XI – Zaštita i sigurnost OS

S A D R Ž A J

11.1 Pojam zaštite i sigurnosti OS

11.2 Domeni zaštite i matrice prava pristupa

11.3 Aspekti sigurnosti

11.4 Autentifikacija korisnika

11.5 Programske i sistemske pretnje

11.6 Tehnike za povećanje sigurnosti sistema

11.7 Kriptografija

11.8 Rangovi sigurnosti

11.1 – Pojam zaštite i sigurnosti OS

- OS je osnovna komponenta većine savremenih računarskih sistema.
- Oni su usko povezani sa hardverom i softverom
- OS možemo posmatrati kao upravljač resursima (*resource manager*)
- Kontroliše pristup aplikacija memoriji i dodelu procesorskog vremena.
- Aplikacije se izvršavaju kao servisi na nivou operativnog sistema, a sama aplikacija ne zna detalje potrebne za razvoj sigurne aplikacije.
- OS je vrlo logično mesto za sprovođenje bezbedonosnih mera.
- Često se ne pravi razlika između termina «**sigurnost**» i «**zaštita**»
- Termin sigurnost se odnosi na celokupan problem bezbednosti sistema, a termin zaštita se odnosi na pojedinačni mehanizam OS koji se koristi
- Zaštita predstavlja kontrolu pristupa programa i korisnika resursima
- Sigurnost predstavlja mnogo širi pojam i ona obuhvata:
  - Neovlašćeni pristup podacima i resursima
  - Zlonamerne modifikacije podataka
  - Zlonamerno uništavanje podataka
  - Sprečavanje da se sistem koristi (***D**enial **o**f **S**ervice*)

11.1 – Pojam zaštite i sigurnosti OS

***Bezbednost OS se realizuje kroz odgovarajuću zaštitu četiri elemenata*:**

1. **Poverljivost** (**C***onfidentiality*) – sprečava ili minimizuje neovlašćeno pristupanje i objavljivanje podataka i informacija. Samo ako vlasnik nekih podataka odluči da dozvoli pristup svojim podacima nekoj grupi korisnika sistem bi trebao to da omogući, a istovremeno mora da obezbedi da neautorizivani korisnici ne mogu pristupiti tim podacima.
2. **Integritet** (**I***ntegrity*) - osigurava da se koriste samo pravi podaci. Neautorizovani korisnici ne bi trebali biti u stanju da modifikuju bilo kakve podatke bez vlasničke dozvole. Modifikacija uključuje ne samo promenu podataka već i brisanje i dodvanje lažnih podatka.
3. **Raspoloživost** (**A***vailability*) - svojstvo sistema ili sistemskog resursa da bude dostupan i upotrebljiv na zahtev autorizovanog sistemskog entiteta koji se vezuje za hardver, softver i podatke. To znači da niko ne može uticati na sistem da dođe u nestabilno stanje.
4. **Autentičnost** (*Authenticity*) - omogućava računarskom sistemu da proveri identitet korisnika koji koristi neki resurs.

11.1 – Pojam zaštite i sigurnosti OS

- Postoji potreba da OS onemogući neautorizovani pristup podacima
- Sigurnost i zaštita su usko vezani za fajl sistem pa je na osnovu toga potrebno onemogućiti pristup nekim fajlovima.
- Sigurnost se odnosi na opšti-filozofski pojam, dok zaštitu predstavljaju usvojeni principi sigurnosti koji se realizuju na nekom OS

Kada sigurnost fajl sistema može biti ugrožena?

1. viša sila (udar groma, požar, zemljotres...)
2. hardverska i softverska greška
3. ljudske greške

- Jedan od načina na koji se branimo od gubitka važnih podataka je pravljenje rezervnih kopija (*backup*)
- Pored ovih slučajnih postoje i namerni napadi na sigurnost fajl sistema. Lica koja žele pristupiti zabranjenim fajlovima mogu biti:

1. Laici - nisu zlobni ali ako im se pruži prilika da “zavire”u tuđu poštu ili pogledaju tuđi fajl to će i uraditi.
2. Eksperti - zaobilaženje mehanizama zaštite predstavlja izazov za njih
3. Špijuni - žele da izvuku materijalnu korist (prevarom, ucenom,...)

11.1 – Slabosti operativnih sistema

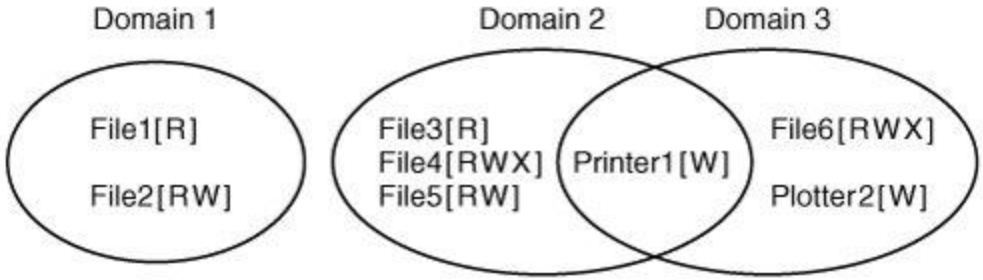
- **Nepravilna ulazna provera** - neophodno je pažljivo proveriti ulaze u softverske rutine, tj., izvršiti proveru ulaza (*input validation*). Provera se može odnositi na tip i broj parametara, ili jednostavno se osigurati da količina ulaznih podataka nije veća od dodeljenog bafera za smeštaj
- **Slabi kriptografski algoritmi** – OS koriste kriptografske algoritme za šifrovanje lozinki. Ako algoritam koji se koristi nije dovoljno jak, napadač može izvući „čistu“ lozinku iz njene šifrovane reprezentacije.
- **Slabi protokoli autentifikacije** - većina autentifikacionih sistema se zasniva na zajedničkoj tajni uključenih strana. Međutim, ostvarivanje bezbedne autentifikacione procedure je složen zadatak, posebno u distribuiranom okruženju.
- **Nesigurni „*Bootstraping*“** - sistem inicijalizacije je veliki sigurnosni problem u današnjim OS. Svi sistemi su ugroženi tokom podizanja.
- **Konfiguracione greške** – u OS bezbednosne funkcije i mehanizmi se retko aktiviraju inicijalno. Bezbedna „*out-of-the-box*“ instalacija je izuzetak pre nego pravilo pa vlasnik mora samostalno da podesi bezbedonosne parametre da bi postigao prihvatljiv nivo bezbednosti

11.1 – Sigurnosni ciljevi

1. **Procena** smatra se pripremom za ostale tri komponente, zato što je u vezi sa pravilima, procedurama, pravnom i drugom regulativom, određivanjem budžeta i drugim upravljačkim dužnostima, a povezana je sa tehničkom procenom stanja sigurnosti. Greška u proceni bilo kog od ovih elemenata, može naškoditi svim operacijama koje slede.
2. **Zaštita**, tj. sprećavanje ili prevencija, podrazumeva primenu protivmera kako bi se smanjila mogućnost ugrožavanja sistema. Ukoliko zaštita zakaže, primenjuje se sledeci korak - otkrivanje.
3. **Otkrivanje** predstavlja proces identifikacije upada, tj. povrede sigurnosnih pravila ili incidenata koji se odnose na sigurnost. Incident se definiše kao svaki nezakonit, neovlašcen ili neprihvatljiv postupak koji je preduzet, a odnosi se na računarski sistem ili mrežu.
4. **Odgovor** ili reakcija predstavlja proces oporavka, tj. lečenja posledica upada. U aktivnosti reakcije spadaju postupci: zakrpi i nastavi ili goni i sudi. Ranije se na prvo mesto stavljalo oporavljanje funkcionalnosti oštećenih resursa, kao što je korišćenje rezervnih kopija podataka za vraćanje sistema u stanje pre izvršenog napada.

11.2-Domeni zaštite i matrice pristupa

- Računarski sistem sadrži mnoge „objekte“ koji treba da budu zaštićeni.
- Ovi objekti mogu da budu hardver (procesori, memorijski segmenti, diskovni uređaji ili štampači), ili mogu da budu i softver (procesi, datoteke, baze podataka ili semafori).
- Svaki objekat ima jedinstveno ime preko koga mu se pristupa, i konačan skup operacija/prava po kojima mu proces može pristupati.
- Domen definiše skup objekata i sve operacije koje se mogu obaviti nad tim skupom pa on predstavlja skup parova (objekata, prava).
- Svaki korisnik, proces ili procedura može da bude domen
- Par specificira objekat i jedan podskup operacija koje se mogu izvršiti
- Pravo u ovom kontekstu, znači dozvolu da se izvrši jedna od operacija.
- Često jedan domen odgovara jednom korisniku, koji govori šta može a šta ne može korisnik da uradi,mada domen može biti i za više korisnika



11.2-Domeni zaštite i matrice pristupa

- Kada proces počne da se izvršava dodeli mu se domen i tada on može da pristupa samo objektima iz tog domena i to kako su prioriteti zadati.
- Oni koji dele domene sa vreme na vreme mogu menjati domen.
- Sistem vodi evidenciju koji objekat pripada kojem domenu pomoću matrice prava pristupa, sa vrstama koje predstavljaju domene i kolonama koje predstavljaju objekte.
- U svakom elementu matrice se nalaze prava pristupa, ako postoje, koje važe za dati objekat i domen.
- Na osnovu podataka iz matrice sistem može kazati kakav je pristup dozvoljen navedenom objektu u određenom domenu.

	Object							
	File1	File2	File3	File4	File5	File6	Printer1	Plotter2
Domain 1	Read	Read Write						
2			Read	Read Write Execute	Read Write		Write	
3						Read Write Execute	Write	Write

11.2-Domeni zaštite i matrice pristupa

- Nekada je potrebno omogućiti prebacivanje jednog procesa iz jednog u drugi domen
- Sama izmena domena može se lako uključiti u model matrice tako što će sam domen predstavljati objekat, sa operacijom ulazak u domen.
- Proces u domenu 1 može preći u domen 2, ali posle toga se ne može vratiti.

	Object										
Domain	File1	File2	File3	File4	File5	File6	Printer1	Plotter2	Domain1	Domain2	Domain3
1	Read	Read Write								Enter	
2			Read	Read Write Execute	Read Write		Write				
3						Read Write Execute	Write	Write			

Implementacija matrice prava pristupa

1. **Globalna lista** – sastoji se od skupa uređenih trojki (domen, objekat i prava pristupa). Prednost je centralizovanje zaštite na nivou sistema a nedostatak je sporost kao i veličina tabele koja može da bude velika.

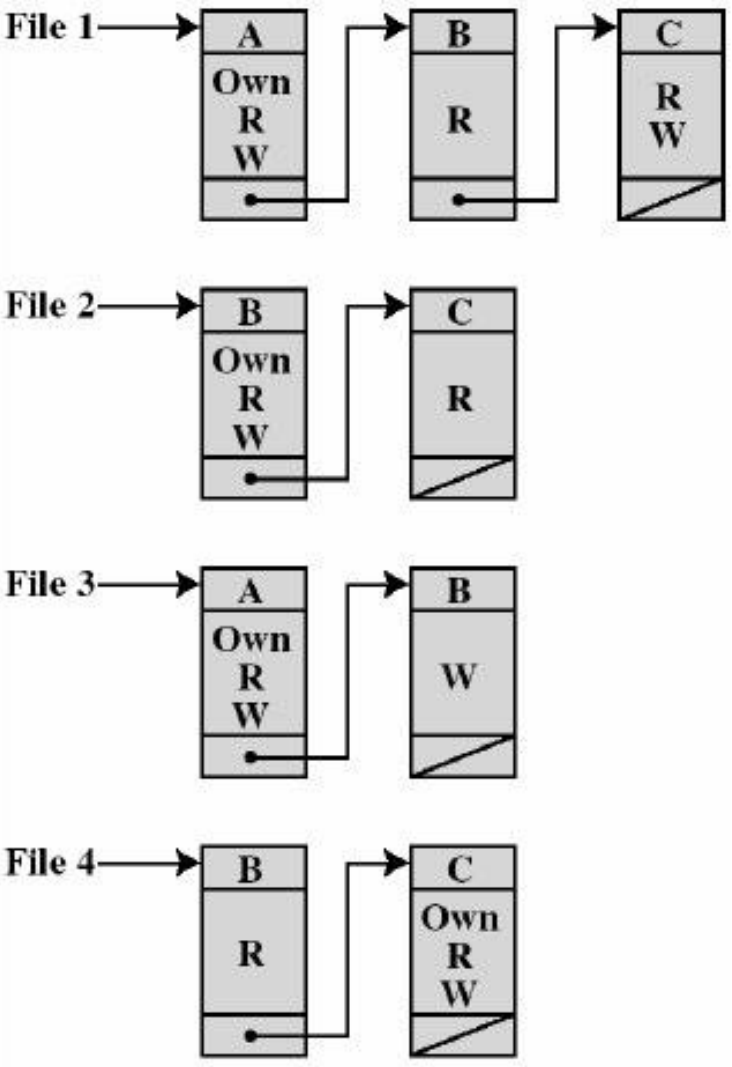
2. **Lista za kontrolu pristupa objektima** (*access list*) – formira se lista za svaki objekat (domen, skup prava) i ona odgovara jednoj koloni u matrici pristupa. Najpodesnije liste za korisnika.

3. **Lista mogućnosti domena** – za svaki domen se formira posebna lista koja prikazuje mogućnosti tog domena (objekat, prava pristupa). Sa korisničke strane ove liste nisu najpodesnije za korišćenje.

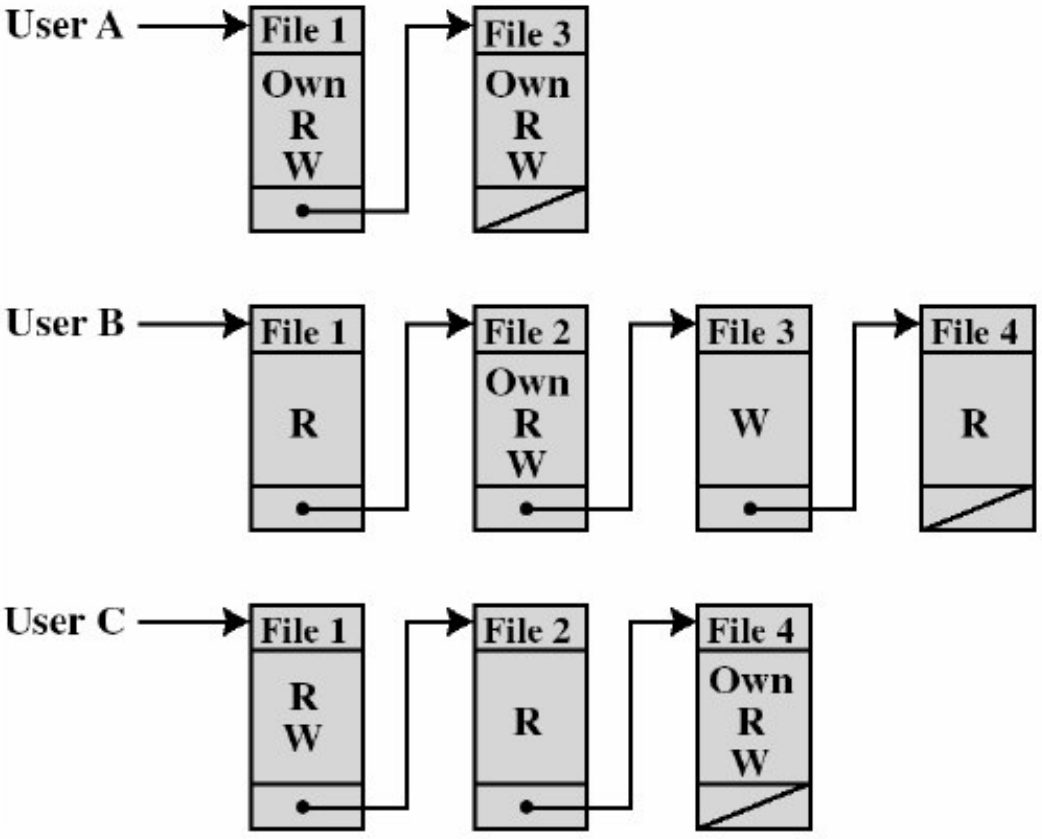
4. **Mehanizam ključeva** (*lock-key*) – predstavlja kompromis prethodne dve implementacije. Ovde se svakom objektu dodeli lista brava (*lock*) a svakom domenu lista ključeva (*key*).
   Proces iz domena može pristupiti objektu samo ako njegov ključ odgovara nekoj od brava koje poseduje taj objekat.

Implementacija matrice prava pristupa

Lista za kontrolu pristupa objektima (*access list*)



Lista mogućnosti domena

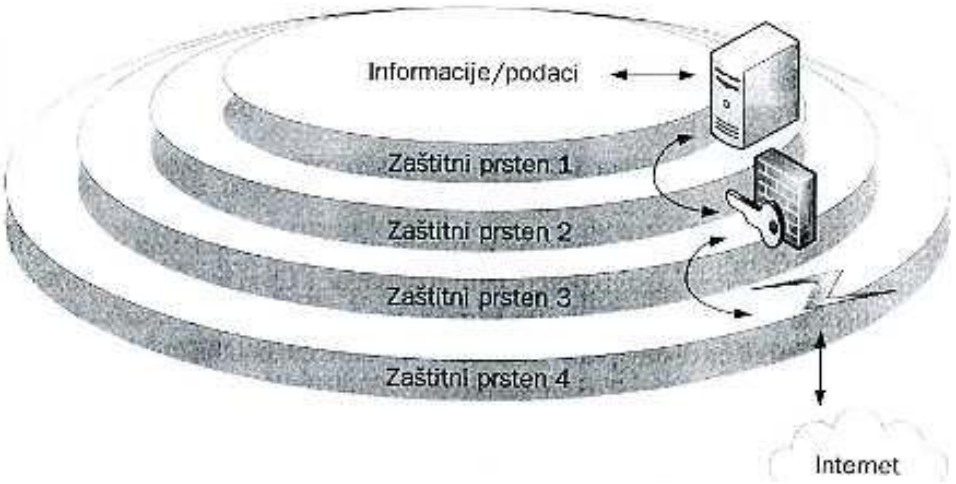


11.2-Domeni zaštite i matrice pristupa

- Jedna od najefikasnijih i najraširenijih strategija je slojevita zaštita.
- Zasniva se na formiranju zaštitnih slojeva (ili prstenova) oko sistema.
- Korisnik koji prolazi kroz slojeve zaštite mora da zadovoljiti dodatne sigurnosne mehanizme koji zadržavaju napadača ili minimizuju njegovu mogućnost pristupa kritičnim resursima.
- Slojevit pristup treba da obezbedi kombinaciju sigurnosnih mehanizama i tehničkih rešenja koji obuhvataju dovoljno široku lepezu sigurnosnih zahteva.
- Uz to, treba da onemogući da probijanje jednog sloja ima katastrofalne posledice po sigurnost celog sistema.
- Naime, verovatnoća da budu probijeni svi slojevi mnogo je manja od verovatnoće probijanja jednoslojne zaštite.

11.2-Domeni zaštite i matrice pristupa

Spoljašni sloj - sigurnosni mehanizmi su mrežne barijere (*firewalls)* i provera identiteta rutera i DNS servera. Ovom sloju zaštite odgovara demilitarizovana zona, tj. javno dostupan deo privatne mreže.



Treći zaštitni sloj štiti sistem od mreže u kojoj se nalazi. Poseduje mehanizme PKI (infrastruktura javnih ključeva), VPN i mrežne barijere. **Drugi sloj** implementira CIA(*cofidentiality,integrity,availibility)* koncepte koristeći mehanizme na sistemskom nivou.Mehanizmi su implementirani na radnim stanicama, serverima ili *mainframe* računarima na nivou OS. **Unutrašnji sloj** štiti informacije i podatke koji se čuvaju na sistemu. U sigurnosne mehanizme spadaju kontrola pristupa na aplikativnom nivou (lozinke ili drugi načini provere identiteta), kontrola pristupa podacima na osnovu matrice pristupa, šifrovanje i digitalno potpisivanje podataka, praćenje (*auditing)* operacija i objekata koji su pristupili sistemu

11.3 – Aspekti sigurnosti

1. **Fizički nivo** – potrebno je fizički obezbediti resurse (vatra, poplava, krađe, ...)
2. **Ljudski faktor** – administratori treba da budu poverljive i ozbiljne osobe. Uspešan napad na sistem u mnogome zavisi od ovog faktora.
3. **Mrežni nivo** – obezbeđivanje udaljenog pristupa resursima, zaštitu resursa od neovlašćenog korišćenja, zlonamerne izmene i/ili uništenja podataka, sprečavanje ulaska virusa i drugih zlonamrenih programa.
4. **Nivo OS** – uključuje mehanizme zaštite: autentifikacija (provera identititeta korisnika) i autorizacija (dodeljivanje prava korisnicima tj. kontrola pristupa na nivou datoteka)

11.4 – Autentifikacija korisnika

- Mnoge zaštitne šeme su bazirane na pretpostavkama da sistem proverava identitet svakog korisnika koji želi da koristi sistem.
- Problem identifikacije korisnika kada se prijavljuju na sistem se naziva autentifikacija korisnika.

Većina autentifikacionih metoda su bazirane na:

1. nečemu što korisnik zna - navođenje poverljivih informacija(lozinka)
2. nečemu što korisnik ima - specijalan hardver (ključ ili ID kartica)
3. nečemu što je korisnik - biološki atributi korisnika (otisak prsta, snimak mrežnjače oka, potpis, izgled lica, glas i td.

- Na Internetu postoji posebna metoda identifikacije koja podrazumeva korišćenje sertifikata (X.509)
- Lozinke predstavljaju najranjivije mesto pa su jedan od omiljenih objekata koje zlonamerni napadači koriste za narušavanje sigurnosti
- Lozinke se mogu lako pogoditi ako su jednostavne i kratke, nehotično otkriti potencijalnom napadaču (putem neobaveznih pitanja, E-mail-a) kao i namerno ilegalno proslediti neovlašćenim korisnicima

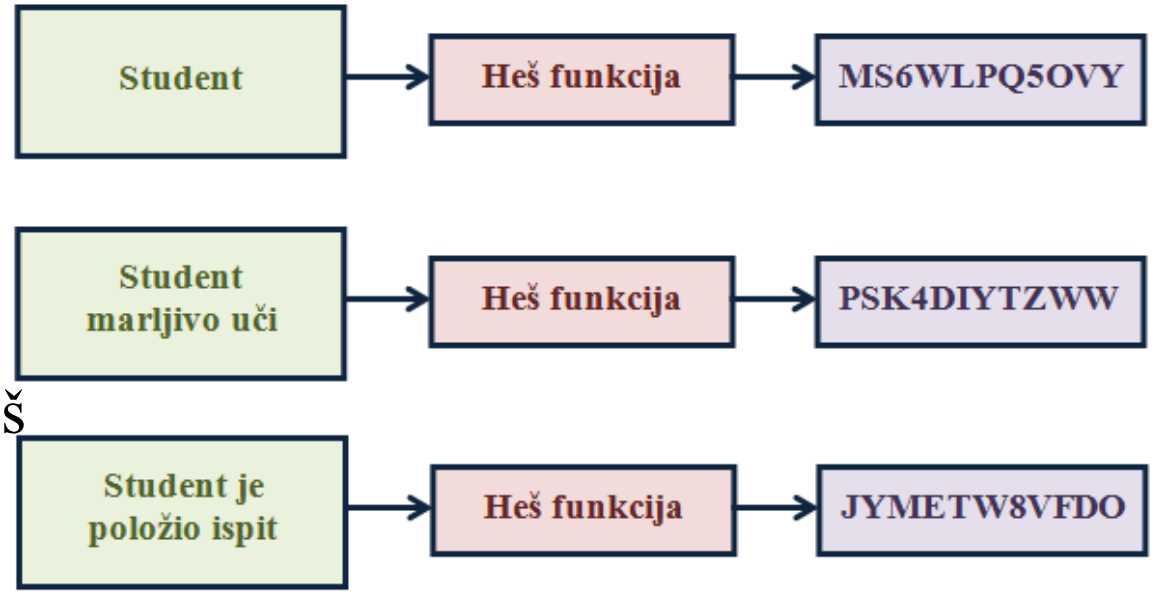
11.4 – Autentifikacija korisnika

- Problem čuvanja informacija o lozinkama rešava se šifrovanjem
- Jednosmerne **heš funkcije** koriste se za čuvanje podataka o lozinkama
- Ulazna poruka je promenljive dužine,ali broj heš bajtova uvek je fiksan

Smeštanje lozinke na disk obavlja se na sledeći način:

1. korisnik unosi novu lozinku l_a
2. operativni sistem računa heš vrednost unete lozinke: $h_a=h(l_a)$
3. dobijena vrednost se smešta na disk u odgovarajuću tabelu koju čine uređeni parovi (*korisničko ime , heš vrednost*)

- Svaki sledeći put kada želi da se prijavi, korisnik navodi korisničko ime i lozinku. Sistem računa heš unete lozinke $h_b=h(l_b)$, u tabeli traži odgovarajući heš
- Ako je $h_a=h_b$ korisnik je autentifikovan



11.4 – Autentifikacija korisnika

Osnovna pravila koja treba poštovati kod lozinki:

- ✓ čuvati poverljivost lozinki,
- ✓ ne beležiti lozinke na papir,
- ✓ lozinke se ne smeju odavati drugim korisnicima, čak ni administratorima, odgovornim osobama i sl.,
- ✓ korisnici ne smeju menjati lozinke ukoliko sumnjaju na nepravilnosti u radu servisa
- ✓ birati kvalitetne lozinke, duge minimalno 6 znakova, da nisu vezane uz imena, datume, telefonske brojeve i sl.,
- ✓ lozinke moraju sadržati različite oznake: brojeve, mala i velika slova, i ako je moguće i specijalne znakove,
- ✓ izbegavati ponovnu uptrebu starih lozinki,
- ✓ izbegavati lozinke koje već koriste na drugim sistemima,
- ✓ redovno periodično menjati lozinke itd.

11.5 – Napadi na sistem

- **Odbijanje usluga (*Denial of Service*) –** izaziva prestanak rada servisa a izaziva se ometanjem nekog servisa koji se izvršava na računaru žrtve -slanje velikog broja *Syn* paketa može ugušiti rad nekog računara
- **Lažiranje DNS-a –** napadač prati IP pakete i predstavlja se kao drugi računar zamenom IP adresa. Kako DNS servis ne proverava pakete moguće je predstaviti se DNS-u kao računar od poverenja
- **Smurf –** napadač svima na mreži šalje poruku **ICMP ECHO REQUEST** a kao odredišnu adresu navodi IP adresu potencijalne žrtve.
- **Njuškanje –** specijalnim programom (*sniffer*) presreću se TCP/IP paketi (nisu šifrovani) i njihov sadržaj se pregleda (očitava).
- **Skeniranje priključka –** pretražuje otvorene priključke (*port*) na potencijalnom računaru žrtve (šalju se SYN ili FIN paketi). Ukoliko se dobije odgovor RTS to znači da su ti portovi neaktivni.
- **Smrtonosni ping (*Ping of Death*) –** napadač šalje veliki broj **ICMP REQUEST** paketa potencijalnoj žrtvi sa namerom da obori OS.

11.5 – Programske i sistemske pretnje

- **Virus** predstavlja program koji može da zarazi druge programe, modifikujući ih tako da uključe njegovu kopiju, koja takođe može biti modifikovana.
- Pod infekcijom (zarazom) se ovde misli na mogućnost virusa da se samostalno izvršava prilikom pokretanja zaraženog programa.
- Ova definicija ključna je za određivanje virusa jer ne smatramo svaki maliciozni program virusom, drugim rečima nije svaki destruktivni program virus, jer bi u tom slučaju i program Format bio virus.
- Struktura virusa može se najlakše podeliti na tri komponente, od kojih virus mora obavezno imati samo prvu.

1. **Prva komponenta** predstavlja mogućnost infekcije. Dakle nije nužno da virus radi bilo kakvu štetu na računaru, sama činjenica da se širi infekcijom dovoljna je da se okarakteriše kao virus.
2. **Drugi deo virusa**,koji nije obavezan,predstavlja nosivu komponentu. Ona definiše sve aktivnosti koje će biti izvedene uz njegovo širenje.
3. **Treći deo** predstavlja funkcija za okidanje koja definiše vreme ili događaj prilikom koga će biti izvršena nosiva komponenta virusa.

11.5 – Programske i sistemske pretnje

- **Crv** je program koji se širi samoumnožavanjem kroz računare. Crv je samostalan i za razliku od virusa ne treba mu program domaćin da bi radio. Takođe, crva u ″pogon″ pušta i kontroliše sam autor.
- **Logička bomba** je metoda aktiviranja procesa na osnovu ispunjavanja nekog logičkog uslova: postojanja ili nepostojanja nekog podatka, nekog protoka podataka, određenog vremena ili u određeno vreme i sl. Logička bomba u stvari predstavlja princip rada, a ne neki mehanizam. Logičke bombe su često sastavni deo mnogih računarskih virusa.
- **Trojanski konj** je program koji naizgled služi za neku drugu operaciju od one za koju je napravljen. Trojanski konj bi recimo bio program koji izgleda kao tekst procesor, a zapravo jednom pokrenut formatira hard disk. Mnogi autori virusa koriste trojanske konje.
- **Klopka (*trap door*)** predstavlja posebnu nedokumentovanu funkciju programa koja se može pokrenuti na unapred određen način. Programeri koji pišu različite programe često znaju da predvide posebnu lozinku ili sekvencu znakova koja kada se unese omogućava pristup do inače nevidljivih funkcija programa.

11.6–Tehnike za povećanje sigurnosti sistema

- Koncept multiprogramiranja uvodi deljenje resursa između korisnika.
- Ovo uključuje deljenje memorije, ulazno/izlaznih uređaja, i podataka.
- Mogućnost deljenja ovih resursa uvodi potrebu za zaštitom.

Operativni sistem može ponuditi zaštitu iz sledećeg spektra:

1. **Bez zaštite** (*No Protection*) - ovo je odgovarajući način kada se osetljive procedure izvršavaju u posebnim vremenskim intervalima;
2. **Izolacija**(*Isolation*)–podrazumeva da svaki proces radi odvojeno od drugih procesa. Svaki proces ima sopstveni adresni prostor i fajlove.
3. **Deliti sve ili ništa** (*Share all or Share Nothing*) - u ovoj metodi, vlasnik objekta određuje da li će objekat biti javan ili privatan.
4. **Deoba preko ograničenja pristupa** (*Share via Access Limitation*) - OS proverava dozvole pristupa objektu za određenog korisnika; radi kao međusloj između korisnika omogučući samo ovlašćene pristupe
5. **Dinamička deoba** (*Share via Dynamic Capabilities*) - omogućava dinamičko kreiranje dozvola za deljene objekte.
6. **Ograničenje korišćenja objekta** (*Limit use of an object*) - ograničava ne samo pristup objektu, već i način na koji se objekat može koristiti.

11.6-Tehnike za povećanje sigurnosti sistema

1.Identifikacija korisnika OS - zahteva se da svaki korisnik koji pristupa sistemu ima važeće korisničko ime na sistemu i odgovarajuću lozinku.

2.Kontrola pristupa na nivou sistema datoteka - u listama za kontrolu pristupa navedeno je ko može da pristupi određenoj datoteci ili direktorijumu i šta sa tom datotekom ili direktorijumom može da radi.

3.Kriptografske mere zaštite - svaki podatak na računaru može se zaštititi šifrovanjem koje može biti na nivou datoteka i na nivou drajvera.

4.Kontrola daljinskog pristupa - svaki OS treba da ima mrežnu barijeru koja će filtrirati podatke na mrežnom/transportnom sloju a poželjno je da OS obezbedi podršku za rad sa kriptografskim protokolima (SSL, IPSec).

5.Praćenje sigurnosnih događaja – potrebno je da OS formira dnevnike događaja(*log file*) za sigurnosne događaje:promena sadržaja ili pristupnih prava direktorijuma, promena polise, prijavljivanje na sistem, pravljenje ili izmena korisničkih naloga, pristup objektima aktivnog imenika.

6.Izrada rezervnih kopija podataka kao najbitniji segment zaštite

7.Izrada plana restauracije – u slučaju nepredviđenih događaja.

11.7 – Kriptografija

- Obuhvata matematičke postupke izmene podataka takve da šifrovane podatke mogu pročitati samo korisnici sa odgovarajućim ključem
- Dva su osnovna matematička postupka:
  1. **Supstitucija** - zamena delova orignalne poruke
  2. **Permutacija** - preuređenje originalne poruke
- Mehanizam šifrovanja čine sledeće komponente: skup ključeva K, skup poruka M, skup šifrata C, funkcija šifrovanja E(M,K)->C i funkcija dešifrovanja D(C,K)->M
- **Simetrični kriptoalgoritmi -** isti ključ i za šifrovanje i za dešifrovanje
- **Kriptoalgoritmi sa javnim ključem** – podaci se šifruju javnim ključem a dešifruju tajnim tj. privatnim ključem
- **Digitalni potpis** – elektronska verzija potpisa kojom se identifikuje pošiljalac ili vlasnik neke poruke ili dokumenta
- **Sertifikati** – sigurnosna transformacija može biti šifrovanje s javnim ključem, a lice od poverenja neka ustanova koja će učesnicima u komunikaciji distribuirati javne ključeve i obezbeđivati potvrdu usaglašenosti identiteta učesnika i ključa pomoću sertifikata (X.509)

11.8 – Rangovi sigurnosti

- Nacionalni centar za sigurnost računara (*National Computer Security Center*) kako bi pomogao pri zaštiti svojine i ličnih podataka u računarskim sistemima vlade, korporacija i kućnih korisnika definisao je nekoliko rangova, odnosno nivoa sigurnosti koji su:
  1. A1 - Verified Design (proverena arhitektura),
  2. B3 - Security Domains (domeni sigurnosti),
  3. B2 - Structured Protection (struktuirana zaštita),
  4. B1 - Labeled Security Protection (označena sigurnosna zaštita),
  5. C2- Controlled Access Protection (zaštita kontrolisanim pristupom),
  6. C1 - Discretionary Access Protection (diskreciona zaštita pristupa),
  7. D - Minimal Protection (minimalna zaštita).

Ključni zahteve koje OS mora da ispuni kako bi dobio rang C2:

- ✓procedura sigurnog prijavljivanja na sistem – jedinstvena identifikacija
- ✓diskreciona kontrola pristupa – vlasnik određuje prava na svom resursu
- ✓praćenje sigurnosnih događaja – njihovo otkrivanje i snimanje
- ✓zaštita od ponovne upotrebe objekata koja sprečava korisnike da vide podatke koje je drugi korisnik već obrisao ili ne dozvoljava pristup memoriji koju je drugi korisnik upotrebio i oslobodio.

Hvala na pažnji !!!

Pitanja

? ? ?