Säkerhetsaspekter och systemkonstruktion

En presentation av
Jan Jönson
jan.a.jonson@aerotechtelub.se
070 - 626 86 05

AerotechTelub

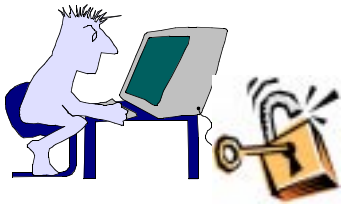
Disposition

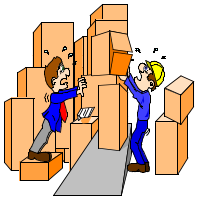
- Bakgrund
- Hotbild
- Krav bild
- Säkerhetsfunktioner
- Sammanfattning
- Frågor

SESAM
00-10-18
Jan Jönson

AerotechTelub

Presentation

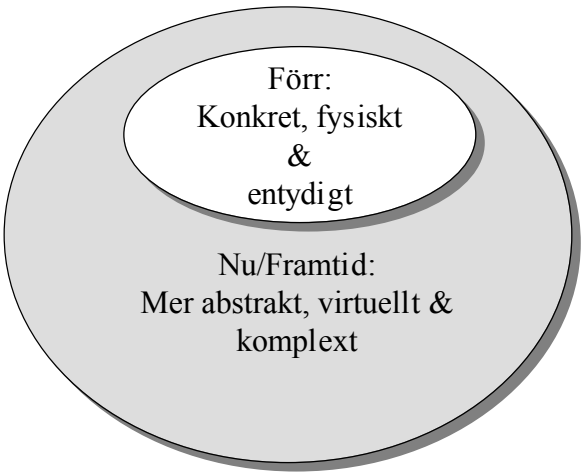




SESAM
00-10-18
Jan Jönson

AerotechTelub

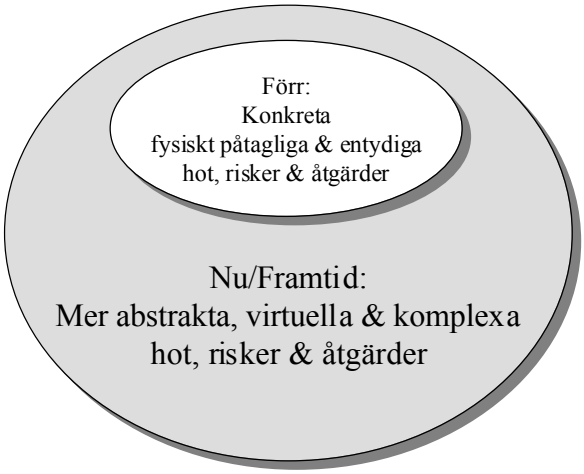
Paradigmskiftet



SESAM
00-10-18
Jan Jönson

AerotechTelub

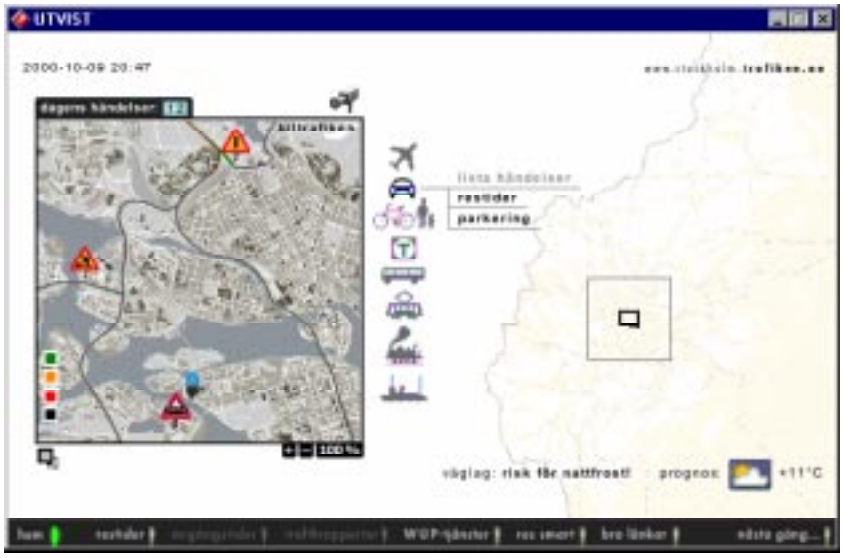
Det säkerhetsmässiga paradigmskiftet



SESAM
00-10-18
Jan Jönson

AerotechTelub

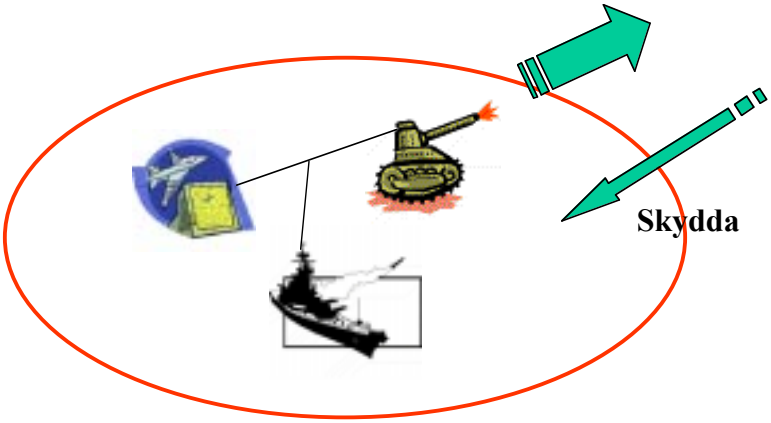
www.trafiken.nu



SESAM
00-10-18
Jan Jönson

AerotechTelub

Vilket är problemet



SESAM
00-10-18
Jan Jönson

AerotechTelub

Hot då

Televäxel scanning (letar modem, fax, toner samt vidarkopplingar)

- **Toneloc** (100-400 nr/tim)
- **THC Scan** (100 nr/tim)
- **PBX hacker** (100-300 nr/tim)
- **BlueBEEP** (100-300 nr/tim)

AIX version 4
(C) Copyright by IBM
and by others 1982,1994
login:

SESAM
00-10-18
Jan Jönson

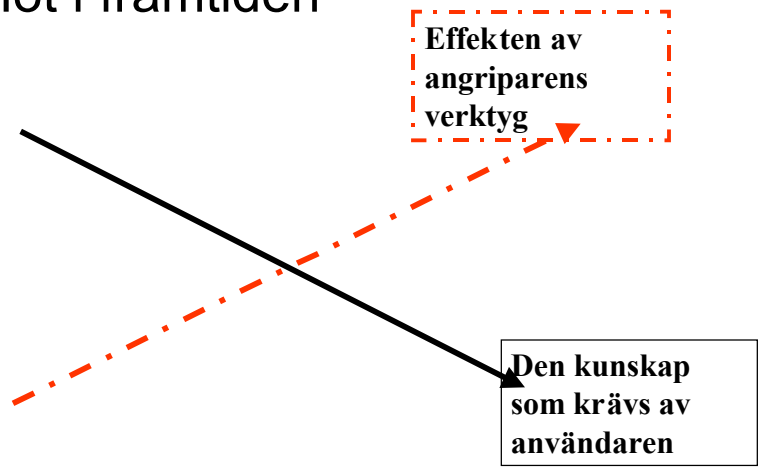
AerotechTelub

Hot då och nu

SESAM
00-10-18
Jan Jönson

AerotechTelub

Hot i framtiden



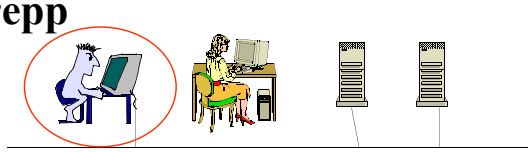
SESAM
00-10-18
Jan Jönson

AerotechTelub

Angriparen

Yttre angrepp

Inre angrepp



SESAM
00-10-18
Jan Jönson

AerotechTelub

Vem är angriparen

Aktivister
Cyberterrorister
Hacktivister

Främmande makt

Insidern

SESAM
00-10-18
Jan Jönson

AerotechTelub

Begrepp

- *Sekretess/confidentiality*
  - avsikten att innehållet i ett informationsobjekt (eller ibland även dess existens) inte får göras tillgängligt eller avslöjas för obehöriga
- *Riktighet/Integritet/integrity*
  - oberörbarhet, helhet med förmåga att upprätthålla ett värde genom skydd mot oönskad förändring, påverkan eller insyn
- *Tillgänglighet/availability*
  - möjligheten att utnyttja resurser efter behov i förväntad utsträckning och inom önskad tid
- *Spårbarhet/accountability*
  - princip innebärande att verksamheten och tillhörande system skall innehålla funktioner som gör det möjligt att entydigt härleda utförda operationer till enskilda individer

Källa: ITS Rapport 6

SESAM
00-10-18
Jan Jönson

AerotechTelub

Begrepp

- Autenticering/authentication
  - 1) kontroll av uppgiven identitet, t ex vid inloggning, vid kommunikation mellan två system eller vid utväxling av meddelanden mellan användare
  - 2) kontroll av att ett meddelande är äkta, i bemärkelsen att det inte förändrats sedan det lämnade avsändaren (användare, dator,kommunikationsnod etc.)
  - Autenticering (1) är synonymt med verifiering av identitet.
  - Autenticering (2) benämnes ofta meddelandeautenticering.
- Oavvislighet/nonrepudiation
  - princip som tillämpas vid överföring av meddelanden vari dessas avsändande och/eller mottagande ej i efterhand skall kunna förnekas

Källa: ITS Rapport 6

SESAM
00-10-18
Jan Jönson

AerotechTelub

FM krav/Autenticering

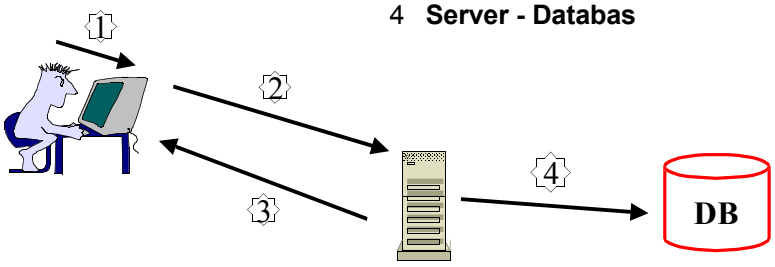
- Ett IT-system som innehåller hemliga uppgifter och som utnyttjas av flera personer skall, där så kan ske, vara försett med förstärkt inloggningsskydd.
- Källa FFS 1999:10 7kap 6§

SESAM
00-10-18
Jan Jönson

AerotechTelub

”Förstärkt” autenticering

1 **Användare - Klient**
2 **Klient - server**
3 **Server - Klient**
4 **Server - Databas**



SESAM
00-10-18
Jan Jönson

AerotechTelub

FM krav på spårbarhet

- Ett förbands databaser skall, där så kan ske, utformas så att det för varje datapost registreras datum för ändring, vem som har utfört ändringen och varifrån ändringen har gjorts. Uppgifterna skall sparas i en logg.

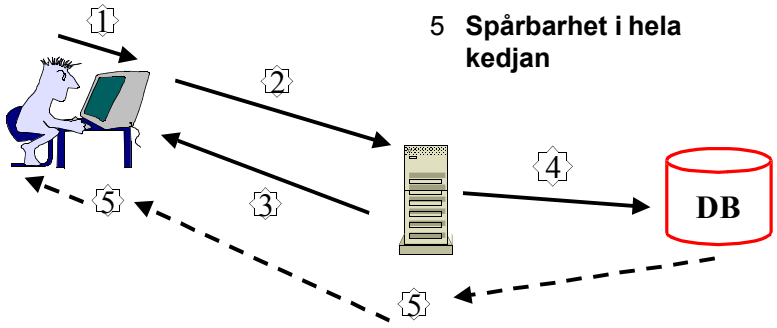
- Källa FIB 1999:5 9kap 3§

SESAM
00-10-18
Jan Jönson

AerotechTelub

Autenticering/Spårbarhet

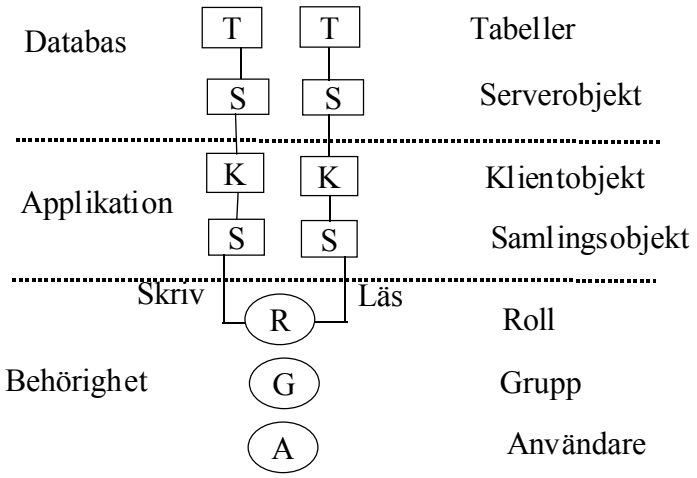
1 **Användare - Klient**
2 **Klient - server**
3 **Server - Klient**
4 **Server - Databas**
5 **Spårbarhet i hela kedjan**



SESAM
00-10-18
Jan Jönson

AerotechTelub

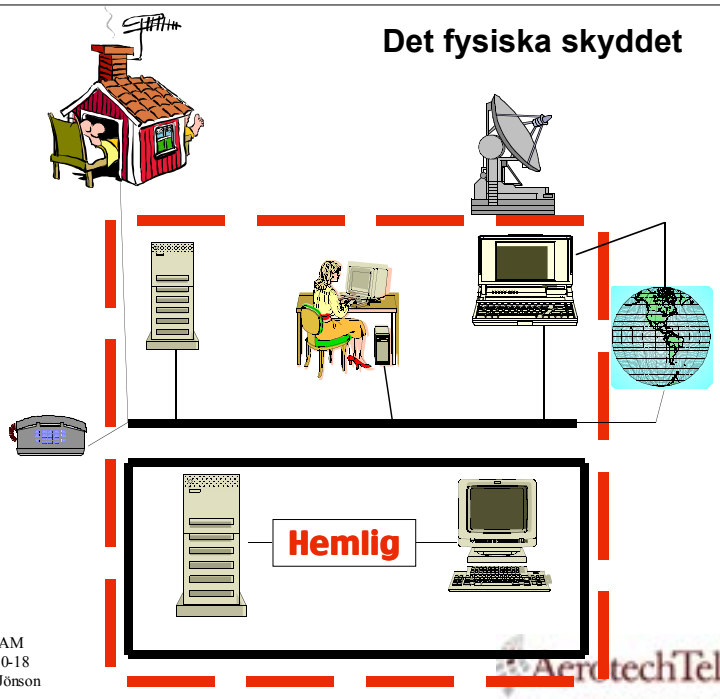
Krav på autenticering/spårbarhet



SESAM
00-10-18
Jan Jönson

AerotechTelub

Det fysiska skyddet



SESAM
00-10-18
Jan Jönson

AerotechTelub

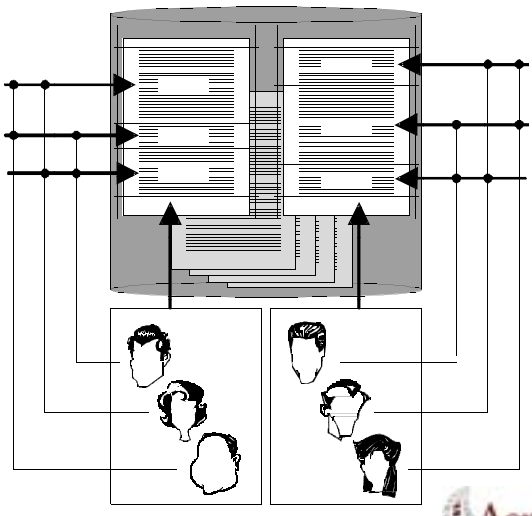
Manipulering/Förvanskning

- Det största hotet mot ett ledningssystem är nedsatt eller ingen tillgänglighet
- Förvanskad information kan alltid värderas och ifrågasättas
- Vid kravsättning bör tillgång till information och funktioner särbehandlas

SESAM
00-10-18
Jan Jönson

AerotechTelub

Säker dokumenthantering

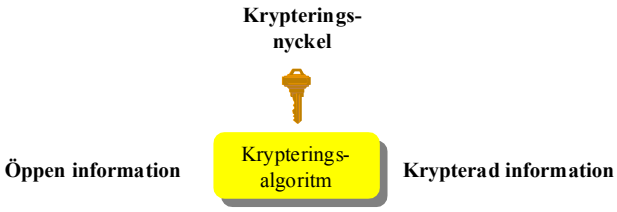


SESAM
00-10-18
Jan Jönson

AerotechTelub

Manipulering/Förvanskning

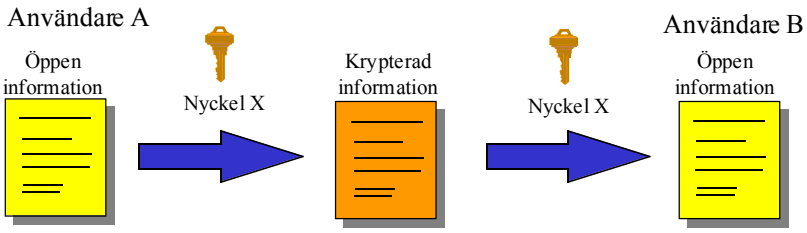
För att realisera säkerhetsfunktioner i IT-system krävs någon form av kryptering.



SESAM
00-10-18
Jan Jönson

AerotechTelub

Symmetrisk kryptering

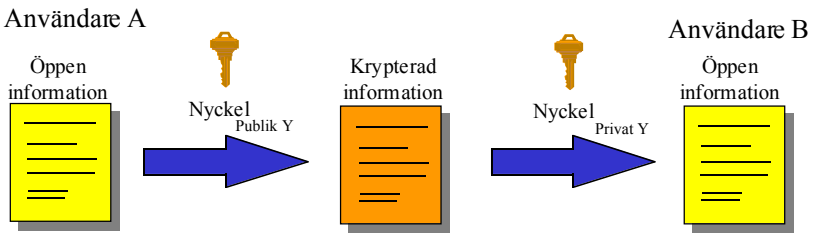


Samma nyckel används
vid kryptering och dekryptering.

SESAM
00-10-18
Jan Jönson

AerotechTelub

Asymmetrisk kryptering

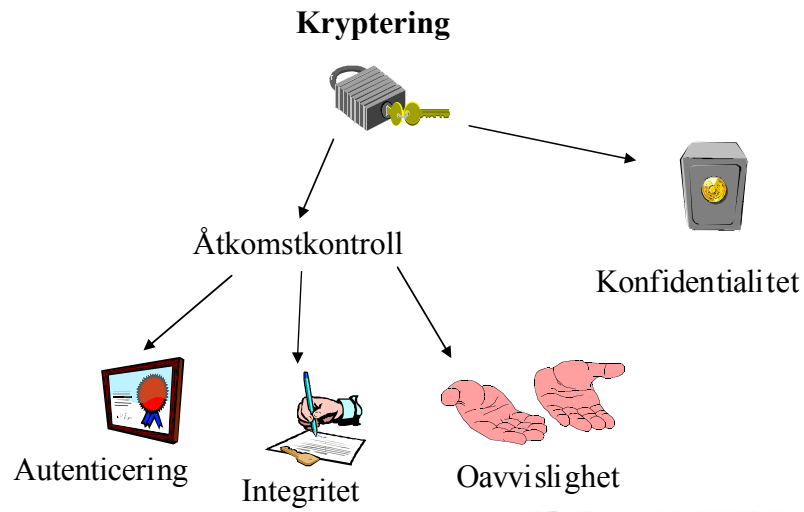


Olika nycklar används
vid kryptering och dekryptering.
Nycklarna utgör ett matchande nyckelpar

SESAM
00-10-18
Jan Jönson

AerotechTelub

Publik nyckelhantering

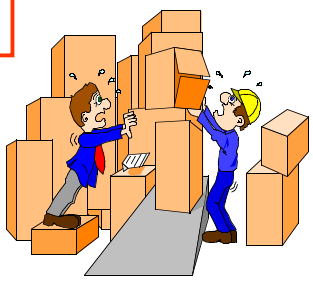


SESAM
00-10-18
Jan Jönson

AerotechTelub

Hur kontrollera program

- Miljontals rader kod
- Säkra program finns ej



- Samla säkerhetsfunktioner i moduler
- Säkra gränsytorna
- Utnyttja kraftfulla säkerhets-funktioner som t.e.x kryptering.
- Implementering viktig

SESAM
00-10-18
Jan Jönson

AerotechTelub

”Eastern eggs”

- Starta Word
- Öppna ett tomt dokument
- Skriv Blue
- Välj format/tecken
- Välj fetstil och blå färg
- Skriv ett blanksteg efter Blue
- Välj Hjälpmenyn/Om Microsoft Word
- Håll nere [Shift] och [Control] samtidigt och klicka på Windowslogotypen
- Spela med z och m

Källa: FOA tidningen nr 3

SESAM
00-10-18
Jan Jönson

AerotechTelub

Lager på lager

- Säkra externa anslutning mot omvärlden
- Avgränsa och säkra särskilt känsliga delar
- Uppdatera/kontrollera kritiska program
- Övervaka systemet
- Kryptera kritiska funktioner
- Utbilda personalen

AerotechTelub

Vad är nytt för försvarsindustrin

?

AerotechTelub

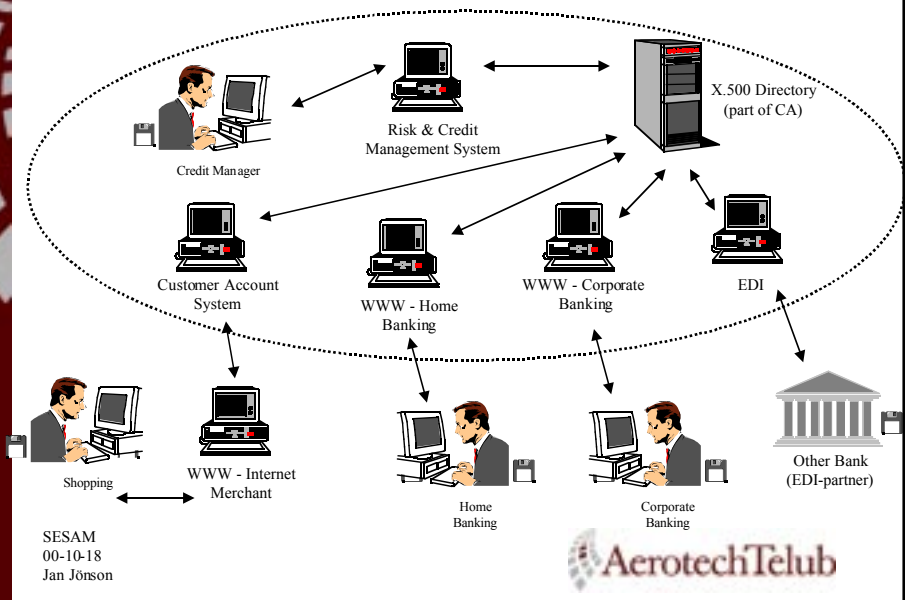
Systemutvecklingsprocessen

- Analys
- Design
- Implementation
- Test
- Drift- och underhåll

SESAM
00-10-18
Jan Jönson

AerotechTelub

Homogen säkerhet i en heterogen värld?



SESAM
00-10-18
Jan Jönson

AerotechTelub

IT-säkerhet är en chimär

Säkerhet har aldrig kommit först
Vems grad av trygghet skall avgöra
Det finns ingen definitiv nivå
Går ej att fuska
För mycket säkerhet = användaren kringår

SESAM
00-10-18
Jan Jönson

AerotechTelub