УДК 004.056.53

Фильтрация сетевых пакетов на основе мандатных меток в операционной системе «Эльбрус»

А.А. Имкенов
Московский физико-технический институт (государственный университет)
АО «МЦСТ»

Обеспечение защищенности информации является одной из важнейших задач при разработке операционной системы. В операционной системе «Эльбрус» применяется мандатное разграничение доступа на действия субъектов над объектами. Всем пользователям (субъектам) и файлам (объектам) назначаются метки (уровни) доступа, например, «несекретно», «секретно», «совершенно секретно». На основе сравнения меток субъекта и объекта принимается решение о предоставлении доступа. Сетевые пакеты, отправляемые процессами, наследуют метки этих процессов. Мандатная метка устанавливается в дополнительное поле заголовка IPv4-пакета по стандарту RFC 1108.

В целях защиты информации при межсетевом взаимодействии применяется межсетевой экран (МЭ) – комплекс аппаратных и программных средств в компьютерной сети, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами. В ядре операционной системы «Эльбрус» фильтрация сетевых пакетов реализована на основе подсистемы Netfilter [2].

Целью работы являлось исследование и расширение схемы фильтрации сетевых пакетов в системе Netfilter для поддержки мандатных меток сетевых пакетов. Рассмотрена схема фильтрации сетевых пакетов в ядре операционной системы «Эльбрус». Основу работы Netfilter составляют цепочки – упорядоченные наборы правил. Сетевой пакет, принятый/отправленный системой, последовательно проходит серию цепочек. Правила состоят из критериев и действий. Если сетевой пакет удовлетворяет критерию правила, к нему будет применено соответствующее действие [1].

В схеме фильтрации применяются 3 цепочки: INPUT – входящие пакеты, FORWARD – исходящие пакеты, OUTPUT – исходящие пакеты. (рисунок 1).

В качестве критериев выступают поля заголовков сетевых пакетов: адрес отправителя/получателя, номер сетевого интерфейса, тип транспортного протокола и др. Допустимыми действиями являются ACCEPT – принять пакет и DROP – отклонить пакет [1].

Результатом работы стало создание модуля ядра xt_LABEL, предназначенного для фильтрации сетевого трафика по мандатным меткам. Модуль xt_LABEL осуществляет разбор заголовков сетевых пакетов в цепочках INPUT, FORWARD и OUTPUT для выделения мандатной метки (Рисунок 2). На основе сравнения этой метки и метки хоста, которому предназначается пакет, принимается решение о принятии либо блокировке.

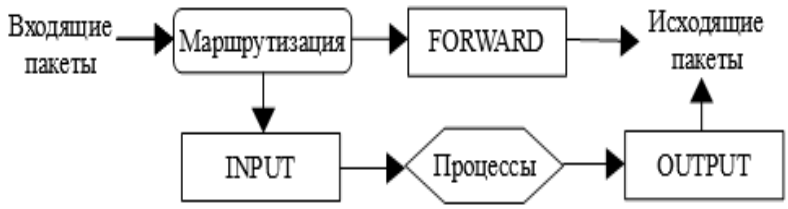

Рис. 1. Схема фильтрации Netfilter

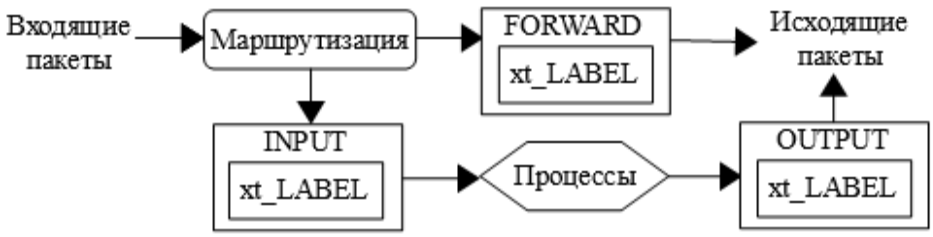

Рис. 2. Разработанная схема фильтрации

Литература

1. *Engelhardt J., Bouliane N.* Writing Netfilter modules. Netfilter Core Team, 2012.
2. *Russel R., Welte H.* Linux netfilter hacking. Netfilter Core Team, 2012.