SELINUX В СОВРЕМЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМАХ НА БАЗЕ ЯДРА LINUX

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

Ключевые слова: модуль безопасности, Linux, контроль доступа.

Security Enhanced Linux (SELinux) – система, использующая модуль безопасности ядра Linux (LSM), которая реализовывает для операционной системы модели мандатного и ролевого управления контроля доступа. SELinux работает поверх классической дискретной модели управления доступом, встроенной в ядро Linux.

Базовой единицей для разграничения доступа в SELinux является политика. Политика определяет доступ пользователей к ролям, доступ ролей к доменам и доступ доменов к типам. Пользователь в SELinux соответствует одному или нескольким пользователям Linux, принципиально совпадает с определением группы пользователей для дискретной модели. Домены объединяют субъекты и объекты в группы, внутри этих групп определяют разрешенные действия субъектов над объектами. Под объектами понимаются файлы, устройства и процессы, над которыми совершаются действия; под субъектами понимаются пользователи и процессы, которые совершают некоторые действия.

Политики разделяются на два типа, в зависимости от модели управления, которую реализуют: для ролевого разграничения доступа –проверка связанных типов (Type Enforcement), для мандатного – Multi-Level Security (MLS), который реализует модель Белла-Лападулы.

SELinux имеет три режима работы: ограничение доступа в соответствии с политиками, когда запрещено все, что не разрешено в явном виде (Enforcing); логгирование действий, нарушающих настроенные политики, все действия разрешены (Permissive); полное отключение (Disabled).

Современные операционные системы на базе ядра Linux чаще всего поставляются вместе с SELinux или похожими системами (AppArmor для Ubuntu). По умолчанию SELinux поставляется в режиме Enforcing.

Программное обеспечение разрабатывается и распространяется с собственными политиками SELinux. Такие политики ограничивают права приложения в системе, так как базовая модель не позволяет точно настроить привилегии приложения, а только использовать права пользователя, который это приложение запускает. Это является глав-

ным недостатком классической модели Linux, так как многие серверные приложения запускаются от имени суперпользователя.

В виртуализации и контейнеризации SELinux используется для изоляции данных каждой виртуальной машины (или контейнера). В этом случае используются MLS политики. Популярный в настоящее время инструмент оркестрации контейнеров Kubernetes (k8s) также поддерживает метки SELinux, т. е. политики применяются и к создаваемым k8s-контейнерам.

SELinux позволяет закрыть некоторые уязвимости приложений, например, в Docker. Уязвимость заключается в том, что пользователь, который имеет право взаимодействовать с приложением (состоит в группе docker), может использовать его для повышения своих привилегий в основной системе. Политика SELinux может заблокировать доступ к критическим файлам системы, через которые реализуется такая уязвимость, несмотря на то, что приложение Docker запускается с правами суперпользователя.

Последние версии популярной мобильной системы Android также поставляются вместе с SELinux, начиная с версии 4.3 (полноценно с версии 5.0). Android использует SELinux для обеспечения мандатного контроля доступа (MAC) ко всем процессам, в том числе работающим с привилегиями суперпользователя. SELinux определяет границ изолированной среды каждого приложения в системе Android.