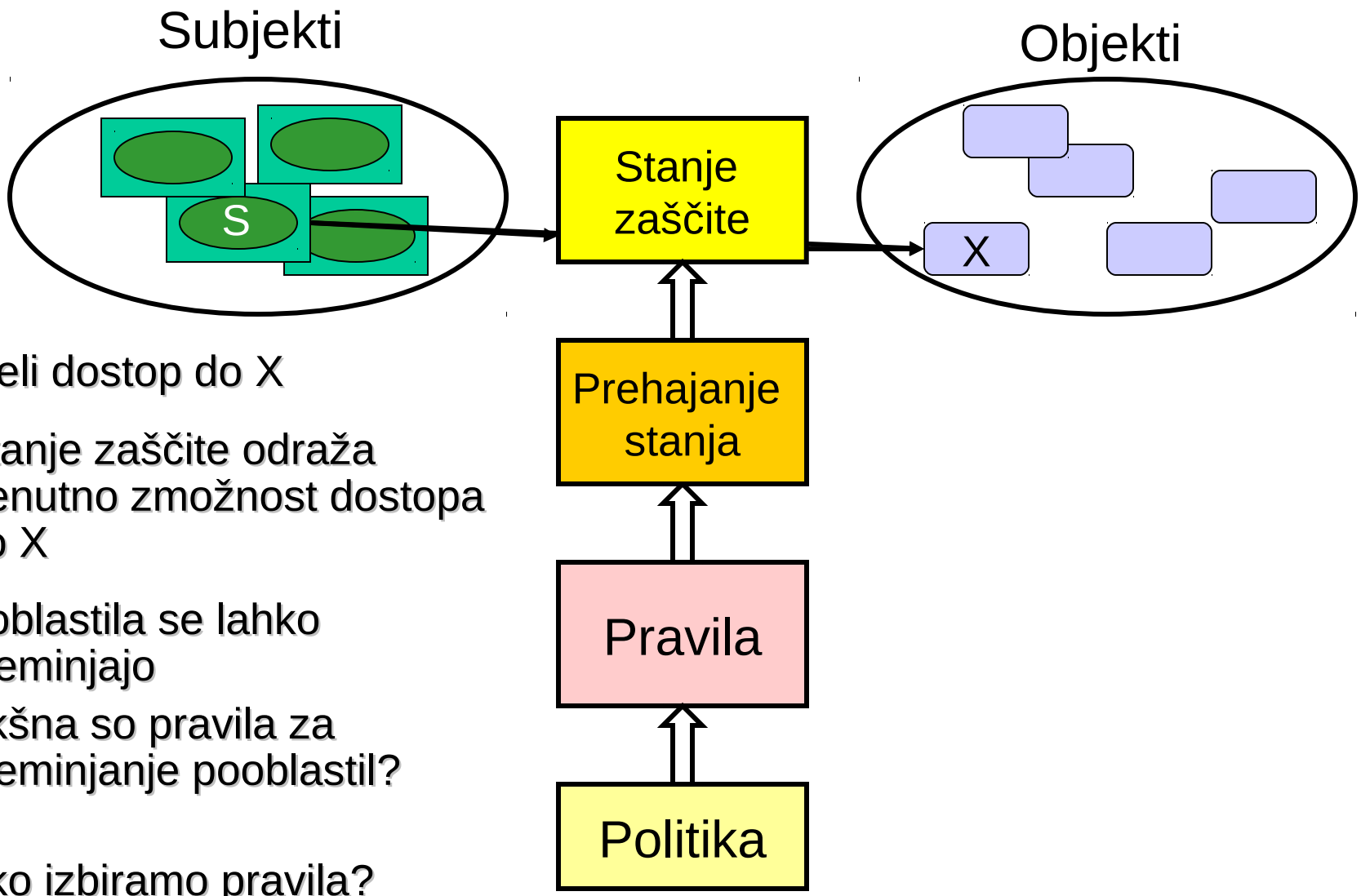
Zaščita
in varnost
operacijskih sistemov

Lampsonov model zaščite

- Aktivni deli (na primer procesi)
  - Delujejo v različnih domenah
  - Subjekt je proces v domeni
- Pasivnim delom pravimo objekti
  - Procesi dostopajo do objektov glede na pravice, ki jih procesi imajo
- Želimo mehanizem zaščite, ki naj omogoča različne varnostne politike za subjekte, ki dostopajo do objektov
  - Možno je več različnih politik
  - Politike se s časom spreminjajo

Sistem zaščite



- S želi dostop do X
  - Stanje zaščite odraža trenutno zmožnost dostopa do X
- Pooblastila se lahko spreminjajo
- Kakšna so pravila za spreminjanje pooblastil?
- Kako izbiramo pravila?

Primer z matriko dostopnosti (Access Matrix) in stanji zaščite

- Matrika dostopnosti subjektov do objektov/subjektov
- Specificira pravice, dodeljenene subjektom za subjekte in objekte
- Pred izvedbo operacije mora sistem preveriti matriko dostopnosti
  - (S_2, spreminja, F_2) dovoljeno
  - (S_2, izvaja, F_2) prepovedano

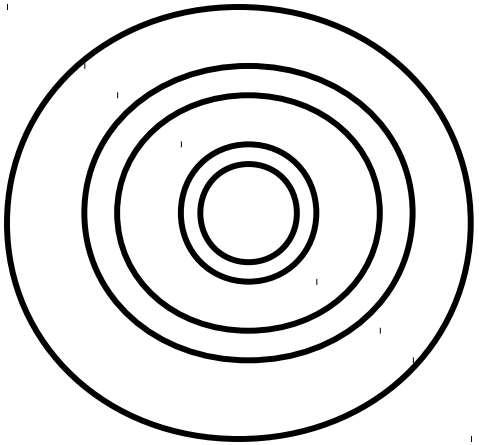
	S_1	S_2	S_3	F_1	F_2	D_1	D_2
S_1	nadzor	blok zbudi lastnika	nadzor lastnika	branje pisanje*		iskanje	last
S_2		nadzor	stop	last	spremi njanje	last	iskanje*
S_3			nadzor	brisanje	izvajaj lastnika		

Pravila politike za stanje zaščite

- Pravila politike krmilijo, kako lahko sistem zaščite spremeni stanje zaščite
  - Pravila specificirajo prehajanja stanj zaščite
  - Kažejo, kako proces prenaša, sbriše in dodeljuje privilegije
- Zakaj je prenos in dodeljevanje pravil politike nevarno?
  - Lahko dovoli procesu (subjektu) prenos privilegijev drugemu procesu
    - Tak privilegij lahko krši politiko varnosti
    - Prenos takih privilegijev drugemu procesu ne smemo dovoliti

Domene zaščite

- Lampson ov model uporablja procese in domene
- Kako implementiramo domeno?
  - Aparaturno: Supervisor/User Mode Bit
  - Programske razširitve -- obroči
- Notranji obroči imajo večja pooblastila
  - Obroč 0 ustreza režimu administratorja
  - Obroči 1 do S imajo manjšo zaščito in jih potrebujemo za implementacijo OS
  - Obroči S+1 doN-1 imajo manjšo zaščito in jih potrebujemo za aplikacije



Domene zaščite (2)

- Prečkanje obroča pomeni spremembo domene
- Prečkanje notranjih obročev⇒ večanje pooblastil
  - Proces pridobi “Sstrožja” pooblastila
  - Proces se mora izvajati v obroču notranje domene
  - Prečkanje pri posebnih vratih
  - Zaščita s mehanizmom avtentikacije
- Prečkanje zunanjih obročev –manj zaščiteni objekti
  - Ni avtentikacije
  - moramo se vrniti nazaj

Uporaba matrike dostopnosti

- Matrika je običajno redko posejana
  - Draga implementacija kot tabela
  - Uporabimo raje seznam
- Seznam po stolpcih imenujemo Seznam nadzora dostopa (***Access Control List (ACL))***
  - Seznam vzdržujemo pri objektu
  - Tipičen primer: zaščitni biti pri datotečnem sistemu Linuxe
- Seznam po vrsticah imenujemo seznam zmožnosti (***Capability List)***
  - Seznam vzdržujemo pri subjektih (na primer procesih)
  - primer "Kerberos Ticket" je zmožnost (Capability)

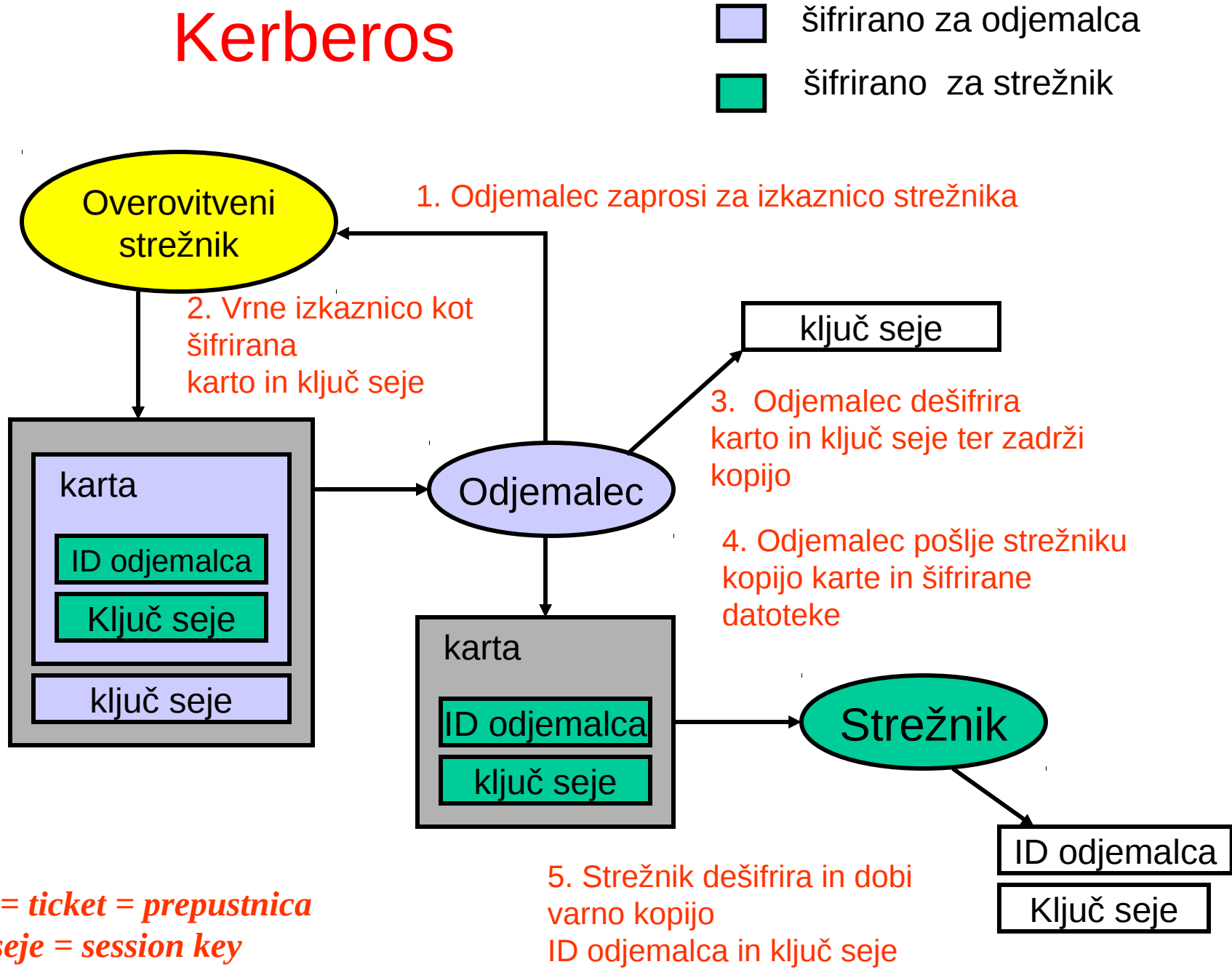
Še o zmožnostih

- Omogočajo naslavljanje objekta iz zelo obsežnega naslovnega prostora
- Lastništvo zmožnosti predstavlja avtorizacijo do dostopa
- Zato mora veljati:
  - Zmožnosti naj bo težko uganiti
  - Zmožnosti morajo biti unikatne in ne ponovno uporabljene

Kerberos

- Kerberos
  - predpostavlja zmešanje podatkov, ki potekajo po omrežju
  - OS na dveh računalnikih nista nujno varna
- Kako deluje Kerberos?
  - Proces na odjemalcu hoče storitev procesa na strežniku
  - Sredstvo komunikacije je omrežje
  - Kerberos nudi strežnik overovitve in protokol
    - Odjemalec in strežnik lahko oddajata overovljena sporočila
    - Overovitvenemu strežniku moramo zaupati!

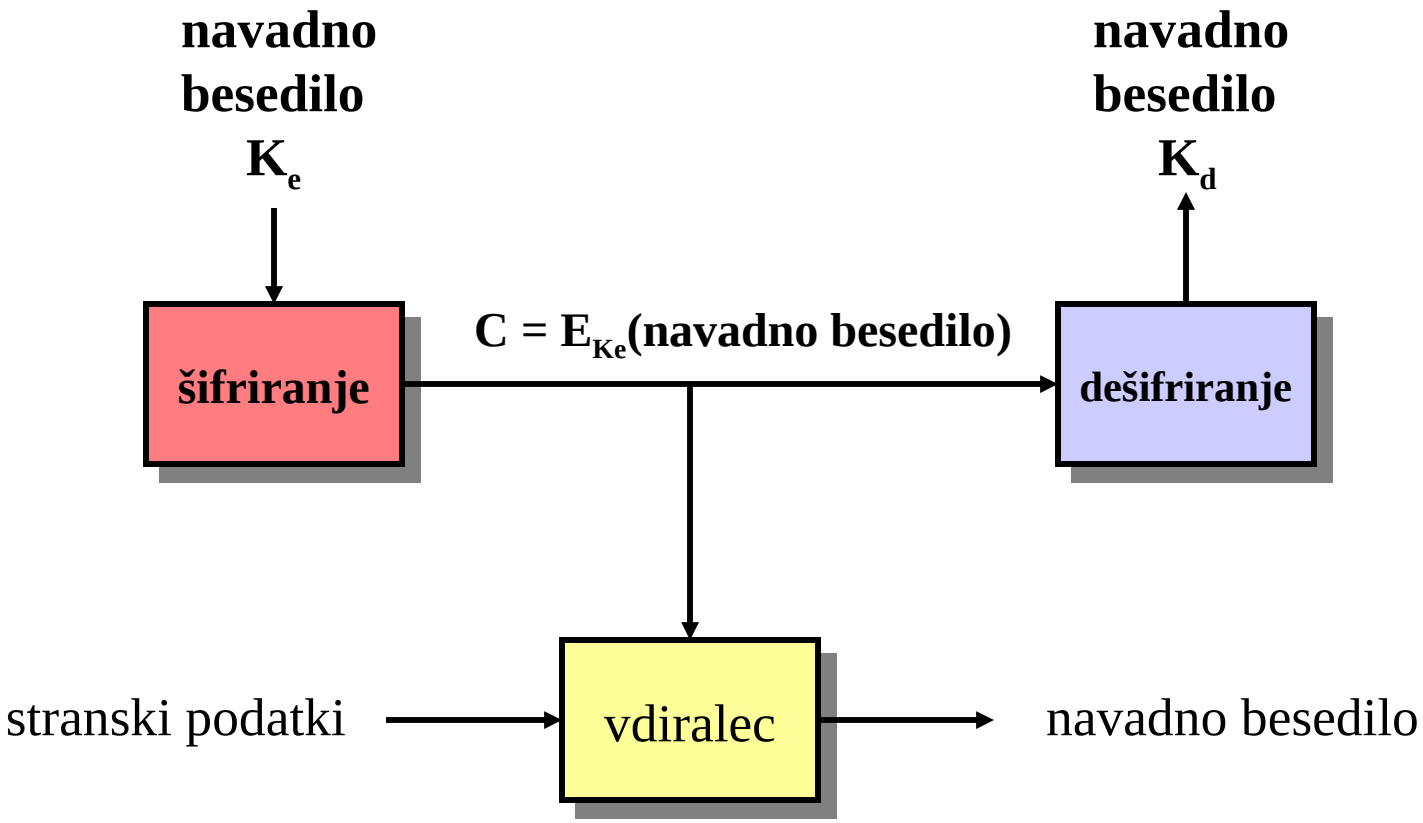
Kerberos


šifrirano za odjemalca
šifrirano za strežnik
Overovitveni strežnik
1. Odjemalec zaprosi za izkaznico strežnika
2. Vrne izkaznico kot šifrirana karto in ključ seje
ključ seje
3. Odjemalec dešifrira karto in ključ seje ter zadrži kopijo
karta
ID odjemalca
Ključ seje
ključ seje
Odjemalec
4. Odjemalec pošlje strežniku kopijo karte in šifrirane datoteke
karta
ID odjemalca
ključ seje
Strežnik
ID odjemalca
Ključ seje
5. Strežnik dešifrira in dobi varno kopijo ID odjemalca in ključ seje
Karta = ticket = prepustnica
ključ seje = session key

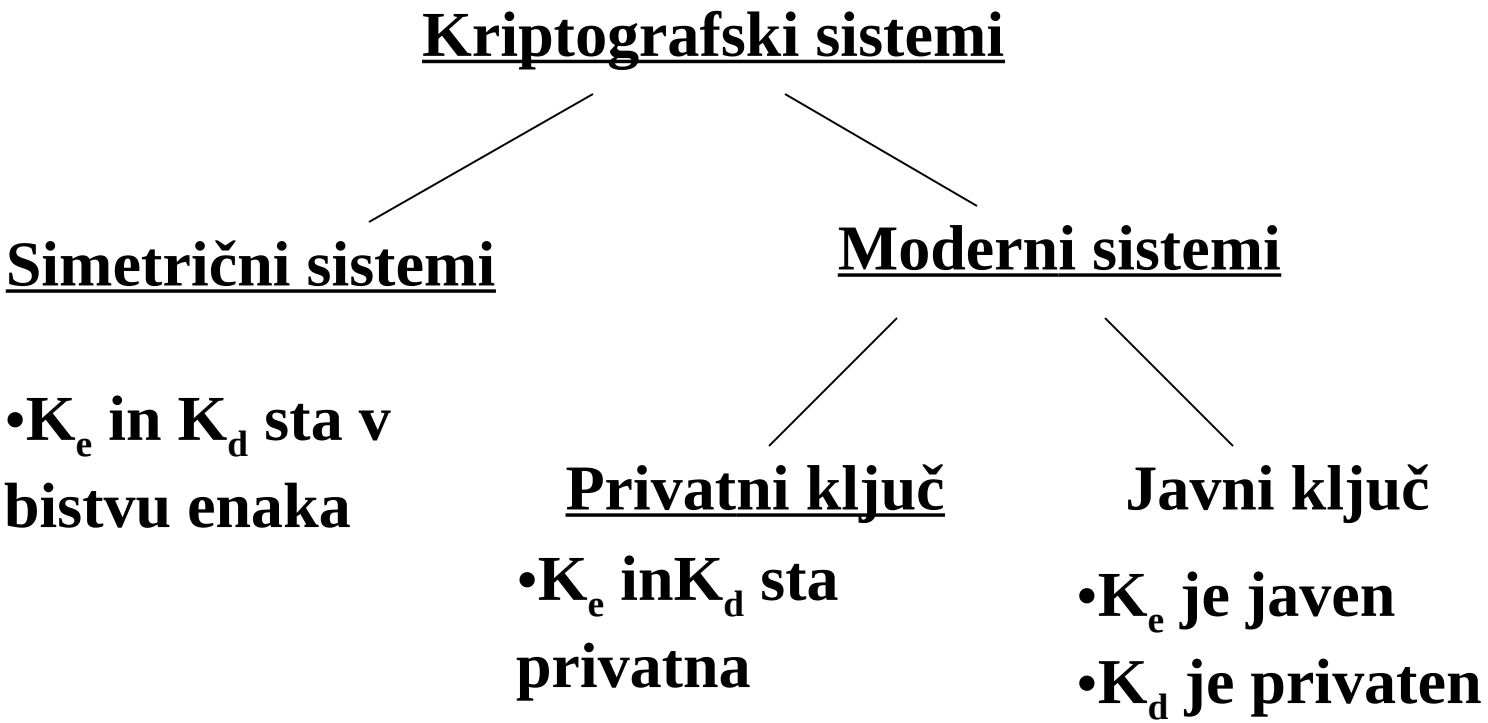
Kriptografija

- Šifriranje: podatke zakodiramo s pomočjo ključa in pošljemo ali zapišemo
- Dešifriranje: pri branju ali sprejemu podatke dekodiramo s pomočjo ključa
- Pogosta uporaba pri varnem prenosu po omrežju
- Matematično ozadje – Tvorba praštevil

Še o kriptografiji



Kriptografski sistemi



Varnost in Java

- Kako lahko apleti postanejo aplikacije?
  - Zaupen ponudnik(tvorec apleta)
  - Podpisani aplet je overovljen
  - "Java Security Manager" lahko dovoli apletu, da je aplikacija izven peskovnika
- Kako lahko podatke prenašamo in izmenjujemo?
  - JAR: arhivske, zgoščene datoteke
  - Kodo in podatke vežemo v javanski arhiv
  - Pridružimo digitalni podpis za overovitev
  - Prenos preko serializacije objektov

Varnostne zmožnosti Javinih ACL (Access Control List)

- Z dovoljenji nadzorovan dostop do virov
- Klasične varnostne tehnike za
  - Podatkovne strukture za zaščito virov
  - Definiranje dovoljen za branje / pisanje za uporabnike in skupine uporabnikov
  - Rokovanje s seznami pooblastil dostopa
  - Podpora pozitivnim in negativnim dovoljenjem
  - Posamezna dovoljenja prekrijejo skupinska
- Implementacija na nivoju programskega jezika za funkcije, tipične za operacijske sisteme

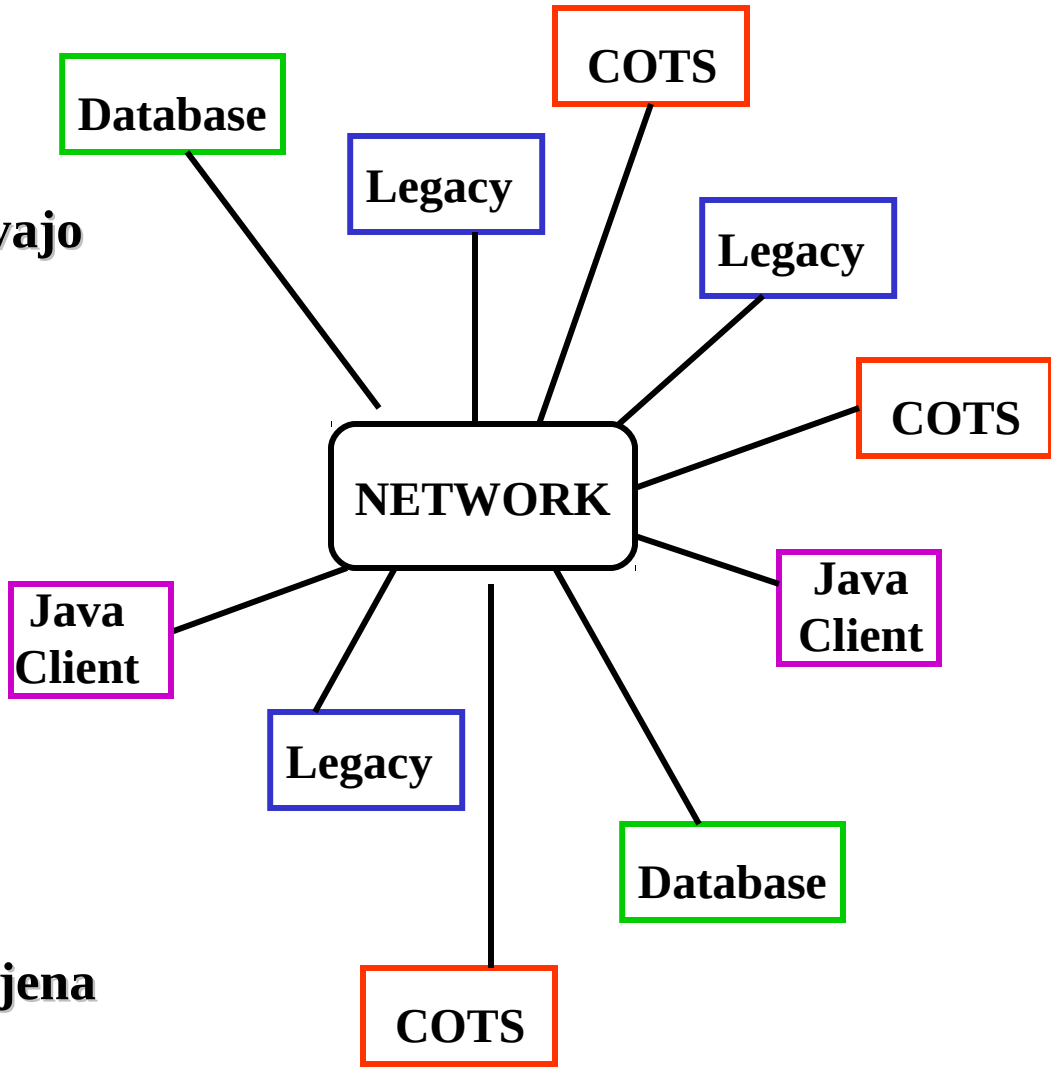
Varnost za porazdeljeno računanje

Kako varnost obravnavajo posamezni sistemi?

Kaj, če ni varnosti pri starejših in komercialnih programih?

Varnost novih odjemalcev? novih strežnikov? vzdolž omrežja

Kaj pa porazdeljena varnost?



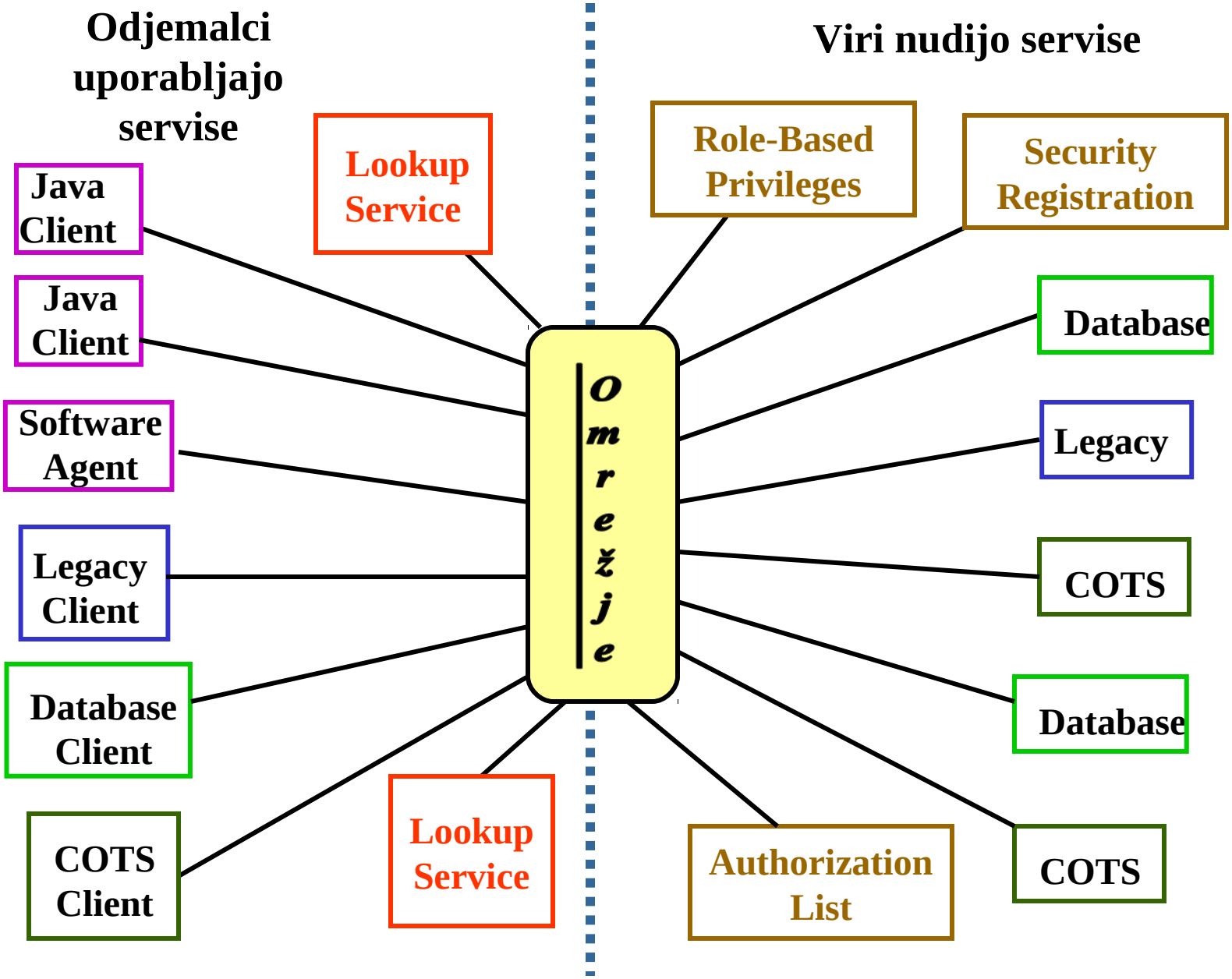
legacy sw – starejši programi
COTS –commercil off the shell sw

Varnost in porazdeljeno računanje

- Avtentikacija (overovitev)
  - Ali je odjemalec res ta, za katerega se izdaja?
- Avtorizacija
  - Ali ima odjemalec dovoljenje za to, kar želi?
- Privatnost
  - Ali kdo prestreza komunikacijo med strežnikom in odjemalcem?
- Ojačitev
  - Centralizirana in porazdeljena "koda"
  - V času izvajanja ojačana varnostna politika

Varnost in porazdeljeni sistemi

- Zavarovanje
  - Ali so varnostni privilegiji vsakega odjemalca primerni za podporo njegove aktivnosti?
  - Ali varnostni privilegiji vsakega odjemalca dosegajo, ne pa presegajo njegovih zmožnosti?
- Konsistenca
  - Ali so definirani privilegiji vsakega odjemalca interno konsistentni?
    - Princip ravno dovolj visokih pooblastil
  - Ali so definirani varnostni privilegiji za klijente globalno konsistentni?
    - Medsebojno izobčenje: Nekateri smejo brati, drugi lahko pišejo



Splošna zgradba odjemalcev in virov.