Критерий безопасного объединения систем с моделью take-grant

В. А. Кузовихина[1]

В работе рассматривается задача безопасного объединения систем с моделью take-grant с точки зрения добавления новых доступов и соответствия субъектов. Объединение систем безопасно, если множество доступов внутри каждой из систем не изменилось. Получены критерии безопасного объединения для каждого из способов объединения.

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

1. Введение

В случае слияния нескольких компаний или создания служб "единого окна" актуальной становится задача безопасного объединения систем. Объединение систем является безопасным, если в результате объединения множество возможных доступов внутри каждой системы осталось неизменным.

Задача безопасного объединения формальных моделей безопасности рассматривалась в работах Иткеса А.А. ([1]) и Шапченко К.А. ([2]). Были получены критерии безопасного объединения в некоторых частных случаях, а также установлена эквивалентность ряда формальных моделей.

На данный момент известно довольно большое количество формальных моделей безопасности, среди которых такие классические модели, как модель take-grant ([3]), модель Белла – Лападула ([3]), и современные модели, например, модель СВАС ([4]).

В данной работе рассматривается задача объединения систем с политикой take-grant с двух сторон. Во-первых, с точки зрения доступов (задаются новые доступы между системами). Во-вторых, с точки зрения соответствия субъектов. Получены критерии безопасного объединения систем с моделью take-grant для каждого из способов объединения.

2. Основные понятия и результаты

Приведем описание модели take-grant, взятое из работы ([3]).

[1] *Кузовихина Веста Андреевна* — учитель, Новая школа, e-mail: pletnyova_va@mail.ru.

Kuzovikhina Vesta Andreevna — teacher, New School.

Состояние системы описывается графом доступов. Множество доступов $R = \{r, w, c, t, g\}$ на чтение, запись, исполнение и пара выделенных доступов take (t) и grant (g). На множестве объектов $O(\tau)$ как на вершинах определен ориентированный граф $G_\tau(V, E)$, где $V = O(\tau)$, а E — множество ребер, помеченных доступами. Будем считать, что множество субъектов $S(\tau) = O(\tau)$. Преобразование графов доступов проводятся при помощи четырех команд: take, grant, create и remove.

Систему будем считать безопасной, если невозможно получить запрещенный доступ с помощью последовательности разрешенных команд. Свойство безопасности модели take–grant разрешимо.

Определение. *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 t или g.*

Теорема (Критерий безопасности системы, [3])**.** *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 ребро (S, α, X).*

2) *S tg-связен с P.*

Таким образом, множество вершин V разбивается в объединение компонент tg-связности.

2.1. Объединение с помощью добавления ребер

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 $v' \in V_2, v'' \in V_1$.

В качестве доступов далее будем рассматривать доступы не из множества $\{t, g\}$. 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. Обозначим множество таких доступов (A, α, b). Множество всех доступов компоненты A обозначим R_A.

Предположим, что в графе G есть две компоненты tg–связности A и B с одинаковыми наборами доступов, то есть $R_A = R_B$. Тогда если соединить компоненты A и B tg–ребрами, то множество всех возможных доступов в графе G не изменится. Без ограничения общности, будем считать, что все tg–компоненты одной системы имеют попарно различные

множества возможных доступов (иначе, tg–компоненты с одинаковыми доступами будем считать одной tg–компонентой). Через R'_A обозначим множество новых доступов, проведенных из компоненты A.

Теорема 1. *Объединение G_1 и G_2 безопасно тогда и только тогда, когда выполнены следующие условия:*

1) *каждая tg–компонента графа G_1 соединена tg–ребрами с не более чем одной tg–компонентой графа G_2 и наоборот;*

2) *если A — tg–компонента графа G_1 соединена tg–ребрами с B — tg–компонентой графа G_2, то $R'_A \subseteq R_B$ и $R'_B \subseteq R_A$.*

2.2. Объединение через соответствие субъектов

Рассмотрим объединение двух систем G_1 и G_2 с помощью отображений $m_1 : S_1 \to 2^{S_2}, m_2 : S_2 \to 2^{S_1}$, где S_1 — множество субъектов первой системы G_1, а S_2 — множество субъктов второй системы G_2.

В такой постановке рассматривал задачу объединения А.А. Иткес в своей работе ([1]).

Будем считать, что субъект $s_1 \in S_1$ отождествлен с субъектом $s_2 \in S_2$, если выполнены следующие условия:

1) $\forall s_i \in S_2$ такого, что есть доступ (s_i, a, s_2), есть доступ (s_i, a, s_1)

2) $\forall s_j \in S_2$ такого, что есть доступ (s_2, a, s_j), есть доступ (s_1, a, s_j).

Содержательно это означает, что пользователь s_1 входит во вторую систему под именем пользователя s_2.

Теорема 2. *Объединение G_1 и G_2 безопасно тогда и только тогда, когда субъект системы G_1 отождествлен с субъектами системы G_2 из не более чем одной компоненты tg-связности и наоборот.*

3. Заключение

В работе рассмотрена задача объединения систем с моделью take-grant. Получены критерии безопасного объединения систем относительно доступов и отождествления субъектов.

Прямого доступа между субъектами может и не быть, но при этом информация может передаваться с помощью информационного потока. Простейшие информационные потоки возникают от объекта O к субъекту S, если субъект S осуществляет доступ на чтение к объекту O, и от субъекта S к объекту O, если субъект S осуществляет доступ на запись к объекту O. Более сложные информационные потоки возникают

при транзитивном замыкании цепочек доступов. Интересно посмотреть на задачу объединения систем с моделью take-grant, рассматривая информационные потоки вместо доступов.

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*, 2010, № 1, 85 – 94.

[2] Шапченко К.А., "Современные методы проверки свойств безопасности в моделях логического разграничения доступа", *Проблемы информатики*, 2009, № 3, 10 – 19.

[3] Грушо А.А., Тимонина Е.Е., *Теоретические основы защиты информации*, Яхтсмен, Москва, 1996.

[4] Afonin S., Bonushkina A., "Validation of Safety-Like Properties for Entity-Based Access Control Policies", *Advances in Soft and Hard Computing*, 2019, 259 – 271.

Criterion of secure union of systems with take-grant models

Kuzovikhina V.A.

In this work we consider the problem of secure union of systems with take-grant models from the point of view of adding new accesses and corresponding of subjects. Union of systems is considered secure if the set of accesses did not change for each individual system. We obtain the criteria of secure union for each union type.

Keywords: formal secutity models, take-grant model, secure union.

References

[1] Itkes A. A., "Union of access control models for complex distributed information systems", *Problemy informatiki*, 2010, № 1, 85 – 94 (in Russian).

[2] Shapchenko K.A., "Modern approaches to verification of security properties in access control models", *Problemy informatiki*, 2009, № 3, 10 – 19 (in Russian).

[3] Grusho A. A., Timonina E.E, *Theoretical Foundations of Information Security*, Yachtsman, Moscow, 1996 (in Russian).

[4] Afonin S., Bonushkina A., "Validation of Safety-Like Properties for Entity-Based Access Control Policies", *Advances in Soft and Hard Computing*, 2019, 259 – 271.