SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 10:

Sigurnost i zaštita operativnih sistema

URLs:

- Zvanična Web strana: www.viser.edu.rs/predmeti.php?id=122
- Dodatni resursi: www.conwex.info/draganp/teaching.html
- Knjige:

  www.conwex.info/draganp/books.html
- Teme za seminarske radove:

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Napomena

- Ovo je skraćena verzija prezentacije / predavanja na temu **“Sigurnost i zaštita operativnih sistema”**

Sigurnost i zaštita operativnih sistema

- Sadržaj poglavlja i predavanja:
  - 10.1 Opšti pregled zaštite i sigurnosnih mehanizama
  - 10.2 Sigurnost i zaštita operativnog sistema Linux
  - 10.3 Sigurnost i zaštita operativnih sistema Windows 2000/XP/2003/Vista/W7

Quote

"Know your enemy and know yourself; in a hundred battles, you will never be defeated. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal. If ignorant both of your enemy and of yourself, you are sure to be defeated in every battle."

–Sun Tzu; The Art Of War, Chapter 3

Potrebna predznanja

- Programiranje
- Za primenu:
  - Računarske mreže i protokoli
  - Operativni sistemi
  - Sistemsko programiranje

- Razvoj operativnih sistema i opšta znanja iz ove oblasti predmet su naše prethodne knjige, "**Operativni sistemi: teorija, praksa i rešeni zadaci**" (Mikro knjiga, 2005). Iz ove knjige steći ćete potrebna predznanja ukoliko naiđete na probleme pri čitanju ovog poglavlja.

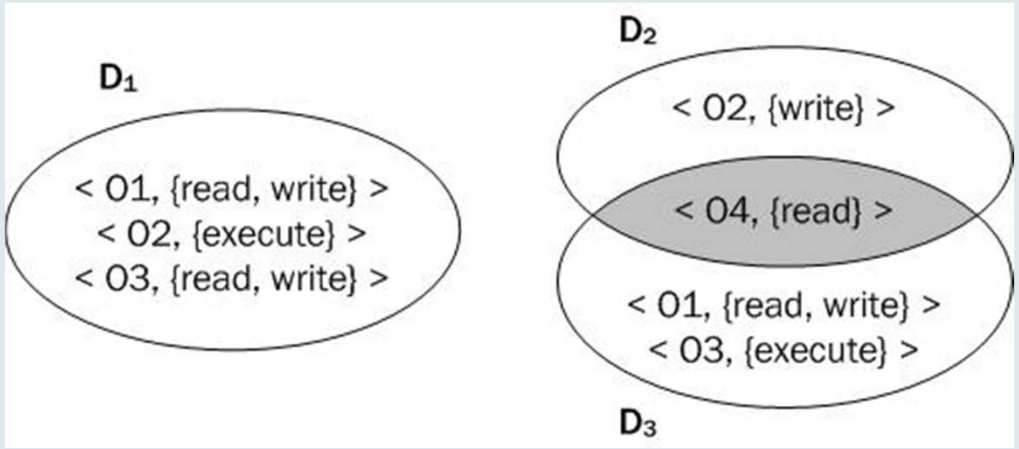
10.1 Opšti pregled zaštite i sigurnosnih mehanizama

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

Domeni zaštite i matrice prava pristupa

- 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 (engl. *access right*).
- Domen je kolekcija prava pristupa koja su definisana parovima (ime objekta, skup prava).

Domeni zaštite



Domeni zaštite...

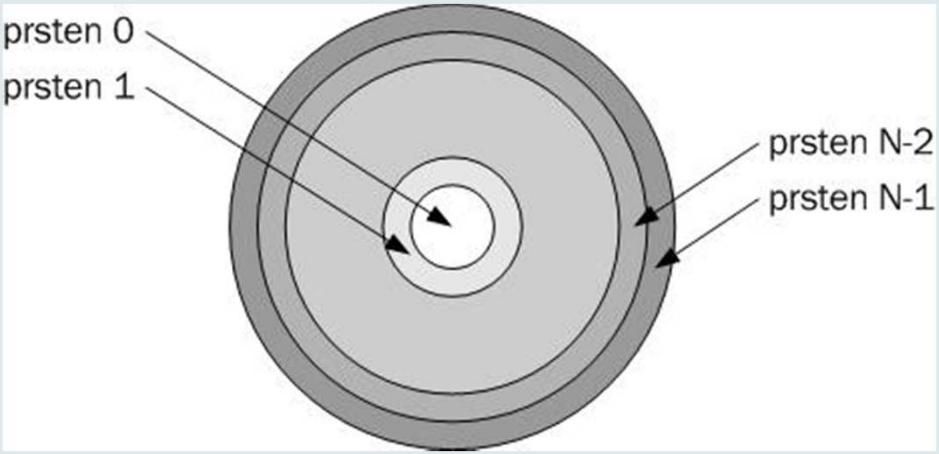
- Alokacija procesa u domene može biti statička ili dinamička, a sam domen može da se realizuje na različite načine:
  - svaki korisnik može biti domen,
  - svaki proces može biti domen i
  - svaka procedura može biti domen.

- Svaki sistem koji ima dva režima rada (korisnički i sistemski) mora da ima najmanje dva domena: **korisnički** i **sistemski**.

Domeni zaštite...

- U operativnom sistemu UNIX, domeni su definisani na **bazi korisnika** (domen = UID)
- Kod Multics sistema, domeni zaštite su organizovani hijerarhijski u kružne strukture – **prstenove**

Hijerarhijska organizacija domena – prstenovi zaštite



Matrica 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.

Primer matrice pristupa

Domen	Objekat			
	Datoteka F_1	Datoteka F_2	Datoteka F_3	Štampač
D_1	read		read	
D_2				print
D_3		read	execute	
D_4	read, write		read, write	

Proširenje matrice pristupa operacijom switch

Domen	Objekat							
	F_1	F_2	F_3	štampač	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch
D_3		read	exec					
D_4	read write		read write		switch			

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, što znači mogućnost da proces iz odgovarajućeg domena kopira pravo u drugi domen, to jest u drugo polje iste kolone.

  - **Kopiranje prava.** Proces u drugom domenu dobija kopiju prava i kopiju prava kopiranja; dato pravo se ne oduzima procesu koji obavlja operaciju copy;
  - **Prenošenje prava.** Proces u drugom domenu dobija kopiju prava i kopiju prava kopiranja; kopirano pravo se oduzima procesu koji obavlja operaciju copy;
  - **Ograničeno kopiranje.** Proces u drugom domenu dobija kopiju prava, ali ne dobija pravo kopiranja.

Primer operacije kopiranja prava

Domen	Objekat		
	F_1	F_2	F_3
D_1	execute		write*
D_2	execute	read*	execute
D_3	execute		

Domen	Objekat		
	F_1	F_2	F_3
D_1	execute		write*
D_2	execute	read*	execute
D_3	execute	read	

Prava

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

- **Pravo upravljanja** u domenu (engl. *control*). Operacije kopiranja, dodele i oduzimanja prava modifikuju sadržaj određene kolone u matrici. U matricu se uvodi i pravo upravljanja u domenu kojim je omogućena promena prava po vrsti. Pravo upravljanja se može dodeliti samo objektima koji predstavljaju domene (na primeru sledeće tabele, to su poslednje 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).

Vlasnik obavlja operaciju prenosa prava

Domen	Objekat		
	F_1	F_2	F_3
D_1	owner, exec		write
D_2		read*, owner	owner, write*
D_3	exec		

Domen	Objekat		
	F_1	F_2	F_3
D_1	owner, exec		
D_2		owner	owner, write*
D_3		read	write

Pravo upravljanja u domenu

- Pravo upravljanja u domenu (engl. *control*). Operacije kopiranja, dodele i oduzimanja prava modifikuju sadržaj određene kolone u matrici. U matricu se uvodi i pravo upravljanja u domenu (control) kojim je omogućena promena prava po vrsti. Pravo upravljanja se može dodeliti samo objektima koji predstavljaju domene (na primeru sledeće tabele, to su poslednje 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).

Pravo upravljanja u domenu

Domen	Objekat							
	F_1	F_2	F_3	printer	D_1	D_2	D_3	D_4
D_1	read		read			switch		
D_2				print			switch	switch control
D_3		read	exec					
D_4	read write		read write		switch			

Implementacija matrice prava pristupa

- Globalna tabela
- Lista za kontrolu pristupa objektima
- Lista mogućnosti domena
- Mehanizam ključeva

Globalna tabela

- Prvi i najprostiji slučaj je realizacija matrice pristupa pomoću globalne tabele koja se sastoji od skupa uređenih trojki (domen, objekat, skup prava).
- Pre 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 premašenje.

Lista za kontrolu pristupa objektima

- Matrica pristupa može se implementirati i pomoću liste za kontrolu pristupa objektima (engl. *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 podrazumevanih prava (engl. *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 određenim domenima jednostavno dodeliti ili oduzeti prava nad tim objektom. Pri određivanju ukupnih prava domena moraju se analizirati svi objekti.

Lista mogućnosti domena

- Treći način implementacije matrice pristupa jeste korišćenje liste mogućnosti domena. Lista mogućnosti (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 mogućnosti nisu najpodesnije za korišćenje, ali su pogodne za lokalizaciju informacija pri analizi prava domena.

Mehanizam ključeva

- Mehanizam ključeva (engl. *lock-key*) predstavlja kompromis prethodna dva načina implementacije matrice pristupa. Svakom objektu se dodeli 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 izmenom bitova koji čine bravicu.

Sigurnosni mehanizmi u operativnim sistemima

- Identifikacija korisnika operativnom sistemu
- Kontrola pristupa na nivou sistema datoteka
- Kriptografske mere zaštite
- Kontrola daljinskog pristupa
- Praćenje sigurnosnih događaja
- Izrada rezervnih kopija značajnih podataka
- Izrada plana restauracije

Rangovi sigurnosti

- Nacionalni centar za sigurnost računara (*The National Computer Security Center*, NCSC) osnovan je 1981. godine kao deo Nacionalne agencije za sigurnost (NSA) pri Ministarstvu odbrane SAD (DoD), kako bi pomogao pri zaštiti svojine i ličnih podataka u računarskim sistemima vlade, korporacija i kućnih korisnika. NCSC je definisao nekoliko rangova, tj. nivoa sigurnosti, kojima se može ukazati na stepen zaštite komercijalnih operativnih sistema, mrežnih komponenata i aplikacija. Ovo sigurnosno rangiranje, zasnovano na Kriterijumu ocene pouzdanih računarskih sistema Ministarstva odbrane (*Trusted Computer System Evaluation Criteria*, TCSEC), definisano je 1983. godine, i zove se "narandžasta knjiga" (*The Orange Book*).
- www.radium.ncsc.mil

Nivoi sigurnosti

- A1 – Verified Design (proverena arhitektura);
- B3 – Security Domains (domeni sigurnosti);
- B2 – Structured Protection (strukturirana zaštita);
- B1 – Labeled Security Protection (označena sigurnosna zaštita);
- C2 – Controlled Access Protection (zaštita kontrolisanim pristupom);
- C1 – Discretionary Access Protection (diskreciona zaštita pristupa);
- D – Minimal Protection (minimalna zaštita)

Primer: C2 rang

- U julu 1995. godine, Microsoft Windows NT 3.5 (radna stanica i server) sa Service Packom 3 bila je prva verzija Windowsa NT koja je zaslužila rang C2.
- Navodimo ključne zahteve koje operativni sistem mora da ispuni kako bi dobio rang C2:
  - Procedura sigurnog prijavljivanja na sistem (engl. *secure logon facility*)
  - Diskreciona kontrola pristupa
  - Praćenje sigurnosnih događaja (engl. *security auditing*)
  - Zaštita od ponovne upotrebe objekta

  Windows NT takođe zadovoljava dva zahteva sigurnosnog nivoa B

10.2. Sigurnost i zaštita operativnog sistema Linux

- Linus Torvalds je 1991. započeo rad na novom operativnom sistemu koji objedinjuje System V R4 i BSD UNIX standarde. Svoj rad je objavio na Internetu i podsticao je druge programere širom sveta da se priključe njegovom daljem razvoju.
- Linux je višekorisnički, višeprocesni operativni sistem sa potpunim skupom alata kompatibilnih sa UNIX-om, projektovan tako da poštuje relevantne POSIX standarde. Linux sistemi podržavaju tradicionalnu semantiku UNIX-a i potpuno implementiraju standardni UNIX-ov mrežni model. Linux je raspoloživ kao besplatan operativni sistem licenciran GNU Opštom javnom licencom (*GNU General Public Licence*, *GPL*). Izvorni kôd Linux sistema javno je dostupan i može se izmeniti tako da odgovara specifičnim potrebama. Linux se može slobodno distribuirati među korisnicima. Brojne profitne i neprofitne organizacije nude Linux u obliku različitih distribucija; distribucije Linuxa sadrže kolekciju CD ili DVD medijuma na kojima se nalaze operativni sistem, izvorni kôd, dokumentacija, i štampana uputstva za instaliranje i upotrebu sistema. Cene ovakvih distribucija su u većini slučajeva simbolične, osim ako se u distribuciji nalazi komercijalni softver ili je distribucija specifične namene.

Opšte razmatranje sigurnosti Linux sistema

- Prevođenje monolitnog jezgra sa odgovarajućim parametrima
- Čišćenje sistema od nepotrebnog softvera
- Sigurnost skriptova u direktorijumu /etc/init.d

Korisnički nalozi i lozinke

- Lozinke korisnika i *shadow* datoteka
- Korisnički nalog root
- Sistemski korisnički nalozi
- Program sudo

Sistemi datoteka i kontrola pristupa

- Podrazumevani vlasnički odnosi i prava pristupa
- Promena vlasničkih odnosa i prava pristupa
- Datoteke bez vlasnika
- SUID i SGID bitovi
- ext2/ext3 – specijalni atributi i indikator nepromenljivosti
- Datoteka /etc/fstab

Linux na mreži

- Datoteke /etc/hosts.allow i /etc/hosts.deny
- xinetd – praćenje aktivnosti i kontrola pristupa
- Datoteka /etc/exports
- Datoteke .rhosts
- Zaštita Apache Web servera
- „chroot jail“

Praćenje događaja i nadzor sistema

- Praćenje događaja – syslog alat
- Zaštita syslog servera
- Nadzor sistema – pregledanje dnevničkih datoteka

10.3 Sigurnost i zaštita operativnih sistema Windows

- Opšte o Windows 2000/XP/2003/Vista/W7 sigurnosti
  - Koliko je sve to zaista sigurno?

Korisnički nalozi, grupe i prava korisnika

- Korisnički nalozi (Windows XP)
- Prava dodeljena korisnicima
- Domenski korisnički nalozi i grupe
- Grupne polise i dodela prava korisnicima domena
- Delegiranje ovlašćenja u aktivnom direktorijumu

NTFS objekti i deljeni mrežni resursi

- Deljeni mrežni resursi

Praćenje događaja i pristupa resursima

- Praćenje pristupa resursima

Sigurnost operativnog sistema Vista

- DEP - Data Execution Prevention
- UAC - User Account Control

DEP

- **Data Execution Prevention** (DEP) is a security feature introduced in Windows XP, Windows Server 2003, Windows Vista, and Windows 7 that looks for malicious code trying to execute. If DEP's analysis of a process beginning execution makes DEP think the resulting code will cause some sort of unwanted activity, DEP intervenes and shuts the process down.

UAC

- **User Account Control** (UAC) is a new security component Windows Vista. UAC enables users to perform common tasks as non-administrators, called standard users in Windows Vista, and as administrators without having to switch users, log off, or use Run As. A standard user account is synonymous with a user account in Windows XP. User accounts that are members of the local Administrators group will run most applications as a standard user. By separating user and administrator functions while enabling productivity, UAC is an important enhancement for Windows Vista.

Literatura

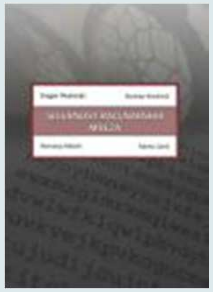
- D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: **"Sigurnost računarskih sistema i mreža"**, Mikro knjiga, Beograd, 2007., ISBN: 978-86-7555-305-2, knjiga – udžbenik
- www.conwex.info/draganp/books_SRSiM.html
- www.mikroknjiga.rs/store/prikaz.php?ref=978-86-7555-305-2

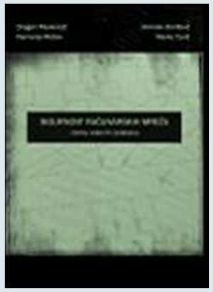
- Za predavanje 10:
  - Poglavlje 10: Sigurnost i zaštita operativnih sistema

Literatura - nastavak

- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-16-5, knjiga - udžbenik
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - priručnik za laboratorijske vežbe"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-49-1
- D. Pleskonjić, B. Đorđević, N. Maček, Marko Carić: **"Sigurnost računarskih mreža - zbirka rešenih zadataka"**, Viša elektrotehnička škola, Beograd, 2006., ISBN 86-85081-55-6

www.conwex.info/draganp/books.html





Dodatna literatura

- **Applied Cryptography**
  Bruce Schneier
  John Wiley & Sons, 1995

- **Cryptography and Network Security**
  William Stallings
  Prentice Hall, 1998

- **The CISSP Prep Guide – Mastering the Ten Domains of Computer Security**
  Ronald L. Krutz, Russell Dean Vines
  John Wiley & Sons, 2001

  Druge knjige i razni *online* resursi

- ***Napomena:*** tokom predavanja će biti naglašena dodatna literatura, po potrebi.

Pitanja

?