Sigurnost operativnih sistema

Sadržaj

- Uvodne napomene
- Zaštita memorije
- Operativni sistem od poverenja
- NGSCB

Uvodne napomene

Sigurnost OS.

- Operativni sistemi (OS) su veliki kompleksni progrgami.
  - Velika verovatnića pojave grešaka.
  - Neke od grešaka predstavljaju sigurnosnu pretnju.
- Razmatraće se model sigurnosti koje pruža OS.
  - Neće se razmatrati pretnje koje potiču od grešaka, koje mogu postojati u loše projektovanim OS.
- Ovo je velika oblast, razmotriće se samo najvažnije celine.

Uvodne napomene

Sigurnost OS: zahtevi.

- Savremeni OS su prijektovani tako da omogućavaju istovremeni rad više korisnika (*multi-user*) i istovremeno obavljanje više poslova (*multi-tasking*).
- OS upravljaju sa radom:
  - memorije,
  - I/O uređaja (disk, štampač, itd.),
  - procesa,
  - mreža, ...
- OS treba da obezbede nesmetani rad pojedinih procesa i korisnika, bez obzira da li je “sukob” slučajan ili zlonameran.

Uvodne napomene

Sigurnost OS: funkcije.

- Zaštita memorije.
  - Organizacija pristupa memorijskim lokacijama od strane korisnika/procesa.
- Zaštita datoteka.
- Zaštita korisnika i sistemskih resursa.
- Autentifikacija.
  - Primena metoda i delovanje na osnovu rezultata autentifikacije.
- Autorizacija.
  - Primena metoda i sprovođenje kontrole pristupa.

Uvodne napomene

Sigurnost OS.

- Osnovni problem: kako efikasno organizovati i kontrolisati podelu resursa računara?
- Podela – moguća rešenja:
  - Fizička – posebni resursi (nepraktično).
  - Privremena podela – istovremeni rad jednog korisnika/procesa.
  - Logička podela – dodela određenog dela resursa (npr. memorije) za korisnika/proces.
  - Kriptografska podela – učiniti podatke nerazumljivim za ostale korisnike/procese.
  - Kombinacije prethodnih podela.

Zaštita memorije

Zahtevi.

- Ne treba omogućiti korisnicima/procesima da pristupe memorijskim lokacijama za koje nemaju ovlašćenja.
  - Nije moguće odrediti apsolutne adrese u toku prevođenja programa.
  - Pristup se mora kontrolisati u toku izvršavanja programa.
  - Ponekad je potrebno da različiti korisnici/procesi mogu da pristupe istim delovima memorije.

Zaštita memorije

Granične adrese.

- Ograničiti pristup delu memorije:
  - koju koristi OS,
  - koji koriste pojedini korisnici/procesi.
- Jedan od modela se naziva model **graničnih adresa** (*fence addreses*).
  - Predstavlja opseg adresa memorije kojima korisnici i njihovi procesi mogu da pristupaju.
  - Opseg adresa je određen graničnim adresama.
  - Korisnici ne mogu da pristupe delu memorije čija adresa izvan definisanih granica.
    - **Statičke granice** – OS određuje konstantne vrednosti ovih adresa.
    - **Dinamičke granice** – granica se može menjati na osnovu definisanja vrednosti u odgovarajućem registru.
  - Koriste se base/bounds registri.
    - Čuvaju granične vrednosti adresa.
    - Korisniku/procesu je dodeljen kontinualni prostor.

Zaštita memorije

Dve krajnosti.

- Kako OS određuje zaštitu za pojedine delove memorije?
  - Ravnopravno za sve korisnike/procese ili
  - posebno definisana pravila za svaku memorijsku lokaciju (*tagging*).
- Ovo su dve krajnosti.

Zaštita memorije

Dve krajnosti.

- ***Tagging*** – odrediti prava pristupa za svaku adresu.
  - Dobre osobine:
    - Izuzetno precizan model zaštite.
  - Loše osobine:
    - Predimenzionirano – može biti vremenski i računski zahtevno.
    - Postoji problem sa kompatibilnošću, ova metoda nije rasprostranjena.
- Rešenje: primena zaštite na skup adresa a ne na svaku pojedinačno.
  - Segmentacija.
  - Straničenje.
- Nije toliko fleksibilno ali je mnogo efikasnije rešenje.

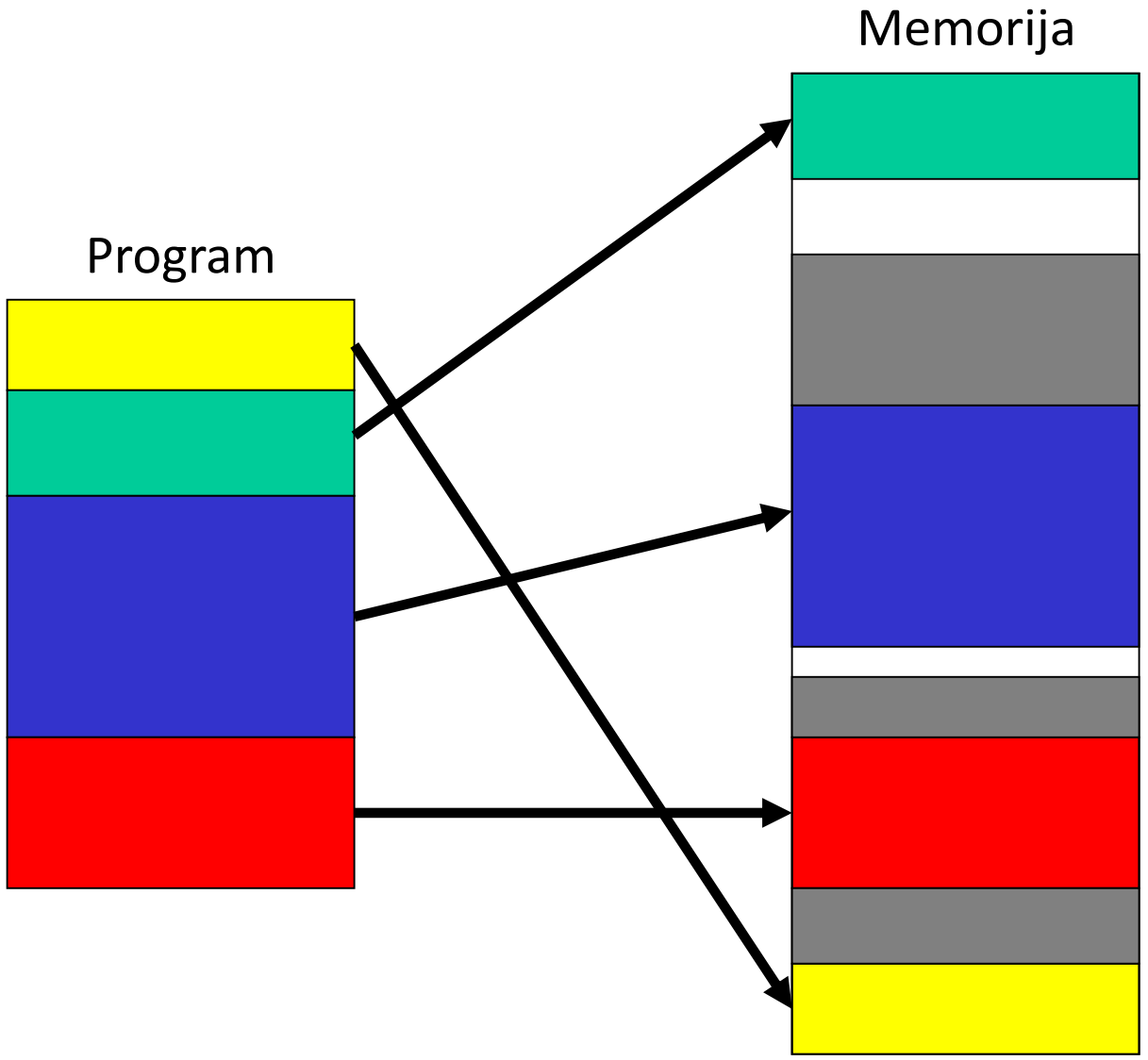
Zaštita memorije

Segmentacija.

- Podeliti memoriju na logičke celine prema:
  - pojedinačnim procedurama ili
  - podacima koji čine celinu.
- Mogu se primeniti različita ograničenja na pristup pojedinim segmentima.
- Segmenti se mogu definisati na bilo kojoj memorijskoj lokaciji.
  - Uslov je da je ta memorijska lokacija dovoljno velika.
- OS ima kontrolu nad lokacijom pojedinih segmenata.

Zaštita memorije

Segmentacija.



Zaštita memorije

Segmentacija.

- OS upravlja podelom memorije na segmente.
  - Segmente može da postavi na različite lokacije.
- OS upravlja raspodelom memorije preko para vrednosti < segment, offset >
  - Segment definiše ime, veličinu i početnu adresu segmenta.
  - Offset definiše udaljenost od početne adrese segmenta.
- Prednosti:
  - Segmenti mogu da menjaju lokaciju u memoriji.
  - Sadržaj segmenta se lako može proslediti iz memorije ili učitati u memoriju.
  - OS upravlja adresiranjem segmenata, pa je moguće ostvariti kontrolu (deljeni ili zasebni resursi).

Zaštita memorije

Prednosti segmentacije.

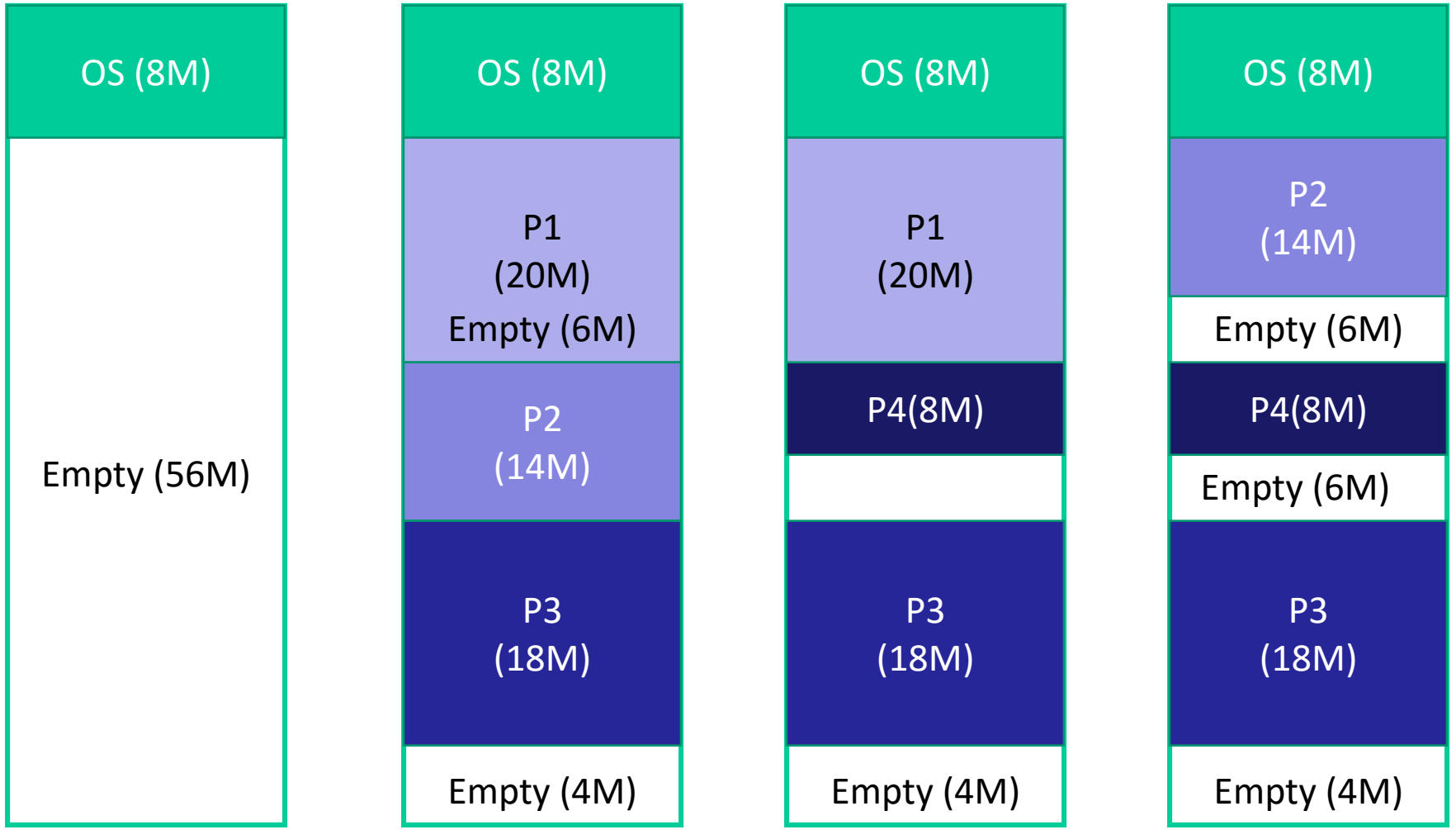
- Moguća je kontrola pristupa pojedinim segmentima na osnovu adrese.
  - OS može da ostvari ulogu nadzora.
- Moguća primena različitih nivoa zaštite nad različitim segmentima
- Može se dozvoliti da više korisnika pristupa istom segmentu.
- Nekim korisnicima je moguće ograničiti pristup određenim segmentima.

Zaštita memorije

Nedostaci segmentacije.

- Kako se koriste podaci < segment, offset > ?
  - OS mora da zna veličinu segmenta (*segment size*) kako bi korisniku/procesu dozvolio pristup željenoj memorijskoj lokaciji.
  - Veličina nekih segmenata može da se menja u toku rada (npr. dinamička dodela memorije).
  - OS mora da prati promene veličine segmenata.
- **Fragmentacija** memorije može da predstavlja problem.
  - Posledica je promenljive veličine segmenta.
- Segmentacija je kompleksna i zahteva veliko angažovanje OS.
- Složenije rešenje $\rightarrow$ veća verovatnoća greške.

Primer fragmentacije.



Zaštita memorije

Straničenje.

- Podeliti memoriju na male celine jednake veličine.
  - Podeliti svaki proces na delove iste veličine.
- *pages*: celine procesa.
- *frames*: celine memorije.

Zaštita memorije

Straničenje.

- U osnovi, slično postuku segmentacije ali segmenti imaju unapred određenu veličinu koja ne može da se menja.
- Pristup memorije preko para podataka: < page, offset >, gde je:
  - page adresa memorijske lokacije.
  - offset udaljenost od početne adrese.
- OS upravlja tabelom (*page table*) svakog procesa.
- Sadrži podatke o svim delovima memorije koji koristi jedan proces.

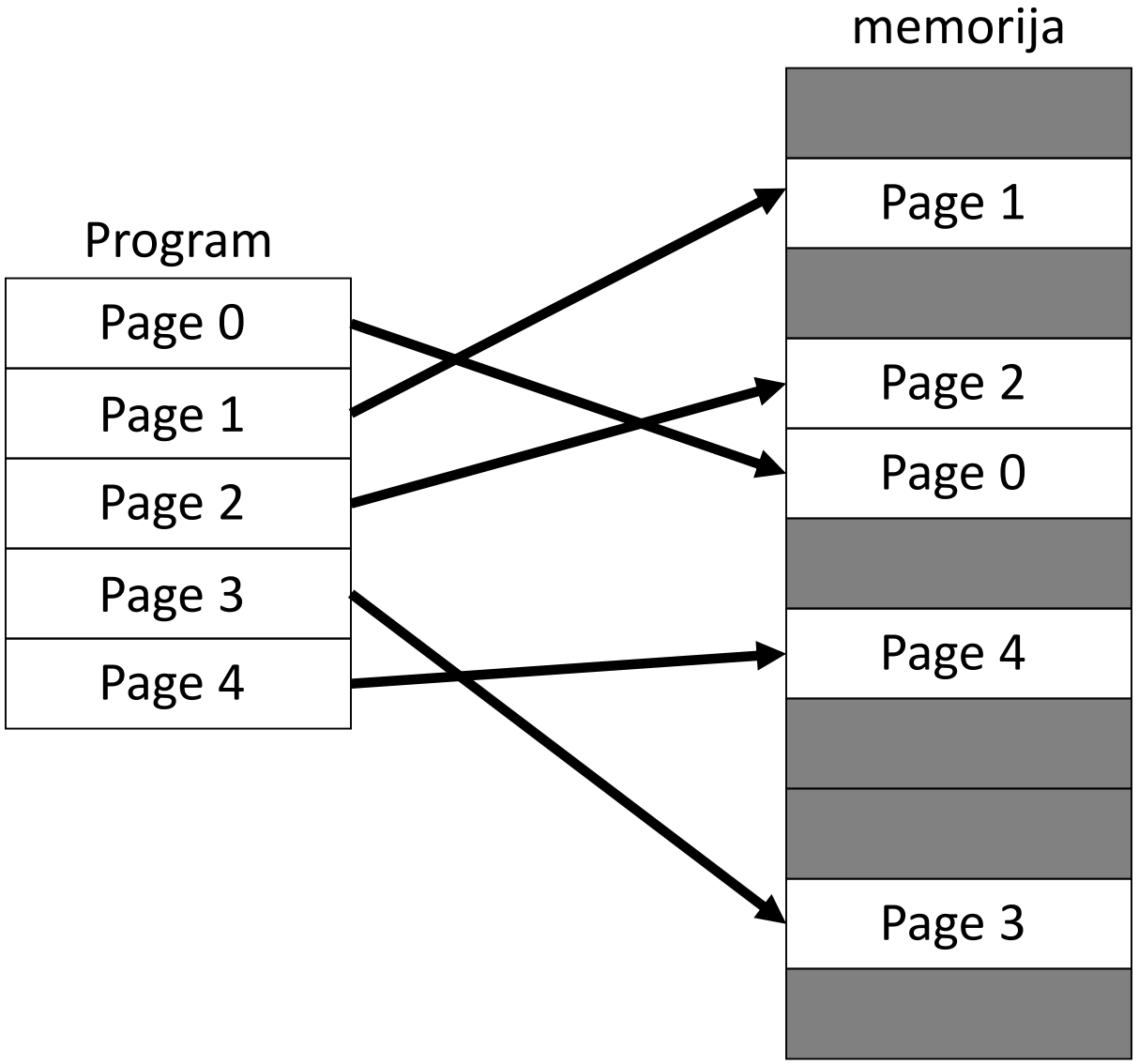
Zaštita memorije

Straničenje.

- Prednosti:
  - Nema fragmentacije $\rightarrow$ veća efikasnost.
  - OS ne mora da prati promene veličine segmenata.
- Mane:
  - Nema logičkih celina.
  - Teško definisati zaštitu pojedinih delova memorije.

Zaštita memorije

Straničenje.



Operativni sistem od poverenja

Šta je operativni sistem od poverenja?

- *Trusted Operating System* (TOS) je onaj OS koji ima integrisane mehanizme za:
  - zaštitu memorije,
  - zaštitu datoteka,
  - autentifikaciju i
  - autorizaciju.
- Većina OS ima ove mehanizme.
- Ako postoje slabosti kod njihove primene, postoji velika opasnost za sigurnost sistema.

Operativni sistem od poverenja

Poverenje i sigurnost.

- **Poverenje** je verovanje.
  - Poverenje je binarna odluka (da/ne).
- **Sigurnost** mora biti dokaziva.
  - Dokazi treba da budu zasnovani na uspešnosti primenjenih mehanizama.
  - Sigurnost zavisi od poverenja!

Operativni sistem od poverenja

Poverenje i sigurnost.

- Poverenje u sistem se zasniva na njegovoj sigurnosti.
- Sistem u koji ne postoji poverenje ne mora biti nesiguran.
- Ako su “razbijeni” svi sistemi u koje ne postoji poverenje, to neće uticati na vašu sigurnost.
- Samo sistem u koji postoji poverenje može da naruši vašu sigurnost!

Operativni sistem od poverenja

Opšti principi sigurnosti.

- Najmanje privilegije – slično principu “*low watermark*”.
- Jednostavnost.
- Otvoreni dizajn (Kerhofovi principi).
- Potpuni nadzor.
- Bela lista (bolje i crna lista).
- Separacija.
- Laka primena.
- Većina komercijalnih OS imaju i mnogo drugih integrisanih svojstava.
  - Rezultat: složenost i mala sigurnost.

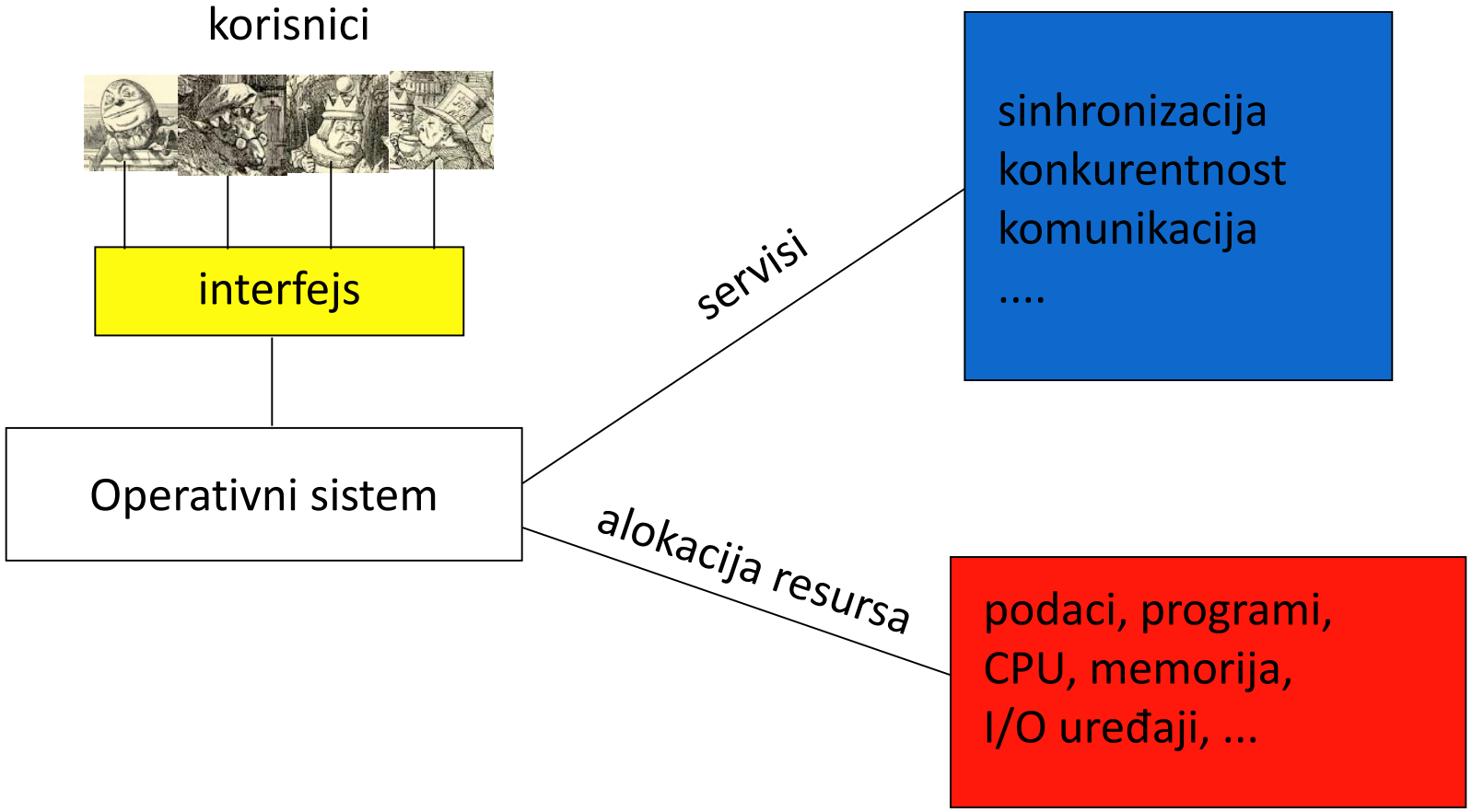
Operativni sistem od poverenja

Šta OS treba da obezbedi?

- Svaki OS treba da obezbedi neki oblik:
  - autentifikacije,
  - autorizacije (korisnika, uređaja i podataka),
  - zaštite memorije,
  - deljenja resursa (s*haring*),
  - međusobne komunikacije i sinhronizacije procesa,
  - zaštite OS.

Operativni sistem od poverenja

Servisi OS.



Operativni sistem od poverenja

Šta treba da obezbedi TOS?

- OS od poverenja treba da obezbedi:
  - autentifikaciju i autorizaciju korisnika,
  - obaveznu kontrolu pristupa – *Mandatory access control* (MAC),
  - diskrecionu kontrola pristupa – *Discretionary access control* (DAC),
  - zaštitu objekata koje koristi više korisnika,
  - potpuni nadzor – kontrolu pristupa,
  - nerizičan put za prenos podataka (*Trusted path*).

Operativni sistem od poverenja

MAC i DAC?

- *Mandatory Access Control* (MAC).
  - Pristup ne kontroliše vlasnik objekta.
  - Primer:
    - Alisa je vlasnik TOP SECRET dokumenta.
    - Alisa ne dodeljuje TOP SECRET ovlašćenja drugim korisnicima.
- Discretionary Access Control (DAC).
  - Vlasnik objekta određuje prava pristupa.
  - Primer:
    - Linux prava pristupa datotekama (korisnik može da dodeli prava za čitanje, upis i izvršavanje).
- Ako su istovremeno primenjeni DAC i MAC, MAC je "stariji".

Operativni sistem od poverenja

Zaštita objekata koje koristi više korisnika.

- OS mora da spreči neželjeni protok informacija.
- Primer:
  - Korisnik kreira datoteku.
  - Dobije prostor na disku koji je pre njega neko koristio.
  - Neiskorišćeni deo dodeljene memorije može da sadrži poverljive informacije.
  - Ponekad se može rekonstruisati prethodni sadržaj i ako je prepisan novim podacima (*magnetic remanence*).

Operativni sistem od poverenja

Nerizičan put (*trusted path*).

- Unosite svoju lozinku.
- Šta se sa njom nakon toga dešava?
- Zavisi od softvera!
- Kako možete da imate potpuno poverenje u sofrver čiju dokumentaciju ne posedujete?
- *Trusted path problem*:
  - Ross Anderson: “*I don't know how to be confident even of a digital signature. I make on my own PC, and I've worked in security for over fifteen years. Checking all of the software in the critical path between the display and the signature software is way beyond my patience*.”

Operativni sistem od poverenja

Nadzor.

- OS treba da obezbedi autentifikaciju korisnika (npr. unos lozinke).
- Treba voditi evidenciju o pristupu sistemu (za npr. kasnije analize napada, i sl.)
- Šta čuvati u *log* fajlovima?
  - Sve? Ko (ili šta) će ih analizirati?
  - Ne želimo da se preoptereti administrator ili proces za analizu.
  - Traži se “igla u plastu sena”.
- Da li pamtiti pogrešne lozinke?
  - Moguće je rekonstruisati prave!
  - Ako se ne pamte kako analizirati moguće napade?
- Ovo je složen problem!

Operativni sistem od poverenja

Kernel.

- Kernel (*kernel*) ili jezgro je najniži nivo operativnog sistema.
- Kernel je odgovoran za:
  - sinhronizaciju,
  - komunikaciju između procesa,
  - prosleđivanje poruka,
  - upravljanje prekidima (*interrupt handling*), itd.
- **Sigurno jezgro** (*security kernel*) je deo kernela koji je zadužen za sprovođenje mehanizama sigurnosti.

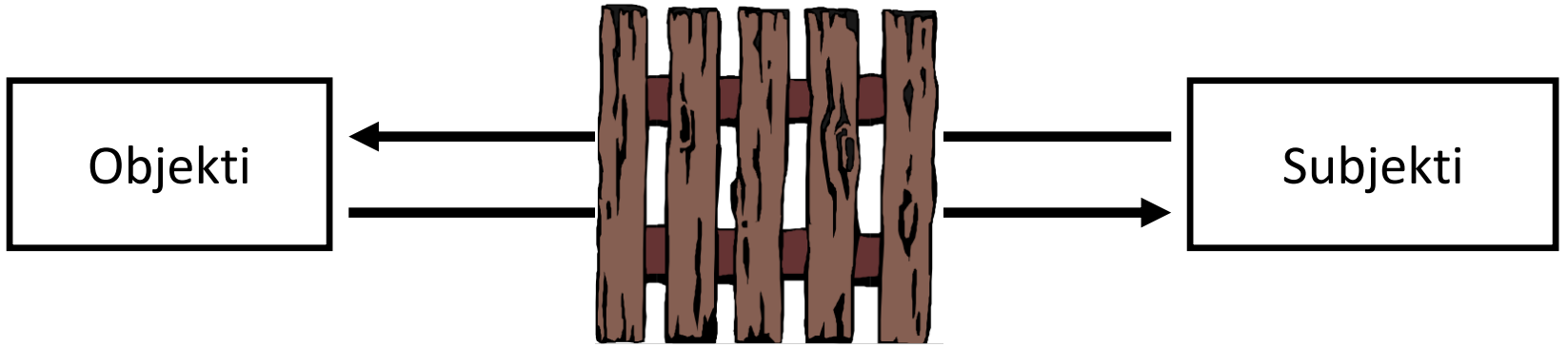
Operativni sistem od poverenja

Sigurno jezgro.

- Šta obuhavata *security kernel*?
- Kernel posreduje u svim pristupima.
  - Idealno mesto za kontrolu pristupa.
- Sigurnosno-kritične funkcije se nalaze na jednoj lokaciji.
  - Lako za analizu i testiranje.
  - Lako za modifikaciju.
- Mnogo teže za napadača da “zaobiđe” sigurnosne funkcije jer se nalaze na najnižem nivou.
  - Napadač često uspeva da zaobiđe sigurnosne funkcije na višem nivou OS.

Monitor referenci.

- Monitor referenci (*reference monitor*) je deo *security kernel*-a zadužen za posredovanje prilikom pristupa subjekata objektima.
  - Otporan na napade.
  - Lak za analizu (mali, jednostovan, ...)



Monitor referenci

Operativni sistem od poverenja

Baza poverljivog računarskog sistema.

- *Trusted Computing Base* (TCB) je skup zaštitnih mehnizama implementiranih u OS (može obuhvatiti i hardver) za koji se veruje da obezbeđuju zahteve sigurnosti.
- Na osnovu definicije poverenja, ako je sve izvan TCB “razbijeno”, operativnom sistemu od poverenja i dalje treba da se veruje (i dalje je TOS).
- TCB štiti jednog korisnika od drugog.
  - deljeni resursi
  - deljeni procesi
  - zaštita memorije za korisnike,
  - I/O operacije, itd.

Operativni sistem od poverenja

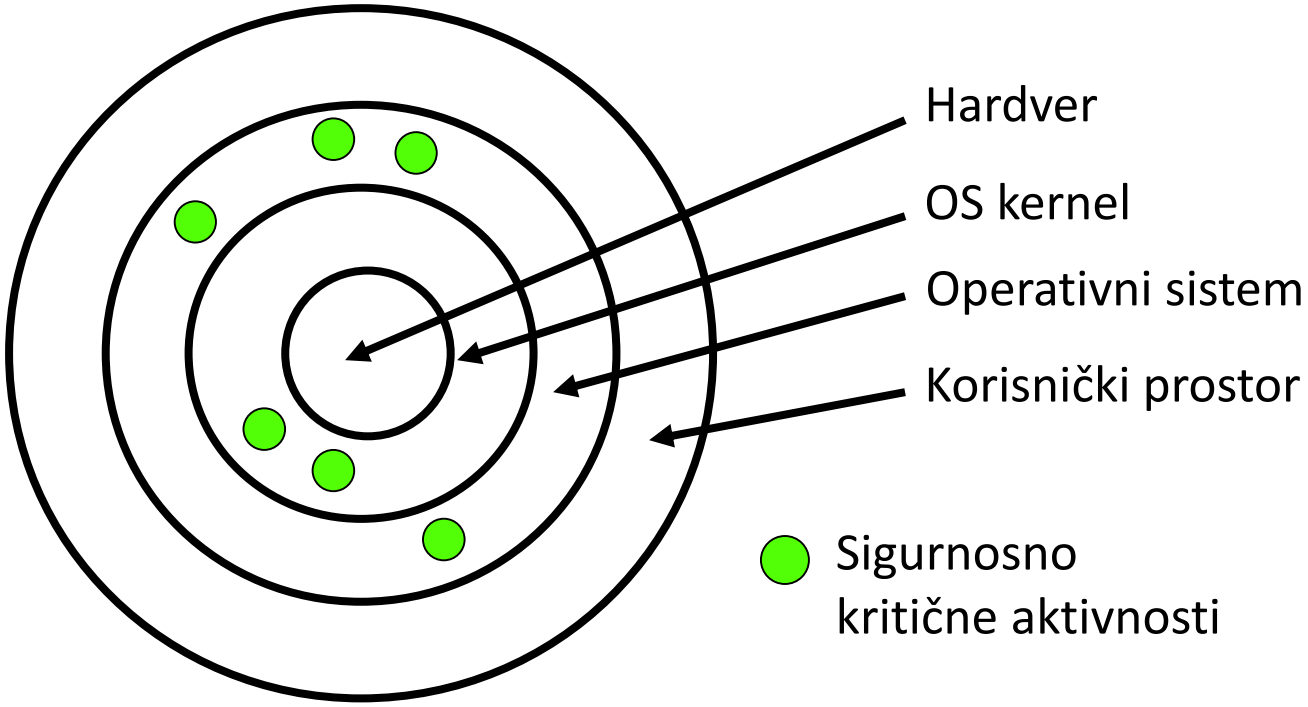
Implementacija TCB.

- Sigurnosno kritične operacije se mogu odvijati u mnogim delovima OS.
- Idealno: prvo dizajnirati *security kernel*, potom ostatak OS oko njega.
- Praksa je najčešće drugačija.

Operativni sistem od poverenja

Loš TCB dizajn.

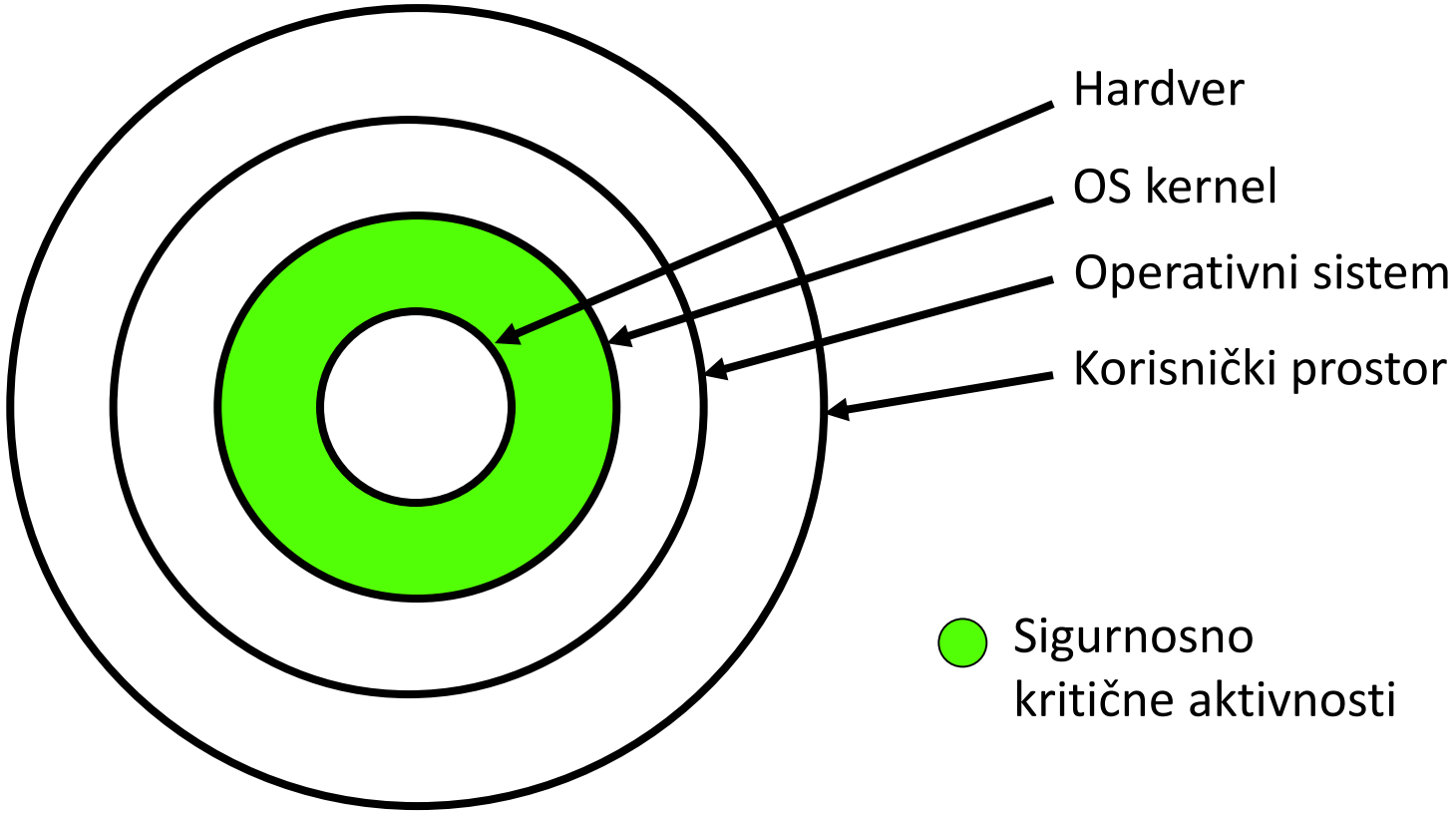
- Problem: sigurnosno kritične aktivnosti nisu definisane na jednom nivou.
- Bilo koja promena sigurnosnih mehanizama može da ima neželjene posledice na rad ostatka OS.



Operativni sistem od poverenja

Poželjan TCB dizajn.

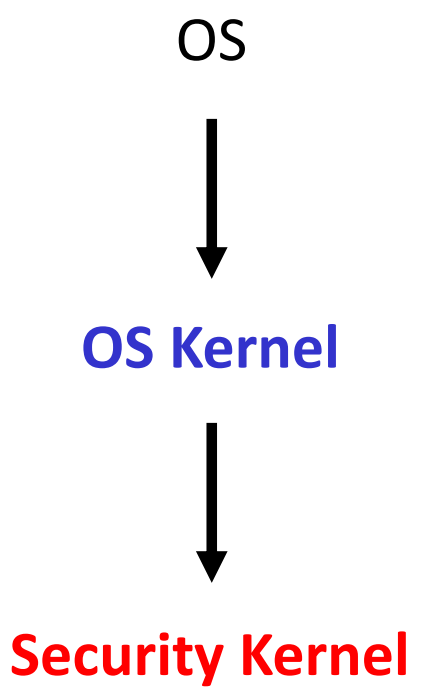
- Sve sigurnosne funkcije su implementirane na jednom mestu (lakša analiza, izmene, odbrana).



Operativni sistem od poverenja

Security kernel.

- TCB je deo OS koji treba da obezbedi sve zahteve sigurnosti.
- Čak i kada je ostatak OS predmet uspešnih napada, ako je TCB siguran, smatra se da je OS od poverenja.
- Ako je TCB “razbijen”, nema sigurnosti ni poverenja.



NGSCB

Next Generation Secure Computing Base.

- Najavljen od Microsoft-a kao koncept narednih OS.
- Zasniva se na hardverskoj tehnologiji dizajniranih od članova grupe TCG (*Trusted Computing Group*).
- Specijalni hardver, RNG, kriptografski koprocesor, čuvanje ključeva, ...
- NGSCB je deo Windows-a koji treba da bude interfejs sa TCG hardverom.
- TCG/NGSCB ranije TCPA/Palladium.

NGSCB

Next Generation Secure Computing Base.

- Početni motiv je bio implementacija mehanizama za *digital rights management* (DRM).
- Danas TCG/NGSCB treba da predstavlja osnovu za implementiranje sigurnosne tehnologije u računarskom svetu.
- DRM je samo jedna od mnogih mogućih primena.
- Postoje različita mišljena o ovom rešenju:
  - *Trusted computing*: http://www.microsoft.com/resources/ngscb/default.mspx
  - *Treacherous computing*: http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html

Razlozi za uvođenje TCG/NGSCB.

- Trenutno stanje.
  - **Zatvoreni sistemi**: konzole za igrice, smartcard, itd.
    - Zaštita autorskih prava (*tamper resistant*).
    - Proizvod se mora platiti.
    - Ograničena fleksibilnost.
  - **Otvoreni sistemi**: personalni računari.
    - Velika fleksibilnost.
    - Prilično loša rešenja za mehanizme sigurnosti.
    - Veoma loša zaštita autorskih prava (softver).
- Cilj TCG je da prednosti zatvorenih sistema primene na otvorene sisteme.

NGSCB

TCG/NGSCB.

- TCG nudi hardver otopran na napade.
  - Sigurno mesto za čuvanje kripto ključeva.
  - Ključevi (ili druge tajne) nisu dostupne čak ni korisniku sa administratorskim privilegijama!
- TCG hardver nije zamena za standardni PC hardver.
- Da bi se iskoristile prednosti TCG hardvera, PC treba da ima dva OS-a: standardni OS i dodatni OS od poverenja (TOS) .
  - TOS treba da bude interfejs za TCG hardver.
- NGSCB je Microsoft-ov TOS.

NGSCB

Ciljevi.

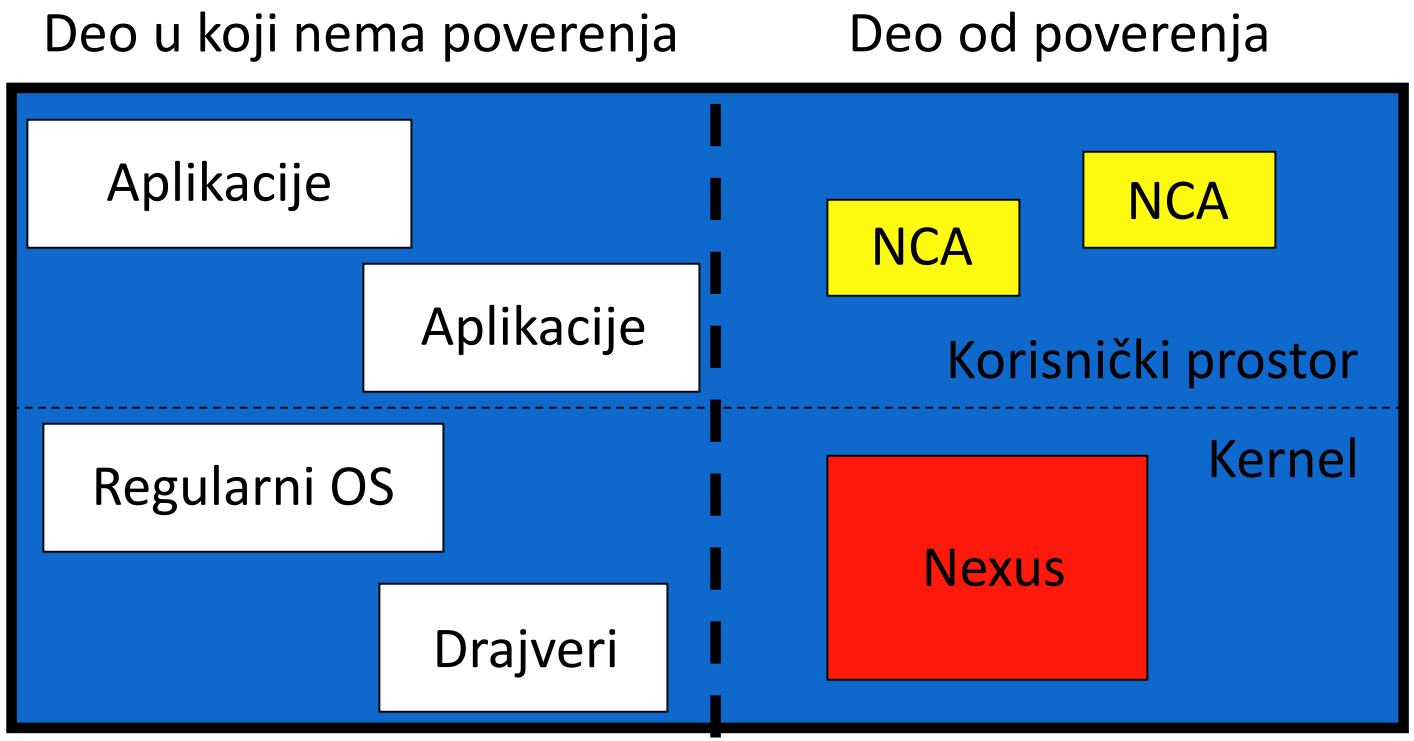
- Obezbediti visok nivo pouzdanosti.
  - Veliko poverenje u sistem.
  - Korektno ponašanje čak i kada je sistem predmet napada.
- Obezbediti autentifikaciju.
  - Autentifikacija softvera, uređaja, ...
- Zaštita od napada na hardver nije cilj NGSCB.
  - To spada u deo nadležnosti proizvođača opreme (TCG).

NGSCB

Arhitektura.

- Postoje dve softverske komponente:
  - *Nexus*, *security kernel* koji je deo operativnog sistema.
  - *Nexus Computing Agents* (NCA), softverski moduli od poverenja koji predstavljaju deo aplikacija koje podržava NGSCB.
- *Nexus* predstavlja bazu poverljivog računarskog sistema (TCB) u NGSCB.
- NCA (*Nexus Computing Agents*) komuniciraju sa *Nexus*-om i delom OS u koji ne postoji poverenje.

Arhitektura.



NGSCB

NGSCB *“feature groups”*.

1. Jaka izolacija procesa.
   - Nema interakcije procesa.
2. Bezbedno skladištenje podataka (*sealed storage*).
   - Podacima mogu da pristupe samo identifikovane i autorizovane aplikacije.
3. Siguran prenos podataka.
   - Zaštićeni prenos podataka.
4. Atest.
   - Potpuna kontrola autentifikacije.
   - Omogućava proširenje TCB preko NCA.

Proces izolacije.

- “Memorija iza zavese” (*curtained memory*).
  - Proces izolacije Nexus-a od ostatka OS-a, BIOS-a, drajvera, ... koji bi mogli da ga napadnu.
  - Blokovi memorije kojima može da pristupi samo TOS (Nexus).
  - Ne može da joj pristupi druga aplikacija.
- Proces izolacije i NCA.
  - NCA su izolavani od softvera u koji ne postoji poverenje.

Sigurno čuvanje podataka.

- Postoje posebni moduli u kojima se čuvaju poverljivi podaci.
- Ako neki kod X želi da pročita ove podatke, heš vrednost koda X mora da se verifikuje (provera integriteta koda X).
  - Implementirano preko simetrične kriptografije.
- Poverljivost je ostvarena jer samo softver od poverenja može da pristupi podacima.
- Integritet tajnih podataka se garantuje karakteristikama modula u kojima se čuvaju.

Siguran prenos.

- Siguran prenos ulaznih podataka.
  - Od tastature do Nexus-a.
  - Od miša do Nexus-a.
- Siguran prenos izlaznih podataka.
  - Od Nexus-a do monitora.
- Upotreba kriptografije u realizaciji zaštićenog prenosa.

Atest.

- Sigurna autentifikacija uređaja, servisa, koda, ...
  - Odvojena od autentifikacije korisnika.
- Koristi se kriptografija sa javnim ključem.
  - Zahteva sertifikovan par ključeva.
  - Korisnik nema pristup privatnom ključu.

NGSCB

NGSCB prema Microsoft-u.

- Sve funkcije regularnog Windows-a će nesmetano raditi u sistemu sa NGSCB.
- Korisnik može da odredi:
  - Koji Nexus će raditi
  - Koji od NCA će raditi
  - Kojim od NCA će dozvoliti da identifikuje sistem ...
- Ova podešavanja ne može da obavi eksterni process.
- Nexus neće blokirati, brisati ili ograničavati pristup podacima (NCA može, ali korisnik ima kontrolu nad NCA).
- Nexus je *open source*.

NGSCB

Andersonova kritika NGSCB.

- Digitalne objekte kontroliše kreator a ne ne korisnik na čijem PC se nalaze. Zašto?
  - Kreator može da definiše NCA.
  - Ako korisnik ne prihvati NCA, nema pristup.
  - Prihvatljivo za npr. sigurnost na više nivoa (MLS).
- Pretpostavimo da Microsoft Word šifruje sve dokumente sa ključem koji je dostupan samo njegovim proizvodima.
  - Teško je prestati da koristite njegove proizvode!
- Citat: “NGSCB pokušava da registruje i kontroliše sve računare”.

NGSCB

Tomborsonova kritika NGSCB.

- NGSCB deluje kao fizičko obezbeđenje.
- Pasivnim aktivnostima, NGSCB može da prikupi sve poverljive informacije.
- Kako korisnik može da zna da ga NGSCB ne špijunira?
- Prema Microsoft-u:
  - Nexus softver će biti javan.
  - NCA može da se debaguje (neophodno zbog razvoja aplikacija).
  - Primena NGSCB je opciona.
- Zadnja vrata?
  - Ne mogu sve verzije NCA da se debaguju. Kontrola je zasnovana na heš vrednostima!

Literatura

1. M. Stamp (2006): *Information Security*. John Wiley and Sons.

Hvala na pažnji

Pitanja su dobrodošla.