1. Министерство образования и науки Российской Федерации
2. Санкт-Петербургский государственный политехнический университет
3. —
4. Институт информационных технологий и управления
5. **Кафедра «Информационная безопасность компьютерных систем»**
6. **ЛАБОРАТОРНАЯ РАБОТА №1**
7. **Модель Харрисона-Руззо-Ульмана**
8. по дисциплине «Безопасность операционных систем»
9. Выполнил
10. студент гр. 43508/1 Е.М.Орел

<*подпись*>

1. Руководитель А.А. Минин

<*подпись*>

1. Санкт-Петербург
2. 2017

# Цель работы

Исследование возможностей и изучение особенностей дискреционных моделей на примере модели Харрисона-Руззо-Ульмана.

# ход работы

1. Создание описания системы, в которой реализована модель Харрисона-Руззо-Ульмана (вариант 6).

Матрица доступа:

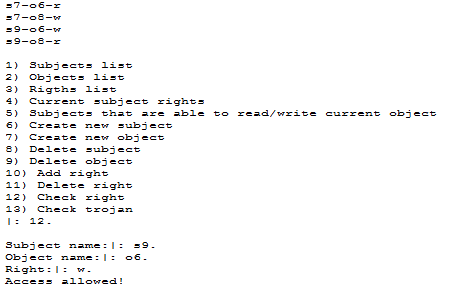
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | O2 | O4 | O6 | O8 |
| S1 | r |  | r | w |
| S3 | w |  |  |  |
| S5 |  | w |  |  |
| S7 |  |  | r | w |
| S9 |  |  | w | r |

Была реализована система, начальное состояние которой отражает матрица доступа, приведенная в таблице. В системе реализована возможность добавлять и удалять объекты и субъекты, отображать права всех субъектов ко всем объектам или права конкретного субъекта к конкретному объекту, а также возможность добавлять и удалять права субъектов.

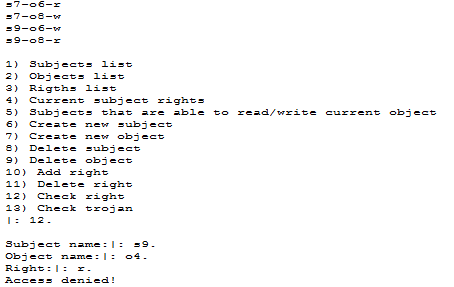
1. Проверка обеспечения защиты дискреционной модели.

Выполним проверку правил доступа для всех операций, прописанных в ячейках матрицы доступа.

Пример проверки права, которое существует:



Пример проверки права, которого не существует:

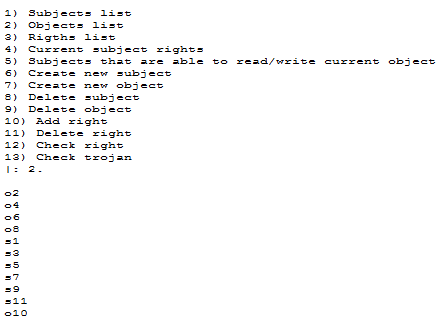


Таким образом, субъекты имеют доступ только к тем объектам, право к которым занесено в матрицу доступа.

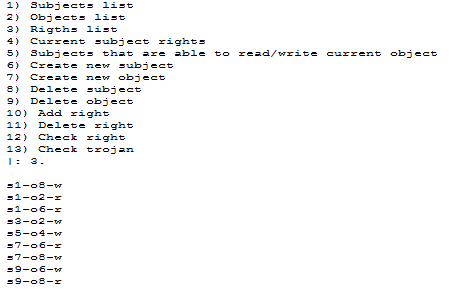
1. Создание новых объектов, субъектов, назначение новых прав и проверка безопасности нового состояния, в которое перешла система.

Создадим по одному субъекту и объекту. Удостоверимся, что изначально у субъекта нет никаких прав, а также что к объекту не применены никакие права других субъектов:

s11 и o10 появились в списке объектов и субъектов.



Также удостоверимся в том, что у них или к ним отсутствуют права.



Добавив новому субъекту s11 право r к объекту o10, удостоверимся, что состояние системы также безопасно.

1. Моделирование в системе поведение “троянского коня”.

Поведение троянского коня было смоделировано путем создания правила checkTrojan. Таким образом, доступ неавторизованному субъекту будет разрешен в любом случае через объект к которому у него есть доступ.

# контрольные вопросы

* Что составляет основу всех дискреционных моделей доступа?

Дискреционное управление доступом – управление доступом субъектов к объектам на основе списков управления доступом или матрицы доступа.

* Каковы признаки принадлежности модели Харрисона-Руззо-Ульмана к моделям дискреционного доступа?

Основной признак заключается в том, поведение системы определяется посредством матрицы доступа, которая является основой дискреционной модели доступа.

* Каковы достоинства и недостатки дискреционных моделей?

К достоинствам модели относятся ее универсальность (полнота охвата); наглядность; гибкость; удобство для пользователей при децентрализованном управлении. К недостаткам можно отнести излишнюю детализированность модели и из-за этого сложность полной реализации модели; при централизованном управлении – сложность администрирования, неудобство для пользователей и недостаток гибкости; при децентрализованном управлении – затрудняется централизованный контроль над безопасностью. Также в системах на основе дискреционных моделей существует проблема троянских программ (троянских коней).

* Каким образом происходит реализация угроз при помощи троянской программы?

Для реализации атаки "Троянский конь" создаются два каталога, соответствующих различным уровням секретности (например, SECRET и NONSEC). Регистрируются два субъекта, имеющих такие права доступа к этим каталогам:

Субъект A имеет права на чтение и запись в каталог SECRET, а также права на запись в каталог NONSEC.

Субъект B имеет права на чтение и запись в каталог NONSEC.

Субъект A имеет право запускать программы из каталога NONSEC.

Субъект B в такой ситуации может реализовать атаку типа "Троянский конь" для раскрытия секретной информации пользователя А. Пусть субъект А создал файл Secret.txt в каталоге SECRET. Тогда в соответствии с правами субъект B не имеет возможности читать этот файл. Раскрытие его содержимого и есть задача нарушителя. Он создает троянскую программу, помещает ее в каталог NONSEC и ждет, пока пользователь A запустит ее. Программа в фоновом режиме копирует файл Secret.txt из каталога SECRET в каталог NONSEC. Это копирование возможно, так как оно не противоречит маске прав субъекта A. Таким образом, содержимое секретного файла Secret.txt становится известным пользователю, не имеющему прав на доступ к ней.

* Каковы способы защиты от “троянского коня”?

Использование модели мандатного управления доступом. Например, в модели Белла-ЛаПадула субъекту запрещено помещать информацию в объекты, чей уровень безопасности ниже, чем у него.

# вывод

В ходе проделанной работы была исследована и реализована дискреционная модель Харрисона-Руззо-Ульмана. Можно сделать вывод, что модель имеет слабые защитные характеристики. При этом ограничения, вводимые с целью повышения защитных свойств, приводят к снижению практического интереса к модели.