

SELINUX ЯК ЗАСІБ ЗАБЕЗПЕЧЕННЯ КРИТЕРІЇВ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ СИСТЕМАХ ВІД НСД

М. В. Кучменко¹

¹Національний технічний університет України «Київський політехнічний інститут»

Анотація

В даній роботі розглянуто розширення базової моделі безпеки SELinux, яка застосовується в ядрі операційної системи Linux. Розкривається принцип роботи системи, переваги та недоліки. Запропоновано використання SELinux в автоматизованих системах для сертифікації по НД ТЗІ та наведено критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, які ця система забезпечує.

Ключові слова: захист від НСД, SELinux, сертифікація, мандатне керування доступом, політика безпеки

Вступ

Одними з головних проблем, з якими стикаються фахівці при проектуванні комп'ютерних систем на підприємствах, є захищеність від несанкціонованого доступу та сертифікація системи згідно з законодавством України. Система прав в UNIX є простою та має обмежені можливості конфігурації. Якщо зловмисник перехопить управління однієї з програм, то зможе отримати доступ до даних або ресурсів, які програма в звичайному режимі не використовує.

SELinux – це модуль безпеки, вбудований в ядро Linux, у якому реалізована система примусового контролю доступу. Ця система може працювати паралельно з класичною системою контролю доступу.

В даній роботі розглянуто принципи роботи модуля SELinux, його переваги та недоліки, а також критерії оцінки захищеності інформації від несанкціонованого доступу згідно з НД ТЗІ, які забезпечують можливість сертифікації обчислювальної системи.

1. Опис SELinux

SELinux – це розширення базової моделі безпеки операційної системи Linux, у якому додано механізм мандатного управління доступом. Розширення SELinux визначає правила звертання до об'єктів системи (файлів та пристроїв) для користувачів та програм (суб'єктів). Таким чином, операційна система забезпечує чітке виконання заданої політики та перешкоджає роботі програм, які працюють всупереч встановленим правилам.

SELinux працює «після» традиційної системи безпеки UNIX (DAC). Це означає, що операції, які заборонені у системі DAC, не можуть бути дозволені в SELinux. Саме тому SELinux конкретизує та доповнює дії, які було дозволено через DAC. При цьому робота SELinux є незалежною від системи DAC.

Виділяють чотири основні кроки, за якими працює SELinux, для забезпечення контролю звернення процесів до ресурсів ОС.

По-перше, всі суб'єкти (процеси) та об'єкти (файли, системні виклики та ін.) взаємодії відмічають за допомогою спеціальних поміток, що називають контекстом безпеки. Процеси помічаються під час запуску, файли – під час створення або установки ОС. Їх мітки зберігаються в розширених атрибутах файлової системи. Системні виклики помічаються при компіляції модуля SELinux.

По-друге, коли суб'єкт намагається виконати яку-небудь дію по відношенню до об'єкта, інформація про цю дію надходить до обробника подій SELinux.

По-третє, обробник подій дивиться на контекст безпеки суб'єкта та об'єкта, та, перевіривши узгодженість цієї дії з прописаною раніше політикою, приймає рішення стосовно можливості виконання зазначеної дії.

І, *четверте*, якщо дія в результаті виявляється правомірною (тобто узгодженою із встановленою політикою) об'єкт (програма) продовжує працювати у звичайному режимі. В іншому випадку вона або примусово завершується або отримує ввічливу відмову. На рисунку 1 показано принцип роботи SELinux

Насправді ж контекст безпеки (мітка) складається не з одного, а з чотирьох компонентів: імені користувача, типу, ролі суб'єкта та рівня доступу. Кожен користувач SELinux може виконувати кілька ролей. В рамках кожної з них йому доступно декілька типів суб'єктів, а кожен суб'єкт, в свою чергу, може мати доступ до певної кількості об'єктів. Подібно до груп користувачів у класичній моделі управління доступом UNIX, ролі виконуються для наділення процесів користувача різними видами уповноважень. Проте фактично вони потрібні лише для того, щоб тонко врегулювати доступ користувачів до певних даних. Таким чином, при супроводі комп'ютерної інфраструктури великих підприємств, їх працівники

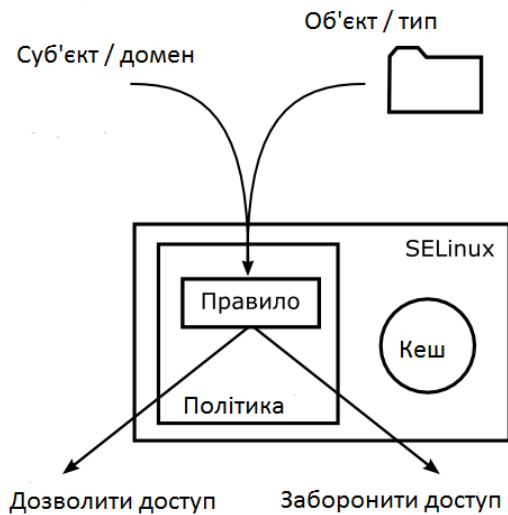


Рис. 1. Схема роботи SELinux з об'єктами та суб'єктами можуть мати різні рівні доступу до певної інформації (це в першу чергу стосується воєнних та державних підприємств).

Спираючись виключно на правила заданої політики SELinux спостерігає за виконанням програм. Цей метод називається обов'язковим контролем доступу – Mandatory Access Control (скорочено MAC). Якщо правило порушується – SELinux забороняє виконувати операцію або реєструє попередження. При цьому SELinux не завершує роботу програми, що порушує правила. Від програми залежить, як вона відреагує на ситуацію, в якій не зможе звернутися до певного файлу або скористуватись мережевим інтерфейсом. Правила MAC забезпечують значно ретельніший контроль безпеки, аніж система прав доступу UNIX. За допомогою MAC програмі можна заборонити доступ до певних каталогів та мережевих функцій, незалежно від прав доступу або облікових записів, з якими вона працює. Оскільки ці правила відслідковуються на рівні ядра, вона діє навіть у тому випадку, коли програма виходить з-під контролю через помилку або недоробку в галузі безпеки.

Робота SELinux засновується на двох базисних принципах. Це, по-перше, правильне позначення всіх файлів та процесів, завдяки так званому контексту захисту. По-друге, це правила, які повинні виконуватись процесами, за якими ведеться спостереження.

SELinux може працювати у двох режимах – Permissive та Enforced. У першому випадку (режим Permissive) дозволяється порушення політики безпеки, воно лише реєструється у журналі безпеки. Тобто, по суті SELinux не працює і не забороняє жодних дій, лише реєструючи порушення у системному журналі. Що ж стосується режиму Enforced – у ньому порушення політики безпеки призводять до блокування дії, яка стала причиною цього порушення. SELinux у цьому режимі працює повністю. Проте, поряд з усіма перевагами, SELinux має певні недоліки. Файли потрібно позначати розширеними атрибутами, щоб забезпечити їх правильну взаємодію з SELinux. Для цього потрібні файлові системи, які підтримують ці розширені атрибути.

Політика безпеки SELinux для всієї системи містить більше ста тисяч правил, так що її створення, налагодження та підтримка в актуальному стані віднімають надто багато часу і сил. У реальності, створення «з нуля» такої політики безпеки для діючої або проектованої комп'ютерної системи виправдано в небагатьох випадках – якщо характер інформації вимагає виняткової надійності та захищеності сервера.

Однак прогрес не стоїть на місці і всі ці проблеми, безумовно, привертають пильну увагу розробників. Уже створено кілька повноцінних наборів правил, які можна використовувати в типових ситуаціях на серверах і домашніх комп'ютерах. Все, що потрібно від системного адміністратора – вибрати одну з готових політик безпеки і перезавантажити комп'ютер з включеним SELinux. При цьому сам SELinux також постійно вдосконалюється – як з точки зору створення та розвитку політик безпеки, так і через взаємодію з розробниками і модифікацію вже існуючих програм.

2. Критерії оцінки захищеності інформації

Критерії оцінки інформаційної безпеки є методологічною базою для визначення вимог захисту комп'ютерних систем від несанкціонованого доступу, створення захисних систем та оцінки ступені захищеності. При розробці захищених комп'ютерних систем важливо порівнювати за допомогою критеріїв функціональність та механізми захисту інформації. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу описані в нормативному документі НД ТЗІ 2.5-004-99. Визначення цих критеріїв необхідне для складання функціонального профілю та сертифікації комп'ютерної системи.

SELinux дозволяє забезпечити на програмному рівні захист інформації, що обробляється в автоматизованих системах класу «1», «2» та «3» від загроз несанкціонованого доступу до інформації однієї або кількох категорій конфіденційності. Навідміну від ОС Windows, де стандартними методами неможливо забезпечити керування доступом адміністративного типу, операційна система з SELinux дозволяє реалізувати довірчий та адміністративний тип керування доступом до інформаційних об'єктів.

Операційна система з активованою суворою політикою SELinux, на відміну від стандартної моделі розмежування прав доступу в Linux, має такі переваги:

- Всі файли в системі промарковані контекстами. Тому політика конфіденційності відноситься абсолютнo до всіх об'єктів комп'ютерної системи;
- Система здійснює розмежування доступу на підставі атрибутів доступу користувача, процесу та захищеного об'єкта;
- Сувора політика дозволяє визначати конкретних користувачів і процеси, які мають і не мають права одержувати інформацію від об'єкта, модифікувати його.

Такі функції дозволяють задовольнити такі критерії як:

- Базова довірча конфіденційність (КД-2);
- Базова адміністративна конфіденційність (КА-2);
- Базова довірча цілісність (ЦД-2);
- Базова адміністративна цілісність (ЦА-2);

Також в SELinux є захищений журнал від НСД, до якого є утиліти, що полегшують роботу з ним. Таким чином, забезпечується критерій «Захищений журнал» (НР-2). SELinux дозволяє визначити множину ролей користувачів та розподілити обов'язки на дві адміністративні ролі: адміністратора безпеки та іншого адміністратора, чим забезпечує критерій «Розподіл обов'язків на підставі привілеїв (НО-3)». Одиночна ідентифікація та автентифікація (НИ-2) гарантується стандартними функціями Linux та механізмами SELinux щодо захисту даних автентифікації від несанкціонованого доступу, модифікації або руйнування. Крім того, для автоматизованих систем першого класу можливо підняти рівень критеріїв гарантій з другого до четвертого і отримати КД-4, КА-4, ЦД-4, та ЦА-4, тому що в такому випадку виконується умова, за якою політика відноситься до всіх об'єктів комп'ютерної системи. Якщо цей список доповнити додатковими утилітами чи налаштуваннями, то легко отримати функціональний профіль, по якому можливо сертифікувати систему комп'ютерну систему.

Висновок

Розширення SELinux є безкоштовним і вбудованим в більшість операційних систем Linux. SELinux задовольняє розглянуті критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Він є надійною системою, яка дозволяє реалізовувати автоматизовану комп'ютерну систему довірчого або адміністративного типу керування доступом до інформаційних об'єктів з високими рівнями гарантій та сертифікувати систему по НД ТЗІ.

Перелік використаних джерел

1. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. — Київ.:ДСТСЗІ СБ України, 1999.
2. Information extraction [Електронний ресурс] — Вікіпедія: 2015. — Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/SELinux_extraction.
3. Fedora project [Електронний ресурс] — Fedora project: 2015. — Режим доступу до ресурсу: https://docs.fedoraproject.org/ru-RU/Fedora/_extraction.
4. DeveloperWorks [Електронний ресурс] — Режим доступу до ресурсу: https://www.ibm.com/developerworks/ru/library/selinux_extraction.