Rule Set Based Access Control

Linux Kernel Security Extension

Втора конференция на “Линукс за българи”
София, 16 януари 2005 г.

Никола Антонов <nikola@linux-bg.org>

Съдържание

История на RSBAC

- Проектът RSBAC стартира като основна идея през 1996 г.
- Първата публична версия 0.9 за Linux ядро 2.0.30 излиза на 9 януари 1998 г.
- Стабилен за сериозна употреба от март 2000 г.
- Текуща стабилна версия - 1.2.3
- Актуална поддръжка на ядра 2.4 и 2.6
- В процес на разработка е версия 1.2.4, която предвижда много нови възможности

Мотивация

- Класическият модел за контрол в Linux/Unix е недостатъчно сигурен
  - Малко възможности
  - Потребителите могат много повече, отколкото е нужно
  - Зловредни програми: троянски коне, вируси...
  - Потребителят root
    - *Пълен достъп до всичко*
    - *Може много повече, отколкото е необходимо*
    - *Голям брой експлойти и средства за взлом*
- Множество подобрени модели за администрация
- Добра преносимост

Инсталация I

- Ядро
  - Разархивиране на RSBAC
  - Пачване на ядрото (с patch-x.y.z-va.b.c.gz)
  - Прилагане на поправките за бъгове (bugfixes)
  - Конфигуриране, компилиране, инсталиране

N.B. От rsbac.org можете да сваляте гототови tar архиви с изходния код на ядрото, предварително пачнат с RSBAC и PaX

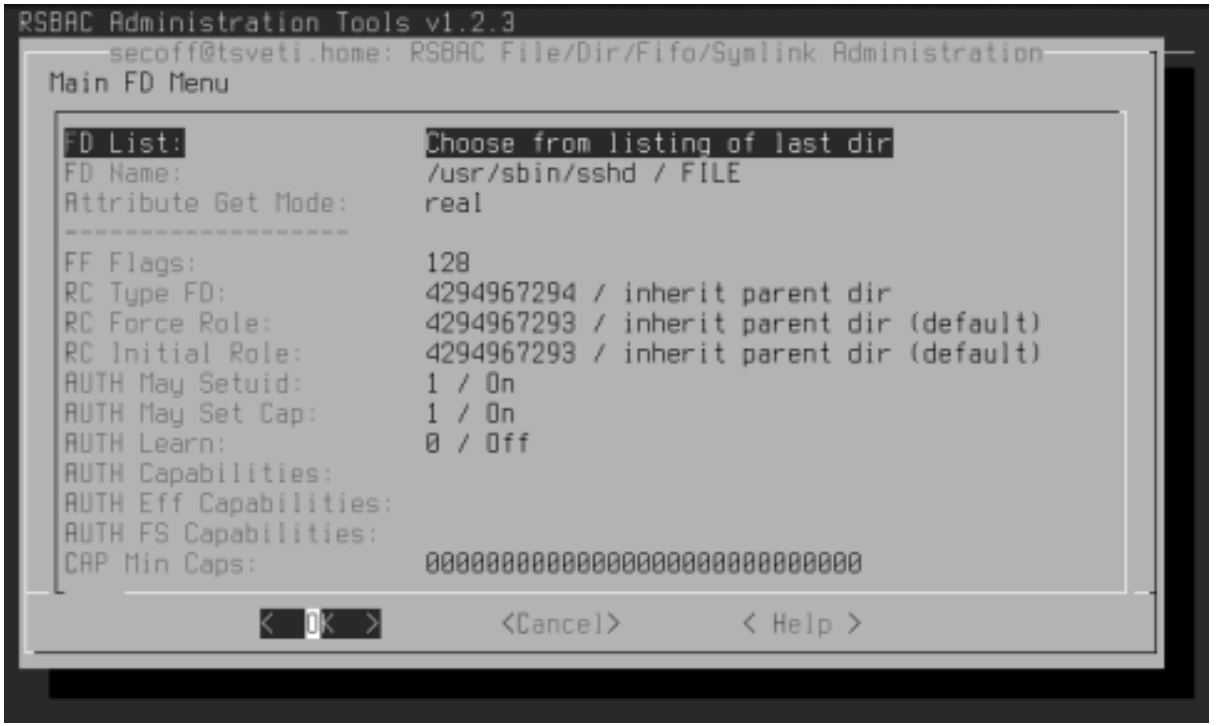
- rsbac-admin
  - Разархивиране на архива
  - ./configure && make && make install

Инсталация II

- Първо зареждане
  - Задължителен параметър за зареждане на ядрото: **rsbac_auth_enable_login**
  - Добавяне на потребител с UID 400 (Security Officer)
  - Настройване на AUTH capabilities за услугите, които не могат да се стартират (т.е. услугите, които не работят с UID 0)

Средства за управление

- Набор от конзолни програми в рамките на пакета rsbac-admin
- Контролен център с навигация чрез менюта - **rsbac_menu**



Приложение I

- Сървъри
  - Пощенски сървъри (виртуални)
    - SMTP, POP3, IMAP, пощенски списъци...
  - Файлови сървъри
    - Samba, Coda...
    - Антивирусна защита
  - Уебсървъри:
    - Apache, Zope
    - Контрол на правата за CGI
    - Защита на критични данни

Приложение II

- Сървъри
  - Защитни стени и прокси сървъри
  - DNS (named в chroot режим)
  - Сървъри за приложения
  - Shell сървъри
- Работни станции
  - Подобрен контрол над потребителите
  - Подобрен контрол над приложенията

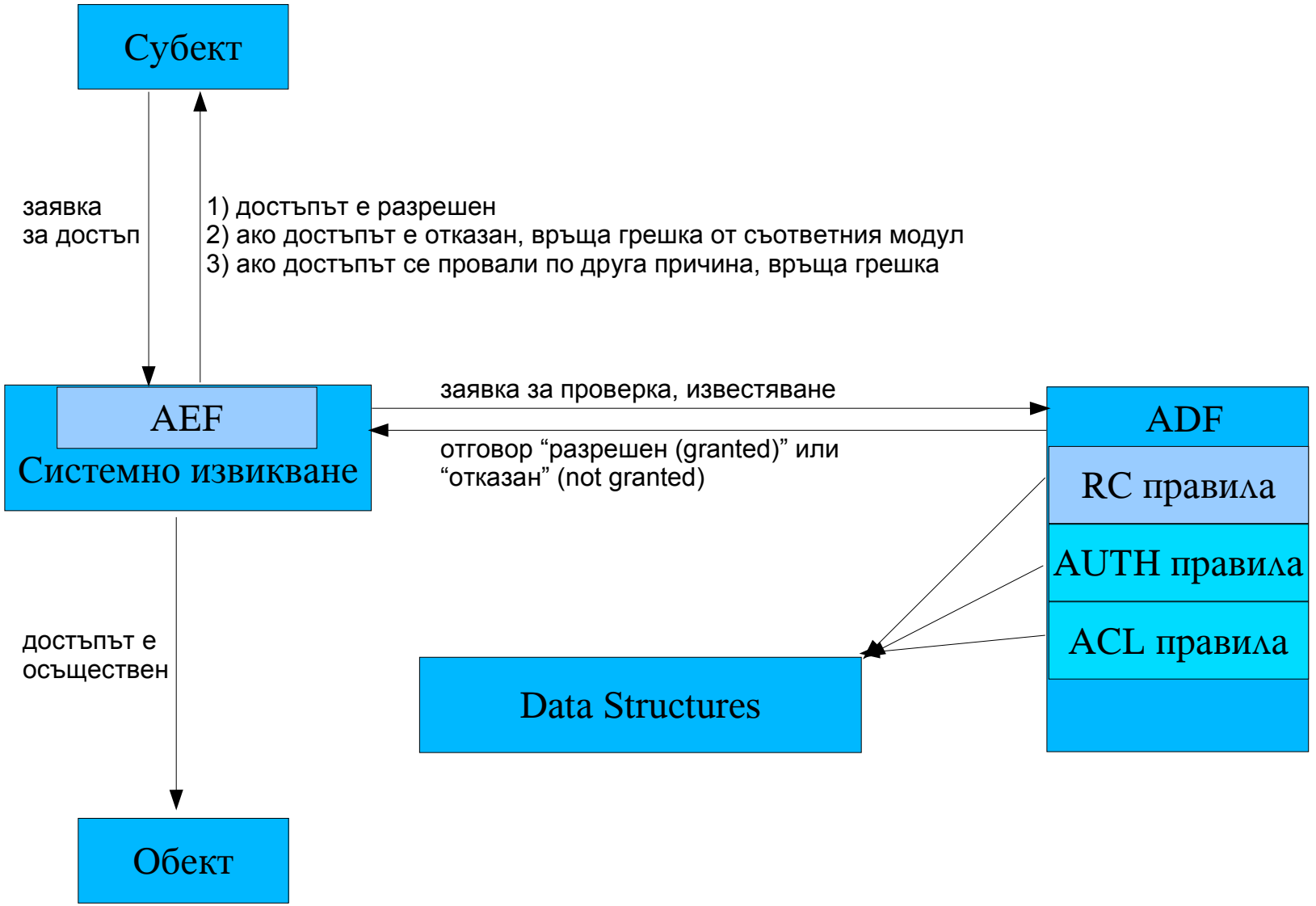
Кратък обзор I

- Module Registration (REG)
- Mandatory Access Control (MAC)
- Functional Control (FC)
- Security Information Modification (SIM)
- Privacy Model (PM)
- Malware Scan (MS)
- File Flags (FF)
- Role Compatibility (RC)

Кратък обзор II

- Authentication (AUTH)
- Access Control List (ACL)
- Linux Capabilities (CAP)
- Process Jails (JAIL)
- Linux Resources (RES)
- Pageexec Support (PaX)

Кратък обзор III



Поддръжка

- Linux kernel
  - 2.4 и 2.6 (към днешна дата включва 2.4.28 и 2.6.10)
  - Бърза интеграция във всяка нова версия
- Linux дистрибуции с RSBAC
  - Adamantix (http://www.adamantix.org, http://adamantix.logos-bg.net), включва и PaX
  - Gentoo Hardened
- Debian kernel patch (официално в testing/unstable)

Ресурси

- Материали и документация
  - http://rsbac.org/documentation
  - ftp://ftp.logos-bg.net/pub/Nikola
- Download
  - http://rsbac.org/download
  - ftp://ftp.logos-bg/rsbac

Rule Set Based Access Control

Linux Kernel Security Extension

Втора конференция на “Линукс за българи”
София, 16 януари 2005 г.

Никола Антонов <nikola@linux-bg.org>