Обзор и сравнительный анализ моделей разграничения доступа на основе атрибутов (ABAC) и на основе ролей (RBAC)

Лифантьев Данил

5 декабря 2022 г.

Содержание

1 Введение

В большинстве информационных систем пользователи, прежде чем получить доступ к полному функционалу системы, должны быть аутентифицированы и авторизованы, иначе это может привести к нарушениям безопасности. Авторизацией называют процесс предоставления прав доступа на выполнение определенных действий. В данной статье рассматриваются наиболее популярные модели управления доступом: на основе атрибутов и на основе ролей. Целью статьи является их общее описание и проведение сравнения между двумя подходами для лучшего понимания преимуществ, подходящих условий применения и недостатков каждого из них.

2 Разграничение доступа на основе атрибутов

Разграничение доступа на основе атрибутов (англ. Attribute-Based Access Control, ABAC) — это метод разграничения доступа, при котором запросы субъекта на выполнение операций над объектами разрешаются или отклоняются на основе следующих параметров: атрибутов субъекта, атрибутов объекта, состояния системы и набора политик, указанных в терминах этих атрибутов и условий.

- Атрибуты – это характеристики субъекта, объекта или состояния системы.
- Субъект — это пользователь, устройство или приложение, которое запрашивает доступ для выполнения операций с объектами. Субъектам присваивается один или несколько атрибутов.

- Объект — это ресурс, с избирательным доступом, например устройства, файлы, сети или домены, содержащие или получающие информацию.
- Операция — это выполнение действия субъекта над объектом. Среди операций могут быть такие, как чтение, запись, редактирование, удаление, копирование и другие.
- Политика — это представление правил, которое позволяет определить должен ли быть разрешен доступ, учитывая значения атрибутов субъекта, объекта и состояния системы.
- Состояние системы — это операционный контекст, в котором возникают запросы на доступ. Состояние системы должно определяться некоторыми значимыми характеристиками, независящими от субъекта или объекта, например, оно может включать в себя текущее время, местоположение пользователя или текущий уровень угрозы.

Таким образом разграничение доступа на основе атрибутов имеет довольно большой набор параметров и их комбинаций, исходя из которых принимается решение о предоставлении доступа. Это факт делает подход разграничения доступа на основе атрибутов высоко динамичной моделью, поскольку политики, пользователи и объекты могут предоставляться независимо друг от друга, а само решение по выдаче доступа осуществляется в момент запроса.

3 Разграничение доступа на основе ролей

В рамках приведенных определений можно сказать, что разграничение доступа на основе ролей (англ. Role-Based Access Control, RBAC) является частными случаями модели ABAC. Модель RBAC использует предварительно определенные роли. Они несут некоторый набор, связанных с ними, привилегий, и также им в соответсвие назначены субъекты. Поэтому роль можно рассматривать как атрибут субъекта, определенный в данной модели, вокруг которого генерируется политика доступа к объектам.

По сути, роль — это набор разрешений, которые можно применять к пользователям. Использование ролей упрощает добавление, удаление и настройку прав доступа, по сравнению с предоставлением доступа пользователям по отдельности. При использовании RBAC для разграничения доступа анализируется потребность множества субъектов и производится их группировка по ролям на основе общих обязанностей. Могут быть назначены от одной до нескольких ролей каждому субъекту, а для каждой роли закрепляется от одного до нескольких прав доступа.

4 Преимущества и недостатки модели RBAC

4.1 Преимущества

Основное преимущество разграничения доступа на основе ролей заключается в том, что эта модель получила широкое распространение и позволяет организациям малого и среднего размера отказаться от реализации индивидуального разграничения доступа. Поскольку политики RBAC могут быть написаны на основе реально существующих в организации ролей, их легко формализовать и назначить. Гибкость данного подхода заключается в том, что при приходе новых сотрудников или внутреннем изменении ролей в системе не требуется создания новой политики, так как эти сценарии могут быть обработаны назначением новых или обновлением существующих ролей.

Кроме того, одному пользователю может быть назначено несколько ролей, которые могут иметь иерархическую структуру. Например, менеджер в организации, в рамках модели RBAC, имеющий роль «отдел кадров», также может иметь роль «менеджер». В этом случае данный субъект будет иметь больше прав доступа, чем его непосредственные подчинённые, имеющие лишь роль «отдел кадров».

Так как данная модель предполагает заблаговременное создание политик и назначение ролей для всех операций в системе, требующих авторизацию, при удачном планировании

это во многих случаях позволяет обойтись единственной крупной настройкой разграничения доступа в системе, с возможными небольшими обновлениями её в будущем, что очень удобно.

4.2 Недостатки

Особенность модели разграничения доступа на основе ролей, которая упрощает процесс её настройки в системе, также является одним из её самых больших ограничений. Для малых и средних организаций RBAC может быть управляемым, однако по мере роста числа пользователей и ролей работа по настройке и обновлению функциональных составляющих модели сильно усложняется, особенно при использовании иерархического подхода. Это означает что возможна ситуация, где для обеспечения всех поставленных требований к разграничению доступа в системе могут потребоваться сотни или тысячи ролей. Например, чтобы контролировать доступ к данным в таблицах или базах данных. Эта трудоемкая обязанность поддержки сложной системы сводит на нет основную причину внедрения RBAC — экономию времени и ресурсов для поддержки функциональности разграничения доступа.

Большое количество ролей в системе создает ситуацию, в которой администратор больше не может с легкостью понять, какие роли принадлежат каким разрешениям на доступ, поэтому преобразование потребности пользователя в фактическое назначение роли может быть очень сложным. Поскольку нет гарантий будущих изменений в системе, администраторы всегда должны помнить о возможной необходимости обновления политик при любых изменениях данных или организационной структуры.

Кроме того, RBAC по своей сути пренебрегает принципом наименьших привилегий. Он гласит, что субъектам должен быть предоставлен доступ только к тем объектам, которые необходимы для выполнения текущей задачи, и не более того. Грубый контроль доступа, предлагаемый в рамках модели RBAC, не позволяет автоматически устанавливать разрешения в зависимости от потребностей пользователя в определенный момент времени. Каждое настраиваемое разрешение становится новой ролью, способствуя упомянутому ранее взрывному увеличению числа ролей.

5 Преимущества и недостатки модели ABAC

5.1 Преимущества

Разграничение доступа на основе атрибутов использует разнообразные комбинации уникальных атрибутов субъектов и объектов, чтобы определить, предоставлять или запрещать доступ к данным. В отличие от статической модели разграничения доступа на основе ролей, многомерный подход ABAC делает процесс доступа к ресурсам более динамичным. При изначальной настройке системы в рамках этой модели, определяются все необходимые атрибуты и для них создаются политики, но после того, как они назначены системным компонентам, система требует минимального обслуживания. Это позволяет избежать ручного создания ролей и последующего значительного увеличения их числа, делая данный подход к разграничению доступа более масштабируемым. Одна политика в модели ABAC может заменить несколько десятков отдельных ролей, которые были бы необходимы для достижения того же результата при использовании подхода RBAC.

Хоть одна из категорий атрибутов ABAC и относится к характеристикам(ролям) пользователей, в отличие от RBAC они учитываются наряду с другими определяющими факторами системы. Таким образом, разграничение доступа на основе атрибутов предоставляет больше переменных управления, чем разграничение доступа на основе ролей, делая доступ к ресурсам в системе более безопасными, что удовлетворяет принципу наименьших привилегий. Это означает, что администраторы системы с моделью ABAC могут быть более уверенными, что данные не будут чрезмерно доступны для субъектов, которым не следует иметь к ним доступ. Также наличие меньшего количества политик для конкретных отношений объектов и субъектов упрощает управление системой и ее мониторинг. Например, позволяя производить усиление политик и их проверку, тем самым снижая вероятность того, что доступ к каким-либо конфиденциальным ресурсам будет получен неправомерными пользователями.

В отличие от модели RBAC, в которой роль объединяет то, кем является пользователь, с тем, какой доступ у него должен быть, в модели ABAC есть разделение между атрибутами объектов и субъектов. Именно эта особенность делает ABAC более динамичным.

5.2 Недостатки

В то время как разграничение доступа на основе ролей легче при первоначальной настройке, но сложнее при масштабировании; разграничение доступа на основе атрибутов имеет противоположные свойства: сложнее при настройке, но легче для масштабирования. Это связано с тем, что администраторам системы сначала поручается определить стандарт для определения политик доступа к ресурсам, а затем создать и единообразно реализовать эти политики в каждой из частей, как правило большой, системы.

Список литературы

[1] Vincent C. Hu, etc. - *Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, National Institute of Standards and Technology, 2014.

[2] William Fisher - *Attribute Based Access Control*, National Institute of Standards and Technology, 2015.

[3] Калимолдаев М.Н., Бияшев Р.Г. - *Анализ методов атрибутного разграничения доступа*, Институт информационных и вычислительных технологий, 2019.

[4] Ferraiolo D. F., Kuhn D. R. - *Role Based Access Control*, 15th National Computer Security Conference, 1992.