УДК 004

РАЗРАБОТКА СИСТЕМЫ КОНТРОЛЯ ДОСТУПА ДЛЯ БАНКА

Бушра Мохаммеджавад
Научный руководитель: Пономарёв А. доцент кафедры АИКС

Национальный Исследовательский Томский политехнический университет,
634050, Россия, г. Томск, пр. Ленина, 30
E-mail: bushra_comp@yahoo.com

Система контроля доступа используется для защищенной передачи информации во многих международных компаниях. В данной работе была представлена система контроля доступа для банка.

Введение

Доверительное управление доступом является наиболее распространенным: пользователи, сами указывают, кто может получить доступ к своим файлам. Система определяет, может ли пользователь получить доступ к файлу. Обязательные атрибуты безопасности назначаются или автоматически с помощью операционной системы, в соответствии со строгими правилами. Атрибуты не могут быть изменены пользователями или их программами. Если система определяет, что обязательные атрибуты безопасности пользователя не подходят для доступа к определенному файлу, то никто, даже владелец файла не сможет сделать файл доступным для пользователей [1].

Списки управления доступом

Одним из наиболее эффективных схем контроля доступа, с точки зрения пользователя, список контроля доступа. Он идентифицирует отдельных пользователей или группы пользователей, которые могут получить доступ к файлу. Недостатком схемы списка управления доступом является производительность: он сканирует каждый раз каждого пользователя, изъявившего желание получить доступ к файлу. Другим недостатком является управление хранением данных: ведение списка переменной длины для каждого файла результатов либо сложной структуры каталогов или неиспользуемого пространства для неиспользуемых записей. Это, как правило, является проблемой только для систем, имеющих огромное количество очень маленьких файлов (типичные пути, в котором используются системы Unix). Список управления доступом используется только для файлов, где группа пользователей слишком велика, чтобы указать желаемый набор пользователей [2].

Список доступа

Другой тип контроля доступа – список доступа. Он является ключом к конкретному объекту, а также режиму доступа (чтение, запись или запуск программы). Субъект может получить доступ к объекту в указанном режиме. На самом высоком уровне в системе, где мы имеем дело с пользователями и файлами, система поддерживает список доступа для каждого пользователя. Пользователи не могут его расширять, кроме как для покрытия новых файлов, которые они создают. При этом им может быть разрешено предоставлять доступ к файлам, передавая копии другим пользователям. Этот тип контроля доступа гораздо больше, чем пароли, страдает от проблемы управления программным обеспечением. Система должна под-

держивать список для каждого пользователя, который может содержать сотни или тысячи записей. При удалении файла, система должна очистить возможности для файла из списка каждого пользователя. Наиболее успешное использование возможностей на более низких уровнях в системе, где возможности обеспечивают основной механизм защиты и не видимых пользователю схемы управления доступом [3].

Методы контроля доступа: обязательный контроль доступа

Он помогает предотвратить некоторые виды троянских атак путем наложения ограничения доступа, который не может быть обойден, даже косвенно. Используя данный вид контроля, система присваивает как субъекты и объекты специальные атрибуты безопасности, которые не могут быть изменены по желанию в качестве атрибутов управления доступом на уровне пользователей. Система решает, может ли субъект доступ к объекту путем сравнения их атрибуты безопасности. Несколько общих концепций, однако, применимы к концепции обязательного контроля доступа [4].

В решеточной системе управления доступом могут быть использованы для комплексных решений контроля доступа с участием нескольких объектов и / или предметов. Модель решетки представляет собой математическую структуру, которая определяет наибольшие нижнего предела и наименее верхнего предела значения для пары элементов, таких как субъект и объект [1].

Методы контроля доступа: дискретное управление доступом

Управления доступом (DAC) – политика доступа определяется владельцем файла (или другого ресурса). Владелец решает, кому разрешен доступ к файлу и какие привилегии у него есть.

Два важных принципа в DAC: 1) файлы и данные о собственности – у каждого объекта в системе должен быть хозяин. Политика доступа определяется владельцем ресурса (в том числе файлов, каталогов, данных, системных ресурсов и устройств); 2) теоретически объект без владельца остается без защиты. Как правило, владельцем ресурса является человек, который создал ресурс.

Права доступа и разрешения: эти элементы управления владелец может присвоить отдельным пользователям или группам для конкретных ресурсов [6].

Дискреционная контроля доступа могут быть применены следующим образом: списки управления доступом (ACL) назвать конкретные права и разрешения, которые назначены субъекту для данного объекта. Списки управления доступом обеспечивают гибкий способ применения дискреционных контроля доступа. Роль контроля доступа на основе членства правопреемников группы на основе организационных или функциональных ролей. Эта стратегия значительно упрощает управление правами доступа и разрешений.

Список литературы

1. Lipner S.B. Non-discretionary controls for Commercial Application. In proceeding of the 1982 symosium on security and privacy, 2001.
2. U.S. federal standard 1037C, 2001.
3. Saltzer J.H., Schroeder M.D. The protection of Information in computer system, 2004.
4. Lynch B.S., Lipner K.S. SE/VMS: Implementation mandatory security in VAX/VMS. In proceedings of the 9th National computer security conference, 2000.
5. U.S. National Information System Security Glossary, 2006.
6. Campbell J.P. Door – Access – Control System Based on finger – vein Authentication, 2006.