SIGURNOST RAČUNARSKIH MREŽA (SRM)

Tema 1:

Pretnje, napadi, sigurnost i metode zaštite

URLs:

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

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

  www.conwex.info/draganp/SRM_seminarski_radovi.html

Pretnje, napadi, sigurnost i metode zaštite

- Sadržaj predavanja:
  - 1.1. Napadi i pretnje
  - 1.2. Šta je sigurnost?
  - 1.3. Klasifikacija informacija
  - 1.4. Metode zaštite

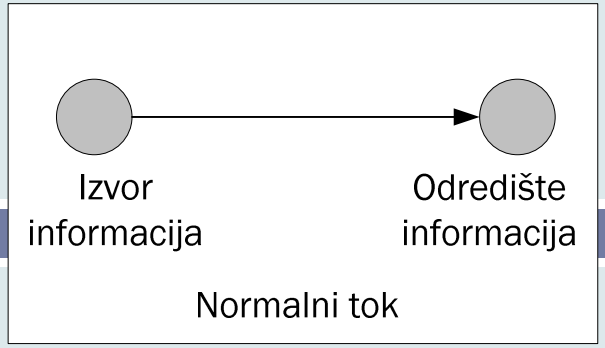
- **Apsolutna sigurnost NE postoji!**

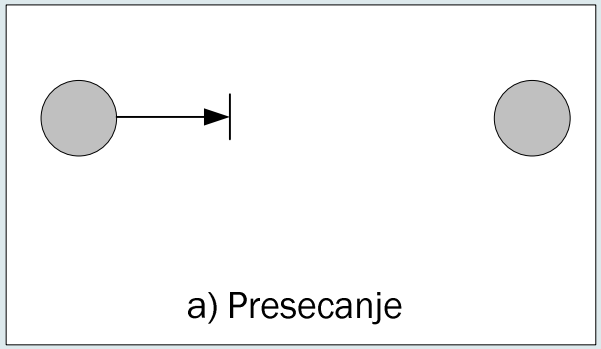
Napadi i pretnje

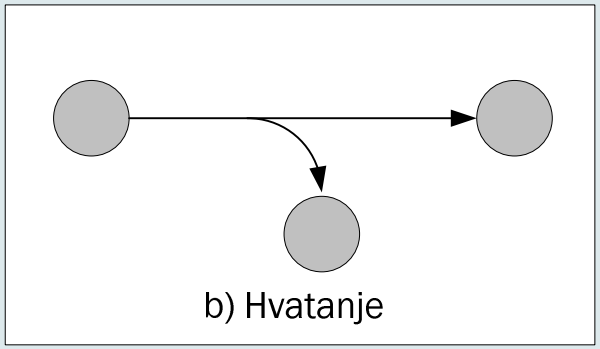
- **Napad** na sigurnost (engl. *security attack*) – bilo koja akcija koja ugrožava sigurnost informacija.
- **Sigurnosni mehanizam** (engl. *security mechanism*) – mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada.
- **Sigurnosna usluga** (engl. *security service*) – usluga koja povećava sigurnost sistema za obradu i prenos podataka. Sigurnosna usluga podrazumeva upotrebu jednog ili više sigurnosnih mehanizama.

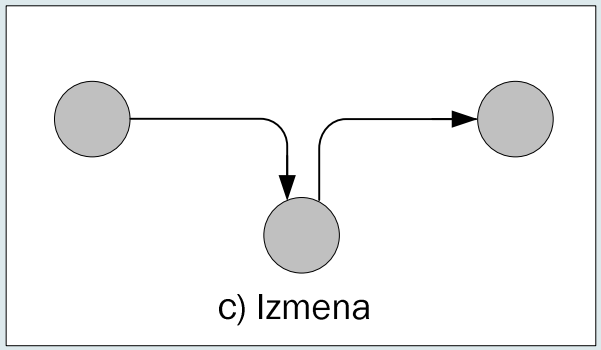
Kategorije napada

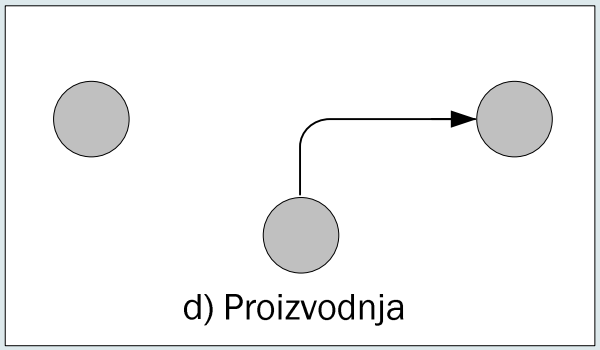
- U osnovi, napadi su akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža. Postoje različite vrste napada, ali se oni generalno mogu klasifikovati u četiri osnovne kategorije:
  - **a) Presecanje, prekidanje** (engl. i*nterruption*)
  - **b) Presretanje** (engl. i*nterception*)
  - **c) Izmena** (engl. *modification*)
  - **d) Proizvodnja, fabrikovanje** (engl. *fabrication*)







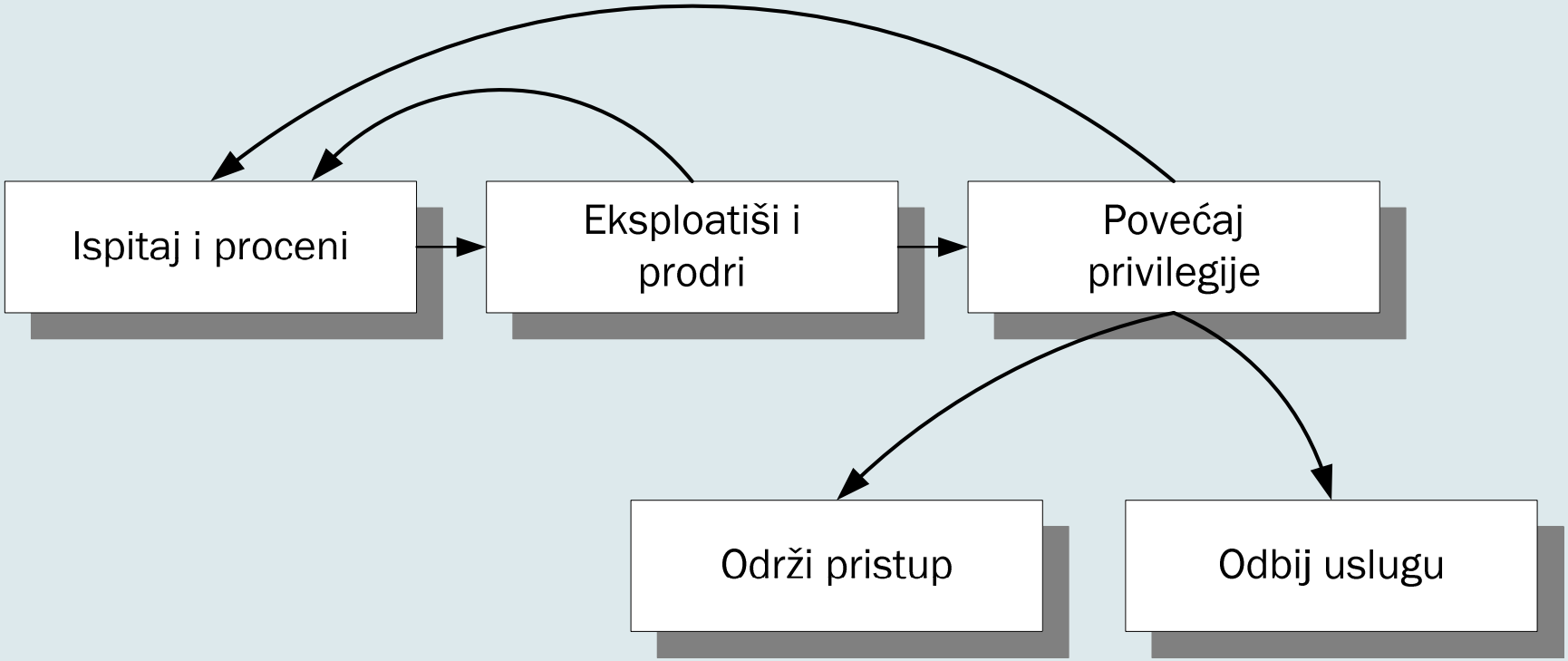




Anatomija napada

1. **Ispitaj i proceni** (engl. *survey and assess*)
2. **Eksploatiši i prodri** (engl. *exploit and penetrate*)
3. **Povećaj privilegije** (engl. *escalate privileges*)
4. **Održi pristup** (engl. *maintain access*)
5. **Odbij uslugu** (engl. *deny service*)

Anatomija napada - šema



Pretnje i jednačina rizika

- **Rizik** je, u kontekstu sigurnosti računarskih sistema i mreža, mera opasnosti, tj. mogućnost da nastane oštećenje ili gubitak neke informacije, hardvera, intelektualne svojine, usluge, prestiža ili ugleda.

  Rizik = Pretnja × Ranjivost × Vrednost imovine

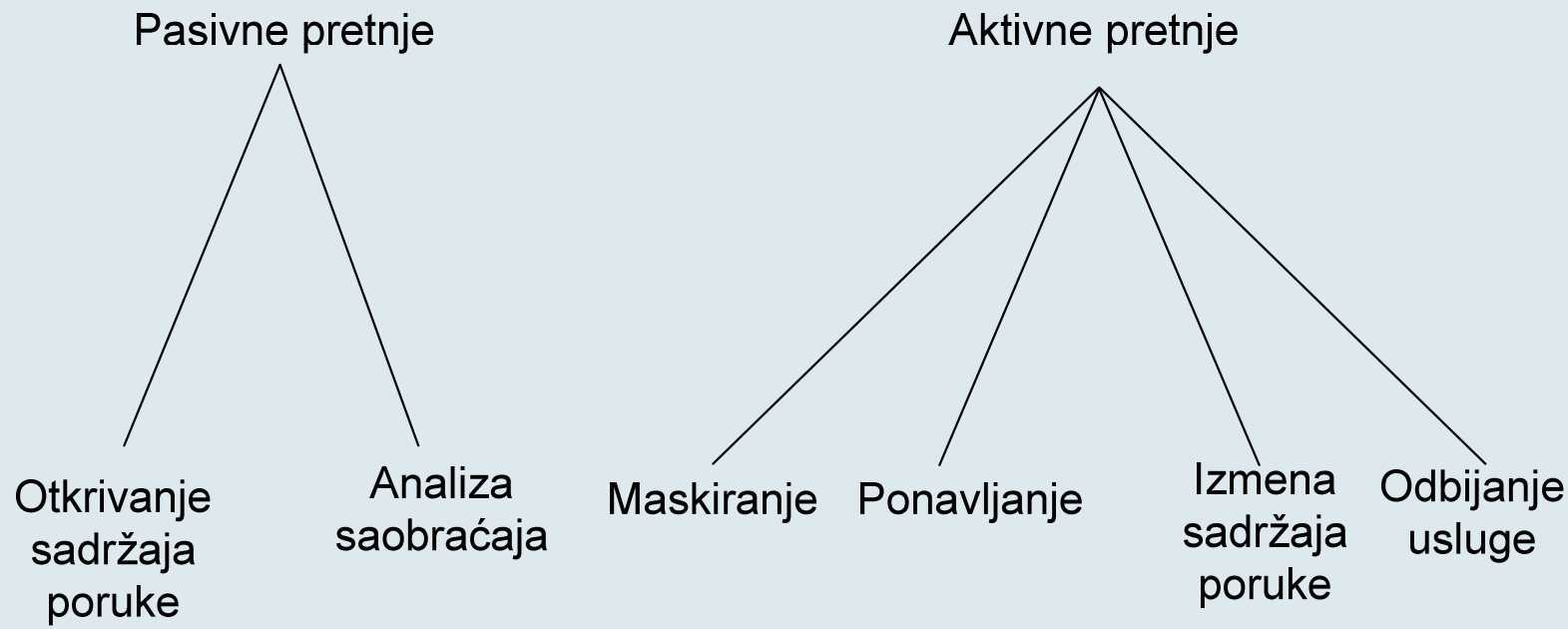
- **Pretnja** (engl. *threat*) je protivnik, situacija ili splet okolnosti sa mogućnošću i/ili namerama da eksploatiše ranjivost.

Pasivne i aktivne pretnje

- **Pasivne pretnje** su one koje ne utiču neposredno na ponašanje sistema i njihovo funkcionisanje. U pasivne pretnje spadaju otkrivanje sadržaja poruka (na primer, prisluškivanje) i analiza saobraćaja.

- **Aktivne pretnje** mogu uticati na ponašanje i funkcionisanje sistema ili na sadržaj podataka. U aktivne pretnje spadaju: maskiranje, tj. pretvaranje, lažiranje (engl. *masquerade*), reprodukcija, tj. ponavljanje mrežnog saobraćaja (engl. *replay*), izmena sadržaja poruke i odbijanje usluge.

Pasivne i aktivne pretnje...



Ranjivost

- **Ranjivost** (engl. *vulnerability*) predstavlja slabost u nekoj vrednosti, resursu ili imovini koja može biti iskorišćena, tj. eksploatisana. Ranjivosti su posledica lošeg projektovanja, implementacije ili "zagađenja".

- **Vrednost imovine** je mera vremena i resursa potrebnih da se neka imovina zameni ili vrati u svoje prethodno stanje. Zato se kao ekvivalentan termin može koristiti i "cena zamene".

Modeliranje pretnji

- Identifikovanje vrednosti
- Izrada pregleda arhitekture
- Dekompozicija aplikacije
- Identifikovanje pretnji
- Dokumentovanje pretnji
- Rangiranje tj. procena pretnji

Najčešće primenjivani napadi i pretnje – neki primeri

- Odbijanje usluga (engl. *Denial of Service*, *DoS*)
- Lažiranje IP adresa (engl. *spoofing*)
- "Njuškanje" (engl. *sniffing*)

- Programske pretnje
  - Trojanski konj (engl. *trojan horse*)
  - Klopka (engl. *trap door*)
  - Prekoračenje, tj. prelivanje bafera (engl. *buffer overrun*, *buffer overflow*)

- Sistemske pretnje
  - Crvi
  - Virusi

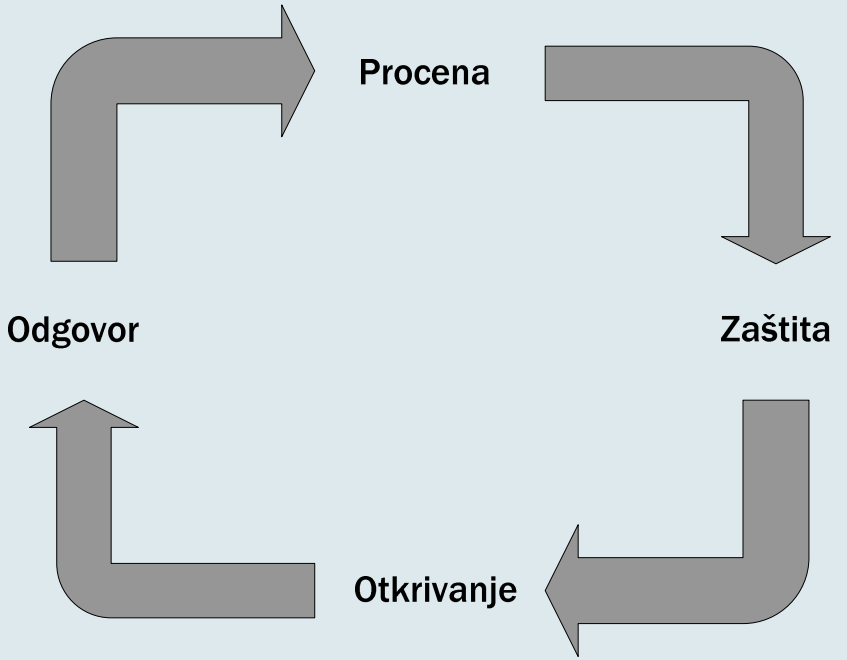
Šta je sigurnost?

- **Sigurnost je proces** održavanja prihvatljivog nivoa rizika. Znači, sigurnost je proces, a ne završno stanje, tj. nije konačni proizvod.

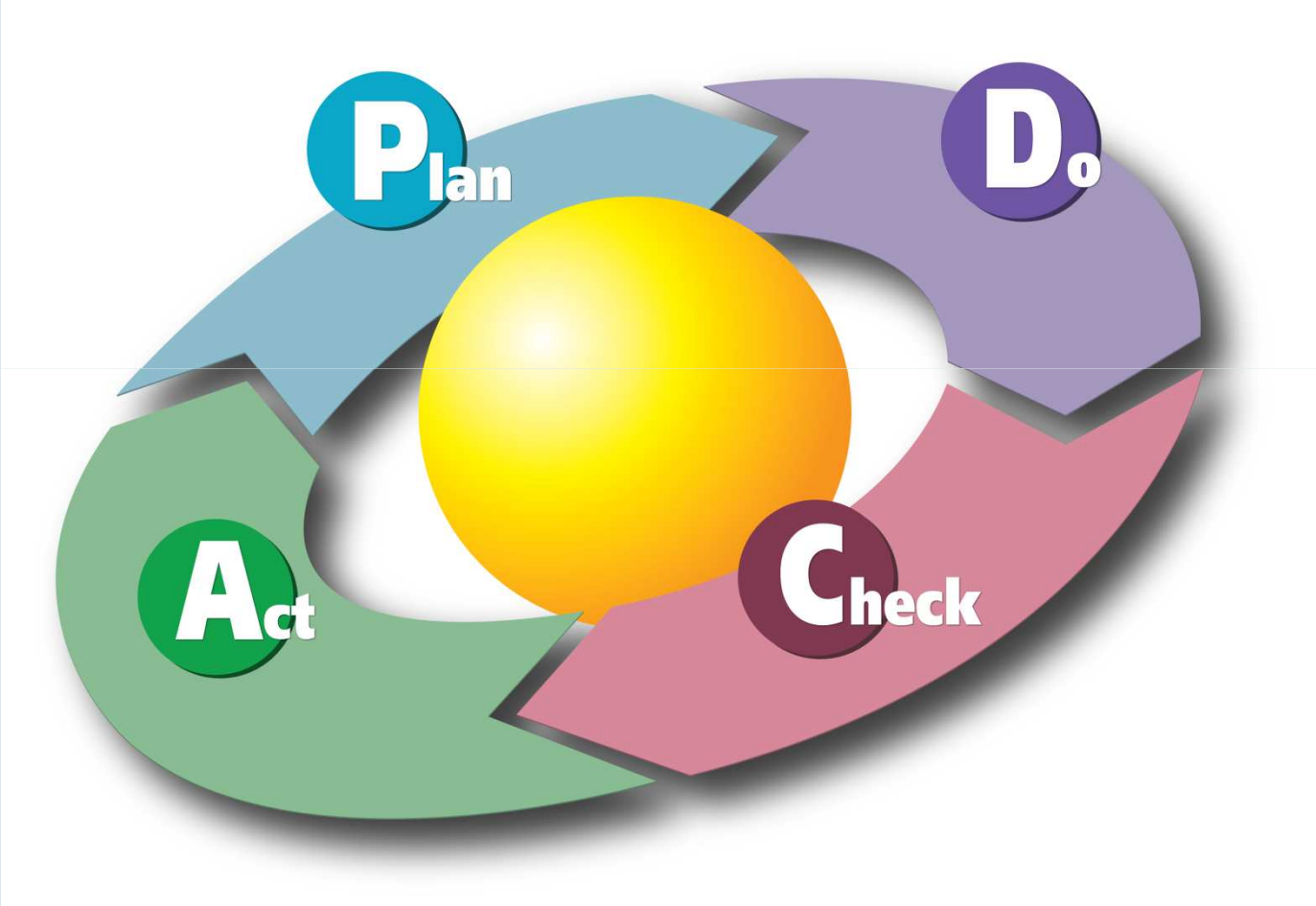
- Kada se govori o sigurnosti i zaštiti informacionih sistema i mreža, nekoliko principa danas važe kao osnovni **postulati**:
  - Sigurnost je **proces**. Sigurnost nije proizvod, usluga ili procedura, već skup koji ih sadrži - uz još mnogo elemenata i mera koje se stalno sprovode.
  - **Ne postoji apsolutna sigurnost**.
  - Uz različite metode zaštite, treba imati u vidu i **ljudski faktor**, sa svim slabostima.

Sigurnost kao proces

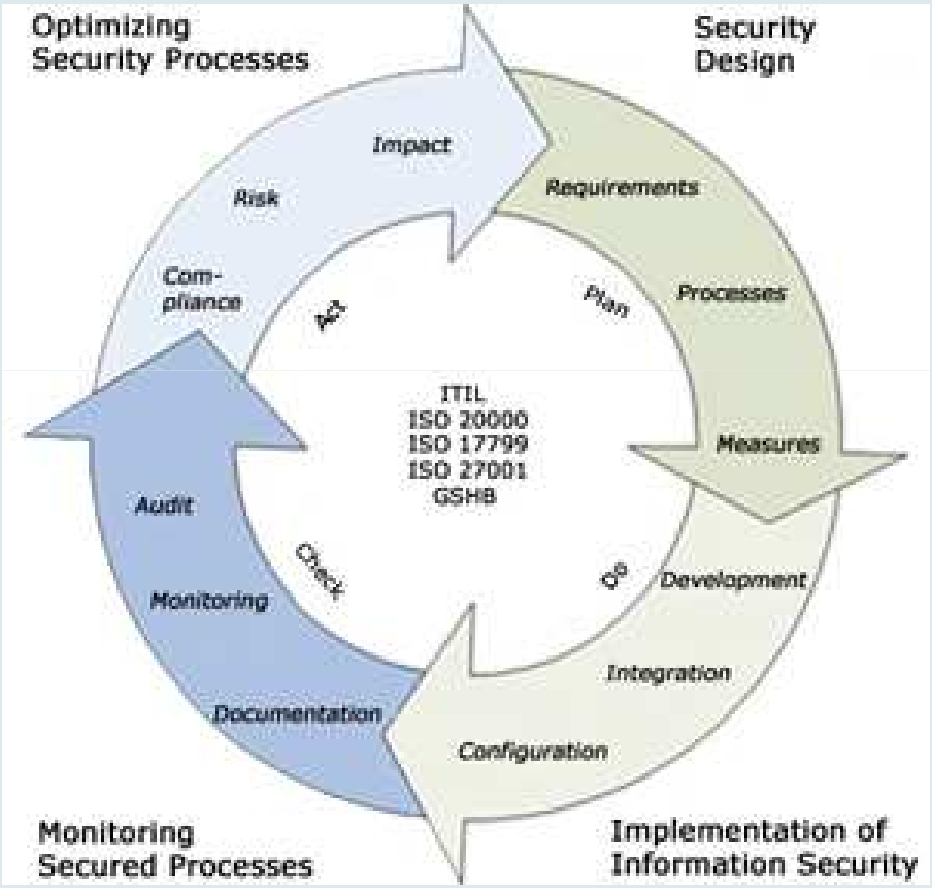
- Procena (engl. *assessment*)
- Zaštita (engl. *protection*)
- Otkrivanje (engl. *detection*)
- Odgovor (engl. *response*)



PDCA Cycle (1)



PDCA Cycle (2)

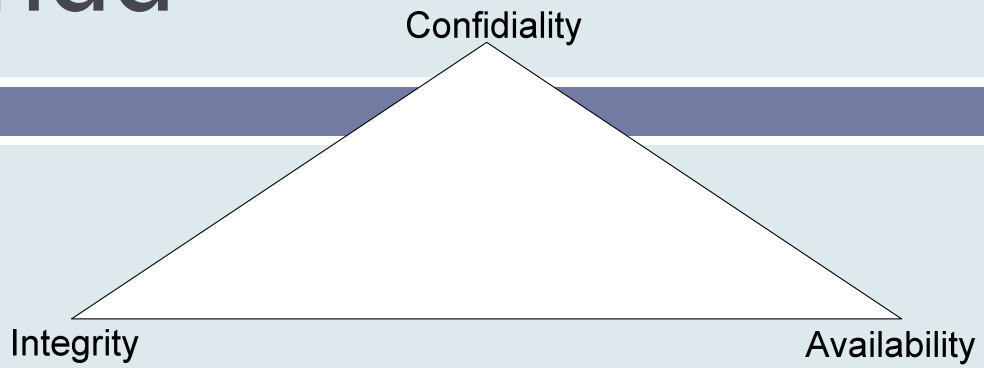


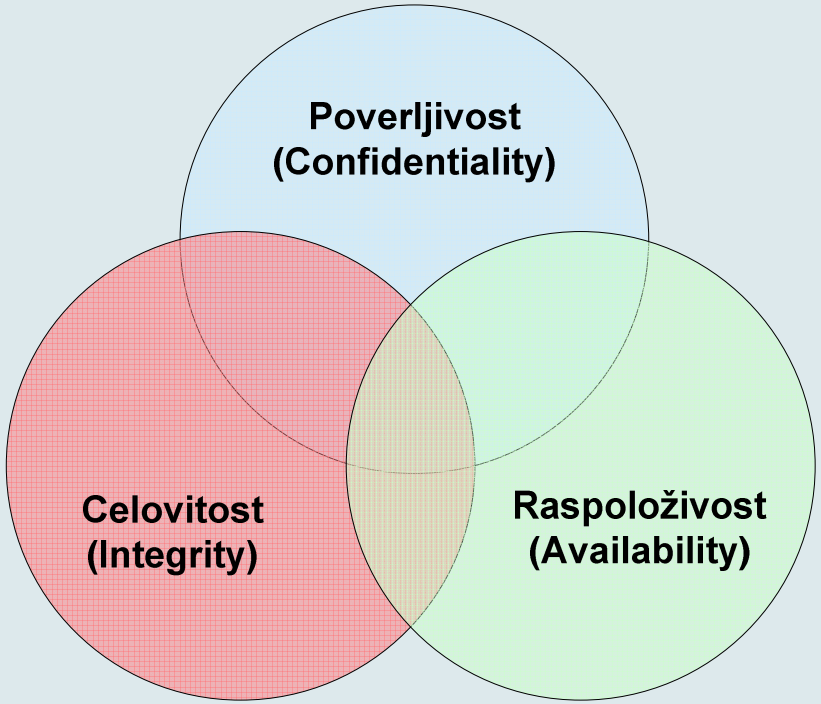
Sigurnosni ciljevi

- Poverljivost (engl. ***C**onfidentiality*)
- Celovitost, integritet (engl. ***I**ntegrity*)
- Raspoloživost (engl. ***A**vailability*)

- CIA - ***C**onfidentiality*, ***I**ntegrity*, ***A**vailability*
- DAD - ***D**isclosure* (otkrivanje, obelodanjenje), ***A**lteration* (izmena, preinačenje), ***D**estruction* (uništenje, razaranje)

CIA triad





Sigurnosne usluge

- **Sigurnosna usluga** (servis) jeste usluga koja povećava sigurnost sistema za obradu i prenos podataka. Sigurnosna usluga podrazumeva upotrebu jednog ili više sigurnosnih mehanizama, tj. mehanizama koji treba da detektuju ili preduprede napad na sigurnost, ili da oporave sistem od napada.

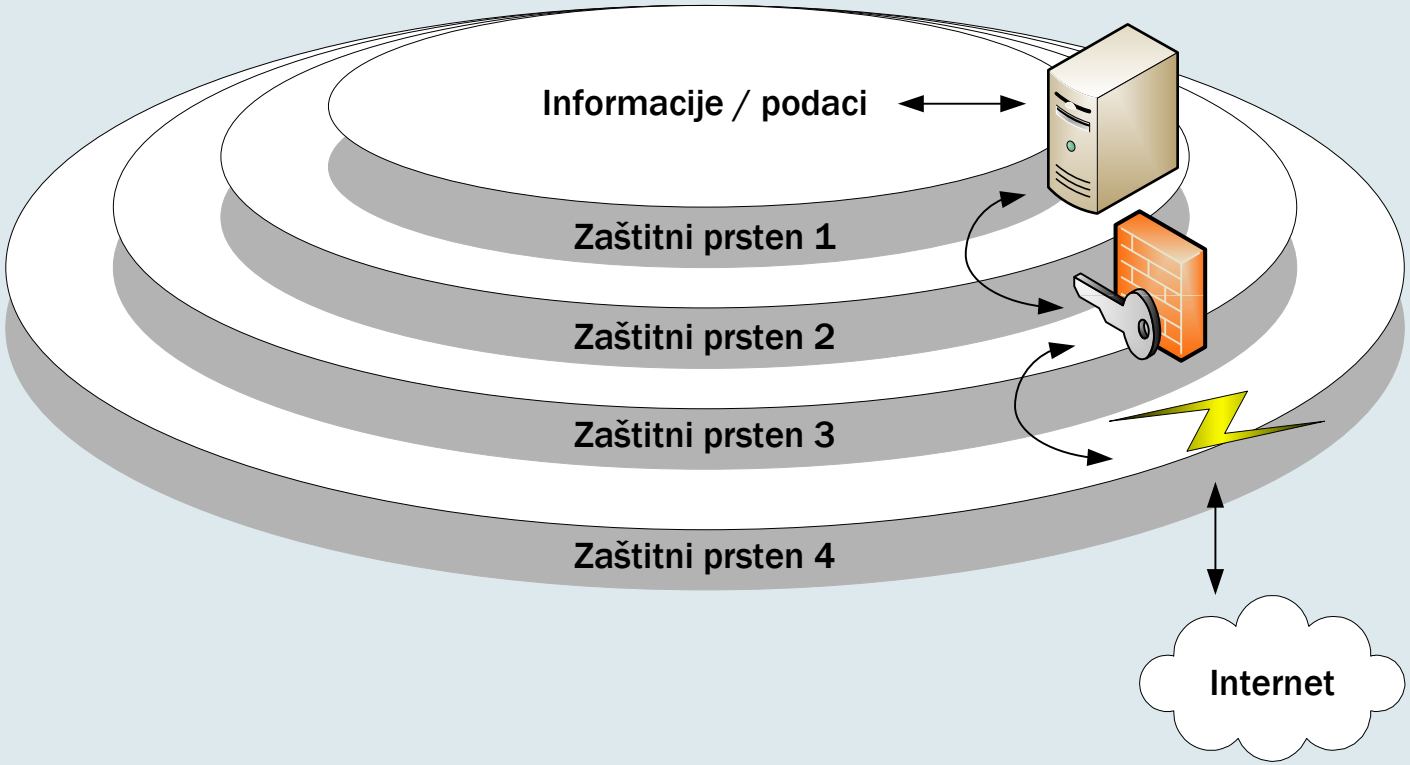
- **Sigurnosni mehanizmi** su rešenja, tehnologije, pravila i procedure koje možemo implementirati na sistemu.

Sigurnosne usluge…

- U sigurnosne usluge spadaju (na primer) mehanizmi koji treba da obezbede:
  - Poverljivost, privatnost (engl. *confidentiality*, *privacy*)
  - Autentifikaciju (engl. *authentication*)
  - Integritet (engl. *integrity*)
  - Neporicanje, priznavanje (engl. *non-repudiation*)
  - Kontrolu pristupa (engl. *access control*)
  - Raspoloživost, upotrebljivost (engl. *availability*)

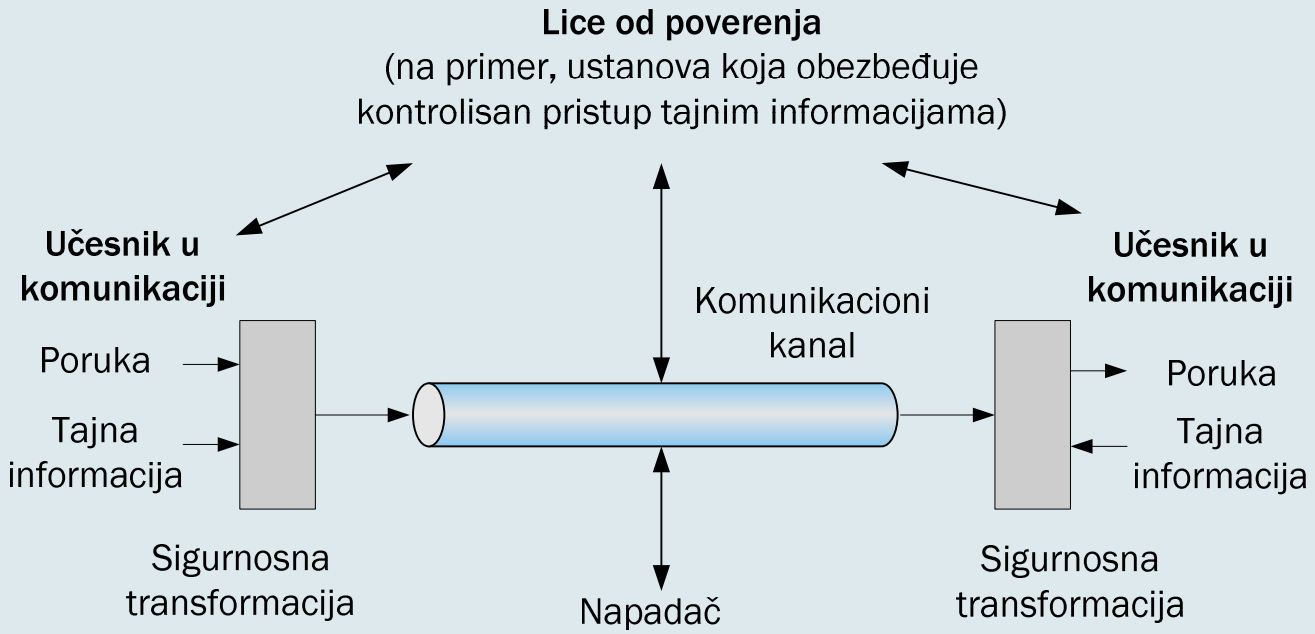
Strategije ostvarivanja sigurnosti

- Slojevita zaštita



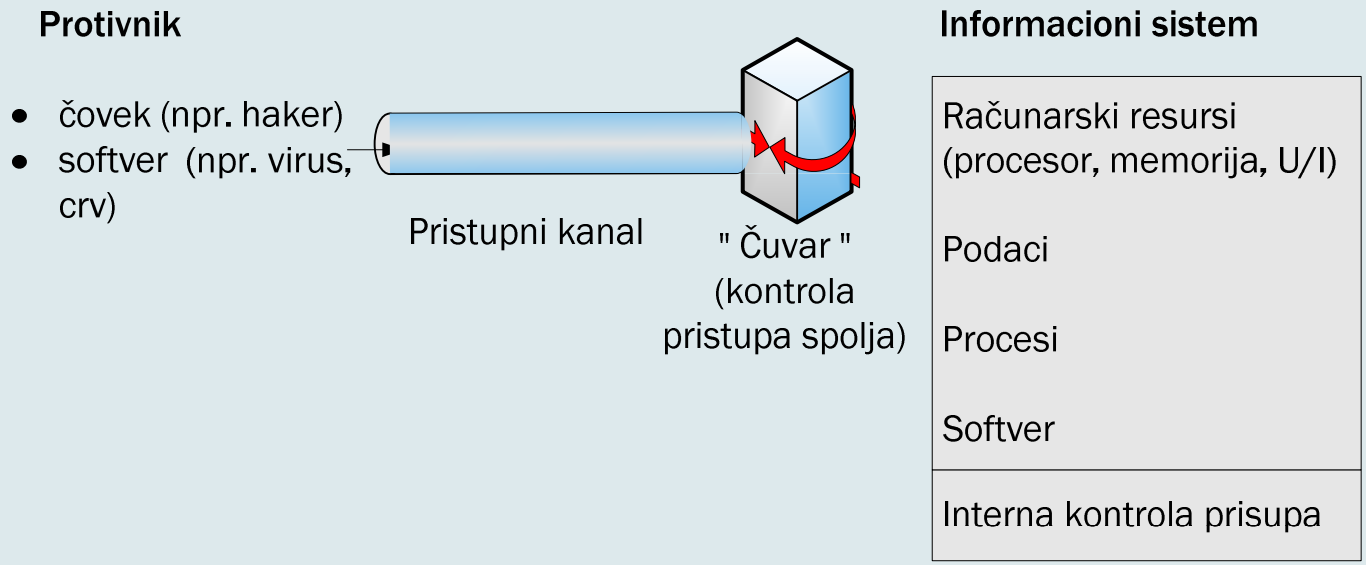
Sigurnosni modeli

- Model sa nesigurnim komunikacionim kanalom



Sigurnosni modeli...

- Model sigurnog pristupa mrežnim resursima



Klasifikovanje informacija

- Jedan od najbitnijih koncepata politike zaštite informacija jeste koncept vlasništva. Ovim konceptom se obezbeđuje da svi računarski resursi - glavni informacioni entiteti (informacioni podsistemi, baze podataka, uređaji, datoteke, prenosni putevi) - moraju imati vlasnika, tj. nekoga ko je zadužen za njih.

- Vlasnik treba da:
  - klasifikuje informacije u jednu od raspoloživih klasa,
  - deklariše ko može da pristupi podacima,
  - bude odgovoran za podatke i za njihovu zaštitu.

Klasifikovanje tajnosti informacija

- Prema jednoj od dominantnih klasifikacija, karakterističnoj za zemlje koje svoje metode zaštite definišu na bazi predinformacionog doba, informacije se dele u četiri osnovne klase:

1. Javne
2. Interne
3. Poverljive
4. Tajne

Drugi načini klasifikacije

- Nivoi klasifikacije sigurnosti državnih informacija:

1. Neklasifikovane (engl. *unclassified*)
2. Osetljive ali neklasifikovane (engl. *sensitive but unclassified*, *SBU*)
3. Poverljive (engl. *confidential*)
4. Tajne (engl. *secret*)
5. Vrhunske tajne (engl. *top secret*)

Klasifikaciona - privatni i komercijalni sektor

- Osnovna varijanta:
  1. Javne informacije (engl. *public*)
  2. Osetljive informacije (engl. *sensitive*)
  3. Privatne informacije (engl. *private*)
  4. Poverljive informacije (engl. *confidential*)

- Jednostavnija varijanta
  1. Javna upotreba
  2. Samo interna upotreba
  3. Informacije poverljive za preduzeće

Predlog zakona o klasifikaciji tajnih podataka

- Zakon definiše klasifikaciju informacije kao:
  - „postupak, kojim se informacija označava tajnom i određuje stepen tajnosti, u skladu sa stepenom štete koja može da nastupi neovlašćenim otkrivanjem”
- Prema predlogu zakona, tajne mogu biti samo informacije koje se odnose na:
  - nacionalnu bezbednost
  - spoljne poslove
  - obaveštajne i kontraobaveštajne aktivnosti države

(uključujući sisteme, uređaje, projekte, planove, naučna istraživanja, tehnologije i ekonomske i finansijske poslove od značaja za njih)

Vrste tajni i stepeni tajnosti

- Vrste tajni
  - Državne
  - Službene
  - Vojne

- Stepeni tajnosti:
  - Strogo poverljivo
  - Poverljivo
  - Interno

*Ovo je podela iz vremena bivše SFRJ

Klasifikacija tajnosti u EU

- Zemlje članice EU ne poznaju posebne vrste tajni, već samo četiri stepena tajnosti podataka:
  - Državna tajna
  - Strogo poverljiva tajna
  - Poverljiva tajna
  - Interna tajna

Slobodan pristup informacijama

- Slobodan pristup informacijama podrazumeva da svaki građanin ima pravo da zna da li vlast poseduje neku informaciju, u kom dokumentu, da ima uvid u njega, kao i da dobije njegovu kopiju ukoliko to želi, ukoliko nije pod ovim statusom - predviđa Zakon o slobodnom pristupu informacijama koji je usvojen u Srbiji krajem 2004. godine.

Metode zaštite

- Kriptografske metode
- Programske metode
- Organizacione metode
- Fizičke metode

- *Napomena:* mnogi autori ovu podelu smatraju prevaziđenom

Različiti aspekti zaštite

- Zaštita na nivou aplikacije
- Zaštita na nivou operativnog sistema
- Zaštita na nivou mrežne infrastrukture
- Proceduralna i operaciona zaštita

Pristup organizacije $(ISC)^2$

- International Information Systems Security Certification Consortium [$(ISC)^2$] ustanovio je postupak CISSP sertifikacije.
- $(ISC)^2$ je neprofitna organizacija čija je jedina funkcija da razvija i administrira programe sertifikacije.
- Značenje titule CISSP je "sertifikovani profesionalac za sigurnost informacionih sistema" (Certified Information Systems Security Professional).
- Uloga ove organizacije je da formira i održava takozvani Zajednički skup osnovnih znanja (engl. Common Body of Knowledge, CBK), koji obuhvata deset oblasti zaštite.

$(ISC)^2$ deset domena

1. Sistemi za kontrolu pristupa
2. Sigurnost razvoja aplikacija i sistema
3. Planiranje oporavka od napada i obezbeđivanje kontinuiranog poslovanja
4. Kriptografija
5. Pravni i etički aspekti sigurnosti
6. Fizička sigurnost
7. Sigurnost operative
8. Upravljanje sigurnosnim sistemima
9. Sigurnosne arhitekture i modeli
10. Sigurnost komunikacionih i računarskih mreža

Certified Ethical Hacker (CEH)

- The Certified Ethical Hacker (C|EH) is a professional certification provided by the International Council of E-Commerce Consultants (EC-Council).

"The CEH Program certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker."

Citat preuzet sa: www.eccouncil.org/ceh.htm

CompTIA Security+™ Certification

- Isečak sa CompTIA Web sajta:

"CompTIA Security+ validates knowledge of systems security, network infrastructure, access control, assessments and audits, cryptography and organizational security. It is an international, vendor-neutral security certification that is taught at colleges, universities and commercial training centers around the world.

Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of on-the-job technical networking experience, with an emphasis on security. The CompTIA Network+ certification is also recommended.

Because human error is the number one cause for a network security breach, CompTIA Security+ is recognized by the technology community as a valuable credential that proves competency with information security."

Citat preuzet sa: http://certification.comptia.org/security/

Sigurnosni standardi i programi sertifikacije

- Više o sigurnosnim standardima i programima sertifikacije
  - -> **Dodatak A** udžbenika **"Sigurnost računarskih sistema i mreža"**

Projektovanje sistema zaštite

- Prilikom projektovanja sistema zaštite potrebno je odrediti sledeće:
  - lice odgovorno za projekat
  - metode identifikacije korisnika i terminala
  - strukture šema ovlašćenja
  - načine detekcije nedozvoljenih pristupa
  - načine integrisanja zaštite u sistemske programe
  - postupke oporavka zbog oštećenja datoteka
  - postupke oporavka zbog otkaza sistema
  - metode nadzora
  - da li treba koristiti kriptografiju ili ne
  - kontrole koje treba ugraditi radi analize i korišćenja statističkih datoteka
  - kontrole koje treba ugraditi u operacije pregledanja datoteka

Principi projektovanja sistema zaštite

- Principi projektovanja sistema zaštite su sledeći:
  - ekonomičnost zaštite (projekat treba da je što jednostavniji)
  - pouzdanost zaštite
  - potpuna provera (inicijalizacija, radni režim, oporavak, isključivanje i održavanje)
  - javnost projekta (mehanizmi zaštite ne bi trebalo da zavise od neznanja potencijalnih napadača)
  - razdvajanje prava
  - najmanja prava
  - redukcija zajedničkih mehanizama
  - psihološka prihvatljivost (sprega između računara i čoveka)
  - radni faktor
  - evidencija ugrožavanja

Funkciju cene gubitaka podataka

- Prilikom projektovanja zaštite potrebno je uzeti u obzir i funkciju cene gubitaka podataka:

C = f(D, I, P)

gde je:

- C – cena gubitaka
- D – tip datoteke kojoj pripadaju podaci
- I – vrsta napadača za koju je zaštita projektovana (neupućena lica, obučena lica, lica koja žele da ostvare dobit, dobro opremljeni kriminalci, finansijski jake organizacije, viša sila)
- P – vrsta posledica po integritet podataka

Literatura

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

- Za predavanje 1:
  - Poglavlje 1: Pretnje, napadi, sigurnost i metode zaštite
  - Dodatak A: Sigurnosni standardi i programi sertifikacije

Literatura - nastavak

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

www.conwex.info/draganp/books.html



Dodatna literatura

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

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

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

- Druge knjige i razni *online* resursi

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

Pitanja

?