Bezbjednost i zaštita informacionih sistema

Sigurnost i zaštita operativnih sistema

Prof. dr Nikola Žarić

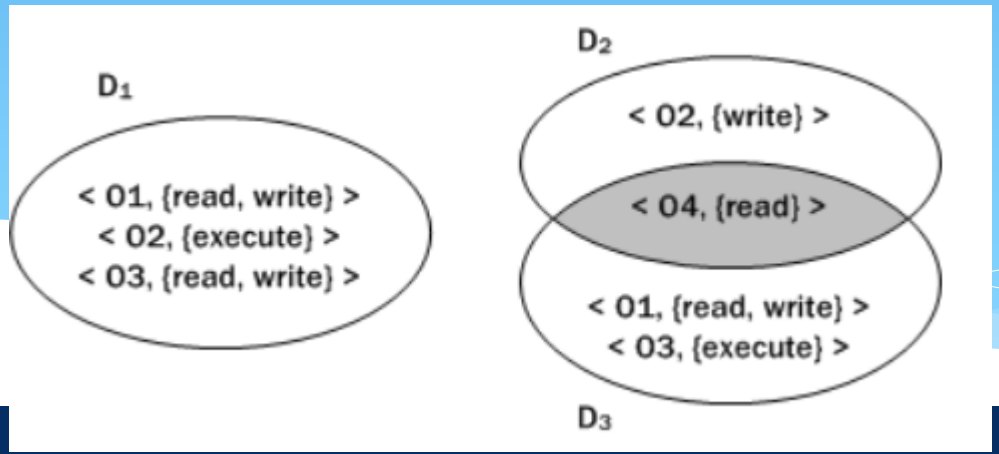
e-mail: zaric@ucg.ac.me

Domeni zaštite

- ✓ Operativni sistem upravlja raznim objektima koji mogu biti hardverski (procesor, memorija, diskovi) i softverski (datoteka, program, semafor).
- ✓ Svaki objekat ima unikatno ime i može mu se pristupati kroz precizno definisani skup operacija.
- ✓ **Zaštita** se, u kontekstu operativnih sistema, odnosi na kontrolu pristupa programa, procesa i korisnika resursima operativnog sistema.
- ✓ Problem zaštite svodi se na kontrolu pristupa objektima operativnog sistema: objektima mogu pristupati samo oni korisnici koji na to imaju pravo, odnosno koji su autorizovani i nad objektom mogu izvšiti samo operacije koje pripadaju dozvoljenom skupu operacija.

Domeni zaštite

- ✓ Domen je kolekcija prava pristupa koja su definisana parovima (ime objekta, skup prava).
- ✓ Svaki domen definiše skup objekata i sve operacije koje se mogu obaviti nad tim objektom.
- ✓ Mogućnost da se izvrši operacija nad objektom nazvaćemo pravo pristupa (access right).



Domeni zaštite

- ✓ Alokacija procesa u domene može biti statička ili dinamička, a sam domen može da se realizuje na različite načine:
  - ✓ svaki korisnik može biti domen,
  - ✓ svaki proces može biti domen i
  - ✓ svaka procedura može biti domen.
- ✓ Svaki sistem koji ima dva režima rada (korisnički i sistemski) mora da ima najmanje dva domena:
  - ✓ korisnički i
  - ✓ sistemski domen.

Domeni zaštite

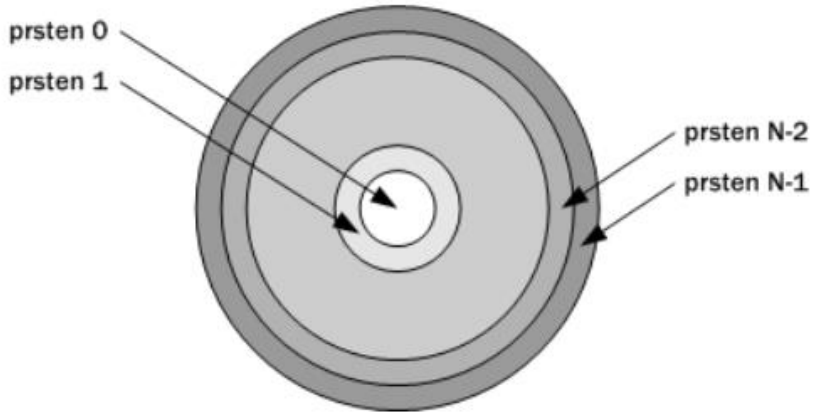
- ✓ Kod UNIX operativnog sistema, domeni su definisani na bazi korisnika

domen = UID

- ✓ Prebacivanje domena može se realizovati putem sistema datoteka - svakoj datoteci može se dodijeliti domenski bit (setuid - SUID bit).
- ✓ Ako se pokrene program sa postavljenim domenskim bitom, korisnik dobija identitet vlasnika datoteke; kada se program završi, UID se resetuje, odnosno vraća na staru vrijednost.

Podjela IDS sistema

- ✓ Kod Multics sistema, domeni zaštite su organizovani hijerarhijski u kružne strukture - prstenove.
- ✓ Svaki prsten predstavlja jedan domen.
- ✓ D0 je najprivilegovaniji domen - to je režim rada jezgra.
- ✓ Prava iz višeg domena uključena su u skup prava nižih domena, dok obrnuto ne važi.



Matrica prava pristupa

- Zaštita se može prikazati kao matrica pristupa (engl. *access matrix*) u kojoj vrste predstavljaju domene, a kolone predstavljaju objekte.
- Element matrice (i,j) predstavlja skup operacija koje proces iz domena Di može da izvrši nad objektom Oj.

Domen	**Objekat**			
	Datoteka F1	Datoteka F2	Datoteka F3	Štampač
D1	read		read	
D2				print
D3		read	execute	
D4	read, write		read, write	

Matrica prava pristupa

- ✓ Matrica reguliše kontrolu pristupa procesa koji pripadaju različitim domenima nad objektima u sistemu.
- ✓ Međutim, u ovako definisanoj matrici procesi u određenim situacijama mogu preći iz jednog domena zaštite u drugi i time ostvariti veća prava nad objektom.
- ✓ U tom smislu, uvodi se izvjesna kontrola prelaska procesa iz jednog domena zaštite u drugi.
- ✓ Naka je prebacivanje procesa iz jednog domena u drugi predstavljeno operacijom *switch*. Matrica se proširuje kolonama koje predstavljaju domene kako bi se mogle definisali moguće operacije prebacivanja iz jednog domena u drugi.

Matrica prava pristupa

✓

Domen	Objekat							
	F1	F2	F3	printer	D1	D2	D3	D4
D1	read		read			switch		
D2				print			switch	switch
D3		read	exec					
D4	read write		read write		switch			

Matrica prava pristupa

- ✓ U nekim situacijama je potrebno izmijeniti sadržaj matrice pristupa, odnosno dodijeliti ili oduzeti pravo procesima jednog domena nad određenim objektom. U tom smislu, uvode se sljedeće operacije:
- ✓ Operacija *copy*. Operacijom copy kopira se pravo nad objektom, pri čemu odredišno polje pripada istoj koloni (procesima iz drugog domena daje se neko pravo pristupa nad tim objektom). Zvezdicom (*) označavamo pravo kopiranja, odnosno mogućnost da proces iz odgovarajućeg domena kopira pravo u drugi domen, odnosno u drugo polje iste kolone.
- ✓

Matrica prava pristupa

- ✓ Postoje tri varijante kopiranja prava:
  - ✓ **Kopiranje prava**. Proces u drugom domenu dobija kopiju prava i kopiju prava kopiranja; dato pravo se ne oduzima od procesa koji obavlja operaciju copy;
  - ✓ **Transfer prava**. Proces u drugom domenu dobija kopiju prava i kopiju prava kopiranja; kopirano pravo se oduzima od procesa koji obavlja operaciju copy;
  - ✓ **Limitirano kopiranje**. Proces u drugom domenu dobija kopiju prava, ali ne dobija pravo kopiranja.

Matrica prava pristupa

Domen	Objekat		
	F1	F2	F3
D1	execute		write*
D2	execute	read*	execute
D3	execute		

Domen	Objekat		
	F1	F2	F3
D1	execute		write*
D2	execute	read*	execute
D3	execute	read	

Matrica prava pristupa

- ✓ **Pravo vlasništva (*owner*)**. U matricu je potrebno uvesti mehanizam koji omogućava dodavanje novih prava ili ukidanja postojećih. Ove operacije nad objektom mogu izvesti procesi iz domena koji ima pravo vlasništva nad tim objektom (owner). Na primjer, ako je u polju (i,j) postavljeno pravo owner, tada se proces iz domena Di može ukidati ili postavljati prava nad objektom j (izmjena je vidljiva u koloni j)

Domen	Objekat		
	F1	F2	F3
D1	owner, exec		write
D2		read*, owner	owner, write*
D3	exec		

Domen	Objekat		
	F1	F2	F3
D1	owner, exec		
D2		owner	owner, write*
D3		read	write

Matrica prava pristupa

- ✓ Pravo kontrole u domenu (*control*). Operacije kopiranja, dodjele i oduzimanja prava modifikuju sadržaj određene kolone u matrici. U matricu se uvodi i pravo kontrole u domenu (control) kojim je omogućena promjena prava po vrsti. Pravo kontrole se može dodjeliti samo objektima koji predstavljaju domene (na primjeru sljedeće tabele, to su posljednje četiri vrste u kojima su opisani domeni D1-D4).
- ✓ Ako je u polju (i,j) dato pravo control, proces koji pripada domenu Di može ukloniti bilo koje pravo dato domenu Dj (pravo u vrsti Dj).

Matrica prava pristupa

Domen	Objekat							
	F1	F2	F3	printer	D1	D2	D3	D4
D1	read		read			switch		
D2				print			switch	switch control
D3		read	exec					
D4	read write		read write		switch			

Implementacija matrice prava pristupa

- ✓ Matrica pristupa može se na sistemu implementirati na četiri načina, zavisnosti od skupa domena/objekata koji su konkretnom matricom opisani:
- ✓ **Globalna tabela**. Prvi i najprostiji slučaj je realizacija matrice pristupa pomoću globalne tabele koja se sastoji od skupa uređenih trojki (domen, objekat, skup prava). Prije nego što proces iz domena Di izvrši operaciju Sk nad objektom Oj, u globalnoj tabeli se traži odgovarajuća uređena trojka (Di, Oj, S), takva da Sk pripada skupu prava S. Ukoliko se takva trojka nađe, operacija se izvršava. U suprotnom, sistem odbija da izvrši operaciju. Prednost ove metode je centralizacija zaštite na nivou sistema, a nedostatak veličina tabele - pretraživanje globalne tabele unosi veliko vremensko kašnjenje

Implementacija matrice prava pristupa

- ✓ **Lista za kontrolu pristupa objektima**. Matrica pristupa može se implementirati i pomoću liste za kontrolu pristupa objektima (access list). Posebna lista kontrole pristupa formira se za svaki objekat sistema i odgovara jednoj koloni matrice pristupa. Listu čini skup uređenih parova (domen, skup prava) - u listi su opisani svi domeni koji nad tim objektom imaju neka prava, a domeni bez prava se ne uključuju. Lista se može dopuniti listom podrazumijevanih prava (default). Jednostavno rečeno, lista opisuje operacije koje procesi koji pripadaju različitim domenima mogu izvršiti nad tim objektom. Liste za kontrolu pristupa su korisniku najpodesnije, jer vlasnik objekta može nad tim objektom jednostavno dodijeliti ili oduzeti prava određenim domenima. Pri određivanju ukupnih prava domena moraju se analizirati svi objekti

Implementacija matrice prava pristupa

- ✓ **Lista sposobnosti domena**. Treći način implementacije matrice pristupa su liste sposobnosti domena. Lista sposobnosti (engl. *capability list*) formira se za svaki domen i odgovara jednoj vrsti matrice prava pristupa. Listu čini skup uređenih parova (objekat, pravo pristupa) - u listi su opisani svi objekti nad kojima taj domen ima neka prava. Jednostavno rečeno, lista sposobnosti jednog domena opisuje operacije koje procesi tog domena mogu izvršiti nad različitim objektima. S korisničke tačke gledišta, liste sposobnosti nisu najpodesnije za korišćenje, ali su pogodne za lokalizaciju informacija pri analizi prava domena.

Implementacija matrice prava pristupa

- ✓ Mehanizam ključeva. Mehanizam ključeva (engl. *lock-key*) je kompromis prethodna dva načina implementacija matrice pristupa. Svakom objektu se dodijeli lista bravica (engl. *lock*), a svakom domenu lista ključeva (engl. *key*). Ključevi i bravice su jedinstveni nizovi bitova. Proces iz domena može pristupiti objektu samo ako njegov ključ odgovara jednoj od bravica objekta. Ovaj mehanizam je fleksibilan i efektivan, zavisno od veličine ključeva. Prava se mogu jednostavno oduzeti izmjenom bitova koji čine bravicu.

Sigurnosni mehanizmi u operativnim sistemima

- ✓ **Opšta sigurnost ne postoji.**
- ✓ Jedan od načina da se poveća opšta sigurnost sistema je periodično provjeravanje mogućih sigurnosnih rupa u sistemu. U tom smislu, potrebno je provjeritida li postoje:
  - kratke lozinke ili lozinke koje se lako pogađaju,
  - opasni programi sa domenskim (SUID) bitom,
  - neautorizovani programi u sistemskim direktorijuma,
  - neočekivani proces koji se veoma dugo izvršava,
  - neodgovarajuća zaštita za direktorijume,
  - neodgovarajuća zaštita za sistemske direktorijume,
  - opasni ulazi u programskoj putanji i
  - promjene u ček-sumama sistemskih programa.

Sigurnosni mehanizmi u operativnim sistemima

- ✓ Zaštita na nivou operativnog sistema je najčešće poslednji nivo zaštite. Operativni sistem mora da zaštiti samog sebe i sistem u celini od slučajnog ili namernog oštećenja. Mehanizmi zaštite na ovom nivou uključuju:
  - ✓ Autentifikaciju korisnika operativnom sistemu. Zahtijeva se da svaki korisnik koji pristupa sistemu ima važeće korisničko ime na sistemu i odgovarajuću lozinku. Na taj način, operativni sistem zna da li se radi o pravom, ovlašćenom korisniku ili ne i shodno tome korisniku dozvoljava ili ne dozvoljava da koristi usluge operativnog sistema. Identifikacija korisnika pomoću povjerljivih informacija je najčešće korišćen metod autentifikacije. Korisnik se, najprije, predstavi sistemu, odnosno identifikuje svojim imenom, a sistem zatim traži potvrdu, odnosno zahtijeva da korisnik navede odgovarajuću lozinku. Ako unijeta vrijednost lozinke odgovara vrijednosti koja se nalazi na sistemu, operativni sistem smatra da je korisnik prošao autentifikaciju.

Sigurnosni mehanizmi u operativnim sistemima

- ✓ **Kontrolu pristupa na nivou sistema datoteka**. Kontrola pristupa je implementirana u sve savremene operativne sisteme i sa njom ćete se prije ili kasnije sresti (osim ako operativni sistem ne koristite isključivo kao root ili Administrator). Implementira pomoću listi za kontrolu pristupa koja određuje ko može da pristupi određenoj datoteci ili direktorijumu i šta sa tom datotekom ili direktorijumom može da radi.

Sigurnosni mehanizmi u operativnim sistemima

- ✓ **Kriptografske mjere zaštite**. Svaki podatak na računaru može se zaštititi šifrovanjem – postoje programi koji šifruju kompletne diskove, prenosive medijume, čak i kod programa instaliranog na računaru. Šifrovanje podataka na diskovima može se obaviti na nivou datoteka i na nivou drajvera. Za šifrovanje na nivou datoteka koriste se klasični sistemi datoteka i posebni programi za šifrovanje datoteka i direktorijuma. Jednostavno se implementira i koristi. Korisnik odučuje šta želi da šifruje i to ručno radi, a pomijeranje podataka na drugi računar ili kreiranje rezervne kopije podataka je relativno jednostavno (na drugi medijum se prenose šifrovani podaci).

Sigurnosni mehanizmi u operativnim sistemima

- ✓ **Kontrola udaljenog pristupa**. Od svakog ozbiljnog operativnog sistema očekuje se da obezbijedi kontrolu udaljenog pristupa sistemu. Konkretno, svaki operativni sistem treba da ima mrežnu barijeru koja će da filtrira podatke na mrežnom i transportnom sloju i da obezbijedi kontrolu pristupa mreži za različite procese (korisnik obučava mrežnu barijeru koja aplikacija smije, a koja ne smije da pristupi mreži). Takođe, poželjno je da operativni sistem obezbijedi podršku za rad sa kriptografskim protokolima (kao što su SSL i IPSec).

Sigurnosni mehanizmi u operativnim sistemima

- ✓ **Praćenje sigurnosnih događaja**. Praćenje sigurnosnih događaja (engl. auditing) i pristupa resursima je jedna od važnijih zaštitnih mjera. Sigurnosni događaji su sve akcije usmjerene na resurse koji su zaštićeni nekom sigurnosnom mjerom kao što je kontrola pristupa. Na primjer, sigurnosni događaj je promjena sadržaja ili pristupnih prava direktorijuma, prijavljivanje na domen, kreiranje ili izmjena naloga i izmjena grupne polise. Praćenje događaja se najčešće primjenjuje na domen kontrolerima i serverima

Sigurnosni mehanizmi u operativnim sistemima

- ✓ **Kreiranje rezervnih kopija značajnih podataka**. O značaju backupa veoma je nezahvalno pisati, zato što čitaoci obično smatraju da je pridavanje značaja kreiranju razervnih kopija podataka ravno “pretjerivanju”. Međutim, kada izgube neke bitne podatke, korisnici obično promijene mišljenje.

- ✓ **Kreiranje plana restauracije** koji identifikuje kritične podatke i opisuje zaštitne mjere koje je potrebno preduzeti u slučaju havarije ili proboja sigurnosti kako bi se brzo i sa minimalnim gubicima obezbijedilo normalno funkcionisanje sistema.