Архитектура и возможности средств защиты информации на основе Linux Security Modules (LSM)

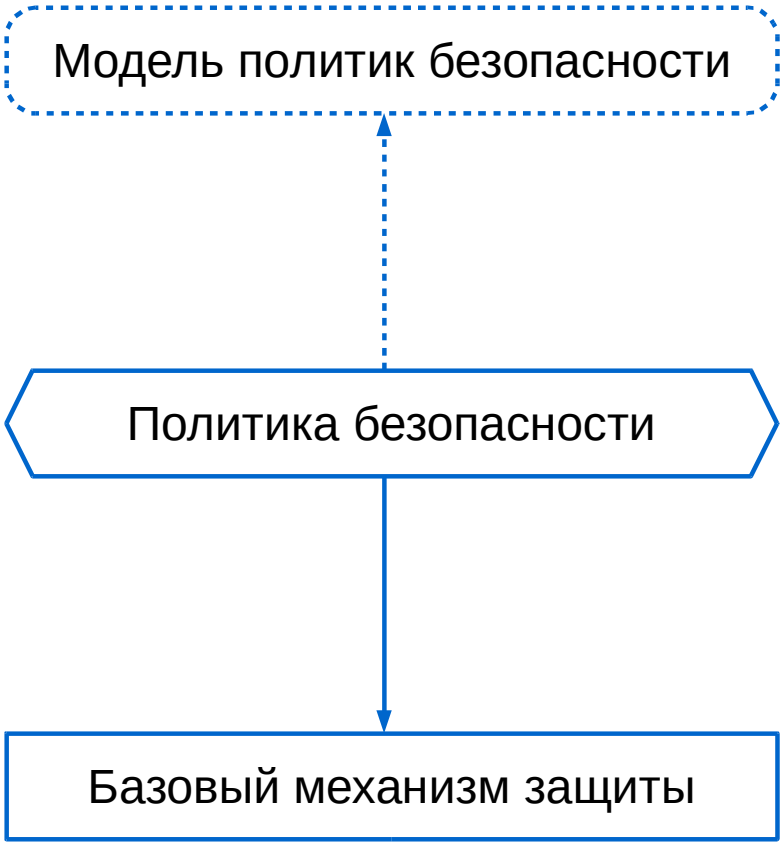
В. Кулямин (ИСП РАН)

Мандатное управление доступом

Mandatory Access Control (MAC)

- Информационные объекты размечены некоторой системой меток
- Обычные пользователи не могут изменять метки (это может только администратор безопасности)
- Метки частично упорядочены
- Разрешен перенос информации только от объектов с меньшей меткой к объектам с большей или такой же меткой
- Контроль крайне строгий

Построение системы защиты ОС



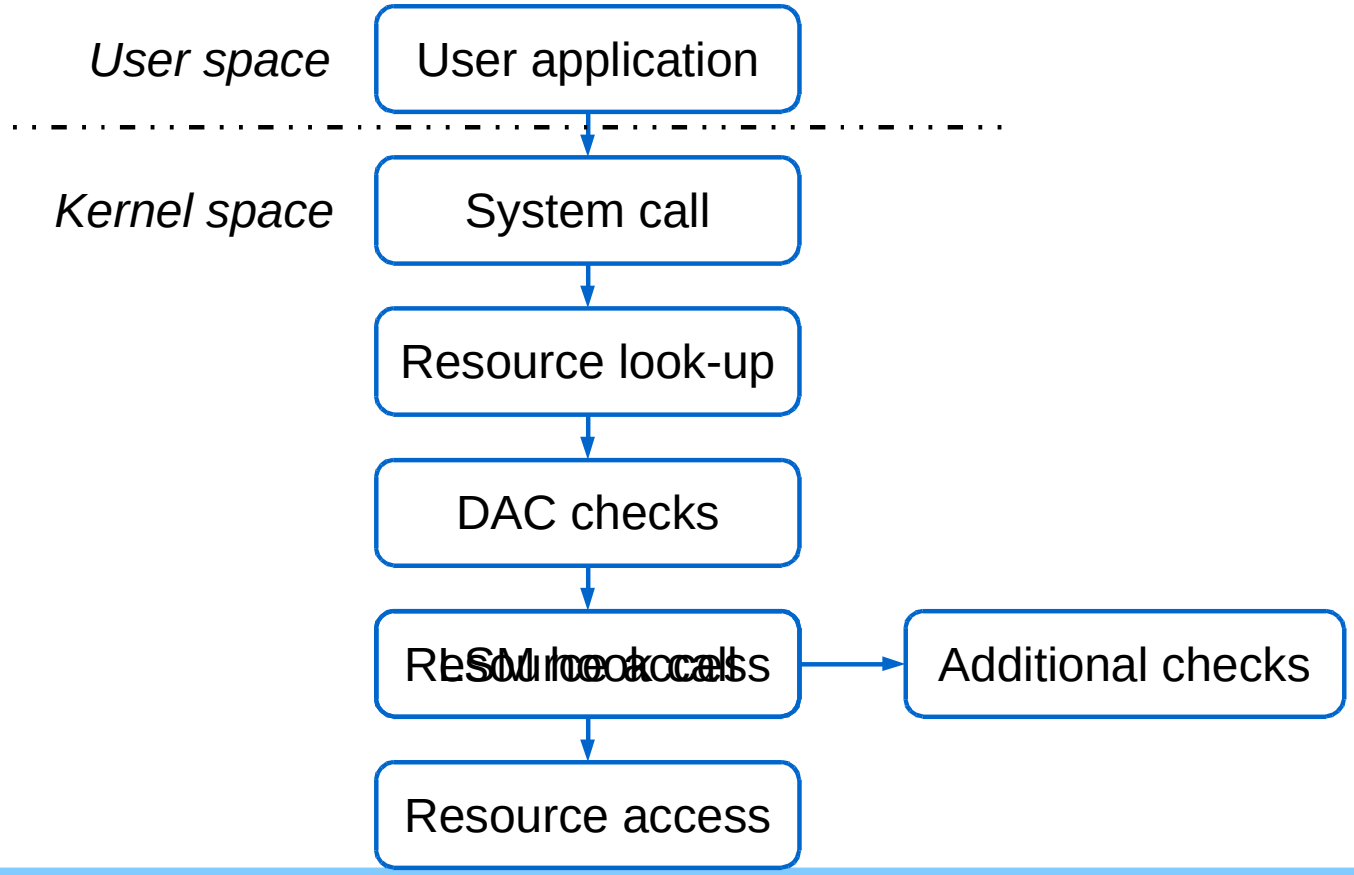
Свойства безопасности, основные функциональные возможности, общая структура меток, абстрактные операции

Набор значений меток (пользователей, ролей, уровней и пр.), разметка объектов, правила разметки процессов и новых объектов, конкретные правила контроля доступа

Конкретная структура меток, конкретные операции, общие правила контроля доступа

Linux Security Modules

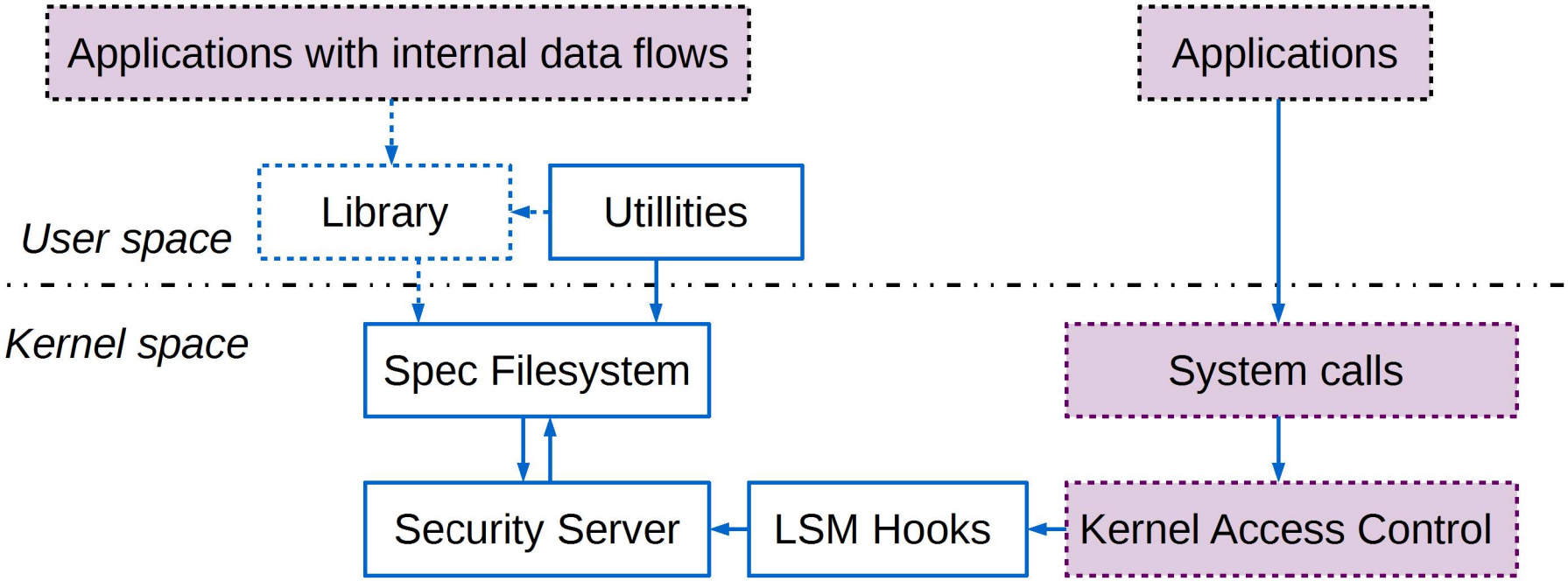
Инфраструктура реализации в рамках ядра Linux механизмов защиты, использующих дополнительные к Unix DAC ограничения



Реализации MAC на базе LSM

- SELinux
  - 12.2000 NSA
    08.2003 RedHat
- Smack
  - 02.2007 C. Schaufler 02.2008
    Samsung, Wind River
- Parsec
  - 2008 РусБИТех
- AppArmor
  - 2004 WireX 07.2009
    Canonical Inc.

Общая архитектура



Сопоставление

	LSM hooks	Access Mngmt	Kernel module size, LOC	Libraries size, LOC	Структура меток	Контрол. операции
SELinux	191	inode	25400 16700	114400 81600	user : role : type : level : cat-set	rwxan++
Smack	111	inode	9200 4100	2200 1400	level : cat-set	rwxan
Parsec	46	inode	14300 9500	-	level : cat-set : int-level	[rwxan]
AppArmor	37	path	16600 9400	3800 2000	-	rwxan
Tomoyo	28	path	12100 8100	-	-	rwxan+