Uvod u računarske sisteme

Odabrana poglavlja iz informacione sigurnosti

Nemanja Maček

Sadržaj

- Uvodna razmatranja
- Terminologija
- Klasifikacija napada
- Sigurnosni ciljevi
- Kriptografija (osnovni pojmovi)
- Kriptografski protokoli
- Mrežne barijere i IDS sistemi
- Kontrola pristupa

Uvodna razmatranja

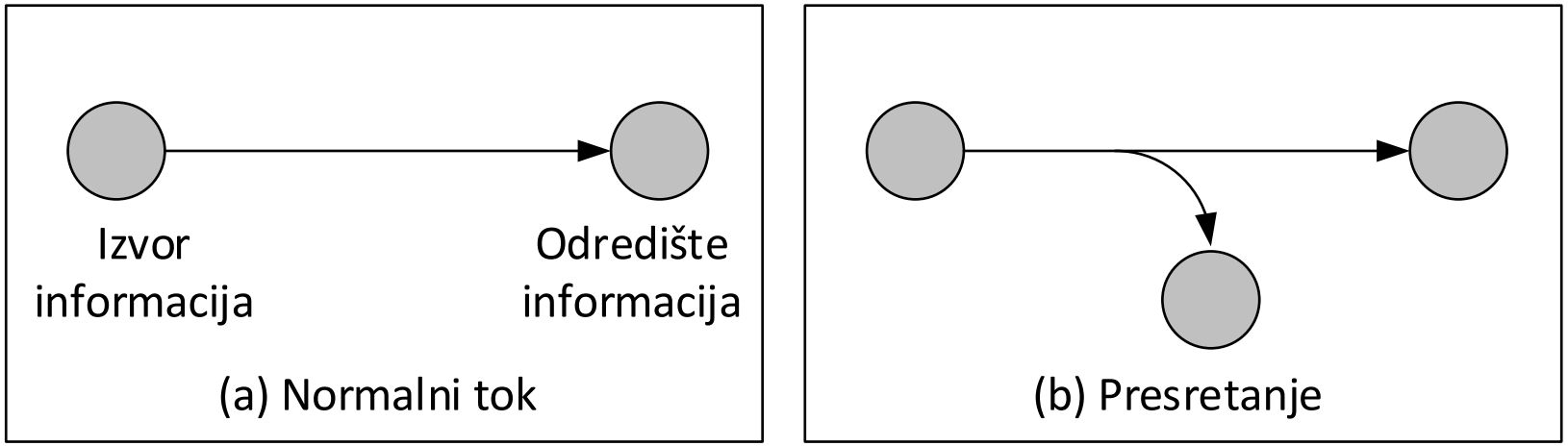
- **Informaciona sigurnost** (*information security*) je široka oblast koja sadrži veliki broj gradivnih elemenata (podoblasti).
- Sve podoblasti su relativno složene (gledano kako sa inženjerskog tako i sa naučnog gledišta).
- Ne može se izdvojiti stučnjak (praktičar) ili istraživač koji u svim podoblastima postiže značajne i upečatljive rezultate!
- Većina praktičara se ograničava na nekoliko **usko povezanih podoblasti**!
  - Primer 1: administrator računarskih mreža ili Linux servera (praktičar).
  - Primer 2: istraživač u oblasti biometrijskih sistema.
- **Dobra praksa**: zadržati širinu, a fokusirati se na srodne podoblasti!
- Čak i policija ima odeljenja za ubistva i narkotike!
  - Svi “znaju” da koriste službenu palicu i vatreno oružje (širina).
  - Specijalizovani su za pronalaženje ubica ili marihuana (dubina).

Napad na sigurnost, sigurnosni mehanizam i usluge

- **Napad na sigurnost** (*security attack*) je bilo koja akcija koja ugrožava sigurnost informacija.
  - Napadi su akcije koje su usmerene na ugrožavanje sigurnosti informacija, računarskih sistema i mreža.
- **Sigurnosni mehanizam** (*security mechanism*) je mehanizam koji treba da detektuje i predupredi napad ili da sistem oporavi od napada.
- **Sigurnosna usluga** (*security service*) je usluga koja povećava sigurnost sistema za obradu i prenos podataka.
  - Sigurnosna usluga podrazumeva upotrebu jednog ili više sigurnosnih mehanizama.
  - Primer: autentifikacija USB tokenom, autentifikacija lozinkom i biometrijskim uzorkom.
- Postoje različite vrste napada i nekoliko načina klasifikacije.
- Generalno, napadi se mogu podeliti u četiri kategorije:
  - **Presretanje** (*interception*)
  - **Presecanje**, tj. prekidanje (*interruption*)
  - **Izmena** (*modification*)
  - **Fabrikovanje** (*fabrication*).

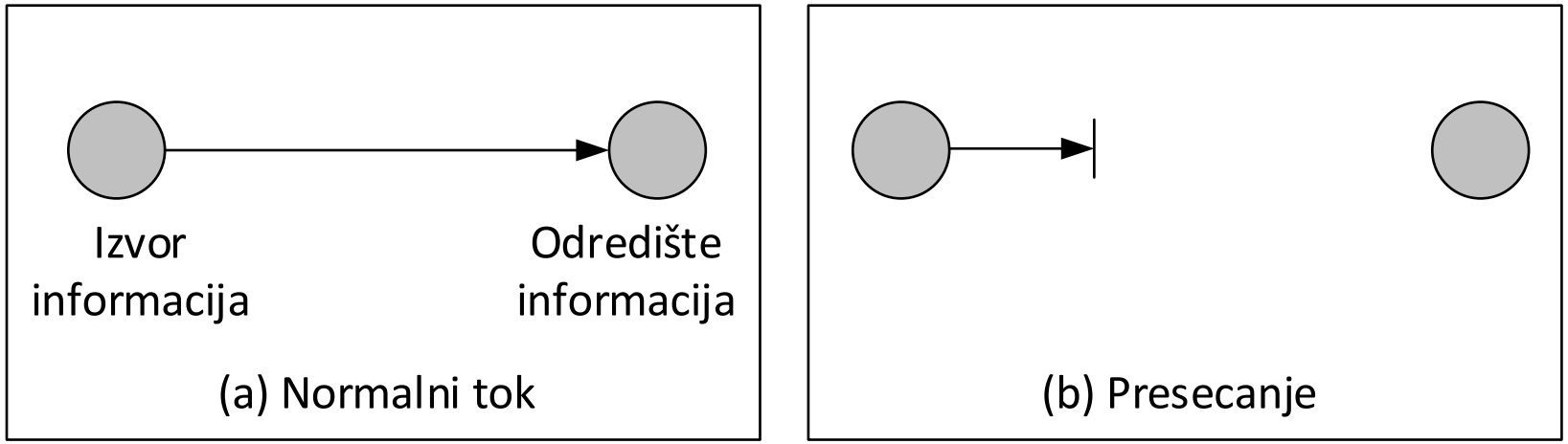
Klasifikacija napada: presretanje

- **Presretanje** je **pasivan** napad na **poverljivost** (*confidentiality*).
- Može biti u praksi sprovedeno kao prisluškivanje saobraćaja, nadziranje njegovog intenziteta, uvid u osetljive informacije ili slično.
- Teško se otkriva jer ne menja podatke, odnosno ne utiče na unutrašnje funkcionisanje sistema.
- Ovakav tip napada ponekad je pripremna faza za neku drugu vrstu napada.



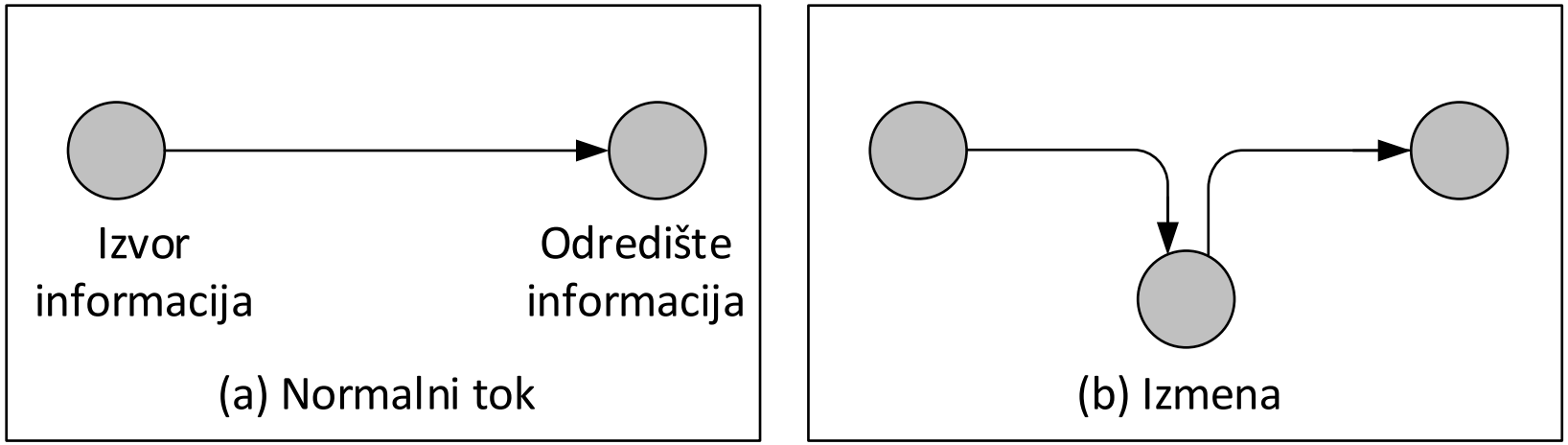
Klasifikacija napada: presecanje

- **Presecanje**, tj. prekidanje je **aktivan** napad na **raspoloživost** (*availability*).
- Presecanjem se prekida tok informacija, tj. onemogućava pružanje neke usluge ili funkcionisanje nekog sistema.
- Primer presecanja bi bio uspešno izvršen DoS / DDoS napad na neku Web stranicu ili uništenje podataka na nekom računarskom sistemu (na primer, infekcija Ransomware-om za koji se zna da se nakon plaćanja otkupa ne dobija ključ za dešifrovanje datoteka).



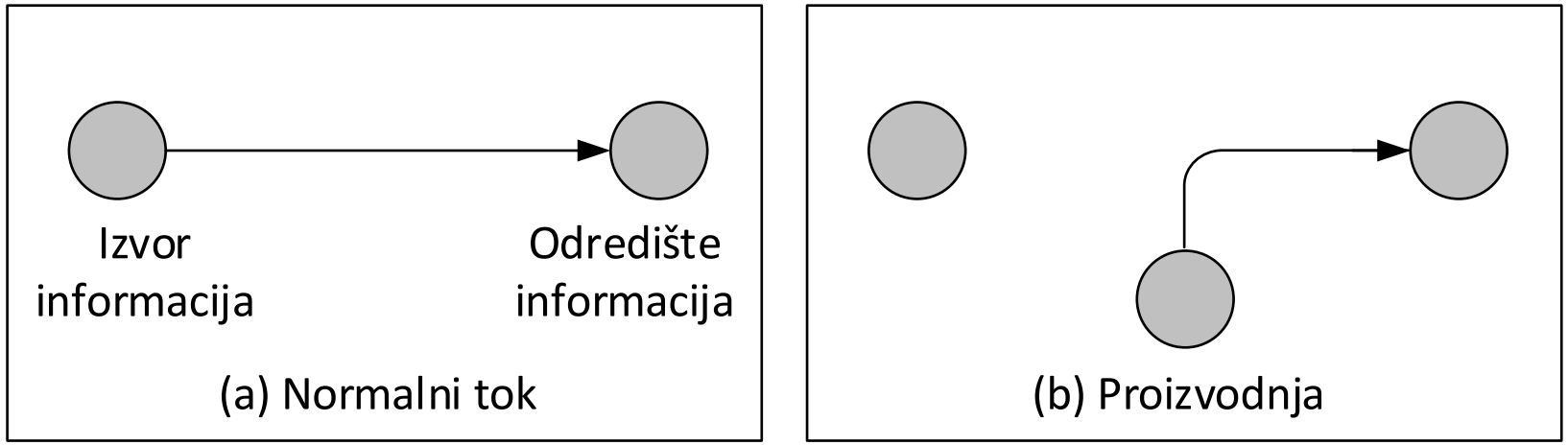
Klasifikacija napada: izmena

- **Izmena** je **aktivan** napad na **integritet** (*integrity*).
- Na prenosnom putu može se ispoljiti kao napad tipa čovek u sredini (*man in the middle*).
- U računarskom sistemu se može ispoljiti kao izmena podataka, pristupnih prava ili načina funkcionisanja programa.
- Iako menja podatke ili sistem, ovaj napad često ostaje neprimećen izvesno vreme, kako zbog nepažnje, tako i zbog složenih tehnika koje se pri ovom napadu koriste.



Klasifikacija napada: fabrikovanje

- **Fabrikovanje** je **aktivan** napad na **autentičnost** (*authenticity*).
- Na primer, napadač generiše lažne podatke, lažni saobraćaj ili izdaje neovlaštene komande.
- U ove napade spada i lažno predstavljanje korisnika, usluge, servera, Web strane ili nekog drugog dela sistema.



Klasifikacija napada prema Kendall-u

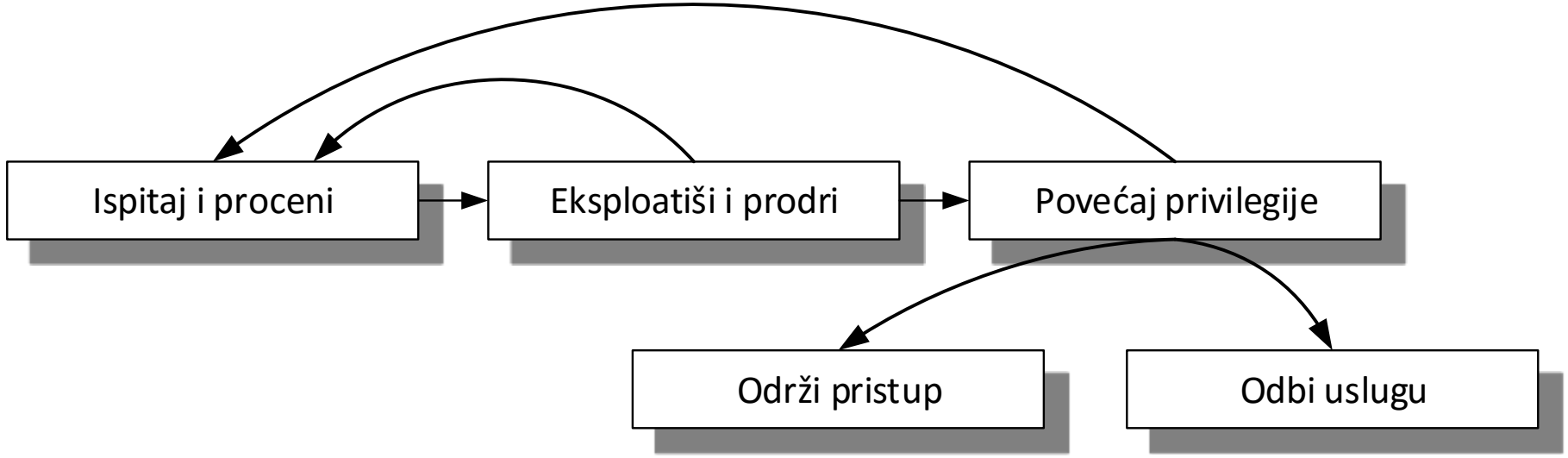
- Alternativno, napadi se shodno Kendall-ovoj taksonomiji mogu klasifikovati i u sledeće četiri kategorije: ispitivački napadi, napadi neovlašćenog sticanja pristupa udaljenom računaru, neovlašćenog povećanja privilegija i odbijanja usluga.
- **Ispitivački napadi** (*probing*).
  - Napadač prikuplja informacije o sistemu ili mreži i traži ranjivosti koje može da iskoristi kao što su neispravno konfigurisani zaštitni mehanizmi.
  - Ovo su pasivni napadi koji se koriste se u fazi pripreme aktivnih napada.
  - Primeri izvođenja: skeniranje portova (nmap), popisivanje (*fingerprinting*), odnosno određivanje tipa i verzije OS kako be se znalo koji sigurnosni propust treba iskoristiti.
- **Napadi neovlašćenog sticanja pristupa udaljenom računaru** (*Remote to Local*, R2L).
  - Napadi kojima se neovlašćeno stiče pristup udaljenom računaru na kome napadač nema legitiman korisnički nalog.
  - Primeri: pogađanje lozinke (rečnika, Rainbow tabele), upotreba rootkit alata.
  - NAPOMENA: rootkit omogućava napadaču da se sakrije i održi privilegovan pristup računaru zaobilaženjem normalne autentifikacije i mehanizama autorizacije.

Klasifikacija napada prema Kendall-u

- **Napadi neovlašćenog povećanja privilegija** (*priviledge escalation*, *User to Root*, U2R).
  - Napadi kojima se eksploatišu ranjivosti operativnih sistema ili softvera.
  - Često su zasnovani na prekoračenju bafera ili dovođenje sistema u stanje trke.
  - Cilj napadača je sticanje većih privilegija na žrtvi, u idealnom slučaju privilegija administratora (odatle potiče naziv *User to Root*).
- **Napadi odbijanja usluga** (*Denial of Service*, DoS).
  - Napadi koji za posledicu imaju nedostupnost resursa.
  - Na primer, napadač neovlašćeno koristi računarske resurse (memorija, CPU), sistem je prezauzet i ne može da odgovori na legitimne zahteve.
  - Primeri izvođenja:
    - Eksploatisanje ranjivosti u sastavljanju fragmenata IP paketa (fragmenti sa preklopnjenim *offest* poljima).
    - Iskorišćavanje ranjivosti uspostavljanja TCP konekcije (veliki broj poluotvorenih konekcija).

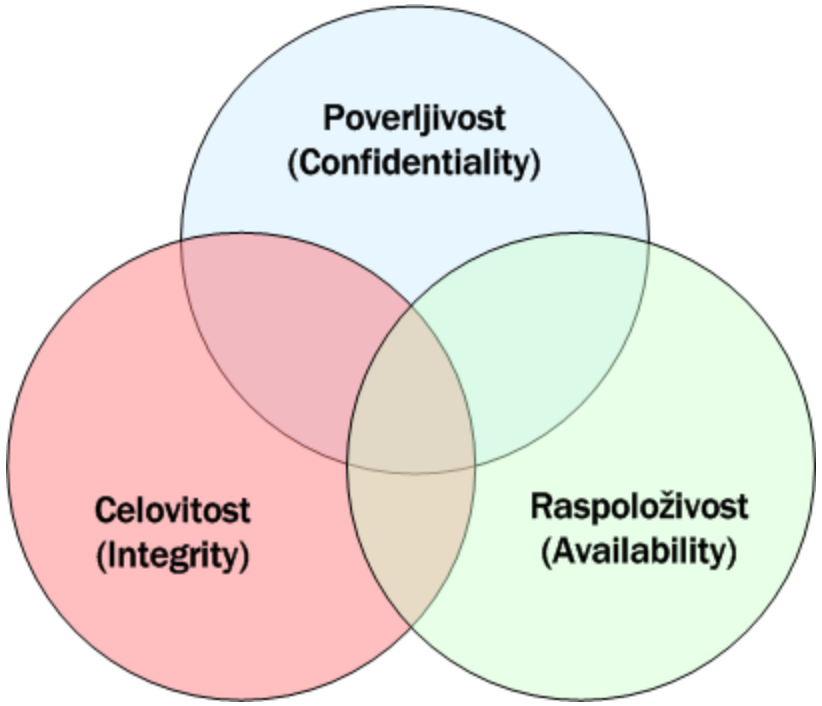
Faze napada

- Ove četiri kategorije usklađene su donekle sa osnovnim koracima metodologije napadača:
  - **Ispitaj i proceni** (istraživanje potencijalne mete, identifikovanje i procena ranjivosti, planiranje i eventualna simulacija napada pre samog izvođenja daljih koraka)
  - **Eksploatiši i prodri** (iskorišćavanje identifikovanih ranjivosti i sticanje pristupa sistemu)
  - **Povećaj privilegije** (u idealnom slučaju privilegije administratora)
  - **Održi pristup** (prikrivanje tragova i postavljanje takozvanih sporednih ulaza)
  - **Uradi ono šta si naumio** (odbi uslugu, preuzmi podatke, izmeni ili generiši lažne podatke).



Poverljivost, integritet, raspoloživost

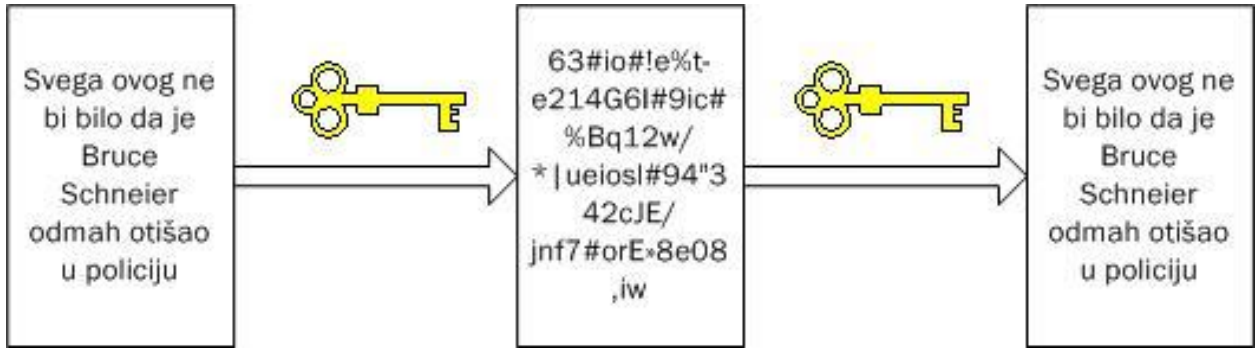
- Poverljivost (*confidetiality*)
- Integritet (*integrity*)
- Raspoloživost (*availability*)



- *Disclosure*, *Alternation*, *Destruction* = DeAD

Kriptografija (osnovni pojmovi)

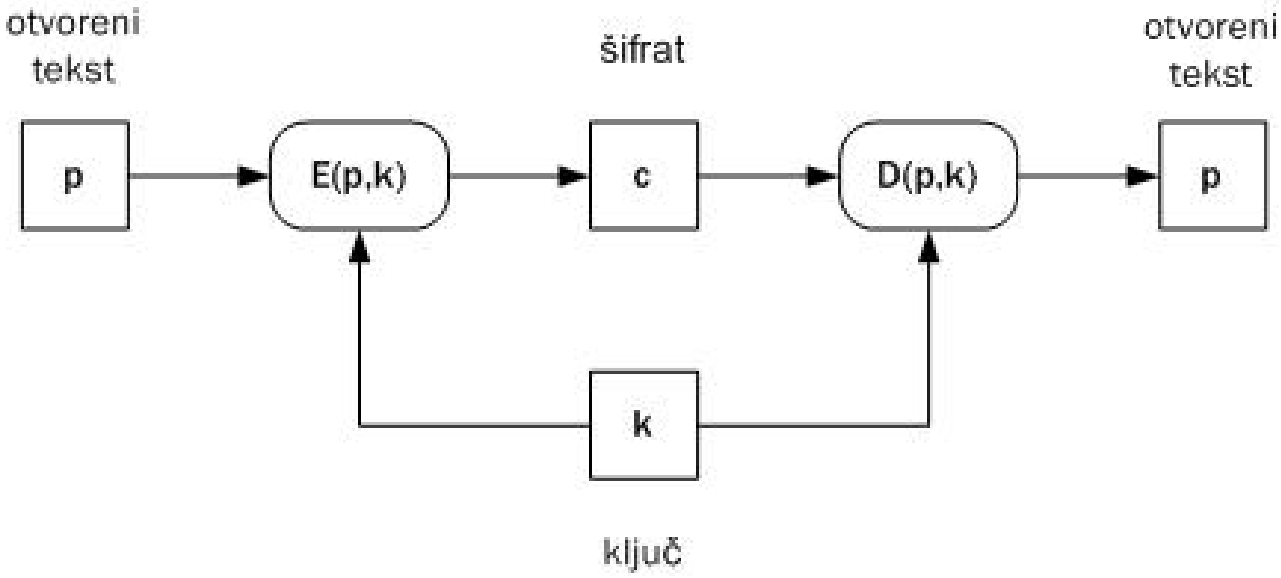
- **Šifrovanje**: otvoreni tekst + ključ → šifrat
- **Dešifrovanje**: šifrat + ključ → otvoreni tekst



- Korisnik bez odgovarajućeg ključa nema pristup šifrovanim podacima.
- Šifrovani podaci se mogu preneti preko nesigurnog kanala ili čuvati na disku koji nije zaštićen!
- Sigurnost šifrata treba da zavisi samo od tajnosti ključa a ne od tajnosti algoritma!

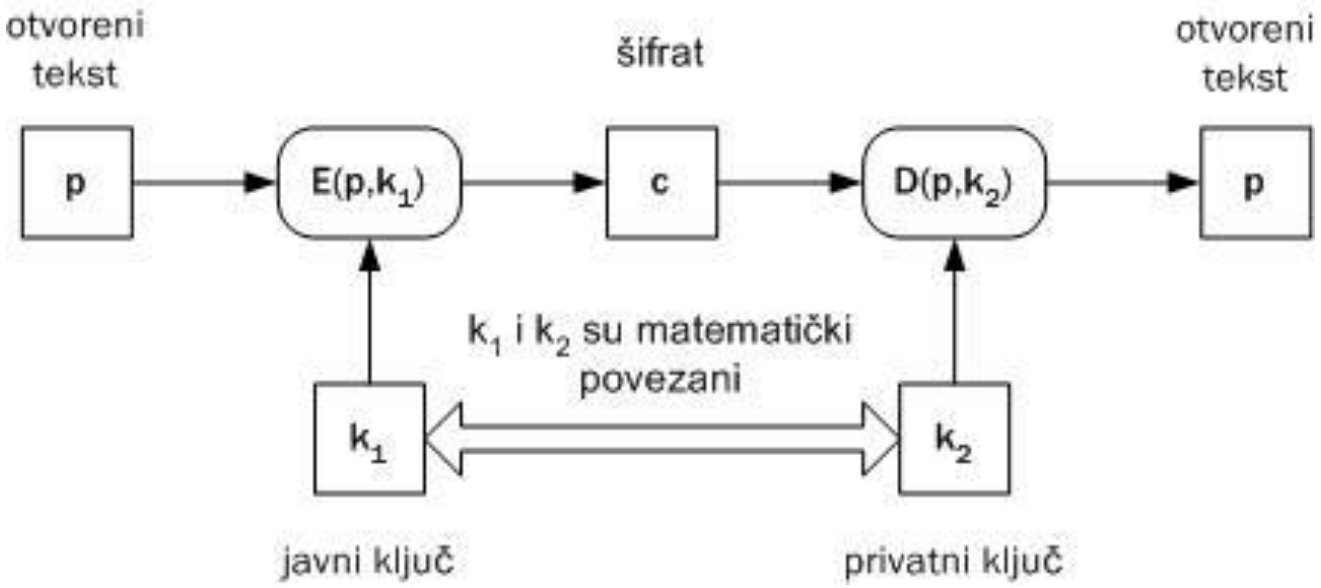
Kriptografija (osnovni pojmovi)

- **Simetrični algoritmi**.



- **Blokovski**. Primeri: DES, AES, Blowfish, Twofish.
- **Sekvencijalni**. Primer: RC4.

- **Algoritmi sa javnim ključem**.



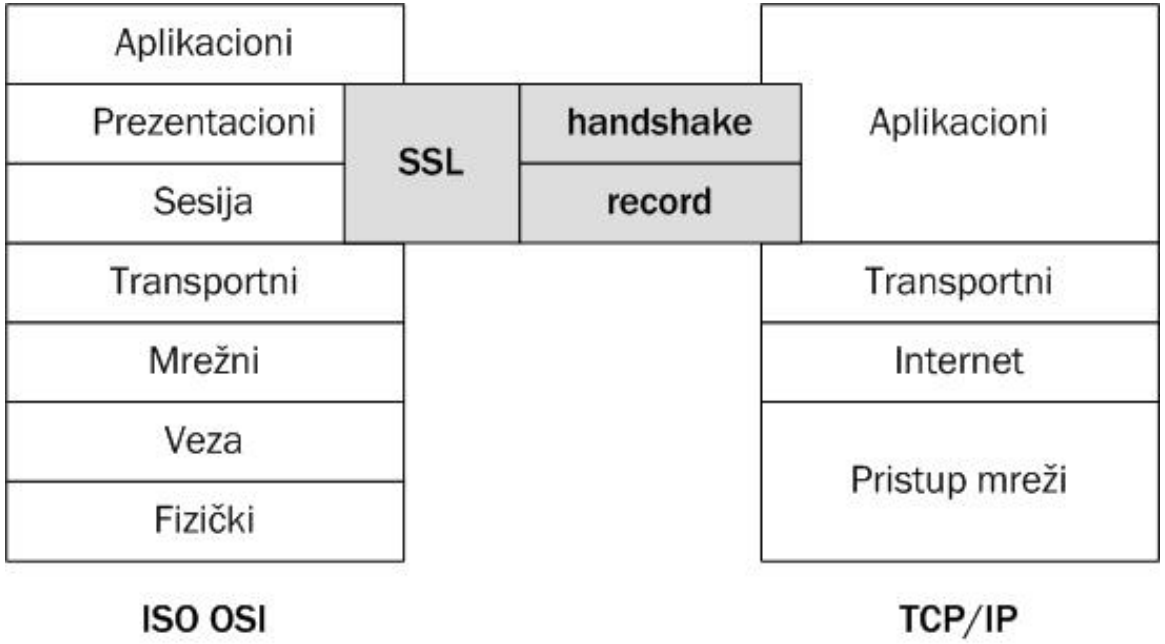
- Primeri: RSA, ElGammal.

Kriptografija (osnovni pojmovi)

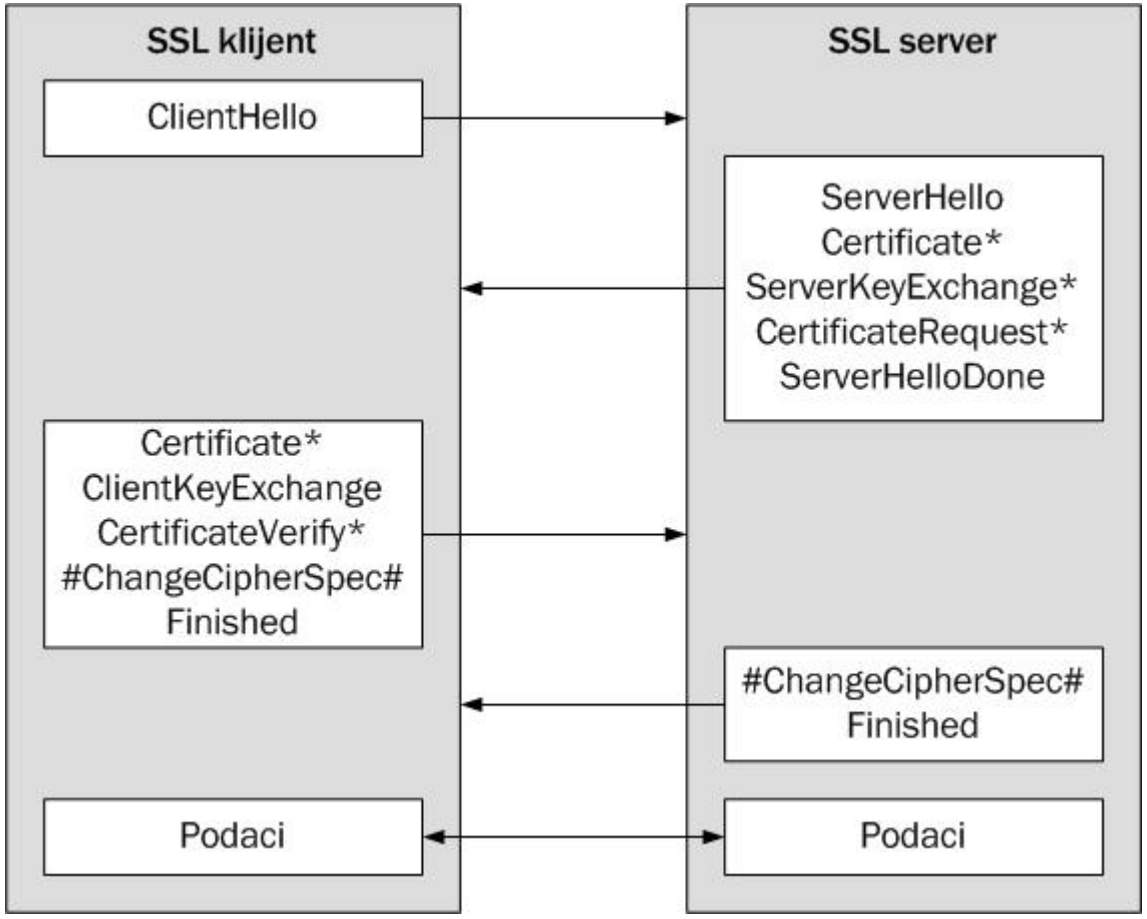
- **Jednosmerne heš funkcije** na osnovu ulaznog podatka proizvodi rezultujući niz tačno određene dužine – heš, koji, uslovno rečeno, jednoznačno identifikuje ulazni podatak.
- **Digitalni potpis** je elektronska verzija potpisa koja identifikuje pošiljaoca i dokazuje verodostojnost poruke.
  - **Potpisivanje**. pošiljalac najpre jednosmernom heš funkcijom računa heš h_1 poruke p, koju nakon toga potpisuje svojim privatnim ključem.
  - **Provera potpisa**. Primalac određuje heš h_2 primljene poruke i proverava primljeni potpis s_1 javnim ključem pošiljaoca.

Kriptografski protokoli – Secure Socket Layer

- Formira poseban komunikacioni sloj smešten **iznad transportnog sloja**.
- Iznad SSL sloja nalazi se aplikacioni sloj.
- Dva protokola: SSL *handshake* i SSL *record*.



Kriptografski protokoli – SSL *handshake*



Kriptografski protokoli – SSL *record*

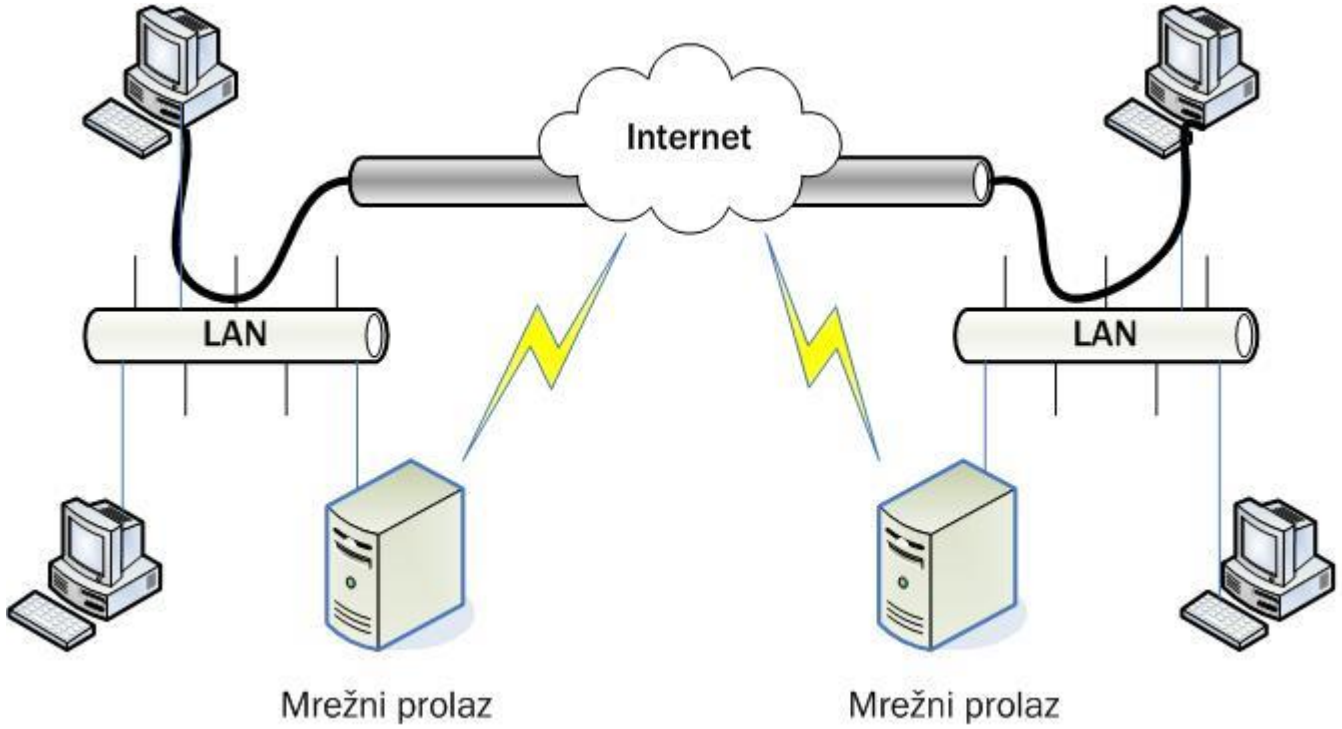
- Kako se nakon rukovanja odvija komunikacija?
- **Pošiljaoc**:
  - SSL prima poruku sa aplikacionog sloja.
  - Rastavlja poruku na manje delove pogodne za šifrovanje.
  - Dodaje kontrolni broj.
  - Delove poruke šifruje i komprimuje.
- **Primalac**:
  - Prima šifrovane delove poruke.
  - Obavlja dekompresiju i dešifrovanje.
  - Proverava kontrolne brojeve.
  - Sastavlja delove poruke i predaje ih aplikacionom sloju.

Kriptografski protokoli – IPSec

- IPSec je:
  - Skup proširenja IPv4
  - Integralni deo IPv6.
- Obezbeđuje: privatnost, integritet, proveru identita i neporecivost.
- IPSec implementira sigurnosne mehanizme mrežne komunikacije **na mrežnom sloju OSI referentnog modela**.
- Podržava dva režima rada:
  - **Prenosni** (*transport mode*). Šifruju se samo podaci (*payload* IP paketa) ali ne i zaglavlja.
  - **Tunelovanje** (*tunnel mode*). Koristi se IPSec tunel tako da su šifrovani kompletni IP paketi.
- Implementacija u vidu dva nezavisna protokola
  - AH (*Authentication Header*): obezbeđuje integritet, autentičnost i neporecivost.
  - ESP (*Encapsulated Security Payload*): osim toga obezbeđuje i privatnost podataka.

Kriptografski protokoli – IPSec

- IPSec tunel.



Kriptografski protokoli – Kerberos

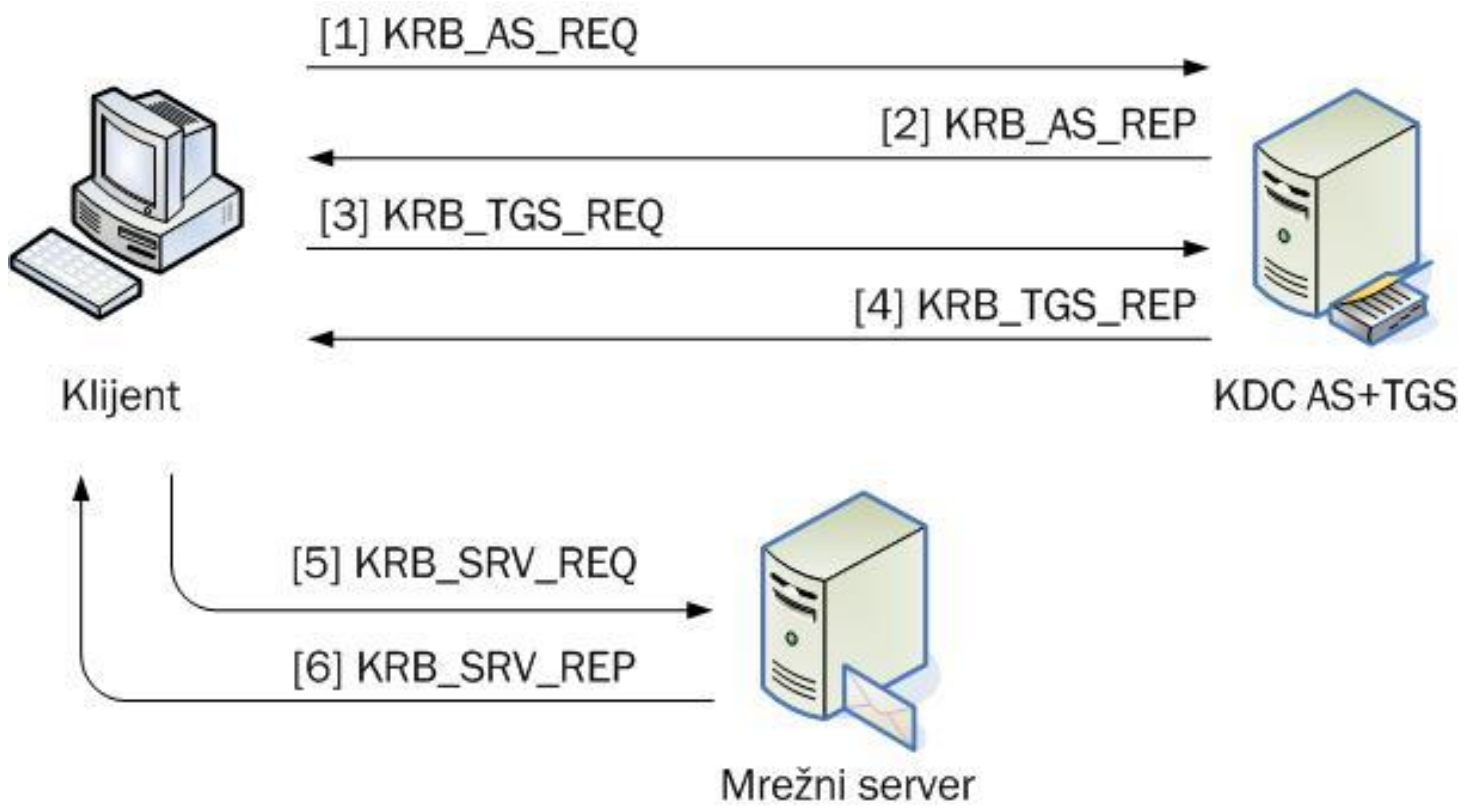
- *History lesson* (ovo nije ispitno pitanje!)

- Κέρβερος, što znači demon iz jame, u grčkoj mitologiji predstavlja troglavog psa čuvara ulaza u podzemlje (Had).
- Kerber je imao rep u obliku zmije, a sluz koja je padala na tlo stvarala je otrovnu biljku akonitu.
- Kerber je imao sestru Himeru i brata Orta, a potomak je Ehidnu i Tifona.
- Nekoliko puta su ga savladali različiti mitski junaci: Heraklo (u svome poslednjem zadatku), Orfej (koji ga je uspavao svojom muzikom), Hermes (koji ga je uspavao vodom iz reke Lete) i Psiha (koja ga je uspavala otrovanim kolačima od meda).

Kriptografski protokoli – Kerberos

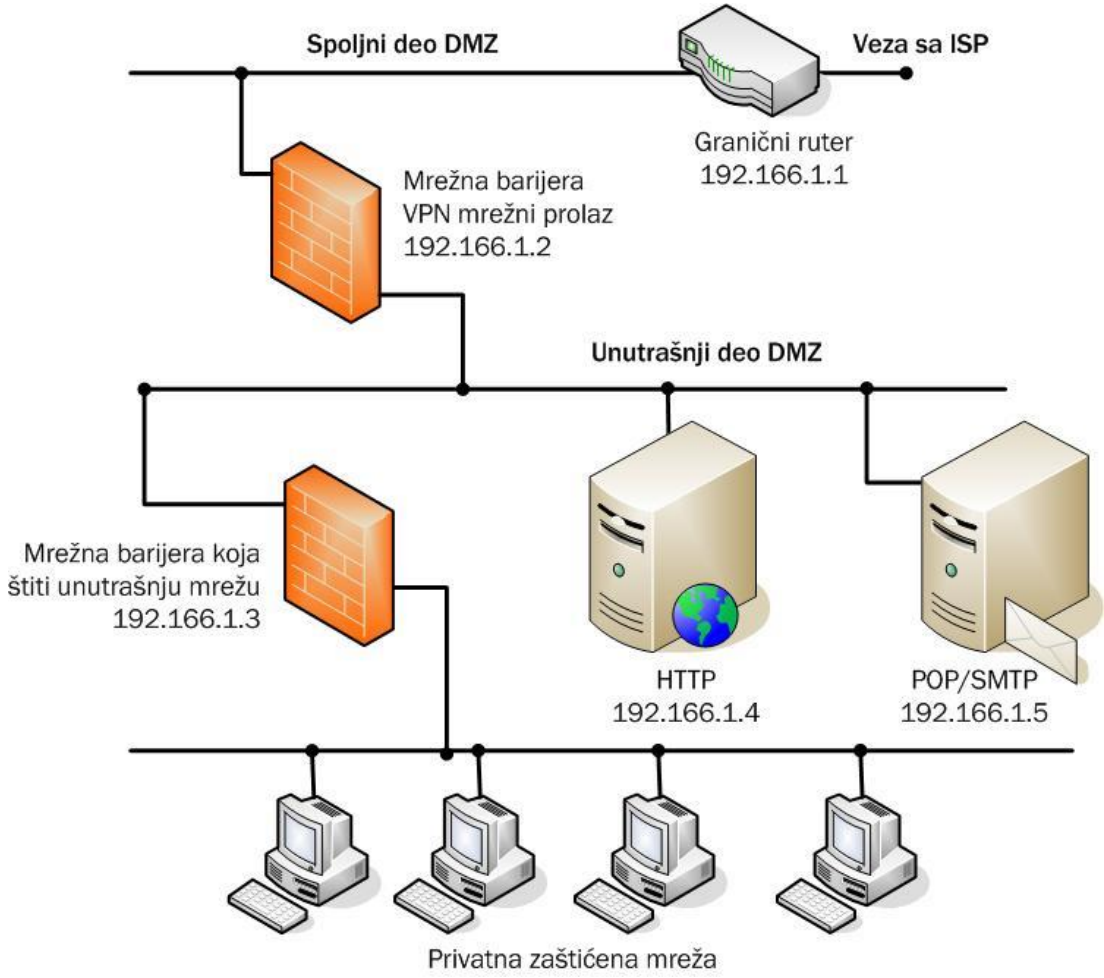
- Autentifikacioni protocol tipa *Single-Sign-On* (prijavi se samo jednom).
  - Korisnik se jednom prijavi na sistem i nakon toga u skladu sa svojim ovlašćenjima ima pristup resursima.
- **Baza principala** sadrži sve principale Kerberos oblasti sa odgovarajućim tajnim ključevima.
- **Server za proveru identiteta** (*Authentication Server*, AS) izdaje takozvanu *Ticket Granting Ticket*.
- **Server za dodelu karata** (*Ticket Granting Server*, TGS) izdaje karte za pristup mrežnim resursima.

Kriptografski protokoli – Kerberos

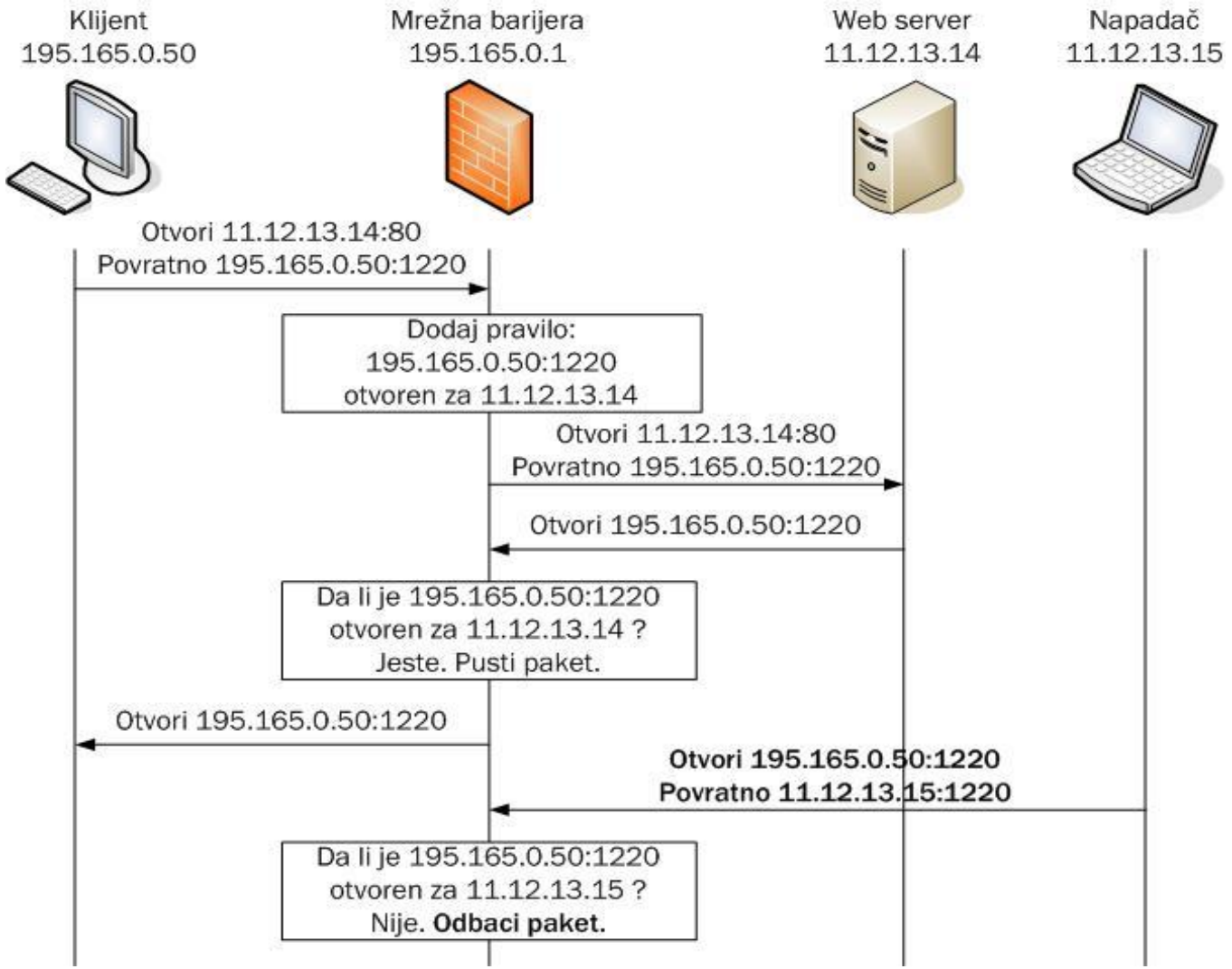


“Firewalls 24/7”

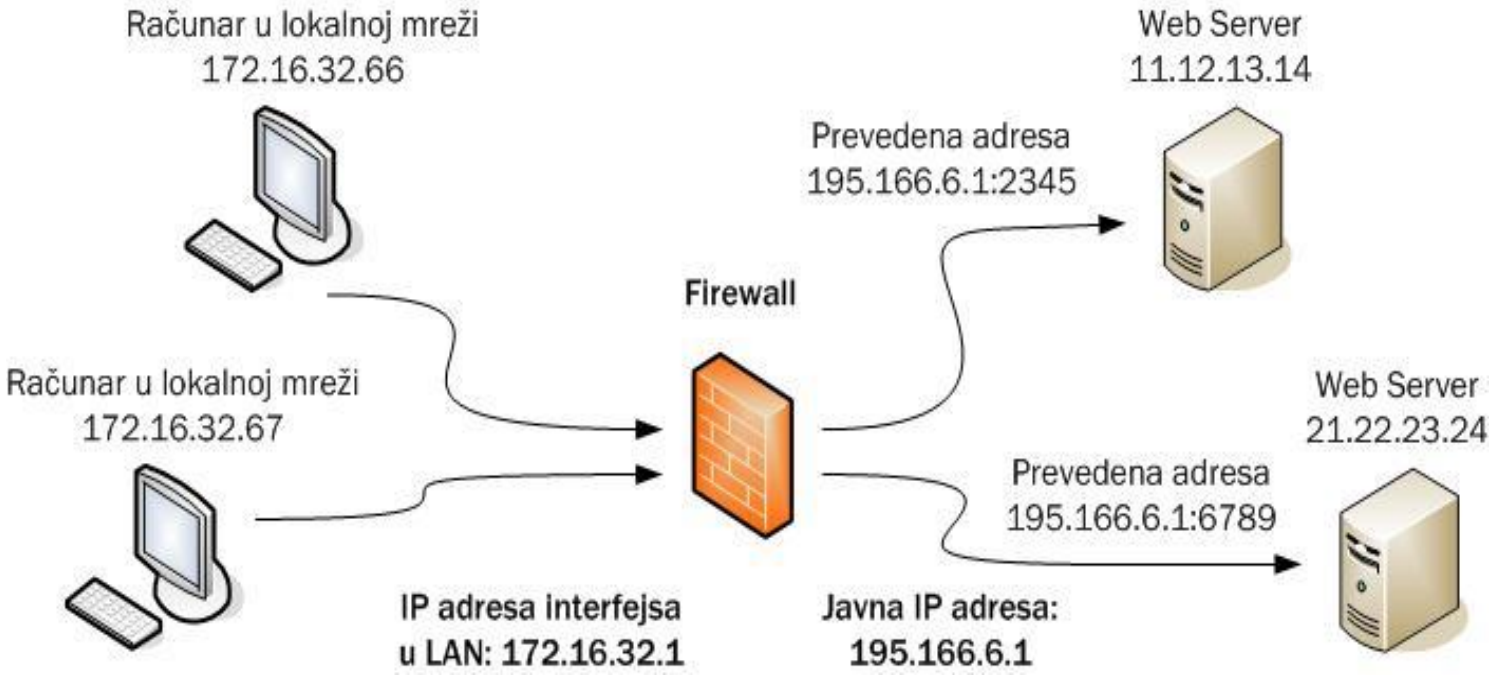
- Funkcije:
  - Filtriranje paketa
    - *Stateless*
    - *Stateful*
  - Prevođenje mrežnih adresa (NAT)
  - Proksi (*proxy*)



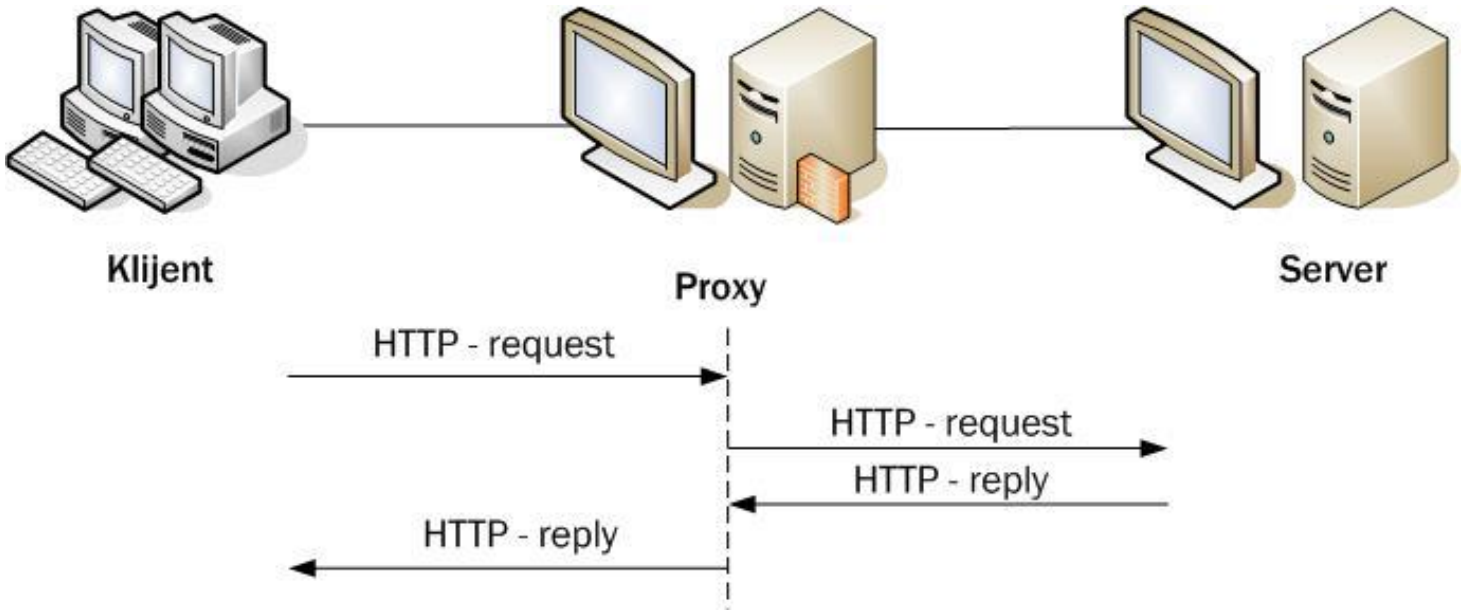
Mrežne barijere – *statefull packet filter*



Mrežne barijere – NAT



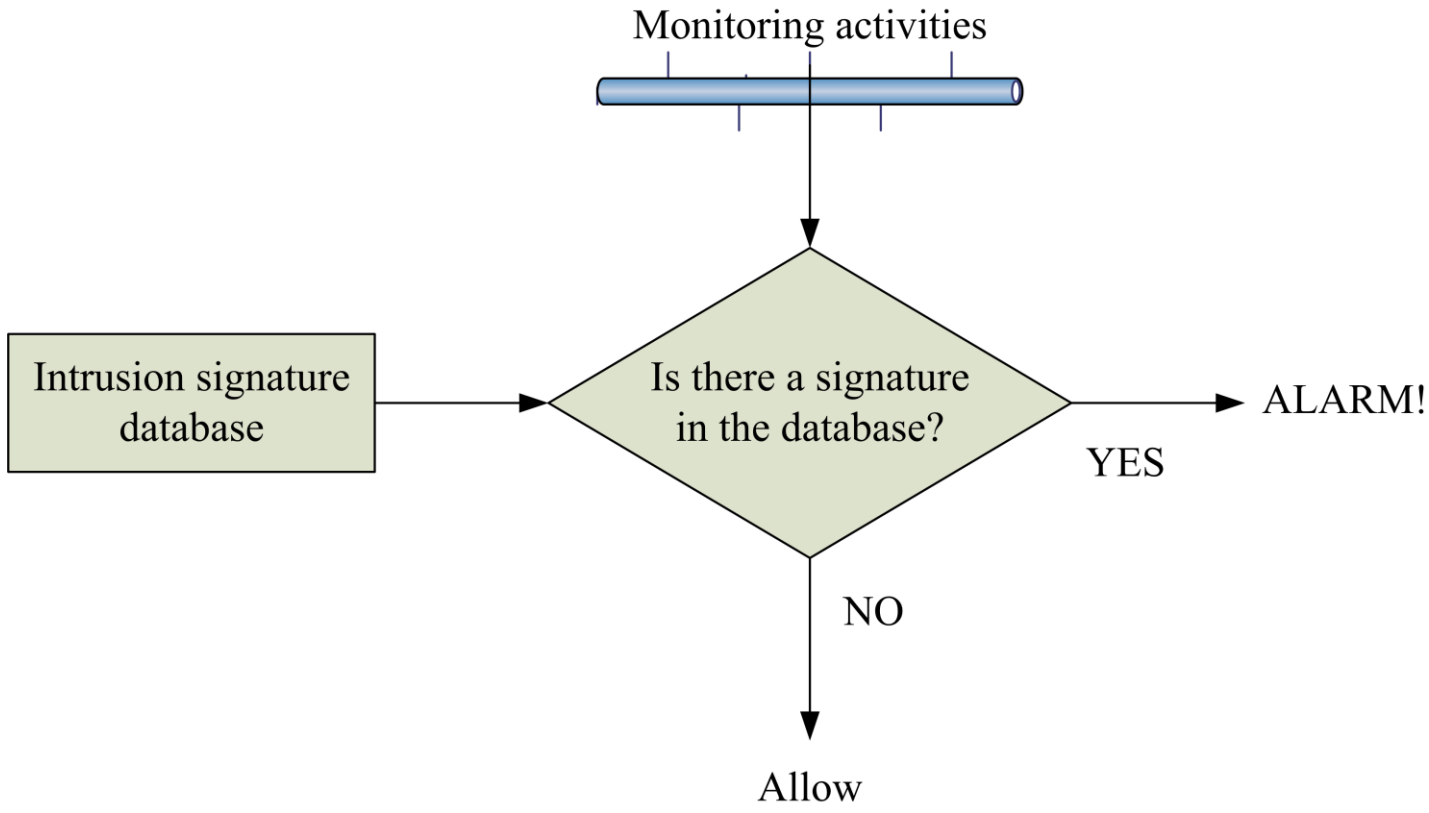
Mrežne barijere – proksi



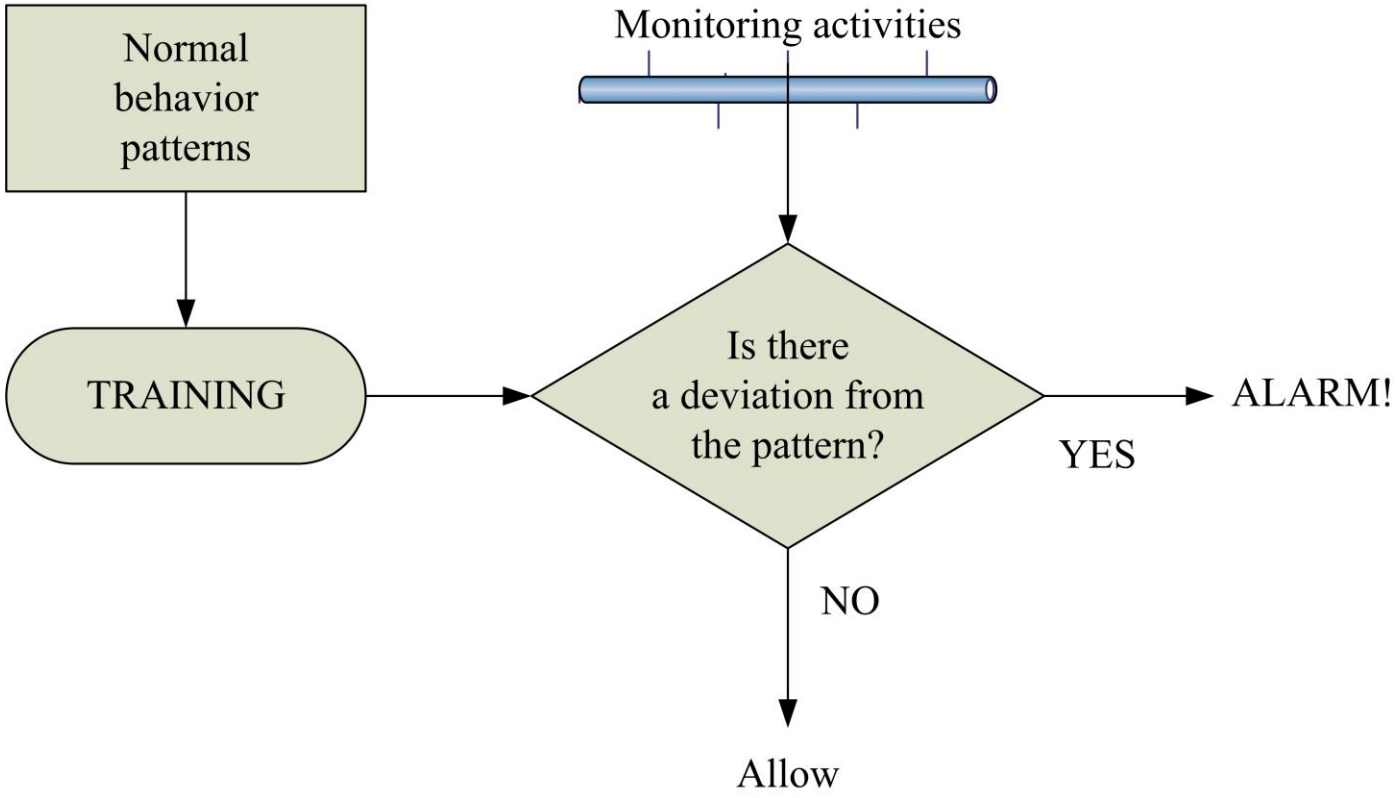
Sistemi za detekciju i sprečavanje upada

- Džim Anderson: upad u računarski sistem ili mrežu je svaki neovlašćeni pokušaj pristupa, izmene ili uništavanja informacija ili dovođenja sistema u nepouzdano ili neupotrebljivo stanje.
- U prevodu: upad je bilo koji skup akcija koji narušava integritet, poverljivost ili raspoloživost resursa.
- Sistem za detekciju upada nadgleda događaje u računarskom sistemu ili mreži i otkriva aktivnosti koje ukazuju na upade.
- Sistemi za detekciju upada su nastali kao odgovor na napade koji se ne mogu otkriti ili sprečiti drugim zaštitnim mehanizmima!

Sistemi za detekciju i sprečavanje upada – detekcija potpisa



Sistemi za detekciju i sprečavanje upada – detekcija anomalija



Kontrola pristupa

- Kontrola pristupa = autentifikacija + autorizacija.
- 4 načina autentifikacije:
  - Nešto što korisnik **zna** (lozinka, PIN).
  - Nešto što korisnik **ima** (*smart* kartica, USB token).
  - Nešto što korisnik **jeste** (otisak prsta, lice, iris).
  - Nešto što korisnik **može da uradi** (verifikacija govornika, potpis).
- Najčešće se koriste lozinke.
  - Problemi sa lozinkama?
  - Napadi na lozinke: *brute force*, *dictionary*, *rainbow*.
- 2-*factor security*.
  - Primer: USB token + lozinka.
- 4-*factor security*.
- “Ekstremna” sigurnost: iris skener na ulazu u Google Datacenter.

Kontrola pristupa (biometrija)

- Utvrđivanje identiteta osobe na osnovu fizičkih ili ponašajnih karakteristika .
- **Fizičke karakteristike** (otisak prsta, iris, geometrija i fotometrija lica) = ono što osoba jeste.
- **Ponašajne karakteristike** (glas, dinamika kucanja) = ono što osoba može da uradi.
- Šta je verifikacija a šta identifikacija?
- Moduli: senzor, izdvajanje obeležja, baza templejta, modul za poređenja.
  - Templejt nije isto što i otisak!
- **Prednosti** u odnosu na ostale metode provere identiteta:
  - Uzorci se teško kradu, dele i reprodukuju.
  - Tolerancija na napade grubom silom.
  - Gotovo apsolutna neporecivosti.
- **Problemi**:
  - Prihvatljivost.
  - Fizička sigurnost.
  - Zaštita privatnosti biometrijskih uzoraka.

Napredni zaštitni mehanizmi

- Zaštitni sistemi zasnovani na veštačkoj inteligenciji (VI) su jedna od (uslovno rečeno) novijih oblasti istraživanja koja dobija sve veći značaj u praksi.
- VI se najčešće koristi da poveća performanse onih mehanizama kod kojih se detektuju anomalije u ponašanju.
- Primeri: IDS sistemi, SPAM filtri itd
- Konkretan primer: IDS sistem zasnovan na binarnoj klasifikaciji implementiranoj preko C4.5 stable.

Literatura

1. D. Pleskonjić, N. Maček, B. Đorđević, M. Carić (2007): Sigurnost računarskih sistema i mreža. Mikro knjiga, Beograd.
2. M. Veinović, S. Adamović (2013): Kriptologija 1. Univerzitet Singidunum, Beograd. *
3. M. Milosavljević, S. Adamović (2014): Kriptologija 2. Univerzitet Singidunum, Beograd. *
4. M. Stamp (2006): *Information Security*. John Wiley and Sons.

* Može se besplatno preuzeti sa portala: www.singipedia.com

Hvala na pažnji

Pitanja su dobrodošla.