

Кластеризация пользователей в дискреционной модели разграничения доступа в древовидных структурах объектов

И.Б. Ларионов
larionov.igor@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация

В работе рассматриваются алгоритм объединения пользователей в группы в древовидных структурах хранения объектов, применяющихся в современных операционных системах. В рамках рассмотрения данного алгоритма предложены вспомогательные алгоритмы, позволяющие объединить пользователей в группы в системах, использующих дискреционную модель разграничения доступа. Так же представлен алгоритм выявления точек ветвления прав в древовидных структурах хранения объектов с возможностью наследования прав доступа, который позволяет уменьшить количество объектов, к которым применяются права доступа. Такой подход позволяет уменьшить матрицу доступа, оптимизация которой происходит в остальных алгоритмах, рассматриваемых в работе.

Введение

Современные информационные системы предназначены, в основном, для обмена информацией между пользователями. На малых предприятиях такой обмен производится, в случае отсутствия специально разработанной CRM или тому подобного программного обеспечения, через общие папки на сетевых хранилищах. В общем случае, разграничение доступа к ресурсам в такого рода хранилищах производится средствами имеющейся операционной системы. Подавляющее большинство операционных систем, используемых для организации сетевых хранилищ используют дискреционную модель разграничения доступа [1–4].

Естественно, что сетевые хранилища предоставляют функционал хранения данных в виде различных общедоступных папок, которые, согласно архитектуре операционной системы, имеют древовидную структуру, где каждый лист является либо конкретным файлом, либо пустой директорией, а не листовые вершины являются директории, потомками которых могут быть как файлы, так и другие директории.

При росте предприятия растет и количество пользователей, пользующихся сервисами по хранению данных в сети. Естественно, для каждого пользователя права на доступ к определенным ресурсам выдается администратором системы персонально. При достаточно большом количестве пользователей производить изменение прав доступа ко всем ресурсам какому-либо конкретному пользователю, например, при смене отдела или повышении, становится затруднительно.

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2018 (DMS-2018), Omsk, Russia, October 2018, published at <http://ceur-ws.org>

Целью данной работы является разработка алгоритма объединения пользователей в группы в дискреционной модели разграничения доступа в древовидных структурах хранения объектов.

Задачами работы, в свою очередь, являются:

1. Разработать алгоритм объединения пользователей в группы при использовании дискреционной модели разграничения доступа на большом количестве объектов.
2. Разработать алгоритм выявления «точек ветвления прав» в древовидных структурах хранения объектов, где применяется дискреционная модель разграничения доступа
3. Разработать алгоритм объединения пользователей в группы в системах, использующих дискреционную модель разграничения доступа и древовидные структуры хранения объектов.

1 Алгоритм объединения пользователей в группы при использовании дискреционной модели разграничения доступа

Данный алгоритм предназначен для объединения пользователей с одинаковыми правами на все объекты, имеющиеся в системе в группы пользователей для упрощения администрирования большого количества объектов.

Использование групп пользователей позволяет изменять права доступа, либо назначать права доступа на вновь созданный объект для всей группы пользователей, что значительно упрощает работу администратора системы в случаях с большим количеством пользователей и объектов.

В первую очередь, для работы требуется собрать информацию о всех пользователях, которые работают в системе. Следует отметить, что существуют «особые» пользователи, рассматривать которых не имеет смысла. К таким пользователям относятся, например, администратор информационной системы, сама система, а также различные вспомогательные пользователи, такие как, например, оператор резервных копий.

На следующем этапе следует собрать информацию о всех объектах в системе и выбрать все действующие права доступа к объекту для конкретного пользователя, используя список, полученный на предыдущем этапе.

Действующие права доступа следует оформить одним списком, где будут перечислены все права для каждого из объектов. Подходящим способом получения такого рода списка является декартово произведение списка всех возможных прав, которые могут применяться к любому объекту на список всех объектов системы.

Итоговую матрицу доступов следует оформлять в виде матрицы, где столбцами будут элементы декартового произведения списка всех возможных прав, которые могут применяться к любому объекту на список всех объектов системы, а строками – сами пользователи, имеющиеся в системе, за исключением «особых» пользователей.

На рисунке 1 представлена матрица доступов, в которой имеются 11 пользователей (строки) и 3 права доступа (столбцы). X показывает, что пользователь, которому соответствует данная строка имеет данное право доступа к данному объекту.

На следующем этапе требуется отсортировать столбцы полученной матрицы в порядке не возрастания количества X в столбце, т.е. сделать самым левым столбцом то право на конкретный объект, которое имеет наибольшее количество пользователей. Пример получившейся матрицы можно посмотреть на рисунке 2. В данном примере столбцы 1 и 2 поменялись местами, т.к. в матрице, представленной на рисунке 1, в первом столбце имелось 7 символов X , во втором – 9, а в третьем – 6.

На следующем этапе следует произвести сортировку строк матрицы в лексикографическом порядке. Предлагается использовать следующий подход: строка, имеющая в соответствующей ячейке символ X должна располагаться выше строки, где соответствующая ячейка пуста, т.е. при сравнении, наличие символа является меньшим значением, чем его отсутствие.

На рисунке 3 представлена матрица с рисунка 2, к которой применили такого рода лексикографическую сортировку. Как видно из рисунка, пользователи, имеющие максимальный набор прав, заняли высшие строки матрицы, а пользователи с меньшими наборами прав расположились ниже.

На следующем этапе следует провести группировку строк по принципу идентичности набора символов X в строке. На рисунке 4 представлена матрица из рисунка 3, в которой цветом выделены нечетные по счету группы пользователей.

x	x	x
	x	x
x	x	x
	x	
	x	
x		
x		x
x	x	
x	x	x
x	x	
	x	x

Рис. 1: Исходные права доступа

Таким образом, применив только два алгоритма сортировки и однопроходный алгоритм сравнения, можно выделить группы пользователей, имеющих идентичные права в системе.

После получения данных групп, следует внести пользователей в соответствующие группы в информационной системе и переназначить права на объектах в соответствии с группами пользователей, после чего права на конкретных пользователей удалить с обработанных объектов.

2 Алгоритм выявления «точек ветвления прав» в древовидных структурах хранения объектов

Данный алгоритм предназначен для выявления точек на дереве объектов, где происходит изменение прав доступа. Эти данные необходимы для корректного назначения прав на группы объектов.

Для начала необходимо построить дерево всех объектов в системе. Все узлы дерева должны содержать весь набор эффективных прав доступа к соответствующему объекту для всех пользователей в системе.

На следующем этапе необходимо обработать все листья получившегося дерева. Следует начать с тех листьев, которые являются предками одной и той же вершины. Обработки предлагается вести следующим образом: все листья с идентичными наборами прав доступа объединить в новую вершину, указав при этом для нее тот же набор прав доступа.

На третьем этапе следует для всех пар «лист-потомок» проверить, являются ли права доступа идентичными. В случае, если они являются таковыми, объединить в одну вершину, при условии, что у предка нет других потомков. При объединении у вновь образованной вершины дерева следует указать права доступа те же, что и у объединенных вершин.

Предыдущие два этапа следует повторять до тех пор, пока хотя бы на одном этапе произошло объединение вершин.

3 Алгоритм объединения пользователей в группы в системах, использующих дискреционную модель разграничения доступа и древовидные структуры хранения объектов

Данный алгоритм направлен на получение корректного и малого набора групп пользователей и групп объектов, которые позволят, не нарушая существующих прав доступа, эффективно и просто администрировать права доступа к объектам, имеющих древовидную структуру для большого количества пользователей.

На первом этапе требуется получить дерево объектов, которое выдает алгоритм выявления «точек ветвления прав» в древовидных структурах хранения объектов. Дальнейшую обработку следует вести, используя в качестве объектов дискреционной политики разграничения прав доступа вершины полученного дерева.

X	X	X
X		X
X	X	X
X		
X		
	X	
	X	X
X	X	
X	X	X
X	X	
X		X

Рис. 2: Права доступа, упорядоченные по количеству пользователей

На втором этапе необходимо произвести объединение пользователей в группы с использованием алгоритма объединения пользователей в группы при использовании дискреционной модели разграничения доступа. На вход данного алгоритма в качестве набора объектов системы с правами доступа предлагается подавать список вершин с соответствующими правами доступа, полученными с использованием алгоритма выявления «точек ветвления прав» в древовидных структурах хранения объектов.

На следующем этапе следует проверить все не листовые вершины дерева на предмет того, что права доступа к этому объекту представляют собой объединение прав доступа ко всем дочерним объектам. В случае, если имеется такая ситуация, эти объекты следует отметить для установки новых групповых прав.

В итоге, после получения списка групп пользователей и списка объектов, имеющих групповые права доступа, следует применить новые права доступа с учетом ситуаций, отмеченных на предыдущем этапе.

Заключение

В заключении следует отметить, что предложенные алгоритмы дополняют друг друга.

Алгоритм объединения пользователей в группы при использовании дискреционной модели разграничения доступа является достаточно громоздким в реализации, т.к. получаемая в ходе его работы матрица доступов может иметь миллионы столбцов, что может крайне негативно отразиться на скорости работы данного алгоритма.

Алгоритм выявления «точек ветвления прав» в древовидных структурах хранения объектов позволяет уменьшить количество объектов в системе, которые будут обрабатываться в ходе изменения прав доступа и выявлении групп пользователей, что, несомненно, скажется положительно на скорости работы алгоритма объединения пользователей в группы при использовании дискреционной модели разграничения доступа.

Алгоритм объединения пользователей в группы в системах, использующих дискреционную модель разграничения доступа и древовидные структуры хранения объектов позволяет правильно подготовить данные для алгоритма объединения пользователей в группы при использовании дискреционной модели разграничения доступа, используя алгоритм выявления «точек ветвления прав» в древовидных структурах хранения объектов.

Список литературы

- [1] M. Abrams et al. Information Security: An Integrated Collection of Essays. *IEEE Comp.*, 1995.
- [2] W. Boebert, R. Kain. A Practical Alternative to Hierarchical Integrity Policies. *Proceedings of the 8th National Computer Security Conference*, 1985.
- [3] B. Lampson et al. Authentication in Distributed Systems: Theory and Practice. *Proceedings of the 13th ACM Symposium on Operating Systems Principles*, 1992.

X	X	X
X	X	X
X	X	X
X	X	
X	X	
X		X
X		X
X		
X		
	X	X
	X	

Рис. 3: Состояние матрицы доступов после лексикографической сортировки

- [4] D. Mazieres, M. Kaashoek. Secure Applications Need Flexible Operating Systems. *Proceedings of the 6th Workshop on Hot Topics in Operating Systems*, May 1997.

Clustering Users in the Discretionary Model of Access Control in Tree Structures of Objects

Igor B. Larionov

The paper discusses the algorithm for combining users into groups in the tree-like structures for storing objects used in modern operating systems. Within the framework of consideration of this algorithm, auxiliary algorithms have been proposed that allow users to be grouped into groups in systems that use the discretionary model of access control. Also, an algorithm is presented for identifying right branch points in the tree-like structures for storing objects with the possibility of inheriting access rights, which allows reducing the number of objects to which access rights are applied. This approach allows us to reduce the access matrix, which is optimized in the other algorithms considered in the paper.

x	x	x
x	x	x
x	x	x
x	x	
x	x	
x		x
x		x
x		
x		
	x	x
	x	

Рис. 4: Группировка пользователей по правам доступа