РЕАЛИЗАЦИЯ ОБЪЕДИНЕНИЯ МАНДАТНОГО И РОЛЕВОГО ДОСТУПА

Ю.С. Ракицкий

Омский госуниверситет им. Ф.М. Достоевского

Необходимость совмещения различных типов разграничения доступа к информации в корпоративных сетях, как правило, обусловлена требованиями политики безопасности к хранению и обработке данных. На сегодняшний день общепринятой практикой стало использование систем управления базами данных для организации доступа к ресурсам. Все современные базы данных используют концепцию ролей для выдачи полномочий пользователям, реализуя, таким образом, ролевое разграничение доступа. Однако в ряде организаций, особенно связанных с защищенным документооборотом, также налагается требование использования меток безопасности и основанного на них мандатного разделения доступа. В рамках мандатного разделения доступа множество разрешенных доступов задается неявным образом в виде уровня конфиденциальности для объектов и уровня доверия для субъектов компьютерной системы. Решение о доступе принимается путем сопоставления уровня конфиденциальности и уровня доверия. При использовании концепции ролей задается множество разрешенных системных операций путем введения дополнительных объектов – ролей, наделенных набором разрешенных доступов. Решение о разрешении доступа принимается, исходя из роли, сопоставленной субъекту.

Попытки предоставления совмещенных сервисов разграничения доступа (мандатного и ролевого) встроены в ряд систем управления базами данных. Так например, в широко распространенной СУБД Oracle уже в версии 7 было разработано дополнительное инструментальное средство Trusted Oracle7, которое позволяло администратору кроме ролей вводить также и метки безопасности. Основным требованием мандатного разграничения доступа в данном приложении было доминирование метки пользователя над меткой строки. Начиная с версии СУБД Oracle 8, этот продукт получил название Oracle Label Security. Однако оба эти продукта не получили широкой популярности в силу двух причин. Во-первых, согласование настроек двух алгоритмов приводит к большому количеству трудностей при администрировании. Во-вторых, остается не очевидной сама возможность непротиворечивого сосуществования двух принципов разграничения доступа в одной компьютерной системе.

Целью данного исследования является развитие модели ролевого разграничения доступа, а также доказательство принципиальной возможности построения политики безопасности, использующей концепцию ролей и мандатное разделение доступа. Также исследуются математические структуры, необходимые для моделирования политики безопасности.

Рассмотрим ситуацию, когда в компьютерной системе кроме ролевой политики безопасности необходимо реализовать также мандатную политику безопасности на основе некоторой решетки L. Основная проблема, возникающая в этом случае, состоит в построении правил доступа, удовлетворяющих требованиям обоих политик безопасности и не противоречащих друг другу. В первую очередь рассмотрим иерархию ролей, образующую дерево.

Теорема 1. Пусть в компьютерной системе действует ролевая политика безопасности на основе дерева ролей T и мандатная политика безопасности на основе решетки L, тогда в компьютерной системе может быть построена непротиворечивая политика безопасности, включающая в себя требования обеих политик безопасности.

Перейдем теперь к иерархии ролей, образующей произвольный ориентированный граф G.

Определение. Допустимым преобразованием ориентированного графа ролей G назовем следующий процесс: если в G имеется более одного стока, то добавляется роль, не обладающая никакими привилегиями, и дуги, ведущие от стоков графа G к новой роли.

Очевидно, что с одной стороны, такое преобразование превращает граф ролей в сеть (в случае единственности источника), а с другой, изменения ролевой политики безопасности несущественны.

Теорема 2. Если граф иерархии ролей является решеточным, либо его можно с помощью допустимого преобразования расширить до решеточного, то ролевая политика безопасности допускает непротиворечивое совмещение с мандатной политикой безопасности.

Доказательство. Расширим, если это необходимо, граф иерархии ролей до решеточного графа, обозначим его GM. Мандатная политика безопасности задается решеткой L. Тогда можно взять декартово произведение решетки, построенной на вершинах решеточного графа GM, и решетки L. Такое декартово произведение, обозначим его через GM × L, является решеткой.

Поскольку GM × L – решетка, то она может задавать мандатную политику безопасности. С другой стороны, на основании решетки GM × L можно построить решеточный граф (см. теорему 1), который будет задавать ролевую политику безопасности. Теорема доказана.

Доказательство теоремы о совмещении является конструктивным. В качестве иллюстрации предложенного алгоритма объединим ролевую политику безопасности и мандатную политику безопасности, построенную на линейном множестве из трех элементов.

Ролевая политика задается шестью ролями, одна из которых (r_0) является «пустой», то есть не обладающей какими-либо привилегиями и подчиненной любой другой роли.

Пусть мандатная политика безопасности задается решеткой L, элементами которой являются узлы l_1, l_2, l_3, причем отношение порядка задано таким образом, что $l_1 \geq l_2 \geq l_3$.

Согласно теореме, возможно непротиворечивое совмещение заданных политик безопасности. Для этого необходимо построить решетку R×L, являющуюся декартовым произведением решеток R и L, где R – решетка, определяемая решеточным графом.

Элементами решетки R×L являются пары (r_i, l_j), при i = 0,...,5 и j = 1,…,3. При этом отношение порядка задается следующим образом: $(r_i, l_j) \geq (r_k, l_m)$, если $r_i \geq r_k$ и $l_j \geq l_m$. Заметим, что узлы r_2 и r_3, r_4 и r_5, r_3 и r_4, r_3 и r_5 попарно несравнимы.

На полученной решетке R×L можно задать мандатную политику безопасности. В свою очередь, на полученном ориентированном графе можно построить ролевую политику безопасности.

Приведен частный случай объединения мандатной и ролевой политик безопасности двух компьютерных систем. Вычисление объединения произвольных политик безопасности требует распределенных вычислений. На базе суперкомпьютера Омского государственного университета возможно вычисление объединения произвольных мандатных и ролевых систем. При этом количество вычисляемых элементов зависит от мощности множества меток и мощности множества ролей. В реальных распределенных системах количество меток и ролей растет с развитием систем. Увеличение числа меток

или числа ролей приводит к увеличению вычислительных операций. Распределение таких операций позволит применить суперкомпьютер для объединения двух компьютерных систем с точки зрения безопасности. Алгоритм необходимый для вычисления объединения:

1. Вычисление декартова произведения множества ролей и множества меток.
2. Выработка отношения частичного порядка для элементов полученного множества.
3. Проверка «решеточности» полученного множества.

Литература

1. Биркгоф Г. Теория решеток. – М.: Наука. Главная редакция физико-математической литературы, 1984. – 568 с.
2. Гретцер Г. Общая теория решеток / Под редакцией Д.М. Смирнова – М.: Мир, 1981. – 456 с.
3. Новиков Ф.А. Дискретная математика для программистов – СПб.: Питер, 2001. – 304 с.
4. Терьо М. Oracle. Руководство по безопасности – М.: Издательство «ЛОРИ», 2004. – 560 с.
5. Решетки – [http://www.eltech.ru/misc/LGA_2007_FINAL/Allpage/Section8/Part8112.htm].