Säkerhet

Grundläggande operativsystem 1DV415

Innehåll

- Introduktion
- Kryptering
- Autentisiering
- Åtkomstkontroll
- Säkerhetsattacker
- Attackförebyggande och säkerhetslösningar

Introduktion

- Säkerhetshot från insidan och utsidan
- Konfidentialitet
- Integritet
- Skydd

Kryptering

- Krypteringssystem
- Nyckel
- Klartext - Krypterad text
- Typer av krypteringsalgoritmer

Delad nyckel

Kryptering

Dekryptering

Publik nyckel

Kryptering

Dekryptering

Autentisiering

- Lösenord
- Brute-force-attack
- Saltning av lösenord

Smart cards och biometri

- Biometri
- Smart card
- Dubbel-faktor-autentisiering

Kerberos

- Skyddar mot interna attacker
- Tickets

Single sign-on

- Login script
- Token-baserad autentisiering

Åtkomstkontroll

- Åtkomsträttigheter
- Privilegium
- Skyddsdomän

Åtkomstkontrollsmodeller

- Säkerhetspolicy
- Säkerhetsmekanismer
- Rollbaserad åtkomstkontroll
- DAC och MAC

Åtkomstkontrollmatris

	Fil A	Fil B	Skrivare
Alice	READ* WRITE*	READ* WRITE*	Utskrift*
Bob	READ* WRITE	READ* WRITE	Utskrift
Kalle	READ		Utskrift
Pelle		READ	
Gäst			

Access Control List

Fil A:
<Alice, {read*, write*}>
<Bob, {read*, write}>
<Kalle, {read}>

Fil B:
<Alice, {read*, write*}>
<Bob, {read*, write}>
<Pelle, {read}>

Skrivare:
<Alice, {Utskrift*}>
<Bob, {Utskrift}>
<Kalle, {Utskrift}>

Attacker

- Kryptoattacker
- Virus och maskar
- DoS-attacker
- Utnyttjande av mjukvarusäkerhetshål

Attackförebyggande och säkerhetslösningar

- Brandväggar
- IDS (intrusion Detection Systems)
- Antivirus
- Säkerhetspatchar
- Säkra filsystem
- Säker kommunikation