Республика, ул. Ф. Агаева, 9, т. (+99412) 390167, fax (+99412) 396121, e-mail: **secretary@iit.ab.az.**