Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Riadenie prístupu

Jaroslav Janáček
Jún 2013

KPMG
cutting through complexity™

Riadenie prístupu

- cieľ:
  - umožniť prístup k informáciám / službám systému výlučne oprávneným používateľom
- „stavebné kamene“:
  - identifikácia
  - autentifikácia
  - autorizácia

Identifikácia

- získanie identifikátora, ktorým je používateľ v systéme jednoznačne určený
  - najčastejšie používateľské meno
  - identifikátor by mal identifikovať konkrétneho používateľa
    - aby bolo možné vyvodzovať zodpovednosť za aktivity v systéme
    - vyhnúť sa zdieľaným kontám

Autentifikácia

- preukázanie skutočnosti, že identifikácia používateľa je pravdivá
  - t.j. je naozaj tým, za ktorého sa vydáva
- základné spôsoby autentifikácie
  - niečo viem
  - niečo mám
  - niečo som

Autentifikácia

- heslá
  - najbežnejší prostriedok autentifikácie
  - kvalita hesiel
    - ľahko zapamätateľné, ťažko uhádnuteľné
  - zmena hesiel
  - rôzne heslá pre rôzne účely
  - ochrany dôvernosti pri prenose
  - ochrana dôvernosti pri úniku databázy hesiel

Autentifikácia

- jednorazové heslá
  - nie sú opakovane použiteľné
    - nevzniká problém s ich „odpočutím“ pri použití
  - klasická papierová podoba
  - elektronické generátory jednorazových hesiel
    - hardvérové „kalkulačky“
    - softvérové – napr. aplikácia do mobilného telefónu

Autentifikácia

- tokeny
  - pamäťové
    - riziko skopírovania
  - inteligentné
    - čipová kryptografická karta obsahujúca súkromný kľúč
- softvérové tokeny
  - súkromný kľúč (+ certifikát)
  - SSH, SSL/TLS s autentifikáciou klienta

Autentifikácia

- biometrické systémy
  - charakteristické vlastnosti človeka
    - odtlačok prsta
    - sken ruky
    - sken oka
    - analýza hlasu
    - ...
  - presnejšie metódy často nepohodlné
  - problém so spoľahlivosťou najmä lacnejších riešení

Autentifikácia

- SMS kódy
  - predpokladá, že kanál pre doručenie SMS je nezávislý od primárneho
  - do značnej miery závisí na (nie celkom oprávnenom) predpoklade o bezpečnosti prenosu v mobilných sieťach
  - často vhodné ako doplnková metóda autentifikácie
  - SMS kód by mal obsahovať aj informáciu o účele

Autentifikácia

- single-sign-on (SSO)
  - používateľ sa autentifikuje raz
  - systém zabezpečí jeho autentifikáciu do ďalších
  - výhody
    - jednotlivé systémy neprichádzajú do styku s primárnymi autentifikačnými údajmi (napr. s heslom)
    - znižuje sa riziko odpozorovania hesla
  - nevýhody
    - kompromitácia používateľovho počítača alebo hesla umožní prístup do všetkých systémov využívajúcich spoločný SSO

Autentifikácia

- príklady SSO
  - Kerberos, MS Active Directory
  - použitie jedného certifikátu a kľúča pre autentifikáciu do rôznych web-aplikácií
  - použitie SSH kľúčov na autentifikáciu pre vzdialený prístup k rôznym systémom

Viacfaktorová autentifikácia

- vyžadovanie úspešnej autentifikácie viacerými spôsobmi
  - napr. heslo + token, heslo + biometria, heslo + SMS
- zníženie pravdepodobnosti prekonania oproti jednofaktorovej autentifikácii
  - je ťažšie prekonať viac rôznych mechanizmov ako jeden

Autorizácia

- rozhodovanie, či daný subjekt (používateľ) má oprávnenie vykonať požadovanú operáciu s daným objektom (súbor, informácia, funkcia systému, ...)
  - rôzne modely
    - rôzna granularita prístupových práv
    - zoskupovanie používateľov do skupín
    - hierarchické vzťahy medzi objektami (napr. adresárová štruktúra)
    - možnosť nastavovania a delegovania práv

Riadenie prístupu na rôznych úrovniach

- sieť
  - firewall-y, autentifikácia na úrovni VPN
- operačný systém
  - riadenie prístupu k súborom a iným objektom
- databázový systém
  - riadenie prístupu k databázam, tabuľkám
- aplikácia
  - riadenie prístupu k aplikačným funkciám

Správa používateľov

- vytváranie a rušenie používateľských kont
  - väzba na vznik a zánik pracovného pomeru
- prideľovanie a odoberanie práv
  - potreba formálnych postupov
- centrálna vs. lokálna správa používateľov
  - centrálne adresárové služby
    - LDAP, MS Active Directory

Riadenie prístupu v OS

- voliteľné riadenie prístupu (DAC)
  - princípy, príklady (Windows, UNIX / Linux)
  - nedostatky, príklady vylepšení (UAC, capabilities)
- povinné riadenie prístupu (MAC)
  - princípy, vybrané modely (Bell – La Padula, Biba, DTE)
  - príklady implementácií (MIC, SELinux, AppArmor)

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

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

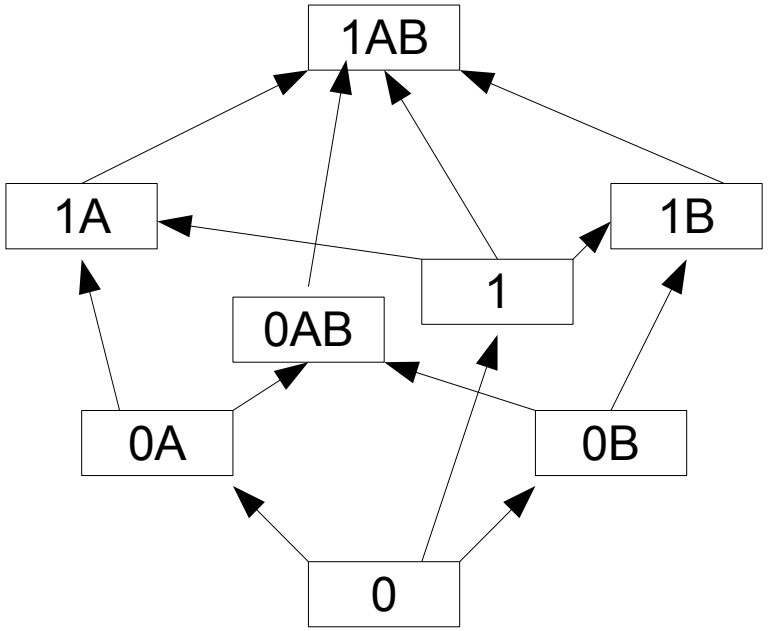
Povinné riadenie prístupu (MAC)

- 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

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

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

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

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

AppArmor

- profily pre obmedzené aplikácie
  - umožňuje striktne obmedziť, k akým súborom môže aplikácia pristupovať (a akým spôsobom)
  - definuje prechody medzi profilmi pri spustení iného programu

Otázky a diskusia

Ďakujem za pozornosť