Uke 38

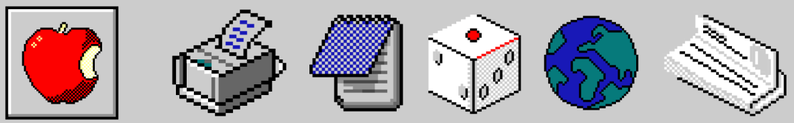
Introduksjon til operativsystemer
Datasikkerhet: Hvordan hackes vi

11:11PM

Forskjellige typer operativsystemer

- Enkel-Bruker, enkel-oppgave
- Enkel-Bruker, multi-oppgaver
- Multi-bruker, multi-oppgaver

Big Man



Home

Forskjellige typer operativsystemer

Distribuert OS:

- Støtte for å kontrollere ressurser på flere datamaskiner

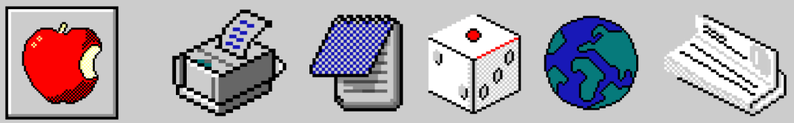
Real-Time OS:

- Støtte for systemer hvor sanntid er viktig som biler, robotter, fly, instrumenter, atomreaktorer, osv.

Embedded OS:

- Bygd inn i enheter for å løse et konkret problem, som for eksempel enkle mobiltelefoner, mikrobølgeovner, vaskemaskiner, dørlås, osv.

Big Man



Home

Hovedkomponenter i et OS - Synlig

Brukergrensesnitt

- Mekanismer for at bruker og programmer skal kommunisere med OS og bruker maskines ressurser

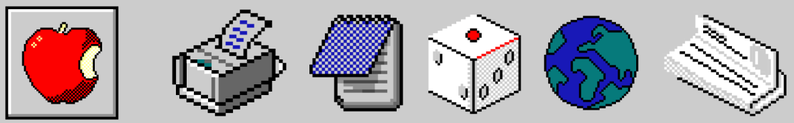
Filsystem

- Mekanismer for at en bruker skal kunne lage, slette, modifisere og manipulere filer

Enhetskontroll

- Gjøre at systemet skal kunne kontrollere enheter som er koblet til som for eksempel mus, tastatur, skjerm, osv.

Big Man



Home

Hovedkomponenter i et OS - Transparent

Prosessorkontroll

- Tilby mekanismer for at systemet effektivt og rettferdig skal kunne dele CPU for programmene skom kjører

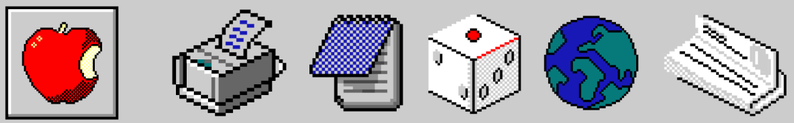
Minnekontroll

- TIlby mekanismer for at systemet skal kunne fordele minneresurser - allokerer plass til programmer

Kommunikasjonstjenester

- Tilby tjenester for at systemer skal kunne kommunisere med andre prosesser (på samme eller andre maskiner)

Big Man



Home

Brukernivå vs. Kjernenivå

OS skiller vanligvis mellom brukernivå og kjernenivå

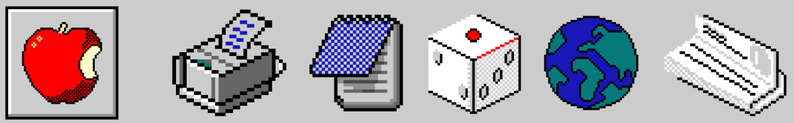
OS kjører i kjernemodus

- Tilgang til hele minne
- Alle instruksjoner kan bli kjørt
- Går forbi all sikkerhet

Vanlige programmer og flere API'er kjører i brukermodus

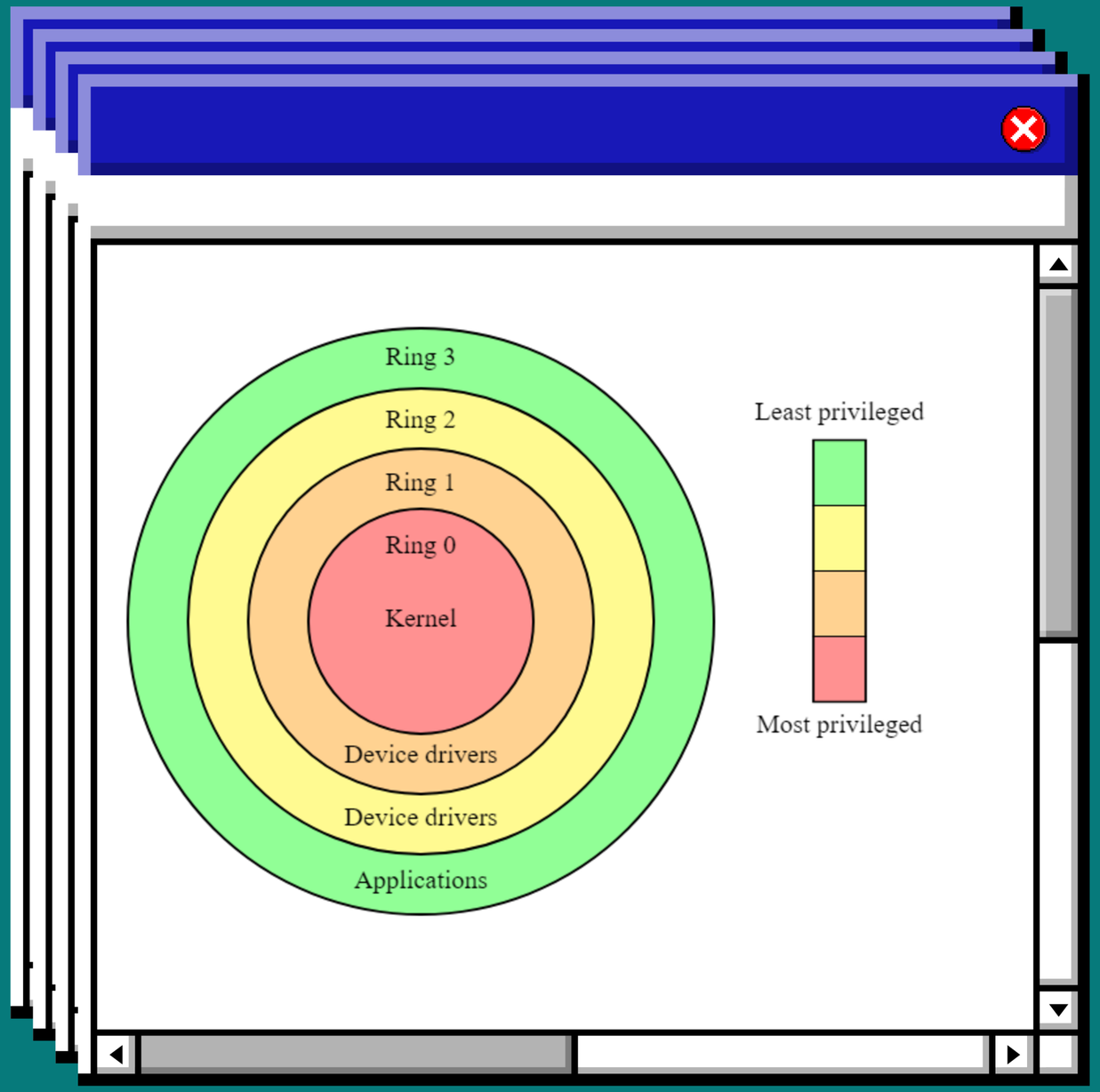
- Protected mode
- Bruker kan ikke kontakte maskinvare eller enheter direkte, kun gjennom API
- Tilgang til kun et begrenset minneområde
- Begrenset tilgang til prosessoren

Big Man



Home

OS - Protection Ring



Home

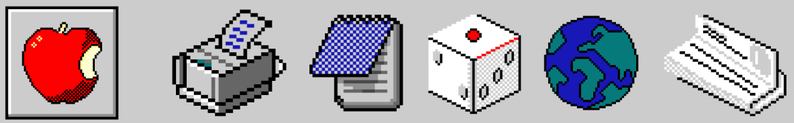
Organisering av operativsystemer

To hovedmodeller

Monolittisk kjerne (“the big mess”)

- Alle beskyttet kode kjører i samme beskyttelsesområde
- Effektivt: Alle komponenter kan kommunisere direkte
- Feil kan få følger for andre komponenter enn der de oppstår
- Store og komplekse
- BSD UNIX, Linux, Windows 10

Big Man



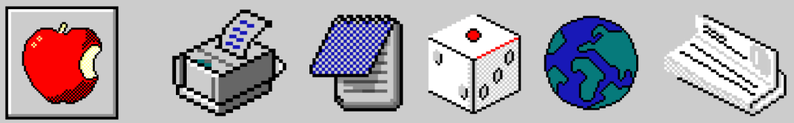
Home

Organisering av operativsystemer

Mikro-kjerner

- Små moduler med minimal funksjonalitet
- Flest mulig tjenester er skrivere i brukermodus
- Ineffektiv: Mange beskjeder fram og tilbake
- Vanskelig å utføre ting i riktig rekkefølge
- Liten, modulær, utvidbar, protable
- MACH, Window NT

Big Man



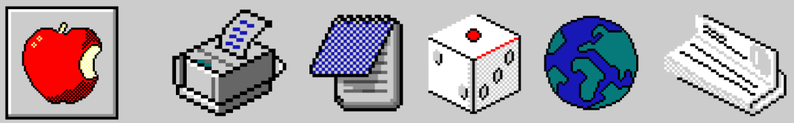
Home

Beskytte lagret informasjon

Å kryptere lagrede data er en strategi for å understøtte konfidensialitet og integritet

- Å sørge for at informasjon ikke kommer uvedkommende i hende ved å gjøre data uleselig/uforståelig for utenforstående
- Å sørge for at modifikasjon av data oppdages
- Eksempel: Laptop mistes/stjeles, datainnbrud på server/tjener der data lagres

Big Man



Home

Beskytte lagret informasjon

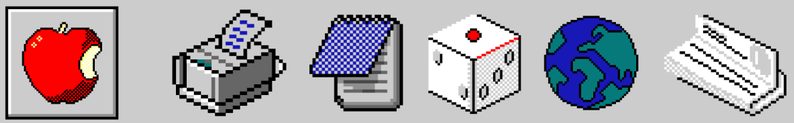
Sikkerhetskopiering er en strategi for å ta vare på informasjon over tid

- Bidrar til økt tilgjengelighet ved å være i stand til å gjenopprette systemer og data ved uønskede hendelser som endrer eller sletter informasjon
- Eksempel: Angrep med løsepengevirus, datainnbrudd der infromasjon er slettet eller endret

Gode retningslinjer for avhending av data

- Hvordan kvitte seg med fysiske enheter som inneholder data, uten å potensielt lekke data

Big Man



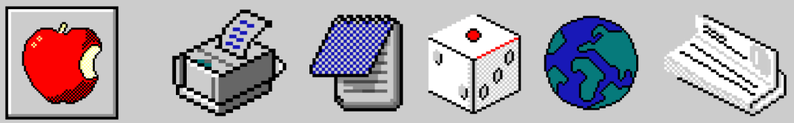
Home

Kommunikasjonssikkerhet

Kommunikasjon i trådløse nett går via radiosignaler:

- “Hvem som helst” kan lytte til signalene
- Signalforstyrrelser (tilsiktet eller utilsiktet) kan føre til utilgjengelighet
- Falske aksesspunkter: En trådløs enhet vil koble seg til aksesspunktet med sterkest signal
- Kompromitterte aksesspunkter, spesielt åpne nett/aksesspunkter

Big Man

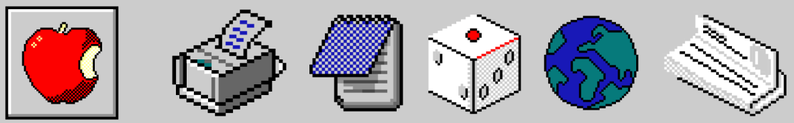


Kommunikasjonssikkerhet

Kommunikasjon i kablede nett går via fysiske kabler

- Avlytting krever fysisk tilgang, men er likevel fullt mulig
- Ødelagt kabel (tilsiktet eller utilsiktet) kan føre til utilgjengelighet
- Kompromittert nettverks-endepunkter (routere/switcher)
- Kompromitterte enheter på samme fysiske nettverk

Big Man



Home

Datasikkerhet

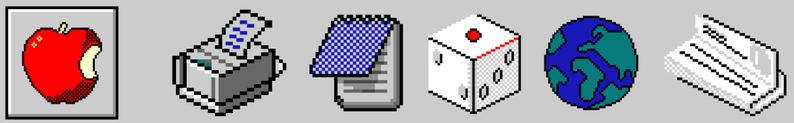
Brannmur:

- Slipper inn eller avvise trafikk inn i og/eller ut fra et nettverk basert på forhåndsdefinerte regelsett
- Brannmur fungerer som en tilgangskontroll for nettverket
- Kan være et dataprogram eller maskinvare laget for akkurat dette formålet

Inntrengningsdeteksjon:

- Overvåker nettverkstrafikk og kan oppdage:
  - Både forsøk på og suksessfulle innbrudd
  - Datavirus og annen ondsinnet programvare
  - Tjenestenektangrep (DoS / DDoS)

Big Man

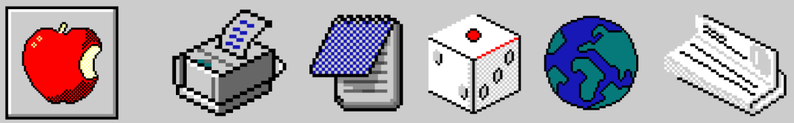


Home

Definisjoner

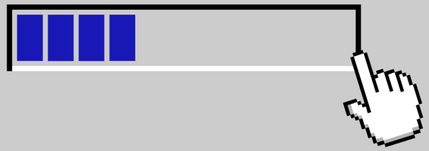
Digital sårbarhet: En feil i et IKT-system som kan utnyttes
Nulldags-sårbarhet: Sårbarhet som noen har kunnskap om, før produsenten/leverandøren eller brukerne av systemet/programvaren kjenner til den
Skadevare: Samlebetegnelse på programvare som har som mål å gjøre skade
Angrepsvektor: Metoden en angriper bruker for å utføre et angrep på en datamaskin, et nettverk eller et datasystem
Sårbarhetsflate: Summen av (de potensielle) sårbarhetene i et system som kan nås og utnyttes av en angriper

Big Man



Home

Typer skadevare



Home

Vius	Dataorm	Trojaner	Bakdør
Kjennetegnes ved at det sprer seg hver gang en fil med virus blir åpnet av bruker eller systemet	Skadevare som på egenhånd er i stand til å spre seg og funne nye ofre	Skadevare som utgir seg for å være et nyttig program	En ubeskyttet og ukjent åpning inn i et datasystem, laget av en angriper
Spionvare	**Tastelogger (Keylogger)**	**Rootkit**	**Exploit**
Programvare for å spionere på en bruker i håp om å få tak i f. eks. informasjon, passord, og liggnende	En enhet eller programvare som er koblet til tastatur eller maskin og som lagrer eller videresender alle tastetrykk. En varian av spionvare	Skadevare som endrer eller erstatter funksjoner i OS eller applikasjoner, med mål å ta kontroll over en maskin eller system	Et program, en sekvens med data, eller instrukser på hvordan en sårbarhet kan utnyttes