IT-säkerhet i distribuerade nätverksbaserade system

- Arkitekturpåverkande aspekter - några exempel

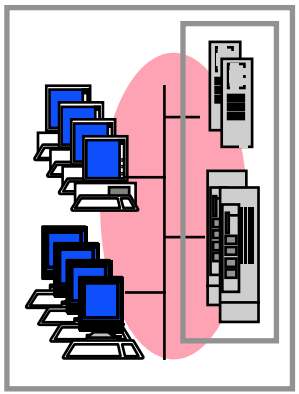
SESAM Höstseminarium 2001-10-24

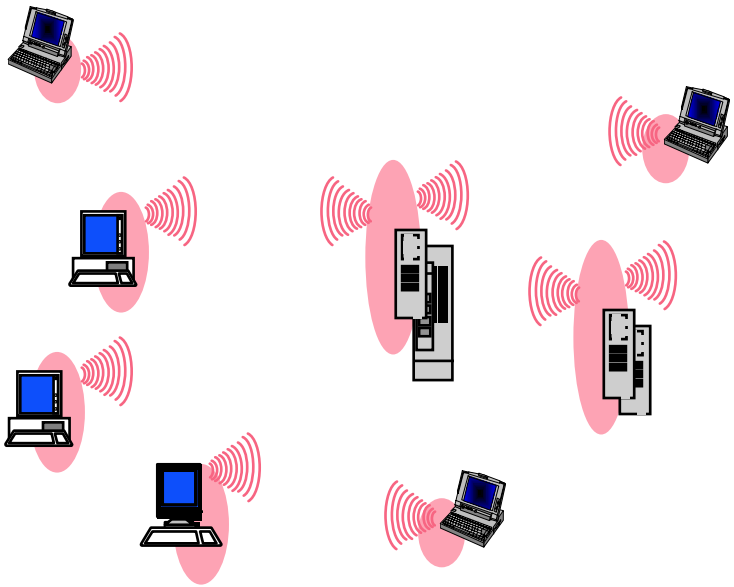
Jaan Haabma
Basesoft Open Systems AB
jaan@basesoft.se
08-13 17 20

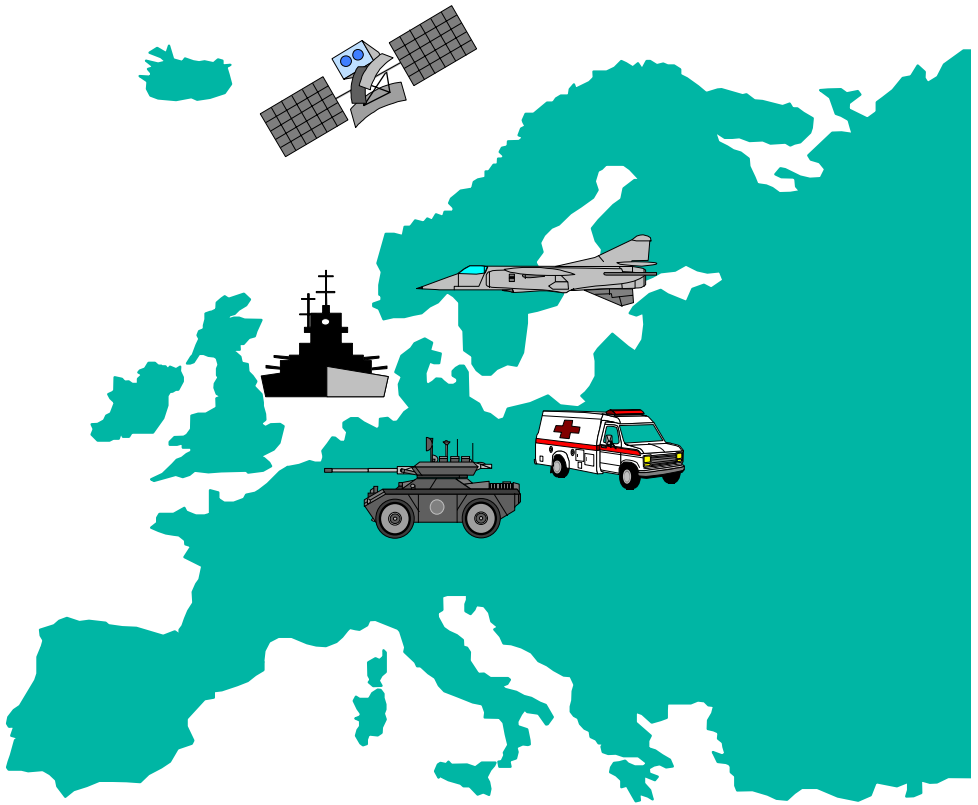
IT-säkerhet i distribuerade nätverksbaserade system

- Nätverksbaserade komponenter
  - => högre krav på IT-säkerhet
- Integritet (”riktighet”) resp konfidentialitet
- IT-säkerheten inbyggd i den tekniska infrastrukturen
- Exempelproblem - delegering
- Säkerhetsmekanismer - ex kryptering

Wired -> Wireless



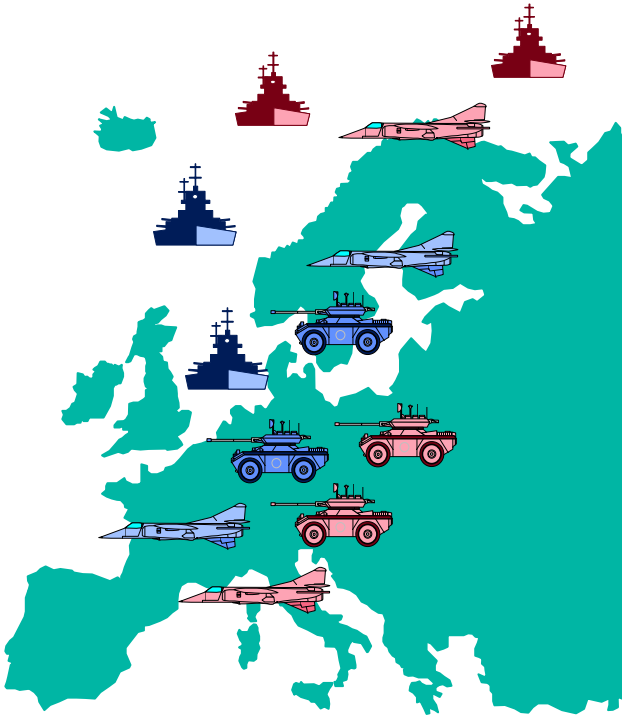




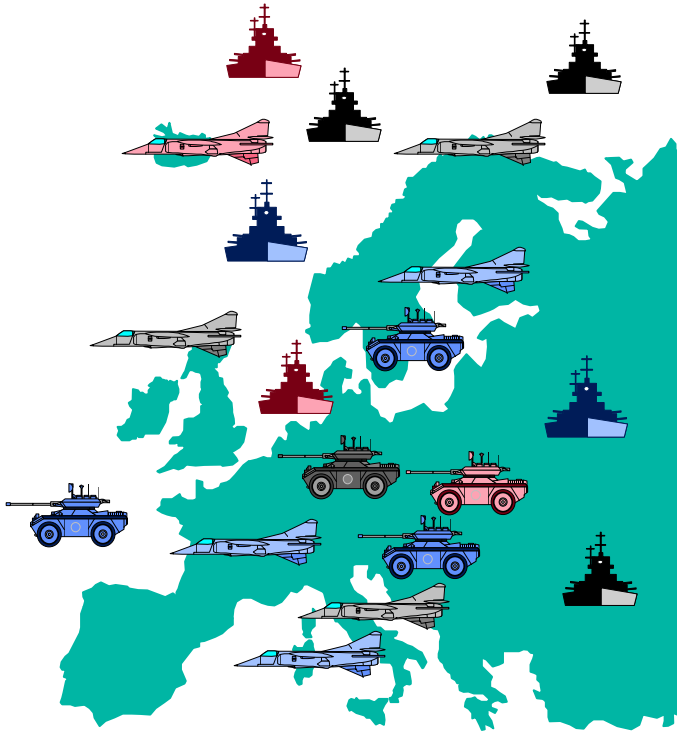
Today’s systems often rely on ”physical protection”!

”Riktighet”? Situation Awareness

If this is the real-world situation...

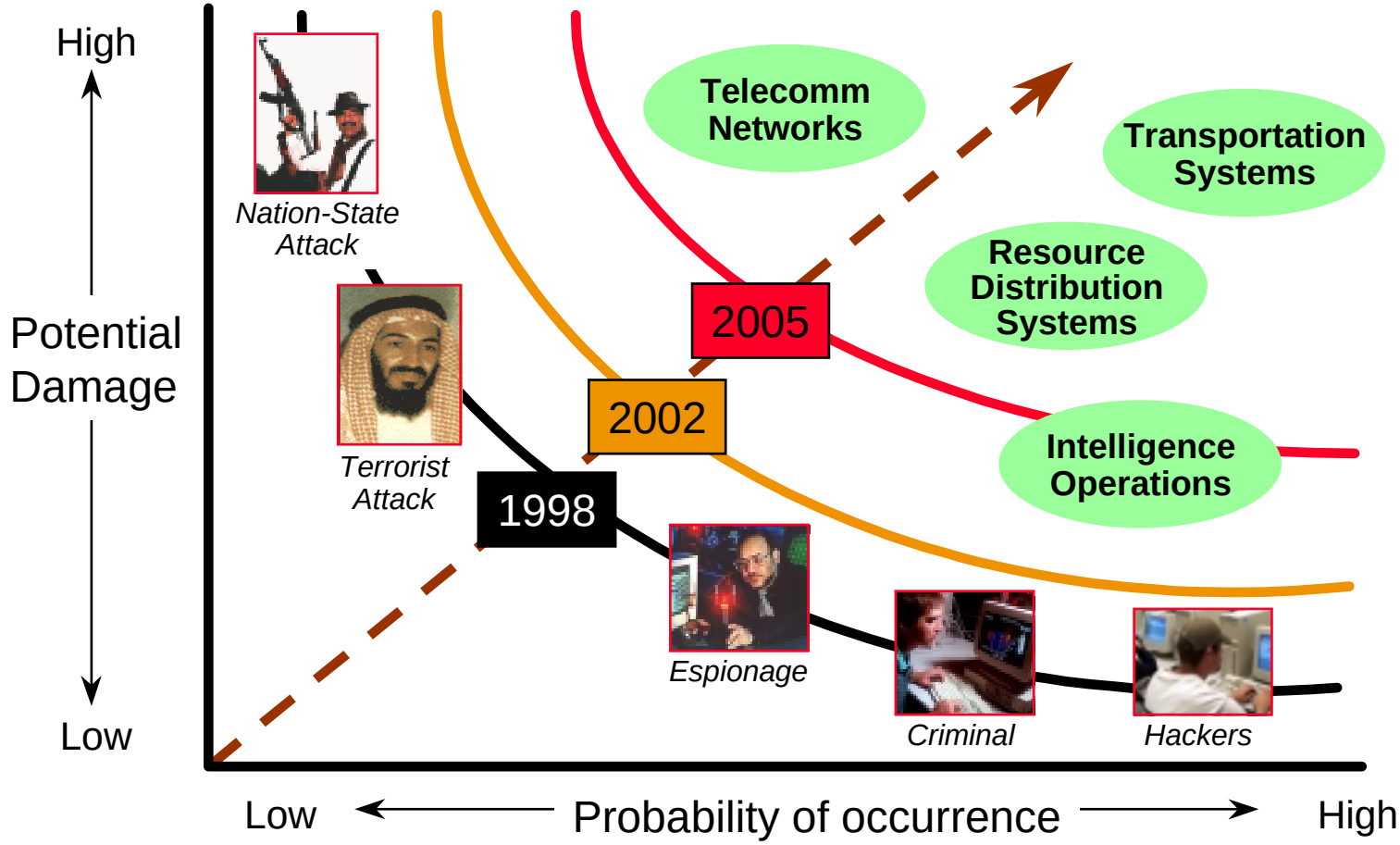


...you don´t want the systems to show this

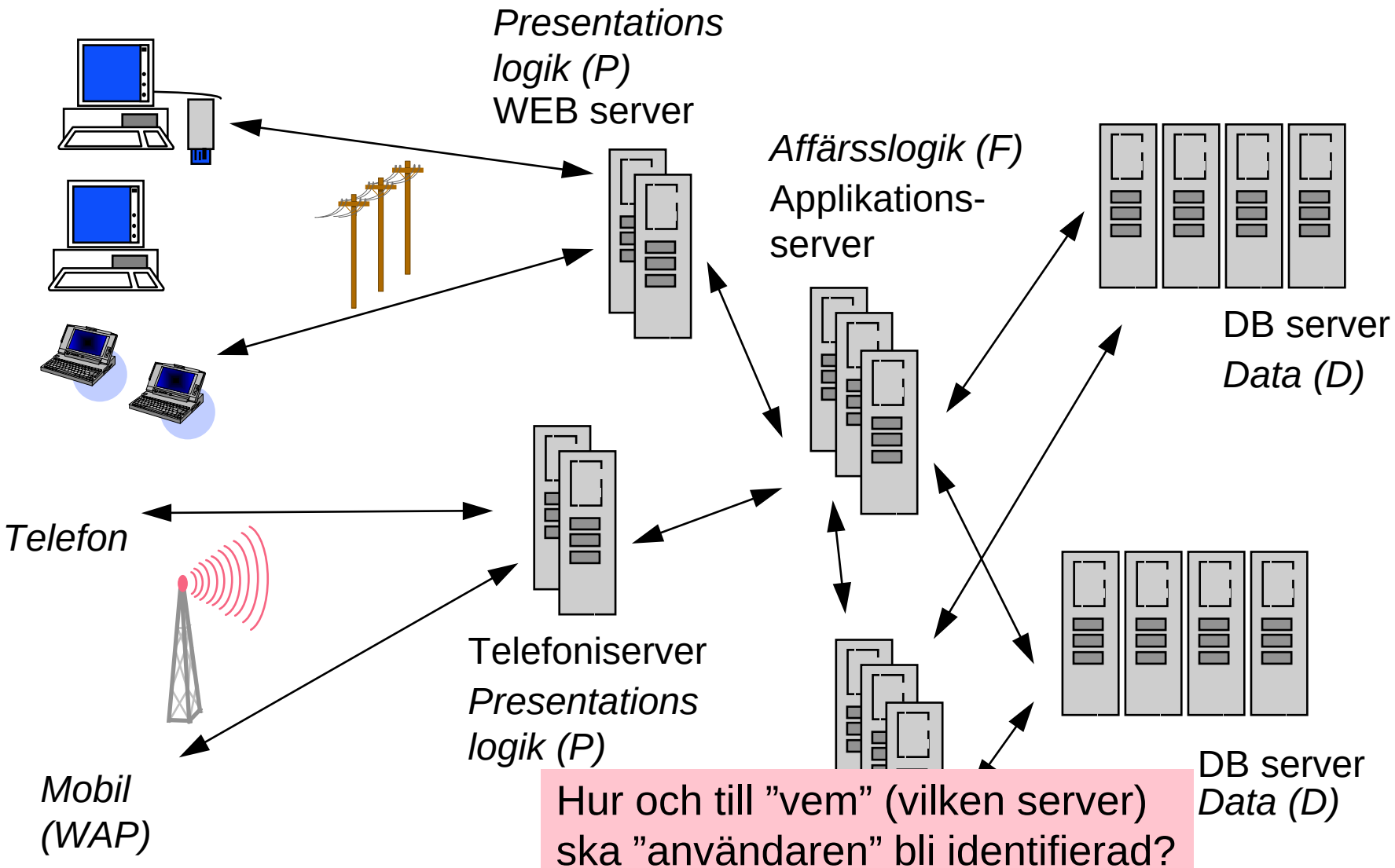


The use and dependence of IT is accelerating
=> New possibilities but also new risks

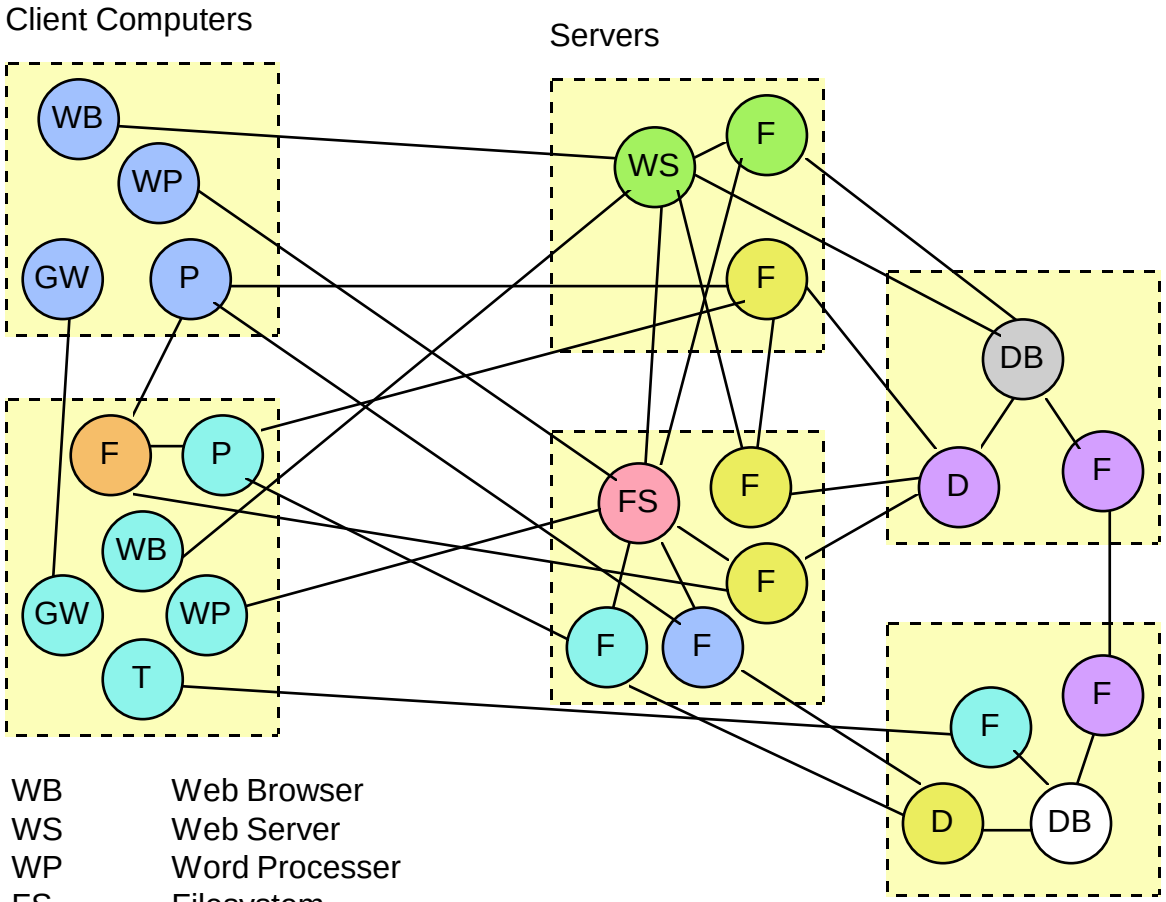
The Threat Over Time



Behov och problem - maskinvara



Behov och problem - processer



WB	Web Browser
WS	Web Server
WP	Word Processer
FS	Filesystem
P	Presentation comp.
F	Function comp.
D	Data handling comp
DB	Database process
GW	GroupWare (C-C comm)
T	Terminal Emulator

Färgerna visar att olika processer (med komponenter) körs som olika ”användare”!

Vilka komponeter kan vi ”lita på”!?

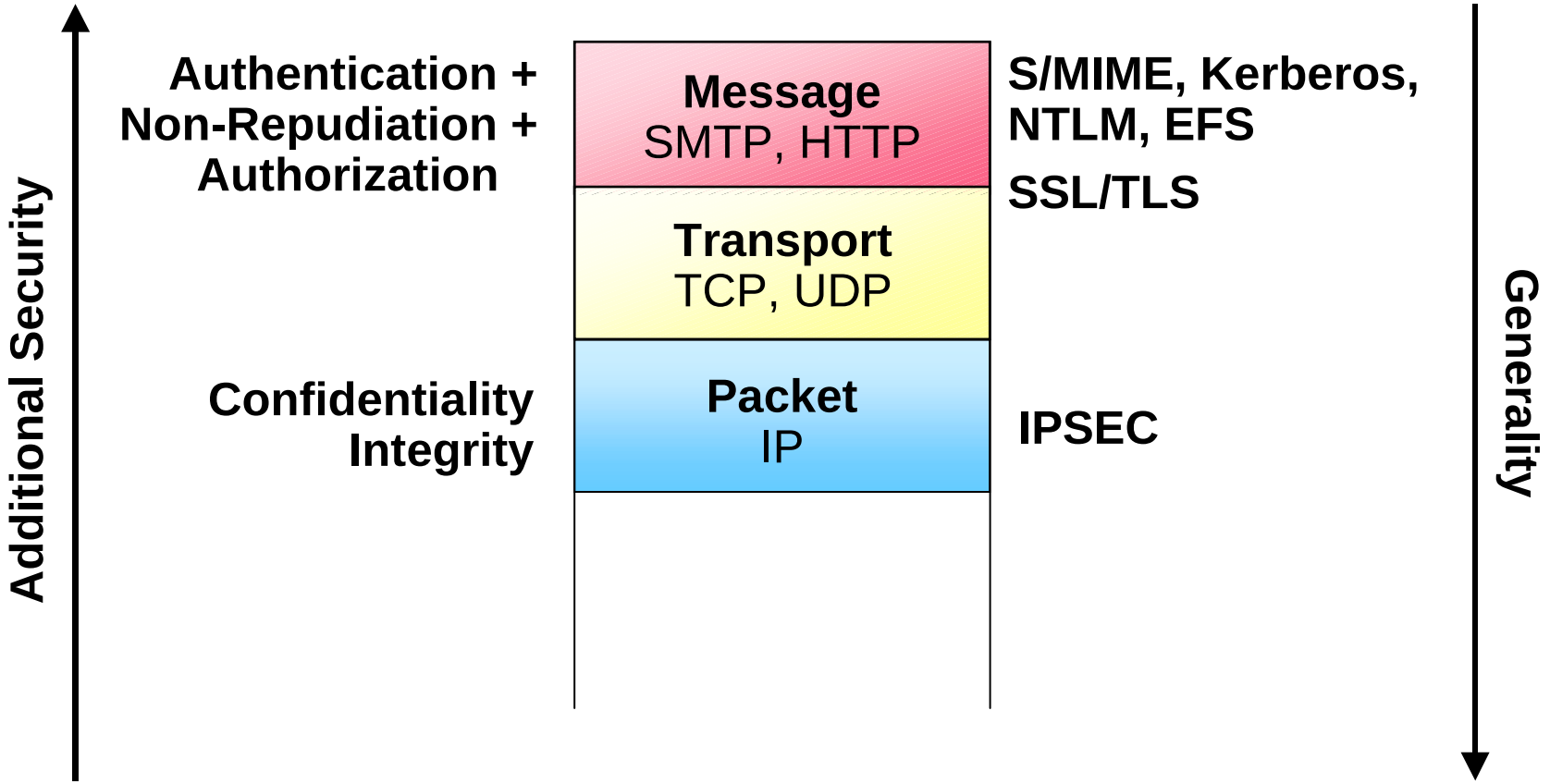
Säkerhet - begrepp

- Säkerhet (”security”) -
  - konfidentialitet, integritet, tillgänglighet
  - spårbarhet
- Systemsäkerhet (”safety”)

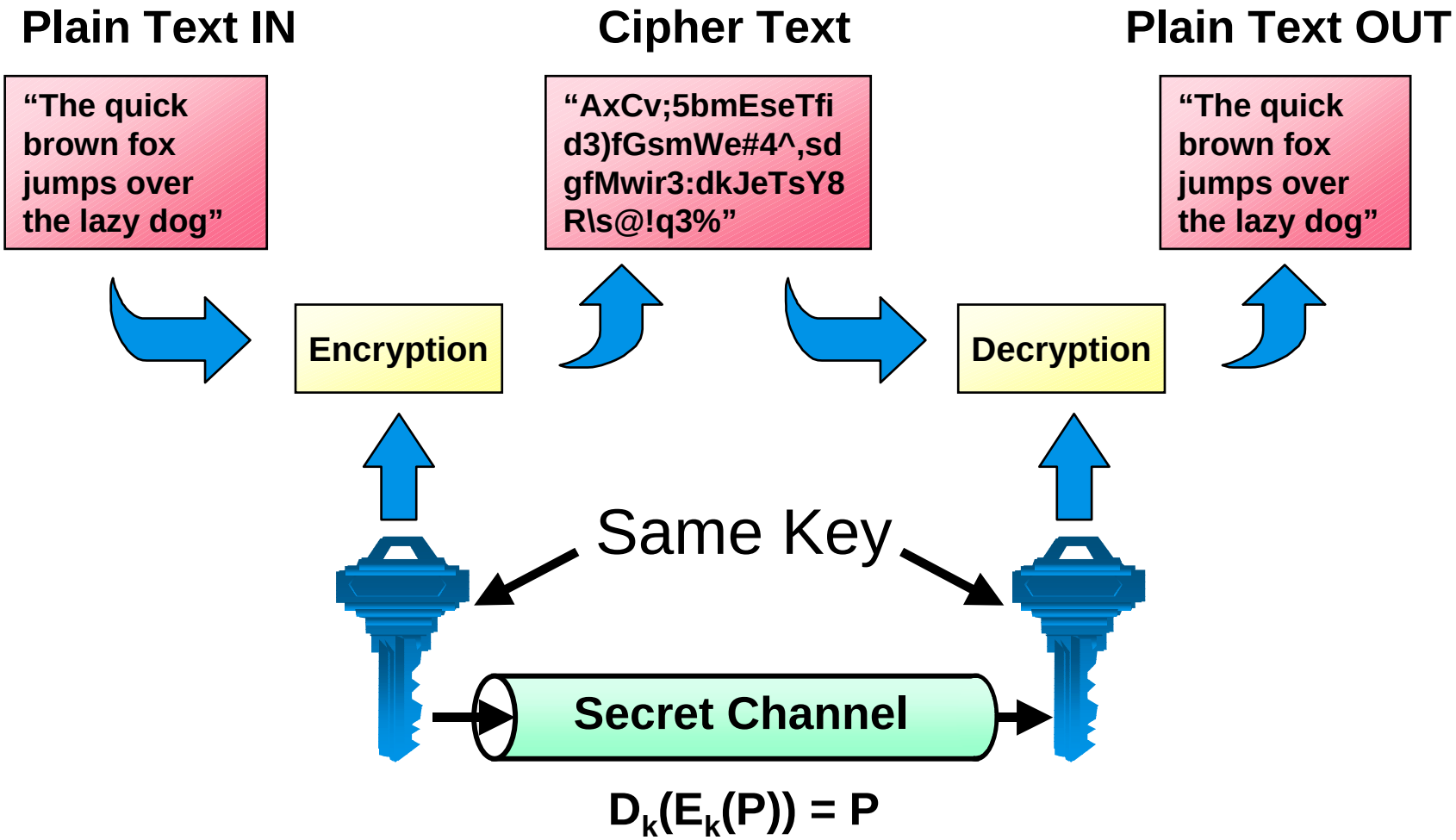
IT-säkerhet ?

- Innebär mycket arbete, men mer och mer nödvändigt ...
- Inga genvägar finns, måste konstrueras med omsorg som en del av en teknisk (samverkans-) arkitektur
- ”Marknaden” löser IT-säkerheten?
  - Trådlösa LAN - inte så säkra ”längre” !?
  - Komponentarkitekturer - MS DCOM/COM+ !? Virusvänlig design? Funktion högre prio än säkerhet?
  - Behov av starkare mekanismer - ex FM krypto
  - Logiska problem/möjligheter i säkerhetsprotokoll - autenticering, nyckeldistribution
- Måste ha känd assurans (Common Criteria), ”tilltro”
- Ny ”målgrupp” - nätverksbaserade komponenter
  - komponenter kan inte realisera säkerheten själva
  - säkerheten måste finnas i ”miljön” för komponenterna

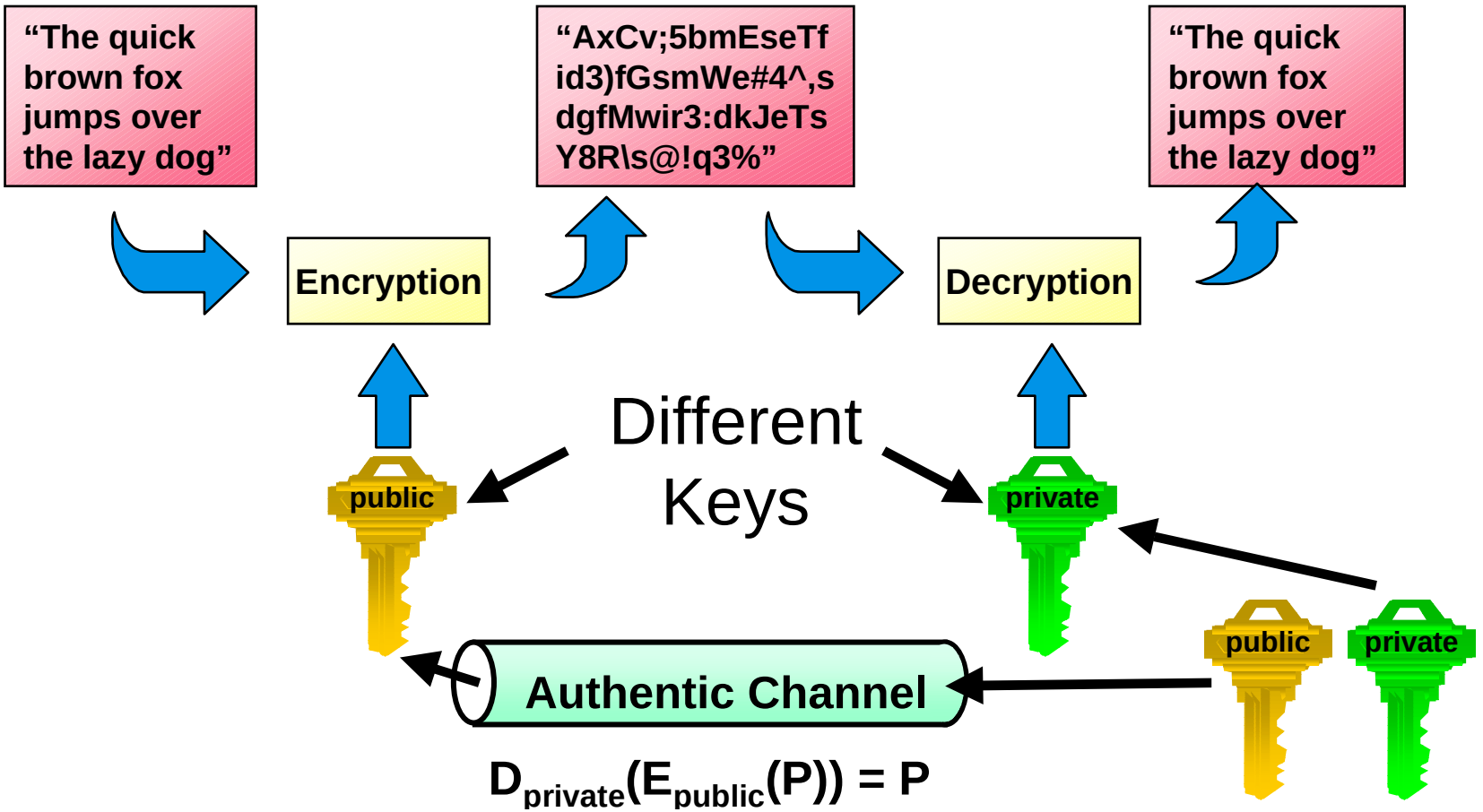
Säkerhet på olika kommunikationsnivåer



Symmetriskt krypto



Asymmetriskt krypto (”Public Key”)



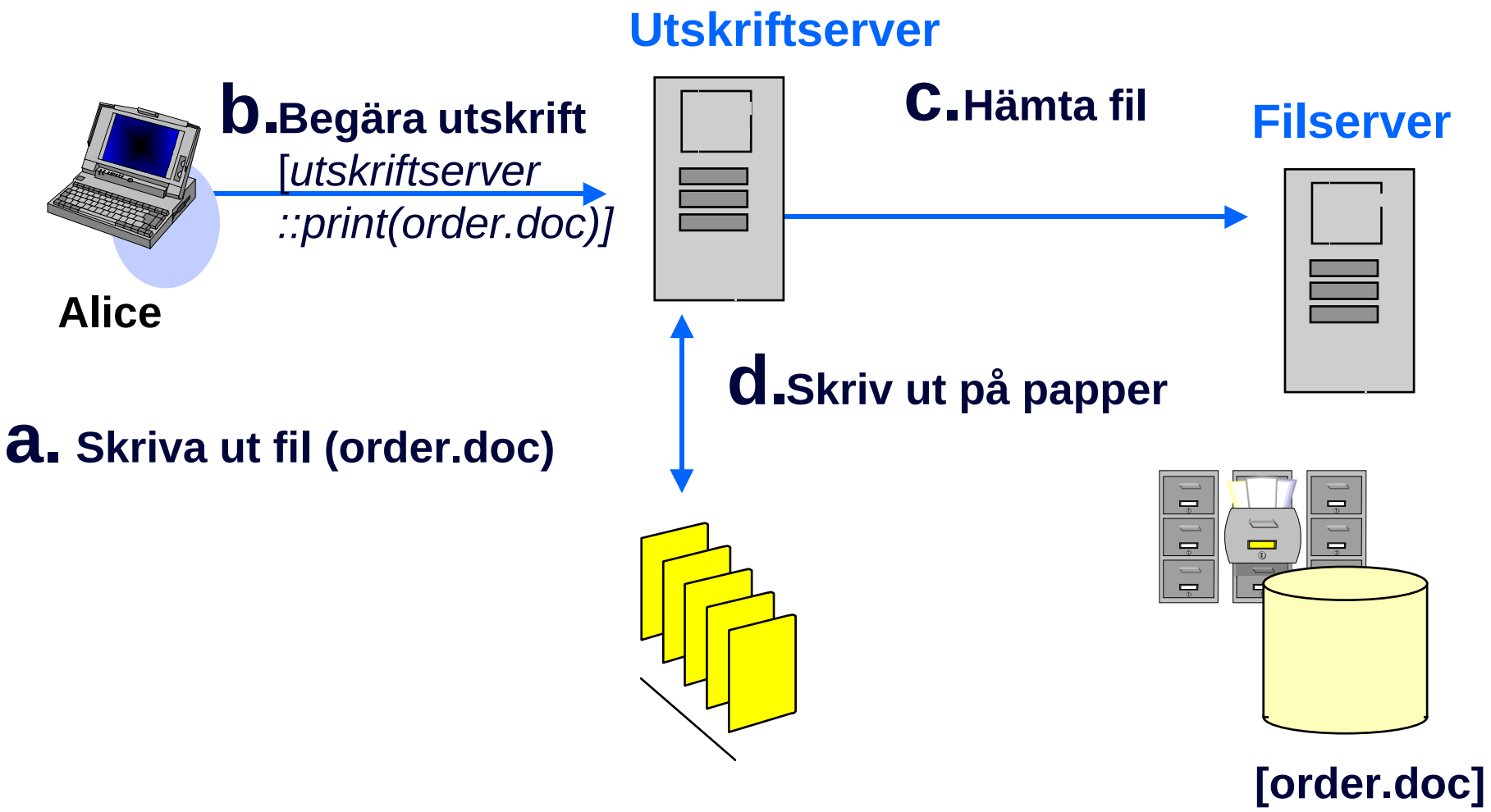
Exempel - delegering

- *Verksamhetsnivå ...*
- Behov av olika slags delegering, exempel
- ”Impersonifiering” - delegera alla mina befogenheter ...
  - firmateckning under semesterperiod
  - reservförfarande, ta befälet
  - *”låna ut” legitimation, bankomatkort, smart-card till system X, lösenord*
- ”Delegering” - delegera en delmängd av befogenheter ...
  - attesträtt endast upp till ett visst belopp
  - genomföra en specifik uppgift/order, engångsorder, stående order, ...
  - *”skriva” fullmakt, utanordna två i förening*

Exempel - delegering

- *Teknisk nivå ...*
- Behov av olika slags delegering, exempel
- Komponent (”server”) för utskrift av fil
  - användaren äger filer (som tex redigeras med Word)
  - filerna förvaras i en filserver
  - hur konstruera utskriftserver som på begäran (men endast då) kan skriva ut användarens fil?
- Exempel lösningsalternativ
  - utskriftsservern har alla behörigheter till alla filer, men kollar själv vid utskrift om ”rätt” användare försöker skriva ut
  - utskriftsservern har ”inga direkta” behörigheter -
    - impersonfiering av användaren *alt*
    - delegering av utskriftbehörighet på begäran av användaren

Ex Utskrift - Delegering

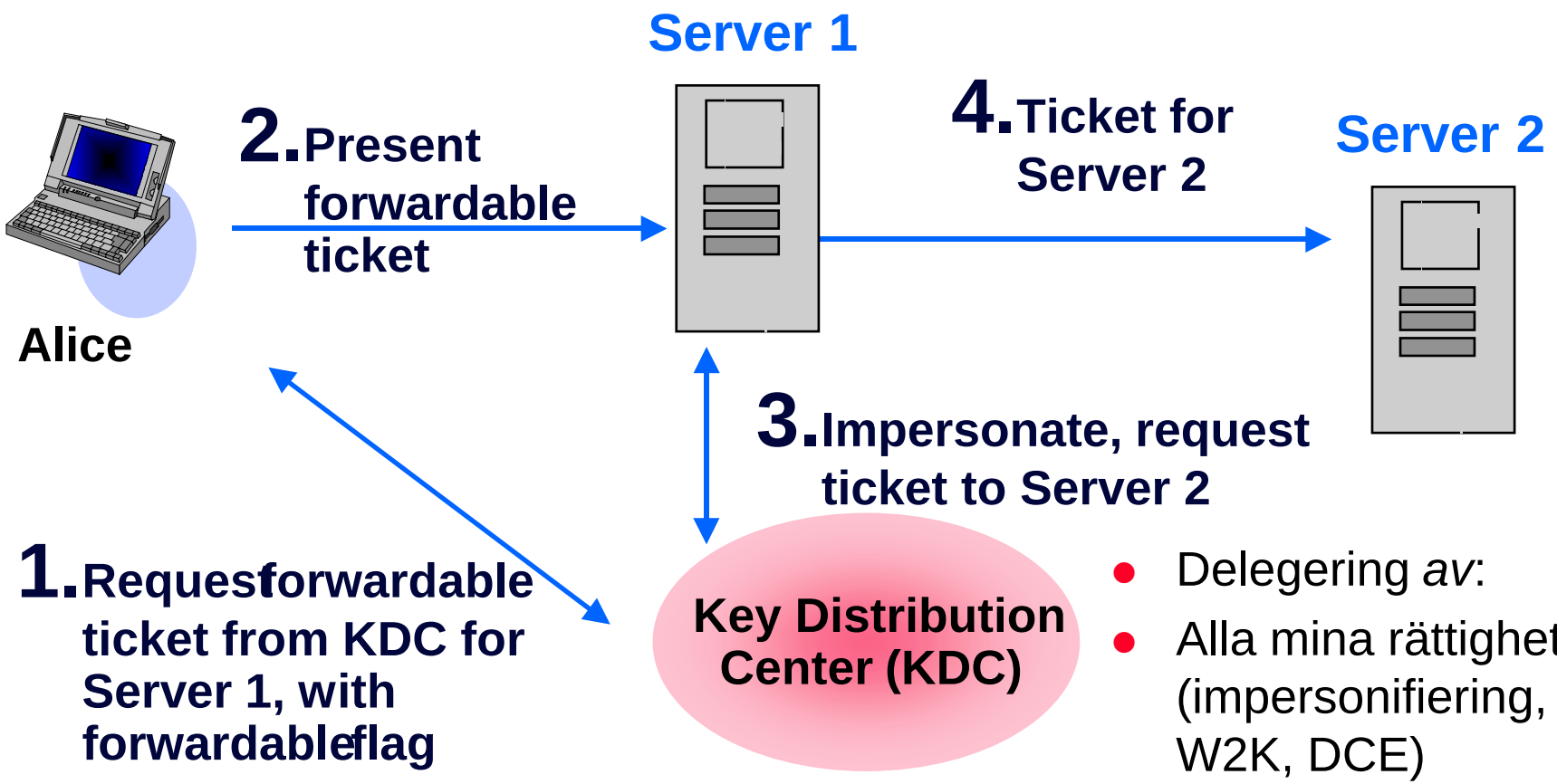


Säkerhetsmekanismer - ex hur delegera ?

- Överföring (generellt) av identitet / kreditiv i distr system ?
- Logga in/kör i serversystemet (telnet, WEB)
  - Transfer the password in: (i) cleartext, (ii) protected in a ”tunnel” (e.g. SSL) or (iii) by some challenge-response auth. protocol
  - E.g. SSL (e.g. WEB) - the client has the server public-key, protects a generated ”random” symmetric encryption key with this and sends to server for establishing a secure data exchange ”tunnel”.
- Filåtkomst (från klient, av fil på server) - överför ID (UID) plus lösen från klient till server - NFS, NTFS/SMB, ...
- Säkerhetsservern tilldelar ”kreditiv” vid login och senare ”servicebiljett” till begärd resurs - DCE Security, KerberosV+, Windows2000 - protokoll för delegering
  - The ”credentials” contain user, groups etc. certified by the security server at initial login

Kerberos

Kerberos V+ - Delegering: impersonifiering



- Delegering *av*:
- Alla mina rättigheter (impersonifiering, ex W2K, DCE)
- Begränsade rättigheter, ex utskrift av min fil om jag begärt det (DCE)

Kerberos implementationer

- CyberSafe (www.cybersafe.com) (i ”TrustBroker”)
- MIT http://web.mit.edu/kerberos/www/index.html
- DCE Kerberos (NT, UNIX, OS/390 mfl, olika lev IBM, Entegrity, Compaq
- Computer Associates (fd Platinum (OpenVision))
- Sun Kerberos (Solaris 7+)
- Microsoft (W2K, DCE-RPC -> MS RPC (DCom))
- Heimdal (KTH)

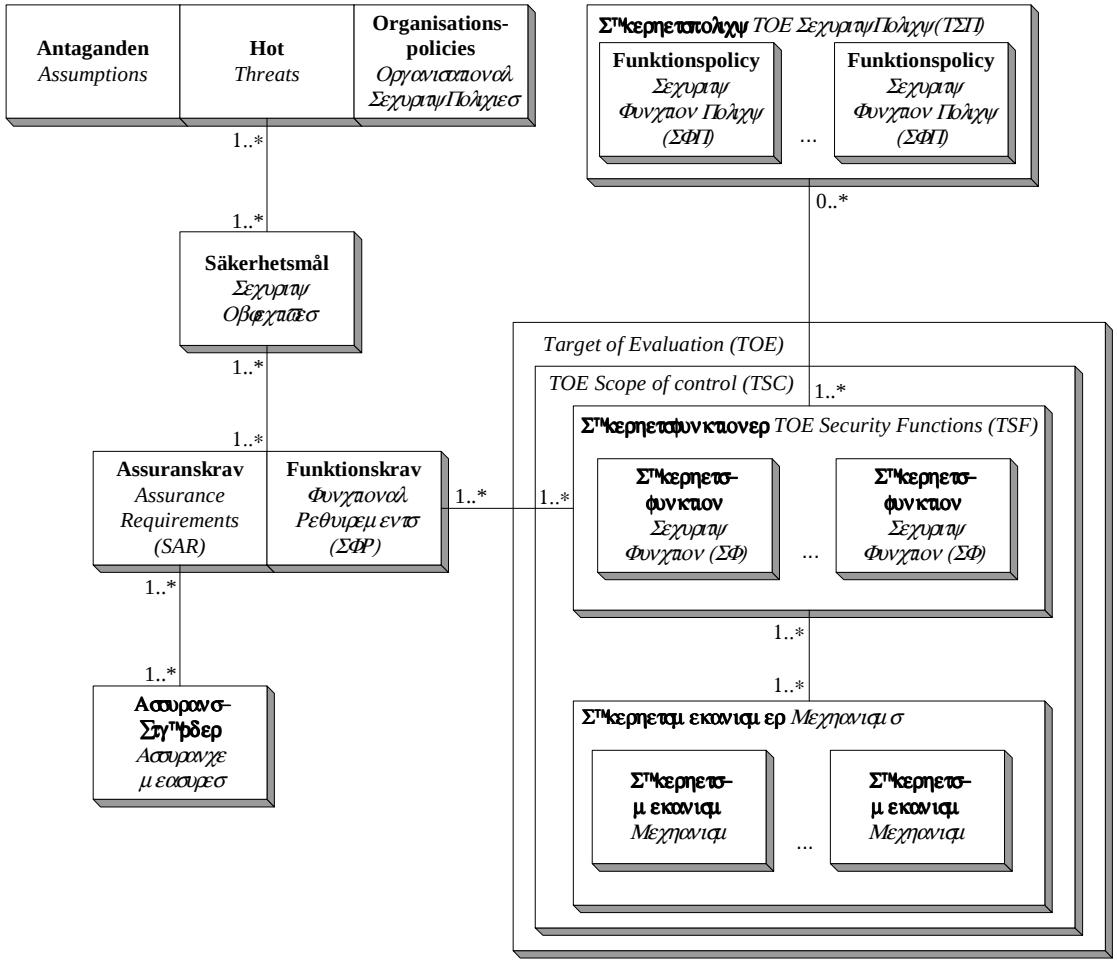
Summering

- Hot- (sårbarhets-) analys - vad är **hoten** och dessa möjliga konsekvenser, vem är **attackeraren**, vilka **resurser/förmågor** har attackeraren?
- Vilket slags säkerhets (-**funktioner**) behövs - och lokaliserade var i den tekniska arkitekturen
- **Mekanismer**? *(i)* Initial autentisering av användaren och ”trovärdiga” (trusted) servrar ***vs*** *(ii)* KerberosV+ arkitektur (serverprogram måste också autenticera sig, delegering//inpersionifering)
- Tilltro till lösningar/**produkter - Assuransnivå**
- Standard för **evaluering** (funktionalitet vs assurans)
  - Internat. Common Criteria (e.g. funktionsuppsättningar/EAL-3)
  - Äldre: Europa ITSEC (e.g. F-C2/E3), US TCSEC (e.g. CS, B1/B2)

Extra - Säkerhet i nätverksförsvaret ?

- Säkerheten måste vara integrerad i den tekniska infrastrukturen (i den tekniska arkitekturen) ...
- Process för assurans - Common Criteria, EAL-4 ::
- Säkdok: Protection Profile resp Security Target
- Antaganden, Hot, Organisationspolicys -
- Säkerhetsmål
- Assuranskrav -
  - Assuransåtgärder
- Funktionskrav -
  - Säkerhetspolicy -> Funktionspolicy
  - Säkerhetsfunktioner -
    - Säkerhetsmekanismer -
- Jämför systemsäkerhet, kvalitetssäkring

Security Target (ST) enligt Common Criteria (CC)



Säkerhetskrav

- Säkerhetspolicy; säkerhetsmålsättning ; Security policy;
  - *formellt fastställd uppsättning mål som beskriver övergripande säkerhetskrav på informationshanteringen inom en organisation eller verksamhet.*
  - Exempel:
    - ”Gällande lagar och förordningar för sekretessbelagd information skall hållas”

Säkerhetsfunktioner

- Säkerhetsfunktion; Security function
  - *specifik teknisk egenskap hos ett system genom vilken det, tillsammans med övriga säkerhetsfunktioner, upprätthåller säkerheten. Begreppet kan även preciseras enligt: urskiljbar del av ett system som utför en säkerhetstjänst. Åtkomstkontroll, autenticering och loggning är exempel på säkerhetsfunktioner*
  - Exempel (GTP) innehåller funktioner för:
    - Identifiering och autenticering,
    - Åtkomstkontroll
    - Integritet (riktighet)
    - Konfidentialitet
    - Datautväxling
    - Spårbarhet (loggning)
    - Tillgänglighet
    - Säkerhetsadministration

Säkerhetsmekanismer

- Säkerhetsmekanism; Security mechanism;
  - *teknik som används vid realisering av en säkerhetsfunktion eller del av denna*
  - Exempel:
  - GTP innehåller stark autenticering med användarid/lösenord alt TAK+PIN. Det är en driftkonfigurationsfråga om TAK (FM Aktiva Kort och kortterminal) skall användas! GTP 2.1.3 stöder båda varianterna av identifiering. Konfigureras efter driftkrav. Vilka mekanismer som konfigureras är transparent för alla verksamhetsfunktioner.

  - GTP 2.1.3 innehåller informationskydd med DES-kryptering. GTP 2.2 innehåller stöd för textskydd med FM kryptokort KK631. Konfigureras efter driftkrav. Vilka mekanismer som konfigureras är transparent för alla verksamhetsfunktioner.
  - Motsvarande gäller övriga säkerhetsmekanismer som hantering av certifikat, lösenordshantering, nyckelhantering etc.

Assurans och säkerhetsgranskning

- Assurans; Assurance
  - *tilltro till att ett systems eller en produkts säkerhetsfunktioner, med hänsyn till korrekthet och ändamålsenlighet, uppfyller fastställda specificerade säkerhetskrav. Tilltron knyts till en bedömning av systemets eller produktens möjlighet att motverka bedömda typer av angrepp. Jämför evaluering, assuransnivå, hotanalys.*

- Evaluering; Evaluation
  - *säkerhetsteknisk utvärdering av ett system eller en systemkomponent gentemot specificerade säkerhetskrav samt bedömning av mekanismstyrkan hos ingående säkerhetsmekanismer. Förekommer framför allt i samband med krav rörande evalueringsobjektets säkerhetsegenskaper (funktionellt, ur assurans- och uppföljningssynpunkt etc). Evaluering syftar till att visa att säkerheten uppfyller kraven på korrekthet och ändamålsenlighet.*

Certifiering och ackreditering

- Certifiering; certification
  - *formellt fastställande av resultatet från en evaluering. Fastställandet baseras på resultatet från en genomförd evaluering varvid ingår granskning att evalueringsarbetet genomförts med erforderlig noggrannhet och med utnyttjande av godkänd metodik samt att resultatet påvisat att evalueringsobjektet svarar mot någon viss kravnivå enligt givna evalueringskriterier. Certifiering utgör ofta ett väsentligt underlag vid ackreditering av system.*

- Ackreditering av system; drifttillstånd; site accreditation
  - *formellt beslut att ett visst informationssystem kan godkännas för drift med användning av en beskriven uppsättning säkerhetsfunktioner. Ackreditering av system är ett formellt driftgodkännade, ibland med stöd från resultatet av genomförd evaluering av hela eller delar av systemet, vilket tillsammans med andra överväganden dokumenterar att vederbörliga säkerhetshänsyn tagits.*

