ZSIS sažetak za međuispit

# Uvod

*Informacijski sustav je bilo koji organizirani sustav za prikupljanje, organizaciju, pohranu i razmjenu informacija.*

Neke posljedice/zanimljivosti definicije

* Informacijski sustav ne uključuje nužno računala i/ili računalnu mrežu
* Iako su današnji informacijski sustavi nezamislivi bez računala
* Informacijski sustav uključuje i ljude i procese

*Informacijska tehnologija (IT) je primjena računala i telekomunikacijske opreme za pohranu, dohvat, prijenos i obradu podataka, često u poslovnom kontekstu*.

Sigurnost (engl. security) - **kontinuirani proces** čijim provođenjem se osigurava određeno

**stanje** (sustava i/ili podataka/informacija). Željeno stanje je definirano određenim **zahtjevima**.

Kada su zahtjevi ispunjeni, kažemo da je sustav i/ili informacija sigurna. Ako neki od zahtjeva nije ispunjen, kažemo da se dogodio **incident**, odnosno, da je **narušena sigurnost**.

## Osnovni sigurnosni zahtjevi

Bez obzira o kojoj sigurnosti govorimo i dalje su bitni sigurnosni zahtjevi

Tri su temeljna zahtjeva:

* Tajnost/Povjerljivost (engl. secrecy, confidentiality)
* Cjelovitost/Integritet (engl. integrity)
* Raspoloživost (engl. availability)

Dodatni zahtjevi

* Autentičnost (engl. autenticity)
* Neporecivost (engl. non-repudation)

## Prijetnje i ranjivosti

Da bi se dogodio incident moraju postojati dva preduvjeta: *ranjivost* i *prijetnja*

*Ranjivost* (engl. vulnerability) je pogreška ili slabost u dizajnu sustava, implementaciji, upotrebi ili upravljanju koja se može iskoristiti za narušavanje sigurnosti sustava ili informacije.

* Pogreške u programskoj podršci (engl. bugs), propusti u protokolima, kriva upotreba programske podrške ili nekog sustava

*Prijetnja* (engl. threat) je bilo kakav događaj koji može iskoristiti ranjivost te na taj način prouzročiti štetu.

* Izvori prijetnji su ljudski (napadači) ili prirodni (potres, nestanak struje);
* Dodatno ljudski izvori mogu biti namjerni (napadači) ili slučajni (nepažnja osobe)

## Načini postizanja sigurnosti

Pojedinu zaštitu koju primjenjujemo kako bi postigli sigurnost nazivamo **kontrola** (engl. control)

Sve kontrole su razvrstane u tri velike grupe:

* Fizičke kontrole
  + Kamere, zaštitari, blindirana vrata, …
* Tehničke kontrole
  + Kriptografija, vatrozidi, sustavi za detekciju napada, …
* Administrativne kontrole
  + Politike, pravilnici, itd.
  + Različiti propisi kojima definiramo što znači biti siguran, kako se ljudi moraju ponašati, kako uređaji moraju biti podešeni, …

# Sigurnost u mreži

**Složenost problema**

* velik broj dobavljača i aplikacija
* preklapanje odgovornosti
* obrana na više razina

*ranjivost* - slabost u izvedbi sustava koju je moguće iskoristiti kako bi se izazvala šteta

*prijetnja* - skup okolnosti koji može nanijeti štetu

*napad* - postupak u kojem se iskorištava ranjivost sustava

*nadzor* - mjere predostrožnosti

prijetnja se sprječava nadzorom ranjivosti

## Vrste napada

*presretanje:*

* prisluškivanje (eavesdropping), nadzor mrežne komunikacije (link monitoring)
* snimanje mrežnog prometa (packet capturing), kompromitacija sustava (system compromisation)
* teško izbjeći kod bežične komunikacije i višeodredišnog i grupnog razašiljanja

*promjena:*

* mijenjanje zapisa u bazi podataka, kompromitiranje sustava
* zlonamjerno iskorištavanje zastoja u komunikaciji, promjena sklopovske podrške

*ubacivanje lažne informacije*

* dodavanje novih zapisa u bazu podataka, ubacivanje IP-datagrama u mrežu (IP spoofing)
* lažne elektroničke poruke, lažna Web-sjedišta

*prekidanje komunikacije*

* uništavanje sklopovlja, fizičko uništavanje komunikacijskih medija
* ometanje komunikacije (šum), narušavanje tablica usmjeravanja
* brisanje programa ili datoteka, uskraćivanje usluge

## Izvori napada

*iznutra*:

* iz sustava i korisnika koji su pod nadležnošću administratora
* autorizirani korisnici - saboteri
* većinom slučajne greške, šteta nije zanemariva!
* zloupotreba ovlasti kod administratora, djelatnici koji imaju pristup sustavu ali nisu zaduženi za uslugu

*izvana*:

* kriminalne ili terorističke organizacije, obavještajne službe
* komercijalne tvrtke (industrijska špijunaža), istražiteljske agencije, državne agencije

## Osnovni sigurnosni zahtjevi

*autentifikacija (authentification)*

* potvrda autentičnosti korisnika; odgovarajuće metode primjenjuju se ovisno o aplikaciji i uslugama koje ih koriste

*neporecivost (nonrepudiation)*

* sudionici ne mogu odbiti ili poreći akciju u kojoj su sudjelovali npr slanje i primanje informacija

*cjelovitost, integritet (integrity)*

* garancija da su informacije poslane, primljene ili pohranjene u izvornom i nepromijenjenom obliku
* samo ovlaštenim osobama dopušteno je pisanje, promjena, promjena statusa, brisanje, stvaranje, kašnjenje ili ponavljanje podataka

*kontrola pristupa (access control)*

* ograničavanje pristupa informacijama i ograničavanje provođenja akcija

*raspoloživost ( availability)*

* informacije moraju biti raspoložive, a sustavi i usluge u stanju operativnosti, usprkos mogućim neočekivanim i nepredvidljivim događajima, primjerice nestanku struje, prirodnim nepogodama, nesrećama i zlonamjernim napadima

*povjerljivost (confidentiality)*

* zaštita komunikacije ili pohranjenih informacija od presretanja i stavljanja na uvid neovlaštenim osobama

# Kriptografija

* omogućuje komunikaciju dviju stranki preko nesigurnog komunikacijskog kanala - treća stranka ne može razumjeti njihove poruke

postupak:

1. šifriranje: transformira se otvoreni tekst (*plaintext*) koristeći unaprijed dogovoreni ključ (*key*)
2. rezultat dobiven šifriranjem naziva se šifrat (*ciphertext*) ili kriptogram
3. pošiljatelj pošalje šifrat preko komunikacijskog kanala

## terminologija

kriptoanaliza ili dešifriranje - znanstvena disciplina koja se bavi proučavanjem postupaka za čitanje skrivenih poruka bez poznavanja ključa

kriptologija - grana znanosti koja obuhvaća kriptografiju i kriptoanalizu

kriptografski algoritam ili šifra - matematička funkcija koja se koristi za šifriranje i dešifriranje

* općenito, radi se o dvije funkcije, jednoj za šifriranje, a drugoj za dešifriranje
* njezini argumenti su ključ i otvoreni tekst, odnosno ključ i šifrat

anonimna komunikacija

steganografija

## Ključ

* matematički algoritam - određuje kako se šifrira otvoreni tekst
* složenost ovisi o duljini ključa - broj bitova
* ključ duljine n bitova generira prostor ključeva od 2n mogućih vrijednosti

matematički algoritmi - tajni i javni

snaga sustava za šifriranje počiva na ključu

* napadač može imati šifrirane tekstove i znati algoritme, ranjivost sustava ovisi o snazi ključa
* dulje ključeve teže je probiti (vrijeme, novac)

## Savršeno sigurne šifre

savršeno sigurne šifre:

dva uvjeta moraju biti zadovoljena

* šifrat ne otkriva nikakav podatak o tome na temelju kojeg je otvorenog teksta mogao nastati
* otvoreni tekst ne otkriva nikakav podatak o tome koji će šifrat od njega nastati

praktički sigurne šifre:

jedan ili oba uvjeta moraju biti zadovoljena:

* trošak razbijanja šifre brzo nadmašuje vrijednost šifrirane informacije
* vrijeme potrebno za razbijanje šifre nadilazi iskoristivo vrijeme važenja šifrirane informacije

pretpostavka: pod uvjetom da novi i brži načini razbijanja šifre nisu na pragu otkrivanja

## Vrste kriptografija

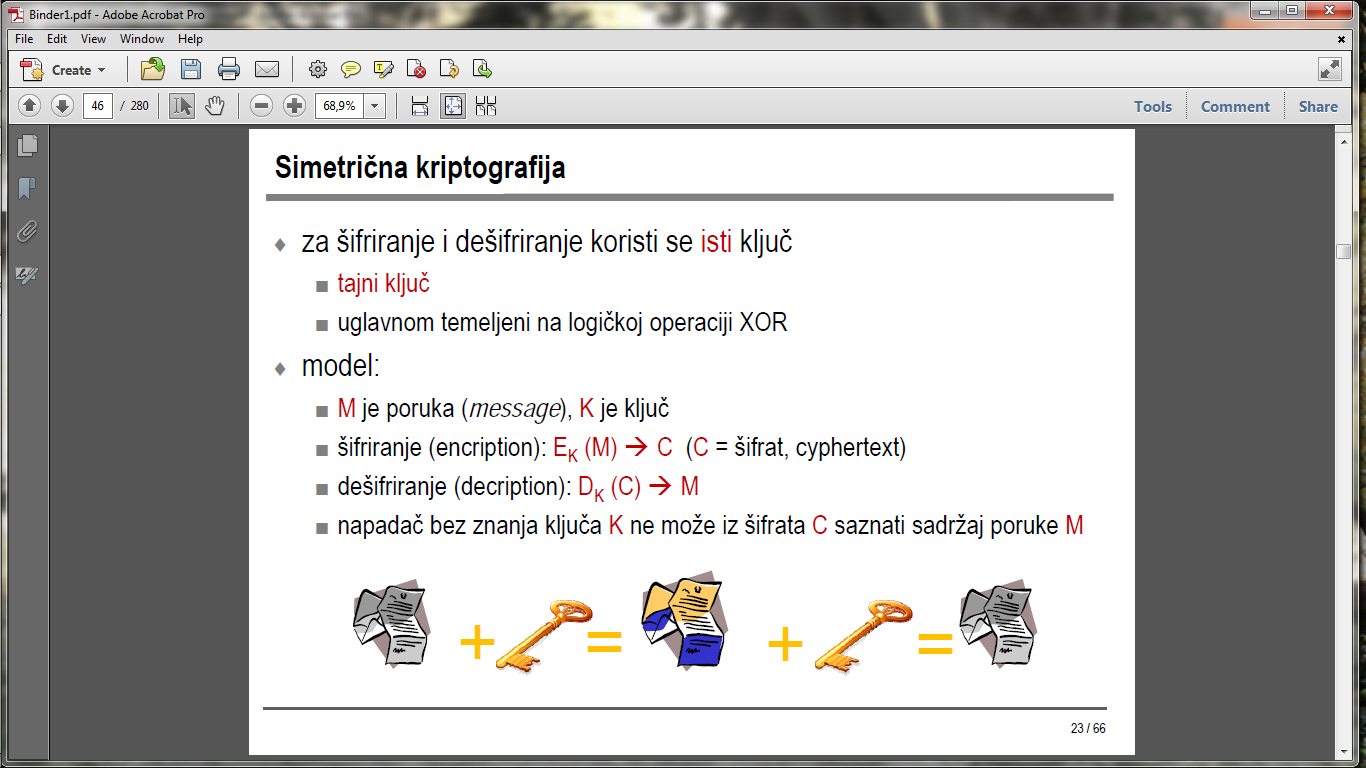
* s obzirom na broj ključeva
  + bez ključeva: hash-funkcije
  + jedan ključ: simetrična kriptografija - tajni ključ
  + dva ključa: asimetrična kriptografija - privatni i javni ključ
* s obzirom na način šifriranja
  + tokovi (stream)
  + blokovi (block)

### Simetrična kriptografija

* za šifriranje i dešifriranje koristi se isti (tajni) ključ

model:

* M je poruka (*message*), K je ključ
* šifriranje (encription): EK (M) C (C = šifrat, cyphertext)
* dešifriranje (decription): DK (C)  M
* napadač bez znanja ključa K ne može iz šifrata C saznati sadržaj poruke M



dužina ključa naznačuje koliko će trebati da se napadom razbije šifra (3DES - trostruki DES, International Data Encryption Algorithm (IDEA, 128 bita), Advanced Encryption Standard (AES, 128, 192, 256 bita), Blowfish (varijabilni ključevi, do 448 bita), CAST (Carlisle Adams & Stafford Tavares, 128, 256 bita) )

### Asimetrična kriptografija

problemi u simetričnoj kriptografiji:

* razmjena ključeva
* nemogućnost digitalnog potpisivanja

asimetrično:

* jedan ključ za šifriranje, drugi ključ za dešifriranje - ključevi su međusobno vezani
* neizvedivo je poznavajući algoritam i jedan ključ otkriti drugi
* često: svejedno je kojim ključem se šifrira, a kojim dešifrira (rade isključivo u paru)
* poznavanjem javnog ključa ne može se izračunati tajni ključ u nekom razumnom vremenu
* vrijeme potrebno za izračunavanje tajnog ključa iz poznatog javnog ključa, tj. razbijanje šifre, mjeri se milijunima godina na danas najjačim raspoloživim računalima

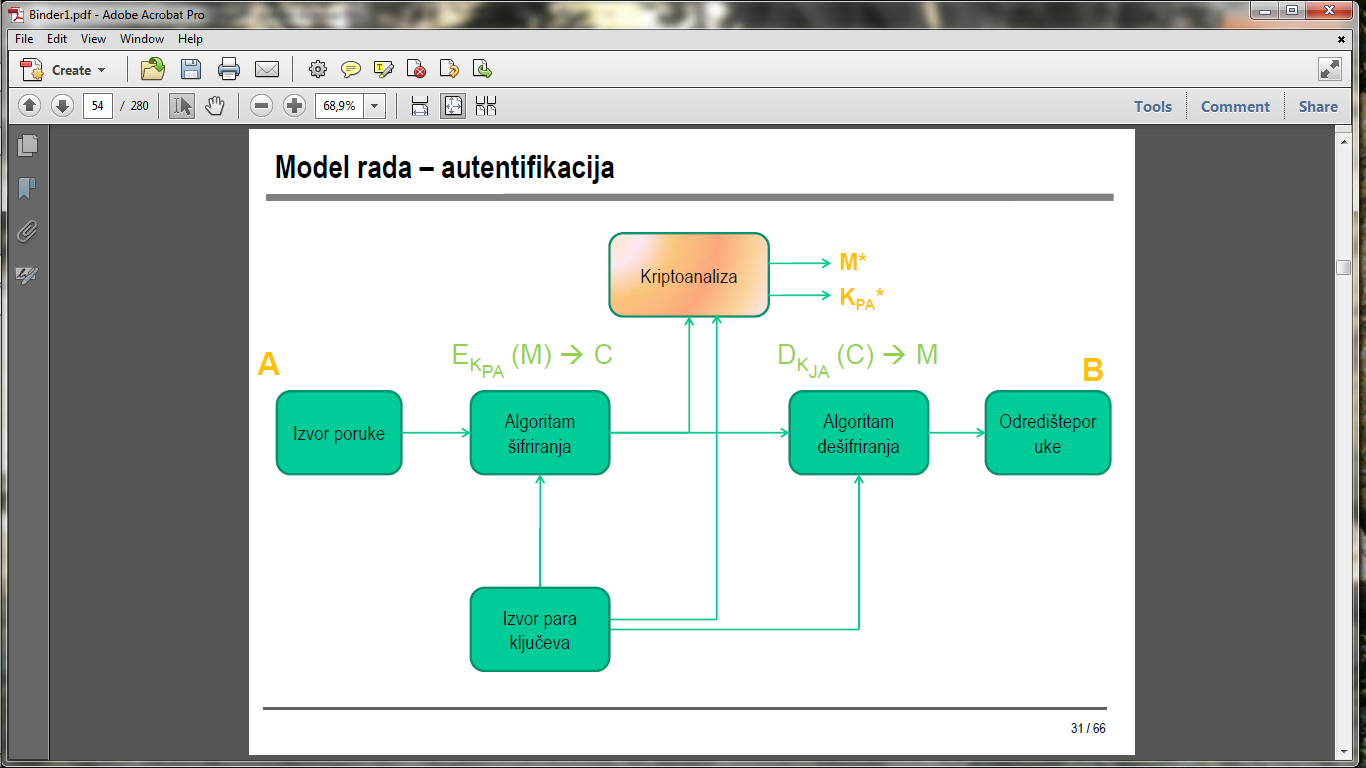
svaki korisnik ima par ključeva:

* privatni ključ KP  (dostupan isključivo korisniku, ne smije se distribuirati!)
* javni ključ KJ (dostupan svima, mora se distribuirati)
* ono što se šifrira javnim ključem, može se dešifrirati samo privatnim:

EKJ ( M) -> C, DKP ( C) -> M

* ono što se šifrira privatnim ključem, može se dešifrirati samo javnim:

EKP (M) -> C, DKJ (C) -> M



* osjetljiva na *brute-force* napad - protumjera: dulji ključ
* problem: matematički izračuni -složenost ne mora rasti linearno s brojem bita
* duljina ključa mora biti: - dovoljno velika da spriječi napad, dovoljno mala da se operacije obavljaju brzo
* napadi pogađanjem poruke
* računanje privatnog ključa na temelju javnog - nije dokazano da nije moguće, svi algoritmi su sumnjivi

### Hibridni pristup

dobre strane simetričnih algoritama:

* 100-1000 puta brži od asimetričnih
* manje računalno zahtjevni

dobre strane asimetričnih algoritama:

* upravljanje ključevima, distribucija i tajnost

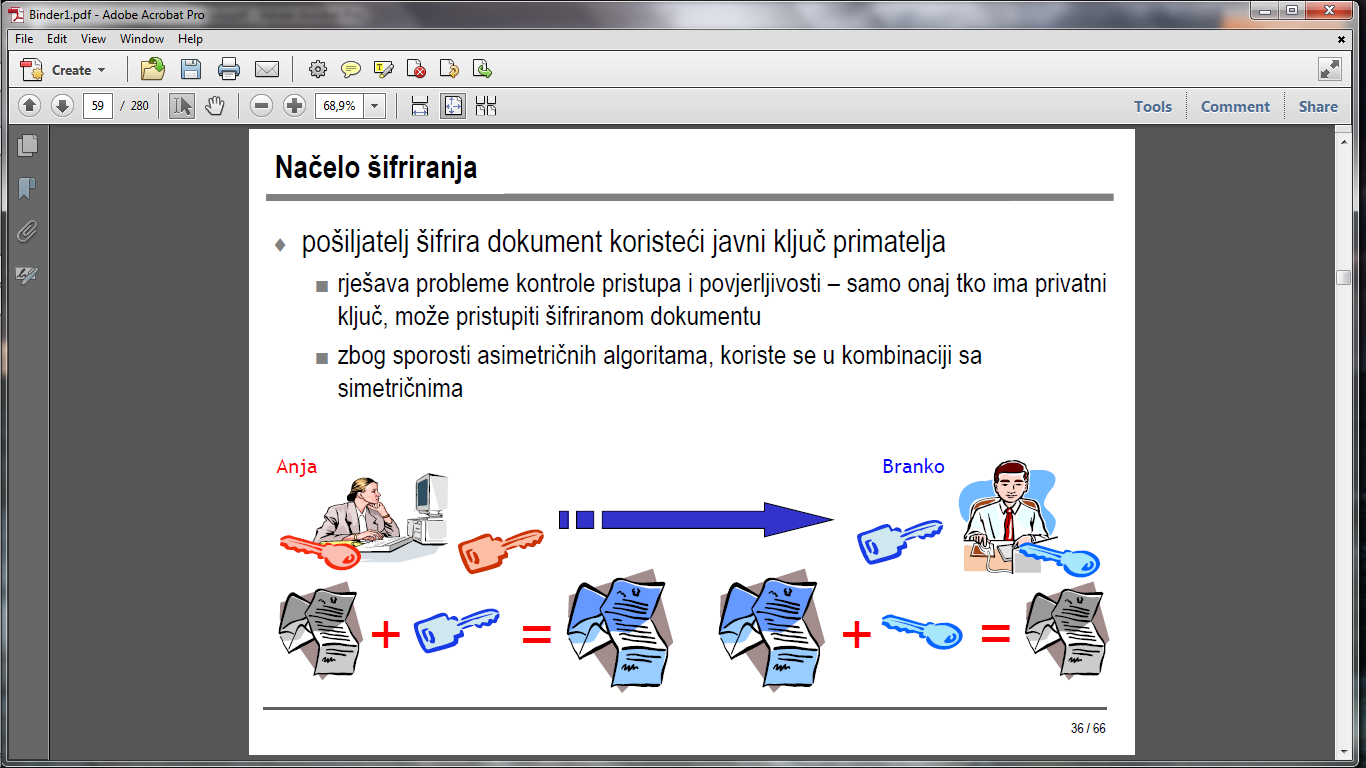
hibridni pristup:

* asimetričnu kriptografiju koristiti za razmjenu simetričnog ključa

Secure Sockets Layer – SSL, Pretty Good Privacy – PGP, GNU Privacy Guard – GPG

pošiljatelj šifrira dokument koristeći javni ključ primatelja

* rješava probleme kontrole pristupa i povjerljivosti – samo onaj tko ima privatni ključ, može pristupiti šifriranom dokumentu
* zbog sporosti asimetričnih algoritama, koriste se u kombinaciji sa simetričnima



### Potpis

vlastoručni potpis

* jedan od temelja tradicionalnih (“papirnatih”) trgovačkih transakcija
* potpis nije zakonski definiran pojam, već se radi o općeprihvaćenom pravnom standardu o kojem nije bilo većih dvojbi sve do pojave elektroničke komunikacije

osnovne funkcije potpisa:

* autentičnost
* integritet
* nepovratnost

elektronički potpis mora:

* biti jedinstven za osobu koja ga koristi
* biti pod isključivom kontrolom osobe koja ga koristi
* mogućiti provjeru identiteta korisnika
* postojati veza između potpisa i potpisane isprave

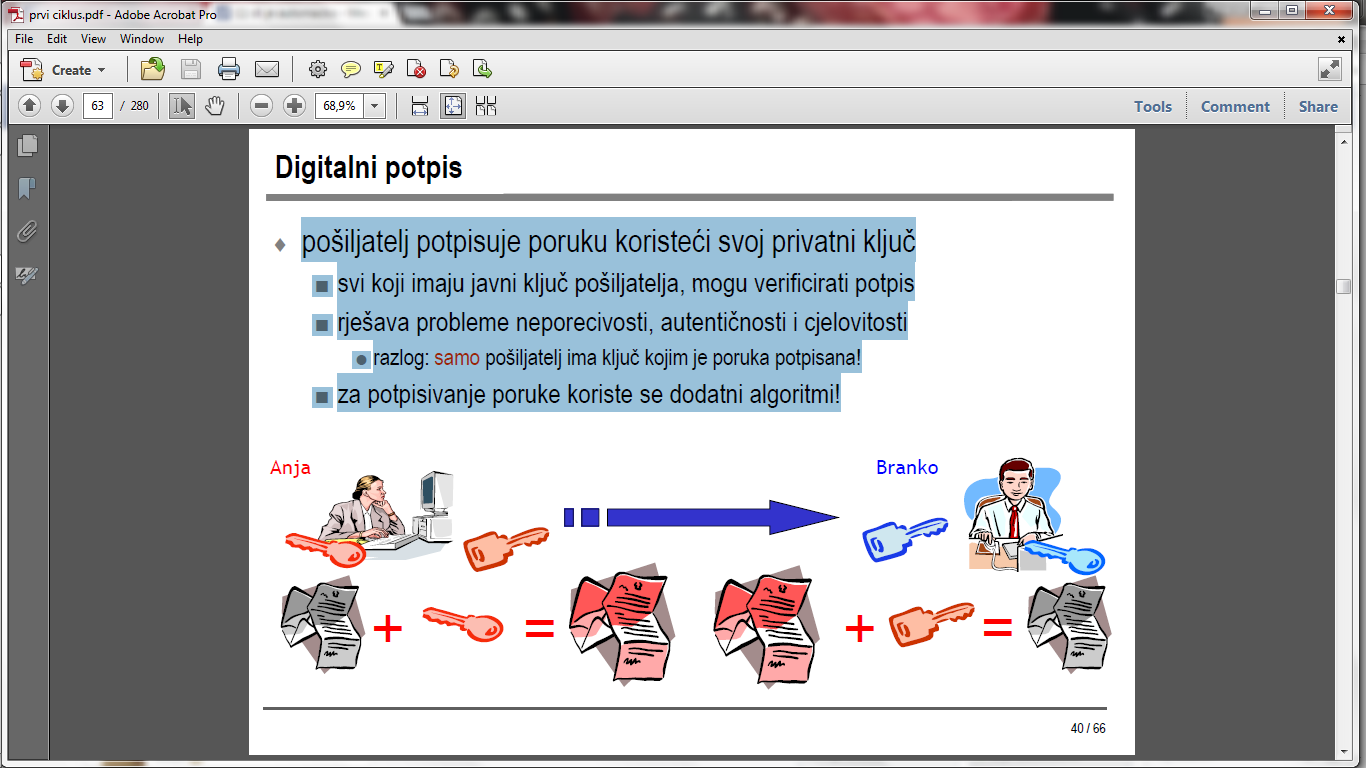
vrste elektroničkih potpisa:

* skenirani ručni potpis (slika ručnog potpisa)
* digitalni potpis - niz znakova u digitalnoj formi dobiven primjenom asimetrične kriptografije
* biometrijski potpis - pohranjivanje karakteristika tijela pojedinca u elektroničkom obliku i njihovo korištenje za identifikaciju (npr. otisci prstiju, mrežnica oka, prepoznavanje glasa, DNK provjera…)

## Digitalni potpis

pošiljatelj potpisuje poruku koristeći svoj privatni ključ

* svi koji imaju javni ključ pošiljatelja, mogu verificirati potpis
* rješava probleme neporecivosti, autentičnosti i cjelovitosti - razlog: samo pošiljatelj ima ključ kojim je poruka potpisana!
* za potpisivanje poruke koriste se dodatni algoritmi!



## Hash funkcija

* prije digitalnog potpisivanja treba generirati sažetak (hash, digest) poruke

hash funkcija

* ulaz: niz znakova proizvoljne duljine
* izlaz: niz znakova fiksne duljine (npr. 128 ili 160 bitova)

osnovna svojstva hash funkcije:

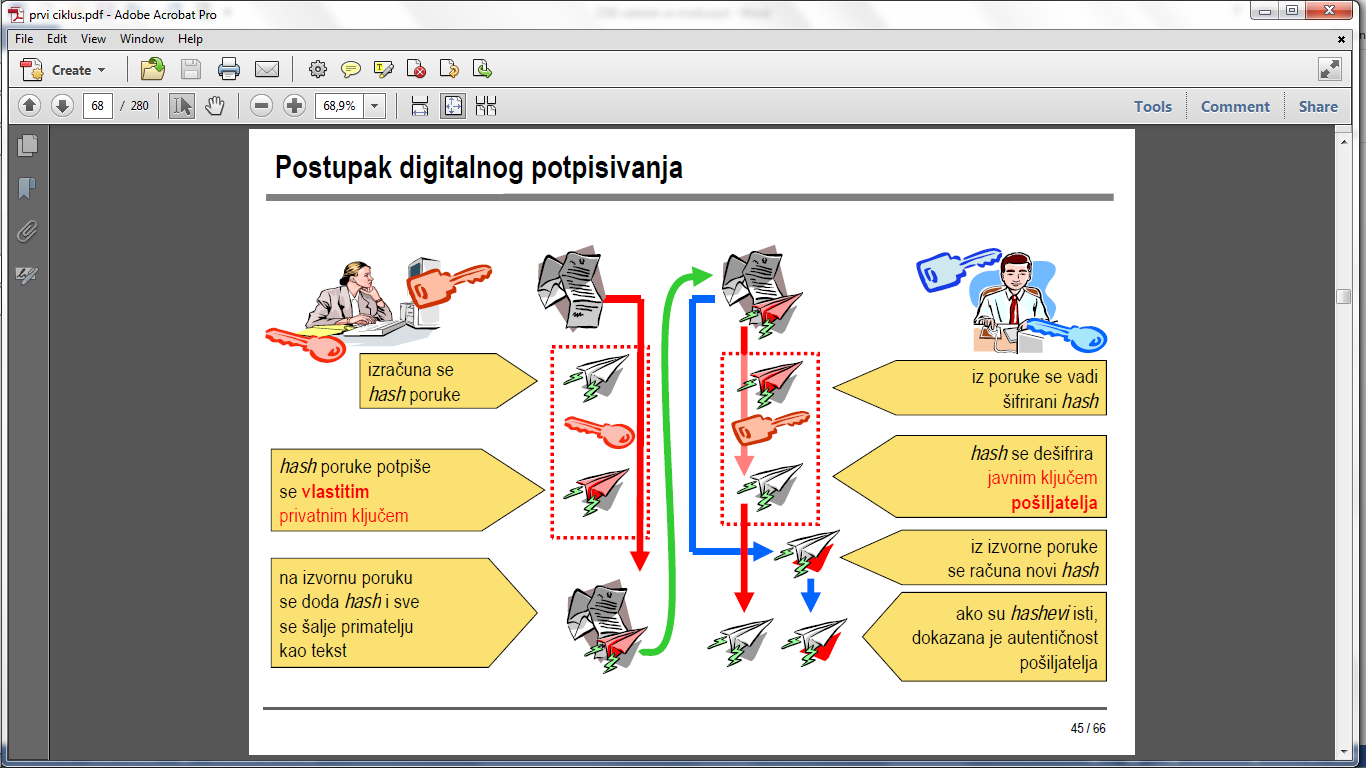
* hash je jednosmjerna funkcija
  + jednostavno ju je izračunati za zadanu poruku
  + nije moguće na osnovu izlaza regenerirati ulaznu poruku
  + nije moguće odrediti ulaznu poruku koja bi imala zadani hash
  + neizvedivo da se pronađu dvije različite poruke koje bi imale isti hash
* promjena jednog bita ulaza rezultira potpuno drugačijim izlazom

primjena :

* digitalni potpisi, Message Authentication Code (MAC), autentifikacija
* za otkrivanje kopija digitalnog sadržaja, za jednoznačnu identifikaciju binarnih sadržaja
* za izračunavanje kontrolne sume (*checksum*)

**Algoritmi za digitalni potpis**

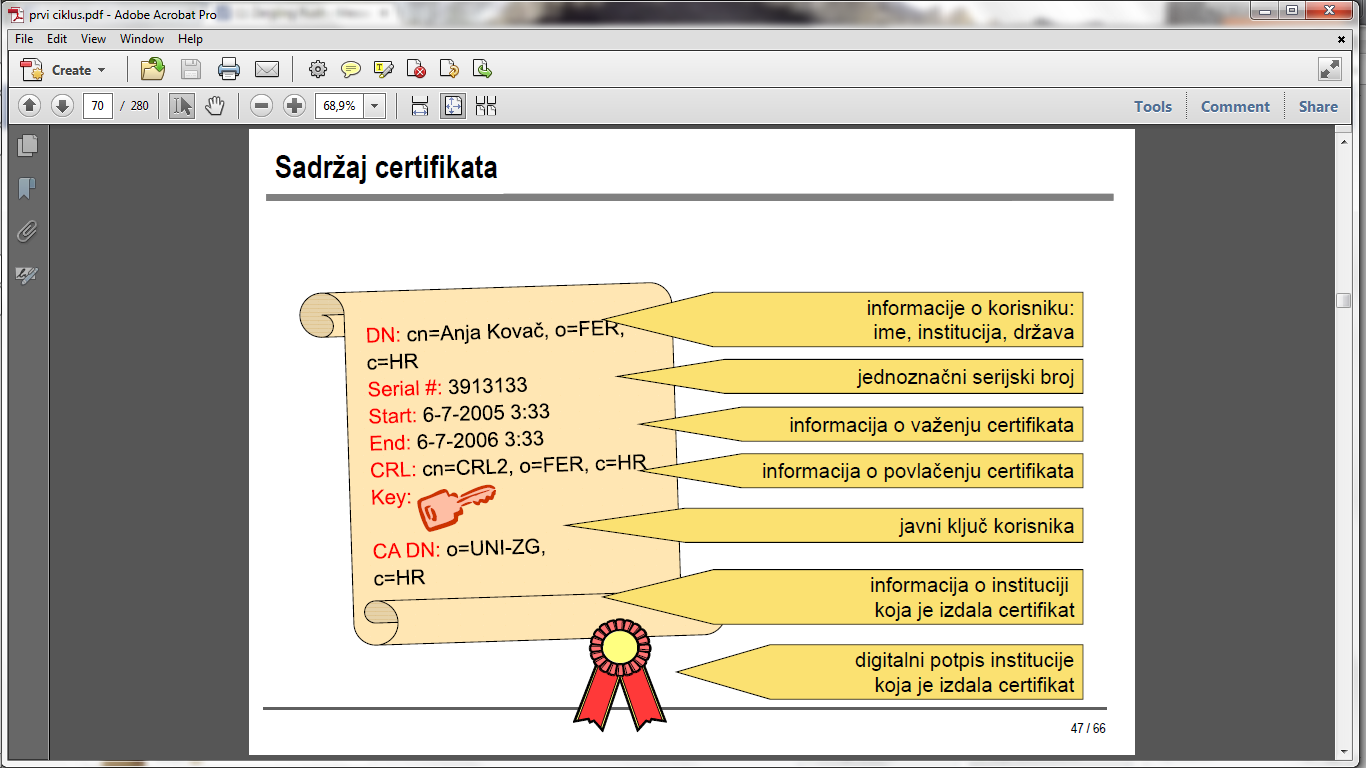
* Secure Hash Algorithm (SHA-1)
  + algoritam američke vlade (NSA), vjerojatno najsigurniji
  + daje *hash* vrijednost duljine 160 bita iz niza znakova bilo koje duljine
  + kolizija otkrivena u 269 hasheva, 2005. godine
  + SHA-2, SHA-3
* Message Digest Algorithm 5 (MD5)
  + daje *hash* duljine 128 bita
  + prethodnik MD4 je probijen
  + MD5 razvaljen 2008.



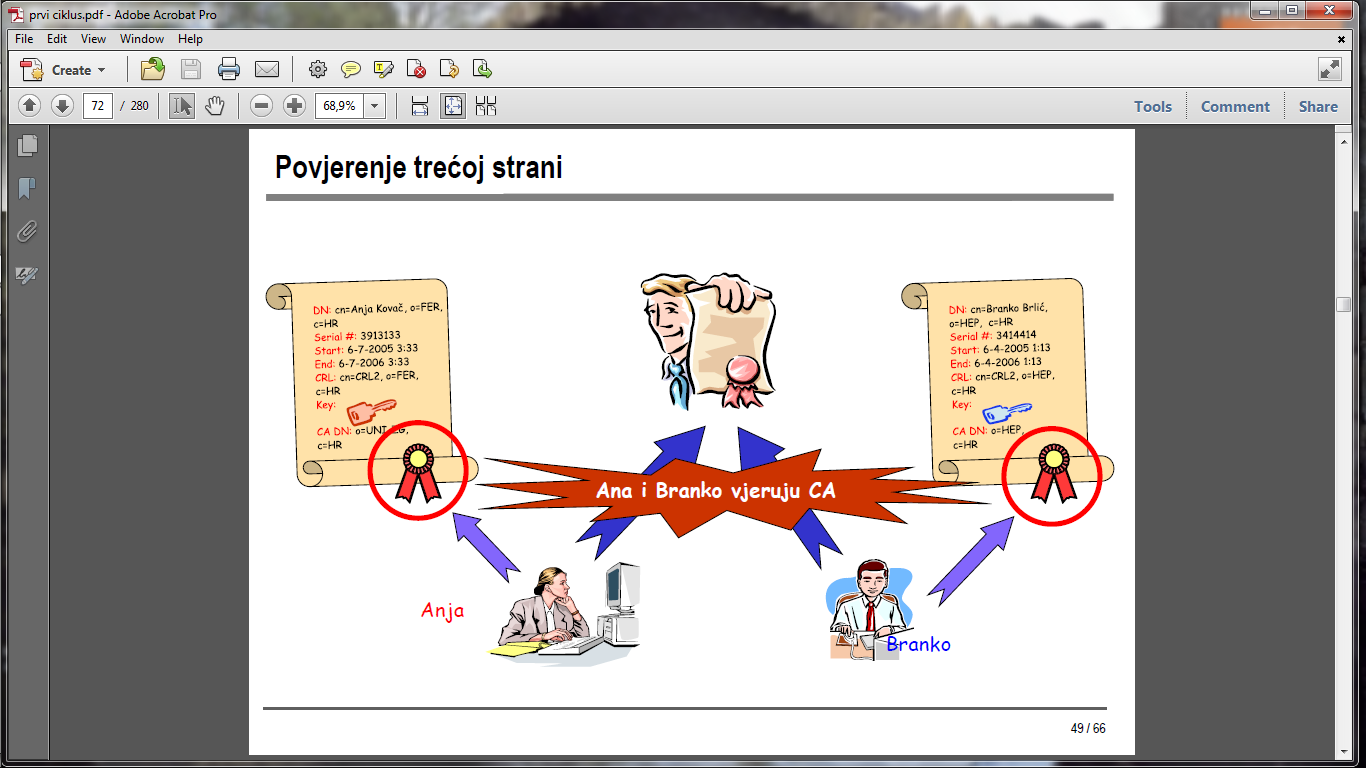
## Digitalni certifikat

* rješava problem dokazivanja autentičnosti
* skup informacija koje autentificiraju korisnika i davatelja usluge certificiranja
* sadržaj certifikata:
  + npr. ime organizacije koja izdaje certifikat, ime organizacije ili korisnika kojem pripada certifikat, njegovog javnog ključa, vremena važenja certifikata, elektroničke adrese organizacije ili korisnika, zemlje porijekla korisnika te ostalih bitnih informacija koje identificiraju stranu kojoj se izdaje certifikat

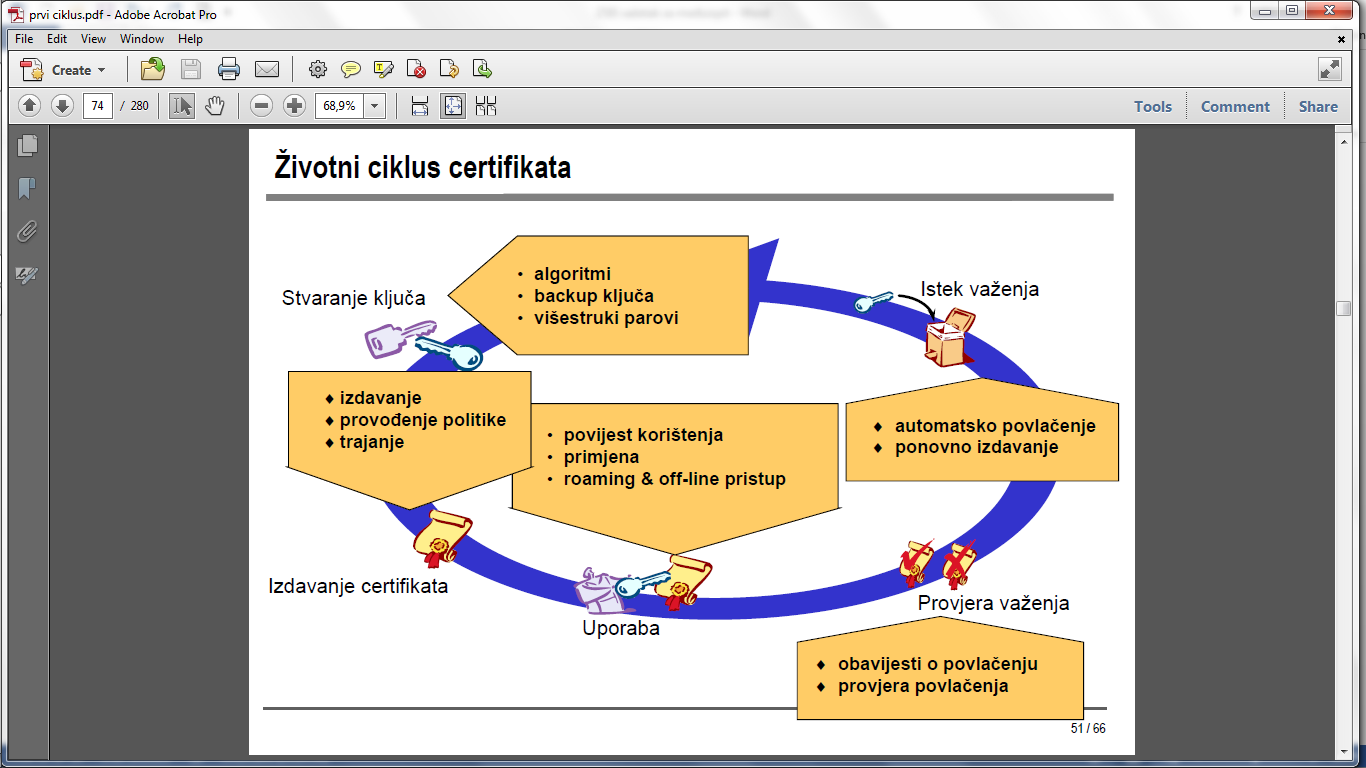
standardizacija: - X.509 format - ISO, ITU-T



Certifikat izdaje certifikacijsko tijelo(CA), te povjerenje funkcionira ovako:



Moguće je povući certifikat, te je to objavljeno na stranicama certifikacijskog tijela



## Javni ključ

* Public Key Infrastructure
* osnova za stvaranje sigurne i povjerljive razmjene podataka između sudionika u sustavu
* temelji se na asimetričnoj kriptografiji: - šifriranje javnim ključem, digitalni potpis i sustav certifikata
* osigurava:
  + zaštitu privatnosti komunikacije osiguravajući komunikaciju od presretanja i neovlaštenog čitanja
  + osiguranje cjelovitosti elektroničke komunikacije onemogućavajući izmjene podataka tijekom njihovog prenošenja mrežom
  + potvrđivanje identiteta strana koje sudjeluju u komunikaciji
  + osiguranje neporecivosti sudjelovanja bilo koje strane u komunikaciji
* jedinstvena registracija javnih ključeva
* automatizacija životnog ciklusa ključa

**Dijelovi PKI**

* certifikacijsko tijelo
  + izdavanje i povlačenje certifikata, održavanje informacija o stanju certifikata, objava važećih certifikata...
* registracijsko tijelo
  + provjerava sadržaj certifikata za CA
* korisnici PKI (vlasnici certifikata)
* klijenti (aplikacije)
  + provjeravaju digitalne potpise i certifikate kod CA
* repozitorij
  + distribuira certifikate i popise povučenih certifikata u realnom vremenu (npr. LDAP poslužitelj)

# Sigurnost i privatnost

## Upravljanje identitetom

Identitet na internetu - internetski identitet / online identitet / *internet persona*

* društveni identitet koji korisnik Interneta uspostavlja u online-zajednicama i na web-sjedištima
* neki koriste prava imena
* neki su anonimni
* neki koriste pseudonime

otkrivaju različite osobne podatke

dvostrana privatnost: npr. studenti i nastavnici

napadači: online-grabežljivci (*predators*)

**Načela Fair Information Practice -** skup smjernica OECD-a

* otvorenost
  + postojanje, ciljevi i svrha sustava za prikupljanje privatnih informacija moraju biti javni
* individualno sudjelovanje
  + pojedinci moraju imati uvid u podatke o njima samima, uz mogućnost ažuriranja
* ograničenje na prikupljanje podataka
  + uz privolu korisnika
* kvaliteta podataka
  + moraju biti relevantni za svrhu za koju su namijenjeni
* konačnost
  + korištenje i odavanje moraju biti ograničeni, samo za svrhu za koju su namijenjeni
* sigurnost
  + zaštićeni od gubitaka, krađe, uništenja, neovlaštenog korištenja, otkrivanja
* odgovornost
  + oni koji ih čuvaju moraju biti odgovorni za njihovo korištenje i prikupljanje

## dimenzije privatnosti

* privatnost osobe (tjelesna, zdravstvena, izazivanje nelagode, genetska)
* privatnost ponašanja (politička, spolna, religiozna pripadnost)
* privatnost osobne komunikacije
  + bez nadzora treće osobe (vlade, drugih pojedinaca, poslodavca)
* privatnost osobnih podataka
  + gotovo nemoguće: treba postojati stupanj nadzora nad vlastitim podacima

**Zaštita privatnosti -** razlozi za zaštitu:

* psihološki - ljudima je potreban osobni prostor
* društveni - sloboda potrebna za otvoreno iznošenje mišljenja
* ekonomski - sloboda je preduvjet za inovativnost
* politički - nadzor ugrožava demokraciju

## Elektroničko poslovanje

* bilo koja transakcija čija je svrha prodaja ili kupnja robe ili usluga ili informacija,
* pogađanja između zainteresiranih strana odvijaju seelektronički, a ne sa stvarnom razmjenom ili s direktnim kontaktom
* pretpostavke
  + stvoriti informacijsku i komunikacijsku infrastrukturu
  + omogućiti njeno korištenje uz razumne troškove
  + definirati zakone

# Voditelj sigurnosti informacijskog sustava

Sve organizacije danas jako ovise o svojim informacijskim sustavima

* Ako je narušena sigurnost informacijskog sustava tvrtka može pretrpjeti velike štete ili čak propasti.

Informacijski sustavi spojeni su na Internet

* Poslovni razlozi diktiraju taj trend i nije ga moguće izbjeći, no
* bilo tko s pristupom Internetu može pristupiti informacijskom sustavu tvrtke

Organizacije, a i njihovi informacijski sustavi ovise o ljudima

* Ljudi su najslabija karika u sigurnosti (!!!!)

Potencijalni napadači variraju u resursima i motivima

Usmjereni napadi mogu biti vrlo sofisticirani

* Advanced Persistent Threat (APT)
* U slučaju napada gotovo nemoguće se je obraniti
  + Napadač mora naći samo jedan propust
  + Danas više nije pitanje AKO već KADA!

Računalni kriminal je u temelju vrlo profitabilnog posla

## Faktori koji utječu na sigurnost informacijskih sustava

**Možemo ih razvrstati u tri grupe**

* Ljudski faktori
* Organizacijski faktori
* Tehnološki faktori

Ljudski faktori čine

* Nedostatak edukacije u području sigurnosti
* Nedostatak komunikacije po pitanju sigurnosti
* Nedostatak svijesti
* Nedostatak kulture
* Neodgovarajuće ponašanje

Organizacijski faktori

* Nedostatak budžeta
* Kratki rokovi
* Nedostatak podrške menadžmenta
* Nedostatak odgovarajuće procjene rizika
* Nepostojanje sigurnosnih procedora

Tehnološki faktori

* Ranjivosti u IT imovini
* Nedovoljni ili neodgovarajući sigurnosni mehanizmi (primjerice vatrozidi, IDSovi, antivirusna podrška, lozinke, šifriranje, itd.)

## Voditelj sigurnosti informacijskog sustava

***Zaštita organizacije zahtijeva ciljan, planiran i dugoročan pristup***

* Mora biti osoba koja razumije sigurnost
* Ali sigurnost nije misija i vizija organizacije, sigurnost samo pomaže postizanje misije i vizije
* Po mogućnosti ne smije se baviti operativnim detaljima
* Različit od osoba koje se bave taktičkim detaljima
* Ta funkcija je *voditelj sigurnosti informacijskog sustava*, VSIS ( Chief Information Security Officer, CISO, Chief Information System Security Officer, CISSO)

CISO je pri vrhu organizacijske strukture

* Direktno odgovara predsjedniku Uprave (CEO) ili nekog od članova Uprave (CFO, COO, head of legal council)
* U slučaju potrebe može imati direktan pristup nadzornom odboru
* Jedna od zahtjevnijih zadaća CISO-a je komunikacija s Upravom

U slučaju većih organizacija radi se o uredu na čijem čelu se nalazi voditelj ureda

* Tvrtka ima voditelja sigurnosti (CSO) kojemu CISO odgovara
  + Voditelj sigurnosti zadužen je za cjelokupnu sigurnost (fizičku, informacijsku, prijevare,…)

**Svrha CISO-a je da**

* Nadzire i koordinira aktivnosti vezane uz sigurnost informacijskog sustava.
* Inicira primjenu dobrih praksi i prihvaćenih standarda vezanih uz sigurnost informacijskog sustava.
* Ima savjetodavnu ulogu u svezi sa sigurnosti informacijskog sustava.

## Zadaće CISO-a

### Izrada internih akata

Razvoj politike sigurnosti informacijskog sustava, standarda, smjernica i ostalih internih akata s ciljem postizanja i održavanja zadovoljavajuće razine sigurnosti -uspostavljanje upravljačkog okvira.

* Temeljni akt je **Politika sigurnosti informacijskog sustava**
* krovni dokument koji definira što za informacijski sustav znači da je siguran.
* Za sigurnost informacijskog sustava taj dokument je kao ustav koji je temeljni pravni akt države.
* Temelj za ostale akte („Zakoni”)

- Bitan akt je i pravilnik o radu CISO-a, međutim on ne spada u skup internih akata koji definiraju sigurnost već je organizacijski

Može se postaviti pitanje čemu interni akti, tj. koja korist od njih?

* Oni predstavljaju *administrativne kontrole*, nadopuna tehničkim kontrolama
* Da svi dionici **jasno i nedvosmisleno** znaju što smiju (ili ne smiju), tko je za što zadužen, što se radi, kada i kako, …

**Vrste internih akata:**

* Politika
  + Piše ju Voditelj sigurnosti informacijskog sustava
  + Definira osnovna načela, smjernice… bez ikakvih konkretnih tehničkih detalja
  + Puna izraza tipa „Trebalo bi …”, „Mora se…”, „Preporučljivo je…”, „Ako je moguće…”
* Pravilnik (voditelj sigurnosti/IT)
  + Detaljnije razrađuje politiku, s konkretnijim detaljima no bez ulaska u veliku dubinu
* Procedura (IT)
  + Detaljna razrada pojedinih dijelova pravilnika, jasno specificira korake

Primjeri internih akata

* Politika sigurnosti informacijskog sustava
  + Po mogućnosti, što kraći dokument, no ima i vrlo dugih
* Politika/pravilnik za izradu pričuvnih kopija
* Politika/pravilnik za vođenje i bilježenje sistemskih i operativnih zapisa
* Politika/pravilnik korištenja informacijskog sustava
* Politika/pravilnik upravljanja sigurnosnim rizicima

***Interni akti su živi dokumenti!***

* Interne akte odobrava i prihvaća Uprava

### Provjera provođenja internih akata

Kontroliranje provođenja politike sigurnosti informacijskog sustava i ostalih internih akata koji se odnose na sve aspekte sigurnosti informacijskog sustava

* Revizija internih sustava i pravilnika
* Po potrebi nadopuna, pojašnjenje ili izmjena pravilnika
  + Sustav se stalno mijenja te je potrebno i interne akte prilagođavati
  + Iskustvom se neke stvari ispostave teške, ili jednostavne, ili (ne)provedive

### Upravljanje rizicima

Temeljni alat u radu CISO-a

* Omogućava da se odrede rizici kojima je izložena organizacija
  + Procjena rizika (engl. risk assessment)
  + Potom je moguće napraviti prioritizaciju
  + Na temelju prioriteta odlučuje se što će se učiniti s identificiranim rizicima
    - Prihvatiti, ovladati (na neki način umanjiti), ili prenijeti na neku treću stranu
    - Uprava organizacije ima konačnu riječ po tom pitanju
* Vrlo bitan element posla CISO-a koji se često radi na vrlo loš način
* Upravljanje rizicima je **proces** (kao i sigurnost)
  + Mora se uvijek provoditi jer se uvjeti stalno mijenjaju
* Propisan internim aktima

### Upravljanje incidentima

Danas nije pitanje AKO se desi incident već KADA će se desiti

Postupak koji bi također **morao** biti definiran internim aktima

* Tko/što/gdje/kada/kako, koga se zove, ovlasti i obaveze
* Uključuje dijelove ili cijelu organizaciju, a CISO (možda i CEO) je koordinator
  + To recimo može ovisiti o incidentu (interni akt!)
* Definira i što se podrazumijeva pod **incidentom**
* Treba biti i uvježban, ili bar na neki način ispitan

**Cilj upravljanja incidentima**

* Što prije detektirati incident
* Utvrditi uzroke incidenta, posljedice i nastalu štetu te djelovati na otklanjanju incidenta i umanjivanju štete
* Uvesti kontrole koje će spriječiti njegovo ponavljanje

### Edukacija i osvještavanje

Upozoravanje na potrebu za izobrazbom! Davanje smjernica za izobrazbu svih osoba koje se koriste informacijskim sustavom banke, a u svezi sa sigurnosti informacijskog sustava

**Osvještavanje uključuje**

* Objašnjavati važnost sigurnosti organizacije.
* Informiranje zaposlenika o njihovim ulogama i očekivanjima od uloge u sklopu sigurnosnih funkcija.
* Davati smjernice u obavljanju pojedinih zadaća vezanih uz sigurnost ili rizike.
* Edukacija korisnika

### Izvješćivanje

CISO mora periodički izvješćivati upravu i nadzornom odboru

* Odnosno, bilo koga koje je organizacijski odgovoran za svoj rad
* Najčešće onaj koga CISO izvještava nije stručnjak za sigurnost

Internim aktom o radu CISO-a ili nekim ekvivalentnim dokumentom propisani su detalji

* Učestalost izvješćivanja
* Sadržaj izvješća
* Kome se izvješće sve podnosi

### Rad s vanjskim suradnicima

Vanjski suradnici su

* Revizori
* Stručnjaci koji testiraju sigurnosti informacijskog sustava

Rad s vanjskim suradnicima znači

* Dogovaranje tipa i opsega poslova
* Pružanje potrebnih informacija nužnih za provođenje ispitivanja
* Analiza rezultata
* Uključivanje rezultata u procjenu rizika
* Iniciranje aktivnosti na temelju rezultata

### Analiza sigurnosnih potreba

Analiziranje sigurnosnih potreba, na temelju analize predlaganje:

* Planiranja, implementacije, testiranja i nadziranja aktivnosti za poboljšanje sigurnosti informacijskog sustava

Planiranje godišnjeg budžeta

* Izlaganje upravi
* Dio planiranih aktivnosti

Planiranje i koordiniranje analize isplativosti preporučenih i postojećih sigurnosnih rješenja

### Sudjelovanje u razvoju i održavanju IT-a

Sudjelovanje u značajnijim fazama u životnom ciklusu informacijskog sustava s aspekta sigurnosti

* CISO je uključen kao savjetnik
* Daje mišljenje o predloženim rješenjima
* Po potrebi vrši analizu
* Predlaže dodatna rješenja

Primjeri

* Odabir novog rješenja za udaljen pristup
* Razvoj nove aplikacije
* Arhitektura novog sustava

Praćenje raznih upozorenja i novog razvoja u računalnom kriminalu

* Na temelju toga davanje smjernica IT-ju
* Ažuriranje procjene rizika

Procjena prijetnji

* Analiza resursa, ciljeva, motiva
* Primjer: Prijetnja DDoS napadom od anonimne skupine

### Sistemski i operativni zapisi

Sistemski i operativni zapisi (logovi) vrlo su bitni za sigurnost informacijskog sustava

* Omogućavaju rekonstrukciju događaja
* Omogućavaju detekciju neočekivanih događaja

Nužno ih je držati na zasebnom mjestu

* Kako bi se zaštitili od neovlaštenih izmjena

Usklađeni satovi vrlo bitni za rekonstrukciju (!)

CISO definira način upravljanja sistemskih i operativnim zapisima

* Vrši nadzor i analizira logove te traži očitovanja

## Problemi (i izazovi) s kojima se CISO susreće

* Vrlo dinamična okolina koju je teško pratiti
  + Prijetnje van organizacije se brzo mijenjaju i puno ih je
  + **Unutarnje prijetnje**
  + Informacijski sustav je vrlo dinamičan
  + Čak ni IT osoblje se ne pridržava pravila (!)
* Evaluacija rizika raznih tehnologija
  + „Cloud” rješenja, BYOD, Mobilni uređaji, Specifične aplikacije
* Operativni i strateški poslovi
* Vanjski dobavljači
* Koordiniranje aktivnosti s organizacijskom jedinicom informacijske tehnologije i unutarnjom revizijom (ponekad nisu na „istoj valnoj duljini”)

### Kompetencije CISO-a

* Upravljačke vještine (engl. management skills)
* Poslovne vještine (engl. business skills)
  + Povećati vrijednost organizacije i integrirati potrebu za sigurnošću s poslovnim ciljevima tvrtke
* Stalno usavršavanje (engl. information systems security education)
* „Soft skills”
* Vještine i znanja iz sigurnosti informacijskih sustava
* Planiranje oporavka od katastrofičnih događaja (engl. Disaster recovery planning)
* Sposobnost istraživanja sigurnosnih incidenata (engl. security breach investigations)

### Nadzor rada voditelja sigurnosti informacijskog sustava

Postoji definiran sustav nadzora rada CISO-a

* Sprečavanje potencijalne štete zbog neodgovornog ili zlonamjernog ponašanja
* Poboljšanje rada CISO-a – povratna petlja

Tu dužnost obavljaju

* Revizije
* Unutarnja i vanjska
* Osoba/funkcija nadređena voditelju sigurnosti (CEO, CIO, CSO, …)

# Sigurnost računalne mreže

## Računalna mreža

* Čini temelj informacijskih sustava
* Omogućava komunikaciju komponenti informacijskog sustava
  + Poslužitelja, radnih stanica, sustava za pohranu podataka, za pohranu rezervnih kopija, telefonski sustav, pisači, …
* Povezuje informacijski sustav na Internet
  + Omogućava pristup na Internet, ali i s Interneta
* Sastoji se od mrežnih uređaja i komunikacijskih veza
* Mnoštvo različitih protokola u svim slojevima
  + Iznimka je treći sloj gdje je dominantan IP

**Sigurnost računalne mreže vrlo je bitan preduvjet za sigurnost cijelog informacijskog sustava!**

* Nužno je poznavanje karakteristika računalnih mreža
  + Ranjivosti koje su prisutne u mrežama
  + Zaštitni mehanizmi koji se koriste

## Podjela ranjivosti

* Fizička ranjivost
* Ranjivosti u protokolima
  + Ako pojedini protokol ima ranjivost, tada sve implementacije imaju tu ranjivost
* Ranjivosti u implementacijama
  + Protokol nema ranjivost već je ona posljedica nekakve pogreške u implementaciji
  + Ako ima više nezavisnih implementacija neće biti sve ranjive
* Ranjivosti u konfiguraciji i korištenju
  + Ranjivost koja je specifična za pojedinu okolinu

### Fizička sigurnost

Temelj svake sigurnosti su odgovarajuće zaštićeni elementi od neovlaštenog pristupa

Razlog je što fizički pristup omogućava privilegirane operacije nad elementom

* Spajanje na upravljačke pristupe uređaja koji omogućavaju privilegirane operacije ili jednostavno omogućava razna fizička i logička „hakiranja”

Neadekvatna fizička sigurnost omogućava pristup

* pojedinim uređajima
* vodičima
* mrežnim utičnicama
* bežičnim mrežama

**Pristup pojedinim uređajima**

* Moguće zamijeniti uređaj vlastitim
* Isključivati i uključivati spojene uređaje
* Pristup upravljačkom portu (slabija zaštita pristupa)

**Pristup vodičima**

* Omogućava pasivne i aktivne napade
* Pasivni napad je prisluškivanje
* Aktivni napadi su onemogućavanje komunikacije, izmjena podataka, ponavljanje, impersonifikacija
  + Aktivni napad omogućava **postizanje** MITM napada
* Korištenje optike nije jamstvo sigurnosti!

**Pristup mrežnim utičnicama**

* Pruža mogućnosti slične kao i sa žicama
* Mreže se dijele u segmente prema povjerenju
  + Što veće povjerenje slabije su kontrole
* Dosta često se previde
* Omogućava MITM napade

**Pristup bežičnim mrežama**

* Posebno problematične zbog dostupnosti
  + Odgovarajućim antenama moguće je ostvariti pristup iz velike udaljenosti
* **Problem su i podmetnute bežične mreže(!)**

### Ranjivosti u protokolima

Dosta protokola je definirano u vrijeme dok sigurnost nije bila na listi prioriteta

* Velik broj danas popularnih protokola je ranjiv na neki način
* S obzirom da je ranjivost u protokolu, nema načina da se implementacijski uklone manjkavosti

Protokol Ethernet

* Nema zaštite integriteta (CRC nije zaštita od namjernih izmjena!), autentičnosti i tajnosti
* Virtualne lokalne mreže (VLAN)
* Radi manipulacija nužan je pristup lokalnoj mreži!
  + Podatkovni sloj omogućava komunikaciju bilo koja dva **direktno spojena** računala(!)
* Na mreži Ethernet postoje upravljački okviri (BPDU, CDP, …) koji su posebno kritični – moguće utjecati na topologiju mreže ili saznati topologiju

**Protokol ARP**

* Prenosi se u Ethernet okvirima i ima iste probleme kao mreža/protokol Ethernet
* Manipulacija omogućava preusmjeravanje prometa – moguće je pozicionirati između bilo koje dvije komunikacijske točke

**Protokol IP (i ICMP)**

* Nema nikakve zaštite autentičnosti, integriteta i tajnosti
* Lako manipuliranje paketima i njihovo lažiranje
* Određene napade moguće je provoditi s bilo koje točke na Internetu
  + Mrežni sloj omogućava komunikaciju bilo koja dva računala (!)
* IPv6 unosi značajnu promjenu – kompleksnija funkcionalnost i veće mogućnosti za napadače(!)

**Protokol TCP**

* Nema nikakve zaštite tajnosti
* Zaštita autentičnosti i integriteta postoji, no ne koristi se često
  + Ne bi bila moguća komunikacija preko NAT uređaja (!)
* Vrlo lako ubacivanje podataka u komunikaciju
* Moguće slijepo ubacivanje podataka
  + Nije potrebno biti na komunikacijskom putu
  + Jedina zaštita je jedan pristup i slijedni brojevi što sa kriptografskog stanovišta i zbog brzine današnjih mreža nije neka zaštita

**Protokol UDP**

* U potpunosti nezaštićen protokol

**Protokol RTP**

* Jedan od protokola za VoIP, koristi UDP za prijenos (tu su još SIP, RTCP)
* Telefoni direktno komuniciraju ili ide preko telefonske centrale
* Nije zaštićen ni na koji način
* Omogućava je prisluškivanje razgovora
* U kombinaciji s ranjivostima nižih protokola čini prisluškivanje lakšim nego u klasičnoj telefoniji
* Telefoni ponekad preuzimaju ulogu preklopnika (engl. switch)
  + Korištenje VLAN-ova
  + Povećava ranjivosti

**Protokol DNS**

* Vrlo kritičan protokol Interneta, i potpuno nezaštićen
* Malverzacijom protokola DNS moguće utjecati na odgovore
  + Omogućava preusmjeravanje komunikacije na lažne stranice
  + Napadi uskraćivanja usluge

**Protokol SNMP**

* Upotrebljava se za nadzor i upravljanje mrežnih uređaja
* Različiti modeli osiguranja sigurnosti, no nedovoljni
* Često uključen „po defaultu” s nekom opće poznatom lozinkom (*public*)

**Protokoli elektroničke pošte**

* Protokoli SMTP, IMAP, POP
* Svi protokoli elektroničke pošte nemaju mehanizama za zaštitu autentičnosti, integriteta i povjerljivosti
* Sadrže mehanizme autentifikacije koji ne prenose lozinku u čistom obliku preko mreže (ili ju uopće ne prenose preko mreže)

**Protokol FTP i HTTP**

* Nema zaštite integriteta, tajnosti i **autentičnosti**
* Prenose preko mreže lozinke ili autentifikacijske podatke (engl. credentials) u nezaštićenom obliku
* Izuzetno popularni protokoli, posebno HTTP te zbog toga vrlo kritični

**Protokoli usmjeravanja**

* Vrlo kritični protokoli (OSPF, ISIS, RIP, BGP)
  + Inicijalno nisu imali definirane mehanizme zaštite te su naknadno dodavani
  + BGP posebno problematičan u današnje vrijeme
* Prvenstveno se temelji na povjerenju

### Implementacijske ranjivosti

* Ranjivosti specifične za pojedinu implementaciju
  + Primjerice Heartbleed bug koji je specifičan za OpenSSL
  + *Shellshock* ranjivost u ljusci bash
* Nisu toliko problematični kao ranjivosti u protokolima
  + Moguće ih je lakše ispraviti
* ALI, ako je pojedina implementacija vrlo popularna predstavljaju veliku prijetnju
  + Primjerice, ranjivost u OpenSSL-u je značajna ranjivost na Internetu
* Sve implementacije imaju ranjivosti!!!
  + Ranjivost za koju znaju napadači i iskorištavaju je, a nije poznata onima koji se brane (ili još nema zakrpe) zovu se *zero day vulnerabilities*

### Konfiguracijske ranjivosti

Ranjivosti u pojedinim instancama implementacija protokola

**Primjeri ranjivosti**

* Administrator nije podesio autentfikaciju i moguće ju je zaobići
* Kombinacija usluga/aplikacija je tako postavljena da omogućavaju zaobilaženja nekakvih ograničenja
* Ograničenja nisu postavljena dovoljno usko i moguće je pristupiti resursima kojima se ne bi smjelo pristupiti

**Posljedice**

* Nekompetencije ili nemara administratora
* Slučanosti
* Podrazumijevanih postavki aplikacije nakon instalacije koji nisu dovoljno dobri sa stanovišta sigurnosti

## Pregled zaštitnih mehanizama

Zaštiti se pristupa sveobuhvatno - samo jedan mehanizam nije dovoljan (*Defense in depth)*

Neki zaštitni mehanizmi

* Fizička sigurnost
* Kriptiranje komunikacije
* Vatrozid (engl. firewall)
* Posrednički poslužitelji (engl. proxy)
* VPN sustavi
* Sustavi za detekciju upada
* Sustavi za prevenciju upada

### Fizička sigurnost

Zaštita prostora u kojima se nalazi mrežna oprema ili kojima prolaze vodiči

* Zasebne prostorije za mrežnu i poslužiteljsku opremu
* Mrežni ormarići
* Kanalice za zaštitu vodiča

Dodatne zaštite

* Video nadzor, zaštitarska služba, zaštita od požara i poplava, neprekidna napajanja...

### Kriptiranje komunikacije

Svim protokolima se na neki način pokušava dodati kriptografska zaštita

* Na mrežnom sloju - IPSec, OpenVPN, …
* Na prijenosnom sloju - TLS (i SSL koji je zastario), DTLS, proširenja protokola TCP
* Na aplikacijskom sloju - DNSSEC

Značajno usložnjava implementaciju i održavanje

Temelji se na PKI-ju, certifikatima, dijeljenim tajnama - svaki od njih ima svojih manjkavosti i prednosti

### VPN sustavi

Poslovni uvjeti i karakteristike tvrtki diktiraju međusobno spajanje različitih lokacija te omogućavanje udaljenog rada

* Nekada su se uzimali iznajmljeni vodovi za tu svrhu
* I danas se to koristi, no ekonomski razlozi diktiraju trend korištenja javne mreže Internet u tu svrhu
* Vrlo popularna upotreba virtualnih privatnih mreža (VPN)
* Dvije osnovne implementacije - temeljene na IPsec protokolima ili na TLS protokolu
* Potencijalni konfiguracijski problemi - Split traffic, autentifikacija, …

### Protokol za sigurnost transportnog sloja

TLS (engl. Transport Layer Security)

Protokol koji se razvija unutar IETF, zadnja verzija 1.2

Zadaće protokola TLS

* Omogućiti klijentu utvrđivanje identiteta poslužitelja (autentikacija), protokol podržava i autentikaciju klijenta poslužitelju ali se to rijetko koristi.
* Zaštita komunikacija od prisluškivanja, lažiranja, ponavljanja, izmjene, fabrikacije

Koristi protokol TCP za prijenos podataka

SSL (engl. Secure Sockets Layer)

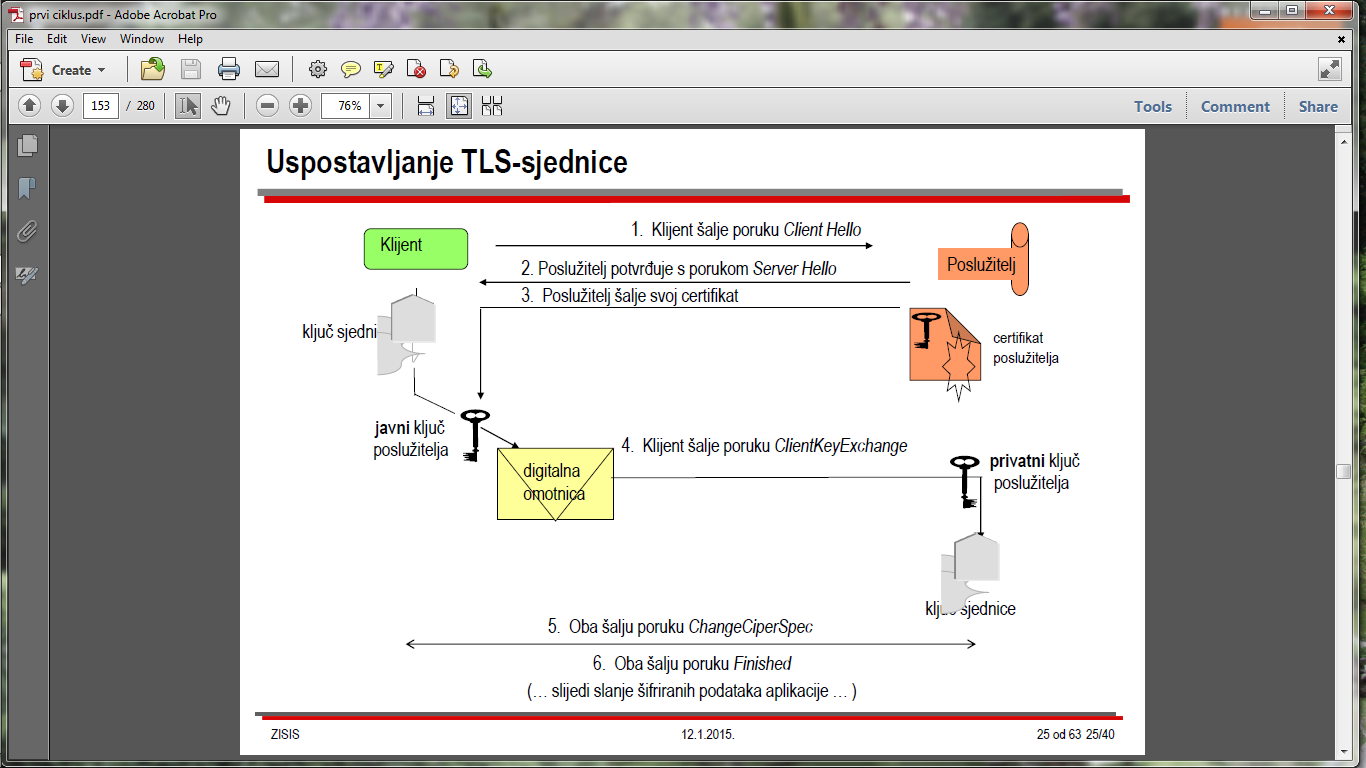
Originalna inačica koju je osmislio Netscape ali koja se više ne smije koristiti zbog propusta u sigurnosti!

Za autentifikaciju se koriste certifikati!

Usluge tog protokola dizajnirane su na takav način da ga aplikacije mogu koristiti s minimalnim izmjenama

* Umjesto direktnog poziva funkcija za slanje i primanje podatka, zovu se funkcije koje će prvo obaviti šifriranje i zaštitu integriteta a potom poslati podatke na drugu stranu.
* U praksi promjena ipak nije tako jednostavna jer kriptografija i kriptografski protokoli nisu jednostavni!

Uspostava TLS sjednice tijekom koje se poslužitelj autentificira klijentu, te se razmjenjuju sjednički ključevi (za šifriranje i zaštitu integriteta!)



### Poboljšanje sigurnosti Weba

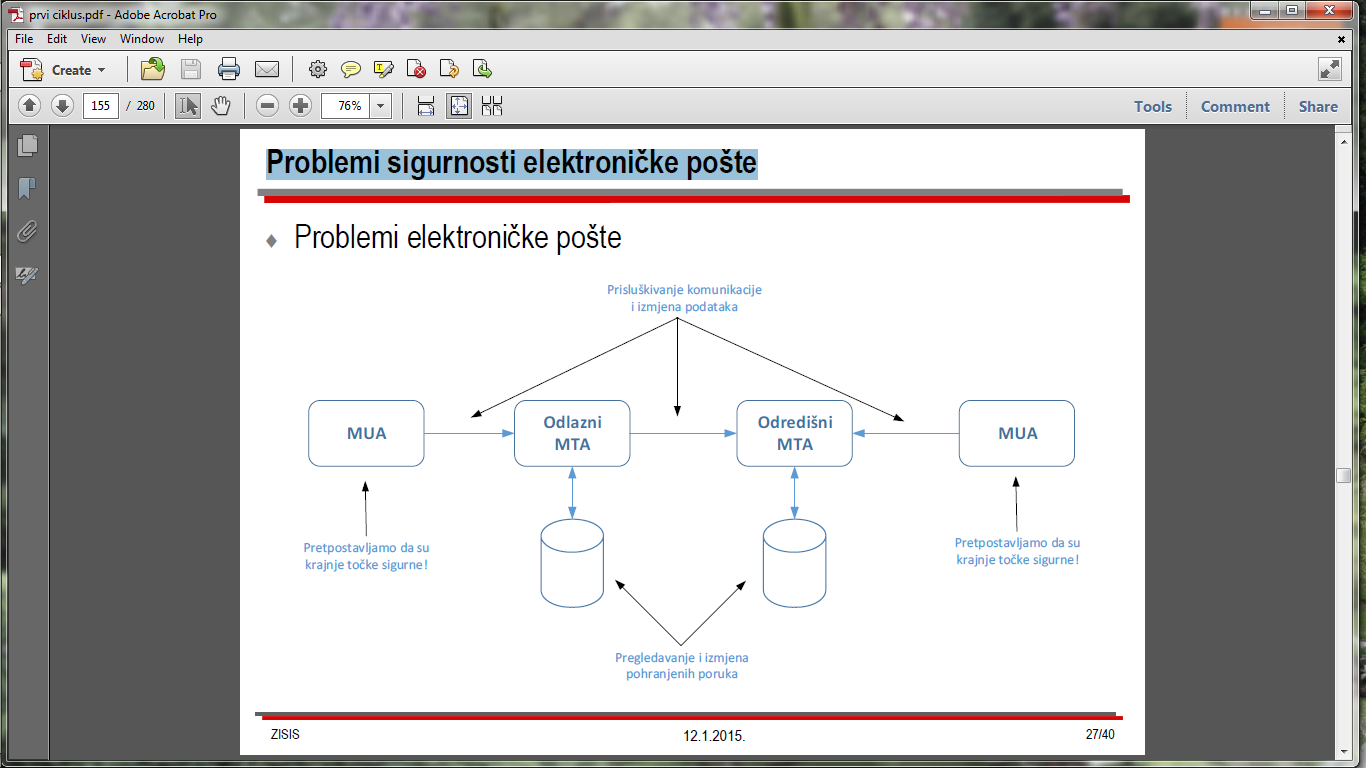
Problemi protokola HTTP preko TCP-a su:

* Nismo sigurni je li poslužitelj kojemu pristupamo onaj za kojeg se on predstavlja.
* Svatko može pratiti komunikaciju koja sadrži osjetljive podatke (lozinke i slično).
* Bilo tko tko se nalazi na komunikacijskom putu može mijenjati komunikaciju i ubacivati lažne informacije

To su vrlo ozbiljni problemi zbog kojih se komunikacija radi zaštite odvije preko protokola TLS

* To je naznačeno sa prefiksom https u URL-u, a podrazumijevani port u tom slučaju je 443
* Ovo ne znači da više ne treba brinuti jer napadači mogu neoprezne korisnike prevariti bez obzira na korištenje protokola https!

### Problemi sigurnosti elektroničke pošte



**Sigurnost komunikacije elektroničke pošte**

* Ako pretpostavimo da su svi poslužitelji sigurni, tada je dovoljno zaštiti komunikaciju
* Moramo štiti komunikaciju zbog
  + Prijenosa lozinki, mogućnosti da netko snima promet, neovlaštena izmjena poruka tijekom prijenosa
* Zaštita komunikacije se može obaviti tako da se SMTP/POP/IMAP prenose preko protokola TLS
  + To se koristi na dva načina, odmah se kreće sa TLS protokolom za što je rezerviran poseban port (IMAPS na portu 993), ili se krene s „običnim” protokolom pa se prebacina TLS (STARTTLS naredbe u protokolu).
* **Problem je što ne možemo jamčiti da će SVA komunikacija ići preko protokola TLS**

**Sigurnost poruka elektroničke pošte**

* Najbolje rješenje je potpisivanje i/ili kriptiranje poruka elektroničke pošte
  + Na taj način se može jamči autentičnost i cjelovitost te po potrebi i tajnost!
* Koriste se dvije norme S/MIME te PGP
* Problem je što klijenti elektroničke pošte variraju u podršci navedenih normi

**S/MIME se temelji na sustavu PKI (**engl. Secure MIME**)**

* Svaki korisnik ima svoj privatni ključ i certifikat.
* Korisnik može sam generirati svoj privatni i javni ključ te zatražiti izdavanje certifikata.
* U korporativnim okruženjima korisnik dobija svoj privatni ključ i certifikat od odgovarajuće službe u tvrtci
* Ovo je dobro rješenje za korporativna okruženja
* Specifično namijenjeno zaštiti elektroničke pošte

**PGP** se temelji na međusobnom dijeljenju javnih ključeva bez centraliziranog nadzora.

* Skraćenica od Pretty Good Privacy
* Prvu verziju razvio i napisao Phil Zimmermann 1991. godine
* Često se pod tim porazumijeva i program za šifriranje, potpisivanje, itd.
* Normirano u sklopu RFC4880 (OpenPGP)
* Pogodniji je za pojedince i slabo povezane grupe
* Može se koristiti za šifriranje i potpisivanje bilo kakvih podataka
  + Nije specifično za poruke elektroničke pošte

### Vatrozid

Uređaj koji radi na mrežnom sloju - princip rada relativno jednostavan

* Svaki paket koji prolazi provjerava se sa bazom pravila koja određuje što treba učiniti s paketom (temeljne odluke su propustiti ili odbaciti)
* Dijele se na vatrozide *bez stanja* i *sa stanjem* (engl. stateless, statefull)

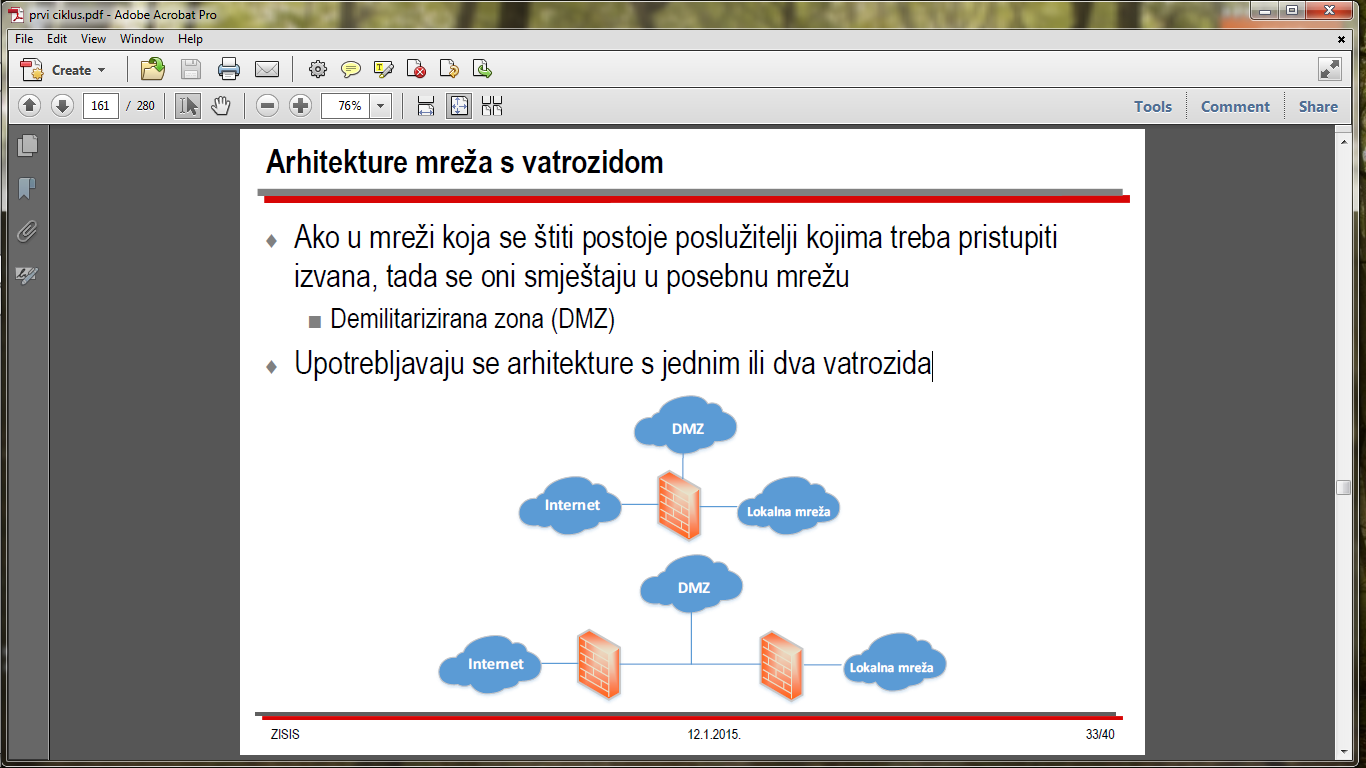
Elementi arhitektura mreža s vatrozidom

* Segmentacija mreže na razne razine povjerljivosti
* Demilitarizirana zona (DMZ)
* Perimetar – granica mreže (danas nije toliko jasan!)
* Konfiguracije s jednim i dva vatrozida

**NAT** - zasebna funkcionalnost, često integrirana s vatrozidom,nije za sigurnost

Ako u mreži koja se štiti postoje poslužitelji kojima treba pristupiti izvana, tada se oni smještaju u posebnu mrežu

* Demilitarizirana zona (DMZ)
* Upotrebljavaju se arhitekture s jednim ili dva vatrozida



Vatrozid je uređaj mrežnog sloja. No, s obzirom da su mu mogućnosti u tom slučaju ograničene svoju funkcionalnost obavlja i na prijenosnom sloju.

* Na aplikacijskom sloju se često koriste aplikacijski posrednici koji „razumiju” pojedini protokol i mogu detaljnije filtrirati promet - primjerice česti su aplikacijski posrednici za SMTP, HTTP
* Prilikom kupovine često je sva funkcionalnost upakirana u jedan uređaj koji proizvođači nazivaju samo vatrozid
* Vatrozid nije rješenje svih problema sigurnosti(!)
* Sve više aplikacija koristi HTTP za komunikaciju kako bi zaobišli vatrozide

### Posrednički poslužitelji

* Vatrozid radi na 3. sloju ISO/OSI RM-a
  + Problematično za protokole koji vrše nekakva multipleksiranja
  + Primjer protokola HTTP, virtualnih poslužitelja i URL-ova
* Posrednički poslužitelji omogućavaju bolji nadzor mrežnog prometa
  + Moguća detekcija zloćudnog koda
  + Crne i bijele liste
  + Bilježenje pristupa radi rektroaktivne analize
  + Dodatno, mreža je efikasnija
* Bez vatrozida nije moguće dosljedno provoditi politiku korištenja posredničkog poslužitelja

### Sustavi za detekciju upada

Temelje se na ideji da se praćenjem ponašanja sustava može detektirati incident

* Praćenje mrežnog prometa
* Praćenje ponašanja računala

Podjele

* Bazirane na pravilima i na detekciji ponašanja
* Mrežni (NIDS) i računalni sustavi (HIDS)

Mrežni sustavi se stavljaju na neke ključne točke na kojima snimaju promet - problem brzine

Mnoštvo različitih sustava na tržištu - popularna implementacija otvorenog koda - SNORT, OSSEC

### Sustavi za prevenciju upada

Osim detekcije rade i prevenciju - *Intrusion Prevention Systems* (IPS)

* Prevencija može biti postavljanje dodatnih pravila na vatrozidu
* Pravila privremena ili stalna
* Ako nisu dobro podešeni mogu onemogućiti ispravan rad mreže!

### Otkrivanje ranjivosti u mreži

Ranjivosti u računalnoj mreži su neizbježne(!) Treba ih što prije otkriti i ukloniti - otkrivanje ranjivosti može se obaviti na dva temelja načina:

* Skeniranje mrežnih raspona
  + Nessus, OpenVAS
  + Jednostavno, ali opterećuje mrežu i puno lažno točnih detekcija
  + Jeftina, ali ne otkrivaju nužno sve ranjivosti
* Penetracijska ispitivanja
  + Obavljaju pojedinci ili timovi koji traže ranjivosti
  + Cilj je i pokušati iskoristiti ranjivost, ne samo ju naći
  + Skuplja od skeniranja, ne otkrivaju nužno sve ranjivosti

# Sigurnost baza podataka

## Baze podataka i sustavi za upravljanje bazama podataka

**Baza podataka** - skup međusobno povezanih podataka, pohranjenih zajedno, uz isključenje bespotrebne zalihosti (redundancije), koji mogu zadovoljiti različite primjene. Podaci su pohranjeni na način neovisan o programima koji ih koriste. Prilikom dodavanja novih podataka, mijenjanja i pretraživanja postojećih podataka primjenjuje se zajednički i kontrolirani pristup. Podaci su strukturirani tako da služe kao osnova za razvoj budućih primjena.

sustav za upravljanje bazom podataka (SUBP) - programski sustav koji:

* omogućava upravljanje podacima u bazi podataka
* može istovremeno upravljati s više baza podataka
* upravlja istovremenim pristupom bazi podataka od strane više korisnika/aplikacija uz osiguravanje sigurnosti i integriteta baze podataka
* temelji se na odabranom modelu podataka (hijerarhijski, mrežni, **relacijski,** objektnorelacijski, objektno-orijentirani)

**Zadaće SUBP-a**

* trajna pohrana podataka (*persistent storage*)
  + skriva od korisnika detalje fizičke pohrane podataka
  + osigurava logičku i fizičku nezavisnost podataka
* osiguravanje programskog sučelja (*programming interface*)
  + omogućuje definiciju i rukovanje s podacima
    - DDL - Data Definition Language
    - DML - Data Manipulation Language
* optimiranje metoda pristupa podacima (*query optimization*)
* zaštita podataka
  + integritet podataka (*integrity*)
  + pristup podacima - autorizacija, sigurnost (*security*)
  + potpora za upravljanje transakcijama
    - Upravljanje istodobnim pristupom (*concurrency control*)
    - obnova u slučaju razrušenja (*recovery*)

**Administratori**

* organiziraju, nadziru i optimiziraju korištenje SUBP-a
* odgovorni za cjelokupnu sigurnost SUBP-a
* administrator poslužitelja baze podataka (*database server administrator* – DBSA)
  + instaliranje i nadogradnja SUBP-a; kreiranje novog korisnika; autorizacija na razini SUBP-a
* administrator baze podataka (*database administrator* - DBA)
  + autorizacija na razini baze podataka (provođenje sigurnosne politike)
  + dodjeljivanje i ukidanje ovlasti korisniku baze podataka
  + dodjeljivanje sigurnosne klasifikacijske razine korisniku u višerazinskom sigurnosnom sustavu, u skladu s politikom organizacije

SQL-sjednica (*SQL-session*) je kontekst u kojem jedan korisnik obavlja niz SQL naredbi putem jedne veze (*SQL-Connection*) prema sustavu za upravljanje bazama podataka

* započinje u trenutku kada korisnik, upotrebom klijentske aplikacije, ostvari vezu (*connect*) sa SUBP-om
* završava u trenutku kada korisnik prekine vezu (*disconnect*) prema SUBP-u

## Sigurnost baze podataka

baze podataka se osigurava zaštitom na nekoliko razina:

* **na razini SUBP**
  + spriječiti pristup bazama podataka ili onim dijelovima baza podataka za koje korisnici nisu ovlašteni
* **na razini operacijskog sustava**
  + spriječiti pristup radnoj memoriji računala ili datotekama u kojima SUBP pohranjuje podatke
* **na razini računalne mreže**
  + spriječiti presretanje poruka
* **fizička zaštita**
  + zaštita lokacije poslužitelja sustava za upravljanje bazama podataka
* **na razini korisnika**
  + spriječiti da ovlašteni korisnici bilo nepažnjom bilo namjerno omoguće neovlaštenim osobama pristup podacima

***Defense-in-depth* strategija -**  zaštita u više slojeva

* ne postoji savršeni zaštitni sloj, metoda ili proizvod
* proboj jednog sloja ne mora značiti i narušavanje sigurnosti podataka iz baze podataka
* nužna zaštita unutar baze podataka, čak i ako je implementiran poseban sustav zaštite baze podataka izvan baze podataka

*neki od postupaka kojima je bazu podataka moguće učiniti sigurnijom:*

* ograničiti pristup g p p važnim resursima koji mogu biti pogrešno korišteni, zlonamjerno ili slučajno kao posljedica pogreške - vatrozidi; upravljanje pristupom; virtual private networks (VPN); antivirusna zaštita
  + upravljanje zakrpama (*patches*)
  + sustavi za otkrivanje i sprječavanje upada (*Intrusion prevention systems* - IPS , *Intrusion detection systems* - IDS)
* onemogućiti nepotrebne komponente i servise sustava za upravljanje bazama podataka (npr. Oracle: XML FTP; SQL Server: Named Pipes access)
* ukloniti/onemogućiti nepotrebne pretpostavljene korisničke račune i lozinke
* izvoditi procese baze podataka pod namjenskim, neprivilegiranim korisničkim računom

### Načelo najmanje ovlasti i razdvajanje dužnosti

načelo **najmanje ovlasti** (*least privilege*)

* korisnik ima minimalan skup dozvola koje su neophodne za njegov trenutni zadatak
* pojedinac ima različite razine ovlasti u različito vrijeme, ovisno o zadaći ili funkciji koju obavlja
* spriječeno obavljanje nepotrebnih i moguće štetnih akcija

**razdvajanje dužnosti** *(separation of duty -* SoD*)*

* osjetljive zadatke u cijelosti ne može obaviti samo jedan korisnik
* smanjuje se mogućnost zloporabe (važno načelo u financijskim i vojnim okruženjima)

**Mehanizmi zaštite na razini SUBP**

* identifikacija i dokazivanje autentičnosti
* upravljanje pristupom
* šifriranje podataka
* praćenje pristupa podacima
* maskiranje podataka

### Integritet i sigurnost baze podataka

Pojmovi *integritet* i *sigurnost* baze podataka se često spominju zajedno, međutim radi se o dva

različita aspekta zaštite podataka

**Integritet baze podataka** (*database integrity*) - operacije nad podacima koje korisnici obavljaju **su ispravne** (tj. uvijek rezultiraju konzistentnim stanjem baze podataka)

* + "podaci se štite od ovlaštenih korisnika"

**Sigurnost baze podataka** (*database security*) - korisnici koji obavljaju operacije nad podacima **su ovlašteni** za obavljanje tih operacija

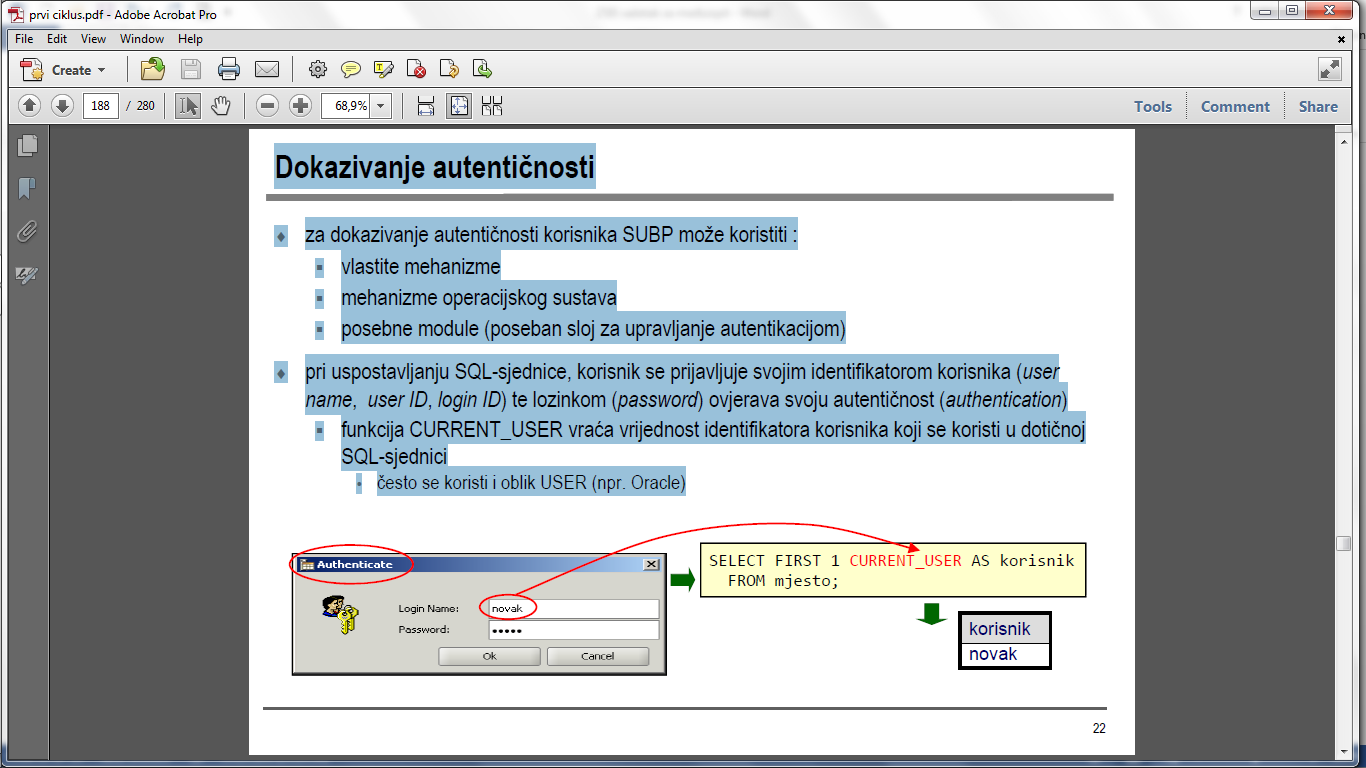
* + "podaci se štite od neovlaštenih korisnika"

Među ovim pojmovima postoje i sličnosti. U oba slučaja:

* moraju biti definirana pravila koja korisnici ne smiju narušiti
* pravila se pohranjuju u rječnik podataka
* nezaobilazna su za sve korisnike
* ne opterećuju aplikacijske programe
* SUBP nadgleda rad korisnika i osigurava poštivanje pravila

**Dokazivanje autentičnosti**

* za dokazivanje autentičnosti korisnika SUBP može koristiti :
  + vlastite mehanizme
  + mehanizme operacijskog sustava
  + posebne module (poseban sloj za upravljanje autentikacijom)
* pri uspostavljanju SQL-sjednice, korisnik se prijavljuje svojim identifikatorom korisnika (*user name*, *user ID*, *login ID*) te lozinkom (*password*) ovjerava svoju autentičnost (*authentication*)
* funkcija CURRENT\_USER vraća vrijednost identifikatora korisnika koji se koristi u dotičnoj SQL-sjednici
  + često se koristi i oblik USER (npr. Oracle)



### IBM Informix: Dokazivanje autentičnosti

interna autentikacija

lozinka pohranjena u poslužitelju baze podataka (*sysIntAuthUsers* tablica *sysUser* baze podataka) - šifrirana SHA-256 algoritmom (*Secure Hash Algorithm*)

operacijski sustav

posebni moduli (autentikacijski slojevi), npr:

* Pluggable Authentication Modules (PAM)

• za IBM Informix na UNIX i Linux OS

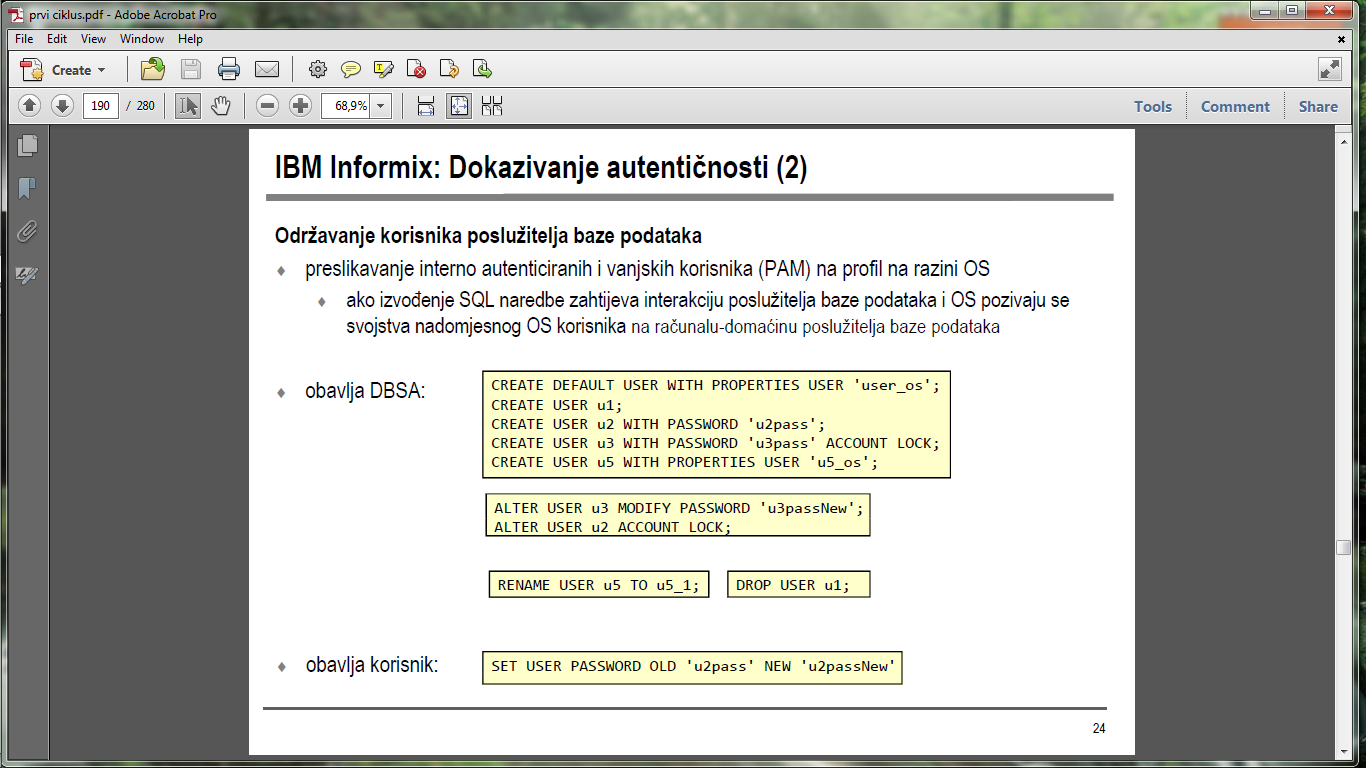
• API za upravljanje autentikacijom, korisničkim računima, sjednicama i lozinkama

* Lightweight Directory Access Protocol (LDAP) Authentication Support za Windows

• za autentikaciju korisnika koristi se LDAP poslužitelj

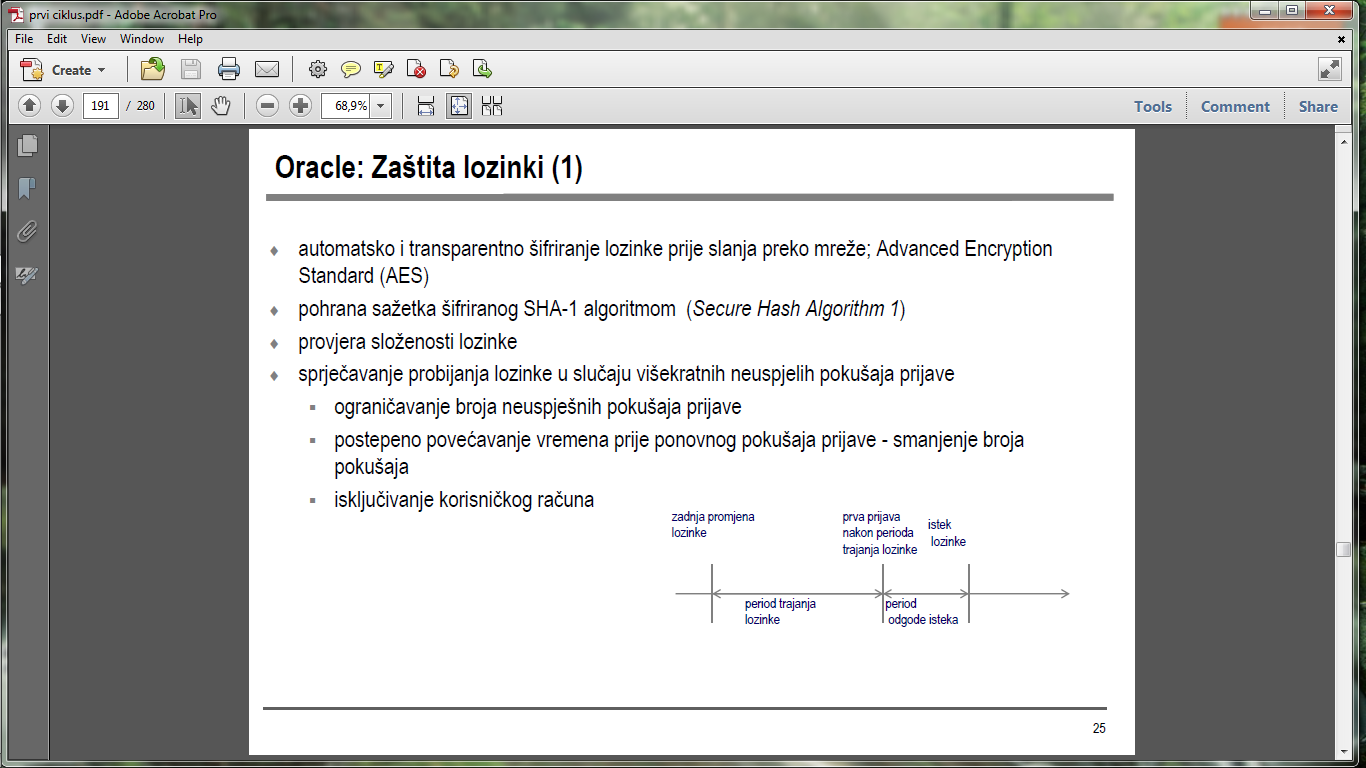
**Održavanje korisnika poslužitelja baze podataka**

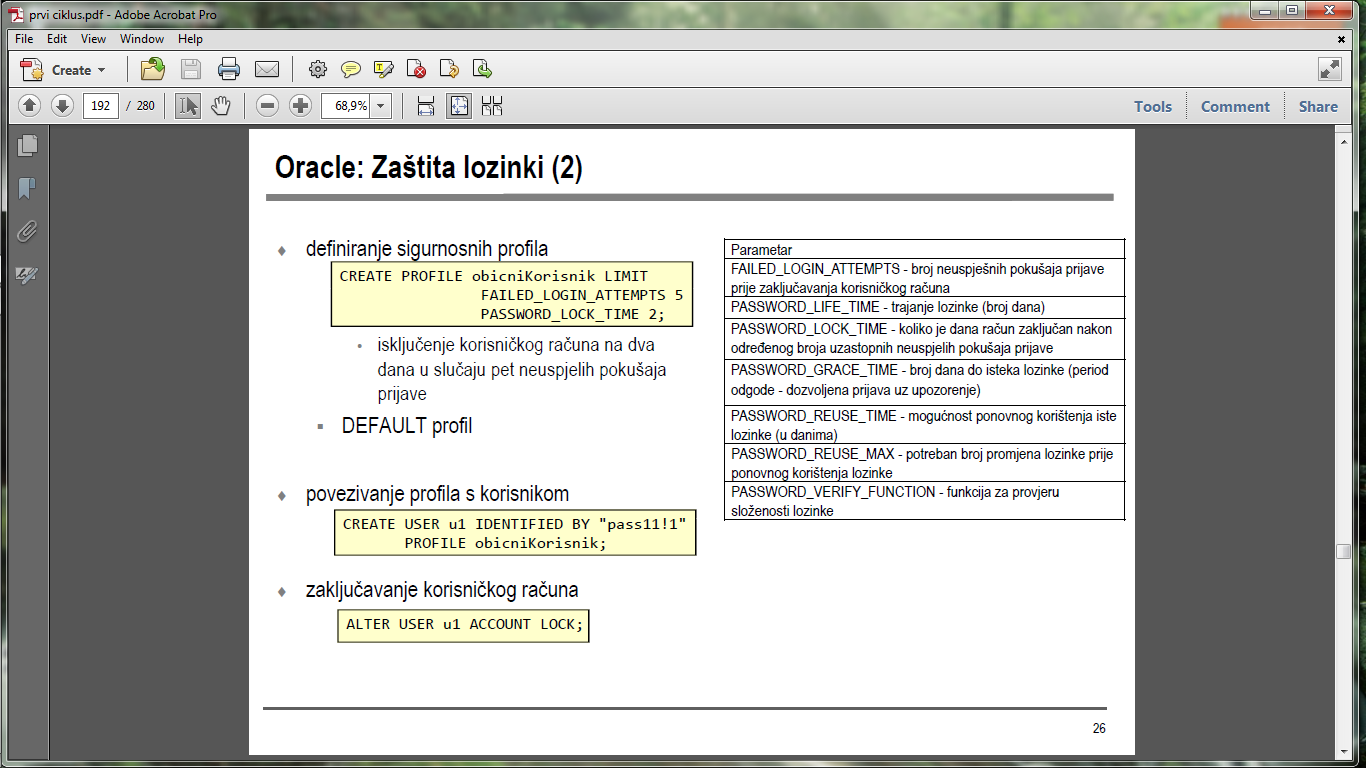
* preslikavanje interno autenticiranih i vanjskih korisnika (PAM) na profil na razini OS
* ako izvođenje SQL naredbe zahtijeva interakciju poslužitelja baze podataka i OS pozivaju se svojstva nadomjesnog OS korisnika na računalu-domaćinu poslužitelja baze podataka



### Oracle: Zaštita lozinki

* automatsko i transparentno šifriranje lozinke prije slanja preko mreže; Advanced Encryption Standard (AES)
* pohrana sažetka šifriranog SHA-1 algoritmom (*Secure Hash Algorithm 1*)
* provjera složenosti lozinke
* sprječavanje probijanja lozinke u slučaju višekratnih neuspjelih pokušaja prijave
  + ograničavanje broja neuspješnih pokušaja prijave
  + postepeno povećavanje vremena prije ponovnog pokušaja prijave - smanjenje broja pokušaja
  + isključivanje korisničkog računa





## Upravljanje pristupom

* niz postupaka kojima se utvrđuje i evidentira pokušaj pristupa, te odobrava ili odbija pristup na temelju unaprijed utvrđenih pravila
* razvoj sustava za upravljanje pristupom - višefazni proces
* ***sigurnosna politika*** *-* pravila pristupa na visokoj razini (zakonski, socijalni, etički aspekt)
  + temeljena na načelu *treba-znati* (*need-to-know*), kompetentnosti, nadležnosti, sukobu interesa…
  + na nju mogu utjecati zakonska i etička pitanja, politike na državnoj ili korporativnoj razini …
  + dinamična - mijenja se u skladu s promjenama poslovnih faktora, regulativa i uvjeta u okruženju
  + problem preslikavanja nejasnih i dvosmislenih zahtjeva u dobro definirana i jednoznačna pravila
* ***sigurnosni model*** *-* formalni prikaz sigurnosne politike (strategijski aspekt)
  + ***diskrecijsko upravljanje pristupom*** (*discretionary access control* - DAC)
  + ***mandatno upravljanje pristupom*** (*mandatory access control* - MAC)
  + ***upravljanje pristupom temeljeno na ulogama*** (*role-based access control* - RBAC)
* ***sigurnosni mehanizam*** *-* (operativni aspekt) funkcije kojima je implementirano upravljanje pristupom

**Mehanizmi upravljanja pristupom**

* *referentni monitor* (*reference monitor*) - pouzdana komponenta koja upravlja svakim pokušajem pristupa objektu sustava i utvrđuje je li taj pristup u skladu sa sigurnosnom politikom utjelovljenom u bazi podataka upravljanja pristupom
* uspoređuje sigurnosne atribute korisnika (npr. identifikator korisnika, grupa kojoj korisnik pripada, razina povjerenja iskazana korisniku) s onima koje imaju resursi (npr. Oznaka osjetljivosti)
* preduvjet: uspješna identifikacija i autentikacija korisnika
* **autorizacija** - postupak evidentiranja pravila pristupa
  + informacije koje opisuju prava pristupa moraju biti zaštićene od izmjene
  + sigurnosni mehanizmi implementirani kroz SQL

**Elementi sustava za upravljanje pristupom**

* **korisnik** – entitet koji koristi računalni sustav (osoba, uređaj)
  + *sjednica* (*session*) - instanca dijaloga korisnika sa sustavom
* **subjekt** – aktivni entitet koji može inicirati zahtjev za obavljanje operacija na objektima
  + proces koji djeluje u ime korisnika
  + korisnik može imati više aktivnih subjekata
* **objekt** - entitet sustava na kojem može biti obavljena operacija
* **operacija** - aktivan proces pozvan od strane subjekta, koji nakon poziva izvršava funkcije
* **dozvola** (*pravo pristupa*, *ovlast*) određenog načina pristupa objektu u sustavu
  + kombinacija objekta i operacije
    - za omogućavanje izvođenja iste operacije (npr. SELECT) na dva različita objekta (npr. tablice *student* i *predmet*) potrebne dvije dozvole
    - za omogućavanje obavljanja dvaju različitih operacija (npr. UPDATE i SELECT) na istom objektu (npr. tablici *student*) potrebne su dvije dozvole
  + **pozitivna** dozvola - ako ne postoji, zatraženi pristup je odbijen
  + **negativna** dozvola - ako postoji, zatraženi pristup je odbijen

**Elementi sustava za upravljanje pristupom – dozvola**

klasični pristupi upravljanja pristupom:

* **zatvorena politika** *-* dozvoljen pristup za koji postoji (pozitivna) dozvola
* **otvorena politika** *-* uskraćen pristup za koji postoji (negativna) dozvola

• ako dozvola ne postoji, pristup je dozvoljen

problemi kod kombiniranog korištenja pozitivnih i negativnih dozvola:

* *nepotpunost* - za pristup nije specificirana dozvola
  + može se izbjeći definiranjem pretpostavljene politike
* *nekonzistentnost* - za pristup postoji i negativna i pozitivna dozvola
  + može se izbjeći definiranjem politike razrješavanja konflikata

politike razrješavanja konflikata:

* *nepostojanje konflikata* – postojanje konflikta smatra se pogreškom
* *prioritetne su negativne dozvole*
* *prioritetne su pozitivne dozvole*
* *ništa nema prioritet –* istovremeno postojanje konfliktnih dozvola poništava te dozvole (kao da nije specificirana nikakva dozvola)

## Diskrecijsko upravljanje pristupom

upravljanje pristupom na temelju:

* identiteta korisnika koji zahtijeva pristup i
* eksplicitnih pravila pristupa koja utvrđuju tko može izvesti koje akcije na kojim objektom sustava

koncept vlasništva nad objektom - vlasnik objekta određuje kome se dozvoljava pristup

**Matrica autorizacijskih pravila (Matrica pristupa)**

**System R model**

* dozvole - *select*, *update*, *insert*, *delete*, *drop*
* subjekt koji kreira tablicu – vlasnik (ima sve ovlasti nad tablicom)
* dozvola s mogućnošću prenošenja (GRANT opcija)
  + subjekt kojemu je vlasnik dodijelio dozvolu može tu dozvolu dodijeliti drugim subjektima (bez ili sa GRANT opcijom)
* ukidanje dozvola
  + kaskadno, na temelju trenutka dodjeljivanja
    - ukidaju se sve dozvole koje je dodijelio korisnik kojem se ukida dozvola, a koje ne bi mogle biti dodijeljene bez postojanja dozvole koja se ukida
    - ukidanje dozvola se iterativno primjenjuje na sve korisnike koji su primili dozvole pristupa od svih korisnika s kojih je dozvola povučena
  + zahtijeva pamćenje povijesti i vremena dodjeljivanja dozvola

**Diskrecijsko upravljanje pristupom u bazama podataka**

* određenom korisniku potrebno je eksplicitno dodijeliti dozvolu za obavljanje određene operacije nad određenim objektom (autorizacija)
* dozvole su opisane trojkama <p j *korisnik*, *objekt*, *vrsta operacije*>, npr:

<horvat, ispit, čitanje>

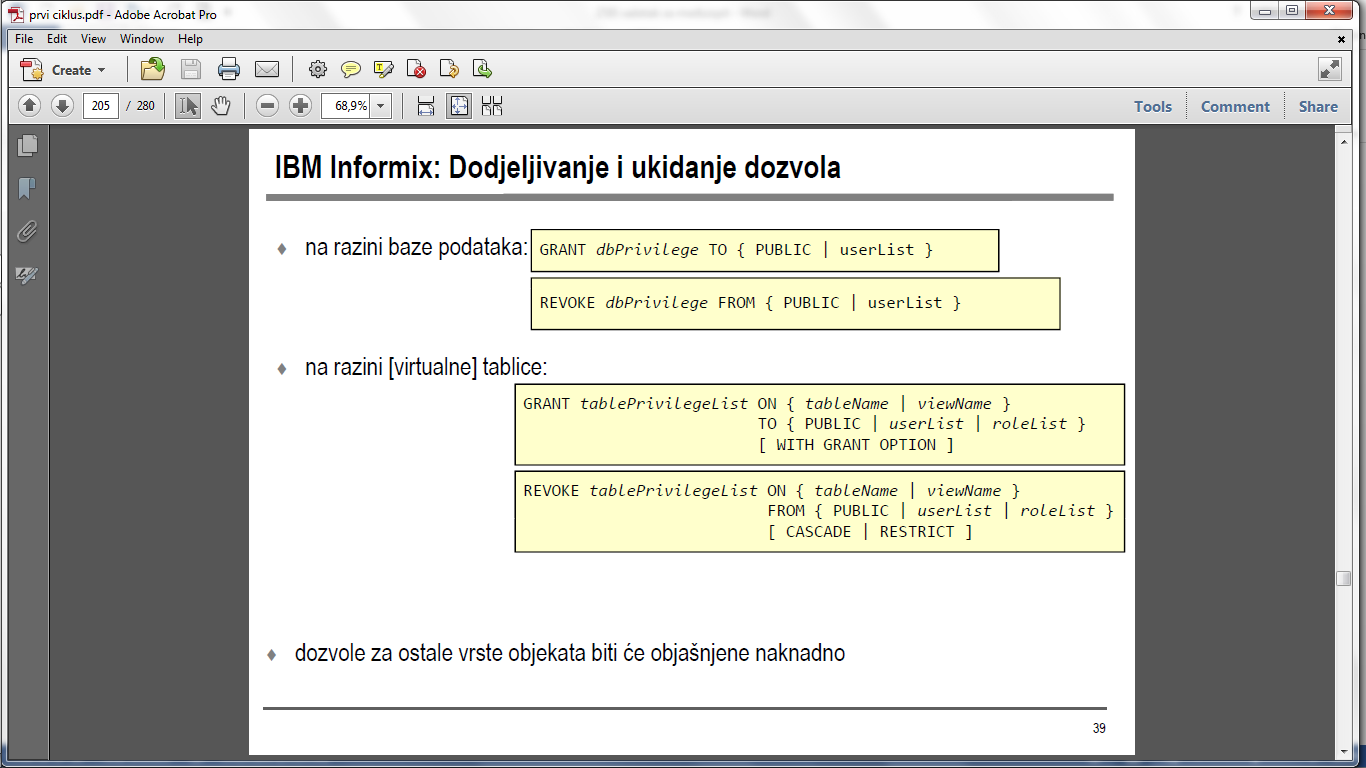
<horvat, ispit, izmjena>

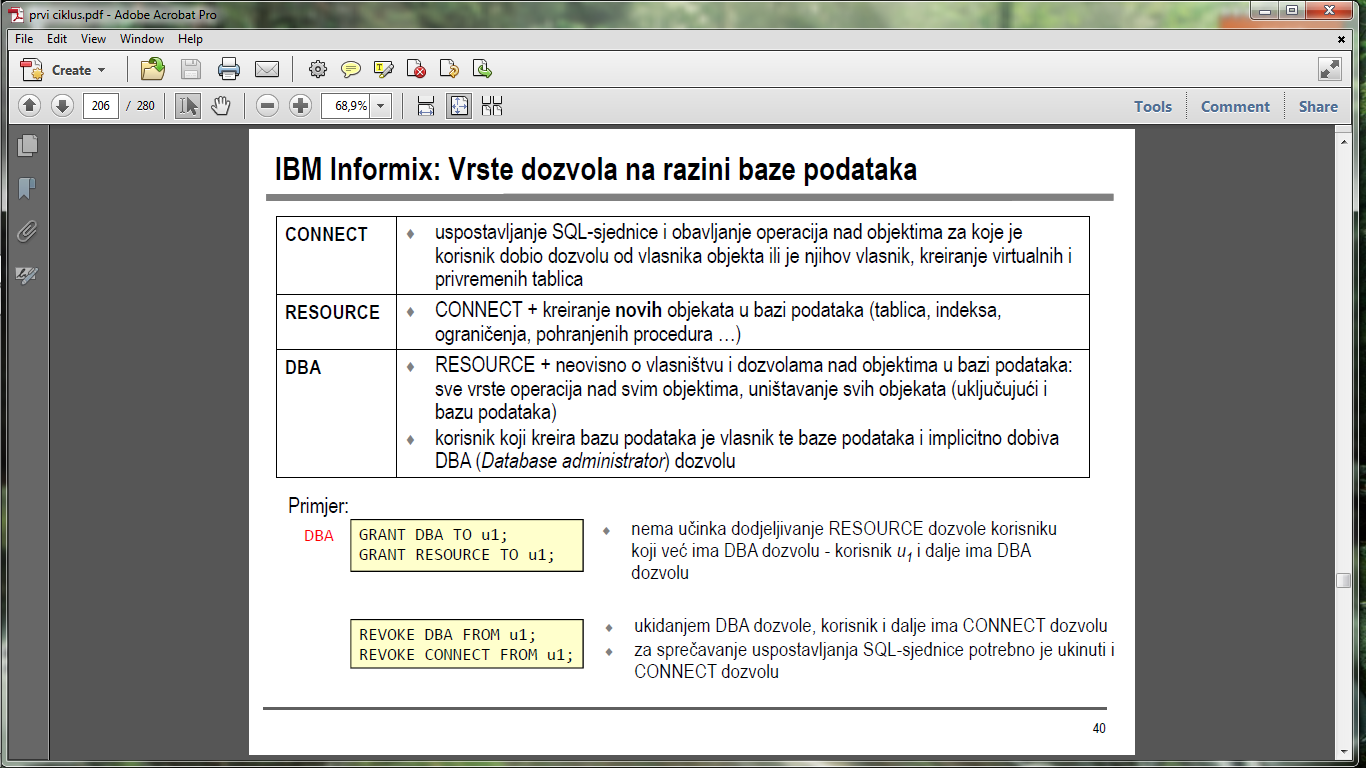
<novak, predmet, čitanje>

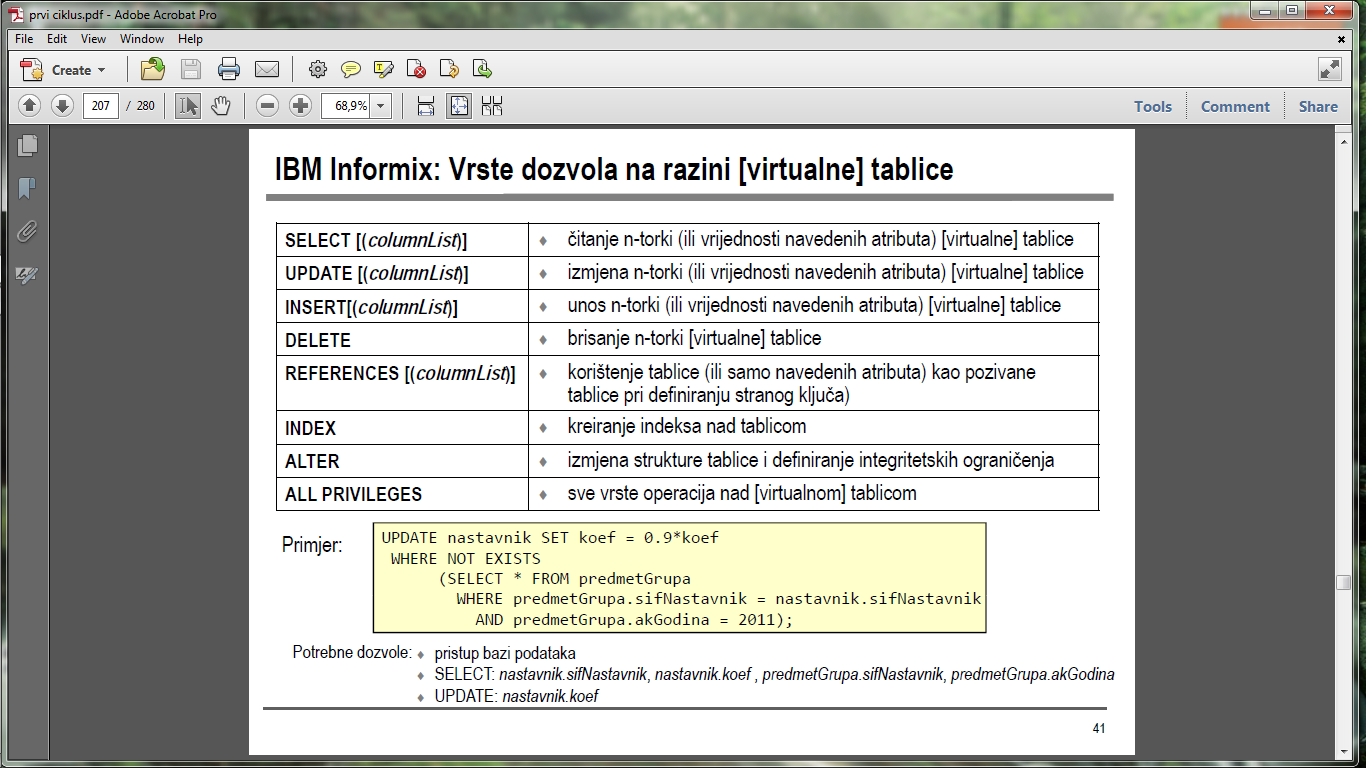
* podaci o dodijeljenim dozvolama pohranjuju se u rječnik podataka
* prije obavljanja svake operacije, SUBP provjerava ima li korisnik dozvolu za obavljanje operacije nad objektom (upravljanje pristupom )
* kada korisnik *novak* pokuša obaviti operaciju čitanja objekta (tablice) *predmet*, SUBP provjerava postoji li dozvola u obliku trojke <novak, predmet, čitanje>

**Upravljanje pristupom u SQL-u**

* **Mehanizmi upravljanja pristupom**
  + naredbe za dodjeljivanje (GRANT) i ukidanje dozvola (REVOKE)
  + virtualne tablice (view)
  + pohranjene procedure
  + modifikacija upita
* **Objekti**
  + tablica (table)
  + atribut (stupac tablice, column)
  + virtualna tablica (pogled, view)
  + pohranjena procedura
  + baza podataka (neki sustavi, npr. IBM Informix)
* **Vlasnik objekta** - korisnik koji je kreirao objekt
  + implicitno dobiva dozvole za obavljanje svih vrsta operacija nad objektom, uključujući
  + dozvole za dodjeljivanje svih vrsta dozvola nad tim objektom drugim korisnicima i
  + uništavanje objekta

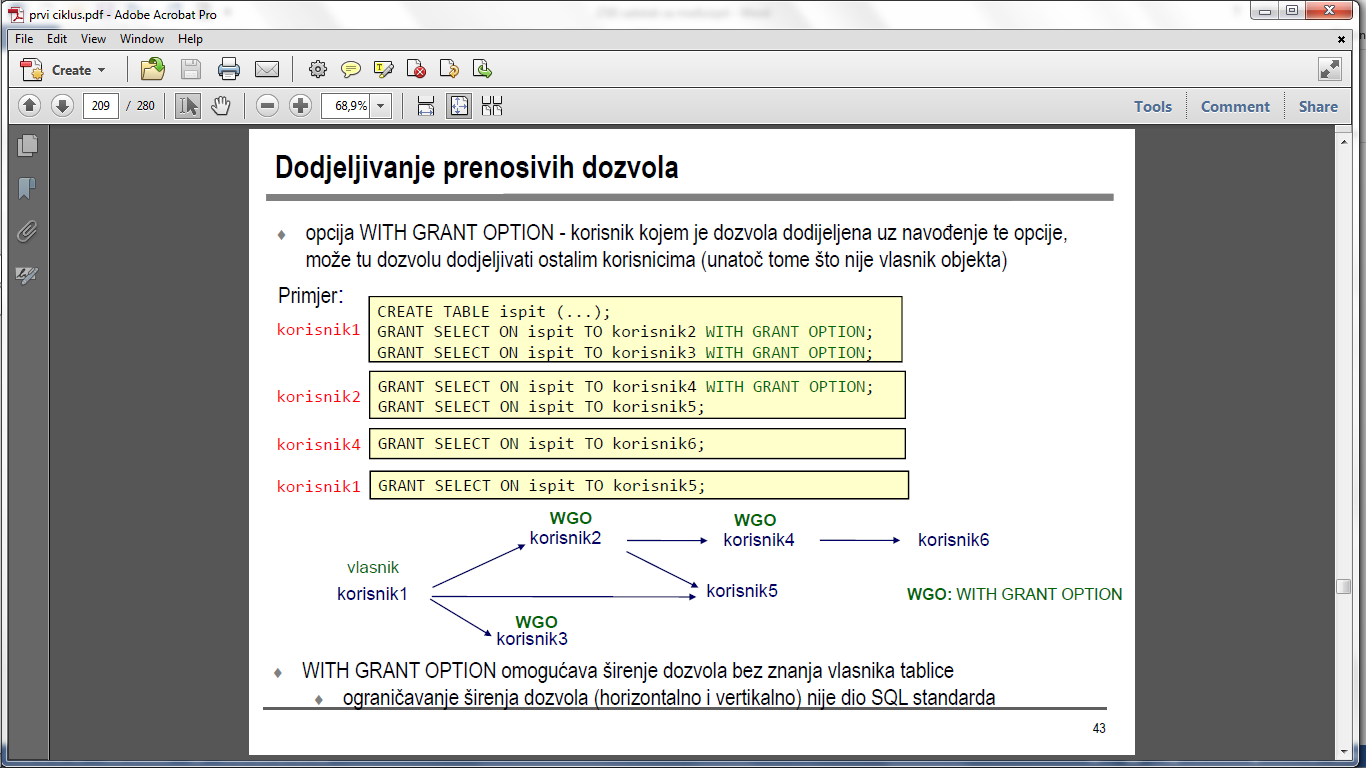






**"korisnik" PUBLIC -** dodjelom dozvole "korisniku" PUBLIC, dozvolu za obavljanje operacije dobivaju svi sadašnji i budući korisnici

* to **ne znači** dodijeliti pojedinačne dozvole svakom od korisnika koji se nalazi u nekom trenutno postojećem, konačnom skupu korisnika



### ORACLE: kategorije dozvola

dozvole se mogu svrstati u dvije općenite kategorije:

* sistemske dozvole
  + omogućavaju izvršavanje različitih tipova naredbi
  + ne odnose se na neki konkretni objekt baze podataka, već na određenu operaciju ili klasu
  + operacija nad tipom objekta
  + neke od sistemskih dozvola su: CREATE USER; ALTER USER; DROP USER; CREATE SESSION; CREATE ANY INDEX; ALTER ANY INDEX; DROP ANY INDEKS; CREATE TABLE;CREATE ANY TABLE; ALTER ANY TABLE; CREATE ANY VIEW; DROP ANY VIEW; CREATE PROCEDURE; CREATE ANY PROCEDURE; EXECUTE ANY PROCEDURE
* dozvole nad objektima
  + GRANT CREATE SESSION TO u1; (korisniku *u1* dozvoljeno je uspostavljanje SQL-sjednice)
  + omogućavaju obavljanje određenih operacija na određenom objektu baze podataka
  + npr. SELECT, UPDATE, INSERT i DELETE operacije na tablicama, ALTER, REFERENCES, INDEX i ALL na tablicama, EXECUTE na pohranjenim procedurama

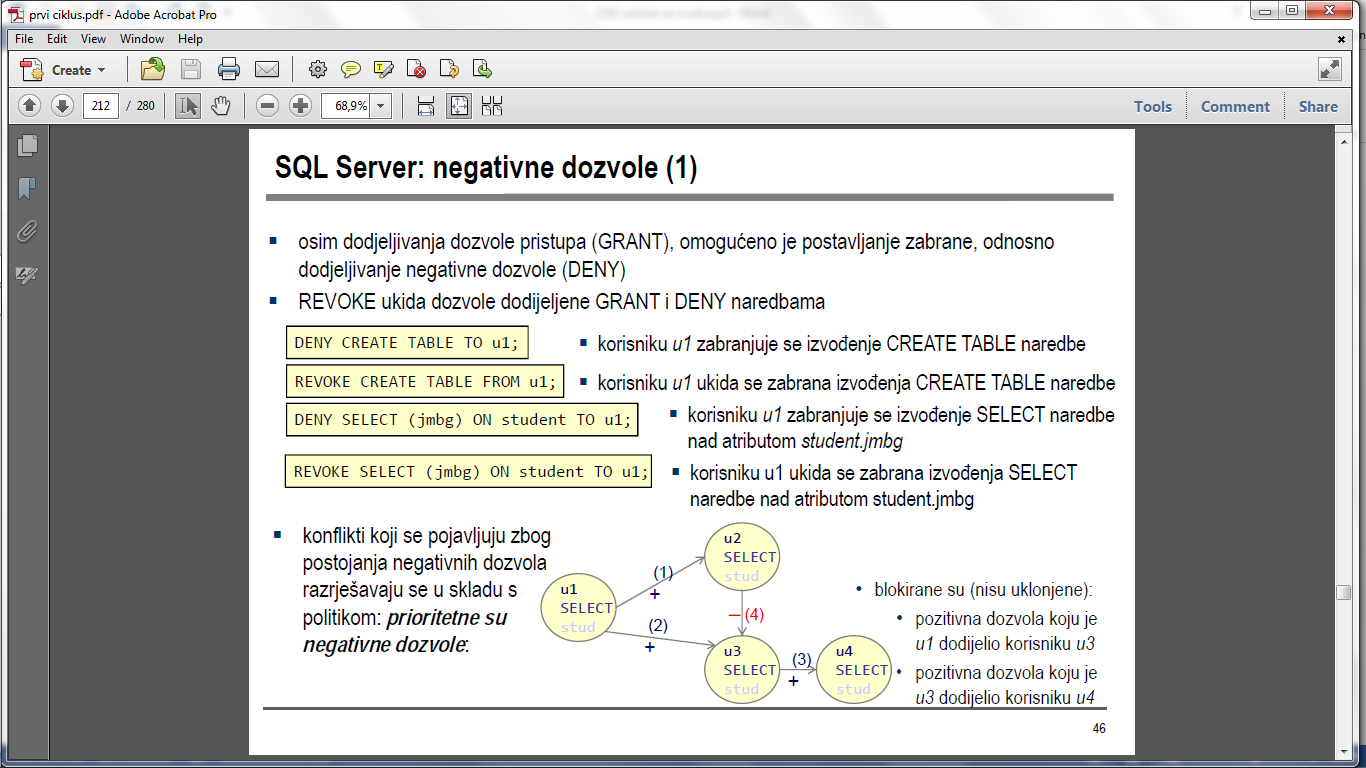
### SQL Server: kategorije dozvola

dozvole se mogu svrstati u dvije općenite kategorije:

• dozvole obavljanja naredbi – upravljaju obavljanjem naredbi kao što su CREATE TABLE,

CREATE VIEW, CREATE FUNCTION, CREATE PROCEDURE, itd.

• dozvole nad objektima baze podataka – upravljaju obavljanjem operacije na postojećem objektu baze podataka, npr. DELETE, INSERT, SELECT, UPDATE, EXECUTE, REFERENCES …



### Upravljanje pristupom ovisno o sadržaju i kontekstu

upravljanje pristupom *ovisno o sadržaju* (*content-dependent, value-dependent, datadependent*)

* + pristup objektu na temelju sadržaja jedne ili više njegovih komponenata

upravljanje pristupom *ovisno o kontekstu* (*context-dependent, system-dependent*)

* + pristup objektu ovisi o trenutnom kontekstu - u obzir uzima predikate sustava (vrijeme, lokacija …), trenutnog korisnika

dva načina implementacije upravljanja pristupom ovisne o sadržaju i kontekstu:

* + definiranje virtualnih tablica koje odabiru objekt čiji sadržaj zadovoljava dani uvjet te dodjeljivanje dozvola na virtualne tablice, umjesto na temeljne tablice
    - podržano u svim komercijalnim SUBP- ovima
  + povezivanje predikata (ili logičke kombinacije predikata) s autorizacijama
    - predikat izražava uvjet nad sadržajem objekta koji mora biti zadovoljen kako bi pristup bio dozvoljen (podržan u Oracle SUBP-u)

### Virtualna relacija (*view*)

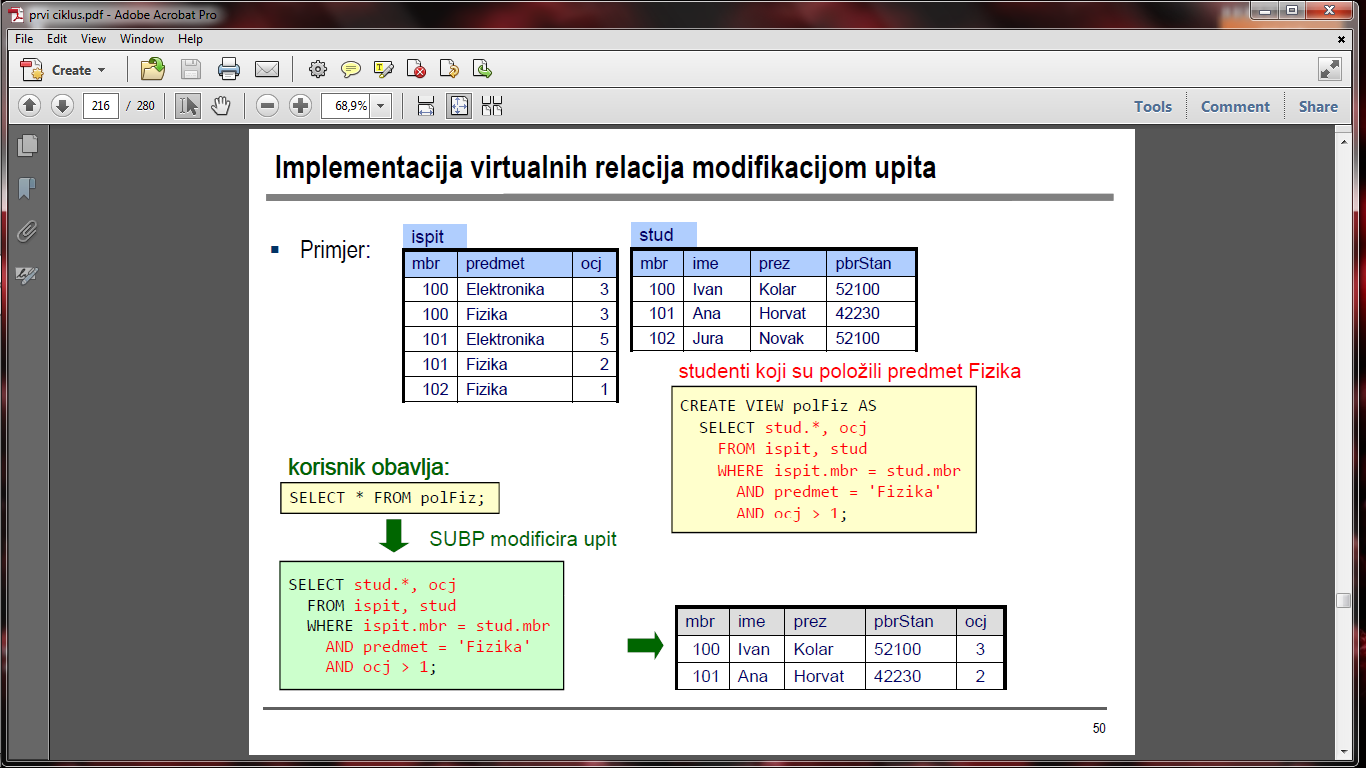
shema i sadržaj virtualne relacije definirani su izrazom relacijske algebre čiji su operandi

temeljne ili virtualne relacije - opisuju se u obliku SQL upita - naredbom CREATE VIEW

* u rječniku podataka pohranjena je definicija virtualne tablice
* sadržaj virtualne tablice uvijek odražava sadržaj temeljnih tablica u trenutku izvršavanja upita u kojem se virtualna tablica koristi

izvršavanje upita koji sadrže virtualne tablice:

* **modifikacija upita**
  + - SUBP ugrađuje elemente definicije virtualne tablice u originalni SQL upit koji koristi virtualnu tablicu - umjesto originalnog SQL upita izvršava se modificirani SQL upit
    - sadržaj virtualne tablice se određuje tek za vrijeme izvršavanja upita koji koristi virtualnu tablicu
* **korištenje materijalizirane virtualne tablice**
  + - SUBP fizički pohranjuje sadržaj virtualne tablice
    - promjenom sadržaja neke od temeljnih tablica pomoću kojih je virtualna tablica definirana, SUBP automatski mijenja i sadržaj materijalizirane virtualne tablice
    - prednost: sadržaj virtualne tablice koja se često koristi, a čiji se sadržaj određuje složenim upitima, ne mora izračunavati prilikom svakog korištenja virtualne tablice
    - nedostatak: ako se često mijenja stanje temeljne tablice pomoću koje je virtualna tablica definirana, troši se dodatno vrijeme radi izmjene sadržaja virtualne tablice



**izmjenjiva** (*updatable*) virtualna tablica - mora biti definirana tako da SUBP može jednoznačno

odrediti koje operacije treba obaviti na temeljnim tablicama u glavnom SELECT dijelu definicije virtualne tablice koristi atribute iz samo jedne temeljne tablice i pri tome:

• ne sadrži eliminaciju duplikata pomoću DISTINCT

• ne sadrži izraze u listi za selekciju (osim trivijalnih izraza koji sadrže samo ime atributa)

• izostavljeni atributi ne smiju imati NOT NULL ograničenje ili moraju imati pretpostavljenu (*default*) vrijednost

• ne sadrži spajanje ili uniju

• ne sadrži grupiranje i postavljanje uvjeta nad grupom (GROUP BY i HAVING)

navedena ograničenja se ne odnose na podupite unutar WHERE dijela SELECT naredbe

**WITH CHECK OPTION -** opcija CREATE VIEW naredbe - nije dozvoljena izmjena ili unos n-torke putem virtualne tablice ako n-torka nakon obavljanja operacije više ne bi pripadala virtualnoj tablici putem koje je izmijenjena ili unesena

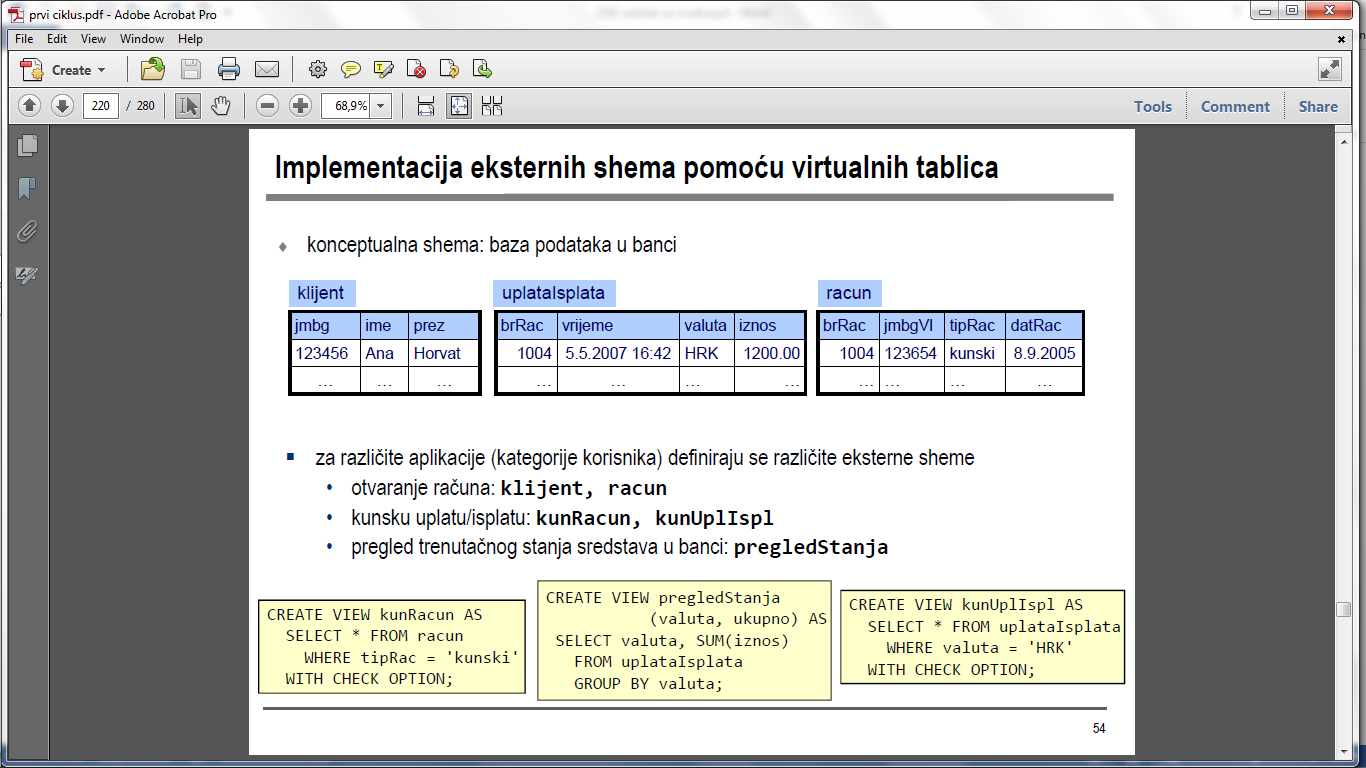
**Primjena virtualnih tablica u provođenju sigurnosne politike**

omogućavaju prikaz samo informacija koje su korisniku potrebne:

* zbirne informacije i/ili samo neke atribute tablice i/ili samo neke n-torke iz tablice
* korisniku se dodjeljuju ovlasti nad virtualnom tablicom

ovlasti dobivene pomoću virtualne tablice mogu biti:

* neovisne o vrijednostima - virtualna tablica sadrži samo neke atribute svih zapisa u temeljnoj tablici
* ovisne o vrijednostima - virtualna tablica sadrži samo neke n-torke iz temeljne tablice
* kontekstno ovisne - u definiciji virtualne tablice, kao uvjet dohvata koristi se informacija vezana uz kontekst prilikom izvođenja upita (korisnik, vrijeme izvođenja upita)



korisnik koji kreira virtualnu tablicu :

* postaje vlasnik virtualne tablice
* za uspješno kreiranje virtualne tablice mora imati dozvolu obavljanja SELECT naredbe za svaku tablicu uključenu u definiciju virtualne tablice
* ovlasti nad tom virtualnom tablicom ovise o njegovim ovlastima nad korištenim objektima:
  + - uvijek ima SELECT dozvolu
    - prenosivu SELECT dozvolu (s GRANT opcijom) ima samo ako ima prenosivu SELECT dozvolu za svaku korištenu tablicu
    - za izmjenjivu virtualnu tablicu bitne su njegove INSERT, DELETE ili UPDATE dozvole nad tablicom na čije se zapise kroz virtualnu tablicu utječe - automatski dobiva jednake dozvole i na tom pogledu

### Oracle Virtual Private Database (VPD)

implementacija upravljanja pristupom ovisnog o sadržaju i kontekstu, povezivanjem predikata s

dozvolama

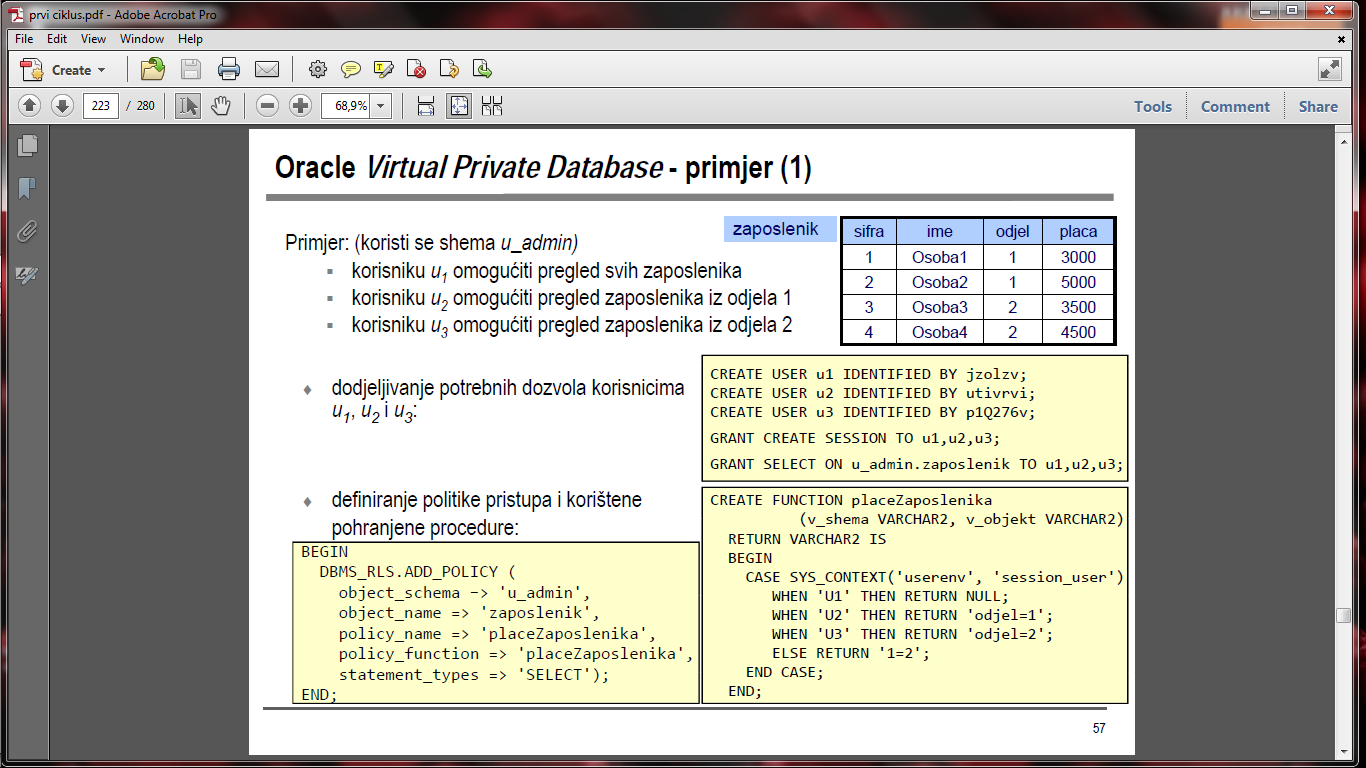
* predikat izražava uvjet nad sadržajem objekta koji mora biti zadovoljen da bi pristup bio dozvoljen
* navedeni uvjet automatski se dodaje u WHERE dio SQL naredbe koju je potrebno obaviti na [virtualnoj] tablici na koju se primjenjuje VPD sigurnosna politika
* alternativa korištenju virtualne tablice

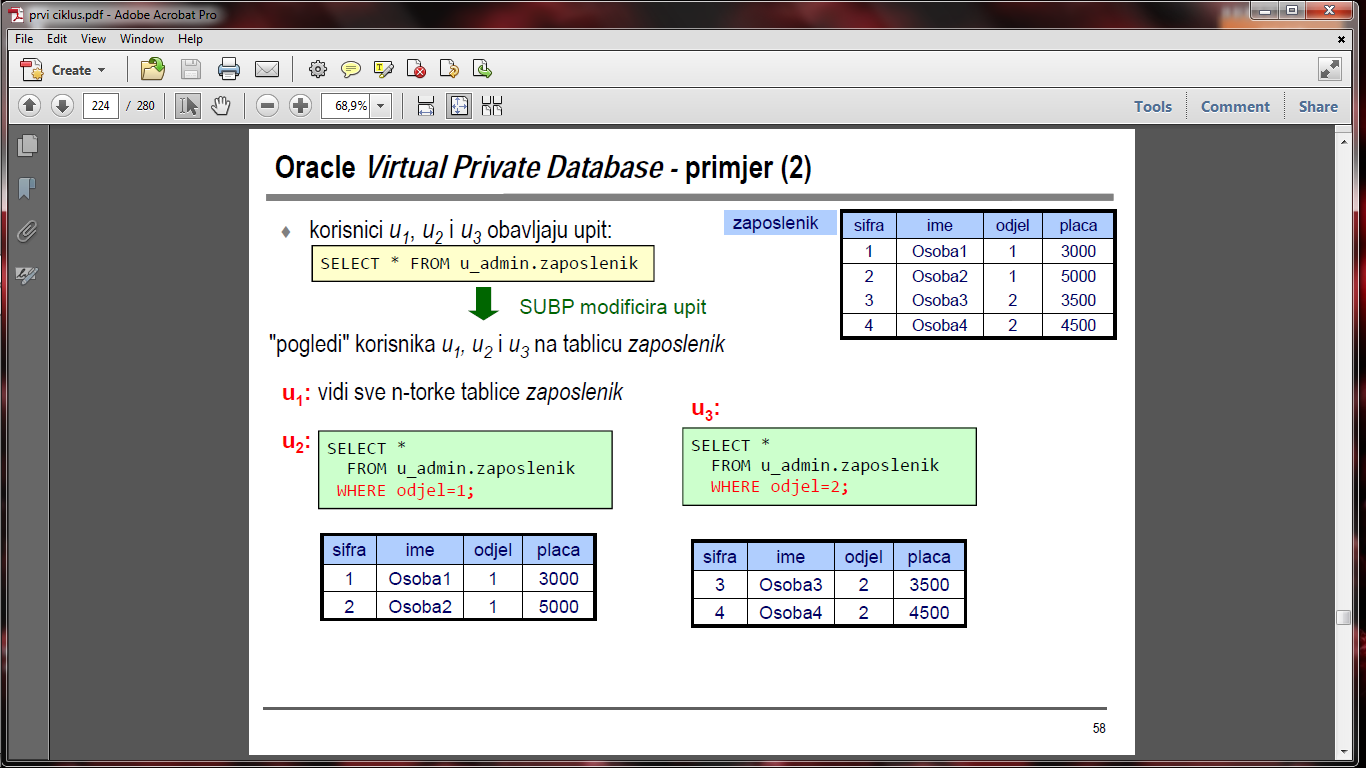
hoće li zapisi biti vidljivi korisniku ovisi o informacijama koje čuvaju (sadržaju i kontekstu)

umjesto skrivanja cijelog zapisa moguće je maskirati samo osjetljive podatke (vrijednosti samo

nekih atributa u zapisu)

ne može se zaobići - svaki upit koristi definiranu politiku koja uključuje korištenu tablicu





### Pohranjene procedure/funkcije

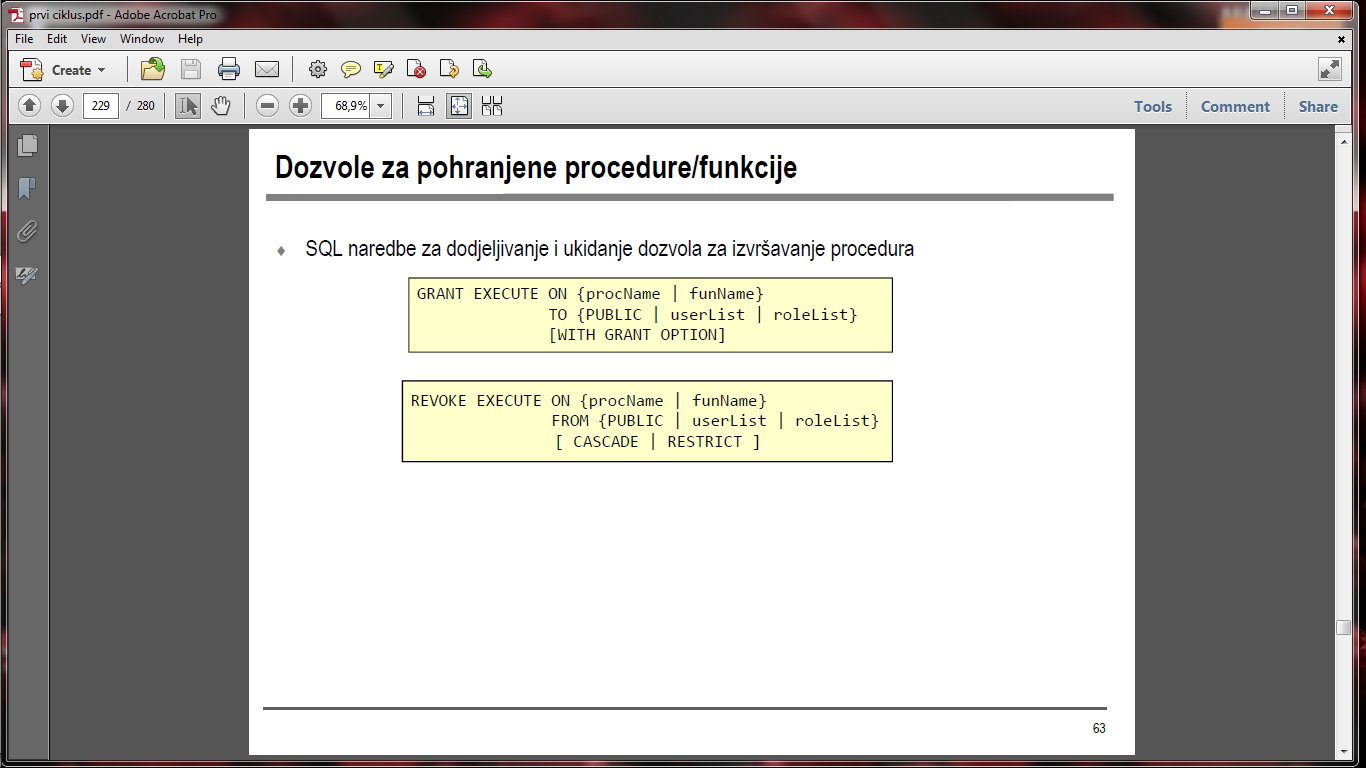
pohranjena procedura/funkcija je potprogram koji je pohranjen u rječniku podataka i koji se

izvršava u kontekstu sustava za upravljanje bazama podataka

* procedura je potprogram koji u pozivajući program ne vraća rezultat
* funkcija je potprogram koji u pozivajući program vraća rezultat
* koristi se i termin *pohranjena rutina* (*stored routine*)

SQL omogućuje zaštitu podataka od neovlaštene uporabe **na razini objekata** (tablice, atributi, virtualne tablice)

* korisniku se može ograničiti pristup do pojedinih objekata i vrsta operacije koju nad tim objektima može obaviti (brisanje, izmjena, unos, dohvat)
* nije moguće ograničiti na j g g čin na koji će korisnik obavljati operacije za koje je dobio dozvolu
* pohranjena procedura omogućuje zaštitu podataka od neovlaštene uporabe **na razini funkcija**
* korisniku se pridijeli dozvola za obavljanje definirane procedure, umjesto dozvole za pristup podacima
* time je precizno određen način na koji korisnik smije obaviti operacije nad podacima
  + - primjena dozvola u skladu s poslovnim pravilima ugrađenim u proceduru
    - princip najmanje ovlasti



## Mandatno upravljanje pristupom

*obavezno upravljanje pristupom (upravljanje pristupom na osnovi mandata)* - sigurnosna politika

na razini sustava određuje tko ima pravo pristupa, a ne vlasnik objekata

* primjenjiva u sustavima u kojima se dozvole dodjeljuju ovisno o poziciji korisnika u hijerarhiji neke organizacije (vojska, državna uprava, ...)
* svaki **objekt** dobiva oznaku klasifikacijske razine (*classification level*), npr. povjerljivo, tajno, ...
* odražava osjetljivost informacije sadržane u objektu
* svakom **korisniku** dodjeljuje se oznaka razine ovlasti (*clearance level*)
* korisnici mogu obavljati operacije nad onim objektima za koje imaju odgovarajuću razinu ovlasti

### BLP model

spriječiti tijek informacije od subjekata/objekata više razine prema subjektima/objektima nižih

(ili neusporedivih) razina

načela koja osiguravaju očuvanje tajnosti:

* **simple property** *(****no-read-up***) - subjektu je dozvoljeno čitanje iz objekta samo ako je klasa pristupa subjekta dominantna klasi pristupa objekta (tj. može čitati iz onih objekata kojima je njegova klasa pristupa dominantna)
* **\*-property** (***star-property*, *no-write-down***): subjektu je dozvoljeno pisanje u objekt samo ako je klasa pristupa objekta dominantna klasi pristupa subjekta

• nije moguće pisati u objekte koje mogu pročitati subjekti s nižom razinom - spriječeno propuštanje informacija

Primjer: koriste se tri klase pristupa sastavljene od sigurnosnih razina (S, C, U)

* relacija *ispit* ima sigurnosnu razinu S
* korisnik *u1* ima razinu ovlasti U: na sustav se može spojiti samo na razini U
  + može kreirati i čitati samo objekte razine U
  + kreira relaciju *xyz* koja ima sigurnosnu razinu U
* korisnik *u2* ima razinu ovlasti S: na sustav se može spojiti na razini S, C ili U
  + ako radi kao S subjekt: može čitati iz relacije *ispit*
  + ne može pisati u relaciju *xyz* koja ima razinu U (*no-write-down*)
* ako radi kao U subjekt: ne može čitati iz relacije *ispit* (*no-read-up*)

**Zajednička primjena DAC i MAC politike**

* DAC i MAC politike nisu međusobno isključive i mogu biti primijenjene zajedno
* DAC politika djeluje unutar granica mandatne politike i može samo spriječiti neki pristup koji bi uz primjenu samo MAC politike bio dozvoljen

**Mandatna politika pristupa u bazama podataka**

klasifikacija na razini: relacije; atributa; n-torke (zapisa); podatka

primjenjuju se osnovni principi MAC-a:

* *simple property* (*no-read-up*)
* *strong-star-property* (umjesto *\*-property*): korisnik može pisati isključivo na svojoj razini (radi sprječavanja uništenja npr. S-podataka od strane U-korisnika)

subjekti na različitim razinama imaju različite poglede na relaciju

* pogled je sastavljen samo od elemenata čijom klasifikacijom dominiraju
* nerazlikovanje NULL vrijednosti – neprikazani podatak može biti posljedica njegove NULL vrijednosti u bazi podataka ili posljedica tajnosti (klasifikacije) podatka

ograničenja radi sprječavanja narušavanja entitetskog integriteta na nekim razinama:

* atributi ključa - uniformno zaštićeni (klasificirani)
* zavisni atributi - klasifikacije dominantne klasifikaciji atributa ključa

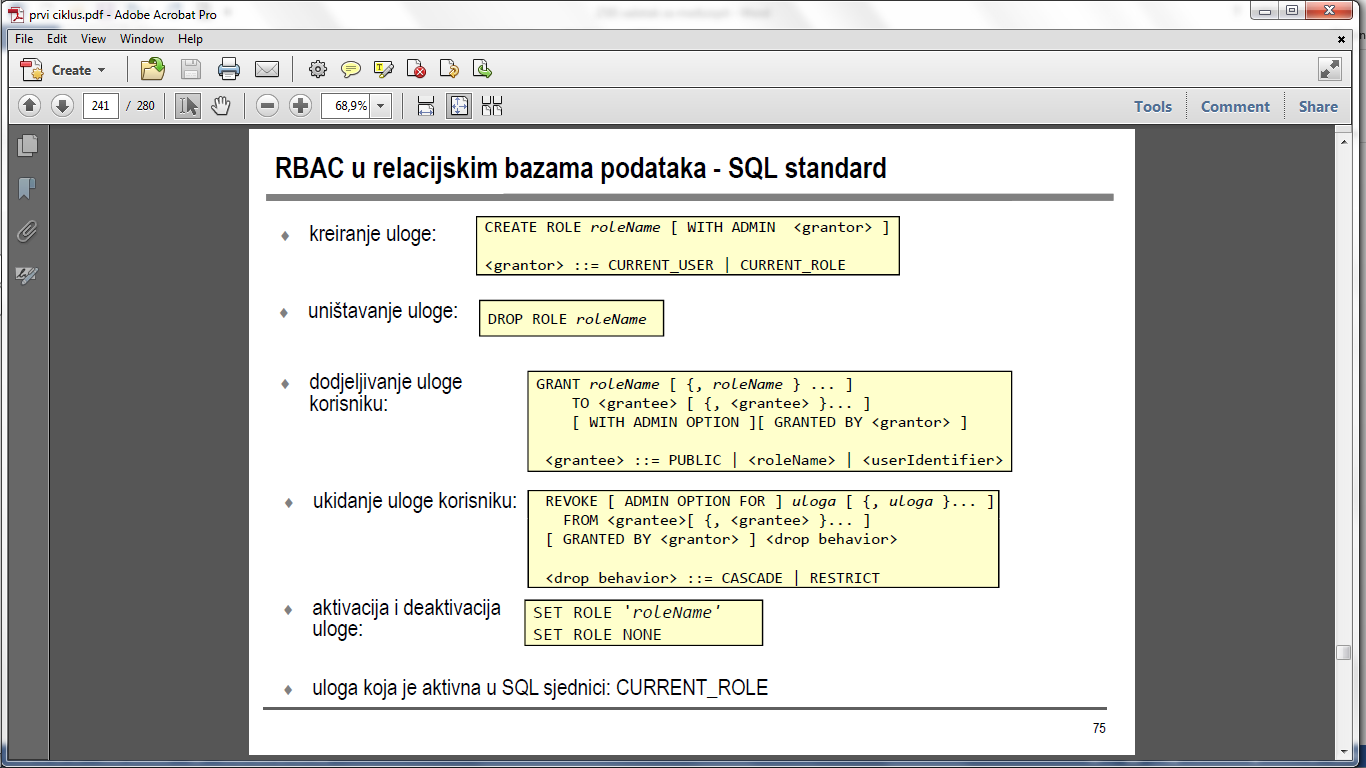
## Upravljanje pristupom temeljeno na ulogama

Osnovne postavke

* podaci vlasništvo poduzeća
  + korisnicima nije dozvoljeno donošenje odluka o pristupu
  + za upravljanje dozvolama zadužen je administrator za sigurnost
* odluke o pristupu temeljene na ulogama korisnika kao dijela organizacije
  + bolnica: liječnik i medicinska sestra; banka: blagajnik i računovođa

glavna osobina RBAC modela:

* svaki pristup podatkovnim objektima i resursima, potreban korisniku za obavljanje njegova zadatka, obavlja se kroz uloge
* uloga predstavlja poslovnu funkciju unutar organizacije
* ovlasti nad podatkovnim objektima i resursima potrebnim za obavljanje zadatka dodijeljene su ulogama umjesto pojedinim korisnicima
* korisnik je ovlašten za obavljanje odgovarajuće uloge



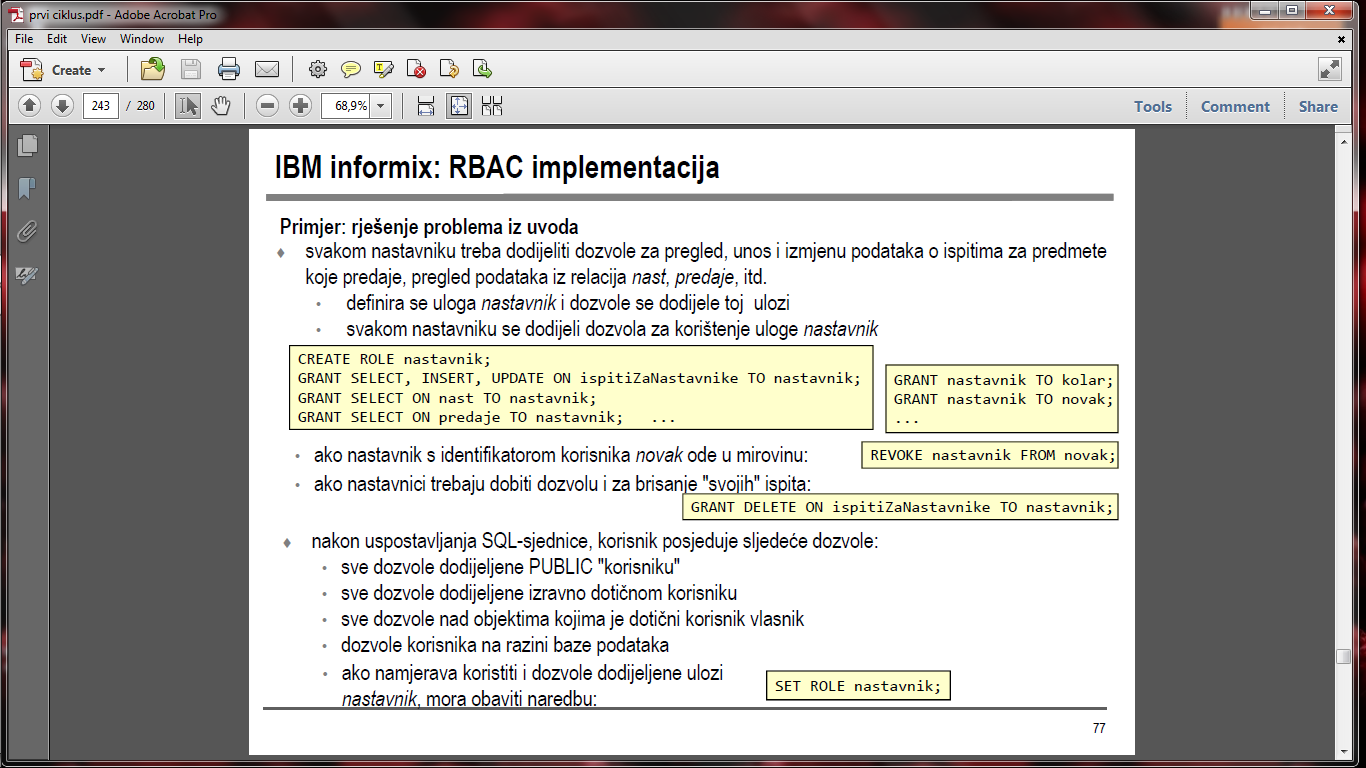
**Vrste uloga:**

* unaprijed definirane uloge
  + uloge s unaprijed definiranim i nepromjenjivim dozvolama
  + ne mogu biti pridružene drugim ulogama
* korisničke uloge
  + uglavnom kreirane od administratora
  + koriste se za pridruživanje dozvola korisnicima koji obavljaju iste poslovne funkcije
* aplikacijske uloge
  + kreirane od administratora
  + dodjeljuju se aplikaciji kroz koju korisnik pristupa podacima u bazi podataka

IBM Informix, Oracle, SQL Server

• omogućena izgradnja hijerarhije korisničkih uloga (uloga može biti dodijeljena drugoj ulozi)

• nije moguće navesti ograničenja nad ulogama



## Šifriranje podataka

dodatna razina zaštite ako neovlašteni korisnik uspije doći do podataka iz baze podataka

* prisluškivanjem komunikacijskih linija ili
* zaobilaženjem sustava za upravljanje bazama podataka (npr. krađom datoteke ili diska)

mjere:

* prijenos šifriranih podataka (*data-in-transit*) i/ili
* pohrana šifriranih podataka (*data-at-rest*)

šifriranje se može koristiti kao zadnji sloj obrane radi zaštite osjetljivih i vrlo povjerljivih informacija - nije zamjena za ostale tehnike zaštite podataka, npr. za upravljanje pristupom

### Prijenos šifriranih podataka

* šifriranje/dešifriranje podataka-u-prijenosu događa se u krajnjim točkama komunikacije između klijenta i poslužitelja
  + podaci pohranjeni u bazi podataka i podaci koje koristi klijentska aplikacija nisu šifrirani
* implementacijske mogućnosti šifriranja podataka u prijenosu:
  + specifične mogućnosti određenog SUBP-a (npr. *Oracle Advanced Security* )
  + *Connection-based methods* (npr. korištenje Secure Sockets Layer [SSL])
  + *Secure tunnels* (npr. korištenje Secure Shell [SSH] tunela)
  + mogućnosti koje podržava operacijski sustav (npr. IPSec)
* u svim, osim u prvoj kategoriji, prijenos šifriranih podataka temelji se na industrijskim standardima i ne ovisi o proizvođaču baze podataka
* većina metoda šifrira cijeli komunikacijski tok

### Pohrana šifriranih podataka

šifriranje vrijednosti koje su pohranjene u bazi podataka

šifriranje/dešifriranje moguće je obaviti na razini:

* **aplikacije**
  + biblioteke za šifriranje/dešifriranje podataka (npr. Java Cryptographic Extensions - JCE)
  + bazi podataka se pristupa s već šifriranim podatkom - transparentno za bazu podataka
  + šifriranje/dešifriranje je možda potrebno obaviti na više mjesta
  + npr. pohranjena procedura koristi podatke šifrirane u Java kôdu aplikacije
  + ograničeno korištenje interaktivnog alata za rad s bazom podataka, čak i uz potrebne ovlasti
* **datotečnog sustava**
  + korištenje mogućnosti naprednog datotečnog sustava za pohranu podataka u šifriranom obliku
  + npr. Windows - Encrypted File System (EFS)
  + šifrirano je sve, a ne samo osjetljivi podaci - lošije performance
* **sustava za upravljanje bazama podataka**

šifriranje/dešifriranje na razini sustava za upravljanje bazama podataka:

* ugrađene rutine baza podataka (npr. T-SQL: DB\_ENCRYPT i DB\_DECRYPT funkcije)
* proširenja SUBP-a (dodatni paketi) (npr. Oracle - DBMS\_CRYPTO paket)

podaci su neupotrebljivi dok se ne dešifriraju

* SUBP ne može obaviti učinkovita uspoređivanja vrijednosti i temeljne operacije nad šifratima
* neizbježan pad performanci, ovisno o opsegu šifriranja i korištenim algoritmima
* ispitivanje Database Server Technologies Group: Oracle 9.2.0.1 - uzorak od 1,6 milijuna šifriranih brojeva socijalnog osiguranja
  + SELECT koji vraća sve zapise: uz korištenje DES algoritma - 200 puta sporiji
  + UPDATE zapisa: uz korištenje DES algoritma - četiri puta sporiji, uz triple DES - osam puta sporiji
* šifrirani podaci zauzimaju više prostora od originalnog teksta
* smjernice:
  + šifrirati selektivno - samo iznimno osjetljive informacije
  + ne šifrirati atribute koji se koriste kao ključevi ili indeksi

### Upravljanje ključevima

kompromitirani ključevi - mogućnost otkrivanja informacije

izgubljeni ključevi - gubitak informacija

* generiranje ključeva
  + npr. Oracle funkcija RANDOMBYTES paketa DBMS\_CRYPTO
* prijenos ključeva
  + prijenos šifriranog ključa od aplikacije do baze podataka
* pohrana ključeva
  + u bazi podataka, u operacijskom sustavu
  + alati koji nude cjelovita rješenja vezana uz upravljanje ključem
  + korisnici upravljaju vlastitim ključevima za šifriranje
  + korištenje transparentnog šifriranja baze podataka
* promjena ključa
  + obaviti dok se podacima ne pristupa
* sigurnosne kopije i obnova baze podataka
  + na koji način i gdje čuvati ključeve korištene u trenutku izrade sigurnosne kopije

šifriranje/dešifriranje podataka obavlja SUBP prilikom pohrane/dohvata podatka

* nije potrebno koristiti posebne funkcije
* transparentno za korisnike baze podataka
* nije potrebna izmjena aplikacija radi rukovanja šifriranim podacima
* poslovi upravljanja ključem su automatizirani
  + korisnik ili aplikacija ne mora upravljati ključem za šifriranje
* implementirano u nekim sustavima za upravljanje bazama podataka:
  + Oracle - *Transparent Data Encryption* (TDE)
  + SQL Server - *Extensible Key Management* (EKM)

## Praćenje rada korisnika

skup evidentiranih informacija, neovisno o kategoriji pristupa:

* **identifikator korisnika**
* **vrijeme obavljanja aktivnosti**
* mjesto s kojeg je upućen zahtjev (terminal, IP adresa klijenta)
* program korišten za ostvarivanje SQL-sjednice

prilikom praćenja promjene osjetljivih podataka, dodatno je potrebno evidentirati:

* korištenu SQL naredbu
* vrijednosti prije i poslije izmjene

nužnost selektivnog praćenja DML aktivnosti zbog mogućnosti stvaranja goleme količine

podataka - praćenje aktivnosti na podskupu tablica baze podataka

u slučaju promjena ovlasti i ostalih sigurnosnih atributa nužno implementirati obavještavanje o

promjenama u stvarnom vremenu

# Testiranje sigurnosti informacijskih sustava

## Važnost informacijske sigurnosti

• **Razina sigurnosti mora odgovarati ciljevima organizacije**

* Usklađenost s misijom, ciljevima i (poslovnom) strategijom
* Idealno se temelji na modeliranju prijetnji i procjeni rizika

• **Prijetnje** sigurnosti mogu biti:

* Vanjske – zlonamjerni napadači
* Unutarnje – zlonamjerni i dobronamjerni zaposlenici

• Apsolutnu sigurnost nije moguće postići

• Pitanja za organizaciju:

* Koji su trenutni sigurnosni rizici i na koji način ih se tretira?
* Primjenjuju li se i u kojoj mjeri najbolje sigurnosne prakse?
* Kakva je statistika sigurnosnih incidenata, kako se detektiraju i koji je status spremnosti na takve incidente?

• Na koji način se rizici realiziraju?

## Obrazac napada na sigurnost organizacije

Uspješan napad podrazumijeva **narušavanje nekog od temeljnih sigurnosnih atributa**, neovisno o motivaciji

* Nije nužan direktan interes napadača za specifičnu metu
* Ipak, upravo određeni izraziti interes može biti ključan (APT)

• Spektar vektora napada se svakodnevno širi napretkom tehnologije

• Zajednički nazivnik većine napada je **izvršavanje zlonamjernog programskog koda**

* Postiže se iskorištavanjem softverskih ranjivosti (CVE, CVSS)
* Izrazito važan je ljudski faktor (uvjerljivo najslabija karika)

• Primjer tipične struktura napada:

* spear phishing uz zloćudnu datoteku > udaljena kontrola računala > dobivanje pristupa kritičnim resursima > prikupljanje i/ili manipulacija podataka

• Kako se obraniti?

## Obrazac implementacije sigurnosti

Strategija obrane vojnog porijekla (eng. **defence in depth**), bazirana na višeslojnim sigurnosnim kontrolama

• **Sigurnosne kontrole** su mjere suzbijanja sigurnosnih rizika i moguće ih je kategorizirati po različitim kriterijima:

* Preventivne, detektivne, korektivne, kompenzacijske
* Fizičke, proceduralne, tehničke, pravne/regulatorne

• Sustav upravljanja informacijskom sigurnošću (**ISMS**)

* Faktori uspješne zaštite informacijskih sustava su brojni
* Sigurnosne kontrole (mjere) definiraju se okvirom internih akata: sigurnosnih politika, pravilnika i procedura
* Npr. "Pravilnik o mrežnoj sigurnosti" može definirati niz stavki koje se odražavaju na implementaciju mreže (dizajn, segmentaciju, konfiguraciju mrežnih uređaja itd.)

• Primjenjuju li se propisane sigurnosne kontrole i **jesu li efikasne**?

**Sigurnost je nužno testirati** – testiranjem sigurnosti verificiraju se uspostavljene sigurnosne kontrole, uočavaju se sigurnosni nedostaci (tehnički, procesni itd.) i rizici te omogućuju poboljšanja sigurnosnih sustava i mjera

• Koncept operativnih sigurnosnih procedura i kontrola

* Predstavljaju periodičko testiranje i evaluaciju efikasnosti uspostavljenih sigurnosnih politika, primijenjenih sigurnosnih praksi i mjera, uz frekvenciju ovisnu o izloženosti nekoj prijetnji

• Uključuju širok spektar mogućih aktivnosti: revizija korisničkih prava pristupa, sigurnosne provjere zaposlenika, provjera konfiguracije vatrozida i dr.

• Iz tehničkog aspekta, najistaknutije su:

* Provjera ranjivosti (upravljanje ranjivostima u širem smislu)
* Penetracijsko testiranje
* Testiranje odgovora na sigurnosne incidente
* Testiranje sigurnosti u životnom ciklusu razvoja softvera

## Provjera ranjivosti

**Upravljanje ranjivostima** (eng. vulnerability management) je ciklički proces neinvazivnog otkrivanja, klasificiranja i otklanjanja ranjivosti

• Podrazumijeva **tehničke ranjivosti** poput nesigurne konfiguracije, poznatih ranjivosti u softveru općenito, kao i ranjivosti web aplikacija

• Podrazumijeva ranjivosti otkrivene **automatiziranim alatima za provjeru ranjivosti** (eng. vulnerability assessment)

* Nessus, OpenVAS, QualysGuard, Nexpose itd.
* Komercijalna rješenja su znatno naprednija

• Osnovna kategorizacija provjera ranjivosti:

* Provjera mrežnih ranjivosti – uglavnom temeljena na testiranju poznatih ranjivosti u poslužiteljskom softveru (npr. Apache)
* Provjera ranjivosti (web) aplikacija – uglavnom temeljena na testiranju prisustva neke od OWASP Top 10 ranjivosti

• Faza otkrivanja ranjivosti:

* Provođenjem periodičkih automatiziranih provjera (moguća različita razina privilegija pod kojima se provjere odrađuju)
* Automatizacija je nužna zbog efikasnosti, pogotovo u većim sustavima.

• Faza klasificiranja ranjivosti:

* Dijelom odrađuje alat za testiranje, no potrebna je ljudska analiza radi otklanjanja lažno pozitivnih rezultata, stavljanja ranjivosti u kontekst i prioritizacije otklanjanja

• Faza otklanjanja ranjivosti:

* Pokretanje implementacije sigurnosne zakrpe
* Ovisno o kontekstu, implementacija potrebnih promjena može biti popraćena složenim procedurama, što produžuje vrijeme od otkrivanja ranjivosti do njenog otklanjanja
* Verifikacija uspješne implementacije zakrpa

Kada sve provoditi provjere ranjivosti? Nekoliko varijanti:

* Periodički uz prikladnu frekvenciju (mjesečno, tjedno, dnevno)
* Prije uvođenja novih sustava ili aplikacija
* Kod većih promjena sustava ili aplikacija

• **Benefiti** kvalitetnog programa upravljanja ranjivostima:

* Pravovremeno otkrivanje i otklanjanje ranjivosti u sustavima
* Smanjenje izloženosti iskorištavanju poznatih ranjivosti
* Evaluacija uspješnosti procesa upravljanja zakrpama (eng. Patch management)

• Alati za provjeru ranjivosti su **tehnički ograničeni**:

* Otkrivaju samo poznate ranjivosti (fuzzeri ne ulaze u ovu kategoriju alata)
* Mogu uzrokovati neželjene poteškoće u radu sustava koji se testira, bez obzira što su načelno neinvazivni

## Penetracijsko testiranje

Metoda evaluacije sigurnosti informacijskih sustava, mreže, odnosno općenito organizacije, **simuliranjem zlonamjernog napada**

* Prvenstveno se odnosi na proboj digitalne informacijske infrastrukture, no može obuhvaćati i ostale segmente sigurnosti organizacije (npr. fizička sigurnost)

• Poznato i pod nazivom "etičko hakiranje", a razlikuje se od obične provjere ranjivosti (eng. vulnerability assessment, scanning) po karakteristikama i svrsi

* Podrazumijeva detaljnu višednevnu analizu i aktivno iskorištavanje otkrivenih ranjivosti

• Najbolja praksa je da PT provode timovi vanjskih konzultanata

• Cilj PT-a, pored same verifikacija sigurnosnih kontrola, je **predstavljanje stvarnih rizika** za poslovanje u slučaju zlonamjernog napada, što predstavlja dodanu vrijednost organizaciji

• Cilj PT- a **nisu** trivijalne detekcije (koje su možda u opsegu VA)

Prije provođenja, važno je potpisivanje odgovarajućeg ugovora (uključujući i ugovor o tajnosti), kao i dogovaranje tehničkih uvjeta testiranja, prvenstveno opseg, vremenska i druga ograničenja

• **Metodologija PT-a** sastoji se od tri temeljna koraka, koja se načelno odvijaju slijedno, no moguće su i povratne veze

* Planiranje – priprema je važan dio PT-a, a uključuje potrebne dogovore s klijentom (dozvole, opseg, dubina, trajanje, termini u kojima je testiranje zabranjeno...)
* Izvođenje – poznato i kao faza napada, sastoji se od pet podfaza: istraživanje, skeniranje, dobivanje pristupa, zadržavanje pristupa, brisanje tragova
* Izvještavanje – dokumentacija metodologije i procesa izvođenja testa te predstavljanje identificiranih rizika

• U literaturi postoje i nešto drugačije raščlambe PT-a, no u svima su zadržane ključne karakteristike

U kontekstu testiranja sigurnosti, posebno značajna je **faza provođenja napada**:

* Istraživanje – prikupljanje čim više informacija o sustavu koji se testira (aktivno i pasivno istraživanje, footprinting)
* Skeniranje – detaljna enumeracija servisa vezanih uz otvorene portove (fingerprinting, identifikacija ranjivosti...)
* Dobivanje pristupa – iskorištavanje pronađenih ranjivosti uz ostvarivanje neovlaštenog pristupa
* Zadržavanje pristupa – ostvarivanje stabilnog i pouzdanog pristupa kompromitiranom sustavu
* Brisanje tragova – prikrivanje neovlaštenog pristupa, kako bi se otežala ili u praktičnom smislu onemogućila forenzička istraga

• Izvođenje napada ovisi i o osobnom iskustvu te razvoju situacije

• Priprema i izvještavanje nisu manje važni – naprotiv, bez kvalitetnog izvještaja, odrađeni posao gubi na vrijednosti

Glavni **kriteriji kategorizacije PT-a**:

* Dostupne informacije: black-box, white-box, gray-box
* Početna točka testa: vanjski, unutrašnji

• Za testiranje se koriste brojni alati, metode i resursi, npr. nmap, Nessus, Metasploit, javno dostupni exploiti, fuzzeri, reverzni inženjering

* U tijeku testiranja se mogu otkriti i zero-day ranjivosti

• Napadači su različiti i pogrešno je stvarati lažni osjećaj sigurnosti – provedeno testiranje treba evaluirati u odnosu na protivnika.

* Npr. NSA je protivnik od kojeg je u praksi nemoguće obraniti se

• PT se provodi u različitim opsezima: na razini pojedine aplikacije, sigurnosnih sustava, ljudi i dr.

• Preporučljivo provesti vanjski i unutrašnji PT generalne infrastrukture barem jednom godišnje te dodatno i kritičnih aplikacija (inicijalno i kod značajnijih promjena)

## Testiranje spremnosti na incidente

**Sigurnosni incidenti** su događaji koji predstavljaju neposrednu prijetnju kršenju sigurnosnih politika, definiranih sigurnosnih praksi i/ili prihvatljivog korištenja sustava.

* Predstavljaju neki oblik narušavanja ili pokušaja narušavanja sigurnosnih atributa

• **Upravljanje incidentima** je proces praćenja sigurnosno relevantnih događaja, detekcija, analiza i prioritizacija incidenata te odgovor na detektirane incidente.

* Važan faktor u održavanju sigurnosti organizacije
* Uloga SIEM (eng. Security Information and Event Management) sustava je važna za vidljivost sigurnosnih događaja

• Internim aktima definira se kompletni proces upravljanja incidentima, uključujući uloge i odgovornosti

* Incident response team – mora biti koordiniran

• **Spremnost na sigurnosne incidente je potrebno testirati**

* Analogno vojnim vježbama

Testiranje spremnosti na sigurnosne incidente može biti u različitom opsegu i scenarijima, primjerice:

* Specifični tip incidenta (sigurnosni incidenti mogu biti različitih tipova i razine (težine, utjecaja) – klasifikaciju definira organizacija prema svojim potrebama)
* Detekcije malicioznog ponašanja sustava
* Napad većih razmjera (mogući su i koncepti tzv. Red team vs. Blue team vježbi, što ima dodirne točke s PT)
* Fizička sigurnost

• Cilj je testirati plan odgovora na incidente, **uočiti eventualne nedostatke u planu i procedurama** (eng. lessons learned) te implementirati poboljšanja

• Testiranje odgovora na sigurnosne incidente se preporuča provoditi minimalno jednom godišnje, a po mogućnosti naravno i češće

## Testiranje sigurnosti u razvoju softvera

**Sigurnosni propusti u aplikacijama** omogućuju izvršavanje zlonamjernog koda i time su uzrok brojnih sigurnosnih incidenata

• Neusvajanje sigurnog razvoja najčešće uzrokovano: financijskim nedostacima, pritiscima brzog plasiranja na tržište (eng. Time-tomarket), nedostacima svijesti o informacijskoj sigurnosti

• Važno je uzeti u obzir **sigurnost od početka razvoja**, jer naknadno ugrađivanje sigurnosnih mehanizama stvara znatno veće troškove

* Sigurnost po dizajnu, u svim fazama razvoja (SDL, SSDLC)

• Pravila za sigurni razvoj softvera definiraju se relevantnim internim aktom, a trebaju uključivati primjenjive dobre prakse:

* Validacija ulaza, izlaza, kontrola pristupa, rukovanje iznimkama...

• **Testiranje je važan dio (sigurnog) razvoja softvera** jer omogućuje pronalaženje i otklanjanje sigurnosnih propusta prije nego softver uđe u uporabu

Testiranje je **iterativno** u životnom ciklusu, a sigurnost zahtijeva posebnu pozornost

* Teško je napraviti kvalitetan softver u smislu funkcionalnosti, a istovremeno osiguravanje sigurnosti je puno teže
* Obavezno nakon većih izmjena (npr. nova verzija aplikacije)

• Značajniji **oblici testiranja u ciklusu razvoja**:

* Revizija programskog koda – (eng. code review) provjera ispravnosti koda, također i u smislu sigurnosti
* Statička analiza koda – automatiziranom analizom koda mogu se uočiti sigurnosni nedostaci
* Nasumično testiranje – generiranjem nasumičnog ulaza mogu se dobiti neočekivani rezultati i pronaći ranjivosti (npr. Whitebox fuzzing)
* Provjera ranjivosti – ranije spomenuti alati za VA mogu se jednostavno integrirati u životni ciklus
* Penetracijsko testiranje – prikladno za visokorizične aplikacije

## Testiranje u sigurnosnim revizijama

**Sigurnosni standardi i regulativa** na različitim razinama objedinjuju određeni skup (minimalnih) sigurnosnih kontrola i operativnih sigurnosnih procedura

* PCI DSS, FIPS, PA DSS i drugi. Sukladnost se tipično iskazuje certifikatima ograničenog trajanja.
* Za organizacije u specifičnim djelatnostima, sukladnost s nekim od tih standarda je obvezujuća, uz odgovornost nadležnom regulatoru

• Regulatori provode nadzor usklađenosti sa standardima putem direktnih (eksternih) sigurnosnih revizija

• Između ostalog, **tijekom sigurnosne revizije provodi se niz testiranja** različite vrste, uobičajeno s ciljem provjere sukladnosti sa standardom (detalji ovise o vrsti revizije)

• Rezultat revizije u užem smislu je izvještaj s nalazima, odnosno uočenim nesukladnostima i/ili rizicima

•Važnu ulogu u organizacijama ima i interna revizija

## Praktični problemi testiranja sigurnosti

**Praktične okolnosti** mogu biti u raskoraku s akademskim aspektom testiranja – primjeri u nastavku

• Problemi upravljanja ranjivostima

* Automatizirani alati često ne ulijevaju povjerenje u odnosu na manualne provjere (pogotovo za aplikacijsko testiranje)
* Moguće narušavanje rada sustava uslijed testiranja
* Lažno pozitivni nalazi i analiza
* Implementacija zakrpa – promjena sustava, testiranje, resursi
* Naslijeđeni (eng. legacy) sustavi, testni i development sustavi

• Problemi penetracijskog testiranja

* Skupo i organizacije često provode zbog regulatornih zahtjeva
* Vremenski ograničeno, većinom ne uključuje socijalni inženjering i napade uskraćivanjem usluge (DoS) -> ograničeni rezultati
* Raskorak sa životnim ciklusom aplikacija
* –Klizanje opsega, moguće narušavanje rada sustava

Problemi testiranja spremnosti na sigurnosne incidente

* Za kvalitetno planiranje i izvedbu odgovora na incidente potrebni su značajni resursi
* SIEM sustavi nisu idealni – sigurnosno relevantni događaji stvaraju mnogo buke i šuma
* Podrazumijeva 24/7 dostupnost odgovornih osoba

• Problemi testiranja sigurnosti u životnom ciklusu razvoja softvera

* Implementacija sigurnosti usporava razvoj
* Razvijatelji aplikacija su rijetko stručnjaci za sigurnost, a edukacije su zahtjevne, novčano i vremenski
* Funkcionalnost softvera može biti otežana povećanjem sigurnosti (eng. usable security)
* Reviziju koda je zahtjevno raditi, pogotovo na velikim sustavima
* Alati za statičku analizu koda nisu savršeni

Problemi testiranja u sigurnosnim revizijama

* Usklađenost sa standardom nije ekvivalent sigurnosti
* Provjera usklađenosti sa standardom je diskretni događaj
* Iako u pravilu predstavlja minimum potrebne sigurnosti, već i tu razinu može biti zahtjevno implementirati, uslijed tehničkih, organizacijskih, kulturnih i ostalih implikacija
* Revizori ponekad nisu eksperti za sigurnost
* Regulativa može biti u kontradikciji s procjenom rizika

• Određene vrste testiranja po definiciji mogu biti vrlo delikatne te zahtijevaju pažljivo planiranje

* Testiranje kontinuiteta poslovanja i oporavka od katastrofe

• Konstantno prisutna opasnost od nepredviđenih okolnosti i pogrešaka