Управление доступом на основе ролей

Управление доступом на основе ролей (англ. Role Based Access Control, RBAC) — развитие политики избирательного управления доступом, при этом права доступа субъектов системы на объекты группируются с учётом специфики их применения, образуя роли.

Формирование ролей призвано определить чёткие и понятные для пользователей компьютерной системы правила разграничения доступа. Ролевое разграничение доступа позволяет реализовать гибкие, изменяющиеся динамически в процессе функционирования компьютерной системы правила разграничения доступа.

Такое разграничение доступа является составляющей многих современных компьютерных систем. Как правило, данный подход применяется в системах защиты СУБД, а отдельные элементы реализуются в сетевых операционных системах. Ролевой подход часто используется в системах, для пользователей которых чётко определён круг их должностных полномочий и обязанностей.

Несмотря на то, что Роль является совокупностью прав доступа на объекты компьютерной системы, ролевое управление доступом отнюдь не является частным случаем избирательного управления доступом, так как его правила определяют порядок предоставления доступа субъектам компьютерной системы в зависимости от имеющихся (или отсутствующих) у него ролей в каждый момент времени, что является характерным для систем мандатного управления доступом. С другой стороны, правила ролевого разграничения доступа являются более гибкими, чем при мандатном подходе к разграничению[1].

Так как привилегии не назначаются пользователям непосредственно и приобретаются ими только через свою роль (или роли), управление индивидуальными правами пользователя по сути сводится к назначению ему

ролей. Это упрощает такие операции, как добавление пользователя или смена подразделения пользователем[3].

История

Элементарные формы модели RBAC были осуществлены во множестве специальных форм на многих системах, начиная с 1970-х годов. Контроль доступа на основе ролей, используемый в настоящее время происходит из модели, предложенной Феррайоло (англ. Ferraiolo) и Куном (англ. Kuhn) (1992) и как образцовая модель позже усовершенствованная Санди (англ. Sandhu), Койн, Фейнштейн и Йоман (1996).

- 1992 год — статья Феррайоло и Куна, определяющая RBAC посредством доступа только через роли, иерархии и ограничения. формальная модель [6];
- 1994 год — DTOS базировал опытный образец RBAC, на прототипе модели, предложенной Феррайоло, Кун, Гаврилья (англ. Gavrila)
- 1994 год — статья Nyanchama и Osborn определяет модель;
- 1994 год — IBM подаёт (в Европе) первую заявку на патент в области RBAC, цитирующую Феррайоло и Куна;
- 1995 год — Феррайоло, Кугини (англ. Cugini), Кун расширили формальную модель, введя определение форм разделения обязанностей [5];
- 1996 год — метод Санди для того, чтобы осуществить MAC на основе RBAC;
- 1997—1998 годы — Sybase, Безопасное Вычисление, Siemens объявляет о продуктах RBAC, описанных как базирующиеся непосредственно на модели
- 1997 год — безопасное вычисление включает модель Феррайоло-Куна RBAC в американскую Глобальную Команду DoD и Систему управления; выходит статья Куна на тему разделения обязанностей, необходимых и достаточных условий для безопасности разделения;
- 1997 год — статья Осборна основанная на отношениях между RBAC и многоуровневой безопасностью мандатной модели политики безопасности; аннотация роли, связывающая RBAC и многоуровневую безопасность [4];
- 1998 год — RBAC — метод Куна для того, чтобы осуществить RBAC на системе MAC;
- 1999 год — Барклей (англ. Barkley), Феррайоло, Кун открывают исходный опытный образец RBAC для развитых веб-серверов;

- 2000 год — Санди, Феррайоло, Кун публикуют статью, определяющую объединенную модели RBAC, и предлагают стандарт RBAC;
- 2004 год — Американский национальный институт стандартов и Международный комитет по стандартам информационных технологий (ANSI/INCITS) принимают предложенную Санди, Феррайоло и Куном модель RBAC как единый стандарт.

  Базовая модель RBAC

Для определения модели RBAC используются следующие соглашения:

S = Субъект (англ. Subject) = Человек или автоматизированный агент (множество пользователей);

R = Роль (англ. Role) = Рабочая функция или название, которое определяется на уровне авторизации (множество ролей);

P = Разрешения (англ. Permissions) = Утверждения режима доступа к ресурсу (множество прав доступа на объекты системы);

SE = Сессия (англ. Session) = Соответствие между S, R и/или P

SA = Назначение субъекта (англ. Subject Assignment)

PA: $R \rightarrow 2^p$ — функция, определяющая для каждой роли множество прав доступа; при этом для каждого $p \in P$ существует $r \in R$ такая, что $p \in PA(r)$; (англ. Permission Assignment)

RH = Частично упорядоченная иерархия ролей (англ. Role Hierarchy). RH может быть еще записана так: ≥

Один субъект может иметь несколько ролей.

Одну роль могут иметь несколько субъектов[2].

Одна роль может иметь несколько разрешений[2].

Одно разрешение может принадлежать нескольким ролям.

Роли назначаются субъектам, вследствие чего субъекты получают те или иные разрешения через роли. RBAC требует именно такого назначения, а не

прямого - назначение разрешений субъектам, иначе это приводит к сложно контролируемым отношениям между субъектами и разрешениями.

На возможность наследования разрешений от противоположных ролей накладывается ограничительная норма, которая позволяет достичь надлежащего разделения режимов. Например, одному и тому же лицу может быть не позволено создать учётную запись для кого-то, а затем авторизоваться под этой учётной записью.

Используя нотацию теории множеств:

$PA\underline{c}PxR$ при этом разрешения назначаются связям ролей в отношении «многие ко многим».

$SA\underline{c}SxR$ при этом субъекты назначаются связям ролей и субъектов в отношении «многие ко многим».

$$RH\underline{c}RxR$$

Обозначение: x ≥ y означает, что x наследует разрешения y.

Субъект может иметь множество одновременных сессий с различными разрешениями [1].

Корреляция развития RBAC и закона Мура

Для выявления корреляции были использованы даты развития модели распределения доступа RBAC и даты закона мура и его расширенных версий.

В инструментом расчета был использован Microsoft Office Excel. Коэффициент корреляции равен 0.97177

Список литературы

1. Управление доступом на основе ролей, [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Управление_доступом_на_основе_ролей.
2. RBAC Авторизация в YII и LDAP, [Электронный ресурс]. – Режим доступа: https://habr.com/ru/post/177873/
3. Доступ к сайту на основе ролей (RBAC) в Yii2, [Электронный ресурс]. – Режим доступа: https://klisl.com/rbac.html
4. Role Based Access Control on the World Wide Web, [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/CSRC/media/Projects/Role-Based-Access-Control/documents/web_servers/rbac-web.pdf
5. Role-Based Access Controls , [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1992/10/13/role-based-access-controls/documents/ferraiolo-kuhn-92.pdf
6. Role-Based Access Control Models, [Электронный ресурс]. – Режим доступа: https://csrc.nist.gov/CSRC/media/Projects/Role-Based-Access-Control/documents/sandhu96.pdf