отдельного модуля сети (например, периметр Интернет, ЦОД, ЛВС, сеть филиала). Затем все сегменты соединяются через сетевые механизмы Cisco Packet Tracer. После развёртывания сетей обучающиеся меняются сетями и модулями. При этом решаются задачи изучения и анализа конфигурации новой сети, поиска и устранения ошибок проектирования и реализации, если таковые имеются. На протяжении всей игры преподавателем могут даваться различные вводные инструкции по изменению политик безопасности, порядка функционирования сетевой инфраструктуры и требований к сетям передачи данных.

ЛИТЕРАТУРА

1. Колегов Д. Н. Обучение на платформе CISCO основам построения защищённых вычислительных сетей // Прикладная дискретная математика. Приложение. 2010. № 3. Р. 53–55.
2. Morozov E. Cisco Packet Tracer King-of-the-Hill Multiuser Game [Электронный ресурс]. Режим доступа: http://www.netskills.hu/registztracio/sites/upload/conf2011/prezi/1-8_evgeny_morozov.pdf

УДК 004.94

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ МАНДАТНОГО И РОЛЕВОГО УПРАВЛЕНИЯ В СИСТЕМЕ *RSBAC*

П. Ю. Свиридов

Рассматриваются особенности реализации мандатных и ролевых механизмов системы управления доступом *RSBAC* [1] в операционной системе (ОС) GNU/Linux. Система *RSBAC* разработана в 1996–1997 гг. Амоном Оттом в целях повышения безопасности ОС на базе ядра Linux и представляет собой надстройку над ядром и набор утилит администрирования. Система построена в соответствии с архитектурой *GFAC*, предложенной Абрамсом и ЛаПадула, и состоит из нескольких модулей безопасности, каждый из которых реализует определенную политику безопасности.

В системе *RSBAC* реализованы механизмы безопасности, использующие следующие политики управления доступом:

- RC (*Role Compatibility*) — политика совместимости ролей Отта;
- MAC (*Mandatory Access Control*) — мандатная политика Белла — ЛаПадулы;
- ACL (*Access Control Lists*) — дискреционная политика на основе механизма списков доступа;
- PM (*Privacy Model*) — политика защиты персональных данных на основе модели Фишер-Хабнера;
- FF (*File Flags*) — политика назначения флагов доступа файлам;
- Auth (*Authenticated User*) — политика авторизации пользователей.

Основными особенностями реализации механизмов управления доступом в системе *RSBAC* являются:

- ассоциирование с каждой сущностью ОС множества атрибутов, отражающих их различные свойства, необходимые для реализации политик управления доступом (например, атрибутами субъектов ОС являются их роли и уровни доступа в рамках ролевой и мандатной модели управления доступом соответственно);
- использование более 30 различных видов доступа и прав доступа;
- использование многоуровневой решетки безопасности;

- при реализации *-свойства в модели Белла — ЛаПадулы задаются верхняя и нижняя границы уровней безопасности;
- интерпретация роли в политике RC, как набора пар расширенных прав доступа и сущностей определенного типа.

Перечисленные особенности реализации системы *RSBAC* не позволяют применить к ней аппарат разработанных ДП-моделей [2] для формального исследования и обоснования свойств и требований безопасности ОС с ролевым и мандатным управлением доступом.

Для адекватного отражения этих особенностей в ДП-моделях предлагается язык описания последних расширить аналогично тому, как это сделано в ДП-модели [3] для пакета безопасности SELinux в ОС GNU/Linux.

1. Вводится множество атрибутов, ассоциированных с сущностями и учитываемых при проверке прав доступа субъектов к сущностям.

2. Дополнительно к правам и видам доступа, традиционно рассматриваемым в ДП-моделях, вводятся новые права, виды и типы доступа, специфичные для *RSBAC*. Такими правами доступа являются $clone_r$ — право доступа на создание (клонирование) процесса, $chdir_a$ — доступ для изменения рабочей директории, $type_comp_ipc_t$ — тип сущностей системы межпроцессного взаимодействия. При необходимости возможно агрегирование прав и видов доступа одним с более высоким уровнем абстракции.

3. С учётом того, что в *RSBAC* выполнено связывание мандатного и ролевого управления доступом, производится согласование механизмов мандатных и ролевых ДП-моделей.

4. Вместо линейной решётки уровней доступа и конфиденциальности информации $(L, \leq)$ вводится многоуровневая решетка безопасности $(X \times L, \leq)$, где $(X, \leq)$ — решётка подмножеств категорий информации.

5. В соответствии с изменением определения роли модифицируются ролевые механизмы ДП-моделей. Если R — множество ролей, R_r — множество прав доступа, T — множество типов, то $P \subseteq (R_r \times T)$ — множество прав доступа ко всем сущностям одного типа, и функция прав доступа ролей $PA : R \rightarrow 2^P$ задает для каждой роли множество прав доступа к сущностям заданного типа.

С использованием этих расширений языка ДП-моделей предполагается разработка ДП-модели системы *RSBAC* по стандартной схеме построения ДП-моделей в [2].

ЛИТЕРАТУРА

1. RSBAC handbook. http://rsbac.org/documentation/hand_book.
2. Девянин П. Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учеб. пособие для вузов. М.: Горячая линия-Телеком, 2011. 320 с.
3. Качанов М. А. Разработка ролевой модели безопасности управления доступом и информационными потоками компьютерной системы SELinux // Прикладная дискретная математика. Приложение. 2011. № 4. С. 44–46.