Порядок установки мандатных атрибутов (Смоленск 1.4, 1.5)

Рекурсивная смена метки безопасности на файлах и директориях

Общие сведения

В операционной системе специального назначения "Astra Linux Special Edition" релиз "Смоленск" (далее ОС СН) начиная с версии 1.4 и позднее невозможна рекурсивная смена метки безопасности на поддереве файловой системы. Например, ситуация возникает при попытке установить метку безопасности на файле или директории превышающую метку безопасности директории, содержащей данный файл или директорию.

Пример:

Корень файловой системы имеет максимальную метку безопасности, а также специальный флаг - ccnr, позволяющий записывать в корень файлы с меткой безопасности >= максимальный

```
root@dcm14:~# pdp-ls -Md
drwxr-xr-xm 30 root root _3::0xffffffffffffffff:CCNRALL
```

Создадим в корне файловой системы новую директорию

```
root@dcm14:~# mkdir /mydir0
```

Метка директории - нулевая

root@dcm14:~# pdp-ls -Md /mydir0

```
drwxr-xr-x 2 root root Уровень_0:Низкий:Нет:0x0 /mydir0
```

Поменяем метку на 1:0:0:0

```
root@dcm14:~# pdp-flbl 1:0:0:0 /mydir0
```

Это возможно, благодаря флагу ccnr родительской директории - /

root@dcm14:~# pdp-ls -Md /mydir0

```
drwxr-xr-xm 2 root root Уровень_1:Низкий:Нет:0x0 /mydir0
```

Теперь создадим ещё одну директорию и запишем в неё файл.

```
root@dcm14:~# mkdir /mydir1 && touch /mydir1/file
```

root@dcm14:~# pdp-ls -Md /mydir1

```
drwxr-xr-x 2 root root _0:::0x0 /mydir1
```

root@dcm14:~# pdp-ls -M /mydir1

```
 0
-rw-r--r-- 1 root root _0:::0x0 file
```

Попробуем рекурсивно поменять метку безопасности на файле и директории

```
root@dcm14:~# pdp-flbl -R 1:0:0:0 /mydir1
```

```
pdp-flbl: /mydir1:
```

Данное поведение обусловлено положениями ДП-модели контроля доступа, разработанной специалистами академии ФСБ России и реализованной в ОС СН, начиная с версии 1.4.

Механизм мандатного контроля доступа реализован, как и механизм дискреционного контроля доступа, в ядре ОС. При этом, принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа операции (чтение/запись/исполнение), мандатного контекста безопасности субъекта и метки безопасности объекта.
Правила принятия решения могут быть записаны следующим образом. Пусть контекст безопасности субъекта содержит уровень L0, уровень целостности iL0 и категории C0, а метка безопасности объекта содержит уровень L1, уровень целостности iL1 и категории C1. Определим операции сравнения для уровней и категорий:
1) уровень L0 меньше уровня L1 (L0<L1), если численное значение L0 меньше численного значения L1;
2) уровень L0 равен уровню L1 (L0==L1), если численные значения L0 и L1 совпадают;
3) уровень целостности iL0 меньше уровня iL1 (iL0<iL1), если численное значение iL0 меньше численного значения iL1;
4) уровень целостности iL0 равен уровню целостности iL1 (iL0==iL1), если численные значения iL0 и iL1 совпадают;
5) категории C0 меньше категорий C1 (C0<C1), если все биты набора C0 являются подмножеством набора бит C1;
6) категории C0 равны категориям C1 (C0==C1), если значения C0 и C1 совпадают;
7) операция записи разрешена, если L0==L1, iL0>=iL1 и C0==C1;
8) операция чтения разрешена, если L0>=L1, C0>=C1, iL0, iL1;
9) операция исполнения разрешена, если L0>=L1 и C0>=C1, iL0, iL1.

Поскольку запись файла в директорию является операцией записи, метки безопасности директории и файла должны совпадать. Т.е. в директории с меткой безопасности 0:0:0:0 при отсутствии специальных флагов (см. ниже) могут быть записаны только файлы с меткой безопасности 0:0:0:0. При изменении метки безопасности на поддерево файловой системы (как в примере выше) правомерность такого изменения проверяется для каждого объекта файловой системы в отдельности. В примере выше нельзя сменить метку безопасности на директорию */mydir1* на 1:0:0:0, т.к. она содержит файл с меткой безопасности 0:0:0:0. В тоже время нельзя сменить метку безопасности файла */mydir1/fil*e на 1:0:0:0, т.к. файл содержится в директории (т.е. объекте-контейнере) с меткой безопасности 0:0:0:0.

Порядок установки мандатных атрибутов

Как упоминалось выше, в ОС СН есть специальные флаги или "типы метки" для объектов-контейнеров, с помощью которых администратор безопасности может решить задачу рекурсивной смены метки безопасности на файловой системе. Их описание из руководства по КСЗ:

В ОС предусмотрено существование объектов-контейнеров (например, каталогов), т.е. объектов, которые могут содержать другие объекты. Метка безопасности объекта-контейнера определяет максимальную метку безопасности вложенных объектов. Тип метки безопасности может использоваться для того, чтобы изменять ее эффективное действие:

– тип метки ehole применяется к объектам-контейнерам и простым объектам для игнорирования мандатных правил разграничения доступа к ним;
– тип метки ccnr применяется к объектам-контейнерам и определяет, что объект 31 РУСБ.10015-01 97 01-1 контейнер может содержать объекты с различными метками безопасности, но не превышающими метку безопасности объекта-контейнера;
– тип метки ccnri применяется к объектам-контейнерам и определяет, что объект контейнер может содержать объекты с различными уровнями целостности, но не превышающими уровень целостности объекта-контейнера;
Ненулевой тип метки безопасности может быть установлен только привилегированным процессом. Перечисленные типы могут использоваться совместно. Таким образом, объект-контейнер может иметь тип: ccnr,ccnri,ehole.

Для того чтобы сменить метку безопасности на поддереве файловой системы в общем виде достаточно выполнить следующее:

1. Установить на все директории поддерева, начиная с верхней, метку безопасности с требуемым уровнем, набором категорий и флагом ccnr
2. Установить на все файлы поддерева метку безопасности с требуемыми уровнем конфиденциальности и набором категорий конфиденциальности
3. Снять (если не нужна) с директорий флаг ccnr

Пример:

```
root@dcm14:~# pdp-ls -Md /mydir1
```

```
drwxr-xr-x 2 root root _0:::0x0 /mydir1
```

```
root@dcm14:~# pdp-ls -M /mydir1
```

```
 0
-rw-r--r-- 1 root root _0:::0x0 file
```

Сначала меняем метку на директорию. И ставим ccnr

```
root@dcm14:~# pdp-flbl 1:0:0:ccnr /mydir1
```

root@dcm14:~# pdp-ls -Md /mydir1

```
drwxr-xr-xm 2 root root _1:::ccnr /mydir1
```

Меняем метку файла

```
root@dcm14:~# pdp-flbl 1:0:0:0 /mydir1/file
```

root@dcm14:~# pdp-ls -M /mydir1/file

```
-rw-r--r--m 1 root root _1:::0x0 /mydir1/file
```

Убираем флаг ccnr

```
root@dcm14:~# pdp-flbl 1:0:0:0 /mydir1
```

root@dcm14:~# pdp-ls -M /mydir1

```
-rw-r--r--m 1 root root _1:::0x0 /mydir1
```

При наличии нескольких вложенных директорий ccnr придётся ставить на каждую

Пример скрипта

Пример bash-сценария для рекурсивной смены метки безопасности.
ВНИМАНИЕ! Сценарий приведен именно для примера. Можете использовать его, но без гарантий.

```
#! /bin/bash

usage()
{
cat << EOF
Usage: $0 mac_label [path...]

EOF
}

set_label()
{
    local root_lbl=$(pdp-ls -Mdn / | awk '{print $5}')
    local max_lev=$(echo $root_lbl | cut -d':' -f1)
    local max_ilev=$(echo $root_lbl | cut -d':' -f2)

    find $2 -type d -exec pdp-flbl ${max_lev}:${max_ilev}:-1:ccnr,ccnri '{}' \;
    find $2 -type f -exec pdp-flbl $1 '{}' \;
    find $2 -type d | tac | xargs pdp-flbl $1
    return 0
}

if [[ -z $1 ]]; then
    usage
    exit 1
fi

mac_label="$1"
shift

if [[ -z $1 ]]; then
    set_label $mac_label $PWD
    exit 0
fi

while [[ -n $@ ]]; do
    set_label $mac_label $1
    shift
done

exit 0
```