Расширенная модель

TAKE-GRANT

Модель Take-Grant

Модель TAKE-GRANT, имеющая важное теоретическое значение в исследовании процессов распространения прав доступа в системах, основанных на политике дискреционного доступа, была представлена Джонсом, Липтоном и Шнайдером в 1976 г.

Модель Take-Grant

Модель распространения прав доступа Take-Grant, предложенная в 1976 г., используется для анализа систем дискреционного разграничения доступа, в первую очередь для анализа путей распространения прав доступа в таких системах. В качестве основных элементов модели используются граф доступов и правила его преобразования. Цель модели - дать ответ на вопрос о возможности получения прав доступа субъектом системы на объект в состоянии, описываемом графом доступов. В настоящее время модель Take-Grant получила продолжение как расширенная модель Take-Grant, в которой рассматриваются пути возникновения информационных потоков в системах с дискреционным разграничением доступа.

формальное описание модели Take-Grant.

Обозначим: O - множество объектов (например, файлов или сегментов памяти);

S ⊆ O - множество активных объектов - субъектов (например, пользователей или процессов);

R (r1, r2,…, rK) U {t, g} - множество прав доступа, где **t(take)** - право брать права доступа, **g(grant)** - право давать права доступа;

G = (S, O, E) - конечный помеченный ориентированный граф без петель, представляющий текущие доступы в системе;

множества **S**, **O** соответствуют вершинам графа, которые обозначим:

⊗ - объекты (элементы множества **O\S**);

• -субъекты (элементы множества **S**);

элементы множества **E ⊆ O x O x R** представляют дуги графа, помеченные непустыми подмножествами из множества прав доступа **R**.

Основные положения модели

Классическая Модель Take-Grant

1. Компьютерная система рассматривается как граф **G (O, S, E)**, в котором множество вершин представлено (см. рис.1.):

- множеством объектов **O** доступа;
- множеством субъектов **S** доступа, причем **S ⊆ O**, а множество ребер:
- множеством **E** установленных прав доступа **(x, y, α)** субъекта **x** к объекту **y** с правом **α** из конечного набора прав **α ⊆ R (r1, r2,…, rK) U {t, g}**, в том числе с двумя специфическими правами – правом **take** (**t** – право брать права доступа у какого-либо объекта по отношению к другому объекту) и правом **grant** (**g** – право предоставлять права доступа к определенному объекту другому субъекту).

Основные положения модели

Классическая Модель Take-Grant

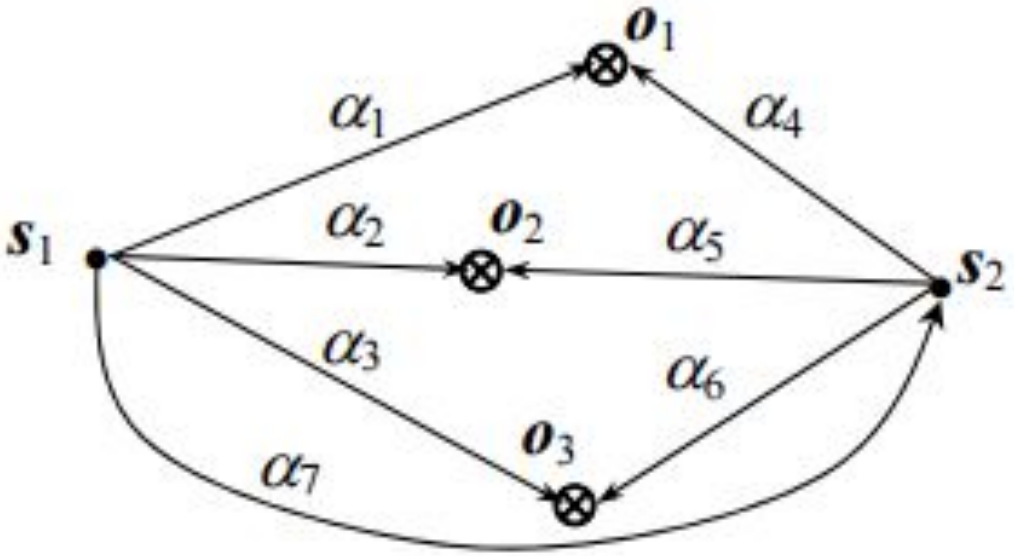


Рис.1. Граф доступов G в модели TAKE-GRANT (обозначения:
• – вершины, соответствующие субъектам, ⊗ – вершины, соответствующие объектам доступа, α1 ⊆ R – права доступа)

Основные положения модели

Классическая Модель Take-Grant

2. Состояния компьютерной системы (т. е. состояние системы разграничения доступа) изменяются под воздействием команд 4-х видов:

2.1. Команда "Брать" – **take (α, x, y, z)** – см. рис. 2.

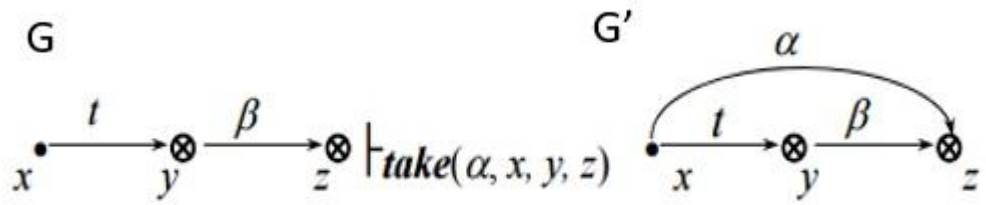


Рис.2. Изменение состояния фрагмента графа доступов **G** по команде "Брать" – субъект **x** берет права доступа **α ⊆ β** на объект **z** у объекта **y** (обозначения: ⊢c – переход графа **G** в новое состояние **G '** по команде **c** ; **x∈ S; y, z∈ O**).

Основные положения модели

Классическая Модель Take-Grant

2.2. Команда "Давать" – **grant (α, x, y, z)** – см. рис. 3.

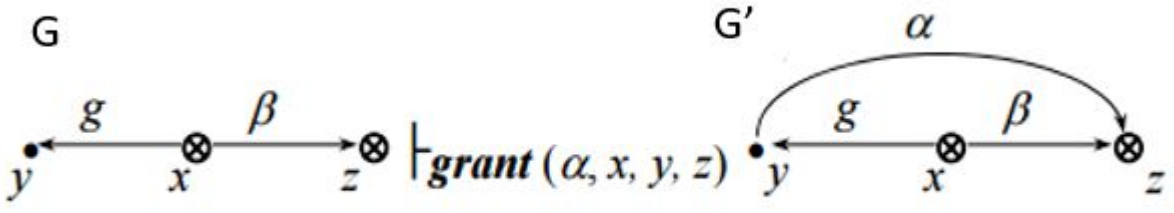


Рис.3. Субъект **x** дает объекту **y** право **α ⊆ β** на доступ к объекту **z**

Основные положения модели

Классическая Модель Take-Grant

2.3. Команда "Создать" – **create (ß, x, y)** – см. рис. 4.

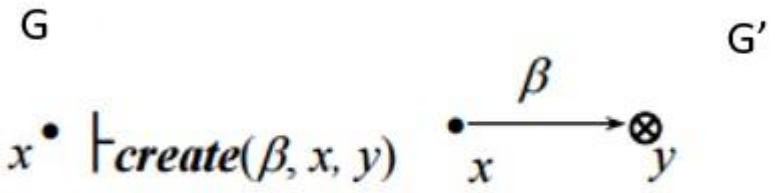


Рис.4. Субъект **x** создает объект **y** с правами доступа на него **ß1 ⊆ R** (**y** – новый объект, **O'=O ∪{y}**)

Основные положения модели

Классическая Модель Take-Grant

2.4. Команда "Удалить" – **remove (α, x, y)** – см. рис. 5.

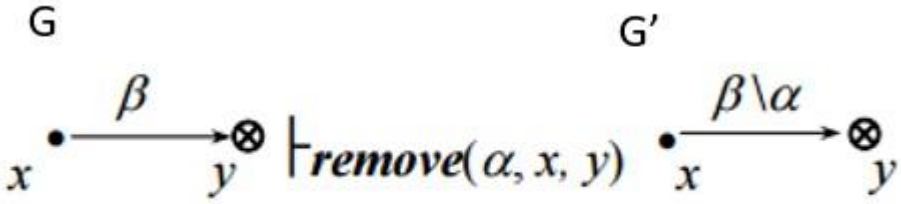


Рис.5. Субъект **x** удаляет права доступа **α ⊆ β** на объект **y**

расширенная Модель Take-Grant

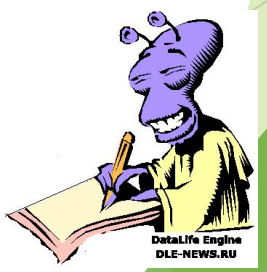
Выразительные методологические возможности модели TAKE - GRANT позволили на ее основе разработать расширенную модель TAKE - GRANT, играющую важную роль в исследовании возможностей неявных информационных потоков в дискреционных системах разграничения доступа.

Расширенная Модель Take-Grant

Определение. Неявным информационным потоком между объектами системы называется процесс переноса информации между ними без их непосредственного взаимодействия.

Расширенная Модель Take-Grant

Наиболее простым и наглядным примером неявного информационного потока является наличие общего буфера (объекта с правом доступа к нему **Read**, **Write**) у двух субъектов. Тогда один из субъектов, просматривая (читая) информацию в буфере, может искать и находить информацию из объектов, которые доступны другому пользователю, и информация из которых в процессе работы с ними может оказаться в общем буфере или, скажем, в общей мусорной информационной корзине. В результате может существовать поток без непосредственного взаимодействия субъекта с объектом доступа.



Основные положения модели

Расширенная Модель Take-Grant

1. КС рассматривается как граф G **(O, S, E)**, в котором множество вершин представлено:

- множеством объектов **O** доступа;
- множеством субъектов **S** доступа, причем **S⊆O**, а множество ребер:
- множеством установленных прав доступа **(x, y, α)** субъекта x к объекту **y** с правом **α** из набора прав доступа **R**, включающего всего два вида (методов) доступа – **Read** и **Write**.

2. Для исследования процессов возникновения неявных информационных потоков вводятся шесть команд (операций) преобразования графа доступов1, каждая из которых сопровождается порождением мнимой дуги, собственно и отображающей неявный информационный поток между объектами системы:

Основные положения модели

Расширенная Модель Take-Grant

2.1. Команда (без названия) – см. рис. 6.

Рис.6. Субъект **x** получает возможность записи (в себя) информации, осуществляя доступ **r** к объекту **y**.

Основные положения модели

Расширенная Модель Take-Grant

2.2. Команда (без названия) – см. рис. 7.

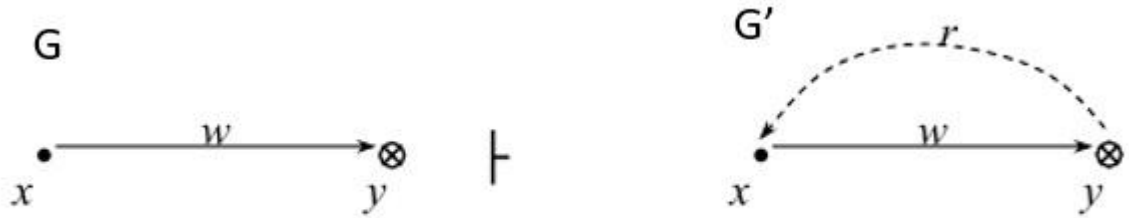


Рис.7. Субъект **x** получает возможность чтения информации, осуществляя доступ **w** к объекту **y**.

Основные положения модели

Расширенная Модель Take-Grant

2.3. Команда **post (x, y, z)** – см. рис. 8.

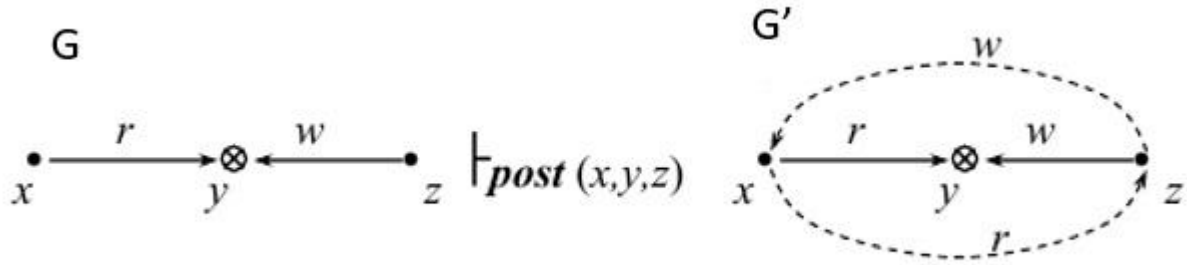


Рис.8. Субъект **x** получает возможность чтения информации от (из) другого субъекта **z**, осуществляя доступ **r** к объекту **y**, к которому субъект **z** осуществляет доступ **w**, а субъект **z**, в свою очередь, получает возможность записи своей информации в субъект **x**.

Основные положения модели

Расширенная Модель Take-Grant

2.4. Команда **spy (x, y, z)** – см. рис. 9.

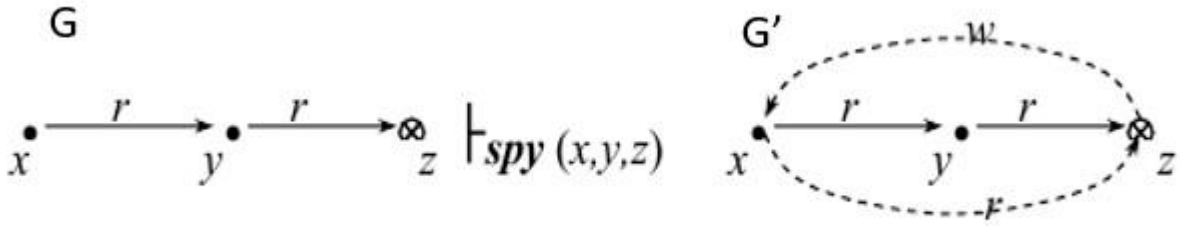


Рис.9. Субъект **x** получает возможность чтения информации из объекта **z**, осуществляя доступ **r** к субъекту **y**, который, в свою очередь, осуществляет доступ **r** к объекту **z**, при этом также у субъекта **x** возникает возможность записи к себе информации из объекта **z**.

Основные положения модели

Расширенная Модель Take-Grant

2.5. Команда **find (x, y, z)** – см. рис. 10.

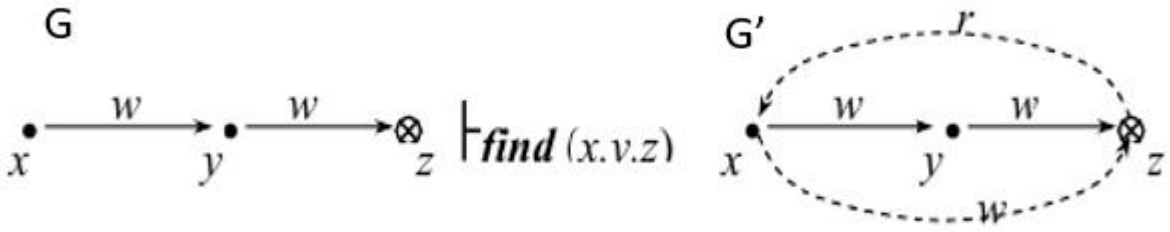


Рис.10. Субъект **x** получает возможность чтения информации из объекта **z**, осуществляя доступ **w** к субъекту **y**, который, в свою очередь, осуществляет доступ **w** к объекту **z**, при этом также у субъекта **x** возникает возможность записи к себе информации из объекта **z**.

Основные положения модели

Расширенная Модель Take-Grant

2.6. Команда **pass (x, y, z)** – см. рис. 11.

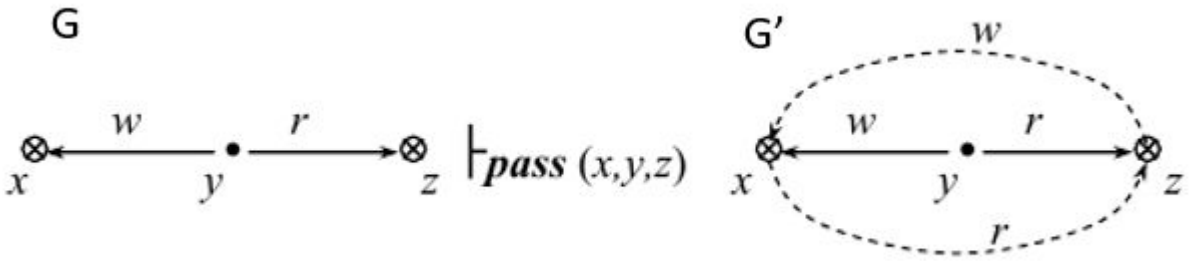


Рис.11. При осуществлении субъектом **y** доступа **r** к объекту **z** возникает возможность внесения из него информации в другой объект **x**, к которому субъект **y** осуществляет доступ **w**, и, кроме того, возникает возможность получения информации (чтения) в объекте **x** из объекта **z**.

Основные положения модели

Расширенная Модель Take-Grant

В классической модели Take-Grant по существу рассматриваются два права доступа: **t** и **g**, а также четыре правила (правила де-юре) преобразования графа доступов: **take**, **grant**, **create**, **remove**. В расширенной модели дополнительно рассматриваются два права доступа: на чтение **r(read)** и на запись **w(write)**, а также шесть правил (правила де-факто) преобразования графа доступов: **post**, **spy**, **find**, **pass** и два правила без названия.

Основные положения модели

Расширенная Модель Take-Grant

3. Анализ возможности возникновения неявного информационного канала (потока) между двумя произвольными объектами (субъектами) **x** и **y** системы осуществляется на основе поиска и построения в графе доступов пути между **x** и **y**, образованного мнимыми дугами, порождаемыми применением команд 2.1,…, 2.6 к различным фрагментам исходного графа доступов.

Теория

Расширенная Модель Take-Grant

В расширенной модели Take-Grant рассматриваются пути и стоимости возникновения информационных потоков в системах с дискреционным разграничением доступа.

Правила де-факто служат для поиска путей возникновения возможных информационных потоков в системе. Эти правила являются следствием уже имеющихся у объектов системы прав доступа и могут стать, причиной возникновения информационного потока от одного объекта к другому без их непосредственного взаимодействия.

теория

Расширенная Модель Take-Grant

В результате применения к графу доступов правил де-факто в него добавляются мнимые дуги, помечаемые r или w и изображаемые пунктиром. Вместе с дугами графа, соответствующими правам доступа r и w (реальными дугами), мнимые дуги указывают на направление информационных каналов в системе.

Важно отметить, что к мнимым дугам нельзя применять правила де-юре преобразования графа доступов. Информационные каналы нельзя брать или передавать другим объектам системы.

теория

Расширенная Модель Take-Grant

Каждое правило де-юре требует для достижения своей цели участия одного субъекта, а для реализаций правила де-факто необходимы один или два субъекта. Например, в де-факто правилах post, spy, find обязательно взаимодействие двух субъектов. Желательно во множестве всех субъектов выделить подмножество так называемых субъектов - заговорщиков - участников процессов передачи прав или информации. В небольших системах эта задача легко решаема. Многократно просматривая граф доступов и применяя к нему все возможные правила де-юре и де-факто, можно найти замыкание графа доступов, которое будет содержать дуги, соответствующие всем информационным каналам системы. Однако, если граф доступов большой, то найти его замыкание весьма сложно.

теория

Расширенная Модель Take-Grant

В заключение, модель Take-Grant служит для анализа систем защиты с дискреционной политикой безопасности. В модели определены условия, при которых происходит передача или похищение прав доступа. Однако на практике редко возникает необходимость в использовании указанных условий, так как при анализе большинства реальных систем защиты не возникают столь сложные по взаимосвязи объектов графы доступов. А сами правила take и grant сравнительно редко используются на практике. В тоже время наиболее часто в реальных системах субъекты используют права доступа на чтение и запись. Поэтому предложенные в расширенной модели Take-Grant подходы к поиску и анализу путей возникновения в системе информационных каналов, определению их стоимости представляются наиболее интересными и актуальными.

расширенная Модель Take-Grant

Список литературы:

1. Гайдамакин Н.А. Теоретические основы компьютерной безопасности. Учебное пособие. — Екатеринбург, 2008.
2. Бречка Д.М. Применение модели Take – Grant для анализа безопасности состояний ОС семейства Windows.
3. Википедия [Электронный ресурс], -https://ru.wikipedia.org/wiki/Модель_Take-Grant - статья в интернете.
4. Зегжда П.Д., Девянин П.Н., Калинин М. О., Москвин Д.А. Теоретические основы компьютерной безопасности. Курс лекций. - Санкт-Петербург — 2008.
5. [Электронный ресурс] Модель распространения прав доступа Take – Grant - http://masters.donntu.org/2006/fvti/zhidkih/ind/kyrs/chapter/ - статья в интернете.
6. The Take-Grant Protection Model [Электронный ресурс], - http://www.facweb.iitkgp.ernet.in - статья в интернете.