MATHEMATICA MONTISNIGRI
Vol XXIX (2014)

О РЕГУЛИРОВАНИИ РОЛЕЙ ПОЛЬЗОВАТЕЛЕЙ В МОДЕЛИ РАЗГРАНИЧЕНИЯ ДОСТУПА СИСТЕМЫ УДАЛЕННОГО УПРАВЛЕНИЯ ДАННЫМИ

Л.С. БЕРБЕРЯН*

* Российско-Армянский (Славянский) университет
Ереван, Армения
e-mail: levon711@mail.ru

Ключевые слова: Модель управления доступом, система удаленного управления данными, ролевая модель, информационная безопасность

Аннотация. В данной работе описывается методика реализации инструментов для управления ролями в модели, предназначенной для разграничения доступа системы удаленного управления данными.

ON THE REGULATION OF USER ROLES IN THE ACCESS CONTROL MODEL FOR REMOTE DATA MANAGEMENT SYSTEM

L. BERBERYAN*

* Russian-Armenian (Slavonic) University, Yerevan, Armenia
Yerevan, Armenia
e-mail: levon711@mail.ru

Summary. This paper describes a method of roles managing tools implementation of the model, designed to restrict access to remote data management system.

2010 Mathematics Subject Classification: 97P20, 97P30, 97R70.
Key words and Phrases: Access control model, remote data management system, role-based model, information security.

1 ВВЕДЕНИЕ

Методика, описываемая в данной работе, адаптирована для работы с вариацией ролевой модели, представленной ранее[1], которая предназначается для управления привилегиями в информационной системе, ресурсы которой представлены с помощью одной из разновидностей файловой системы, а сама она была разработана для решения задачи обеспечения удаленного доступа к данным на основе клиент-серверной архитектуры.

2 АДМИНИСТРАТИВНЫЕ РОЛИ

Ранее было приведено описание модели для управления ресурсами[2], с помощью которой можно решить задачи разграничения доступа. В ее рамках были введены и описаны понятия ресурсов и операций доступа к ним, пользователей и соответствующих ролей, ассоциируемых с ними, однако вне ее рамок остались такие функции, как создание ролей, их назначение и отзыв. В рамках стандартов ролевых моделей[3] принято вводить понятие административных ролей, выполняющих подобные операции.

В силу того, что описываемая в работе модель базируется на ролевой[4], все термины по управлению структурой будем рассматривать в ее рамках. Для выполнения задач, упомянутых выше, в модель добавим соответствующий требованиям новый тип ролей, условно называемых административными. Данное разделение ролей на несколько разновидностей, каждая из которых служит своей общей группе целей, позволит более прозрачно демонстрировать состояние системы, обеспечить более гибкое и удобное управление ее структурой.

Разделение ролей и административных ролей позволяет более четко передать реальную картину иерархий в группах и организациях. Ведь даже если сама группа находится на более высоком уровне привилегий, чем какая-то другая, это еще не значит, что все ее члены вправе управлять иерархией группы на более низком уровне.

3 ФУНКЦИОНАЛ АДМИНИСТРАТИВНЫХ РОЛЕЙ

Для начала вспомним функционал, предоставляемый в рамках стандарта ролевой модели[5]. В стандарте ролевой модели для управления ролями используются следующие функции, заданные для каждой административной роли:

- функция, с помощью которой определяется множество ролей, которые могут быть ею назначены пользователям системы при выполнении некоторых предварительных условий;
- функция, с помощью которой определяется множество ролей, которые могут быть ею отозваны у пользователей системы, опять же при выполнении некоторых предварительных условий.

Таким образом, для каждой административной роли в модели определим несколько следующих функций, исходя из стандартов ролевой модели и конструкции модели в данном конкретном случае:

- функция AssignRole, имеющая два параметра, среди которых роль и пользователь, назначаемый на нее, с помощью которой уполномоченный пользователь с

административной ролью может назначить роль из множества заданных ролей R пользователю из множества зарегистрированных в системе пользователей U;
- функция RevokeRole, имеющая два параметра, среди которых роль и пользователь, у которого она отзывается, с помощью которой уполномоченный пользователь с административной ролью может отозвать роль из множества ролей R, ассоциируемых с пользователем из множества зарегистрированных в системе пользователей U.

В силу того, что в нашем случае ролевая модель модифицированная, что означает присутствие дополнительных элементов, введем некоторые параметры для вышеопределенных функций, необходимые для работы с ними.

Определим сперва параметры роли:
- параметр RoleID, который однозначным образом указывает на роль;
- параметр RoleT, с помощью которого определяется время, в которое роль будет активна для пользователя;
- параметр RoleP, определяющий множество привилегий, относящихся к роли, и, в случае необходимости, также зависящий от временных параметров.

Для самого пользователя задается его идентификатор UserID, позволяющий однозначным образом указать на него.

В функционал административных ролей также могут входить следующие функции:
- функция AssignAdministrativeRole, имеющая два параметра, среди которых административная роль и пользователь, назначаемый на нее, с помощью которой уполномоченный пользователь с административной ролью может назначить административную роль из множества заданных ролей AR пользователю из множества зарегистрированных в системе пользователей U;
- функция RevokeAdministrativeRole, имеющая два параметра, среди которых административная роль и пользователь, у которого она отзывается, с помощью которой уполномоченный пользователь с административной ролью может отозвать административную роль из множества ролей AR, ассоциируемых с пользователем из множества зарегистрированных в системе пользователей U.

По аналогии с обыкновенными ролями введем соответствующие этим функциям параметры.

Для административной роли зададим следующие параметры:
- параметр AdministrativeRoleID, который однозначным образом указывает на административную роль;
- параметр AdministrativeRoleT, с помощью которого определяется время, в которое административная роль будет активна для пользователя;
- параметр AdministrativeRoleP, определяющий множество привилегий для административной роли и, в случае необходимости, также зависящий от временных параметров.

Для самого пользователя опять же задается его идентификатор UserID, позволяющий однозначным образом указать на него.

4 ИЕРАРХИЯ АДМИНИСТРАТИВНЫХ РОЛЕЙ

Для административных ролей по аналогии с обыкновенными определено понятие уровня L_j, j=1,2,...n, где n-количество уровней, определенных на данный момент, позволяющее определить иерархию для них.

Административные роли могут быть связаны между собой отношениями наследования. В таком контексте административная роль на более высоком уровне имеет доступ к ролям на более низком уровне в случае, если они входят друг с другом в отношениях типа предок-потомок, где административная роль на более высоком уровне в соответствующей цепочке наследования является предком для находящейся на более низком уровне.

На одном уровне может присутствовать произвольное количество административных ролей, независимых друг от друга, то есть для любых двух из них $AR(x, L_j)$ и $AR(y, L_k)$ выполняется условие $AR(x, L_j) \neq AR(y, L_k)$. Подобное расположение позволяет отразить связи между членами в реальных группах.

5 АВТОМАТИЗАЦИЯ НЕКОТОРЫХ ПРОЦЕССОВ

Одной из особенностей классической ролевой модели, а также большинства ее производных является то, что назначение и отзыв ролей выполняются полностью вручную группой администраторов системы. В случае управления нагроможденными ролями системами, существование которых оправдано сложной структурой данных во многих организациях даже среднего масштаба, возникают проблемы, связанные как с задержкой принятия решений администраторами, так и с большими затратами ресурсов для создания команды администраторов, а также понижением уровня безопасности в силу нагруженности задачами и сроками их выполнения, что может привести к большей вероятности ошибок при принятии решений. В связи с подобными проблемами предлагается ввести в элементы управления описанные выше, механизмы автоматизации, позволяющие упростить процессы, связанные с администрированием ролей, понизив требования к ресурсам при реализации системы и при этом повысив безопасность.

Для добавления механизма автоматизации, модифицируем само построение структуры. Модифицируем и рассмотрим процесс инициализации, процессы добавления ресурсов, ролей, административных ролей и соответственно процессы их удаления.

5.1 Инициализация модели

Опишем сперва процесс инициализации модели, условно разбив его на несколько этапов: 1)построение дерева классов, 2)построение дерева ролей, 3)построение дерева административных ролей, 4)создание учетных записей пользователей информационной системы. Разберем подробнее эти этапы.

1 этап. Первоначально в системе могут быть заданы ресурсы, представленные в нашем случае в виде файлов. Ресурсы описываются с помощью классов данных и ассоциируются с соответствующими буферами для непосредственной работы с ними. В случае присутствия групп и подгрупп ресурсов, представленных, например, в виде директорий автоматически строятся уровни для классов.

2 этап. Согласно модели параллельно с деревом классов данных строится дерево ролей. На данном этапе оно представляет собой лишь одну роль, которая находится на самом

высоком уровне иерархии и соовтетственно обладает всеми привилегиями в соответствующей структуре.

3 этап. Наряду с деревом ролей строится дерево административных ролей. Как и дерево ролей на данном этапе оно представляет собой лишь одну административную роль, которая находится на самом высоком уровне иерархии и соовтетственно обладает всеми привилегиями в соответствующей структуре.

4 этап. В процессе инициализации создается одна учетная запись пользователя с наивысшими привилегиями, ему назначается соответствующая созданная роль с максимальными привилегиями, а также административная роль с максимальными привилегиями. Впоследствии владелец этой учетной записи уже лично сможет расширить круг ресурсов, пользователей, соответствующих им обыкновенных и административных ролей.

Во время создания нового ресурса или же при загрузке в нее существующего извне в системе автоматически создается новый класс, соответствующий ему с набором привилегий, доступных в рамках среды, ассоциируемым буфером. При создании можно редактировать сами привилегии, отключив некотороые из них или же ограничив с помощью временных переменных.

Соответственно при удалении ресурса автоматически удаляется и класс с его описанием и соответствующим буфером, так как его существование уже лишается какого-либо смысла. При этом, если задана роль на той же позиции и том же уровне, то и она удаляется, как и административная роль с теми же данными.

5.2 Создание и удаление ролей

Роли в системе создаются вручную и соответственно настраиваются пользователями с административными ролями.

Административные роли дают право на создание обыкновенных ролей с соответствующим уровнем и позицией, либо дочерней по отношению к ней, в противном случае присутствие административной роли не будет оправдано.

Если требуется создать роль на несколько уровней ниже уже созданной, то в промежутке для сохранения порядка иерархии автоматически создаются пустые роли на соответствующих уровнях и позициях.

При удалении роли в случае необходимости, то есть в случае присутствия дочерних для нее, которые после этой операции не должны быть затронуты, на место удаляемой автоматически вставляется пустая для сохранения целостности иерархии.

Административные роли в системе также создаются вручную пользователями с административными правами и имеющими полномочия на проведение подобных операций.

При создании административной роли на несколько уровней ниже уже созданной в промежутке для сохранения порядка иерархии автоматически создаются пустые административные роли на соответствующих уровнях и позициях.

В случае удаления административной роли при необходимости, то есть в случае присутствия дочерних для нее, которые после этой операции не должны быть затронуты, на место удаляемой автоматически вставляется пустая для сохранения целостности иерархии.

Не все административные роли имеют право на создание и удаление подобных, так как на практике не всегда член административной команды может иметь право привлекать новых членов или отзывать старых, пусть даже они находятся в более низких по отношению к нему позициях в общей с ним цепочке.

6 ЗАКЛЮЧЕНИЕ

Таким образом, в данной работе была описана методика реализации управления ролями в модели, предназначенной для разграничения доступа системы удаленного управления данными, были введены и описаны соответствующие типы ролей, функционал, связанный с ними, а также была проведена автоматизация некоторых происходящих при этом процессов.

REFERENCES

[1] L.S.Berberyan, "About one Extended Role-based Access Control Formal Model", Computer Science and Information Technologies Conference, Armenia, Yerevan, 99-102(2013).
[2] Л.С.Берберян, "Разработка и реализация модели информационной системы с возможностью управления доступом", Вестник РАУ, Армения, Ереван, 42-48(2012).
[3] R.S.Sandhu, V.Bhamidipati and Q.Munawer, "The ARBAC97 model for role-based aministration of roles", ACM Trans. Information and Systems Security, No. 2(1), NewYork, ACM Publishing, 105–135(1999).
[4] D. F.Ferraiolo, D. R.Kuhn, "Role Based Access Control", 15th National Computer Security Conference, 554–563(October 1992).
[5] R.Sandhu, D.F.Ferraiolo and D.R.Kuhn, "The NIST Model for Role Based Access Control: Toward a Unified Standard", *5th ACM Workshop Role-Based Access Control*: 47—63(July 2000).

Поступила в редакцию 15 января 2014 года