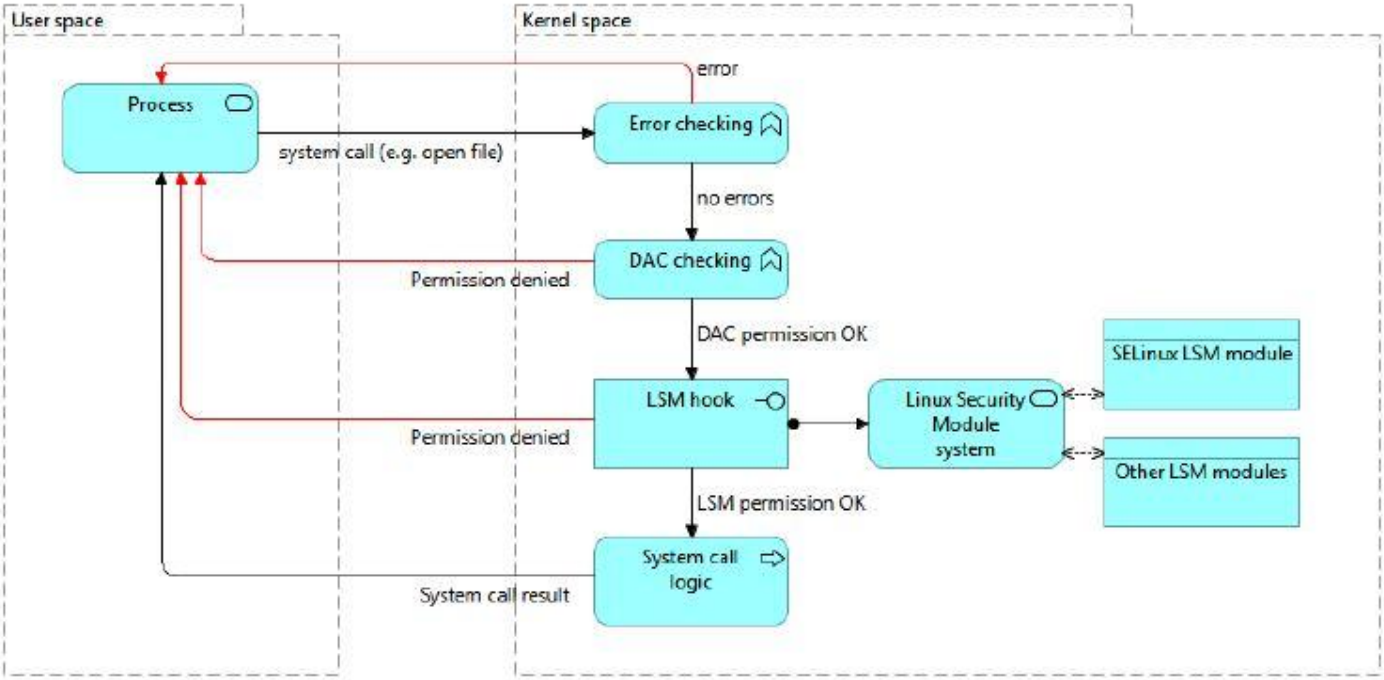
???????? ? Linux security modules

Система безопасности основана на дополнительном хуке (LSM hook) при вызове системных (ядерных) функций. Система модульная, и SELinux - один из модулей, который предоставляет функции безопасности. DAC система находится ниже. Стек вызовов функции:



LSM hook не предоставляет функций безопасности - это просто хук. Далее идет вызов зарегистрированного модуля(ей) LSM Framework. В LSM Framework можно зарегистрировать один эксклюзивный модуль и неэксклюзивные.

Модуль	Особенности	Где используется	Тип
SELinux	Метки безопасности (label-based), очень гибкая и строгая политика	RHEL, Fedora, CentOS, Android	Экск.
AppArmor	Основан на путях (path-based), проще в настройке	Ubuntu, Debian, openSUSE	Экск.
Smack (Simplified Mandatory Access Control Kernel)	Проще, чем SELinux, тоже использует метки, но менее гибкий	Встроенные системы (Tizen, некоторые IoT-устройства)	Экск.
TOMOYO Linux	Основной акцент на управление доступом на основе процессов и истории их действий (обучение)	Япония, встраиваемые системы	Неэкск.

Модуль	Особенности	Где используется	Тип
Yama	Маленький LSM для ограничения `ptrace` (трассировки процессов)	Включён в ядро по умолчанию (Ubuntu, Debian, Arch)	Неэкск.
Landlock	Новый LSM (с 2021 г., Linux 5.13+), даёт приложениям возможность ограничивать **себя** (sandboxing)	Современные Debian/Ubuntu, используется для sandbox-браузеров и контейнеров	Неэкск.
LoadPin	Гарантирует загрузку модулей ядра только из доверенной FS	Chromebook, сервера	Неэкск.
Integrity (IMA/EVM)	Контроль целостности файлов (подписи, хэши)	Корпоративные Linux-системы	Неэкск.
Lockdown	Ограничивает root-доступ к ядру (часть upstream ядра с 5.4)	Включён в Debian, Ubuntu, Fedora	Неэкск.
Capability	Базовый модуль, модель минимально необходимых привилегий. Всегда включён.		Неэкск.
bpf	Контроль безопасности eBPF-программ		Неэкск.
ipe	Политики целостности (разрешение/запрет запуска бинарников)		Неэкск.

Список используемых LSM модулей

```
cat /sys/kernel/security/lsm
lockdown,capability,landlock,yama,apparmor,tomoyo,bpf,ipe,ima,evm
```

Естественно модули для непересекающихся задач не конфликтуют.

Revision #1
Created 25 August 2025 15:20:34 by Admin
Updated 1 September 2025 16:54:56 by Admin