ROMAB
ROBERT MALMGREN AB

Säker informationshantering

Robert Malmgren

rom@romab.com

+46-708330378

Electronic copies of the slides available at
http://www.romab.com/documents.html

ROMAB
ROBERT MALMGREN AB

Säker informationshantering

….finns det?

Robert Malmgren
rom@romab.com
+46-708330378

Electronic copies of the slides available at
http://www.romab.com/documents.html

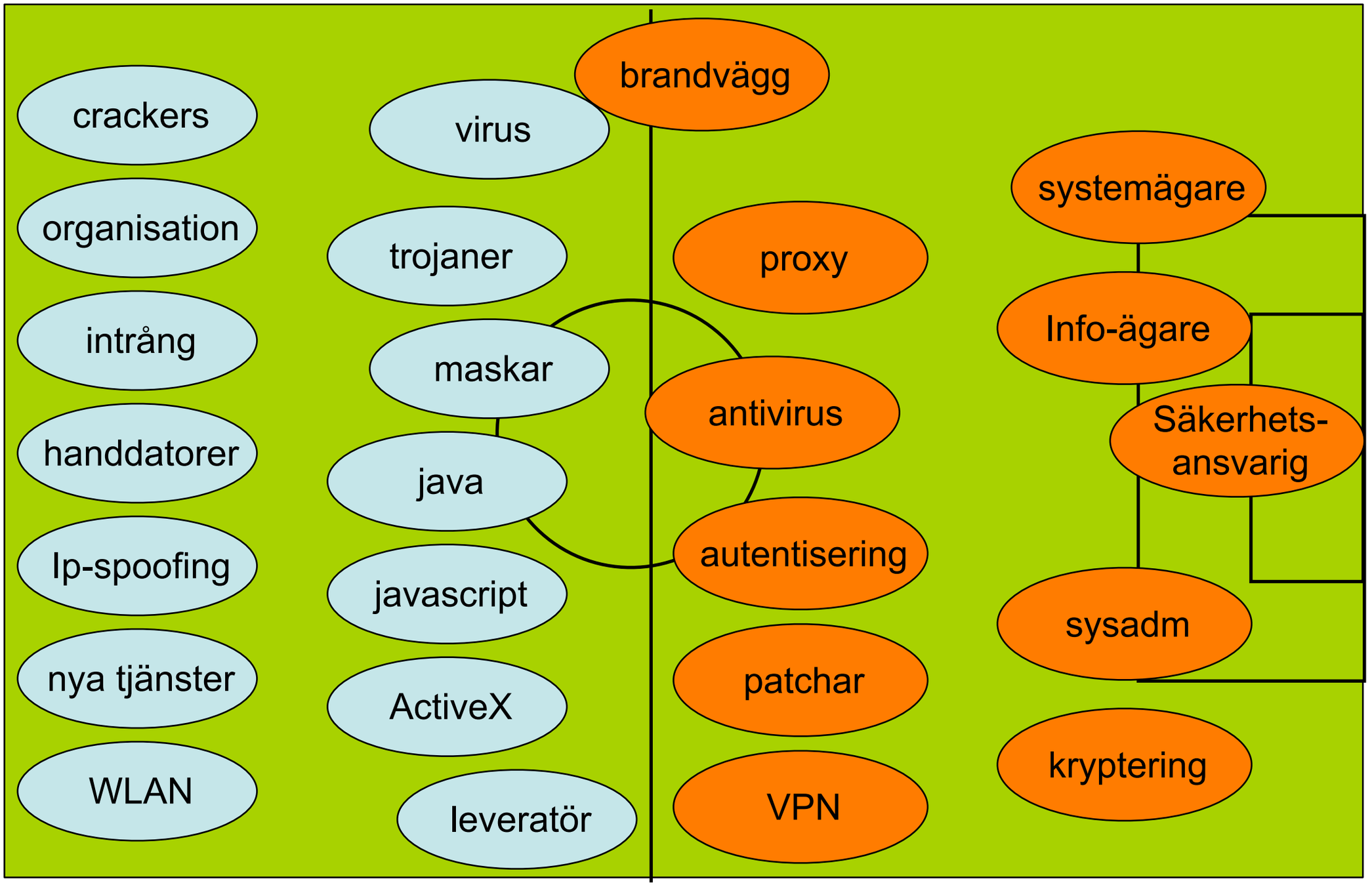
ROMAB
ROBERT MALMGREN AB

Kort definition

- *Information* i detta sammanhang är såväl
  - Dokument
  - transaktioner
  - annan överförd data, tex styrkommandon, datainsamlig

ROMAB
ROBERT MALMGREN AB

Säkerhetsmatchen



ROMAB
ROBERT MALMGREN AB

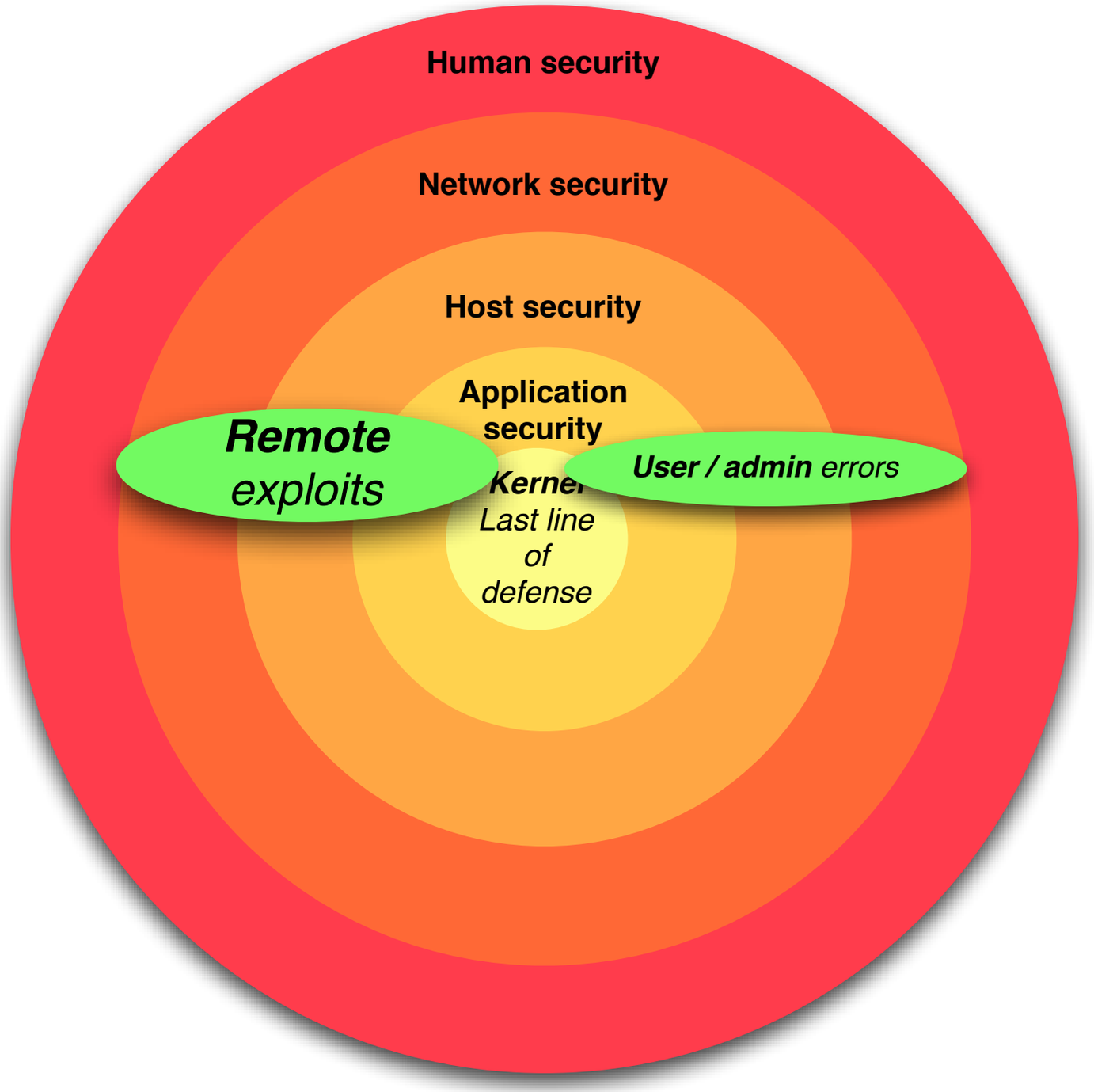
Var inträffar säkerhetsproblem?

ROMAB
ROBERT MALMGREN AB

Var inträffar säkerhetsproblem?

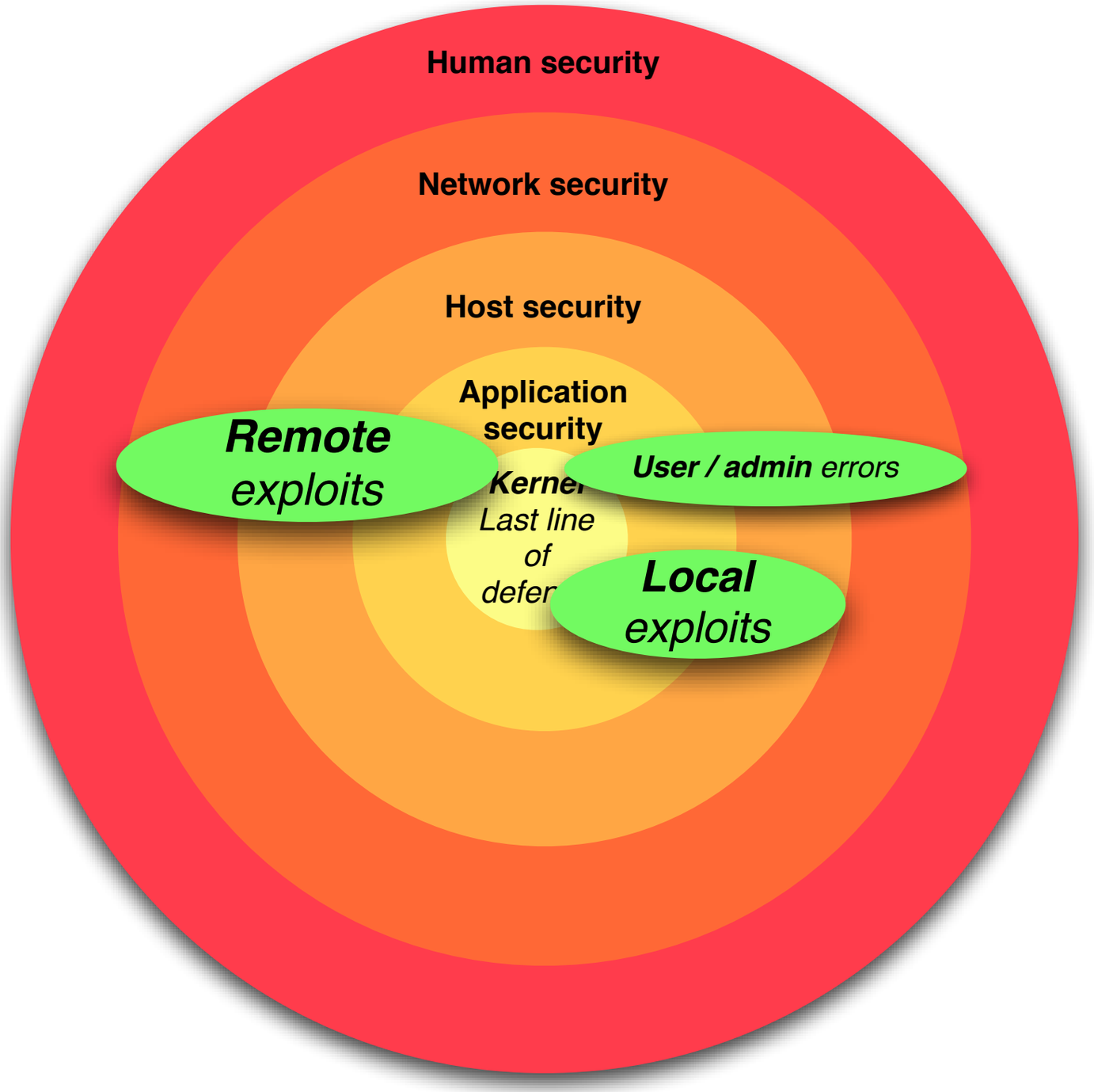
ROMAB
ROBERT MALMGREN AB

Var inträffar säkerhetsproblem?



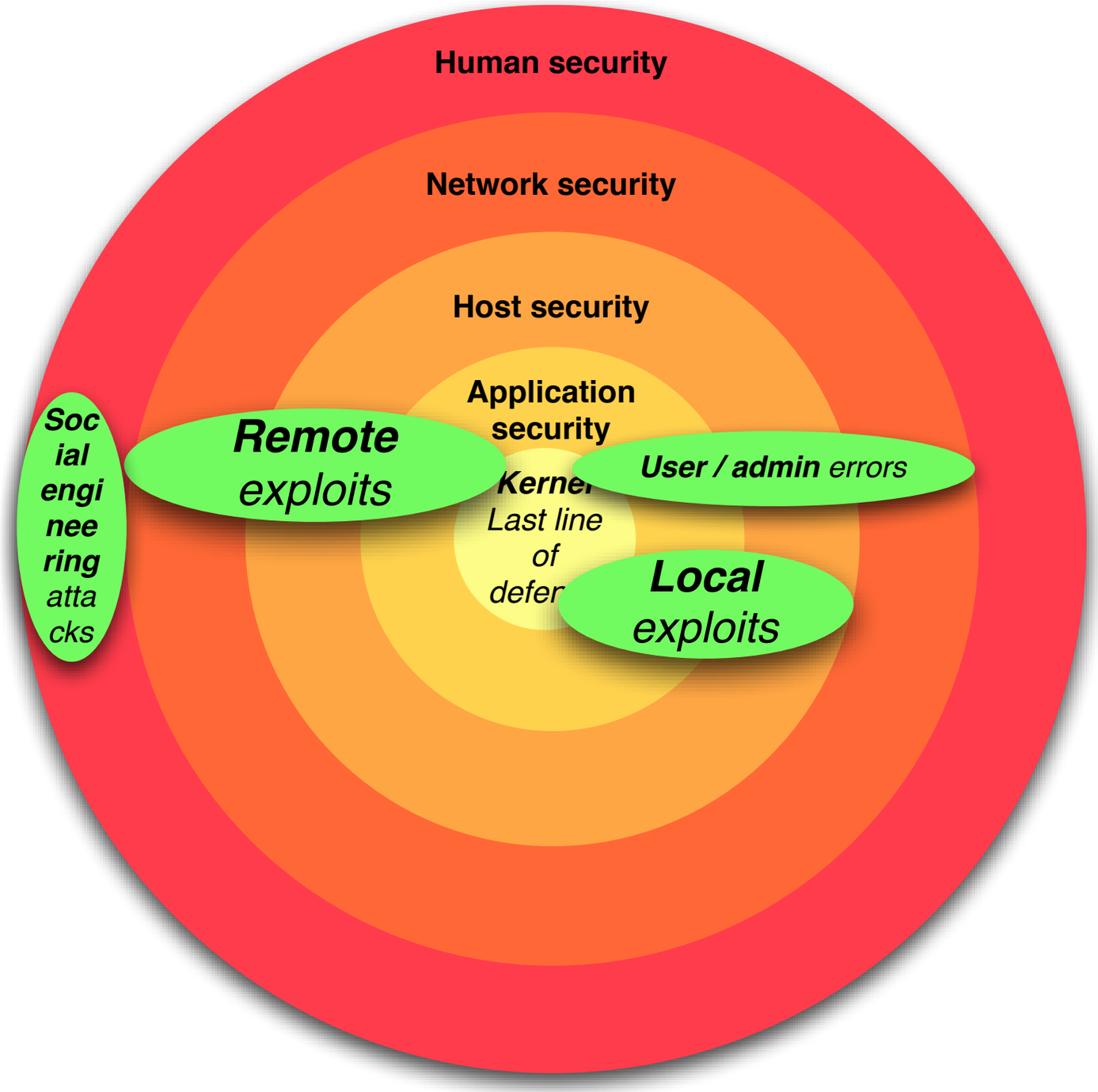
ROMAB
ROBERT MALMGREN AB

Var inträffar säkerhetsproblem?



ROMAB
ROBERT MALMGREN AB

Var inträffar säkerhetsproblem?



ROMAB
ROBERT MALMGREN AB

Utvecklingen på hotsidan

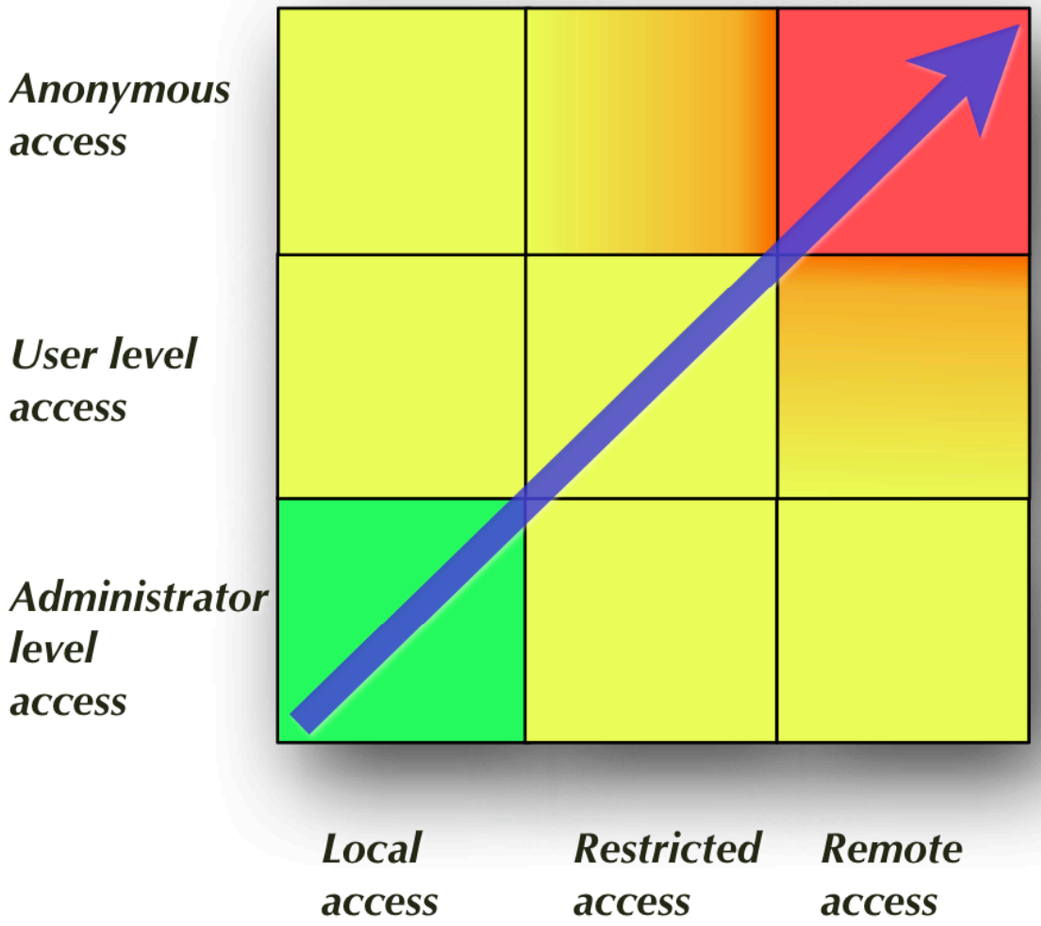
Remote Exploits in application

Remote Exploits in sub system -
database, XML parser, add-on stack

Remote Exploits
in operating system

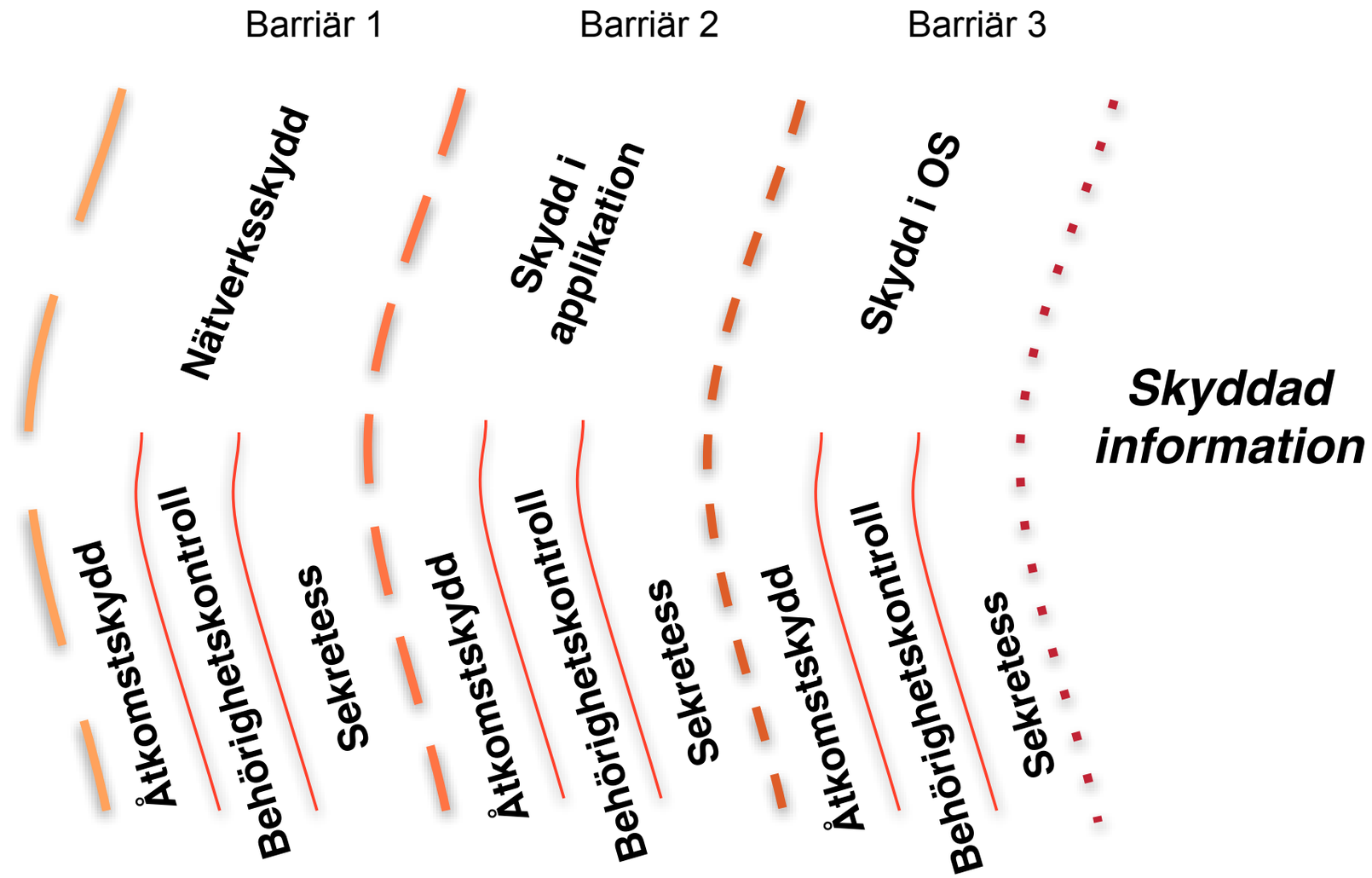
Configuration misuses -
Standard passwords, open services

Attacks on network level -
sniffing, replay, data manipulation



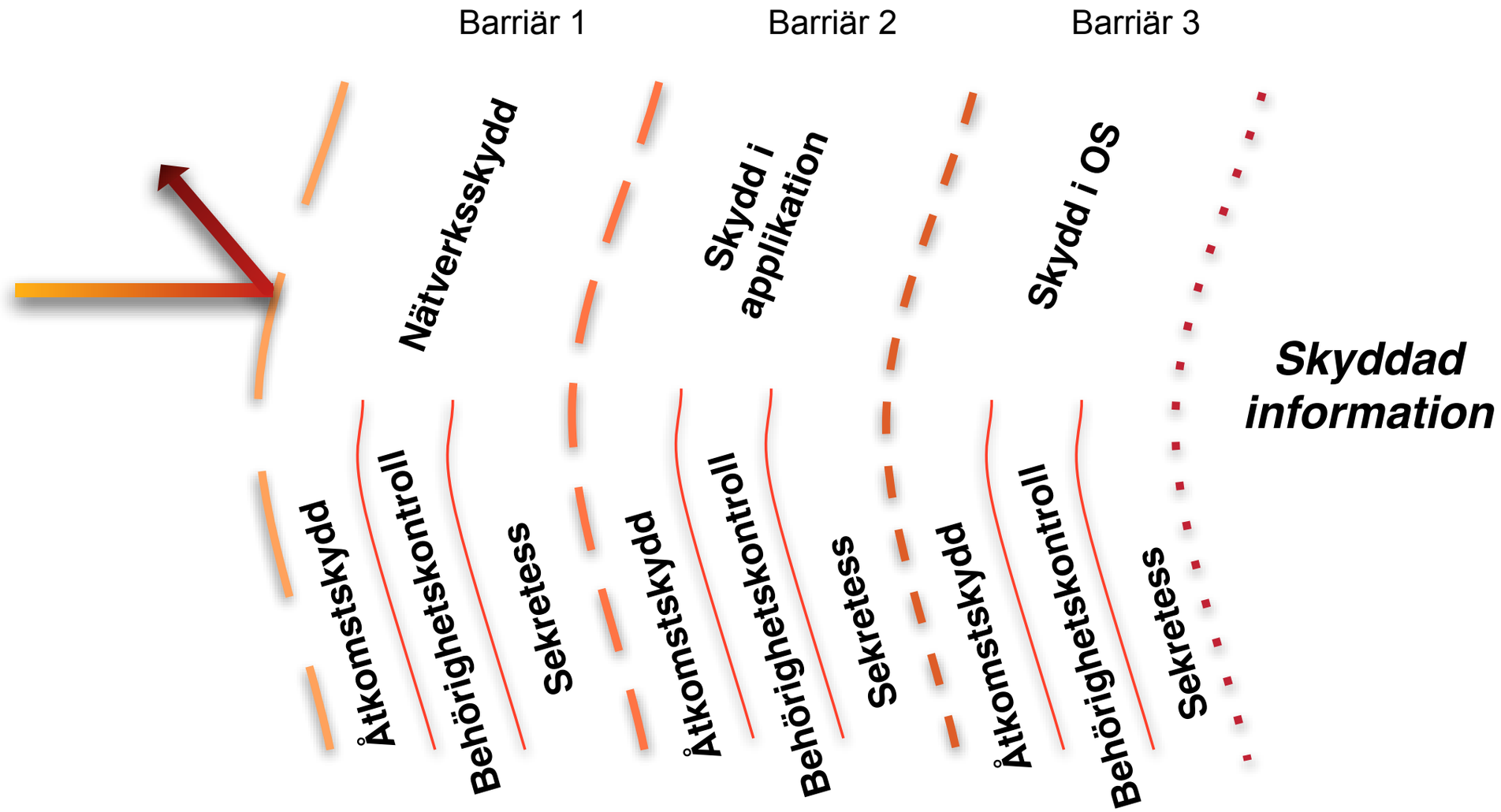
ROMAB
ROBERT MALMGREN AB

Grundläggande koncept
Försvar i djupled



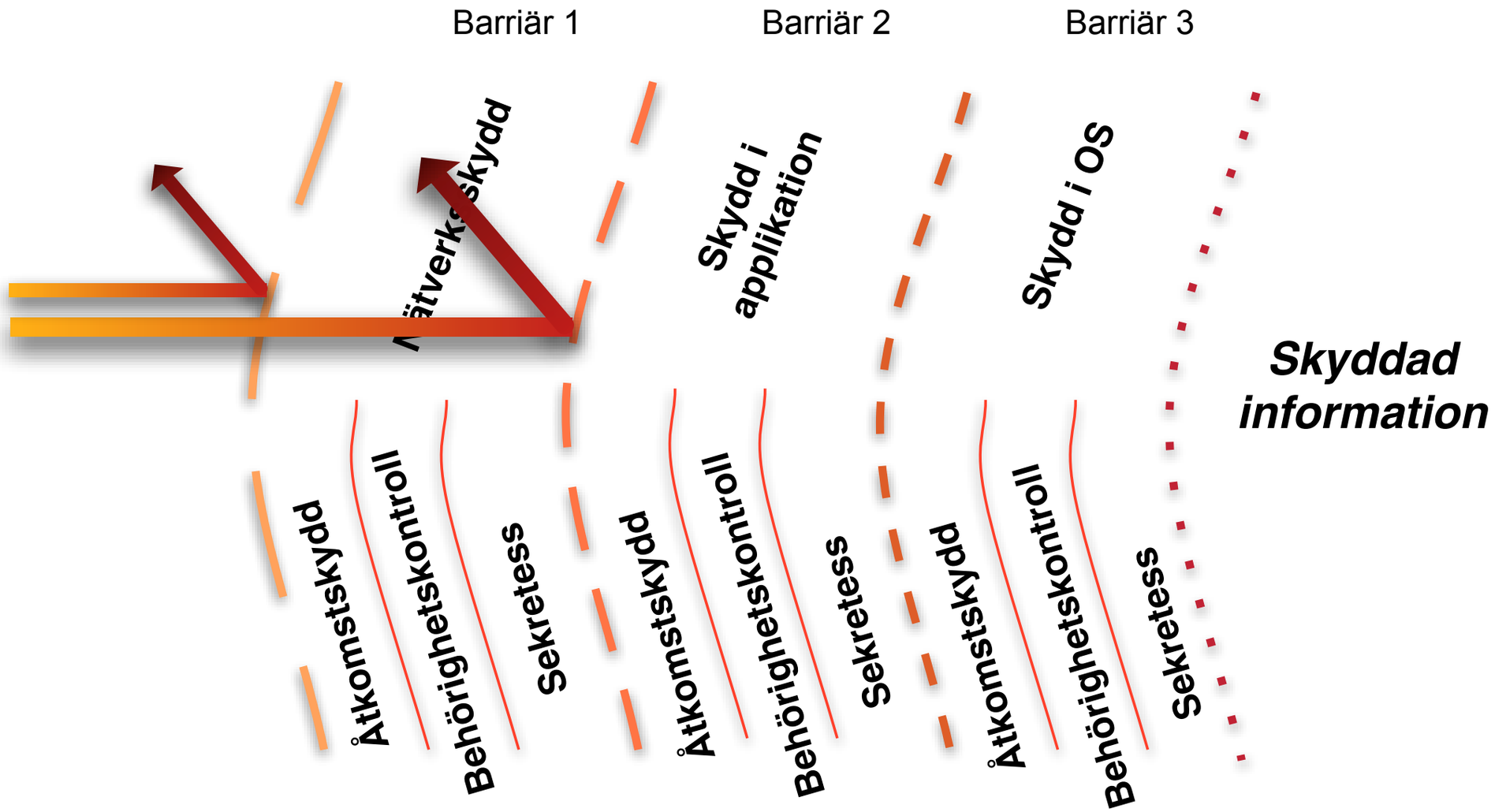
ROMAB
ROBERT MALMGREN AB

Grundläggande koncept
Försvar i djupled



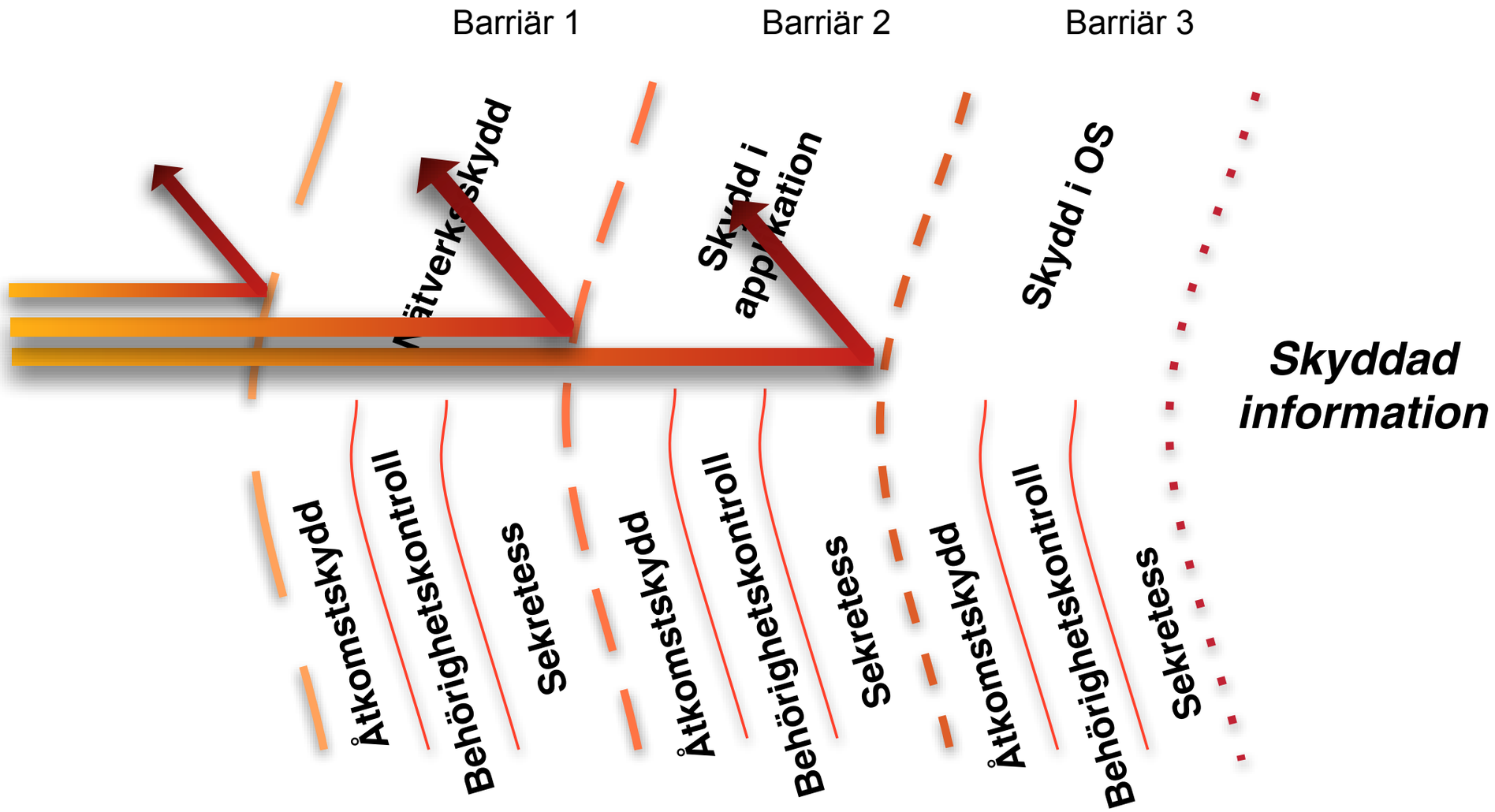
ROMAB
ROBERT MALMGREN AB

Grundläggande koncept
Försvar i djupled



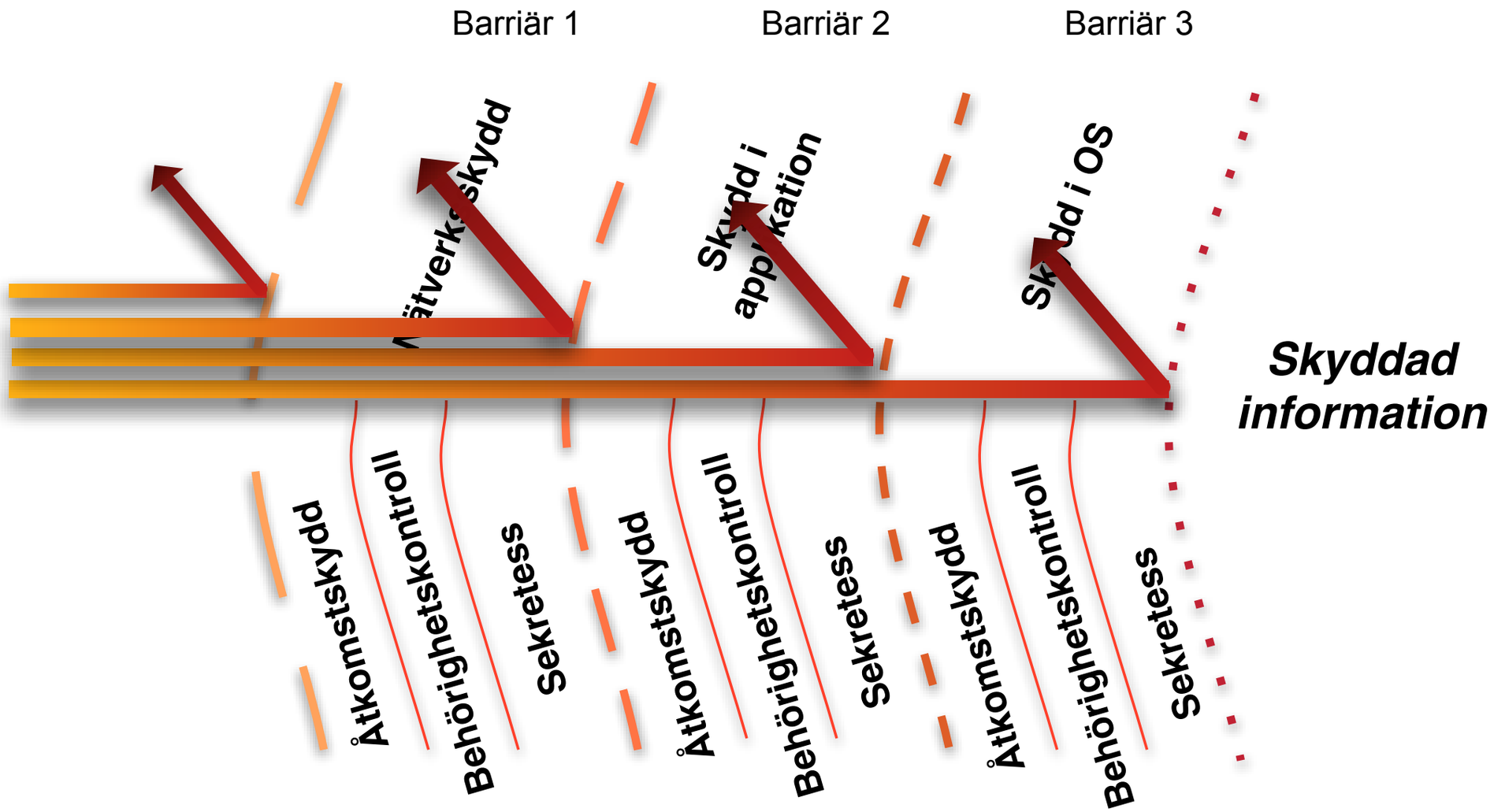
ROMAB
ROBERT MALMGREN AB

Grundläggande koncept
Försvar i djupled



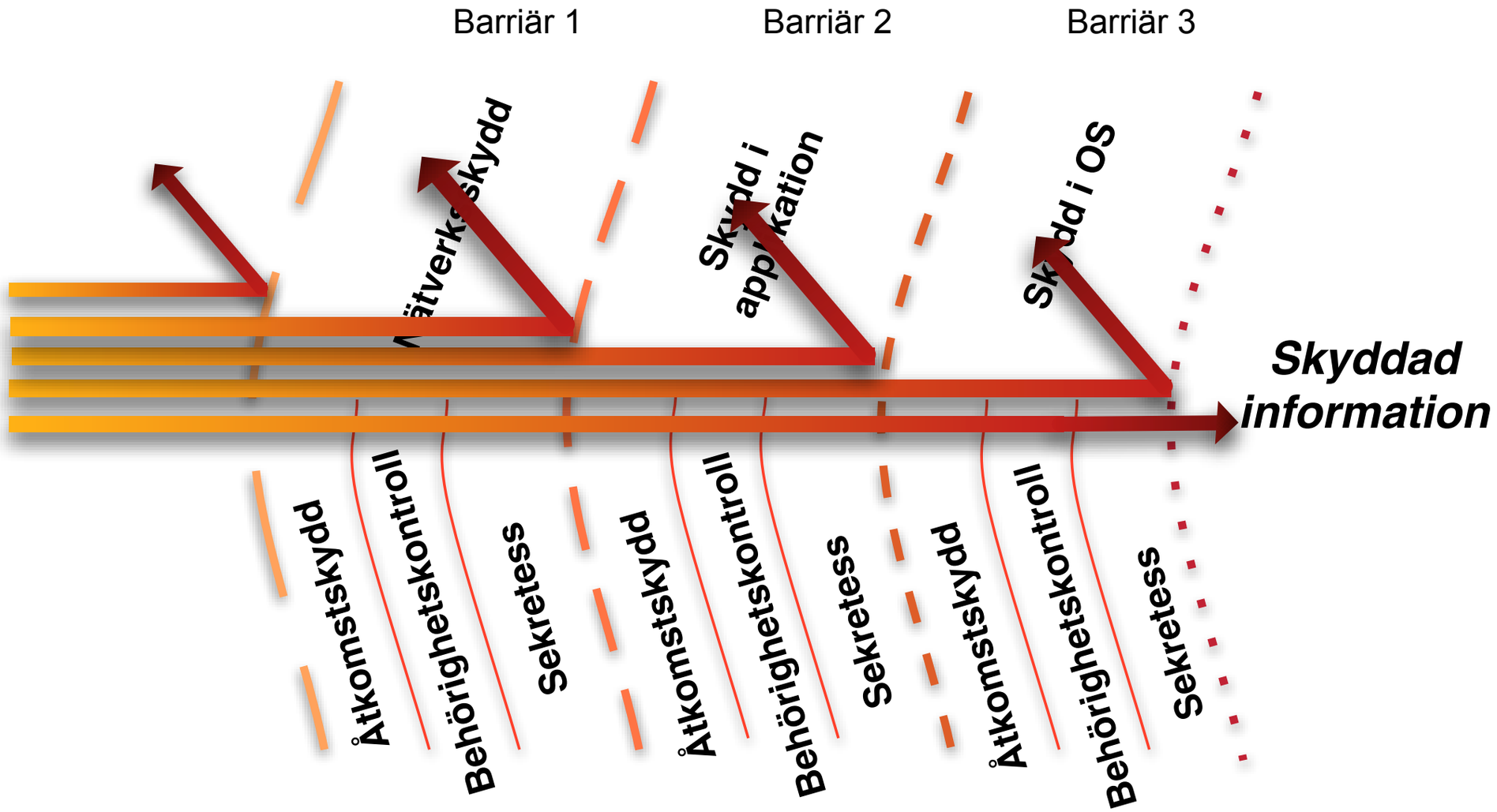
ROMAB
ROBERT MALMGREN AB

Grundläggande koncept
Försvar i djupled



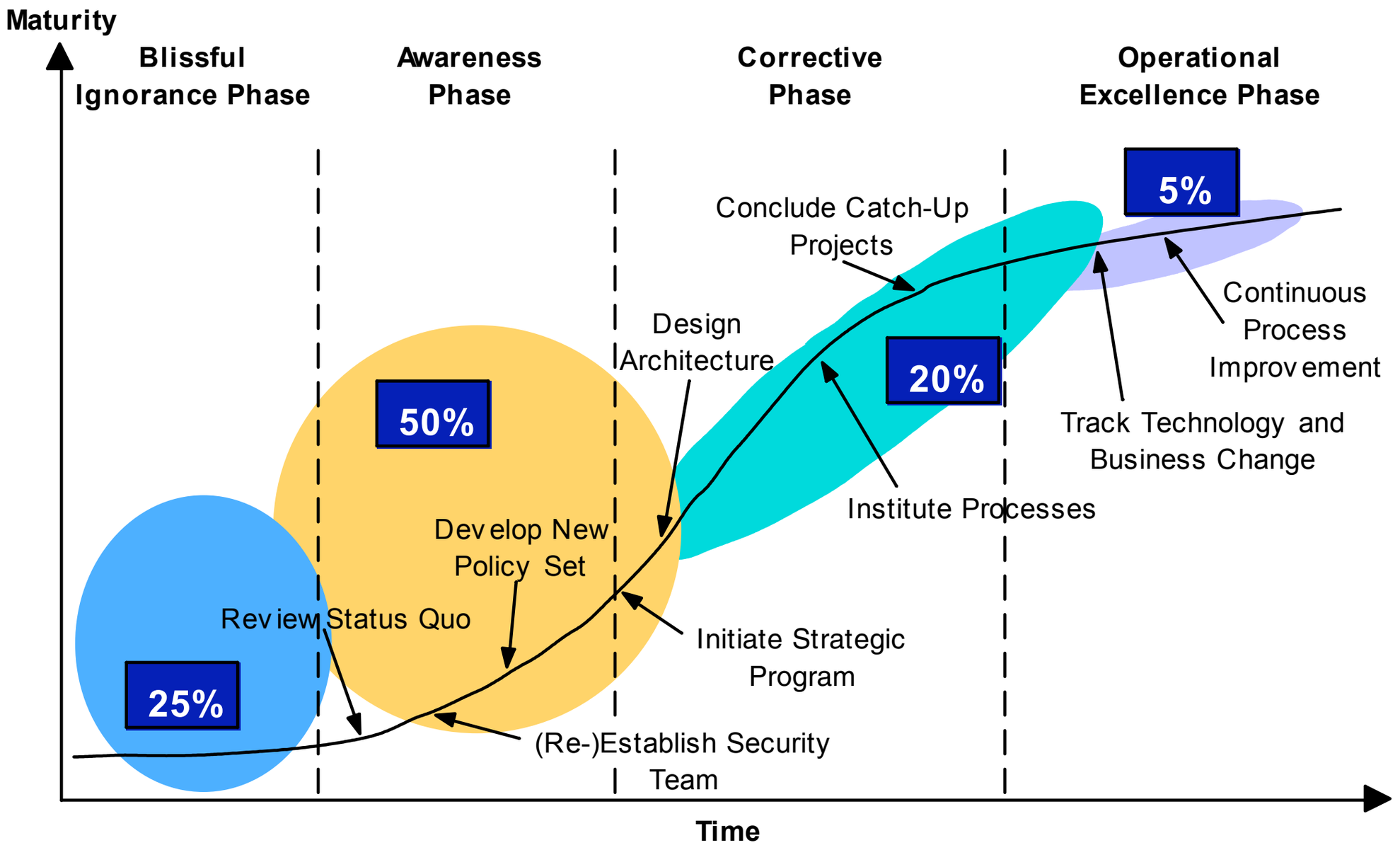
ROMAB
ROBERT MALMGREN AB

Grundläggande koncept
Försvar i djupled



ROMAB
ROBERT MALMGREN AB

Utvecklingskurvan för säkerhet inom en organisation

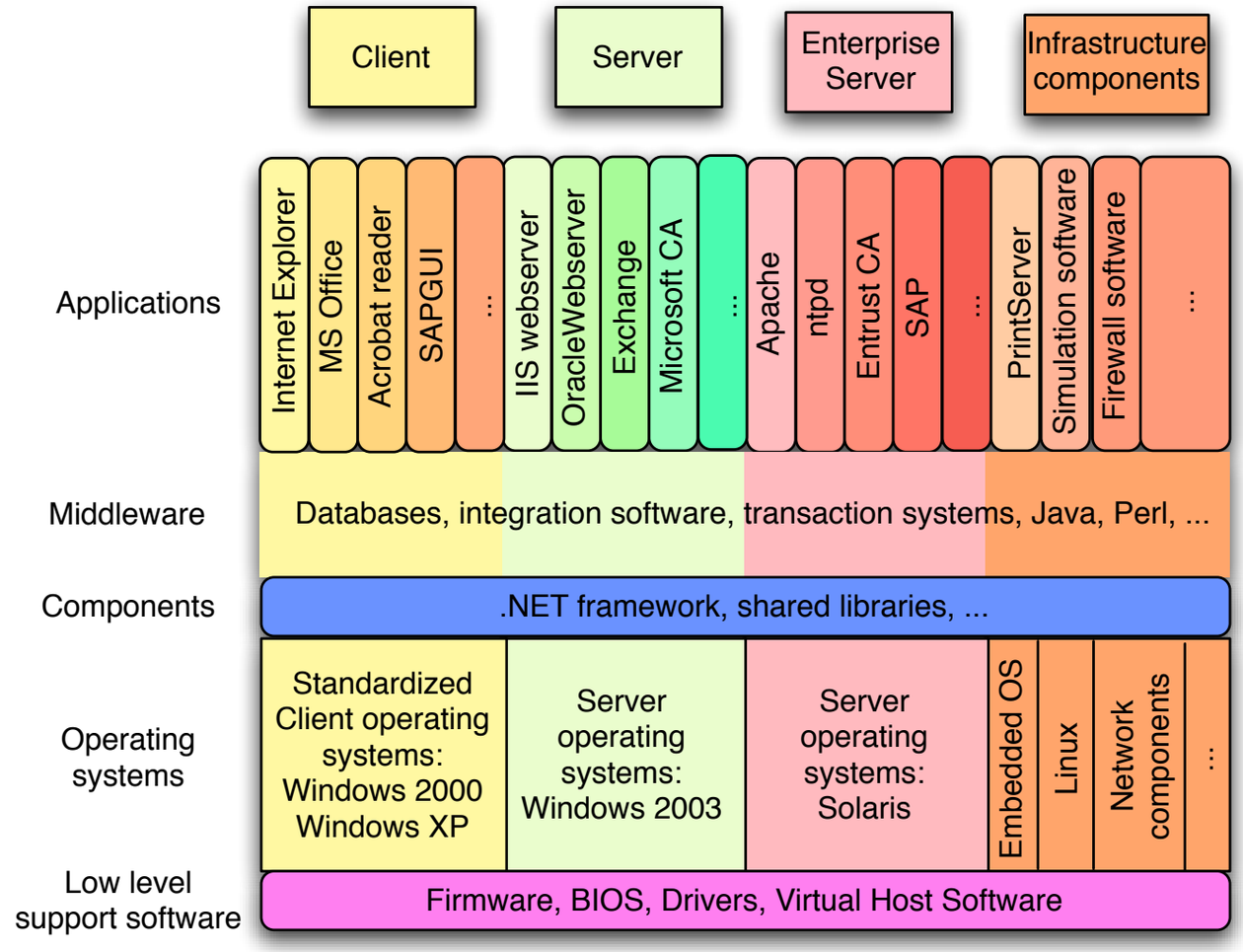


Note: The population distributions represent typical large G2000-type organizations.

Source: Gartner (July 2006)

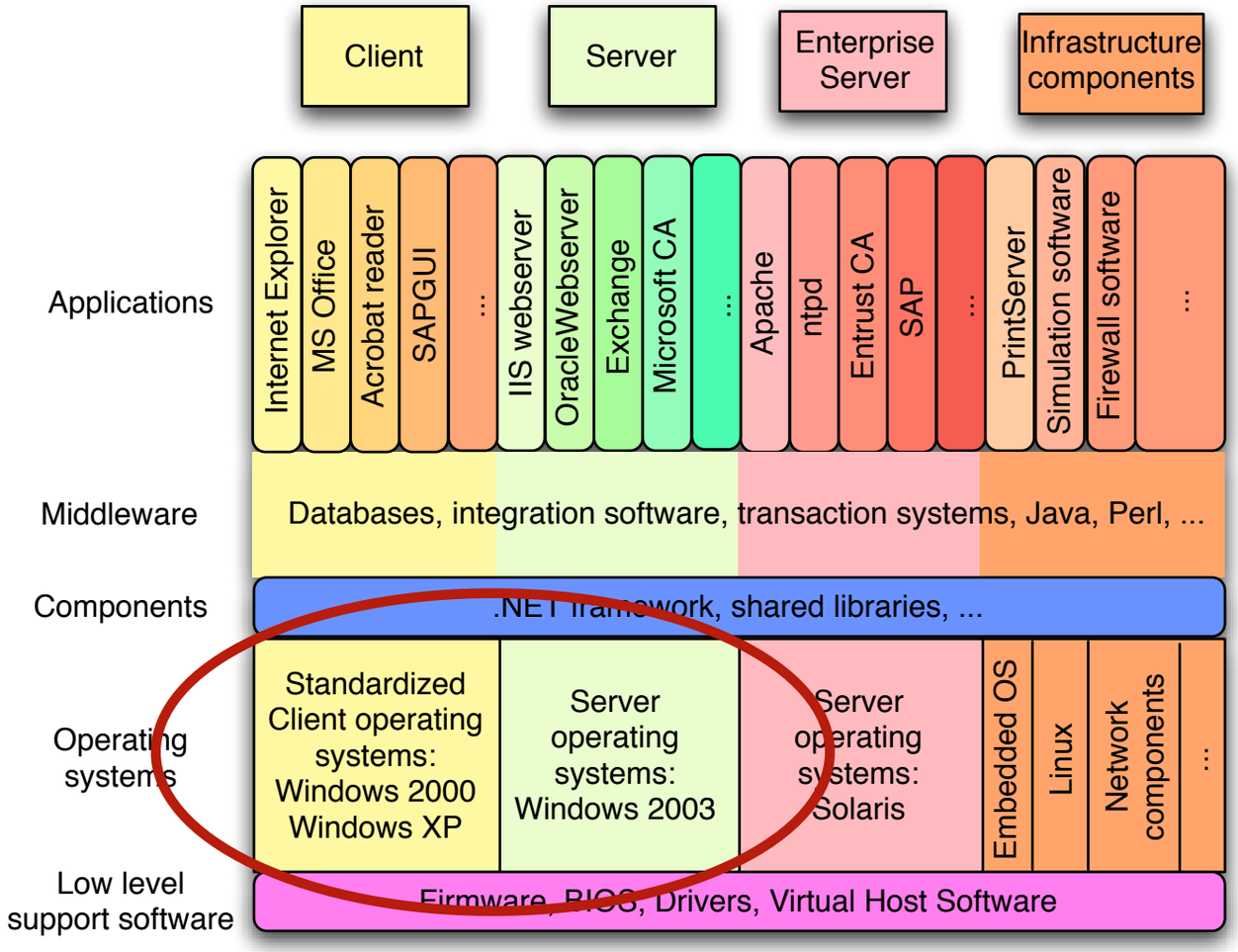
ROMAB
ROBERT MALMGREN AB

Designprincipen för lagerindelning



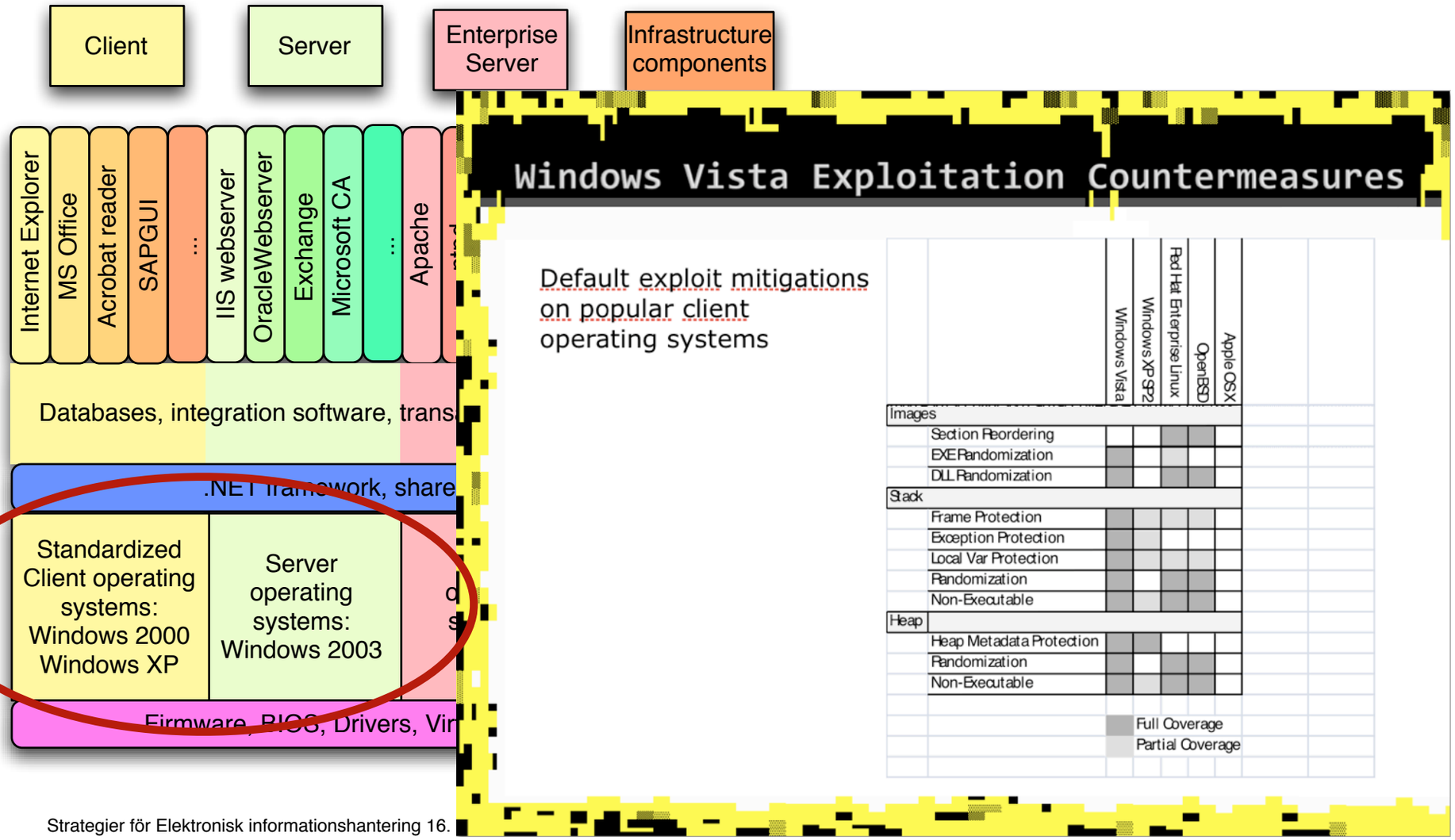
ROMAB
ROBERT MALMGREN AB

Designprincipen för lagerindelning



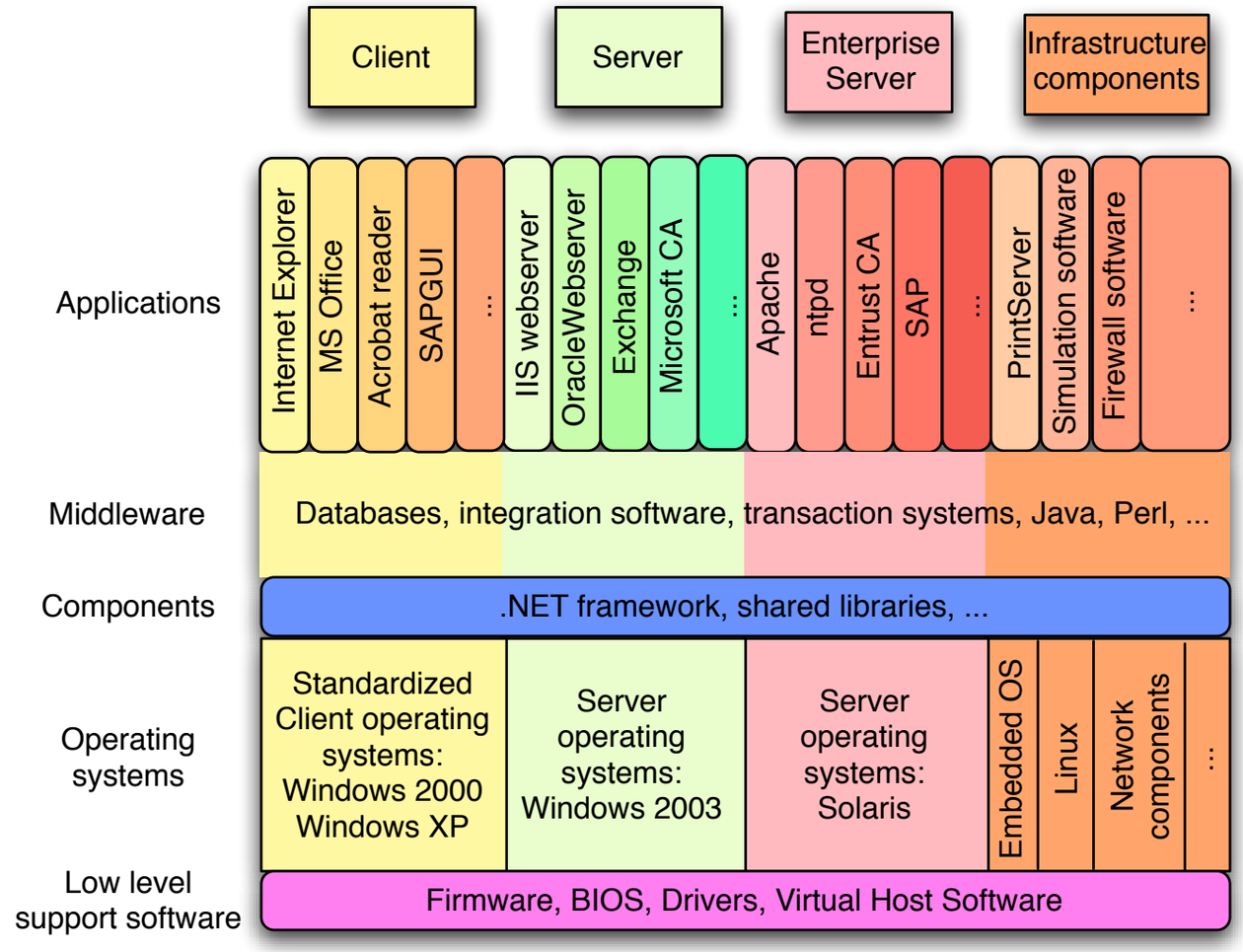
ROMAB
ROBERT MALMGREN AB

Designprincipen för lagerindelning



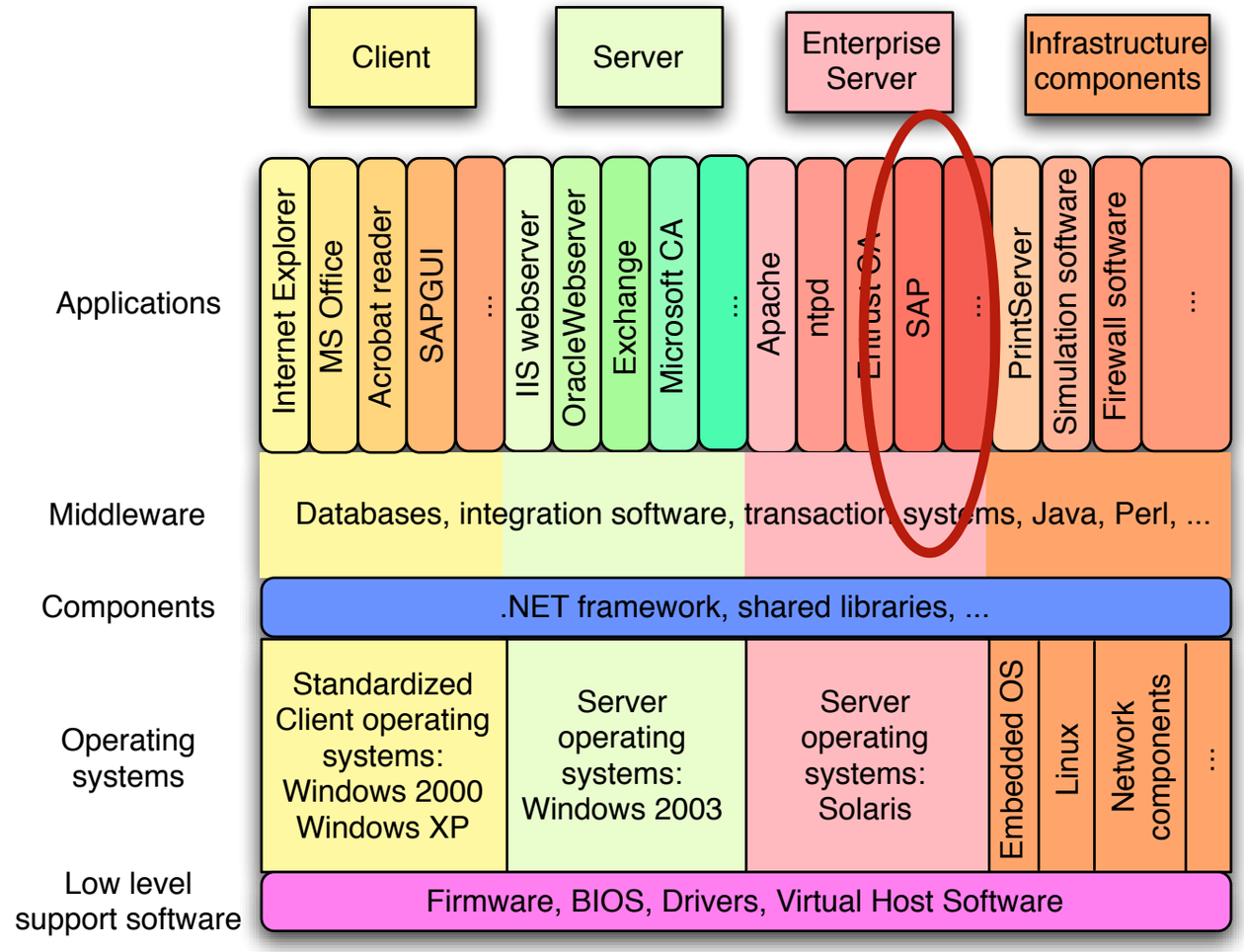
ROMAB
ROBERT MALMGREN AB

Designprincipen för lagerindelning



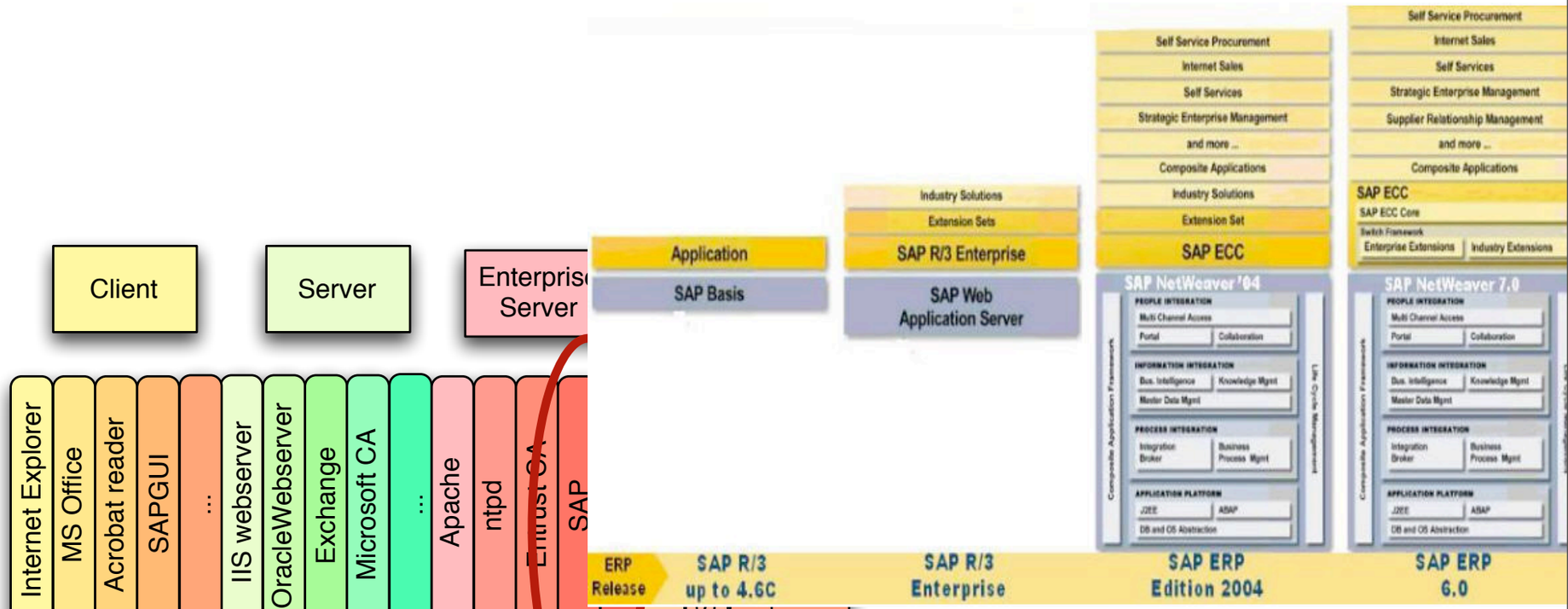
ROMAB
ROBERT MALMGREN AB

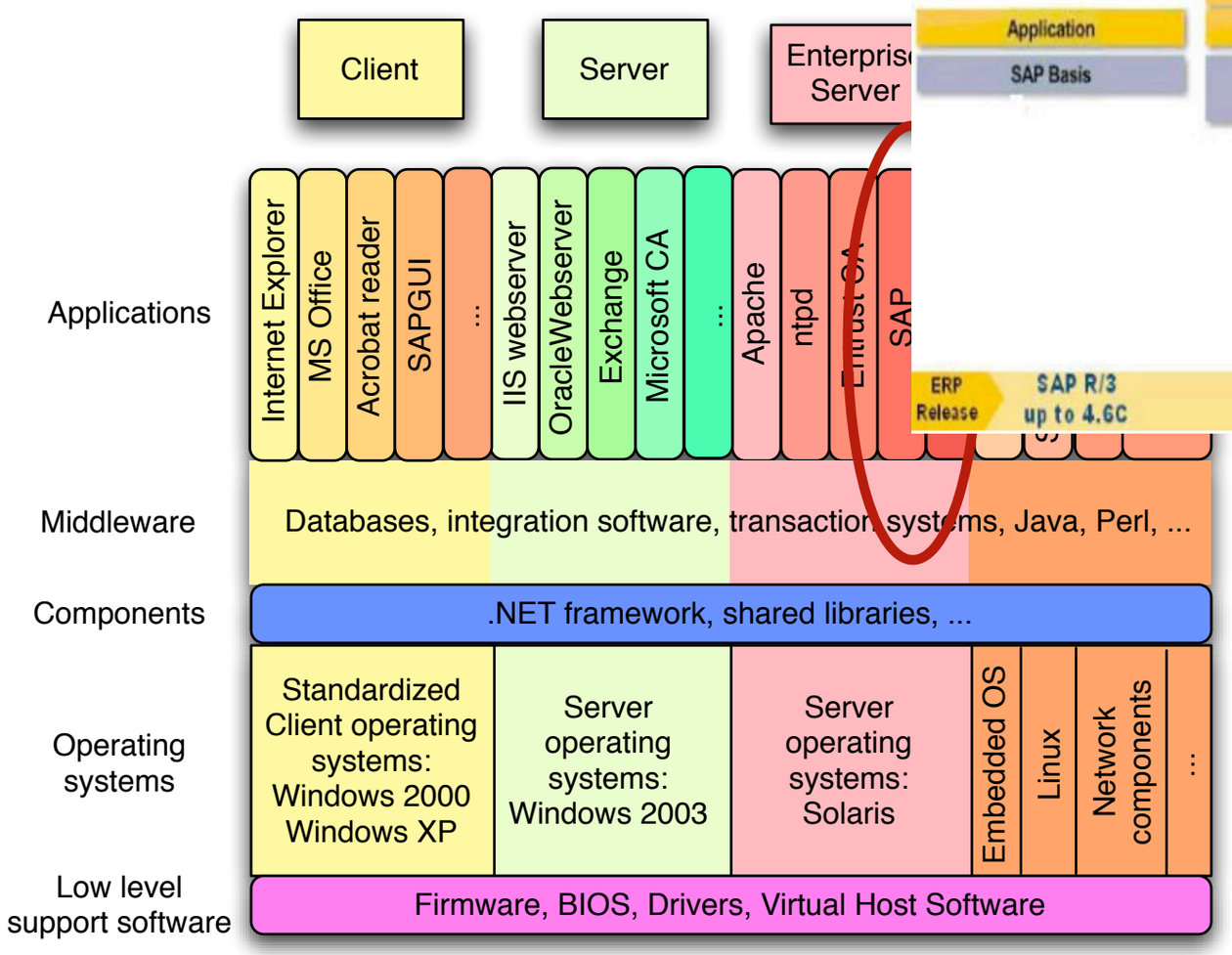
Designprincipen för lagerindelning



ROMAB
ROBERT MALMGREN AB

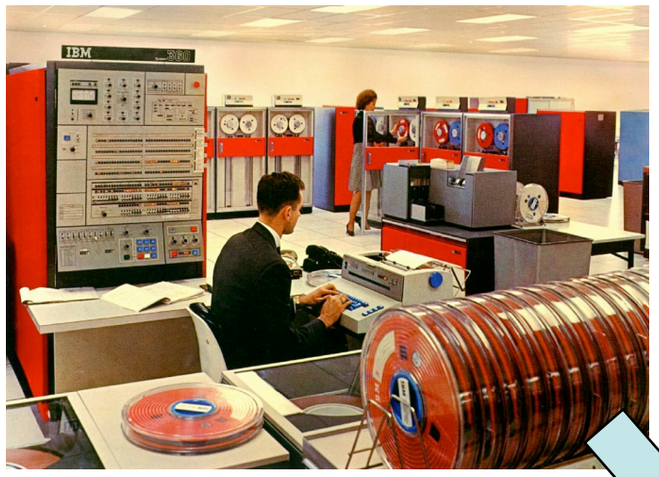
Designprincipen för lagerindelning

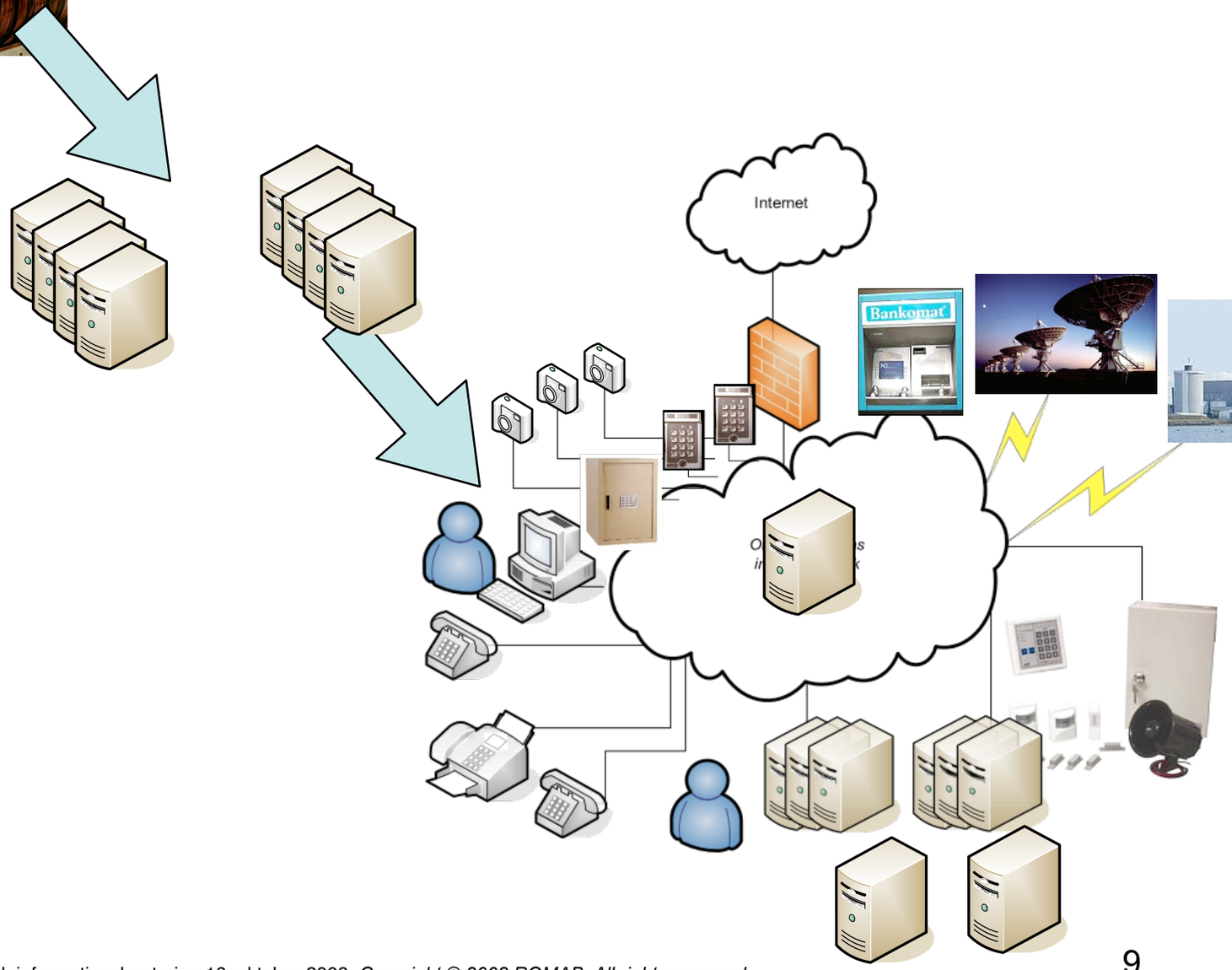




ROMAB
ROBERT MALMGREN AB

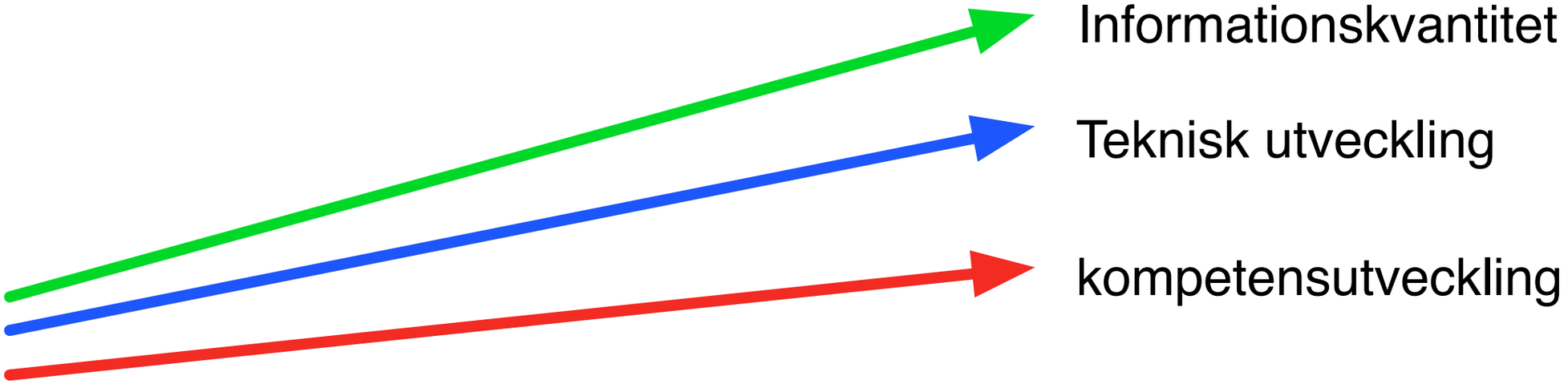
Utvecklingen





ROMAB
ROBERT MALMGREN AB

Utvecklingen



200x

2008

ROMAB
ROBERT MALMGREN AB

Delsammanfattning hot&attacker

- Säkerhetsbrister finns på mängder av ställen i ett systemlandskap
  - trenden har länge varit mot fjärrangrepp
- Angrepp sker på alla nivåer
  - trenden har flyttat från OS-angreppet mot applikationer
- Vi har en alltmer komplex IT-miljö
- Ökande gap map informationsmängder, angreppsmetodiker, etc

ROMAB
ROBERT MALMGREN AB

Viktiga säkerhetsfrågor

- Kritiska infrastrukturkomponenter, tex integrationsfunktionen, “ägs” inte av någon ⇨ styvmoderligt behandlad
- Högsta eller lägsta kraven lägger ribban?
- Förstår man “impact” av ett säkerhetsproblem i en sådan komponent?
- Delade konton för tex projekt
- Spårbarhet? *Riktig* spårbarhet?

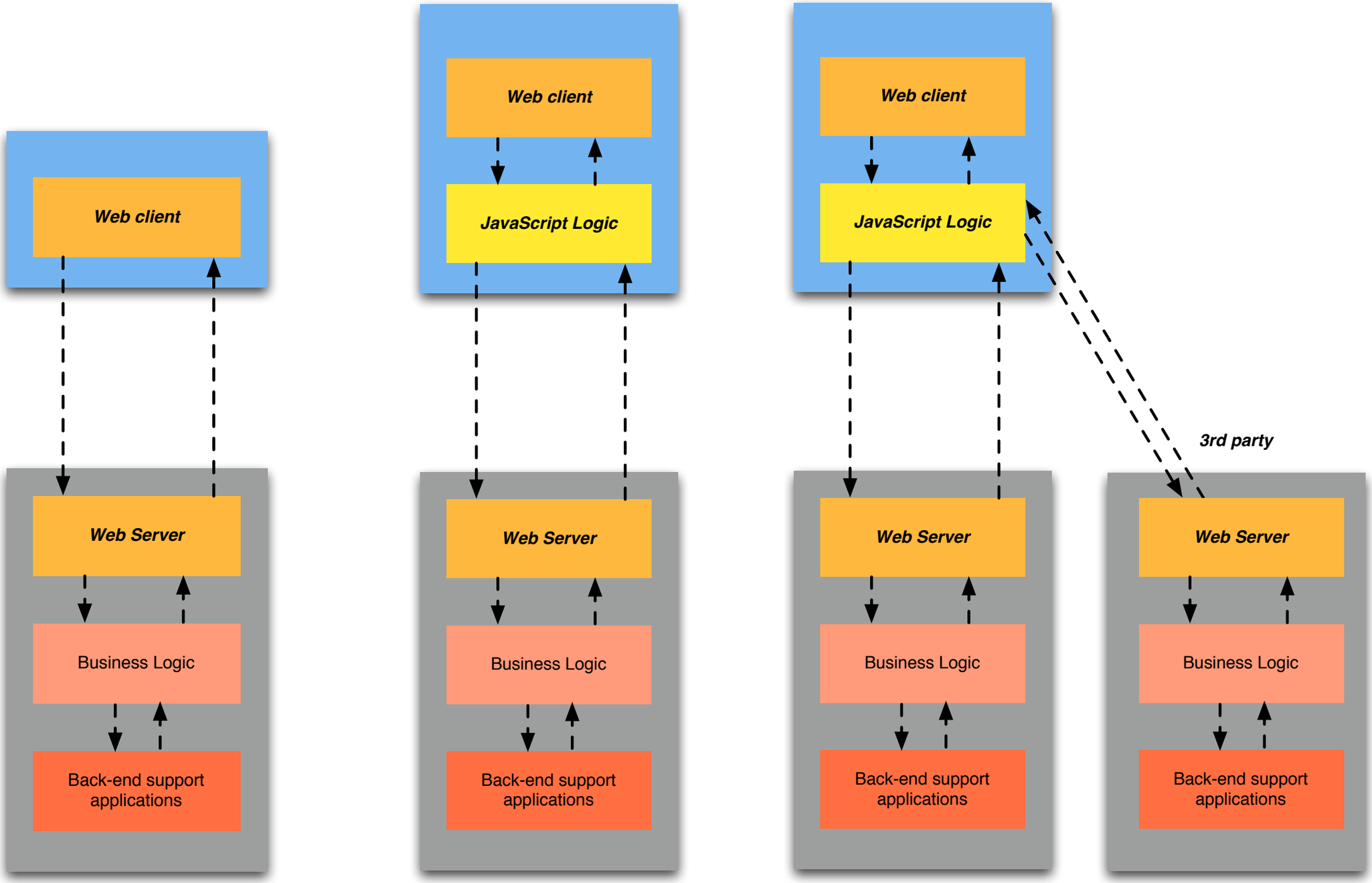
ROMAB
ROBERT MALMGREN AB

Viktiga säkerhetsfrågor

- Skydd av *data-at-rest* och/eller *data-in-transit*?
- Vilken säkerhetspåverkan har centraliserad information vs replikerad information?
  - Olika scenarion för skydd och angrepp
  - Vem är i slutändan ansvarig för *information X* när den migrerat/kopierats nedströms?

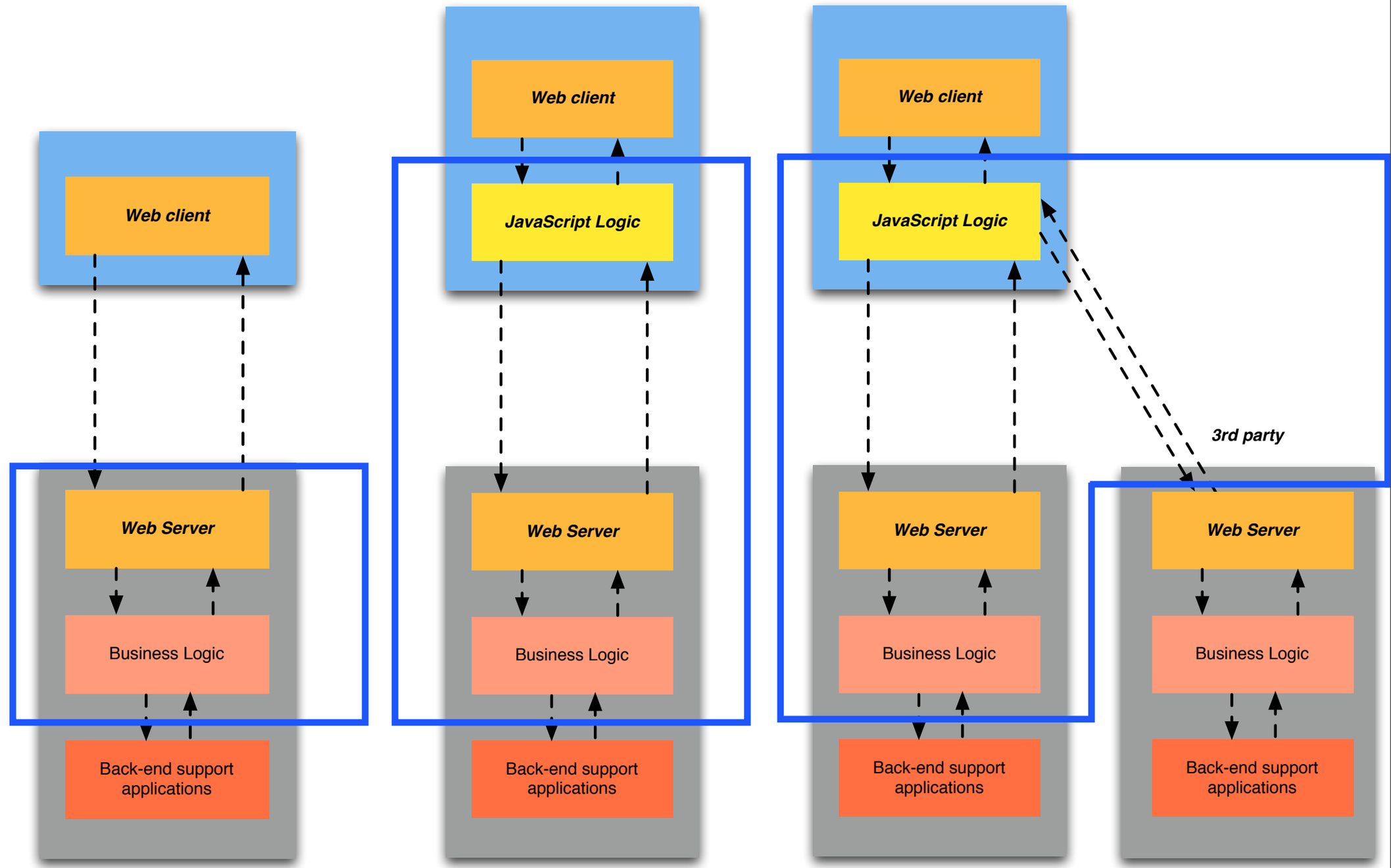
ROMAB
ROBERT MALMGREN AB

Webbarkitekturer



ROMAB
ROBERT MALMGREN AB

Webbarkitekturer



ROMAB
ROBERT MALMGREN AB

Risker med AJAX & webb 2.0

- Mer logik på klientsidan. I värsta fall utför klientsidan säkerhetsbeslut - utan motsvarande kontroll på serversidan (feldelegerad logik)
- Större attackyta
  - State som hålls på klientsidan, XML-fuzzing
- Angriparen är på applikationens “insida”

ROMAB
ROBERT MALMGREN AB

Risker med AJAX & webb 2.0

- Användargenererat innehåll....
  - Datakvalitet? Legala effekter?

- Andra möjligheter för Cross-Site Scripting, Cross- Site Request Forgering, etc

ROMAB
ROBERT MALMGREN AB

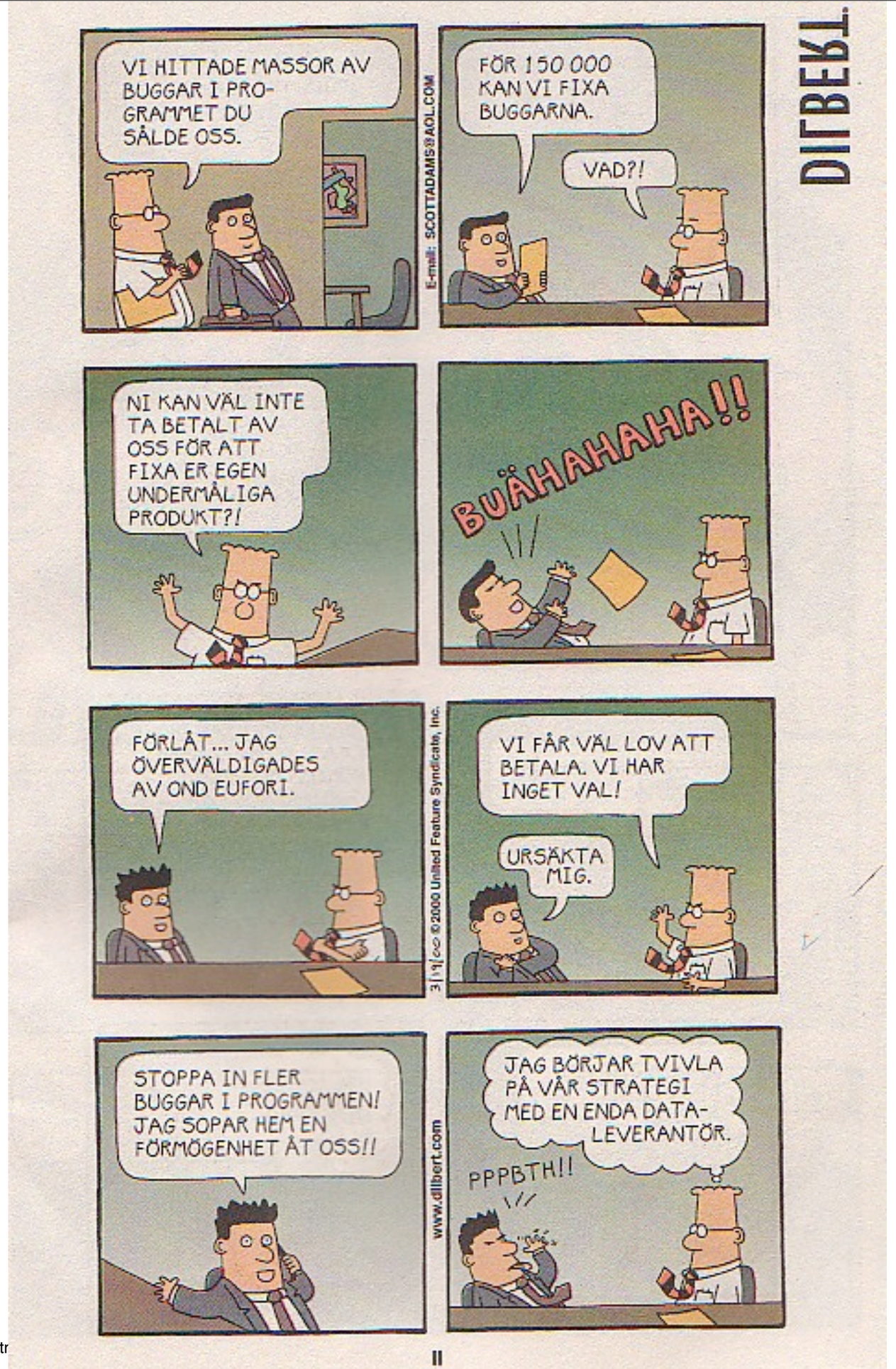
“Topp 5” säkerhetsproblem map informationshantering

1. Prestige är säkerhetsens fiende nr 1
2. Integration, utbyggnad eller införande av ny teknik genomförs i rasande tempo, utan RM/ ROS. Finns återvändo?
3. Informationsklassning inte genomfört fullt ut
4. Ojämn fördelning på skydd. Skydd finns inte på alla lager i mjukvarustacken
5. Drifts- och andra avtal täcker inte viktiga delar: metadata, dynamisk information, konstiga användningsfall

ROMAB
ROBERT MALMGREN AB

Partners, integration, etc

- Vad behöver man tänka på?
  - Framtidssäkert
  - Skalbart
  - Saker utanför den egna organisationens kontroll
- Vanliga fel
  - ...


VI HITTADE MASSOR AV BUGGAR I PROGRAMMET DU SÅLDE OSS.
FÖR 150 000 KAN VI FIXA BUGGARNA.
VAD?!
E-mail: SCOTTADAMS@AOL.COM
DILBERT.
NI KAN VÄL INTE TA BETALT AV OSS FÖR ATT FIXA ER EGEN UNDERMÅLIGA PRODUKT?!
BUÄHAHAHA!!
FÖRLÅT... JAG ÖVERVÄLDIGADES AV ONDA EUFORI.
VI FÅR VÄL LOV ATT BETALA. VI HAR INGET VAL!
URSÄKTA MIG.
3|19|00 ©2000 United Feature Syndicate, Inc.
STOPPA IN FLER BUGGAR I PROGRAMMEN! JAG SOPAR HEM EN FÖRMÖGENHET ÅT OSS!!
JAG BÖRJAR TVIVLA PÅ VÅR STRATEGI MED EN ENDA DATA-LEVERANTÖR.
PPPBTH!!
www.dilbert.com