О сложности проверки существования доступа в RelBAC-политиках

Д. Е. Александров, А. В. Галатенко
(МГУ им. М. В. Ломоносова, Москва)

В работе исследуется сложность решения следующей задачи. Дана система, разграничение доступа в которой основано на RelBAC-модели, введенной в статьях В. А. Васенина с соавторами, и пара (субъект, объект). Требуется определить, существуют ли условия, при которых субъект может получить заданный доступ к объекту. Мы показываем, что в общем случае эта задача NP-полна. Если же максимальная длина путей ограничена константой, то задача становится полиномиальной.

Ключевые слова: информационно-аналитические системы, NP-полнота, графы, информационная безопасность.

1. Введение

Реляционная модель разграничения доступа (Relation-Based Access Control, RelBAC) была введена в работе [1] как удобное средство выражения политик безопасности в системах управления наукометрической информацией, таких как ИАС «ИСТИНА» ([3]). Если говорить содержательно и абстрагироваться от ряда непринципиальных с нашей точки зрения свойств, модель представляет собой ориентированный нагруженный граф. Множество вершин составляют объекты системы. Ребра соответствуют бинарным отношениям на множестве объектов. Нагрузка ребра представляет собой имя отношения и предикат, зависящий от переменных нескольких типов: атрибуты объектов, инцидентных ребру, значения переменных окружения, тип доступа и т. п. Правила разграничения доступа бывают двух типов: разрешающие и запрещающие. Доступ субъекта s к объекту o разрешается, если для пары (s, o) существует хотя бы одно разрешающее правило и не существует запрещающих пра-

вил. Если говорить неформально, то правило — это путь в графе, ребра которого удовлетворяют каким-либо ограничениям.

В качестве примера рассмотрим следующую ситуацию. Путь в системе есть публикация p, автором которой является субъект a, обладающий всевозможными правами доступа к p. Субъект a является сотрудником кафедры, кафедра входит в состав факультета, факультет является частью Университета. Возникает иерархия подразделений, причем для каждого уровня иерархии i имеется ответственный сотрудник r_i, обладающий всеми или по крайней мере частью прав доступа ко всем объектам сотрудников подразделений более низкого уровня. Заметим, что субъект a мог менять место работы, поэтому для определения возможности доступа ответственного сотрудника необходимо учитывать время выхода статьи p. Рассмотрим граф, в котором вычислены значения предикатов для права доступа, имеющегося у ответственного сотрудника r_i. Тогда в графе для субъекта r_i возникает путь через его подразделение и подразделения нижележащих уровней иерархии до подразделения субъекта a и самого субъекта a. Первое ребро помечено предикатом, обращающимся в истину, если начало соответствует субъекту r_i, а конец — подразделению, в котором он является ответственным. Последующие ребра, кроме двух последних, отмечены предикатами, обращающимися в истину, если концы ребра соответствуют подразделениям, причем начало ребра соответствует подразделению на один уровень выше, чем подразделение, которому соответствует конец ребра. Предпоследнее ребро помечено предикатом, обращающимся в истину, если начало ребра соответствует подразделению, а конец — сотруднику, работающему в этом подразделении. Последнее ребро помечено предикатом, обращающимся в истину, если начало ребра соответствует сотруднику, а конец — публикации, написанной этим сотрудником.

Из рассмотренного примера видно, что пути в графе могут быть потенциально сколь угодно длинными, так как может возникнуть еще один уровень иерархии. Кроме того, между парой вершин могут быть кратные ребра, соответствующие различным отношениям.

Пусть задано множество объектов и множество правил разграничения доступа. Для оценки безопасности требуется уметь отвечать на вопрос, существуют ли условия, при которых субъект s может получить доступ к некоторому объекту o. Мы покажем, что для формальной модели, являющейся упрощением модели RelBAC, эта задача NP-полна.

Также будет показано, что в случае ограничения длины пути некоторой константой задача становится полиномиальной.

2. Определение модели и формулировка результата

Пусть $k \in \mathbb{N}$, $X_k = \{x_1, \ldots, x_k\}$. Интерпретируем элементы X_k как булевы переменные. Рассмотрим множество предикатов P, такое что каждый предикат из множества P есть либо переменная из множества X_k, либо отрицание переменной. Содержательно булевы переменные могут трактоваться, например, как результат сравнения значения некоторой переменной окружения с константой.

Пусть O — конечное множество (объектов), $|O| = n$. Моделью разграничения доступа $M_{k,n}$ назовем произвольный ориентированный нагруженный граф без ориентированных циклов, вообще говоря имеющий кратные ребра, множество вершин которого совпадает с O, а каждое ребро помечено элементом множества P, причем пометки всех ребер, идущих из вершины o_1 в вершину o_2, попарно различны для любых $o_1, o_2 \in O$, $o_1 \neq o_2$. Таким образом, число ребер не превосходит $2k * n(n-1)$.

Для простоты будем рассматривать только разрешающие правила. Пусть $o_1, o_2 \in O$. Говорим, что o_1 может получить доступ к o_2, если найдется значения переменных из множества X_k и ориентированный путь из o_1 в o_2, такой что предикат на каждом ребре пути обращается в истину. С содержательной точки зрения возможность получения доступа означает, что существуют такие условия, при которых доступ появится.

Рассматривается следующая массовая проблема. На вход подается модель $M_{k,n}$ и пара объектов o_1, o_2. Требуется проверить, может ли объект o_1 получить доступ к o_2 при каких-либо условиях. Можно считать, что задача параметризована значением kn. Несложно увидеть, что задача может быть закодирована словом, длина которого есть полином от kn.

Теорема 1. *Задача проверки возможности получения доступа NP-полна.*

Теорема 2. *Пусть длина путей ограничена сверху костантой $N, N \in \mathbb{N}$. Тогда задача проверки возможности получения доступа полиномиальна.*

3. Доказательство Теоремы 1

Принадлежность задачи классу NP очевидна, так как при заданном наборе значений предикатов достаточно проверить существование пути в графе, а эта задача полиномиальна.

Для доказательства полноты сведем задачу о выполнимости КНФ ([2, §2.6]) к задаче проверки возможности получения доступа. Пусть $C = (x_{i^1_1}^{\sigma_{i^1_1}} \vee \ldots x_{i^1_{j_1}}^{\sigma_{i^1_{j_1}}}) \wedge \ldots \wedge (x_{i^t_1}^{\sigma_{i^t_1}} \vee \ldots x_{i^t_{j_t}}^{\sigma_{i^t_{j_t}}}) = D_1 \wedge \ldots \wedge D_t$ — КНФ. Пусть k — число различных переменных в C. Отобразим C в $M_{k,t+1}(C)$ следующим образом. Ребра из вершины o_i ведут только в вершину o_{i+1}, $i = 1, \ldots, n-1$. Ребро из o_i в o_{i+1} с меткой x_i^σ проводится тогда и только тогда, когда соответствующий литерал присутствует в элементарной дизъюнкции номер i. Так как и k, и n очевидным образом не превосходят удвоенной длины КНФ, сведение полиномиально. В качестве объектов, существование доступа между которыми требуется проверить, выберем o_1 и o_n. По построению, доступ существует если и только если одновременно существует доступ из o_1 к o_2, из o_2 к o_3, …, из o_{n-1} к o_n. Доступ из o_i к o_{i+1} существует если и только если хотя бы один предикат на ребрах между этой парой вершин обращается в истину, то есть тогда и только тогда, когда элементарная дизъюнкция D_i выполнима. Следовательно, КНФ C выполнима тогда и только тогда, когда в $M_{k,t+1}(C)$ существует доступ из вершины o_1 в o_n. Теорема доказана.

Заметим, что в силу NP-полноты задачи 3-выполнимости КНФ при ограничении допустимой полустепени исхода всех вершин графа модели константой 3 NP-полнота сохраняется.

4. Доказательство Теоремы 2

Пусть задана модель разграничения доступов $M_{k,n}$, где k — количество булевых переменных, которые либо сами, либо их отрицание используются в качестве предикатов, а n — количество объектов модели. Назовем обобщенным путем такую последовательность вершин графа $o_1, o_2, \ldots o_t$, где $t \in \mathbb{N}$, что от вершины o_i к вершине o_{i+1} идет хотя бы одно ребро. Пусть требуется определить, существуют ли условия, при которых субъект s может получить доступ к объекту o. То есть требуется определить, существует ли такой путь от s к o, что предикаты, соответствующие ребрам пути, обращаются в истину.

По условию максимальная длина пути ограничена константой N. Но тогда количество обобщенных путей длины не более N от субъекта s к объекту o не превосходит полинома от общего количества вершин — n. Проверка, найдется ли хотя бы один путь, предикаты которого обращаются в истину, в обобщенном пути, очевидно, сводится к задаче о выполнимости КНФ с количеством конъюнкций, не превосходящим N. Данная задача, в свою очередь, полиномиально зависит от k.

Таким образом, исходная задача полиномиально зависит от kn.

Благодарности и ссылки на гранты

Авторы благодарят профессора В. А. Васенина, н. с. А. А. Иткеса и В. Ю. Бухонова за плодотворное обсуждение.

Работа выполнена в рамках проекта «Развитие и сопровождение информационно-аналитической системы подготовки принятия решений на основе анализа информации о результатах научно-исследовательской, педагогической и инновационной деятельности „Наука МГУ“ („ИСТИНА“), этап 3» под руководством профессора В. А. Васенина.

Список литературы

[1] Васенин В. А., Иткес А. А., Шапченко К. А., Бухонов В. Ю. Реляционная модель логического разграничения доступа на основе цепочек отношений // Программная инженерия. — 2015. — 9. — С. 11–19.

[2] Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. — М.: Мир, 1982.

[3] Домашная страница системы «Истина». — [Эл. ресурс] https://istina.msu.ru