

Безопасное объединение систем с моделью take-grant

В. А. Плетнева (МГУ им. М. В. Ломоносова, Москва)

В работе исследуется задача объединения двух систем, в каждой из которых реализована политика безопасности take-grant. Объединение называется безопасным, если внутри каждой из объединяемых систем не появляется новых доступов. Предлагается критерий безопасности объединения, а также легко проверяемое достаточное условие безопасности.

Ключевые слова: формальные модели безопасности, модель take-grant, безопасное объединение.

Введение

Задача объединения систем состоит в следующем: имеется ряд подсистем, в каждой из которых реализована своя политика безопасности; требуется объединить эти системы в одну таким образом, чтобы безопасность каждой подсистемы не нарушилась. Примерами ситуаций, когда такая задача встает на практике, являются создание служб «единого окна» и интеграция корпоративных сетей объединившихся компаний.

Попытка решения такой задачи была предпринята в работе [1], в которой предлагается подход, основанный на отображении множества пользователей одной подсистемы в множество пользователей другой подсистемы. С нашей точки зрения, при таком подходе происходит сужение задачи, так как, в частности, после объединения «внешние» пользователи могут получить новый набор доступов.

Для полного решения задачи требуется либо отдельно рассмотреть объединение всевозможных пар политик безопасности, либо выразить все политики через небольшое подмножество. В настоящее время известно довольно большое число различных моделей политик безопасности. Модели могут быть графовыми, например, take-grant [2] (по сути, примерами обобщения модели take-grant являются модели RelBAC [3] и eBAC [4]), или иметь автоматную реализацию, как, например, модель

Белла-Лападула [5] и модель невлияния (в работе [6] рассматривается случай конечных автоматов, в работе [7] — вероятностных, в работе [8] — квантовых). Имеется ряд более общих парадигм, через которые выражаются все модели (модель АВАС [9, 10]). В данной работе мы исследуем безопасность объединения подсистем с моделью take-grant.

Модель take-grant — это модель распространения прав доступа в системе с дискреционной политикой безопасности. Модель была представлена в 1976 году Джонсом, Липтоном и Шнайдером. Основной проблемой дискреционной политики безопасности является проблема контроля распространения прав доступа. Чаще всего бывает, что владелец файла передает содержание файла другому пользователю, при этом не хочет, чтобы некий субъект S имел доступ к информации. Но за счет распространения прав доступа, через несколько шагов передача прав может состояться независимо от его воли. Возникает задача об условиях, при которых в такой системе некоторый субъект рано или поздно получит требуемый ему доступ. Эта задача и исследовалась в модели take-grant.

В данной работе рассматривается задача безопасного объединения систем take-grant с точки зрения доступов: имеется две системы, мы хотим проводить между ними доступы так, чтобы множество доступов внутри каждой подсистемы осталось неизменным. Задача состоит в описании всевозможных способов безопасного объединения. В работе доказывается критерий безопасного объединения, а также предлагается легко проверяемое достаточное условие безопасности.

Основные понятия

Состояние системы описывается графом доступов.

Пусть $O(t)$ — конечное множество объектов, $S(t) \subseteq O(t)$ — множество субъектов в момент времени t . На множестве объектов как на вершинах определен ориентированный граф $G_t(V, E)$, где $V = O(t)$, а ребро (v_1, v_2) с меткой $p \in R$ принадлежит E , если v_1 имеет доступ p к v_2 . Множество $R = \{r, w, c, t, g\}$, где r — читать, w — писать, c — вызывать и еще 2 права: take (t) и grant(g).

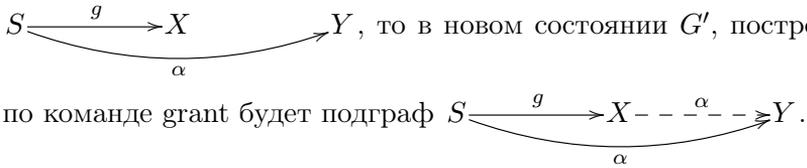
Преобразование графов доступов проводятся при помощи 4 команд, которые опишем графически:

- 1) Take. Если в исходном графе доступов G был подграф

$$S \xrightarrow{t} X \xrightarrow{\alpha} Y$$
 то в новом состоянии G' , построенном по команде take будет подграф

$$S \xrightarrow{t} X \xrightarrow{\alpha} Y$$
 где дуга $S \xrightarrow{\alpha} Y$ является пунктирной.

- 2) Grant. Если в исходном графе доступов G был подграф



- 3) Create. Данная команда создает новую вершину X , и в графе G' появляется подграф $S \xrightarrow{\beta} X$.

- 4) Remove. В G был подграф $S \xrightarrow{P} X$, тогда в G' будет подграф $S \xrightarrow{P \setminus \beta} X$.

Определение 1. В графе доступов G вершины P и S называются tg-связными, если существует путь в G , соединяющий P и S , безотносительно ориентации дуг, но такой, что каждое ребро этого пути имеет метку, включающую t или g .

Заметим, что доступ в графе возможен тогда и только тогда, когда он возможен без применения команды Remove.

Следующий критерий и его доказательство можно найти в работе [1].

Теорема 1. Пусть в системе все объекты являются субъектами. Тогда субъект P может получить доступ α к субъекту X тогда и только тогда, когда выполняются условия:

- 1) Существует субъект S такой, что в текущем графе G есть дуга $S \xrightarrow{\alpha} X$.
- 2) S tg-связна с P .

На основе данного критерия видно, что множество вершин V разбивается в объединение компонент tg-связности.

Пусть $G_1 = (V_1, E_1)$, $G_2 = (V_2, E_2)$ — две системы, реализующие модель take-grant, $V_1 \cap V_2 = \emptyset$. Система $G = (V, E)$ называется объединением G_1 и G_2 , если $V = V_1 \cup V_2$, $E = E_1 \cup E_2 \cup E_3$, причем все ребра из E_3 имеют вид (v', v'') , где $v' \in V_1, v'' \in V_2$ или $v' \in V_2, v'' \in V_1$.

Определение 2. Объединение систем является безопасным, если в результате объединения множество доступов внутри каждой системы осталось неизменным.

Критерий безопасного объединения систем

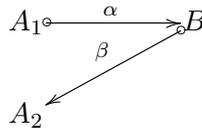
Теорема 2. Пусть даны графы G_1 и G_2 , A — tg -компонента первого графа, B — tg -компонента второго графа. Пусть a_1 и a_2 вершины tg -компоненты A , такие что из a_1 нет доступа в a_2 . После объединения графов доступ из a_1 в a_2 появляется тогда и только тогда, когда есть доступ $\alpha \in \{t, g\}$ между tg -компонентами A и B , и из компоненты B есть произвольный доступ в вершину a_2 .

Пусть в G_1 есть 2 компоненты tg -связности A_1 и A_2 , а в G_2 есть компонента B . Вершины $a_1 \in A_1, a_2 \in A_2$ такие, что между ними нет доступов в графе G_1 . Рассматриваем объединение графов G_1 и G_2 . Доступ между вершинами a_1 и a_2 после объединения графов возникает тогда и только тогда, когда выполнены следующие условия:

- 1) Есть доступ $\alpha \in \{t, g\}$ между tg -компонентами A_1 и B .
- 2) Либо есть произвольный доступ β из некоторой вершины B в вершину a_2 , либо есть доступ $\beta \in \{t, g\}$ из некоторой вершины компоненты A_2 в некоторую вершину компоненты B .

Доказательство теоремы основывается на рассмотрении возможных случаев объединения:

1)



По критерию безопасности системы, для возникновения доступа от a_1 к a_2 необходимо и достаточно существование вершины S такой, что S tg -связна с a_1 и S имеет доступ к a_2 .

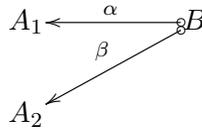
Если $\alpha \notin \{t, g\}$, то вершина $S \in A_1$, а, значит, вопрос о возникновении доступа от a_1 к a_2 сводится к подграфу G_1 , где указанного доступа нет.

Если $\alpha \in \{t, g\}$, то вершина S может принадлежать B . Сделаем очевидное замечание, следующее из критерия безопасности системы.

Замечание. Если вершина a компоненты tg -связности A имеет доступ α к вершине b , то любая вершина $a' \in A$ имеет доступ α к вершине b .

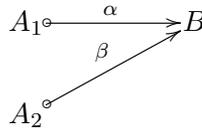
Из замечания следует, что вершина S имеет доступ β к вершине из A_2 . В данной ситуации возникает новый доступ внутри подграфа G_1 .

2)



Если $\alpha, \beta \notin \{t, g\}$, то новых доступов не появляется, так как по критерию безопасности системы нужная вершина $S \in A_1$ или $S \in A_2$, таким образом вопрос о возникновении новых доступов сводится к подграфу G_1 . Если хотя бы один из доступов α или $\beta \in \{t, g\}$, задача сводится к 1 пункту.

3)



Рассуждая аналогично, приходим к выводу, что новый доступ между A_1 и A_2 возникает тогда и только тогда, когда α и β одновременно из множества $\{t, g\}$.

Для каждого из случаев получены необходимые и достаточные условия, при которых новые доступы внутри подсистем не возникают.

На основе этих условий доказывается теорема.

Из представленного критерия легко получается следующее следствие.

Следствие 1. *Если при объединении систем take-grant не используются доступы из множества $\{t, g\}$, то такое объединение безопасно.*

Автор благодарит научного руководителя к.ф.-м.н. Галатенко А. В. за постановку задачи и помощь в работе.

Список литературы

- [1] Иткес А. А. Объединение моделей логического разграничения доступа для сложноорганизованных распределенных информационных систем // Проблемы информатики. — № 1. — С. 85–94.
- [2] Lipton R., Snyder L. A Linear Time Algorithm for Deciding Subject Security // Journal of the ACM. — Addison-Wesley. — 24 (3). — P. 455–464.

- [3] 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.
- [4] Bogaerts J., Decat M., Lagaisse B., Joosen W. Entity-based access control: supporting more expressive access control policies // Proceedings of the 31st Annual Computer Security Applications Conference. — ACM, 2015. — P. 291–300.
- [5] Bell D. E., La Padula L. J. Secure Computer System: Unified Exposition and Multics Interpretation. — [Эл. ресурс]
URL: <http://csrc.nist.gov/publications/history/bell76.pdf>
- [6] Moskowitz I. S., Costich O. L. A classical automata approach to non-interference type problems // Proc. Comp. Security Found. Workshop. — 1992. — 5. — P. 2–8.
- [7] Галатенко А. В. Об автоматной модели защищенных компьютерных систем // Интеллектуальные системы. — 1999. — Т. 4, вып. 3–4. — С. 263–270.
- [8] Терехина И. Ю. Модель невлияния для квантовых автоматов // Интеллектуальные системы. Теория и приложения. — 2015. — Т. 19, вып. 2. — С. 209–216.
- [9] Hu V. C., Ferraiolo D., Kuhn R., Schnitzer A., Sandlin K., Miller R., Scarfone K. Guide to Attribute Based Access Control (ABAC) Definition and Considerations. — [Эл. ресурс] URL: <http://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.sp800-162.pdf>
- [10] Галатенко А. В., Галатенко В. А. К постановке задачи разграничения доступа в распределенной объектной среде // Программная инженерия. — 2013. — 5. — С. 27–30.