Bezpečnostný model OS Linux

- systém typu UNIX
  (vlastník, skupina, ostatní)
- čítanie, zápis a vykonanie
- jeden správca s neobmedzenými právami
  - *root*
- POSIX capability
  (súbory, procesy, sieť, IPC, administračné)

Projekty zvýšenia bezpečnosti OS Linux

- Projekt LIDS
  (Linux Intrusion Detection System)
- Projekt VXE
  (Virtual eXecuting Environment)
- Projekt RSBAC
  (Rule Set Based Access Control)
- Projekt Medusa DS9

Projekt Medusa DS9

- Autorizačný server
- Virtuálne subsystémy

Virtuálne subsystémy

- oddelenie rôznych častí systému
- testujú sa priamo v jadre

Príslušnosť objektov k subsystémom

- určuje autorizačný server
- princíp dedičnosti

Procesy majú definované subsystémy

- ktoré vidia
- z ktorých môžu čítať
- do ktorých môžu zapisovať

Návrh implementácie RBAC

- Množina používateľov /etc/passwd
- Množina rolí, hierarchia, priradenie používateľov /etc/roles
    - názov:rid:podrole:popis:používatelia
    - názov:rid:podrole:popis:súbor

Relácia priradenia práv

- Typ a cieľ práv (/etc/permissions)
- Definície cieľov práv (/etc/targets)

Typy práv

- CREATE - Právo vytvárať objekty
- ERASE - Právo rušiť objekty
- RECEIVE - Právo prijímať informácie
- SEND - Právo posielať informácie
- ENTER - Právo nadobúdať stav
- CONTROL - Právo riadiť

Jednotný priestor mien