Добавление новых классов доступа в защищенную операционную систему

Задание:

1. Изучить основы работы с политиками SELinux
2. Добавить новый класс доступа в политику SELinux
3. Написать модуль политики безопасности для добавленного класса
4. Реализовать проверку доступа к объектам добавленного класса, используя библиотеку libselinux

Студент: Холявин Виталий Борисович

Группа: К8-361

Объявление класса

Reference Policy.

policy/flask/security_classes:

```
class mybutton
```

policy/flask/access_vectors:

```
common gui
{
        set_enabled
        set_disabled
}
class mybutton
inherits gui
{
        click
}
```

Модуль политики

mybutton.te:

- Объявление типов
- Объявление доменов
- Правило перехода доменов
- Связывание ролей и доменов
- Правила вектора доступа (разрешения)

mybutton.if:

- Документация

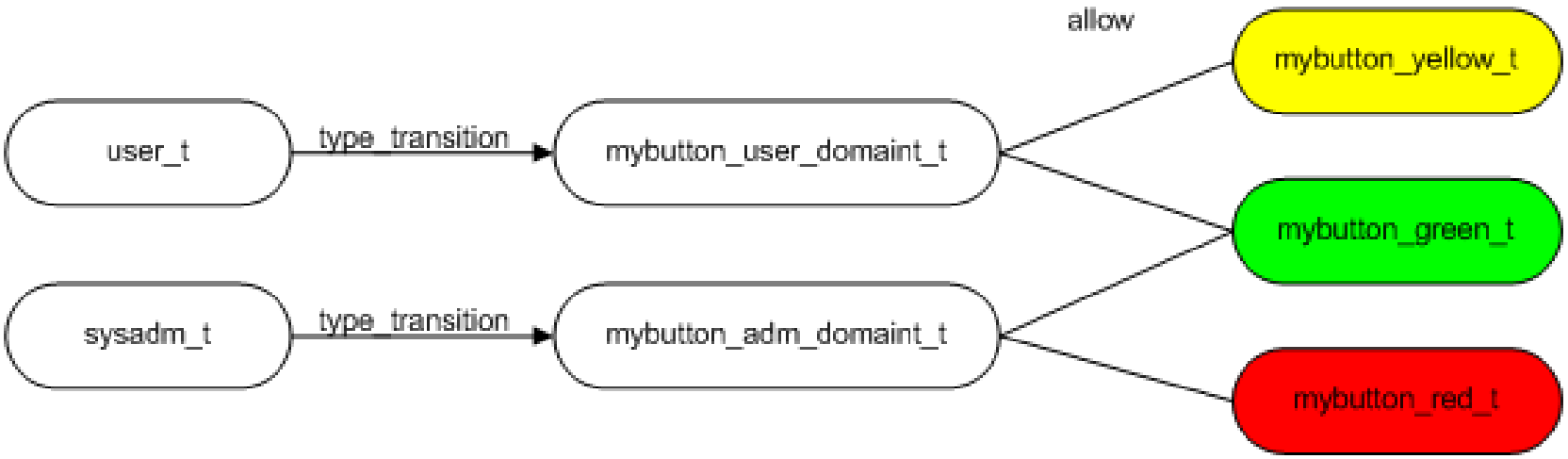
mybutton.fc:

- Маркирование файлов по умолчанию

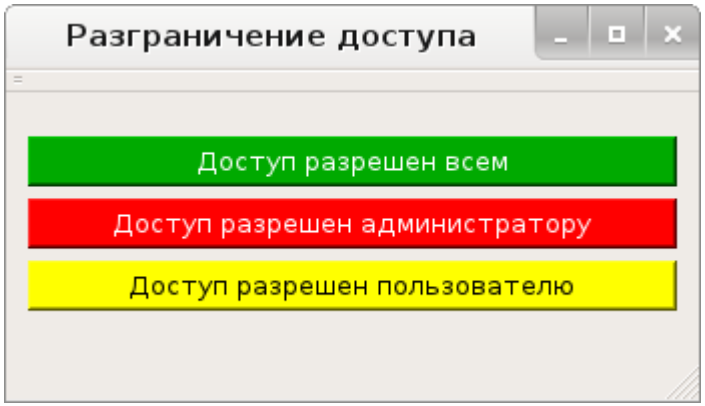
mybutton.pp:

- Бинарный модуль политики

Логика модуля политики



Программа, демонстрирующая разграничение доступа



Алгоритм проверки доступа:

1. Получение контекста программы
2. Инициализация проверки вектора доступа
3. Получение SID для контекста программы и контекста кнопки (myid, buttonid)
4. Инициализация вектора доступа (avd)
5. Проверка доступа:

int result = avc_has_perm(myid, buttonid, SECCLASS_MYBUTTON, MYBUTTON__CLICK ,NULL, &avd);