Bezpečnosť IT infraštruktúry

Riadenie prístupu v operačných systémoch

RNDr. Jaroslav Janáček, PhD.
Katedra informatiky

Voliteľné riadenie prístupu (DAC)

- už dlho štandardná súčasť bežných OS
- vlastník objektu určuje prístupové práva pre iné subjekty
- každý proces beží v mene nejakého používateľa
  - a teda má všetky práva tohto používateľa
  - aj prípadné práva na nastavovanie práv

Voliteľné riadenie prístupu

- UNIX/Linux
  - práva: read, write, execute / use
  - subjekty: používateľ, skupina, ostatní
    - klasicky len vlastník, 1 skupina
    - ACL – rozšírenie na ľubovoľný počet skupín a používateľov, default práva pre nové objekty pre adresár
- Windows
  - jemnejšie členenie práv, allow/deny práva
  - subjekty: používateľ, skupina

Nedostatočnosť DAC

- používateľ spustí chybnú aplikáciu a spracuje ňou zlomyseľný dokument
  - aplikácia začne vykonávať zlomyseľný kód s právami používateľa
  - má prístup ku všetkým dátam v mene používateľa
- používateľ (ne)úmyselne nastaví chybne prístupové práva
  - iní používatelia získajú prístup k dátam
  - veľký problém vo svete „utajovaných skutočností“

Zneužitie práv používateľa

- najvypuklejšie pri používateľoch s vysokými právami
  - UNIX/Linux root
  - Windows Administrators
- prirodzená ochrana
  - minimalizovať množinu procesov s takými právami
  - aj minimálna môže byť priveľká

Minimalizácia práv procesu

- Windows Vista / 7
  - UAC
    - pokus o použitie administrátorských práv vyžaduje explicitný súhlas
- Linux
  - capabilities
    - rozmenenie práv root-a na „drobné“
    - väčšina privilegovaných procesov potrebuje len časť práv
    - v minulosti veľmi sa neujalo – chýbala podpora v súborovom systéme (pred 2.6.24)

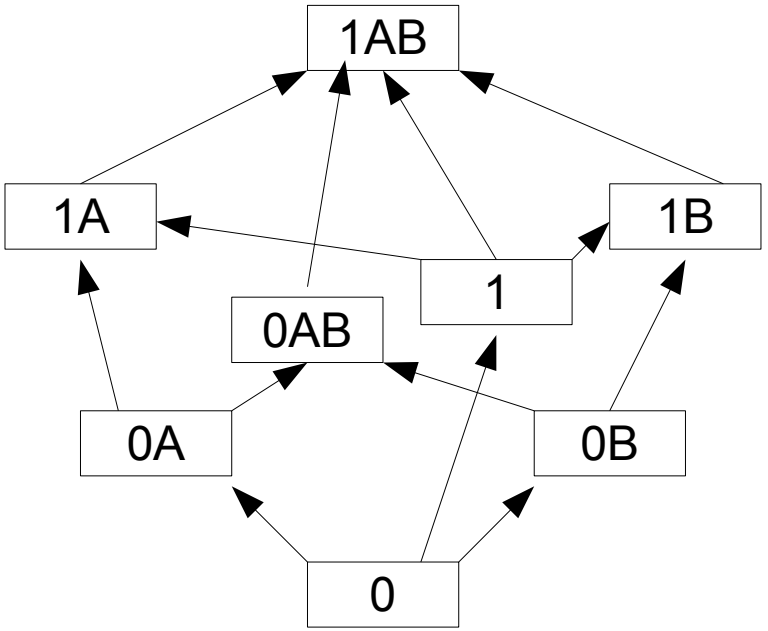
Povinné riadenie prístupu (MAC)

- základná myšlienka
  - obmedzenia prístupu určené politikou, ktorú bežné procesy a používatelia nemôžu ovplyvniť
  - zlomyseľný kód vykonávaný v rámci procesu nemôže vykonať nič, čo danému procesu politika neumožňuje
- výsledok
  - procesy majú obmedzené možnosti
    - a teda obmedzené dopady chýb

Bell – La Padula model

- zo sveta utajovaných skutočností
  - ochrana dôvernosti
  - informácie sú označené značkami (label)
    - stupeň utajenia *s* (hodnoty z usporiadanej množiny)
    - množina kategórií *C*
  - subjekty majú oprávnenie na prístup
    - max. stupeň utajenia, množina kategórií
  - značky sú čiastočne usporiadané
    - $(s_1, C_1) \geq (s_2, C_2) \Leftrightarrow s_1 \geq s_2 \ \wedge C_1 \supseteq C_2$
    - nie všetky značky sú porovnateľné

Bell – La Padula model



Bell – La Padula model

- subjekt s úrovňou S môže objekt s úrovňou O
  - čítať, ak S $\geq$ O
    - no read up
  - modifikovať, ak O $\geq$ S
    - no write down
    - v niektorých systémoch dokonca len ak O = S
- špeciálne – dôveryhodné subjekty nie sú obmedzené druhou podmienkou
  - môžu teda „znížiť“ stupeň utajenia informácie

Bell – La Padula model

- subjekt môže mať rozsah značiek
  - aktuálnu
    - používa sa pri kontrole prístupu
  - maximálnu
    - subjekt môže svoju aktuálnu úroveň zvýšiť po túto hranicu
    - ale nemôže svoju aktuálnu úroveň znížiť

Biba model

- ochrana integrity
  - namiesto stupňa utajenia stupeň „dôveryhodnosti“
  - opačné pravidlá ako Bell – La Padula
    - no read down, no write up
  - zaisťuje, že
    - subjekty s nižšou úrovňou nemôžu zmeniť dáta s vyššou úrovňou
    - subjekty s vyššou úrovňou nemôžu byť ovplyvnené dátami s nižšou úrovňou

Windows Vista/7 MIC

- Mandatory Integrity Control
  - implementuje **časť** Biba modelu
  - úrovne Low, Medium, High, System
  - iba no write up
  - voliteľne no read up (Bell – La Padula)
  - určené na ochranu proti nežiadúcej modifikácii údajov kódom z pochybných zdrojov

Domain and Type Enforcement

- subjekty majú priradenú **doménu**
- objekty majú priradený **typ**
- politika určuje
  - operácie, ktoré subjekt v doméne môže aplikovať na objekt daného typu
  - povolené prechody medzi doménami
  - typ nového objektu na základe domény subjektu a „rodičovského“ objektu

SELinux

- DTE
  - nerozslišuje formálne medzi doménou a typom
- Bell – La Padula (alebo Biba)
  - pravidlá sú konfigurovateľné
- Role Based Access Control
  - roly majú určenú množinu domén
  - používatelia majú určenú množinu rol
    - rozlišuje sa medzi UNIX používateľom SELinux používateľom

SELinux

- každý subjekt a objekt má priradený kontext
  - user:role:type[:mls_range]
- politika
  - typy, atribúty
    - atribúty slúžia na označenie množiny typov
  - pravidlá pre stanovenie nového typu objektu/subj.
  - povolené operácie
  - roly, povolené domény
  - používatelia, povolené roly
  - obmedzenia

SELinux

- kontext pre objekty súborového systému
  - uložený v extended attributes
  - vyžaduje podporu v súborovom systéme
- kontext pre niektoré iné objekty
  - určený špeciálnymi pravidlami v politike
  - odvodený od procesu, ktorý objekt vytvoril

SELinux

```
attribute domain;
attribute files_type;
type user_t, domain;
type spec_t, domain;
type spec_exec_t;
type_transition domain spec_exec_t:process spec_t;
allow domain spec_t:process transition;
allow spec_t spec_exec_t:file entrypoint;
allow domain spec_exec_t:file {read execute};
allow spec_t files_type:file *;

role user_r types {user_t spec_t};
user user_u roles user_r;
```

SELinux

- referenčná politika
  - targeted vs. strict
    - dnes spoločná – kombinovaná
    - unconfined_u:unconfined_r:unconfined_t
      - neobmedzený
  - modulárna
    - modul definuje svoje typy, atribúty, pravidlá
    - modul definuje interface, ktorý môžu použiť iné moduly
    - modul definuje značky pre súbory

SELinux

- chcon
  - zmena kontextu súboru
- runcon
  - spustenie programu v určenom kontexte
- semodule
  - zavádzanie/odstraňovanie modulov
- semanage
  - administrácia niektorých parametrov
- /etc/selinux/...

AppArmor

- profily pre obmedzené aplikácie
  - popisujú sa jednoduchou textovou formou
  - súborom určujú prístupové práva
  - môžu definovať prechody medzi profilmi pri spustení iného programu
- neukladá svoje informácie do extended attributes objektov súborového systému
- všetka konfigurácia je uložená v profiloch
  - ich binárna reprezentácia sa nahráva do jadra

AppArmor

```
/usr/bin/prog {
  /path/to/file  rw,
  /etc/**        r,
  /bin/*         ix,
  /usr/bin/prog1 px,
  network inet stream
 }
```

Demo

- capabilities
  - setcap cap_net_raw=pe ping
    - umožní procesu používať raw socket-y
- SELinux MLS
  - chcon -l s0:c0 x.txt
  - runcon -l s0 bash
    - prístup k x.txt nebudeme mať

Demo

- SELinux
  - semanage user ...
    - správa SELinux používateľov a povolených rolí
  - semanage login ...
    - správa mapovania medzi Linuxovým používateľom SELinux používateľom
  - semanage login -a -s user_u user
    - používateľ *user* bude vystupovať ako SELinux *user_u*
  - newrole -r sysadm_r
    - zmena aktuálnej roly