LUENTO 22

Tietoturva – osa 2

UNIX/Linux: Ch 10.7 [Tane 01]
W2000: Ch 11.8 [Tane01],
Ch 16.6 [Stal 05]

1

Suojautuminen (protection)

eli
Miten uhkia torjutaan?

2

Suojaustasoja (1 / 2)

- Ei suojausta, mutta
  - haavoittuvat prosessit ajetaan erillään muista
- Eristäminen
  - kukin prosessi toimii itsenäisesti
  - ei yhteiskäyttöä tai kommunikointia muiden kanssa
- Kaikki tai ei mitään julkiseksi
  - omistaja antaa resurssin julkiseen jakeluun tai pitää yksityisenä
- Rajoitettu (kiinteä) yhteiskäyttö
  - käyttöoikeus tietyillä käyttäjillä tiettyihin resursseihin
  - KJ tarkistaa käyttöoikeuden resurssia käytettäessä
    - ainakin silloin, kun käyttö alkaa

3

Suojaustasoja (2/2)

- Dynaaminen käyttöoikeuksien hallinta
  - (omistaja) voi muuttaa
- Käyttöoikeuksien/tavan rajoittaminen
  - käyttöoikeuden lisäksi voidaan määritellä myös käyttötapa
    - esim. käyttäjä saa tilastollisia tunnuslukuja, mutta ei näe yksittäisiä arvoja
    - tilastolliset tunnusluvut saa vain jos
      - populaatio > 3?
      - populaatio > 10?
      - populaatio > 100?

4

Muistinsuojaus

- Moniajojärjestelmä
  - muistissa useiden käyttäjien prosesseja
  - saavat viitata vain hallitusti muistiin
    - eivät saa luvatta viitata toisten data-alueelle
    - eivät saa vaihtaa toisten funktioita toisiksi
- Toteutus: virtuaalimuisti
  - osittain laitteistolla, osittain KJ:ssa
- Yhteiskäyttö
  - sivu/segmentti esiintyy useassa sivu/segmenttitaulussa
  - toteutus helpompi segmentoinnissa
    - oma segmentti yhteiskäyttöalueelle

5

Käyttäjän tunnistus

- Käyttöoikeus vain rekisteröidyillä käyttäjillä
  - käyttäjätunnus ja salasana
- Vierailla voi olla guest / visitor tunnuksia
  - rajoitetut oikeudet
- Rekisteröinnin jälkeen tunnus mukana käyttäjän prosessien PCB:ssä
  - oikeuksien tarkistaminen
  - prosessien oikeudet perustuvat käyttäjän identiteettiin
    - yleensä tämä ei riitä!

6

Käyttöoikeudet

- Kuka saa käyttää ja mitä?
- Peruslähtökohta
  - käyttäjän tunnistus (user)
  - toimialue (suojausympäristö, domain)
    - mitä resursseja ja miten tähän suojausympäristöön kuuluva käyttäjä tai muu subjekti (subject, principal) saa käyttää
- Pääsymatriisi — Fig 16.5 (a) [Stal 05]
  - rivi: toimialue (domain)
  - sarake: resurssi, objekti (object)
  - alkio: toimialueen subjektin käyttöoikeus resurssiin
    - domain on myös objekti! — Fig 9-24 [Tane 01]

7

	File 1	File 2	File 3	File 4	Account 1	Account 2
User A	Own R W		Own R W		Inquiry Credit	
User B	R	Own R W	W	R	Inquiry Debit	Inquiry Credit
User C	R W	R		Own R W		Inquiry Debit

(a) Access matrix

[Stal 05]

Domain	File1	File2	File3	File4	File5	File6	Printer1	Plotter2	Domain1	Domain2	Domain3
1	Read	Read Write								Enter	
2			Read	Read Write Execute	Read Write		Write				
3						Read Write Execute	Write	Write			

Object

[Tane 01]

Fig. 9-24. A protection matrix with domains as objects.

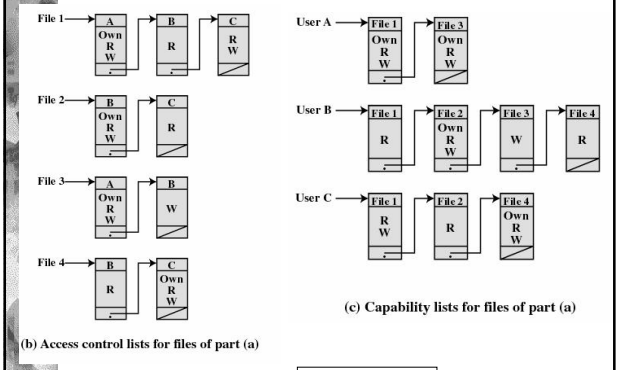
8

Käyttöoikeudet

Fig 16.5 (c) [Stal 05]

- Käyttöoikeudet käyttäjän yhteydessä (mitä käytetään?)
  - käyttäjäprofiili
  - valtakirjalistat (capability lists), väärentämättömät
- Käyttöoikeudet kohteen yhteydessä (kuka käyttää?)
  - kohde: data, ohjelma
  - pääsylistat (ACL, access control list) — Fig 16.5 (b) [Stal 05]
  - yleisempi, helpompi toteuttaa
    - tieto vain yhdessä kohdassa
- Molemmat
  - vain pääsymatriisin ei-tyhjät alkiot
- KJ tarkistaa oikeudet käytön yhteydessä
  - esim. vertaa PCB:ssä olevaa uid+gid paria tiedoston attribuutteihin talletettuun uid+gid pariin

9



(b) Access control lists for files of part (a)

(c) Capability lists for files of part (a)

[Stal 05] Fig 16.5

10

Käyttöoikeuspolitiikat

- DAC – discretionary access control — harkinnan-varainen
  - tiedon omistaja päättää, kuka siihen pääsee käsiksi ja miten
  - käyttäjä voi dynaamisesti muuttaa omistamiensa tietojen (tiedostojen) pääsyoikeuksia — poista lukuoikeus?
    - vaikutus alkaa ... milloin?
  - normaali yksityiskäyttö — pakollinen
- MAC – mandatory access control
  - keskitetty politiikka, joka oletusarvoisesti määrittelee kuka pääsee käsiksi mihin tietoon ja miten
  - käyttäjä ei voi muuttaa pääsyoikeuksia
  - luokitellun tiedon käyttöympäristöt

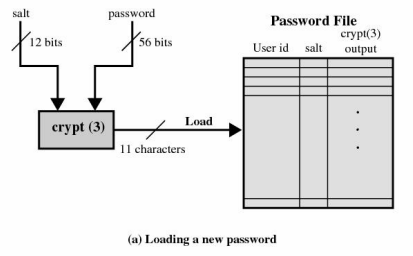
11

Hyvä salasana

- Koneen generoima
  - vaikeampi arvata
  - vaikeampi muistaa → paperille?
- Käyttäjän valitsema
- hylkää liian lyhyet ja helpohkosti arvattavat — Fig 16.6 [Stal 05]
  - järjestelmä voi laajentaa, salaisella 'suolalla'
    - sama salasana ei näytä aina samanlaiselta kryptattuna
    - salasana käytännössä pitenee
    - brute-force hyökkäys hidastuu (suola salainen tai ainakin kaikilla erilainen)
- Järjestelmä yrittää itse aktiivisesti arvata salasanan
  - vaihdettava, jos osoittautui liian helpoksi
  - hakkeri voi tehdä tätä kopioimallaan passwd-tiedostolla
    - login-yritysten rajoittaminen ei hidasteena
    - "suolaus" on hyvä hidaste
    - passwd-tiedosto suojatulle muistialueelle olisi hyvä idea

12

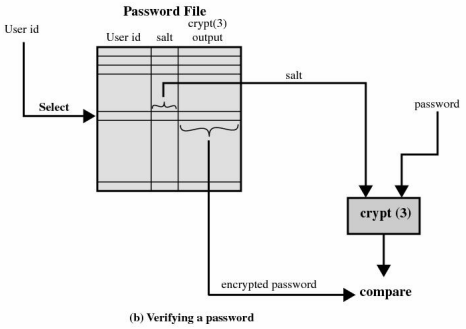
UNIXin salasanamalli



(a) Loading a new password

13

UNIXin salasanamalli



(b) Verifying a password

14

Tunkeilijan huomaaminen

- Tunkeilijaa vaikeaa estää vaikeuttamatta samalla normaalia käyttöä
- Tunnuksen käyttöprofiili muuttuu yllättäen
  - aamu-uninen Arskako töissä kello 5?
  - eikö Villen pitäisi olla lomalla?
- Tilastollinen poikkeama
  - kerää perustietoa laillisten käyttäjien tyypillisestä kuormasta tietyn jakson ajan
  - vertaa uutta jaksoa perusjaksoon
  - mikä on normaalia? mikä poikkeavaa?
- Mitä on automatisoitavissa?

15

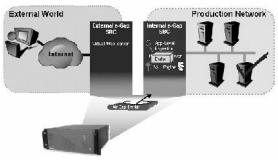
Tunkeilijan huomaaminen

- Sääntöpohjainen eksperttijärjestelmä
  - perussäännöstö normaalille käytölle
    - eri yrityksissä/kulttuureissa erilaista
  - mikä on normaalia? mikä poikkeavaa?
- KJ tarjoaa perusvälineet
  - kirjaa tietoa käyttäjän login-ajoista, CPU-ajasta jne.
  - loki- ja historiatiedostot
- Omat räätälöinnit parempia
  - tunkeilija tuntee perus-KJ:n
- Erillinen audit-järjestelmä
  - kerää tunkeilijan huomaamisessa tarvittavaa tietoa
- Ansat
  - *user* guest, *password* guest ⟶ login OK, soita poliisille
- Kuka on tunkeilija? Kuka tuntee nykyisen lain?

16

Palomuuri (Firewall)

- Suodatus (Packet-filtering)
  - Säännöstö
  - Päätös pakettikohtaisesti otsikkotietojen perusteella
- Sovellustason yhdyskäytävä (Application-level gateway)
  - Tutki pakettien dataa
- Ilmarako (Air-gap technol.)
  - Palomuuriin tyhjä tila
  - Esim. Kaksi palvelinta ja muistipankki niiden väliin
  - E.g., e-Gap Systems (Whale Communications)



http://www.whalecommunications.com

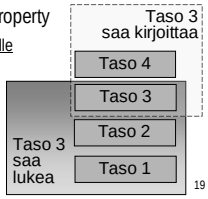
17

Luotettu järjestelmä (trusted system)

18

Multilevel Security

- Tieto luokitellaan tärkeyden mukaan
  - unclassified, confidential, secret, top secret
- Käyttäjälle määritelty 'luottamustaso'
- No-read-up eli simple security property
  - kukin saa nähdä vain omalle tai sen alapuoliselle tasolle luokiteltua tietoa
- No-write-down eli *-property eli star-property
  - tietoa saa tuottaa vain omalle tai ylemmälle tasolle
  - tietoa saa 'vuotaa' alemmille tasoille vain, jos siihen on saatu erikseen lupa
- Esimerkki MAC-suojauksesta
  - Mandatory Access Control



19

Reference Monitor

Fig 16.10 [Stal 05]

- Säätelee/laillistaa käyttäjien (subject) pääsyä kohteisiin (object) kumpiinkin liitettyjen attribuuttien mukaisesti
- Security kernel database
  - käyttäjien pääsyoikeudet, liikkumavara
  - kohteiden käyttöoikeudet, luokittelutasot
- Pakottaa noudattamaan säännöstöä
  - MAC: no-read-up, no-write-down
- Toteutus laitteistossa ja KJ:ssa
  - pelkkä ohjelmallinen toteutus liian hidasta
  - "viittausvalvoja", tarkkain (reference monitor)
    - jatkuvaan seurantaan tarkoitettu laite

20

Reference Monitor

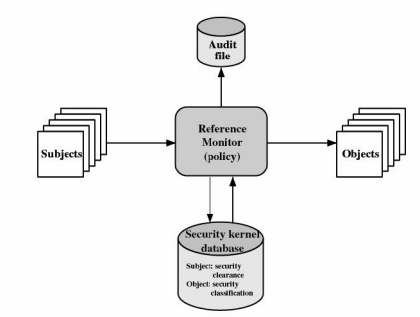


Figure 16.10 Reference Monitor Concept

21

Reference Monitor -politiikka

- Ominaisuudet
  - täydellinen sääntöjen noudattaminen (mediation)
    - säännöt tarkistetaan jokaisella viitteellä, ei pelkästään esim. tiedostoa avattaessa
  - eristäminen (isolation)
    - sekä monitori että tietokanta suojattu täysin luvattomilta muuttajilta
  - todennettavuus (verifiability)
    - monitorin oikeellisuus pitää pystyä osoittamaan matemaattisesti
- Jos verifioitavissa, sallitaan käyttää termiä luotettu järjestelmä (trusted system)
  - aika paljon vaadittu …

22

Reference Monitor

- Audit-file
  - tärkeät tietoturvaan liittyvät tapahtumat rekisteröidään
    - muutokset tietokantaan eli oikeuksiin
    - login ja logout -tapahtumat
    - tietoturvan rikkomisyritykset
- Tutkittavissa jälkikäteen
  - jos rikosta ei voi estää, niin toivottavasti …
    - se voidaan edes myöhemmin havaita ja
    - pahatekijä saadaan kiinni
      - kiinnijäämisen pelko on viisauden alku

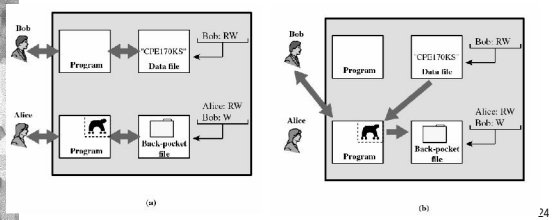
Audit: tarkastus, arviointi, tilintarkastus

23

Esimerkki

Fig 16.11 (a, b) [Stal 05]

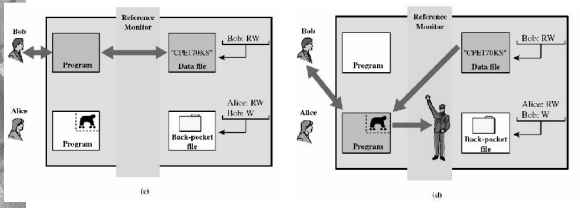
- Troijan hevonen ja normaalit käyttöoikeudet
  - Alice vokottelee Bobin ajamaan ohjelmansa
    - lukee Bobin yksityistä tietoa
    - luo tiedoston, jonka Alice voi lukea, mutta Bob ei



24

Esimerkki

Fig 16.11 (c, d) [Stal 05]



- Troijan hevonen ja luotettu järjestelmä
  - Tasot: arkaluonteinen (harmaa), julkinen (valkea)
  - Bob tasolla, jolla oikeus arkaluonteiseen tietoon
  - Alice tasolla julkinen
  - Kun Bob suorittaa Alicen ohjelman, se ei voi kirjoittaa Bobin tasoa alemmalle tasolle (*-property)

Æ suojaustaso tässä tärkeämpi kuin käyttöoikeudet !

25

OpenBSD (www.openbsd.org)

- Tavoitteena turvallinen käyttöjärjestelmä
  - ”Try to be the #1 most secure operating system”
  - “Only one remote hole in the default install, in more than 10 years!”
- Oletusasetukset (Default setup)
  - Turvatasot ylhäällä
  - Oletusarvoisesti lähes kaikki estetty
  - Integroitu salaus, ennakoiva salasanatarkistus
  - Kaikkien lähdetiedostojen koodin analysoitu
  - Open source – voit itsekin tarkistaa koodin

26

ROOTKIT

- Wikipedia: ”Rootkit on *ohjelmisto*, joka asennetaan tietokoneelle *hyökkääjän saatua sen hallintaansa*. Rootkitin eri osat pyrkivät *piilottamaan itsensä* tuhoamalla jäljet tartunnasta ja piilottamalla tietokoneella olevat vieraat prosessit tai verkkoyhteydet. Rootkittiin kuuluu usein etähallintamahdollisuus (takaovi) ”
- Erilaisia piiloutumiskeinoja:
  - Virtualisointi – piiloudutaan KJ:n ja laitteiston väliin
  - Ytimeen, esim. uusi ajuri tai ladattava moduuli
  - Kirjastorutiiniin – muokkaa systeemikutsuja
  - Käyttäjän sovellukseen

27

Virtualisointi

28

Virtualisointi (virtualising, virtualization)

- Jatketaan abstraktiotasojen lisäämistä ja ohjelmistojen ja laitteistojen eristämistä
- Erilaisia tavoitteita
  - Turvallinen suoritusympäristö: ohjelmistotestaus, epäluotettavat sovellukset
  - Kustannusten säästö: yhdelle koneelle enemmän töitä
  - Kuorman tasaus: helpompi siirto kesken suorituksen
  - Sovelluksilla erilaisia KJ-tarpeita, mukautuminen niihin
- Valitettavasti voidaan käyttää myös haittaohjelmien apuna, erityisesti rootkit
- Vanha idea: jo 60-70-luvuilla
- Käytetty isoissa palvelimissa jo pitkään

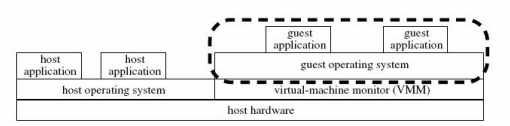
29

Virtualisointi

- Väliohjelmistot tarjoaa yhtenäisen rajapinnan sovellusohjelmille erilaisten KJ:en ja laitteistojen suuntaan
- Virtualisointi tarjoaa
  - Yhtenäisen rajapinnan KJ:lle laitteiston suuntaan (vrt. HAL- hardware abstraction layer)
  - Suojauksen samassa koneessa suoritettavien käyttöjärjestelmien välille
    - Pahantahtoinenkin sovellus on eristetty virtuaalikoneeseen

30

Arkkitehtuuri



Hypervisor, virtual machine monitor (VMM)
- KJ:n ja laitteiston väliin
- Suorittaa eri KJ:t omissa virtuaalikoneissaan
- Vuorottaa virtuaalikoneiden välillä
- Varaa resurssit laitteistolta kohdeKJ:en pyyntöjen mukaan

Kuva artikkelista: Samuel T. King, Peter M. Chen, Yi-Min Wang, Chad Verbowski, Helen J. Wang, Jacob R. Lorch, "SubVirt: Implementing malware with virtual machines", Proceedings of the 2006 IEEE Symposium on Security and Privacy , May 2006

31

Lähestymistapoja

- Emulointi
  - Tulkataan kaikki virtuaalikoneessa suoritettavan käyttöjärjestelmän konekieliset käskyt
- Porting
  - Muokataan kohdeKJ:n koodia, jotta voidaan suorittaa tässä ympäristössä
- Binääriyhteensopiva
  - KJ voidaan suorittaa ilman muokkausta ko. virtuaalikoneessa

32

Lähestymistapoja

Teknologia-esimerkkejä:	Käyttöjärjestelmiä	Laitteisto-arkkitehtuureja
VMware Xen	Useita (Linux, Windows)	1 (Vain x86)
Linux-Vserver User Mode Linux	1 (vain Linux, mutta eri versiot OK)	Useita (x86, IA64)

Lähde: B. des Ligneris, "Virtualization of Linux based computers: the Linux-VServer project", Proceedings of 19th High Performance Computing Systems and Applications, IEEE, 2005

33

Samankaltainen lähestymistapa: RTLinux

- Kaksi ydintä:
  - Varsinainen linux-ydin on vain yksi tosiaikaprosessi tosiaikaisen mikroytimen päällä
  - Perus-Linuxin toiminnasta on vaihdettu vain keskeytyskäsittelijä
  - Tosiaikaydin vuorottaa kaikki tosiaikaiset prosessit. Perus-Linuxia ajetaan taustaprosessina ja se saa kaiken vapaaksi jäävän ajan
- Ei kutsuta virtualisoinniksi
  - Vaikka sama perusratkaisu
  - Mutta eri tavoite
  - Vain yksi kohdeKJ (ei useita rinnakkain)

34

Virtualisoinnin ongelmia

- Eristämisen ja kontrolloinnin vuoksi
  - Etuoikeutettu tila? VMM vai KJ?
  - Keskeytykset? VMM, miten tieto KJ:lle?
  - Muistinsuojaus ja osoiteavaruus? VMM:n kirjanpidon sijainti?
- Ihan samat ongelmat kuin KJ:llä on prosessien suorittamisessa
- VMM:lle KJ on vain yksi prosessi!

35

UNIX tietoturva

Ch 10.7 [Tane 01]

36

Unix tietoturva

- Käyttäjän tunnistus, tiedot PCB:ssä
  - UID (User ID)
    - kokonaisluku 0-65535
  - GID (Group ID)
- Tiedostossa vastaavasti
  - omistaja, joka voi muuttaa oikeuksia
  - oikeudet omistajalle, ryhmälle ja muille
- Tiedoston käyttö: tarkista onko omistajalla/ryhmällä tarvittavat oikeudet tiedostoon
  - tarkistus vain tiedoston avaamisen yhteydessä
- Kaikki KJ oliot ovat "tiedostoja"

37

UNIX käyttöoikeudet

- Tiedoston attribuutit (i-node)
  - omistaja (uid), ryhmä (gid)
  - käyttöoikeudet (mode-kentän rwx-bitit)
- Käyttäjän uid ja gid käyttäjätietokannasta
  - **`/etc/passwd`** uid ja ensisijainen gid
  - **`/etc/group`** käyttäjän muut ryhmänumerot
- uid ja gid periytyvät lapsiprosesseille ja edelleen luoduille tiedostoille
  - voi vaihtaa ohjelmallisesti

38

UNIX käyttöoikeudet

- rootilla (uid=0) kaikki oikeudet kaikkeen
- Käyttäjien jaottelu
  - u omistaja
  - g samaan ryhmään kuuluvat
  - o muut käyttäjät
- Oikeuksien jaottelu u, g, o
  - - ei mitään
  - r lukuoikeus
  - w kirjoitusoikeus (oikeus muuttaa)
  - x suoritusoikeus
- Uusien tiedostojen käyttöoikeudet prosessin kuvaajassa (PCB) olevan umask-oletuksen mukaan
  - periytyy rajoitetusti
  - käyttäjän oikeudet, umask, luonnin optiot

39

UNIX käyttöoikeudet

- Hakemiston käyttöoikeudet
  - r oikeus listata hakemiston sisältö
  - w oikeus poistaa tiedosto hakemistosta
  - x oikeus käyttää hakemistonimeä polkunimessä

normal

- rw- --- --- 1 root

- Oikeudet oltava kaikkiin polkunimen osiin
- Käyttöoikeuden hetkellinen laajennus, esimerkki:
  - vain rootilla w-oikeus */etc/passwd* tiedostoon
  - *passwd*-ohjelmalle asetettu SETUID bitti
    - effective userid on tämän ohjelman (tiedoston passwd) ownerid
  - käyttäjä saa *passwd*-ohjelman suoritusajaksi root-oikeudet (koska root on owner), ja voi muuttaa oman salasanansa
  - SETGID bitti vastaavasti (SETGID bitti)
    - effective groupid

- srw- s--- t--- 1 root

advanced special permissions

"sticky bit" keep file on swap device

40

System call	Description
s = chmod(path, mode)	Change a file's protection mode
s = access(path, mode)	Check access using the real UID and GID
uid = getuid( )	Get the real UID
uid = geteuid( )	Get the effective UID
gid = getgid( )	Get the real GID
gid = getegid( )	Get the effective GID
s = chown(path, owner, group)	Change owner and group
s = setuid(uid)	Set the UID
s = setgid(gid)	Set the GID

Fig. 10-39. Some system calls relating to security. The return code *s* is −1 if an error has occurred; *uid* and *gid* are the UID and GID, respectively. The parameters should be self explanatory.

[Tane 01]

41

UNIX: Käyttöoikeudet

- Eräissä järjestelmissä myös käyttäjäkohtaisia pääsylistoja (ACL)
  - Solaris, HP-UX
    - esim. tietotekniikkaosaston kone "sirppi"
    - man acl
  - Linux
    - ext2:ssa varauduttu toteuttamaan
      - 8 tavua *i-node*:ssa
      - File ACL ja Directory ACL -kentät

setfacl -m u:jussi:r tiedostoX

42

Linux PAM

http://www.kernel.org/pub/linux/libs/pam

- PAM – Pluggable Authentication Module
- Parannettu tunnistus, hylkää huonot salasanat, vaadi salasanan vaihtoa aika ajoin
- Kerberos optio
  - keskitetty organisaation turvajärjestelmä
  - käyttäjän tunnistaminen
  - TGS – Ticket Granting Service
    - valtakirjat verkkopalveluihin
    - väärentämättömiä, vain vähän aikaa voimassa olevia valtakirjoja
- Älykortti- ja äänitunnistus optiot

43

Linux ext2fs tiedonsuojaus

- Kuten standardi UNIX
  - user, group, other
  - r, w, e, x
  - setuid, setgid
- Tiedostolle myös
  - a - append only
  - i - immutable
    - ei voi muuttaa, tuhota tai vaihtaa nimeä
    - ei voi linkittää (hard link, symbolic link)

44

LSM - Linux Security Module

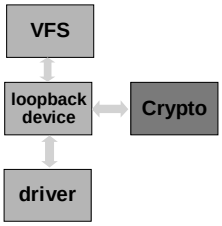
- Määrittely ylimääräiselle valvontamoduulille
  - ladattava ytimen moduuli
  - aktivoituu vasta, kun std pääsynvalvonta on ensin hyväksynyt käyttäjän tai resurssin käytön (LSM on lisäsuoja)
- LSM SELinux (Security Enhanced Linux)
  - NSA – National Security Agency (USA)
  - MAC – Mandatory Access Control

    http://www.nsa.gov/selinux/
    - joka tiedostolle selkeät oikeudet (write up, read down)
    - sääntöjoukko, jota käyttäjät eivät voi manipuloida
  - jäykkä, tehokas, luotettava
- LSM Capabilities
  - valtakirjaperustainen pääsynvalvonta
    - i-node:n kentät File ACL ja Directory ACL
  - tarkemmat oikeudet sovellukselle käyttäjästä riippumattomasti
  - POSIX.1e suojausstandardi

45

Linux salausmoduuli

- Cryptographic API - määrittely
- VFS (virtual file system) ei kutsu laiteajuria suoraan, vaan välissä on loopback device
- Loopback device käyttää tarvittaessa kryptomoduulia aina tiedostoa käytettäessä
- per hakemisto?
- per tiedostojärjestelmä?



46

Windows 2000 Tietoturva

47

W2K Tietoturva

http://www.dynamoo.com/orange/summary.htm

- Noudattaa "Orange Book" C2 luokitusta
  - Dept of Defence (US) Security requirements C2
  - Trusted Computer System Evaluation Criteria
- C2 – ei kovin paljoa vaadittu
  - henkilökohtainen kirjautuminen (ei ryhmä)
  - pääsy vain sallittuihin tiedostoihin ja ohjelmiin
- Muita, parempia turvatasoja
  - B1, B2, B3
    - B1: kuten C2 ja Mandatory Access Control (MAC)
    - B3: kuten B2 ja kaiken monitorointi ja suojausdomainit
  - A1, A2
    - A1: kuten B, mutta formaalisti todistettu oikein toimivaksi
    - A2: määritellään joskus myöhemmin

48

W2K Suojausympäristö

- Joka prosessilla suojauslipuke (access token)
  - prosessin tunnistetiedot, "kuka minä olen" Fig 16.12 (a) [Stal 05]
    - annetaan järjestelmään kirjautumisen yhteydessä
    - omistaja, ryhmä (POSIX)
  - luotaville objekteille määrätyt oletusoikeudet (default ACL)
  - mahdolliset erityisoikeudet ('special power', priviledges)
    - shutdown, write file Y
  - periytyy lapsiprosesseille
  - voidaan muuttaa prosessikohtaisesti
- Joka oliolla suojauskuvaaja (security descriptor)
  - suojauskuvaajassa pääsylista
    - discretionary ACL Fig 16.12 (b,c) [Stal 05]
- Tarkistus: vertaa prosessin (käyttäjän) pääsylippua olion (kohteen) pääsylistaan

49

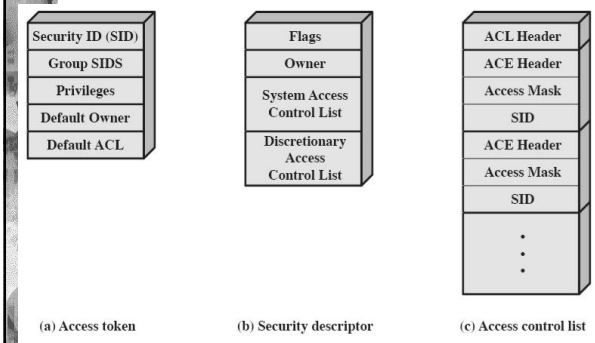


Figure 16.12 Windows Security Structures

50

W2K suojauskuvaaja (security descriptor)

- Joka oliolla oma suojauskuvaaja Fig 16.12 (b) [Stal 05]
  - "kuka saa tehdä mitä?"
  - lipukkeita (esim. mitkä kentät käytössä)
  - kohteen omistaja (owner SID) tai ryhmä (group SID)
    - joku olion luojan suojauslipukkeen SID'eistä
  - DACL pääsylista (discretionary access control list)
    - ketkä käyttäjät, mitkä ryhmät saavat käyttää
    - omistaja voi manipuloida
  - SACL pääsylista (system ACL)
    - mitä auditiointilokiin, erityisoikeuksien käyttö
    - omistaja ei saa manipuloida (yleensä)

discretionary = vapaa harkinta, päätösvalta, harkinnan varainen

51

W2K suojattujen olioiden käyttö

- Ensimmäinen viite (esim. tiedoston avaus)
  - vertaa prosessin pääsylippua olion pääsylistaan (DACL)
  - etsi ensimmäinen ACE (access control element), joka sopii tähän käyttäjään tälle käyttötavalle
  - jos kaikki kunnossa, anna kahva (handle, valtakirja) olioon
- Myöhemmät viitteet kahvan avulla
  - tarkista aina, että käyttötapa on sellainen, joka oli mukana jo ensimmäisellä kerralla kun pääsy olioon sallittiin
  - jos prosessi yrittää saamansa "read"-oikeuden asemesta kirjoittaa, niin se ei onnistu
  - jos olion omistaja poistaa "read" oikeuden, niin se ei estä vanhoja käyttäjiä lukemasta

52

W2K DACL – Discretionary ACL

- Koostuu useasta pääsyelementeistä Fig 16.12 (c) [Stal 05]
  - ACE (Access Control Element)
- Kaksi ACE-tyyppiä Fig 11-43 [Tane01]
  - Allow – kuka saa käyttää ja miten
  - Deny – kuka ei saa käyttää ja miten
- Käyttö: käy listaa läpi kunnes tälle käyttäjälle (SID) ja käyttötavalle löytyy ensimmäinen ACE ja menettele sen mukaan
  - sijoita Deny ACE -elementit ennen Allow ACE –elementtejä!
    - esim. kaikki saa, mutta Elvis ei
- Käyttötavat koodattu pääsyoikeusmaskiin (access mask)

53

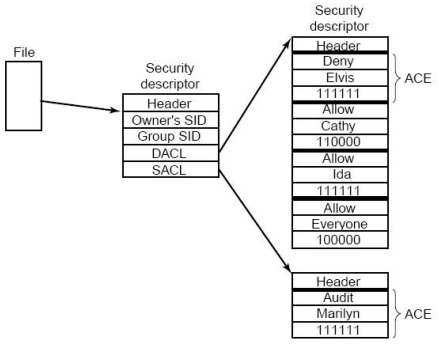
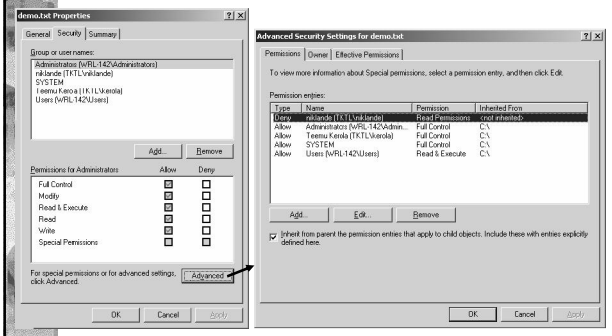


Fig. 11-43. An example security descriptor for a file. [Tane 01]

54

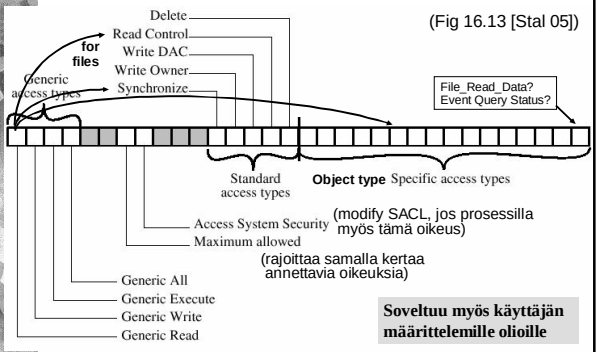
W2K DACL Esimerkki (NTFS)



55

W2K pääsyoikeusmaski (access mask)

(Fig 16.13 [Stal 05])



Soveltuu myös käyttäjän määrittelemille olioille

56

W2K SACL – Security ACL

- Mistä tapahtumista tähän olioon kerätään auditointilokia
  - käyttäjä ei tiedä
  - olion omistaja ei tiedä, ei voi muuttaa
- Esimerkkejä
  - Marilyn'in kaikki operaatiot tähän olioon pistetään lokiin
  - Kaikkien käyttäjien kaikki operaatiot tähän suojattuun olioon pistetään lokiin

Fig 11-43 [Tane 01]

- Auditointiloki on olio, jolla oma suojauskuvaaja ja DACL pääsylista

57

W2K Security API

Win32 API function	Description
InitializeSecurityDescriptor	Prepare a new security descriptor for use
LookupAccountSid	Look up the SID for a given user name
SetSecurityDescriptorOwner	Enter the owner SID in the security descriptor
SetSecurityDescriptorGroup	Enter a group SID in the security descriptor
InitializeAcl	Initialize a DACL or SACL
AddAccessAllowedAce	Add a new ACE to a DACL or SACL allowing access
AddAccessDeniedAce	Add a new ACE to a DACL or SACL denying access
DeleteAce	Remove an ACE from a DACL or SACL
SetSecurityDescriptorDacl	Attach a DACL to a security descriptor

Fig. 11-44. The principal Win32 API functions for security.[Tane 01]

ACL tarkemmin: Microsoft TechNet artikkeli

58