Литература

1. Мащенко П.Л., Пилипенко М.О. Технология Блокчейн и ее практическое применение // Наука, техника, образование. – 2017. – №32. – С. 61-64.
2. Melanie S. Blockchain: Blueprint for a New Economy. – Boston: O'Reilly Media, Inc., 2015. – 152 p.
3. Архипов А.О, Гизатуллин З.М. Применение технологии блокчейн в системах автоматизированного проектирования электронных средств // Современные материалы, техника и технология: Сб. науч. статей 7-й Междунар. науч.-практ. конф. – 2017. – С. 21-25.
4. Тахаутдинов Р.Ш. Многослойные печатные платы. Первые шаги в освоении операции прессования // Технологии в электронной промышленности. – 2010. – №3. – С. 28-31.
5. Гизатуллин З.М. Анализ электромагнитной обстановки внутри зданий при воздействии разряда молнии // Известия высших учебных заведений. Проблемы энергетики. – 2008. – №1-2. – С. 38-47.
6. Гизатуллин З.М., Гизатуллин Р.М., Зиатдинов И.Н. Анализ функционирования вычислительной техники при воздействии электромагнитных помех по сети электропитания // Известия высших учебных заведений. Проблемы энергетики. – 2015. – №7-8. – С. 98-105.
7. Гизатуллин З.М., Фазулянов Ф.М., Шувалов Л.Н., Гизатуллин Р.М. Целостность информации в USB флэш-накопителе при воздействии импульсного магнитного поля // Журнал Радиоэлектроники. 2015. – №8. – С. 8.
8. Гизатуллин З.М., Гизатуллин Р.М., Нуриев М.Г. Методика физического моделирования воздействия разряда молнии на летательные аппараты // Известия вузов. Авиационная техника. – 2016. – №2. – С. 3-6.
9. Гизатуллин З.М., Нуриев М.Г., Шкиндеров М.С., Назметдинов Ф.Р. Простая методика исследования электромагнитного излучения от электронных средств // Журнал радиоэлектроники. – 2016. – №9. – С. 7.

А.И. Белоусов, Т.А. Щетинина

ПРИМЕНЕНИЕ АТРИБУТИВНОГО ПОДХОДА РАЗГРАНИЧЕНИЯ ПРАВ ДОСТУПА К УНИФИЦИРОВАННЫМ ФРЕЙМОВЫМ СТРУКТУРАМ ХРАНЕНИЯ ДАННЫХ

(Самарский университет)

В настоящее время, в основном, используются два способа для разграничения прав доступа: атрибутивный (ABAC) и ролевой (RBAC) [1]. Наиболее распространенным и широко используемым является ролевой контроль доступа, так как его реализация более проста и понятна. При авторизации пользователя в системе в соответствии с бизнес-правилом ему присваивается роль, в соответствии с которой он получает доступ только к определенным ресурсам и

видит только ту информацию, которая с ними связана. На основе этих ролей проверяется возможность выполнения пользователем того или иного действия.

Но бизнес-правила неизбежно усложняются и становятся многомерными. Это приводит к тому, что одного атрибута (роли) для выражения бизнес-правил становится недостаточно и начинают добавляться другие атрибуты (город, страна, филиал, день недели, владелец, лимит и т. п.). Чтобы справиться с этой сложностью, необходимо создавать дополнительные роли, число которых равно числу различных комбинаций всех атрибутов.

После каждого добавления нового значения атрибута приходится добавлять новые роли. Кроме этого, появляются и другие проблемы:

- одно бизнес-правило «размазывается» среди множества ролей и становится неочевидным, что усложняет понимание такого правила и его поддержку;
- начинается взрывной рост числа ролей, что значительно усложняет управление ими.

Получается, что как только бизнес-правила становятся многомерными или требуют контроля данных, ролевая модель не только не решает текущие проблемы контроля доступа, но и создает новые.

Чтобы справиться с нерешаемыми в рамках RBAC проблемами, был создан другой подход, который основывается на атрибутах.

Основное отличие этого подхода в том, что каждая ситуация оценивается не с точки зрения роли пользователя и действия, которое он хочет совершить, а с точки зрения атрибутов, которые к ним относятся.

Бизнес-правило, по сути, представляет собой набор условий, в которых различные атрибуты должны удовлетворять предъявляемым к ним требованиям.

Можно явно выделить несколько категорий атрибутов:

- атрибуты ресурса (тип, создатель, стоимость);
- атрибуты субъекта (имя, отдел, должность);
- атрибуты действия (название);
- атрибуты среды (IP-адрес, время, устройство).

Для выполнения авторизации значения всех атрибутов берутся в момент проверки прав и сравниваются с ожидаемыми значениями. Выполнение всех условий обеспечивает доступ к ресурсу.

Простые правила реализуются простыми условиями, а многомерные правила в этой модели не становятся более сложными.

Таким образом, ABAC позволяет избежать проблем, которые появляются в RBAC:

- бизнес-правило не «размазывается» по системе, что делает его понимание и поддержку достаточно простыми;
- не происходит взрывного роста числа условий, что упрощает их сопровождение.

Но самое главное, ABAC позволяет решить проблемы, которые невозможно решить с помощью RBAC, поскольку в этом подходе нет ограничений

на сложность бизнес-правил. Бизнес-правила любой сложности, в том числе с использованием заранее неизвестных атрибутов, не создают новых проблем и просты в сопровождении.

Также упростить ведение и поддержку базы данных или знаний может унификация данных и их хранение в качестве фреймов.

Термин унификация означает приведение к единообразной системе или форме. Фрейм – это модель абстрактного образа, минимально возможное описание сущности какого-либо объекта, явления, события, ситуации, процесса; структура, содержащая описание объекта в виде атрибутов и их значений [2]. Каждый фрейм состоит из имени и отдельных единиц – слотов. Все фреймы имеют однородную структуру и позволяют хранить любую базу знаний.

База данных представляет собой связанные таблицы (фреймы):

- объекты (идентификатор, имя, транзакция, версия, тип);
- параметры (идентификатор, транзакция, версия, тип, значение, ссылка на объект);
- типы (идентификатор, транзакция, версия, наследование, тип, значение по умолчанию).

Применение RBAC модели разграничения прав к унифицированной форме хранения знаний является не тривиальной задачей, так как набор данных и атрибутов заранее неизвестен. Поэтому для унифицированной формы хранения бизнес правила распространяются на фреймы и параметры фреймов, и действуют на любые из созданных сущностей (фреймы-экземпляры). Данный подход позволяет унифицировать и RBAC правила для разграничения прав доступа, что так же позволяет применять наследование в самих правилах.

Таким образом, атрибутивный способ контроля доступа, унификация данных и представление их в виде фреймов значительно упрощают ведение, манипулирование данными и их хранение, а так же позволяют использовать данную структуру для любой предметной области.

Литература

1. Подходы к контролю доступа: RBAC vs. ABAC [Электронный ресурс] // Официальный сайт Habrahabr. – Режим доступа: https://habrahabr.ru/company/custis/blog/258861/ , свободный. – (Дата обращения 15.12.2017).

2. Фрейм [Электронный ресурс] // Официальный сайт Wikipedia. – Режим доступа: https://ru.wikipedia.org/wiki/Фрейм_(инженерия_знаний) , свободный. – (Дата обращения 16.12.2017).