БАЗОВАЯ СИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ В LINUX

Мурадов Э. К., Петров С. Н.
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники» (г. Минск)

В Linux разграничение прав доступа к ресурсам базируется на дискреционной модели управления доступом. Все ресурсы системы, в том числе устройства, представлены в виде файлов или ссылок на файловой системе. Каждый такой ресурс имеет базовые атрибуты доступа, согласно которым определяется возможность выполнения операции конечным пользователем.

Базовые атрибуты поделены на три подгруппы: права владельца, права прикрепленной группы пользователей и права для других, не попадающих под первые две группы пользователей. Каждая подгруппа состоит из атрибута права на чтения, права на запись и права на исполнения. Следует отметить, что права родительской директории не наследуются при создании нового файла или директории внутри, но учитываются при выдаче прав.

Помимо базовых атрибутов, могут использоваться расширенные атрибуты в POSIX-совместимых системах. Такие атрибуты позволяют выдать права доступа конкретному пользователю, при этом, не изменяя владельца файла, группы и принадлежности самого объекта. Расширенные атрибуты могут наследоваться в рамках одной директории и ее содержимого. Для этого требуется настройка расширенных атрибутов директории для нового содержимого в ней – по умолчанию атрибуты родителя не наследуются.

Процессы в Linux используют права доступа того пользователя, который его запустил. Для этого система клонирует UID (уникальный идентификатор пользователя) и GID (уникальный идентификатор группы пользователя) и применяет их к процессу.

В операционных системах на базе Linux присутствует суперпользователь – root. Для этого пользователя отсутствует проверка атрибутов доступа вне зависимости от того, кто является владельцем файла.

От имени суперпользователя выполняются многие процессы в системе как раз из-за того, что необходимы права разным процессам к разным ресурсам на файловой системе. Так же, многие системные службы, которые работают исключительно с данными обычного пользователя, требуют прав суперпользователя для своей корректной работы. Это является большим недостатком базовой системы управления доступами.

Из-за того, что все устройства в системе представлены в виде файлов и вышеуказанного ограничения, пользователю нельзя делегировать управление (полное либо частичное) некоторым устройством.

С суперпользователем связано еще одно ограничение системы: только он позволяет запускать процессы, которые могут использовать сетевые порты до 1024 включительно. Остальные порты после 1024 могут быть использованы любым пользовательским приложением без управления доступом. Это значит, что любое запущенное приложение может беспрепятственно использовать сетевые возможности всего устройства.

Для повышения безопасности и более гибкого управления доступами в ядро Linux, начиная с версии 2.6, добавлена программная платформа расширения LSM (Linux Security Modules). Данная платформа позволяет Linux поддерживать различные модели управления доступом, не отдавая предпочтения какой-либо отдельной реализации. При этом LSM работает на уровень выше, чем базовая система управления доступами. Запрос к программе, реализующей LSM, перейдет только в том случае, если будет разрешен доступ базовой системой.

Для реализации мандатной модели управления доступом в систему может быть добавлена система принудительного контроля доступа SELinux (Security-Enhanced Linux).