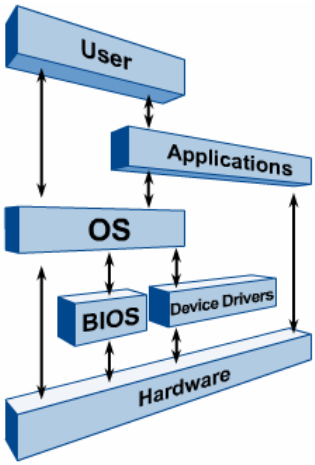
Datasäkerhet och integritet

OH-4 v1

- Operativsystem
- Systemsäkerhet
- Filskydd
- Virus och datorskydd
- Fysisk säkerhet
- Backup

Operativsystemet (OS)

- Operativsystemet är mjukvaran som kontrollerar och tillhandahåller funktionalitet mot hårdvara och applikationsprogram etc.
- Utan OS är datorn inte mer än en hög med elektronikskrot!
- Det finns i huvudsak två typer av OS
  - Klientoperativsystem
    - Hanterar en klient (dator, mobiltelefon, fordonsdatorn etc.
  - Nätverksoperativsystem
    - En server som hanterar många klienter
- De är ofta också samma operativ men med lite andra inställningar på server



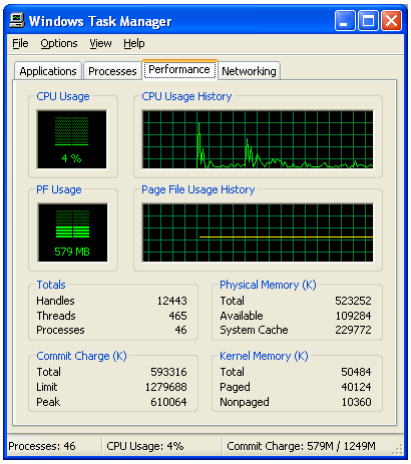
Olika kategorier av OS

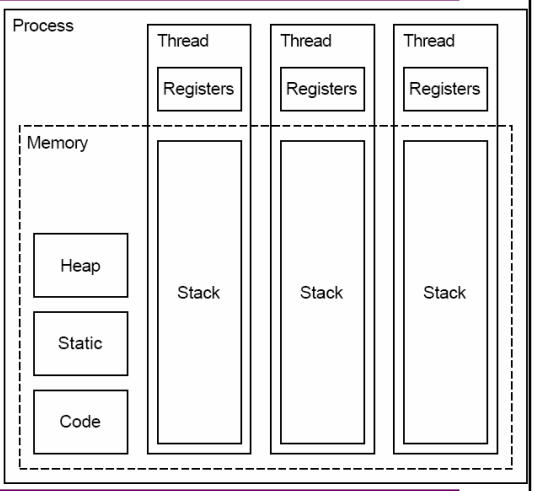
- Realtids-OS
  - Hanterar krav på korrekt resultat en viss tidpunkt
  - Styr och kontrollsystem inom industri och transport etc.
- Inbäddade (embedded) OS
  - Telefoner, sattelitmottagaren etc.
  - Linux, Symbian, Windows XP embedded
- Enanvändar OS, GPOS (General Purpouse OS)
  - Single task, Palm OS, Windows 3.1, Mac OS, DOS
  - Multi task, Windows >= 95, Pocket PC, **alla OS nedan**
- Fleranvändar OS (serveroperativsystem)
  - Exempel HP AIX, Novell Netware, SUN Solaris, Microsoft Windows Server, Linux och FSF, Mac OS X

Processer och trådar, CPU

- Operativsystemet hanterar hela tiden ett antal processer och trådar, dvs. applikationer och drivrutiner m.m.
- CPU:n växlar mellan de processer/trådar som behöver service utifrån operativsystemets skedulerare (prioritet används oftast), växlingarna sker oerhört snabbt vilket ger sken av samtidighet
- Datorer med single core (en kärna) kan endast köra en process/tråd åt gången, dvs. inga äkta parallella operationer
- Avbrott (interrupt) kan komma från en mjukvaru eller hårdvaru resurs närsomhelst
  - När datorn får ett avbrott stoppar OS:et och CPU:n all annan aktivitet för en oerhört kort stund och ger service till resursen som gjorde förfrågan (man kan därför säga att interrupt har högsta prioriteten)

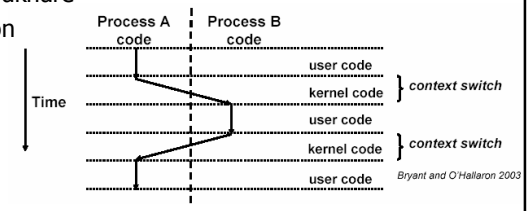
Processer och trådar, CPU





Processer och Task Control Block

- Varje process tror den har exklusiv tillgång till allt minne i datorn
- Vid varje växling (context switch) måste viss information om processen sparas undan i OS:ets TCB eller PCB
- TCB/PCB lagrar bland annat:
  - Unika Process id-numret
  - Process status - (exekverande, redo, väntande, blockerad, zombie (terminerad) och prioritet
  - Registerdata och programräknare
  - Öppna filer, IPC information
  - Minnes information
  - Processägarinformation
  - m.m.



Minneshantering

- OS tilldelar först minne till sig själv och drivrutiner (tolken mellan elektriska signaler och OS), sedan till applikationer i minnesblock så inga krockar sker
- Ett 32-bitars OS har kan adressera ca: 4 GB minne, omkring 2 GB av detta är tillgängligt för applikationer
- Olika nivåer på minne
  - Register (CPUns hjärta) : GPR och FPU i olika bitlängd < 100
  - Cache i CPU : 32 – 64 kB
  - Extern cache (i samma kapsel som CPUn) : 128 kB – 4 MB
  - RAM : upp till 4 GB
  - Virtuellt minne eller swap (fil på hårddisken) : ca 1.5 * RAM
  - Hårddisken för arkivering och lagring

Systemets svagheter

- Ett flertal mekanismer kan bli exploaterade (exploited) för att ta sig in i ett system, t.ex.
  - Brister i säkerheten hos OS
  - OS designfel eller buggar
  - Felaktigt konfigurerat OS
  - Virus
- Mekanismerna är oftast specifika för en viss funktion i ett visst OS och/eller applikation
- Syftet med attacken är oftast
  - Stöld av confidentiell data
  - Stöld av autentiseringsdata
  - DoS (Denial Of Service)
  - Använda systemet för att attackera andra system, endera direkt eller som en zombie

Systemsäkerhet

- Systemsäkerhet innebär följande uppgifter
  - Konfigurera användarkonton
  - Sätta rätt fil och katalogrättigheter
  - Ta bort onödig mjukvara
  - Installera säkerhetsuppdateringar och patchar för mjukvara
  - Konfigurera och installera verktyg för diskhantering
  - Installera olika former av säkerhetsmjukvara
  - Konfigurera system för loggning och intrångsdetektion
- De flesta enanvändar OS kan ställas in så ingen autentisering behövs
  - Ingen mekanism för filrättigheter osv. det som återstår är fysisk säkerhet, lösenord i BIOS och kryptering
- Fleranvändar OS
  - Kräver alltid autentisering för filer eller resurser för att bli auktoriserad
  - Personen eller applikationen får då en identitets token som heter för windows – Security Identifier (SID) och UNIX – user identity (uid)

Filrättigheter

- Admin, superuser eller root har alltid full access annars är systemresurser (filer, kataloger, system) accesskyddade med:
  - Read – läs
  - Write – skriv
  - Change permission – ändra
  - Execute – exekevera
- Oftast har resurserna en ägare och/eller ägs av en grupp som har change rättigheter, t.ex. UNIX
  - Skillnad på stora och små tecken, ”ls -al” visar användarrättigheter
  - -rwxr--rw- 1 hjo users 4766 9 jan 10 13:46 testfile
  - r= read access, w= write access, x= execute access
  - Change rights (order is UserGroupOther - rwxrwxrwx)
    - chmod g+w testfile
      - -rwxrw-rw- 1 hjo users 4766 9 jan 10 13:46 testfile
  - Change owner (owner.group)
    - chown hjo.hjo testfile

Information Rights Management (RM)

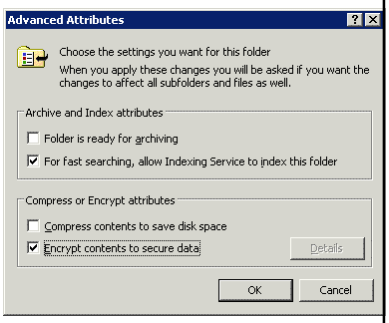
- RM försöker förhindra att känslig information från att spridas vidare, avsiktligt eller oavsiktligt (Windows Server 2003)
  - Vem har rätt att öppna ett dokument och hur många gånger dokumentet får öppnas
  - Vad den personen/rollen/gruppen får göra med informationen (skriva ut, förändra, vidarebefordra, kopiera)
  - Hur länge informationen är giltig
- Tillvägagångssätt (3 övergripande steg i en RM-miljö)
  - Skapa information som skyddas med hjälp av RM. Mallar etc.
  - Licensering och distribution av RM-skyddad information. Informationen krypteras med en privat nyckel från utfärdaren.
  - Hämtning av licens och användning av RM-skyddad information. Autentiserarde mottagare måste ha en betrodd klient som valideras mot en server som sedan dekrypterar informationen med en publik nyckel. Licensen är kopplad till informationen enligt uppsatta villkor.

Skydd av bärbara datorer

- Bärbara datorer är en stor potentiell säkerhetsrisk!
  - Rymmer mycket data, liten och lätt
- Lösenordskydd i BIOS
  - Endast mot tjuvar utan datorvana om inte speciella kretsar finns i datorn som lagrar lösenordet fast batteriet töms
- Någon form av ”säker” autentisering mot operativsystemet
- Hårddisken går trots allt att plocka ur för ovanstående metoder
- Kryptering av filer på hårddisken (Windows EFS)
  - Varje fil får en unik EFS-nyckel kallad, FEK (File Encryption Key)
  - Nyckeln krypteras i sin tur och skyddas av användarens publika nyckel som matchar användarens motsvarande EFS-certifikat
  - FEK skyddas av en publik nyckel
  - Alla krypterade nycklar sparas i en lista, DDF (Data Decryption Field)

Windows XP EFS (Encrypting File System)

- Andra OS
  - BSD & Linux – TCFS (Transparent Cryptographic File System)
  - Andra UNIX – CFS (Cryptographic File System)
- För att kryptera en fil/katalog i Windows
  - Öppna Windows explorer
  - Högerklicka på fil/katalog, välj egenskaper
  - Klicka sedan på avancerat knappen
  - Kryptera fil/katalog genom att markera **Encrypt contents to secure data**



- Se artiklar här:
  - www.microsoft.com/technet/prodtechnol/winxppro/evaluate/xpsec.mspx
  - www.microsoft.com/technet/prodtechnol/winxppro/support/dataprot.mspx

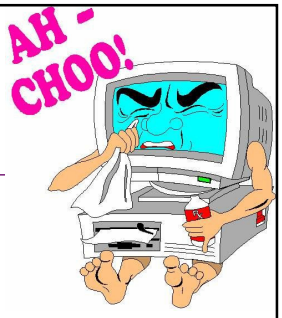
Andra skyddsverktyg

- Några 3dje-parts krypteringsalternativ
  - Proffs
    - Pointsec, Compusec, Safeboot etc.
  - Enklare
    - PGP Desktop, Winguard, Folder Lock etc.
- Enklare skydd finns inbyggt i vissa applikationer
  - Lösenordsskyddad fil
  - Är ej tillräckligt skydd mot seriösare attacker
- Data återställning
  - På något sätt bör skyddade/krypterade filer/diskar vara möjliga att återfå i läsbart skick
  - Borttappad nyckel, slutat arbetet, rättsliga krav
  - Användare som har access till denna process kallas för ”recovery agents”, vanligen superuser plus ett till konto

OS Hardening (härdning)

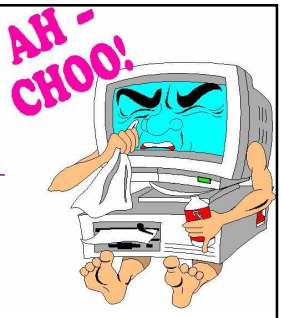
- Går ut på att konfigurera datorn så chans för intrång minimeras
  - Användarkonton
    - Ta bort guest och andra konton som inte används
    - Ändra default lösenord på de konton som har det
    - Superuser - använd många och olika tecken > 15 st. tillåt om möjligt endast inloggning från lokal/fysisk plats
  - Ta bort all onödig programvara
    - Minimerar säkerhetshål och ger även enklare administration
  - Säkerhetspatchar (mycket viktigt!)
    - Eftersom OS är extremt komplexa programvaror så plågas de av buggar och ospecificerade operationer som utnyttjas
  - Diskhantering
    - Vissa attacker går ut på att fylla all tillgänglig diskplats
    - Använd egen diskvolym för temporära filer
    - Sätt disk quota (maxgräns) per användare, process etc.

Skadlig kod (datavirus)



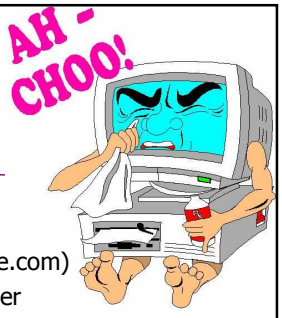
- Datavirus har ofta liknats vid sin biologiska motsvarighet och det är inte helt fel
- Är en undergrupp av flera slags program som kan infektera en dator och brukar benämnas skadlig, fientlig eller elak kod. Diagnos: allt mellan snuva och döden
- Virus
  - Litet program som kopierar in sig i ett befintligt program (värden), sprider sig sedan från program till program, kan ej spridas utan värd (program att infektera)
- Makrovirus (script)
  - Förknippat med vissa program och är därför plattformsoberoende
- Maskar
  - Ett fristående program som själv reproducerar sig och sprider sig via användarens mail eller fildelningsprogram etc., förändrar ej andra program eller filer

Skadlig kod (datavirus)



- Trojan
  - Ett fristående program som är maskerat och dolt inuti ett annat program eller fil
  - Infekterar datorn när användaren försöker använda programmet eller filen
  - Kan göra allt som användaren kan göra på datorn!
- Virus minskar men maskar och trojaner ökar
- Är det en fara och varför skydda sig?
  - En infekterad dator kan utnyttjas som bas för nya attacker
- Borttagning?
  - Kan vara enkelt ibland men också svårt om själva OS:et smittats ner
- Skydd?
  - Antivirusprogram, personlig brandvägg och kunskap/sunt förnuft
  - Uppdatering och skötsel av program samt vaksamhet på Internet

Maskar och trojaner - skador



- Skydd forts.?
  - Verifiera filintegriteten med hashsumma för varje OS/program fil, t.ex. Tripwire (http://www.tripwire.com)
  - Centraliserad virus scanning med firewall mailserver
- Fjärrstyrning av datorn
  - Leder i sin tur ofta till intrång på andra platser för ägaren
  - Eller för att attackera andra datorer
- Vissa brandväggar kan inte stoppa fientlig aktivitet på applikationsnivå
  - Personlig brandvägg eller brandvägg som filtrerar på paketnivå nödvändig
- ”Keyloggers” lagrar slagna lösenord m.m. – sänds iväg till hackaren
- Installera om datorn oftast enda säkra åtgärden!

Virusskyddet

- Aktivt virusskydd kräver en policy och organisation
- Varje företags IT-miljö är unik - virusskyddet bör utvärderas och ta hänsyn till faktorer som:
  - Systemmiljö - operativsystem, applikationer
  - Infrastruktur – nätverk och kommunikationslänkar
  - Administrationsmodell – centraliserad eller eller decentralicerad
  - Driftövervakningsprogram och distributionslösningar
  - Signaturfilsuppgraderingar – format, frekevens, storlek
  - Respons på nya virus – maximala tiden för skydd mot nytt virus?
  - Skanning och igenkänning av virus
  - M.m. …
- Administratörsrutiner för att hantera uppdateringar m.m.
- Alla användare bör veta hur man hanterar antivirusprogrammet och hur man skall bete sig om man upptäcker ett virus

Systemloggar

- De flesta OS har möjlighet till omfattande loggning
- Loggar är ovärderliga vid
  - Detektering av intrång via IDS (Intrusion Detection System)
  - Återhämtning efter säkerhetsincidenter
  - Hur intrånget gick till
  - Spåra vem som gjorde intrånget
- Om attackeraren har access till loggfiler så kan de modifieras eller raderas
  - Loggarna måste skyddas genom att skrivas på CD-R eller lagring på annat datasystem

Fysisk säkerhet

- Handlar om att säkra informationssystemet mot fysisk åverkan eller åtkomst genom utrustningens placering
  - Skydd mot åtkomst, obehöriga, tjuvar, skadegörelse etc.
  - Skydd mot dåliga miljöaspekter, brand- och vattenskydd m.m.
- Inpasseringssystem
  - Finns en många olika varianter, vissa kopplade mot katalogtjänst
  - Byggnadens arkitektur, arbetsrutiner och loggning
- Larm och galler
- Datahallen och arbetsplatsplanering
  - Planera och bygg rätt för att undvika skador
- Reservplan
  - Redundans
- Avbrottsfri kraft - UPS

Datasäkerhet (en mycket bred benämning)

- Säkerhetskopiering eller backup
  - En självklar sak kan man tro…
  - Orsaker till datainformationsförlust
    - Hårdvarufel, slitage MTBF (Mean Time Before Failure)
    - Avmagnetisering/förstörelse pga. ålder eller dålig miljö
    - Fysiska skäl (se tidigare OH)
    - Mänskliga faktorn (oavsiktlig radering)
    - Tekniska fel i hårdvara eller mjukvara
    - Avsiktlig förstörelse (virus, hackers)
- Minimikrav för en säkerhetskopieringspolicy
  - All programvara skall skyddas m.h.a. säkerhetskopiering
  - Systemdata bör upprätthållas med minst en månads intervall
  - Användardata bör vara kopierat dagligen enligt ett bestämt schema

Säkerhetskopiering

- Olika säkerhetskopiering eller backup typer:
- Privat
  - Sprida ut datat på flera datorer, diskar, CD-RW/DVD-RW
- Professionellt
  - Full säkerhetskopiering, (alltid allt)
  - Differentiell …, endast det som förändrats sedan sista fulla kopian
  - Inkrementell …, endast det som förändrats sedan sista fulla kopian och senaste differentiella kopian
  - Speciellt inkrementell … kräver att man har bra koll på sitt schema och backupband annars kan allt gå åt skogen
- Tumregeln är ta backup på det som är omöjligt/svårt eller dyrt/tidsödande att ersätta på annat sätt
- Servrar med viktiga tjänster är speciellt viktiga, de får inte gå ner!

Säkerhetskopiering

- Ansvar och uppföljning
  - Vem och hur?
- Testa och verifiera
  - Kontrollera regelbundet att data går att återskapa, helst med och till andra hårdvaror
- Program för säkerhetskopiering
  - Felfritt, lättanvänt och hög automatiseringsnivå är grundkrav
- Backup media
  - CD-RW/DVD-RW
  - Band är vanligast (äldsta teknologin nämnt först)
    - DAT, 12 GB okomprimerat
    - DLT, 40-110 GB okomprimerat och 6-11 MB/s i överföringshastighet
    - AIT, 50 GB okomprimerat
    - Ultrium, 100-200 GB okomprimerat och 20-30 MB/s i överföringshastighet