На следующем шаге выделим границы рисунка вен на исходном изображении. Для этого реализован детектор границ Канни.

Применив к результату работы детектора границ Канни метод адаптивной пороговой обработки Вульфа, получим рисунок границ вен (границы отмечены белым цветом).

На следующем шаге необходимо получить рисунок вен ладони, где вены полностью закрашены черным цветом. Для этого модифицируем детектор границ Канни. Детектор границ Канни позволяет находить направление градиента в каждой точке исходного изображения, если в направлении, противоположном направлению градиента, заполнять пиксели изображения. Действуя таким образом, можно получить полностью локализованный рисунок вен ладони [3].

На полученном изображении применим алгоритм утоньшения линий Зонга-Суня, чтобы получить тонкую структуру рисунка вен ладони.

Таким образом, применяя алгоритмы цифровой обработки изображений, изображение рисунка вен ладони было полностью локализовано и подготовлено для последующего процесса выделения особых точек, необходимого для решения задачи биометрической идентификации личности.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Nadort A. The Hand Vein Pattern Used as a Biometric Feature: Literature thesis for Master of Science Programmed Physics of Life // Amsterdam: Medical Natural Sciences at the Free University, 2007. 179 c.
2. Note on CASIA Palmprint Image Database [Electronic resource]. – Mode of access: http://biometrics.idealtest.org/dbDetailForUser.do?id=5. – Date of access: 19.03.2020.
3. Исмаилов Р. Р., Мельников В. А. Локализация рисунка вен ладони в биометрической системе идентификации с использованием детектора границ Канни // Актуальные исследования и инновации: сборник статей II Международной научно-практической конференции. Самара: ЦНИК, 2018. 68 с.

ПОЛИТИКИ МАНДАТНОГО РАЗГРАНИЧЕНИЯ ДОСТУПА В SELINUX

Е. Е. Попко, Ю. М. Минин, И. Н. Щербак

Белорусский государственный университет, Минск, Беларусь
E-mail: popko@bsu.by

Изучение моделей контроля доступа и механизмов их реализации в современных операционных системах является актуальной задачей в подготовке специалистов по специальности «Компьютерная безопасность» и смежных с ней. Для изучения различных механизмов контроля доступа рассмотрена возможность использования операционной системы CentOS, в которой в качестве основного механизма применяется

дискреционный контроль доступа, а управление доступом на основе ролей, мандатное управление и контроль доступа на основе типов могут быть реализованы в рамках широко известной подсистемы защиты ОС Linux, SELinux. В статье рассмотрена реализация подсистемы безопасности SELinux: поддерживаемые формы контроля доступа, модули политик, сценарии реализации, что позволяет использовать изложенный материал для обучения студентов по соответствующим дисциплинам.

Ключевые слова: операционная система; мандатное управление доступом; Type Enforcement (TE); SELinux; многоуровневая политика безопасности (MLS/MCS); политика безопасности minimum; CentOS.

Изучение моделей разграничения доступа и механизмов их реализации в современных операционных системах является актуальной задачей в подготовке специалистов по специальности «Компьютерная безопасность» и смежных с ней.

Операционные системы управляют большим количеством объектов с различными требованиями к ограничениям доступа к ним и в настоящее время редко встречаются подсистемы защиты, использующие только дискреционное управление доступом. Как правило, применяется нескольких различных механизмов разграничения доступа, основными из которых являются: дискреционный (discretionary access control, DAC), мандатный (mandatory access control, MAC) и ролевой (role-based access control, RBAC). Рассмотрим их реализацию на примере операционной системы семейства Linux.

В Linux в качестве основного механизма применяется дискреционный контроль доступа, реализованный в виде битов защиты. Для каждого файла определены владелец, группа, а также указаны права доступа к этому файлу. Права доступа определены для трех категорий: пользователь - владелец файла, группа-владелец и все остальные пользователи. Каждая из категорий может иметь комбинацию разрешений на чтение, запись и выполнение (r, w, x) для файла или каталога. В качестве дополнительного механизма используются списки контроля доступа (access control list, ACL).

Управление доступом на основе ролей, мандатное управление доступом и контроль доступа на основе типов (type enforcement, TE) могут быть реализованы в рамках широко известной инфраструктуры защиты ОС Linux, SELinux [1]. Подсистема безопасности SELinux включает в себя модули ядра, разделяемые библиотеки для написания приложений, утилиты.

Все процессы, пользователи и файлы в рамках SELinux имеют контекст безопасности, который представляет собой набор полей, с различным содержимым в зависимости от политики безопасности. Контекст безопасности – это набор меток, имеющих вид:

пользователь : роль : тип : [уровень], где

- пользователь - атрибут в системе SELinux, ассоциированный с одним или более пользователем компьютерной системы;
- роль - атрибут в системе SELinux, ассоциированная с одним или более типом, к которым пользователь SELinux имеет доступ;
- тип - атрибут в системе SELinux, определяющий возможные виды доступа сущностей данного типа при использовании механизма Type Enforcement;
- уровень - атрибут в системе SELinux при использовании мандатных механизмов Multy-Level Security или Multy-Category Security.

Политики определяют набор правил, которые описывают возможные отношения между процессами и файлами согласно их контекстам безопасности. Для файлов контексты безопасности хранятся в виде расширенных атрибутов в файловой системе, для процессов и портов маркировкой управляет ядро. Помимо ограничений на выполнение операций могут быть заданы правила присваивания и трансформации меток.

SELinux позволяет писать собственные политики или использовать поставляемые вместе с дистрибутивом Linux. Рассмотрим реализацию SELinux на примере операционной системы CentOS.

По умолчанию в CentOS используется целевая политика, которая реализует 4 формы контроля доступа [2]:

- Type Enforcement (TE) – принудительное использование типов, основной механизм контроля доступа,
- Управление доступом на основе ролей (RBAC) основано на пользователях SELinux и не используется в конфигурации целевой политики по умолчанию.
- Многоуровневая безопасность (MLS) редко используется и может скрываться в целевой политике по умолчанию.
- Multi-Category Security (MCS) – расширение Multi-Level Security, используемое в целевой политике для реализации разделения виртуальных машин и контейнеров через sVirt.

В данном дистрибутиве операционной системы доступны три типа политик: целевая политика targeted, minimum, MLS/MCs [3]. Рассмотрим их более подробно.

Целевая политика targeted – это политика по умолчанию. Если используется данная политика, процессы, которые являются целевыми, запускаются в ограниченном домене, остальные процессы запускаются в неограниченном домене. Например, по умолчанию пользователи, прошедшие авторизацию, работают в домене unconfined_t и системные процессы запущенные init-ом запускаются в домене initrc_t - оба домена неограниченные. Процессы, работающие в неограниченных доменах, ис-

пользуют исключительно правила DAC. Целевая политика призвана защитить ключевые процессы без отрицательного влияния на работу конечных пользователей, и большинство пользователей системы могут даже не знать, что SELinux работает.

Политика безопасности minimum разработана на основе политики targeted специально для пользователей, желающих потренироваться в создании собственных политик для SELinux. Политика minimum содержит те же модули, что и политика targeted, однако, не задействует их. Изначально SELinux не ограничивает объекты системы безопасности, но при желании можно, например, установить модули для контроля процессов. В этом случае потребуется явно настроить необходимые разрешения в политике безопасности.

Данная политика нужна для использования в системах с небольшим количеством ресурсов или для того что бы ограничить определенное количество доменов, не тратя время на выгрузку модулей при использовании политики targeted.

Многоуровневая политика безопасности (MLS/MCS) реализует модель Bell-LaPadula и позволяет применять более сложные элементы управления. Для поддержки MLS используется уровень допуска из контекста безопасности, который состоит из:

- чувствительности (является иерархической, диапазон s0 (самый низкий) - s15 (самый высокий)),
- категории (является необязательной, диапазон c0 - c1023).

Для того что бы субъект имел право чтения объекта, чувствительность субъекта должна быть больше или равна чувствительности объекта, а категория объекта совпадала или входила в диапазон категорий субъекта. Для того что бы субъект имел право записи объекта, чувствительность субъекта должна быть меньше или равна чувствительности объекта, а категория субъекта совпадала или входила в диапазон категорий объекта.

Основными этапами настройки SELinux являются: выбор или создание собственной политики, включение модулей, настройка пользователей, портов, контекстов, кастомизация политик.

Заключение. В данной статье рассмотрены три модуля политик подсистемы безопасности SELinux и описаны сценарии, реализующие различные варианты политик, что позволяет использовать изложенный материал для обучения студентов по соответствующим дисциплинам.

БИБЛИОГРАФИЧЕСКИЕ ССЫЛКИ

1. Девянин П. Н., Кулямин В. В., Петренко А. К. и др. Интеграция мандатного и ролевого управления доступом и мандатного контроля целостности в верифициро-

ванной иерархической модели безопасности операционной системы // Труды ИСП РАН, Т.32, вып. 1, 2020. С. 7–26.
2. Vermeulen S. SELinux System Administration. Second Edition // UK Birmingham: Packt Publishing. 2016. 300 p.
3. CentOS 8: SELinux. [Electronic resource]. – Mode of access: https://www.server-world.info/en/note?os=CentOS_8&p=selinux&f=2. – Date of access: 14.02.2020.

ПРИМЕНЕНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ПРОЦЕССЕ ПРОГНОЗИРОВАНИЯ НАУЧНО-ТЕХНОЛОГИЧЕСКОГО И ИННОВАЦИОННОГО РАЗВИТИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Н. Л. Михальченко[1], И. В. Салтанова[2]

[1]ООО «Customertimes Corp», [2]ГУ «БелИСА», г. Минск, Беларусь
E-mail: natalya.mihalchenko@customertimes.com; saltanova@belisa.org.by

Разработан информационный ресурс для обработки различного типа данных при прогнозировании научно-технологического и инновационного развития страны. Используемое программное обеспечение и языки программирования обеспечивают динамику и гибкость системы. Разработанное веб-приложение позволяет отслеживать изменение тенденций научно-технического прогресса.

Ключевые слова: технологическое прогнозирование; форсайт; инновации; экономический рост; реляционные базы данных; анализ больших данных.

В течение 2018-2019 гг. в Республике Беларусь выполнялись работы по формированию Комплексного прогноза научно-технического прогресса для Республики Беларусь на 2021 – 2025 гг. и на период до 2040 г. (КП НТП).

В настоящее время в мировой практике прогнозирования используются самые разные методологические подходы, что является следствием постоянно изменяющихся экономических условий и имеющихся у исследователей возможностей. В отличие от предыдущих прогнозов национального масштаба, впервые в Республике Беларусь проект КП НТП выполнялся как Форсайт-исследование.

Одной из первоочередных задач разработки прогноза являлось формирование перечня перспективных для Республики Беларусь инновационных технологий, продуктовых групп, товаров или услуг (объектов прогнозирования) [1].

Формирование экспертного сообщества для такого масштабного Форсайт-проекта производилось впервые. Работа экспертов была организована по методу Дельфи в три этапа в составе групп, которые были сформированы по отраслям экономики. В Форсайт-исследовании приня-