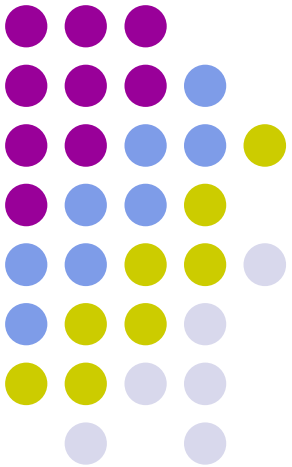
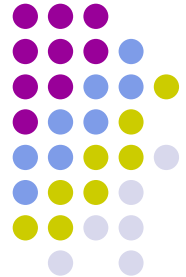
Upravljanje sadržajem



Upravljanje sadržajem



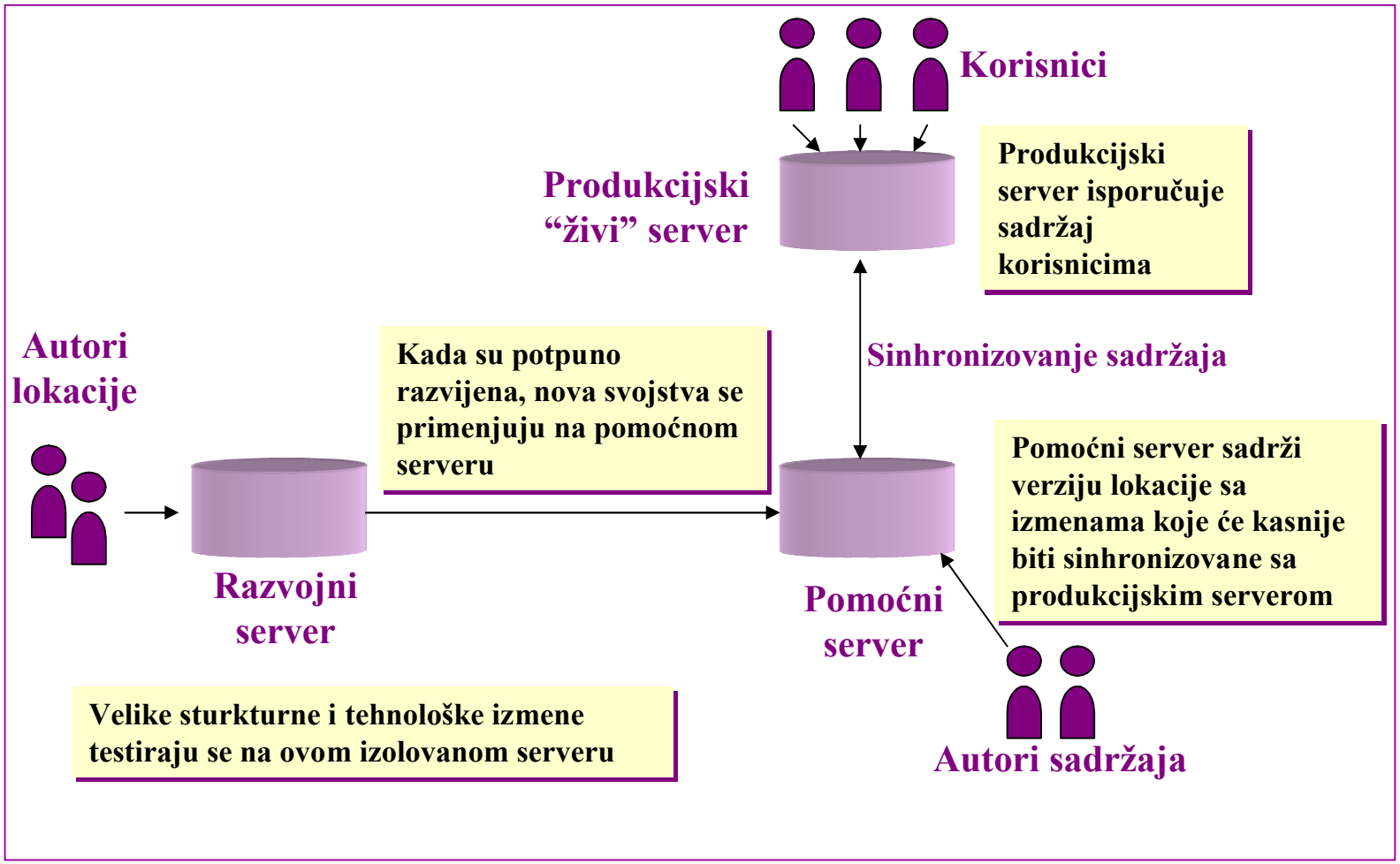
Pravilo imenovanja datoteka:

- Izbegavati upotrebu podvlake u imenima datoteka – upotrebiti crticu ili dve reči spojiti u jednu
- U imenima datoteka ili direktorijuma ne treba koristiti velika slova ili ih mešati sa malim
- Kao nastavak imena datoteke izabrati .html ili .htm, potom je dosledno koristiti
- Mogu se uvesti ograničenja u dužini imena datoteka ili šeme za imenovanje datoteka:
  - Na primer, neke datoteke mogu sadržati datume, recimo saopštenja za javnost – imena datoteka pr021299.htm i pr010500.htm mogu da ukažu na saopštenja za javnost od 02.12.1999. i 01.05.2000.

Uobičajena imena direktorijuma

Ime direktorijuma	Sadržaj
/cgi-bin	Tradicionalna lokacija za smeštanje CGI programa koji se koriste na Web lokaciji
/scripts	Sadrži skriptove koji se koriste na lokaciji. Tu spadaju JavaScript skritpovi, CGI skriptovi, ColdFusion, ASP skriptovi. Neki autori prave zasebne direktorijume za različite tipove skriptova, na primer /js za JavaScript
/styles ili /css	Trebalo bi da sadrži sve spoljašnje kaskadne stilove koji su upotrebljeni na lokaciji
/images	Sadrži sve slike upotrebljene na lokaciji, uključujući GIF, JPEG i PNG datoteke
/video	Sadrži video materijal, uglavnom nestrujeće video zapise.
/audio	Sadrži audio materijal, uglavnom nestrujeće zvučne zapise.
/pdfs	Sadrži dokumentaciju u formatu pdf.
/download ili /binaries	Centralna lokacija za smeštanje programa i drugih binarnih datoteka koje je moguće preuzeti sa lokacije.

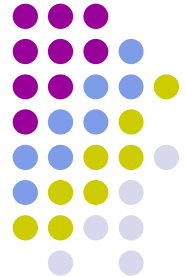
Upravljanje sadržajem – arhitektura tri lokacije



Upravljanje sadržajem

- Pravila:
  - Nikada ne treba raditi direktno na aktivnoj lokaciji – arhitektura tri lokacije
  - Redovno proveravati hiperveze na lokaciji
  - Redovno proveravati detalje na Web stranama – pravopis, pravne napomene i fontove
  - Obezbediti adresu urednik@domen.com na koju će korisnici moći da šalju predloge, postavljaju pitanja i obaveštavaju o uočenim greškama

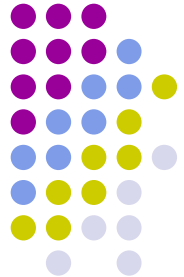
Analiza posećenosti – brojači poseta



- Mnoge lokacije za nadzor posećenosti koriste jednostavne brojače na stranicama
- Osim što broje posete lokaciji – ne mogu se upotrebljavati ni za kakvu drugu svrhu
- Neki korisnici na osnovu brojača odlučuju da li će detaljnije pregledati lokaciju
- Ako brojač ukazuje da je lokaciju posetilo nekoliko korisnika – posetilac će pomisliti da na lokaciji nema ništa zanimljivo i napustiće lokaciju
- Brojač je pod punom kontrolom administratora – može biti uvećan broj poseta
- Većina profesionalnih i ozbiljnih lokacija ne sadrži brojače – korisnici misle da su lokacije sa brojačima amaterske
- PREDLOG:

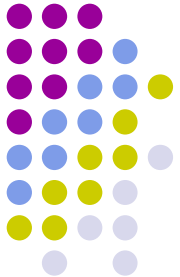
  Ne postavljati na lokaciju vidljiv brojač poseta.

Analiza posećenosti – dnevnici servera



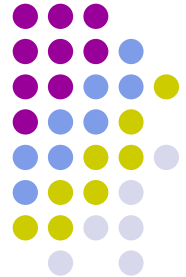
- Dnevnici Web servera sadrže detaljne informacije o tome šta su korisnici tražili na lokaciji
- Analizirajući zapise iz dnevnika može se videti koju stranu je korisnik pročitao, a koju nije – odluka koje će se strane staviti bliže matičnoj strani lokacije, a koje dublje u hijerarhiju
- Sa dnevnikom servera nije teško raditi – ali zahteva malo planiranja
- Dnevnik se mora analizirati veoma pažljivo – postoje specijalizovane organizacije, na primer **HitBox** (www.hitbox.com)
- Dnevnici su vrlo slični

Analiza posećenosti – dnevnici servera



- Web server vodi dva dnevnika:
  - **Dnevnik pristupa**
  - **Dnevnik grešaka**
- Mogu se voditi i dnevnici:
  - **Dnevnik reference** u koji se zapisuju informacije o tome sa koje je lokacije određeni korisnik došao
  - **Dnevnik agenata** – pamti informacije o agentima (najčešće čitačima Weba) koji su upotebljeni za pristupanje lokaciji
- Često se informacije u referencama i upotrebljenim agentima upisuju u dnevnik pristupa lokaciji
- Najčešći format dnevnika i pristupa ima prikladno ime – popularni format dnevnika

Struktura popularnog formata dnevnika



- Host identd authenticated-user [Time of request]
  "request made" result-code bytes-transferred

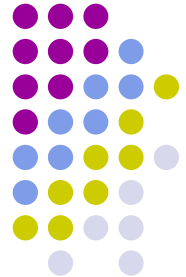
Izvod iz tipičnog dnevnika:

206.251.142.45 – [22/Feb/2007:16:29:09 – 0800]
"GET /badfile.htmHTTP/1.0" 404 222
sj.ix.netcom.com - - [22/Feb/2007:16:29:12 - 0800]
"GET /HTTP/1.,1" 200 7947
sj.ix.netcom.com - - [22/Feb/2007:16:29:13 - 0800]
"GET /images/about.gif HTTP/1.1" 200 506
sj.ix.netcom.com - - [22/Feb/2007:16:29:14 - 0800]
"GET /images/staff.gif HTTP/1.1" 200 580
sj.ix.netcom.com - - [22/Feb/2007:16:29:14 - 0800]
"GET /images/products.gif HTTP/1.1" 200 620
pheoenix.goodnet.com – lsw[22/Feb/2007:16:40:50 - 0800]
"GET /images/whatsnewtop.gif HTTP/1.1" 200 874

Polja dnevnika pristupa

Polje	Opis	Primer
Host	Adresa klijenta koji zahteva objekat. Ovo polje ponekad sadrži samo IP adresu jer ime domena ne može biti razlučeno.	192.102.249.5 Pc1.lažnidomen.com
Identd	Informacija koju vraća identd. Ukoliko nije upotrebljena, u dnevniku stoji crtica.	-
Authenticated user	Ovo polje sadrži korisničko ime poslato za identifikaciju korisnika. Ukoliko nije zadato, u dnevniku će stajati crtica.	- bigboss
Time of request	Ovo polje sadrži datum, kada je objekat zahtevan. On je najčešće u formatu DD/Mon/YYYY:hh:mm:ss-GMT GMT-razlika u odnosu na griničko vreme.	[22/feb/ 2007:13:52:54-08000
Request made	Ovo polje sadrži aktuelni HTTP zahtev koji je klijent prosledio.	"GET/products/books. htmlHTTP/1.0"
Result code	Ovo polje sadrži numerički statusni HTTP kôd koji server vraća i koji ukazuje na uspeh ili neuspeh izvršavanja zahteva.	200 404
Bytes transferred	U ovom polju zapisan je broj bajtova koji su poslati klijentu.	2358

Analiza posećenosti

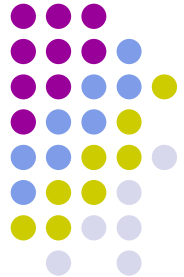


- U dnevnik se zapisuju zahtevi za svim objektima lokacije – oni vrlo brzo postaju veoma veliki
- Datoteke sa dnevnicima treba podeliti na manje celine (po danima, nedeljama ili mesecima) kako bi mogle efikasno da se analiziraju
- Postoje mnogi programi – automatizacija analiziranja dnevnika na primer WebTrends Log Analyzer (www.webtrends.com)

Automatizacija analiziranja dnevnika

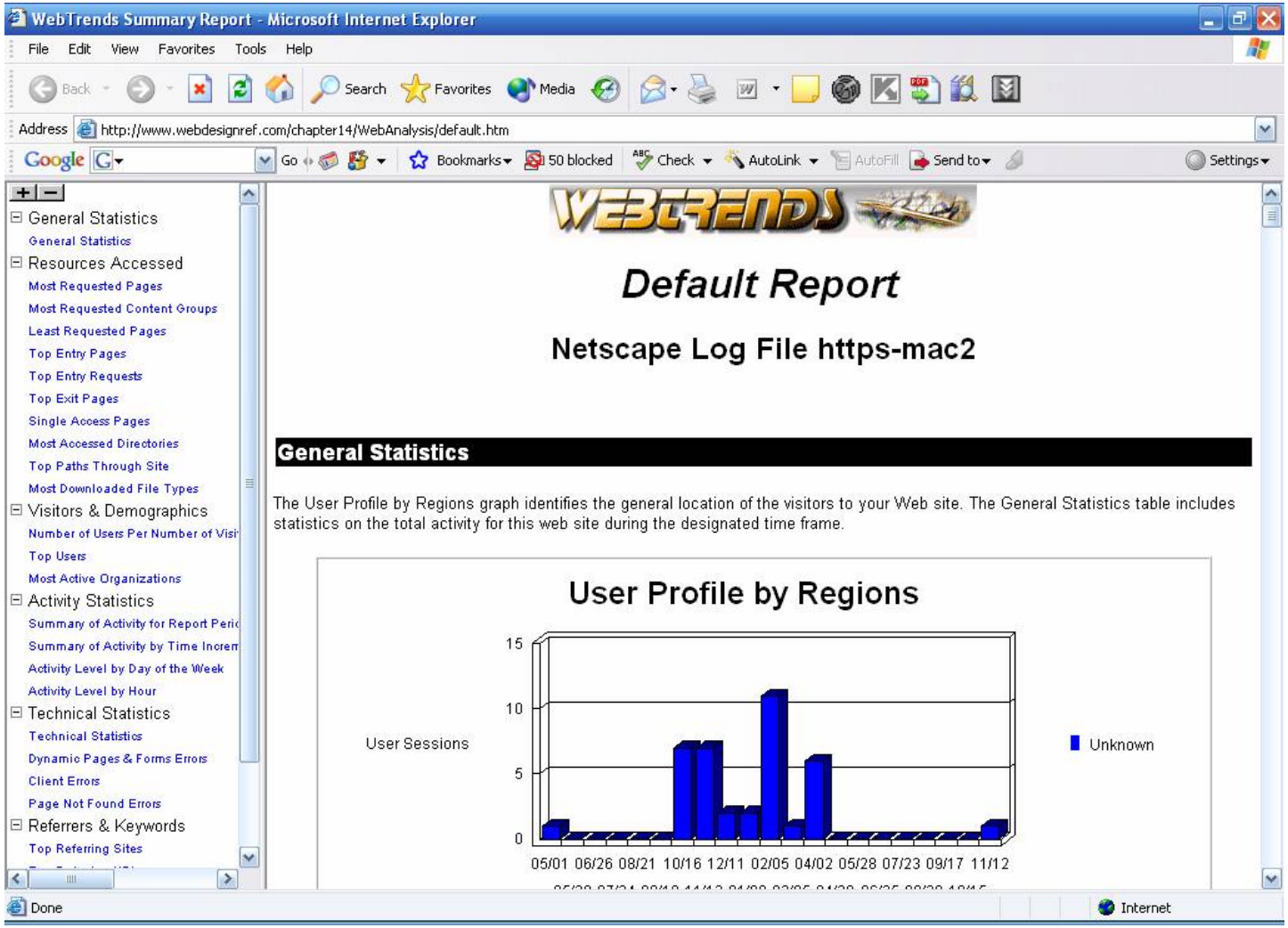
- Jednostavniji programi za analizu samo će pročitati datoteke sa dnevnikom i sačiniti izveštaj
- Lokacije sa više od nekoliko hiljada poseta mesečno – za analiziranje dnevnika koristiti programe koji koriste baze podataka da pomoću njih naprave arhivu dnevnika za duži period
- Arhiva postaje veoma velika
  - Odluka o tome koliko podataka je zaista potrebno čuvati
  - Ukoliko lokaciju posećuje veliki broj posetilaca - jedan računar nameni samo za obradu i analizu dnevnika

Analiza upotrebe lokacije



- Poslednja svrha snimanja dnevnika – njihova obrada i izrada izveštaja o upotrebljavanju lokacije
- Programi za statističku analizu generišu izveštaje koji ilustruju različite aspekte upotrebe lokacije
- Pažljivo analizirati dnevnike servera i dobijene podatke upotrebiti da se poboljša lokacija ili proceni njena efikasnost
- Ekonomska efikasnost lokacije – analiza dnevnika iz dužeg vremenskog perioda
  - Lokacija za prodaju preko Interneta – analizirati troškove poseta i prodaja – isporuka lokacije nije besplatna – dobro poznavati troškove svake posete lokaciji

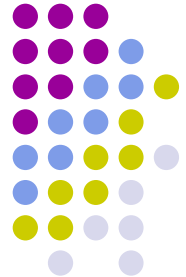
Primer izveštaja o upotrebi lokacije



Uobičajeni poslovi pri analizi dnevnih servera

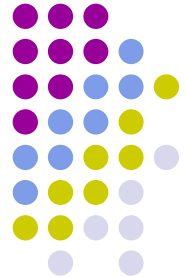
- Pregled tačaka ulaza
- Pregled tačaka izlaza
- Pronalaženje staza kojima se korisnici najčešće kreću
- Određivanje tačnog trajanja prosečne posete lokaciji
- Otkrivanje korisnika i domena sa kojih korisnici najčešće posećuju lokaciju
- Utvrđivanje da li su uobičajene jednokratne ili višekratne posete
- Uočavanje dnevne šeme poseta
- Uočavanje šema vezanih za geografiju i jezike
- Uočavanje čitača koji se najčešće koriste
- Uočavanje lokacije sa referencama
- Otkrivanje ključnih reči na pretraživačima Interneta
- Pregled dnevnika grešaka, otkrivanje greške 404

Problem sadržaja lokacije



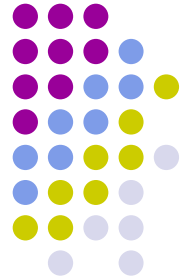
- Odluka o tome koji sadržaj je prihvatljiv za postavljanje na Internet
- Filtriranje lokacija – tehnologija koja se najčešće koristi poseban program za filtriranje proverava ocenu sadržaja lokacije pre nego što dozvoli da ona bude učitana
  - ako je zahtevani sadržaj prihvatljiv biće prikazan korisniku u suprotnom
  - sadržaj neće biti prikazan
- Sa aspekta isporuke lokacije – ključni problem vezan za prihvatljivost sadržaja je adekvatno obeležavanje neprikladnog sadržaja i izbegavanje situacija u kojima je prihvatljiv sadržaj označen kao neprihvatljiv i filtriran

Problem sadržaja lokacije



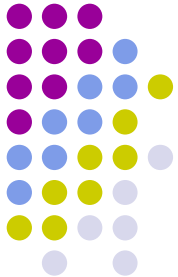
- Konzorcijum W3C predložio je platformu za izbor sadržaja na Internetu, **PICS** (http://www.w3.org/pub/WWW/PICS/) kao rešenje za filtriranje sadržaja na Webu
  - Ocenjena lokacija sadržaće određeni element `<meta>` u zaglavlju HTML dokumenta – taj elemenat sadržaće ocenu prihvatljivosti lokacije
  - Sadržaj lokacije ocenjuje služba za ocenjivanje sadržaja – grupa, organizacija ili kompanija
  - U službe za ocenjivanje sadržaja spadaju i nezavisne, neprofitne grupe, poput organizacije *Recreational Software Advisory Council (RSAC)* koja već ocenjuje prihvatljivost kompjuterskih igara
  - Ocena mora biti zasnovana na dobro definisanom skupu pravila koji opisuje
    - kriterijum za ocenjivanje,
    - skalu vrednosti za svaki aspekt ocenjivanja i
    - opis kriterijuma koji je upotrebljen za donošenje ocene

Problem sadržaja lokacije



- Dodeljivanje ocene prikladnosti dokumentu ili lokaciji – u zaglavlje HTML datoteke dodaje se oznaka `<meta>`
- Ona mora da sadrži:
  - URL adresu organizacije koja je dodelila ocenu
  - Informacije o sistemu ocenjivanja (verzija, podnosilac i datum donošenja)
  - Samu ocenu
- Da bi se generisala RSAC i PICS ocena, potrebno je samo popuniti obrazac i odgovoriti na nekoliko pitanja o sadržaju lokacije
- Nakon što se popuni i priloži upitnik, organizacija podnosiocu zahteva šalje Web stranu ili elektronsku poruku sa sadržajem oznake `<meta>` koji treba dodati u zaglavlje HTML dokumenta

Primer PICS ocene u obliku oznake <meta>

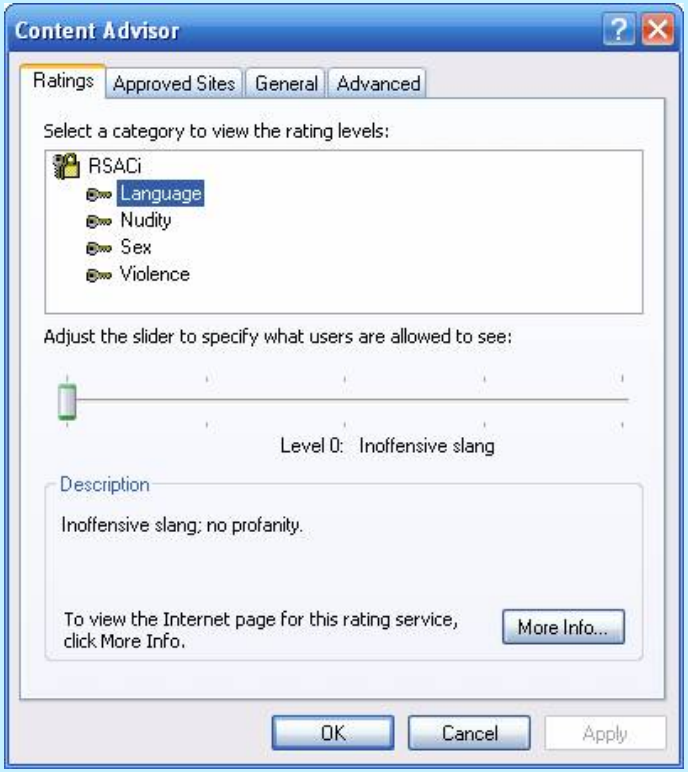


```
<metahttp-equiv="PICS-Label"
Content=' (PICS-1.1" http://www.rsac.org/ratingsv01.html
l gen true comment "RSACi North America Server" for
http://www.democompany.com on "2000.01.31T03:52-0800" r
(n 0 s 0 v 0 l 0))'>
```

- Po sistemu ocenjivanja RSACi informacije se ocenjuju od 0 do 4,
- Ocena 0 daje se bezazlenim sadržajima, dok ocenu 4 zaslužuju najekstremniji slučajevi
- Dok filtrira lokaciju, program za filtriranje čita ocenu i na osnovu nje odlučuje da li će sadržaj biti prikazan ili ne

Problem sadržaja lokacije

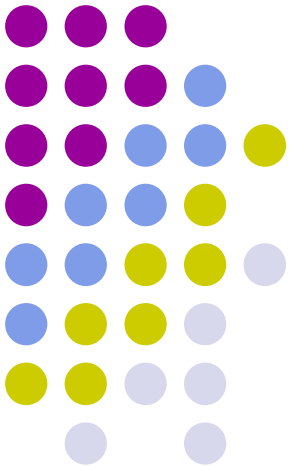
- Tehnologije filtriranja postaju sve popularnije – Internet Explorer sadrži ugrađen filtar koji radi sa platformom PICS



Zaključak

- Brza isporuka lokacije veoma je važna – korisnikov opšti utisak o lokaciji zavisi od toga koliko ona brzo reaguje
- Kada se lokacija optimizuje – uzeti u obzir sve aspekte isporuke – protokole, servere i mreže
- Pri projektovanju Web servera, najpre proceniti potrebe lokacije – na osnovu njih izabrati: hardver, operativni sistem i Web server
- Ozbiljno razmotriti i mogućnosti smeštanja lokacije na server – najbolje rešenje je neki vid ugošćavanja
- Nakon završetka lokacije – pažljivo nadgledanje – održavanje lokacije ne odnosi se samo na održavanje hardvera i softvera servera, već i na sadržaj lokacije

Bezbednost Web aplikacija

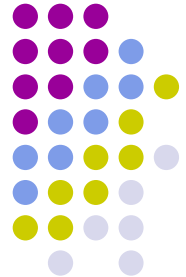


Bezbednosne mere u komunikaciji

- Računarska konkurencija, osnažila je, s jedne strane, poslovnu konkurenciju, ali isto tako s druge strane doprinela razvoju kriminala koji novim, moćnim sredstvima nastoji da izvrši razne pronevere i gubitke sredstava.

- Iz tih razloga bezbednosne mere u komunikaciji putem računarske tehnologije dobijaju na značaju kako u poslovnom tako i u privatnom sektoru.

Osnovni ciljevi mera bezbednosti



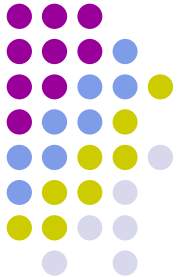
- Osnovni ciljevi mera bezbednosti u sistemima su:
  - **Poverljivost** – obezbeđuje nedostupnost informacija neovlašćenim licima.
  - **Integritet** – obezbeđuje konzistentnost podataka, sprečavajući neovlašćeno generisanje, promenu i uništenje podataka.
  - **Dostupnost** – obezbeđuje da ovlašćeni korisnici uvek mogu da koriste servise i da pristupe informacijama.
  - **Upotreba sistema isključivo od strane ovlašćenih korisnika** – obezbeđuje da se resursi sistema ne mogu koristiti od strane neovlašćenih osoba niti na neovlašćen način.

Opasnosti od hakera

Nakon što je lokacija postavljena i pokrenuta, hakeri mogu da je napadnu na različite načine:

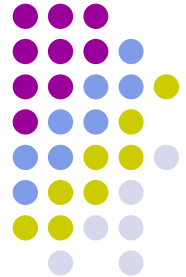
- **Presretanjem, pregledanjem i verovatno menjanjem HTTP poruka** koje server razmenjuje sa čitačima korisnika
- **Pristupanjem datotekama koje se nalaze na serveru** i koje mogu da sadrže osetljive informacije kao što su podaci o kreditnim karticama korisnika
- **Pokretanjem hiljade zahteva serveru** koji troši resurse lokacije i posetiocima sprečavaju pristup lokaciji
- **Inficiranjem računarskim virusom datoteka**, diskova ili elektronskih poruka koje dolaze na lokaciju
- **Zaustavljanjem skriptova** zasnovanih na CGI-u da ne bi pristupili serveru

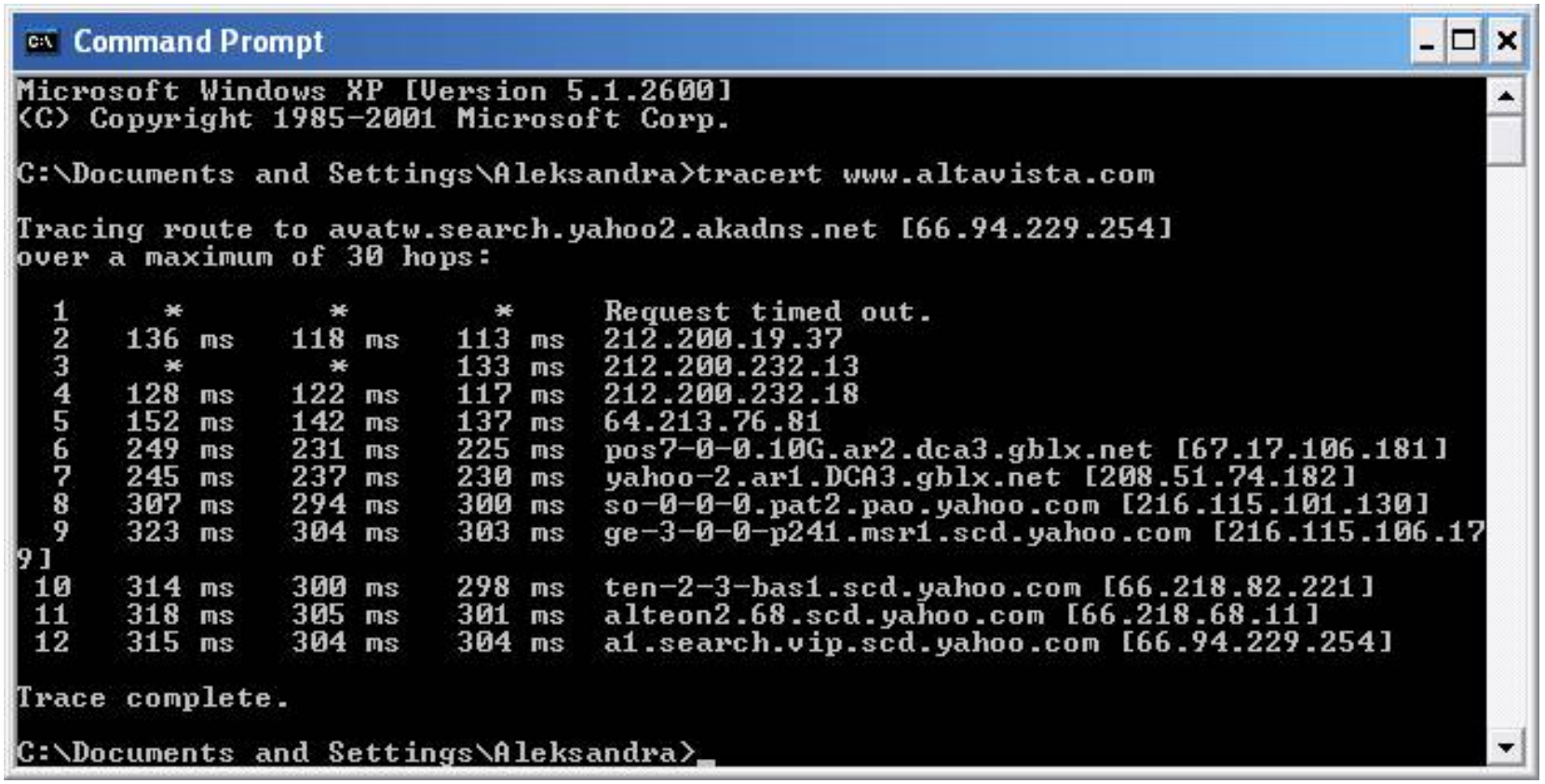
Presretanje mrežnih poruka



- Kada programi šalju informacije udaljenim računarima preko Interneta, poruke ne putuju direktno od računara koji ih šalje do primaoca poruke
- Poruka prolazi kroz veliki broj lokacija na mreži
- Zadavanjem komande **tracert** (*trace route* – praćenje putanje) – dobija se spisak lokacija kroz koje poruka putuje do udaljene lokacije
- Sledeći listing ilustruje putanju kojom je putovala poruka od autorovog računara do lokacije **yahoo.com**

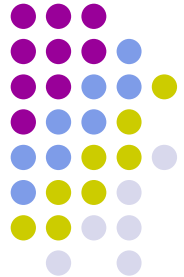
Spisak lokacija kroz koje poruka putuje do udaljene lokacije





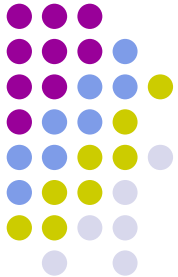
Poruka putuje kroz mnogo lokacija dok se kreće preko Mreže

Presretanje mrežnih poruka



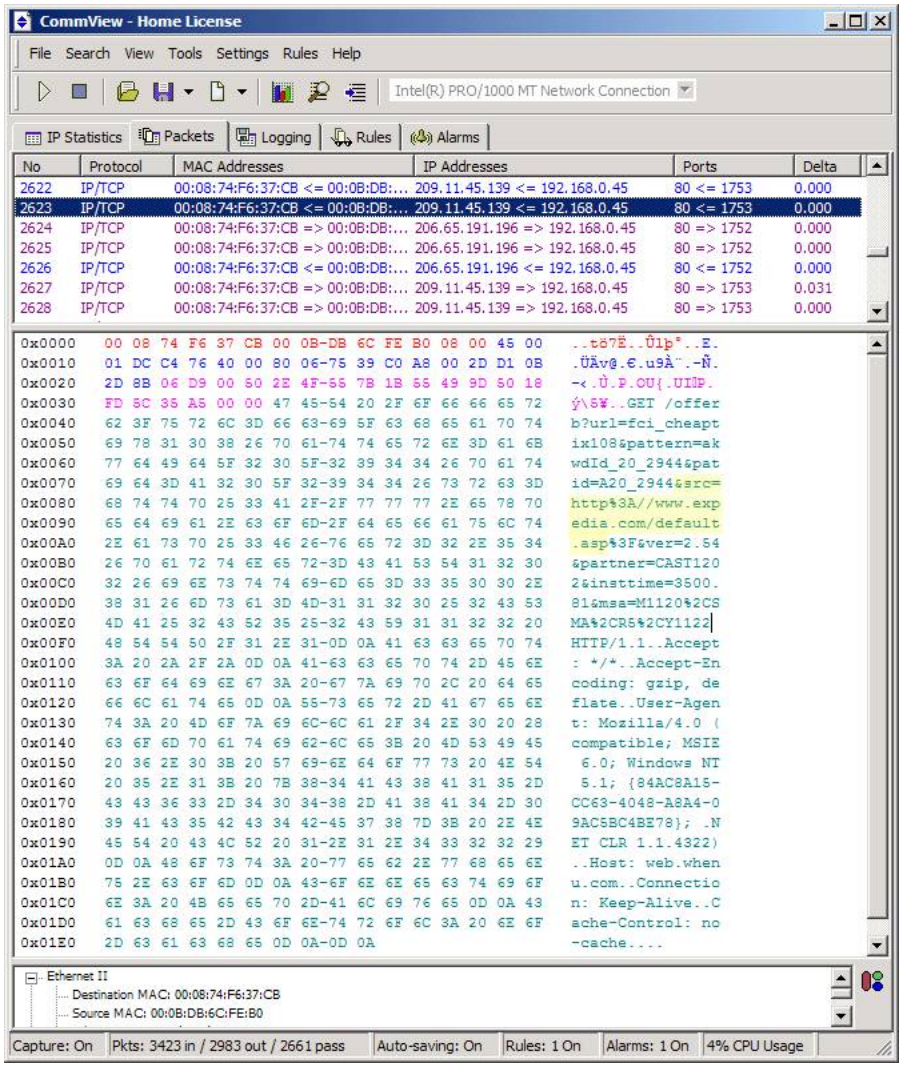
- Haker kroz čiji sistem poruka prolazi tokom putovanja može da pročita i izmeni sadržaj poruke u bilo kom trenutku tokom putovanja poruke
- Pretpostavimo da poruka sadrži informacije o kreditnim karticama
- Dok poruka prolazi kroz hakerov sistem, on može da čita i snima podatke o kreditnim karticama

Korišćenje programa CommView za pregledanje HTTP poruka

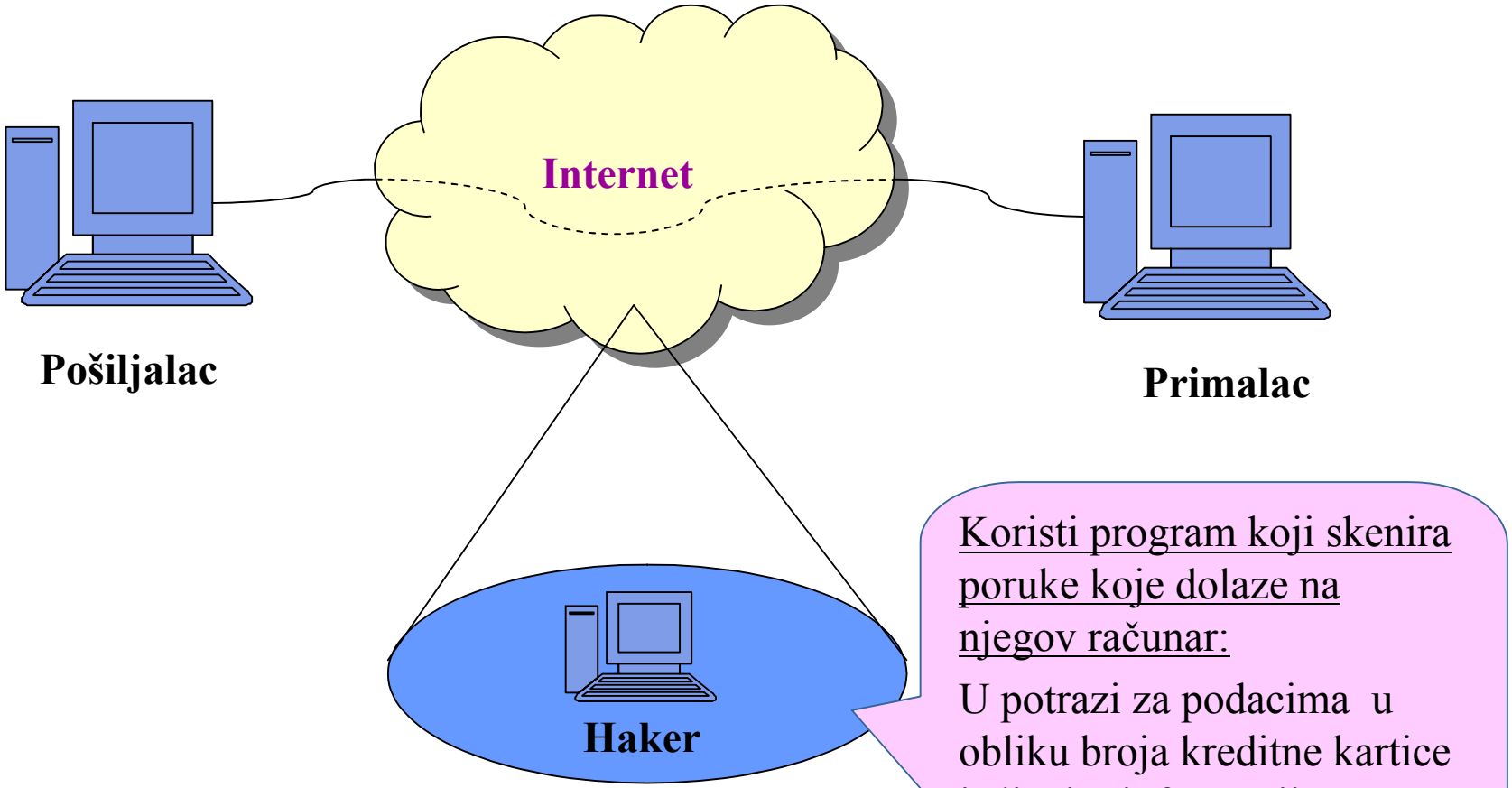


- Kada korisnik pošalje sadržaj obrasca “iza scene” čitač šalje podatke iz obrasca serveru korišćenjem protokola HTTP
- HTTP prosleđuje poruke kao običan tekst. Što znači da haker veoma lako može da pregleda sadržaj poruke
- Korišćenjem programa **CommView** može se pregledati sadržaj velikog broja tipova poruka koje uđu u sistem
- Haker može da koristi program sličan CommView da bi nadgledao poruke koje dolaze na njegov računar

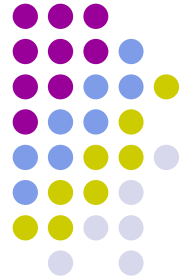
Korišćenje programa CommView za pregledanje HTTP poruka



Hakeri preuzimaju osetljive informacije iz poruka koje presreću

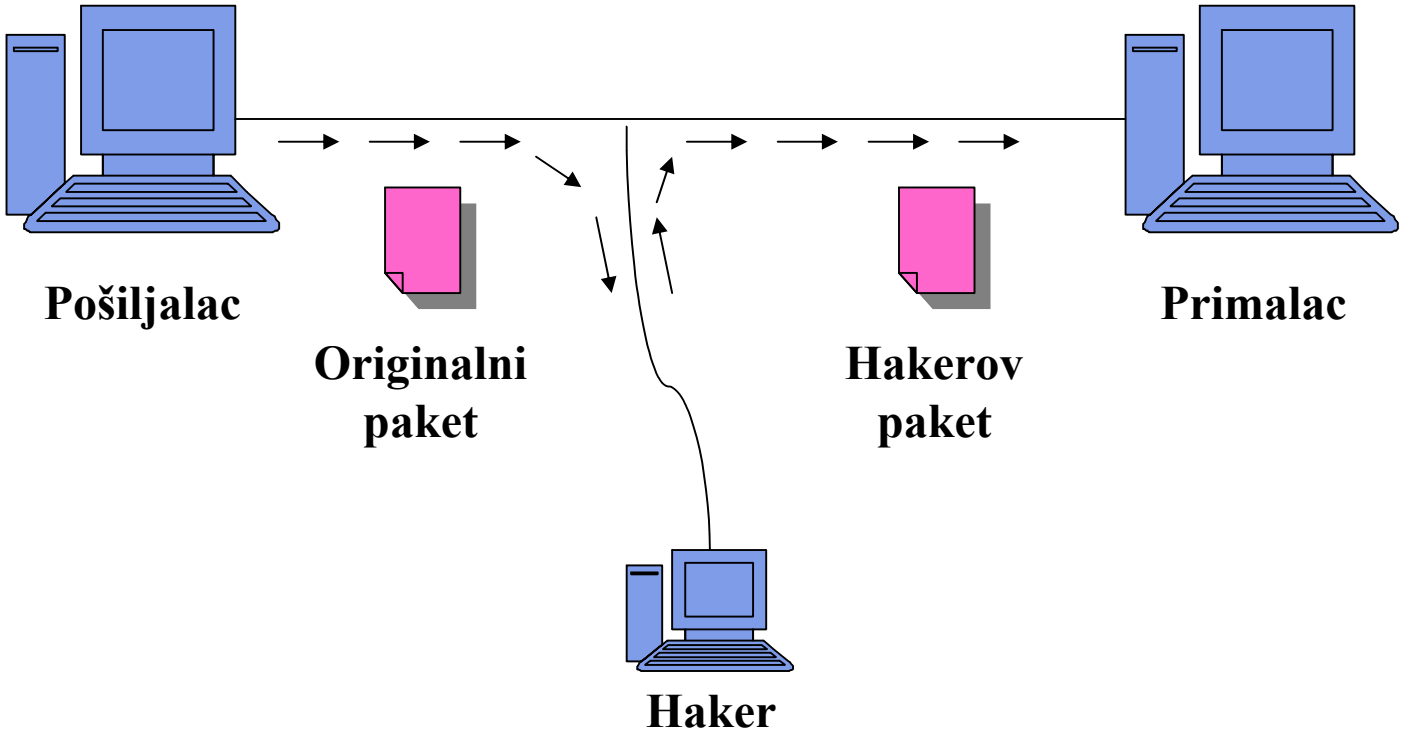


Hakeri preuzimaju osetljive informacije iz poruka koje presreću

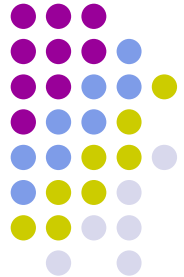


- Pored toga što presreće poruke, haker može i da im menja sadržaj
- Pretpostavimo da haker presretne poruku koja sadrži narudžbinu za kupovinu
- On može promeniti količinu robe i adresu prispeća, tako da će roba stići njemu umesto stvarnom poručiocu
- Zaštita poruka sa lokacije od ovakvih opasnosti, može se realizovati šifrovanjem i bezbednim Web stranicama

Hakeri preuzimaju osetljive informacije iz poruka koje presreću

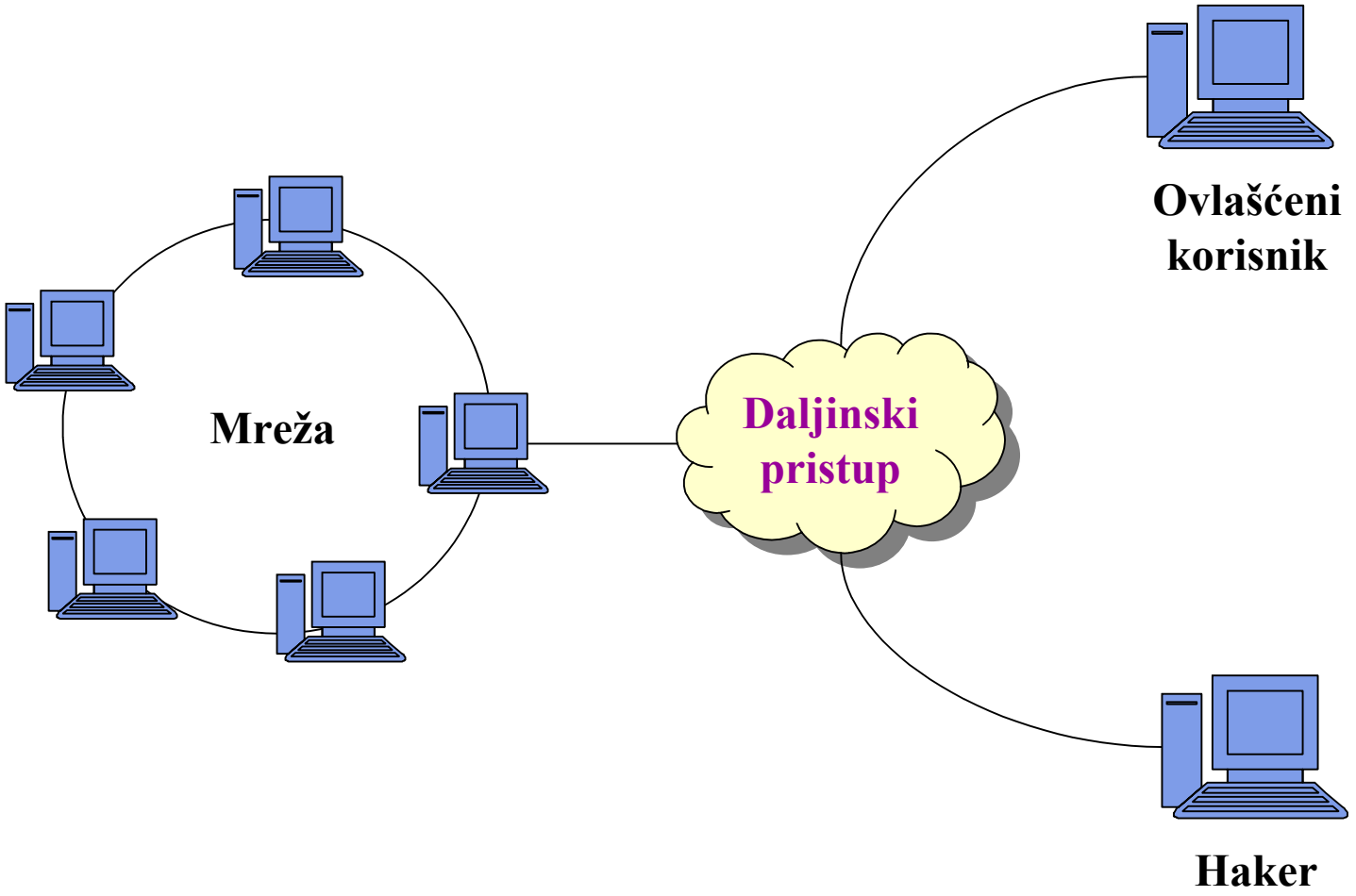


Kako hakeri “provaljuju” sistem

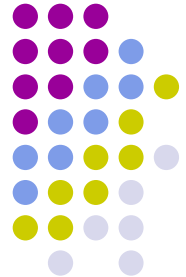


- Mnogi sistemi omogućavaju korisnicima da se preko Interneta prijave na mrežu sa udaljenih mesta
- Kompanija može, na primer, omogućiti svojim trgovačkim putnicima da se prijave na mrežu kompanije, tako da mogu pregledati, formirati ili ažurirati informacije u narudžbini ili pristupiti elektronskoj pošti
- Sistem može omogućiti programerima, Web dizajnerima i drugim korisnicima da se povežu sa udaljenih mesta kako bi poslali ili preuzeli datoteke
- Kada je sistem osposobljen za daljinski pristup, hakeri mogu da zloupotrebe programe i usluge za daljinski pristup da bi provalili u mrežu

Kako hakeri “provaljuju” sistem

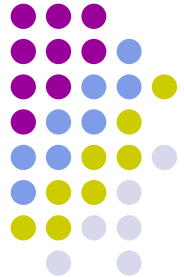


Kako hakeri “provaljuju” u sistem



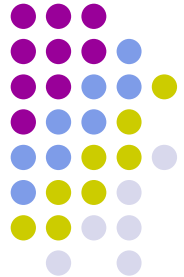
- Da bi provalio u mrežu koja koristi daljinski pristup, haker obično mora da zada važeće korisničko ime i lozinku
- Haker pristupa važećim korisničkim imenima i lozinkama pomoću velikog broja tehnika:
  - Koristi program za razbijanje lozinke koji napada datoteku lozinki sistema
  - Cilja na opšte podrazumevane naloge za koje mrežni administratori nisu promenili lozinke
  - Pita korisnika s važećim nalogom koje mu je korisničko ime i lozinka

Softver za razbijanje lozinke



- Godinama ranije, hakeri su koristili posebne programe pod nazivom razbijači lozinke koji su uzastopno unosili kombinacije korisničkog imena i lozinke
- Korišćenjem razbijača lozinke, haker je za minut mogao da isproba hiljade različitih kombinacija korisničko ime/lozinka
- Danas operativni sistemi blokiraju nalog ako korisnik ne unese ispravan par korisničko ime/lozinka u zadatom broju pokušaja
- Većina operativnih sistema smešta informacije o korisničkim nalozima u datoteku
  - Da bi sprečili neovlašćene korisnike da pregledaju informacije o lozinkama ta datoteka je obično šifrovana – međutim na Webu postoje programi koji dešifruju lozinke – najbolje će se zaštiti datoteke kad se zaštite nalozi administratora

Zaštita podrazumevanih naloga



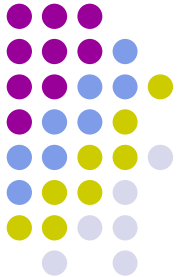
- Kada se prvi put instalira operativni sistem ili velika aplikacija, softver obično obezbeđuje nekoliko podrazumevanih naloga koji se mogu koristiti da bi se obavila instalacija, proverili parametri sistema i slično
- Mnogi korisnici ne isključuju ove podrazumevane naloge nakon instaliranja aplikacije
- Mnogi hakeri provaljuju u sistem preko Interneta korišćenjem podrazumevanih naloga koji nisu isključeni
- Obavezno promeniti lozinke za sve podrazumevane naloge i, još efikasnije, onemogućiti korišćenje nepotrebnih podrazumevanih naloga
- Bezbednost lokacije, često se može poboljšati vremenskim ograničavanjem mnogih korisničkih naloga na pristup samo tokom radnih sati

Kako hakeri onemogućavaju pristup sistemu

- Kada haker ne može da provali u sistem on može da spreči druge, izvođenjem sabotaža koje troše resurse sistema, ili delimično (usporava lokaciju) ili potpuno (sprečava pristup posetiocima)
- Pre nekoliko godina, hakeri su oborili server za elektronsku poštu Bele kuće bombardovanjem elektronske adrese desetinama hiljada velikih elektronskih poruka – iako sami hakeri nisu mogli da provale na lokaciju Bele kuće onemogućili su druge da koriste usluge lokacije
- Sledeća HTML datoteka koristi oznaku <meta> da bi usmerila čitač da preuzima veliku grafičku datoteku sa lokacije www.SomeVictim.com svakih 30 sekundi

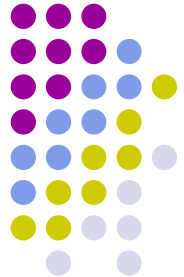
```
<html>
<meta http-equiv="Refresh" content="30" />
<img
src=http://www.SomeVictim.com/LargeImageFile.jpg  />
</html>
```

Kako hakeri onemogućavaju pristup sistemu



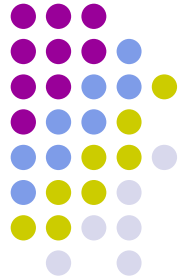
- Onemogućavanjem keširanja, HTML datoteka primorava Web server da šalje sadržaj zahtevane Web stranice svakih 30 sekundi
- Dok server odgovara na ovaj zahtev, on ne može da usluži druge
- Haker može, na primer, otvoriti 10 ili više prozora čitača u kojima učitava stranicu
- Što je veći broj prozora u kojima haker otvara ovu jednostavnu datoteku, sve više se smanjuje mogućnost servera da usluži druge
- Da bi se zaštitila lokacija od ovakve vrste napada može se koristiti barijera (firewall) koja prati ponavljajuće HTTP zahteve ili slične ponovljene zahteve
- Pored toga može se pregledati datoteka evidencije lokacije

Kako hakeri napadaju CGI skriptove



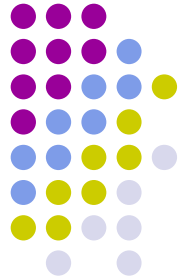
- Godinama su hakeri ciljali CGI skriptove da bi provalili na Web lokacije
- Zato što skript programi koji se izvršavaju na Web serveru mogu da pristupe podacima smeštenim na disku servera
- Zavisno od obrade koju obavljaju skriptovi, haker može da (zlo)upotrebi skript tako što ga izvrši koristeći vrednosti koje mu dodeljuje izvan procesa slanja obrasca
- Ako haker može da pristupi hard disku Web servera, može da zameni skript datoteku vlastitom
- Zavisno od obrade koju obavlja hakerov novi skript, moglo bi da prođe dosta vremena dok administratori lokacije ne otkriju promenu

Napadi preopterećenjem bafera



- Preopterećenje bafera se pojavljuje kada korisnik (koji ne mora da bude haker) pošalje više podataka nego što skript može da smesti
  - Na primer, korisnik u polje za unos teksta unese više karaktera nego što je predviđeno
- Problem sa greškama preopterećenja bafera leži u tome što neki skript jezici izazivaju kvar skript procesora
- Zavisno od operativnog sistema koji se izvršava na serveru, takve greške mogu hakeru omogućiti pristup serveru i datotekama koje sadrži
- Da bi zloupotrebio grešku preopterećenja bafera, haker prvo izaziva kvar skript procesora – kada pristupi serveru, haker može da kopira ili briše datoteke ili pokreće druge programe koji se nalaze na serveru

Kako hakeri napadaju CGI skriptove

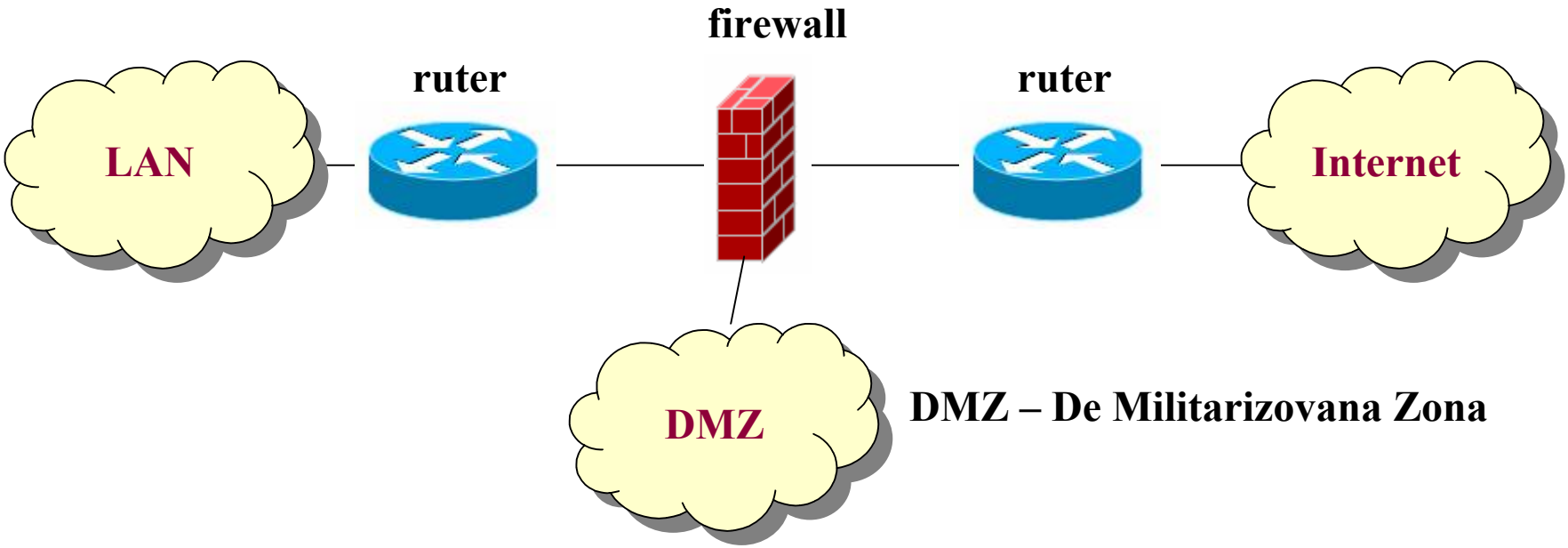


- Tokom godina, programeri operativnih sistema, programeri skript procesora i programeri koji prave Web skriptove, postali su svesni rizika od greške preopterećenja bafera
- Mnoge novije aplikacije ne kvare se nakon greške preopterećenja bafera tako da haker ne može da preuzme kontrolu nad serverom
- Na Web lokaciji CERT-a na http://www.cert.org postoji pregled aplikacija koje su ranjive preopterećenjem bafera, kao i slabosti drugog softvera, poput PHP, ActiveX, ASP i sl.

Kako barijere (firewall) štite lokaciju

- Da bi zaštitili mrežu od napada hakera, mnogi administratori mreže stavljaju barijeru između Interneta i mreže
- Barijera filtrira mrežne poruke koje dolaze sa Interneta u mrežu – mrežne poruke su podaci koje programi kao što su čitači Weba i programi za ćaskanje šalju sa jednog računara na drugi
- Barijera može da bude posebna hardverska kutija ili računar na kojem je pokrenut odgovarajući softver
- Barijera dozvoljava samo HTTP porukama poslatim sa udaljenog čitača da uđu u mrežu, a sprečava poruke iz aplikacija kao što su programi za ćaskanje ili programi za prenos datoteka (kao što je FTP) da uđu u mrežu

Korišćenje firewall-a za zaštitu (tipska šema)



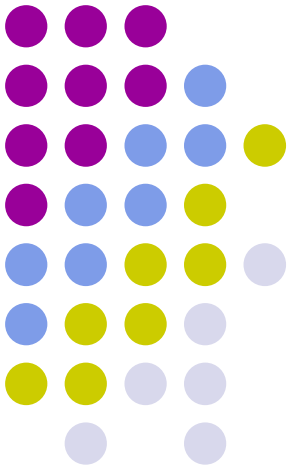
Po pravilu, *firewall* se realizuje kao uređaj sa dva ili više *ethernet* interfejsa. U zavisnosti od načina realizacije može da bude:

- **Softverski** – softver koji se instalira na računar opšte namene
- **Hardverski** – namenski razvijen računar sa odgovarajućim softverom
- **Integrisan sa ruterom**

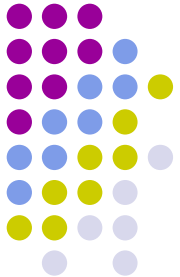
DMZ

- U DMZ se smeštaju serveri koji treba da budu vidljivi i sa Interneta i iz lokalne mreže
- U slučaju postojanja DMZ-a, firewall najčešće ne dozvoljava direktnu komunikaciju LAN <-> Internet već isključivo kroz DMZ
- U slučaju kompromitovanja nekog od servera u DMZ-u to ne znači da je automatski cela mreža kompromitovana

KRIPTOGRAFSKE TEHNOLOGIJE

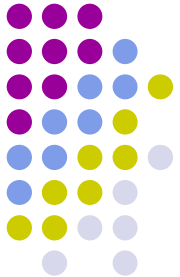


Kako šifrovanje štiti poruke koje se šalju preko mreže



- Nemoguće je sprečiti hakere da presreću poruke koje prolaze kroz njihov računar
- Međutim, šifrovanjem poruka koje se šalju sprečava se haker da pregleda informacije u njima i da ih značajno izmeni
- Da bi izmenjivali šifrovane poruke, dva programa, kao što su programi čitača i servera, moraju prvo da usvoje zajednički algoritam koji će koristiti da bi šifrovali poruke
- Na primer – šifrovanje podataka povećanjem ili smanjenjem slova za jedno – ABC šifruje se kao BCD pomeranjem unapred svakog slova za jedno mesto
- Nakon što čitač i server urtvrde koju metodu će koristiti moraju da se slože o broju mesta za koje će se znakovi pomerati – broj oko kojeg se slože – ključ za šifru

Kako šifrovanje štiti poruke koje se šalju preko mreže



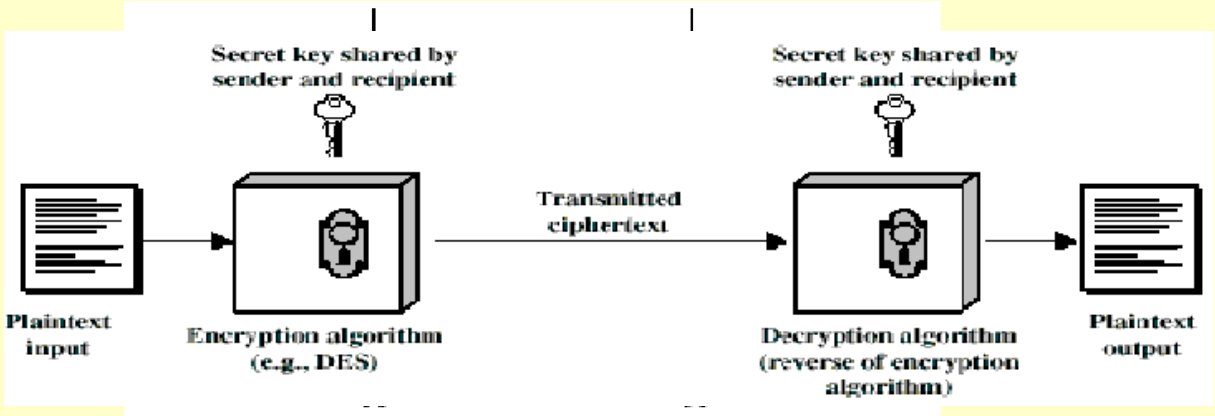
- Algoritmi šifrovanja na Webu uključuju više od jednostavnog pomeranja slova unapred ili unazad
- Postupak koji programi koriste da bi utvrdili algoritam i izabrali ključ sličan je ovom
- Kada čitač Weba pokrene bezbedan prenos na Webu prvo šalje serveru spisak algoritama šifrovanja koje podržava
- Server pregleda spisak i bira algoritam koji podržavaju i on i čitač i potom čitaču šalje poruku koja zadaje izabrani algoritam
- Pre nego što dva programa mogu da koriste algoritme za šifrovanje poruka, oni moraju da se slože oko ključa za šifru

Kriptografske mere bezbednosti

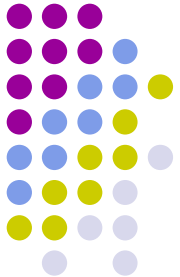
- Svaki šifarski sistem obuhvata par transformacija podataka, koje se nazivaju šifrovanje i dešifrovanje.
- **Kriptovanje (šifrovanje)** je procedura koja transformiše originalnu informaciju (otvoreni tekst) u šifrovane podatke (šifrat).
- Inverzna operacija, **dekriptovanje (dešifrovanje)**, rekonstruiše otvoreni tekst na osnovu šifrata.
- Kriptovanje i dekriptovanje koriste određeni vid tajne informacije, poznate pod nazivom **ključ** (*eng. Key*).

Kriptografske mere bezbednosti

- Šema šifrovanja ima 5 komponenti:
  1. Tekst koji se šifruje (plaintext)
  2. Algoritam šifrovanja
  3. Tajni ključ
  4. Šifrovani tekst (ciphertext)
  5. Algoritam dešifrovanja

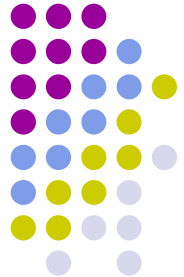


Kriptografske mere bezbednosti



- Šifrovanje je, pojednostavljeno, matematičkom funkcijom čiji izlaz zavisi od dva ulazna parametra :
  - originalna poruka koja se šifrira P (Plaintext)
  - ključ K
- Rezultat je niz naizgled nepovezanih brojeva koji se mogu, bez straha od mogućnosti da poruka dođe u neželjene ruke, prenositi do osobe kojoj je namenjena.
- Da bi šifrovanu poruku druga osoba mogla da koristi potrebno je sprovesti obrnuti postupak od šifrovanja, dešifrovanje.

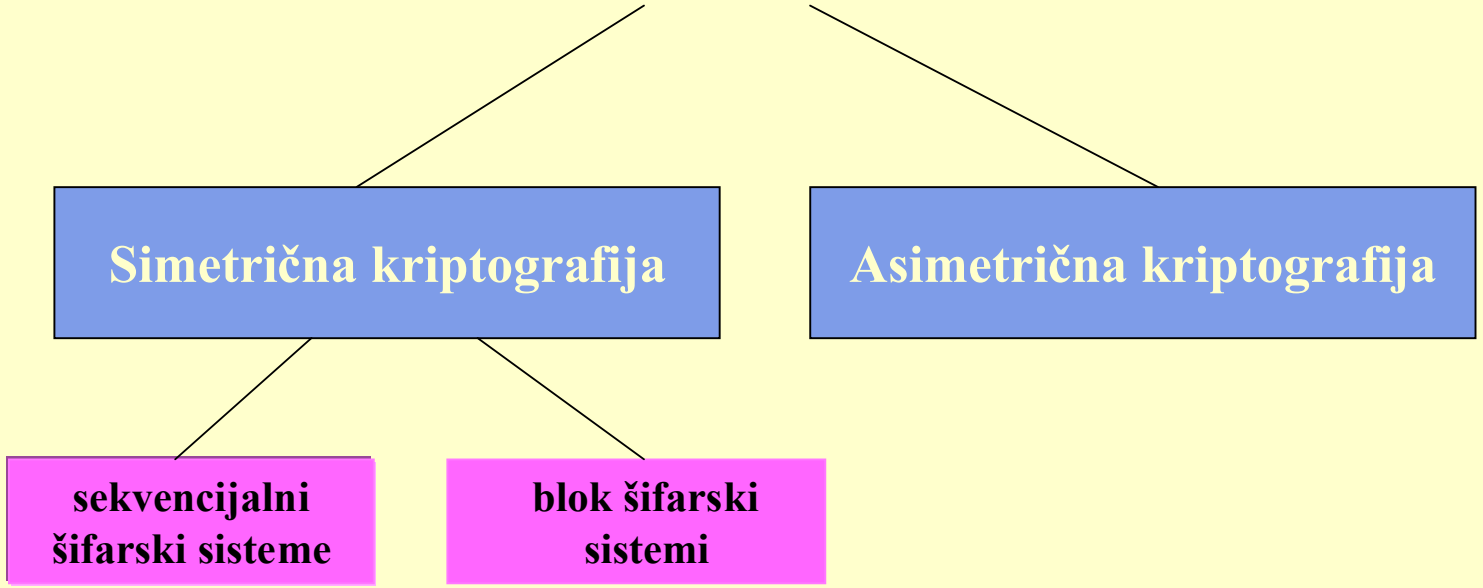
Kriptografske mere bezbednosti



- Dešifrovanje je pojednostavljeno matematičkom funkcijom čiji izlaz zavisi od dva ulazna parametra:
  1. šifrovana poruka C (Chipertext)
  2. ključ K^{-I}
- kao rezultat funkcije dobija se originalna poruka
- Minimalna i potrebna informacija koju dve osobe moraju da dele, ako žele da razmenjuju podatke na siguran način, skup ključeva (K, K^{-I})
- Prema odnosu ključeva K i K^{-I} kriptografske sisteme delimo na simetrične i asimetrične.

Vrste kriptografskih mehanizama

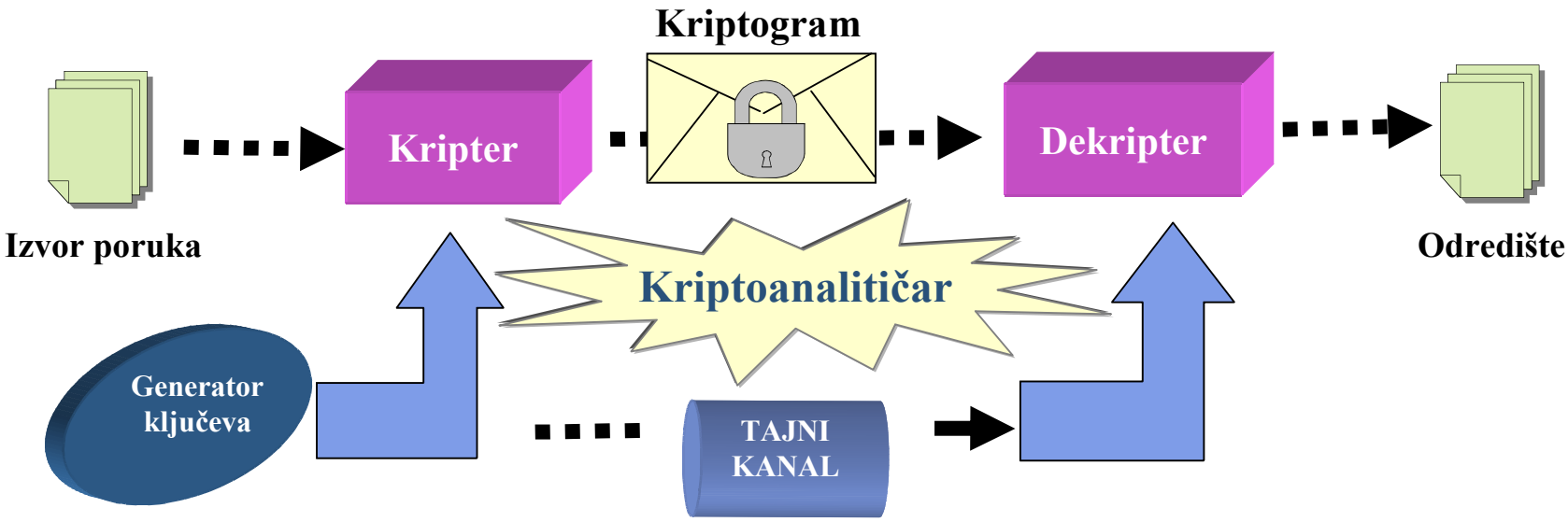
- Postoje dve osnovne vrste kriptografskih mehanizama:



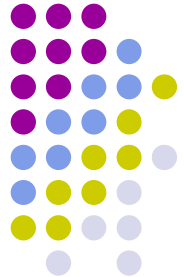
Simetrična kriptografija

- **Simetrična kriptografija** ili **kriptografija sa tajnim ključem** - tradicionalni oblik kriptografije u kom se isti ključ koristi kako za kriptovanje tako i za dekriptovanje. $K = K^{-I}$
- Kriptografski algoritam vrši obradu originalne poruke, koja se naziva **kriptogram** (*eng. ciphertext*), kojom se ostvaruje prvi cilj kriptografije.
- Kako oba korespodenta koriste identične ključeve potrebno je na odgovarajući način razmeniti ključ - uveden je pojam tajnog kanala kojim se ključ razmenjuje.
- Egzistencija tajnog kanala je najslabije mesto simetričnog kriptografskog sistema.

Simetričan kriptografski sistem

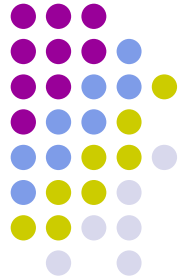


Simetrična kriptografija



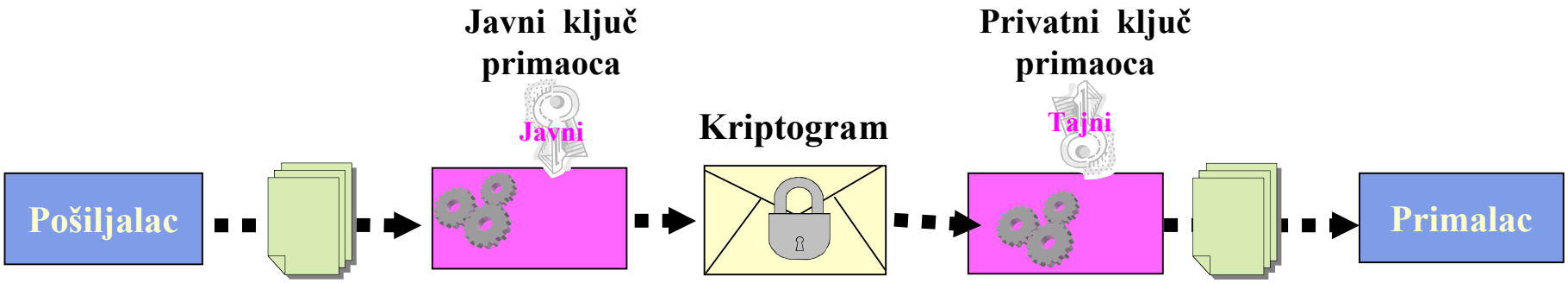
- U klasičnoj kriptografiji oba korespodenta znaju i koriste isti tajni ključ.
- Svako ko zna tajni ključ može da ga upotrebi kasnije za čitanje, modifikaciju i zloupotrebu svih poruka koje su kriptovane ili autorizovane pomoću tajnog ključa:
- Generisanje, prenos i skladištenje ključeva zove se **upravljanje ključem** (*eng. key managment*).
- Kriptografija sa tajnim ključem ima očit problem u obezbeđivanju tajnosti u upravljanju ključem, naročito u otvorenim sistemima sa velikim brojem učesnika.
- Prednost simetrične kriptografije leži u praktičnoj realizaciji gde se ovaj metod pokazuje kao vrlo brz, jer nema velikih zahteva u računanju.

Asimetrična kriptografija

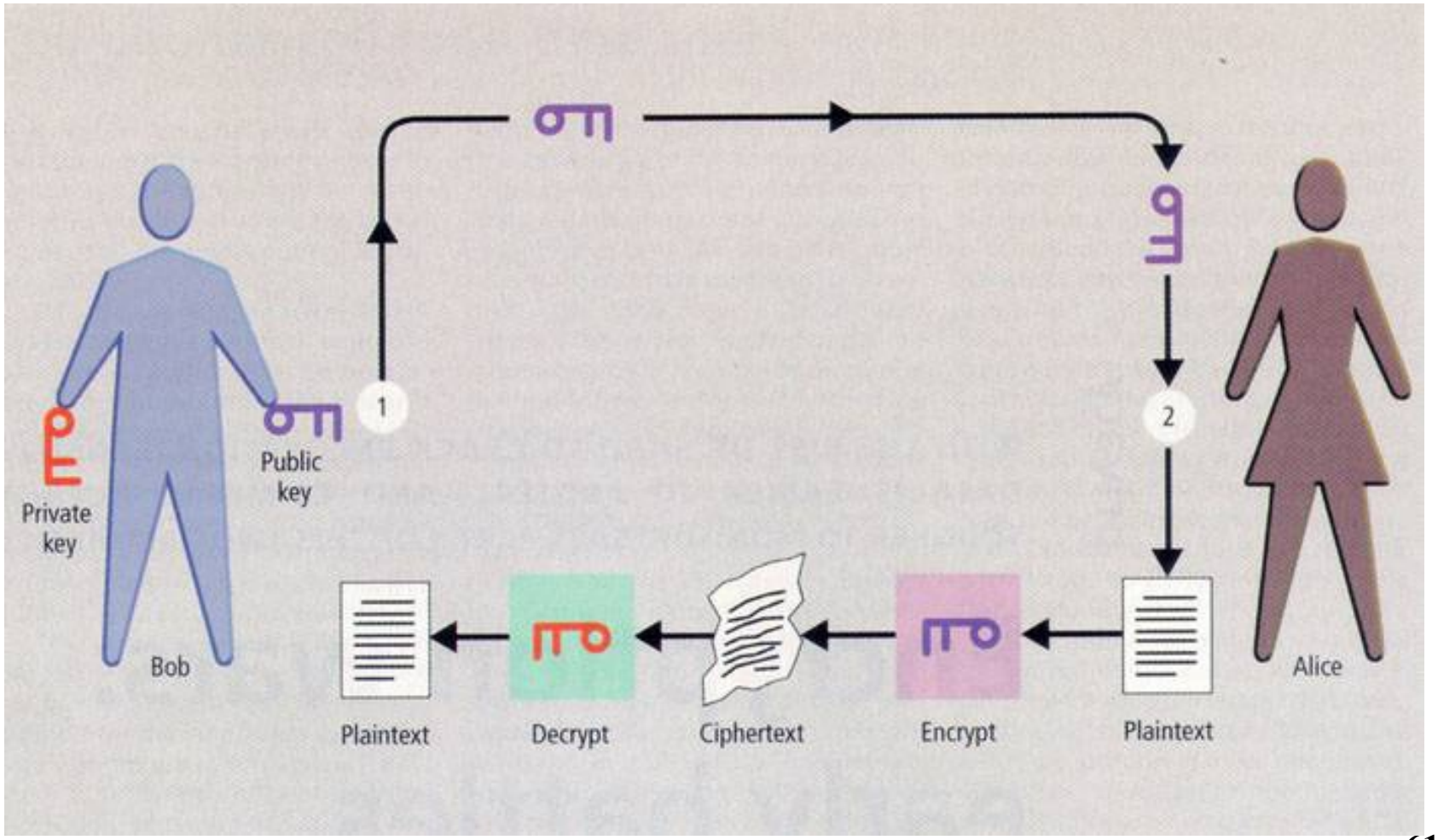


- Motivisani problemom upravljanja ključem, *Diffie* i *Hellman* su 1976. godine predstavili koncept **kriptografije sa javnim ključem**
- Kriptografija sa javnim ključem ima dve značajne primene:
  - kriptovanje i
  - digitalni potpis.
- U takvom sistemu koji koristi asimetričnu kriptografiju, svaki učesnik dobija par ključeva:
  - jedan **tajni** ključ i
  - jedan **javni** ključ.
- Javni ključ se objavljuje dok tajni čuva korisnik.

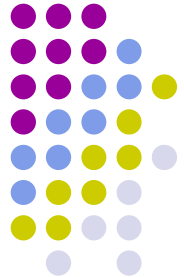
Asimetričan kriptografski sistem -



Asimetričan kriptografski sistem - suština rada sistema

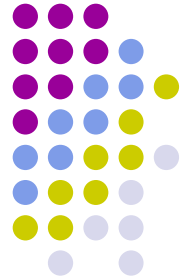


Asimetričan kriptografski sistem



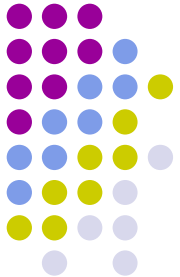
- Ako pošiljalac hoće da pošalje poruku, prvo potraži javni ključ primaoca u imeniku, koristi ga za kriptovanje poruke i šalje kriptogram
- Primalac pak koristi svoj tajni ključ za dekriptovanje kriptograma i čita poruku
- Svako može slati kriptovane poruke primaocu, ali samo primalac može da ih čita (jer jedino on zna svoj tajni ključ)
- Primarna prednost kriptografije sa javnim ključem jeste rešavanje problema distribucije ključeva

Sigurnost kriptovanog algoritma



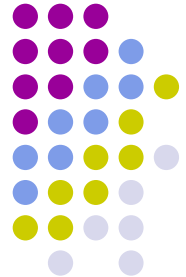
- Vreme potrebno za “razbijanje” algoritma mora da bude duže od vremena u kome podaci moraju da ostanu tajni.
- Takođe, potrebno je da bude zadovoljen i uslov da broj podataka šifrovanih jednim ključem bude manji od broja potrebnih podataka da se dati algoritam “razbije”.

Cena “razbijanja” algoritma mora da bude veća od cene šifrovanih podataka



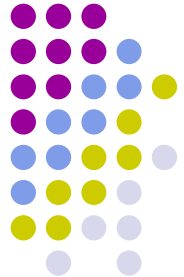
Dužina ključa (bit)	Broj alternativnih ključeva	Potrebno vreme pri 10^6 dekriptovanja/μs
32	$2^{32} = 4.3 \times 10^9$	2.15 milisekundi
56	$2^{56} = 7.2 \times 10^{16}$	10 sati
128	$2^{128} = 3.4 \times 10^{38}$	5.4×10^{18} godina
168	$2^{168} = 3.7 \times 10^{50}$	5.9×10^{30} godina

Preuzimanje i instaliranje javnog ključa



- Postoji nekoliko načina da se preuzme javni i privatni ključ
- Web lokacija Verisign (http://verisign.com) omogućava da se preuzme probni skup (važi 60 dana) javnih i privatnih ključeva ili da se kupe ključevi za šifru
- U uputstvima o preuzimanju koja se prime sa VeriSigna navode se koraci koji se moraju slediti da bi se koristili ključevi
- Pored toga, sa Web lokacije M.I.T na http://web.mit.edu/network/pgp.html može se preuzeti besplatan softver za korišćenje **PGP (Pretty Good Privacy)** šifrovanje
- Obe navedene Web lokacije nude uputstva koja vode kroz korake za slanje i primanje šifrovanih poruka

Pronalaženje korisnikovog javnog ključa



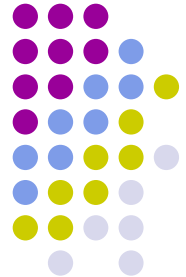
- Nakon što primite svoj javni ključ, možete ga poslati prijateljima preko elektronske poruke – oni će ga koristiti za šifrovanje poruka koje vam šalju
- Pored toga, svoj javni ključ možete postaviti u spisak javnih ključeva na Webu – kada korisnik kojem niste poslali svoj javni ključ treba da šifruje poruku da bi vam je poslao, on može da pronađe ključ na serverima sa javnim ključevima
- Naredna slika prikazuje server sa javnim ključevima na MIT-u na kome možete potražiti korisnikov javni ključ

Server sa javnim ključevima

Preuzimanje identifikatora servera

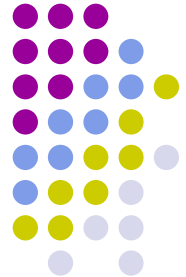
- Nekoliko kompanija, tzv. Nadležne organizacije, nude identifikatore Web servera preko Interneta
- Uopšteno, nakon ispitivanja kompanije, nadležna organizacija izdaje identifikator servera koji garantuje pravo da kompanija može da koristi svoje ime i Web adresu
- Pre nego što nadležna organizacija izda identifikator servera, ona pregleda dokumente kompanije, kao što su registracioni broj i ugovori
- Pre kupovine identifikatora servera potrebno je proveriti da li je tip sertifikata kompatibilan sa softverom servera koji koristi kompanija
- Većina sertifikata o identifikatoru servera podržavaju SSL – protokol koji koristi većina Web servera da bi izvela bezbedne operacije

Fino podešavanje dodele priključaka barijere



- Da bi komunicirao preko mreže, program pošiljalac mora da zada adresu udaljenog računara
- Pored toga, program pošiljalac mora da identifikuje aplikaciju na udaljenom računaru kojoj šalje poruku
- Mrežni programi identifikuju udaljene aplikacije korišćenjem broja koji programeri označavaju kao broj priključka aplikacije
- Sledeći spisak prikazuje brojeve priključaka koji odgovaraju opštim aplikacijama

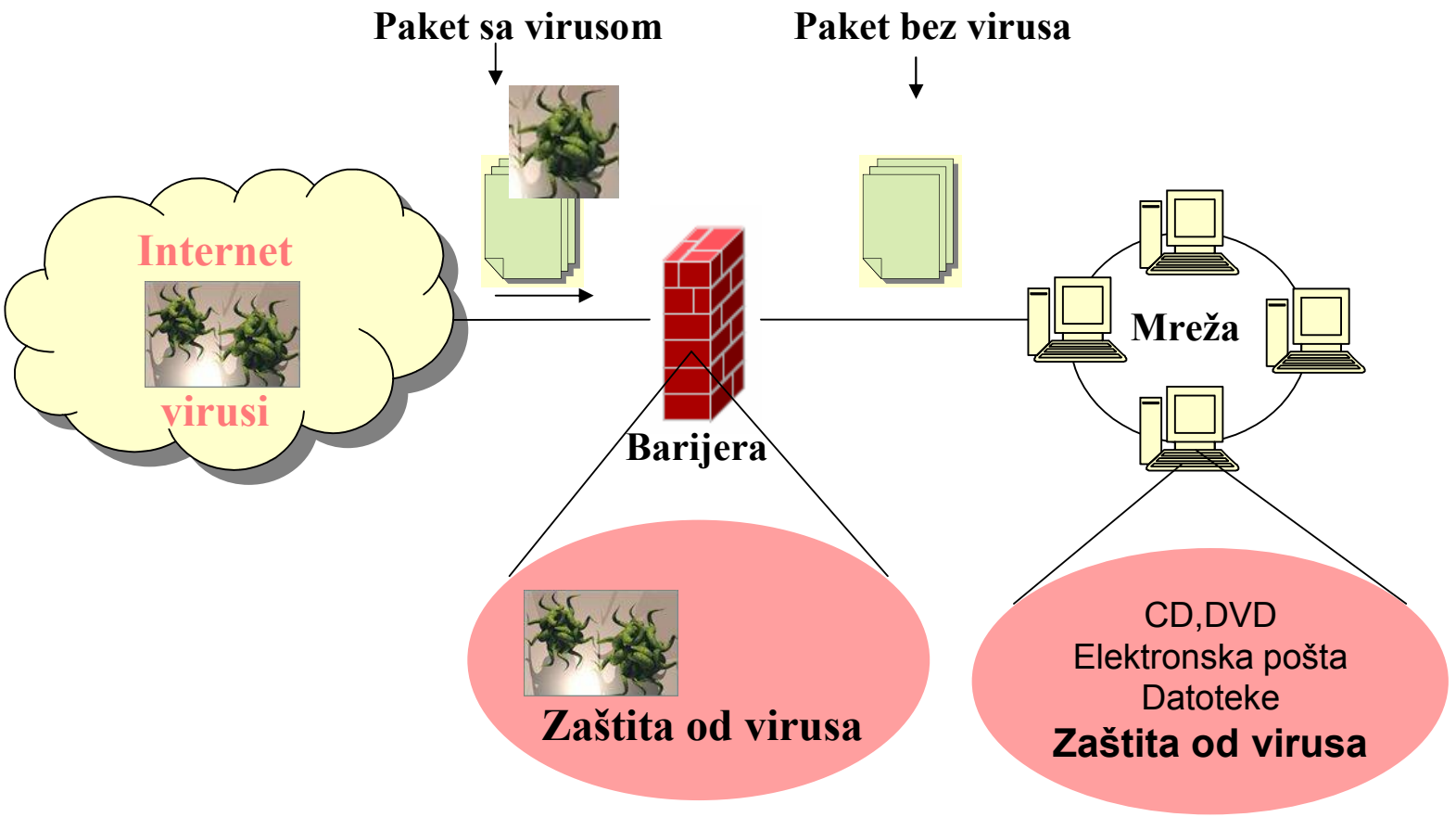
Brojevi priključaka koji odgovaraju opštim aplikacijama



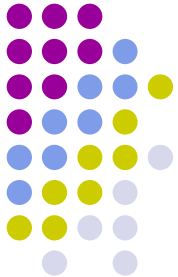
Broj priključka	Aplikacija
21	Protokol za prenos datoteka (FTP)
23	Telnet
25	Jednostavni protokol za prenos pošte (SMTP)
80	Protokol za prenos hiperteksta (HTTP)
139	Sesijska usluga NetBIOS

Tokom konfigurisanja barijere, prvo je potrebno onemogućiti poruke za sve priključke, a zatim omogućiti pristup samo onim posebnim priključcima koji su potrebni

Smanjenje izloženosti lokacije virusima



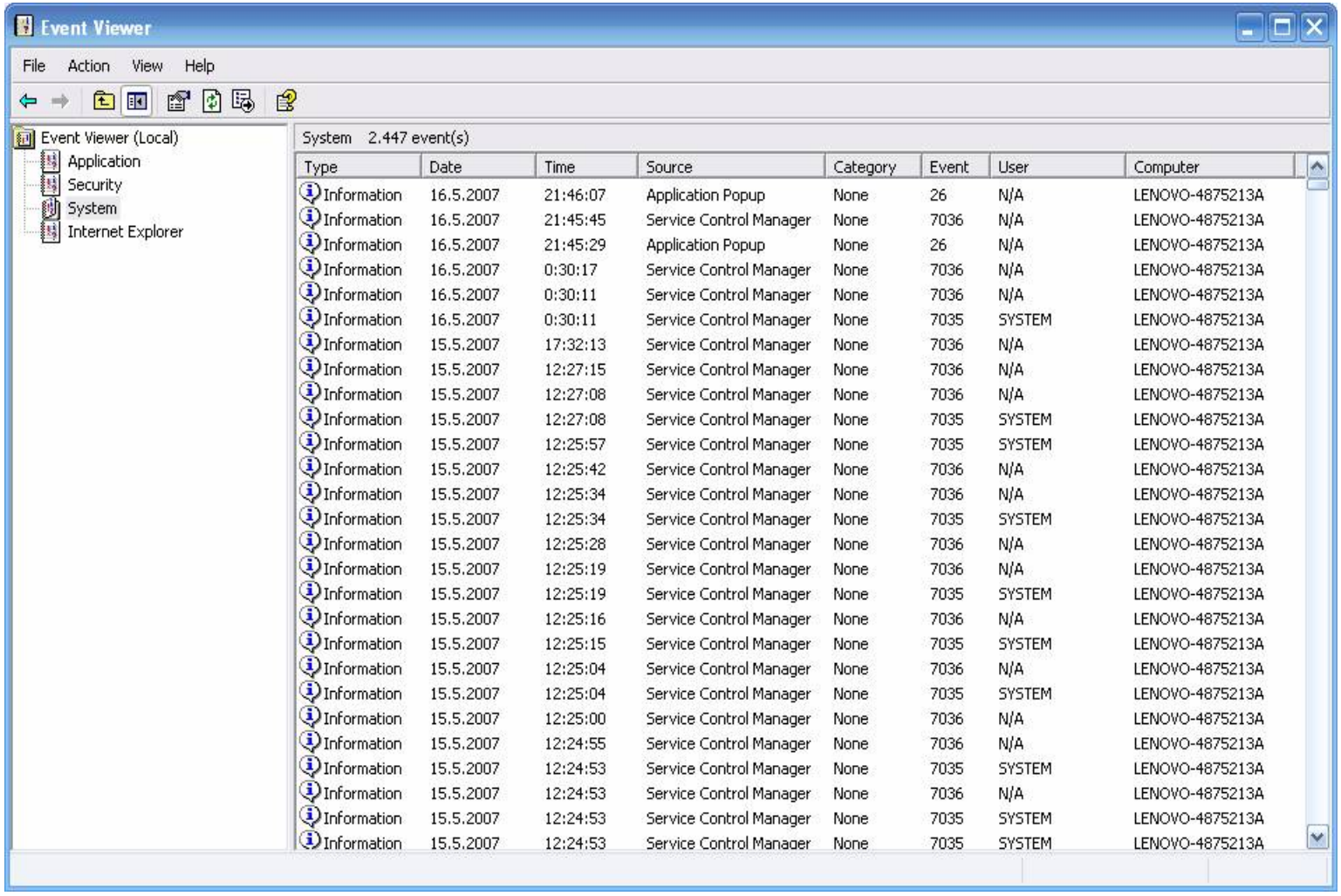
Nadgledanje sistemskih događaja radi otkrivanja uljeza



- Hakeri koriste mnoge tehnike za napade na sisteme
- Evidencija događaja se sastoji od jedne ili više datoteka evidencije koje održava operativni sistem radi praćenja korisnikovih aktivnosti
- Evidentiranje događaja pomaže da se uhvati haker koji je sa uspehom provalio u sistem
- U Windowsu poseban program pod nazivom **Event Viewer** omogućava administratorima sistema da pregledaju evidenciju različitih događaja
- **Event Viewer** evidentira tri tipa događaja: aplikacijski, bezbednosni i sistemski

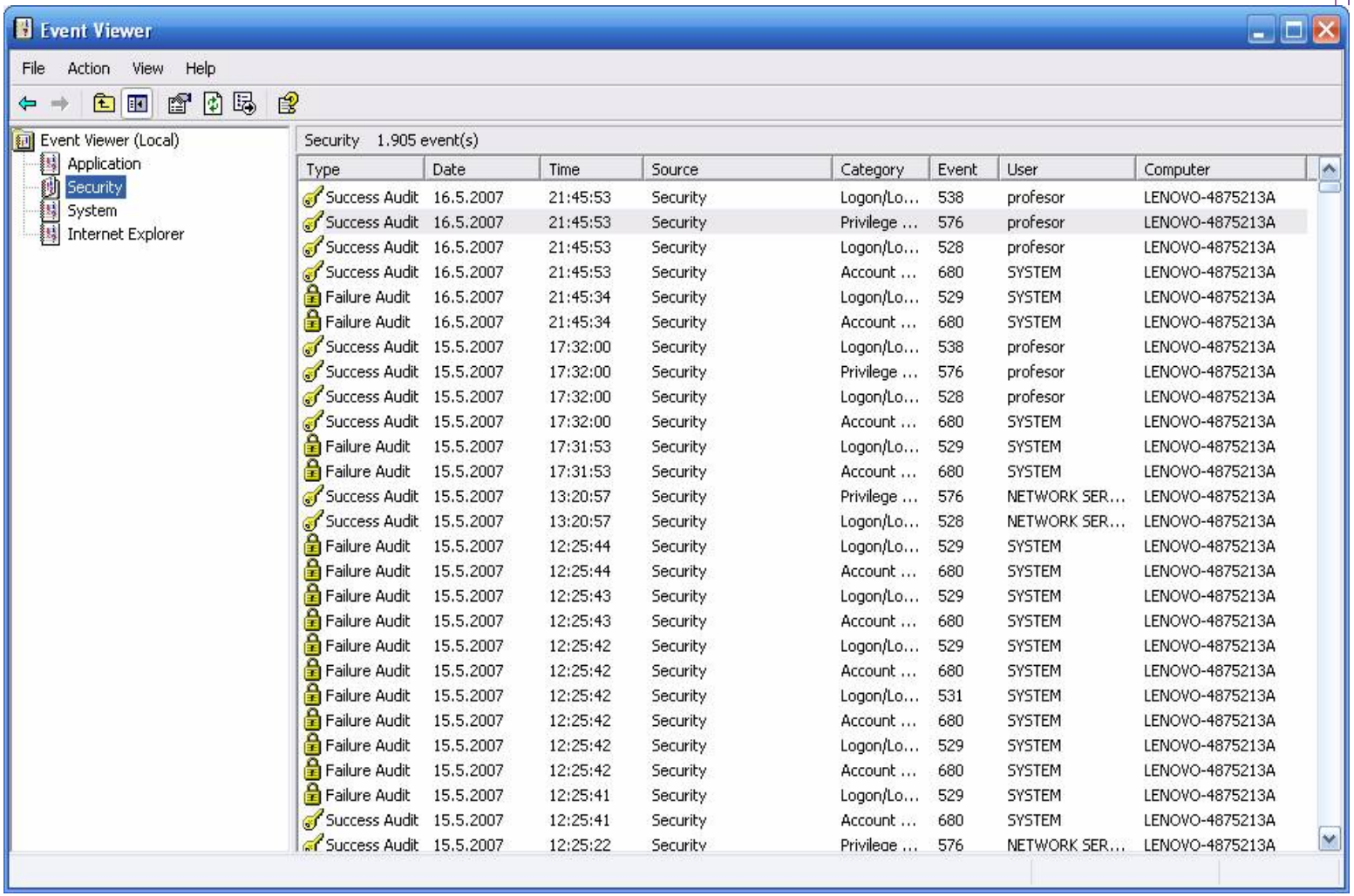
Event Viewer za praćenje događanja na sistemu

Start|Settings|Control Panel|Administrative Tools|Event Viewer



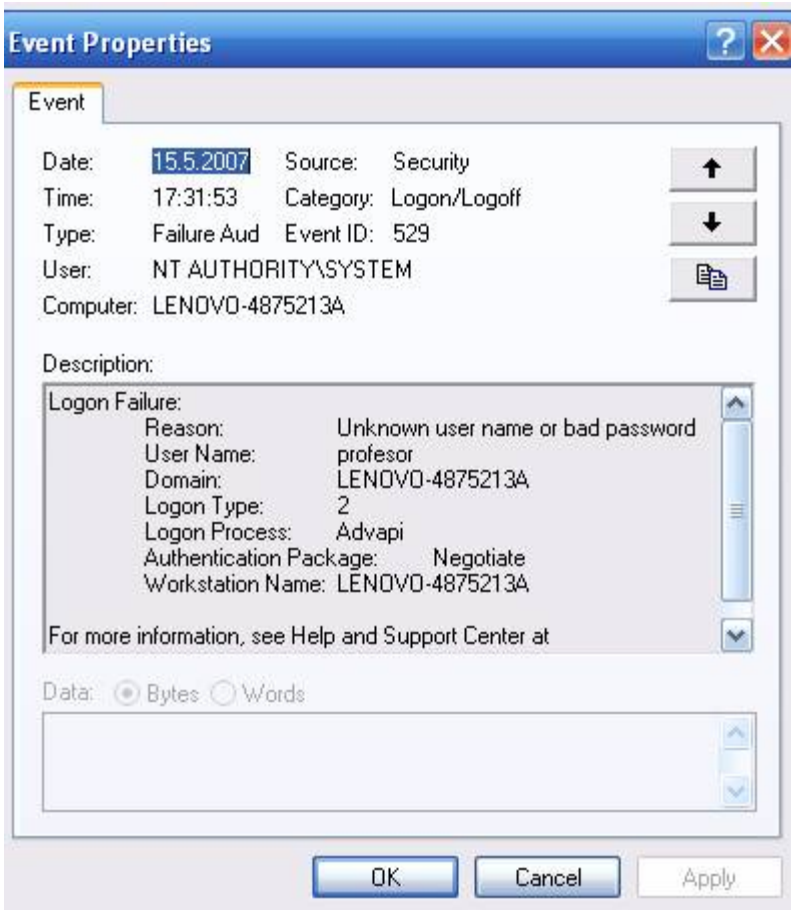
Type	Date	Time	Source	Category	Event	User	Computer
Information	16.5.2007	21:46:07	Application Popup	None	26	N/A	LENOVO-4875213A
Information	16.5.2007	21:45:45	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	16.5.2007	21:45:29	Application Popup	None	26	N/A	LENOVO-4875213A
Information	16.5.2007	0:30:17	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	16.5.2007	0:30:11	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	16.5.2007	0:30:11	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	17:32:13	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:27:15	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:27:08	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:27:08	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	12:25:57	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	12:25:42	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:25:34	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:25:34	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	12:25:28	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:25:19	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:25:19	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	12:25:16	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:25:15	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	12:25:04	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:25:04	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	12:25:00	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:24:55	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:24:53	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	12:24:53	Service Control Manager	None	7036	N/A	LENOVO-4875213A
Information	15.5.2007	12:24:53	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A
Information	15.5.2007	12:24:53	Service Control Manager	None	7035	SYSTEM	LENOVO-4875213A

Izgled evidencije bezbednosti u Event Vieweru



Type	Date	Time	Source	Category	Event	User	Computer
Success Audit	16.5.2007	21:45:53	Security	Logon/Lo...	538	profesor	LENOVO-4875213A
Success Audit	16.5.2007	21:45:53	Security	Privilege ...	576	profesor	LENOVO-4875213A
Success Audit	16.5.2007	21:45:53	Security	Logon/Lo...	528	profesor	LENOVO-4875213A
Success Audit	16.5.2007	21:45:53	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Failure Audit	16.5.2007	21:45:34	Security	Logon/Lo...	529	SYSTEM	LENOVO-4875213A
Failure Audit	16.5.2007	21:45:34	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Success Audit	15.5.2007	17:32:00	Security	Logon/Lo...	538	profesor	LENOVO-4875213A
Success Audit	15.5.2007	17:32:00	Security	Privilege ...	576	profesor	LENOVO-4875213A
Success Audit	15.5.2007	17:32:00	Security	Logon/Lo...	528	profesor	LENOVO-4875213A
Success Audit	15.5.2007	17:32:00	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	17:31:53	Security	Logon/Lo...	529	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	17:31:53	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Success Audit	15.5.2007	13:20:57	Security	Privilege ...	576	NETWORK SER...	LENOVO-4875213A
Success Audit	15.5.2007	13:20:57	Security	Logon/Lo...	528	NETWORK SER...	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:44	Security	Logon/Lo...	529	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:44	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:43	Security	Logon/Lo...	529	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:43	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:42	Security	Logon/Lo...	529	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:42	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:42	Security	Logon/Lo...	531	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:42	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:42	Security	Logon/Lo...	529	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:42	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Failure Audit	15.5.2007	12:25:41	Security	Logon/Lo...	529	SYSTEM	LENOVO-4875213A
Success Audit	15.5.2007	12:25:41	Security	Account ...	680	SYSTEM	LENOVO-4875213A
Success Audit	15.5.2007	12:25:22	Security	Privilege ...	576	NETWORK SER...	LENOVO-4875213A

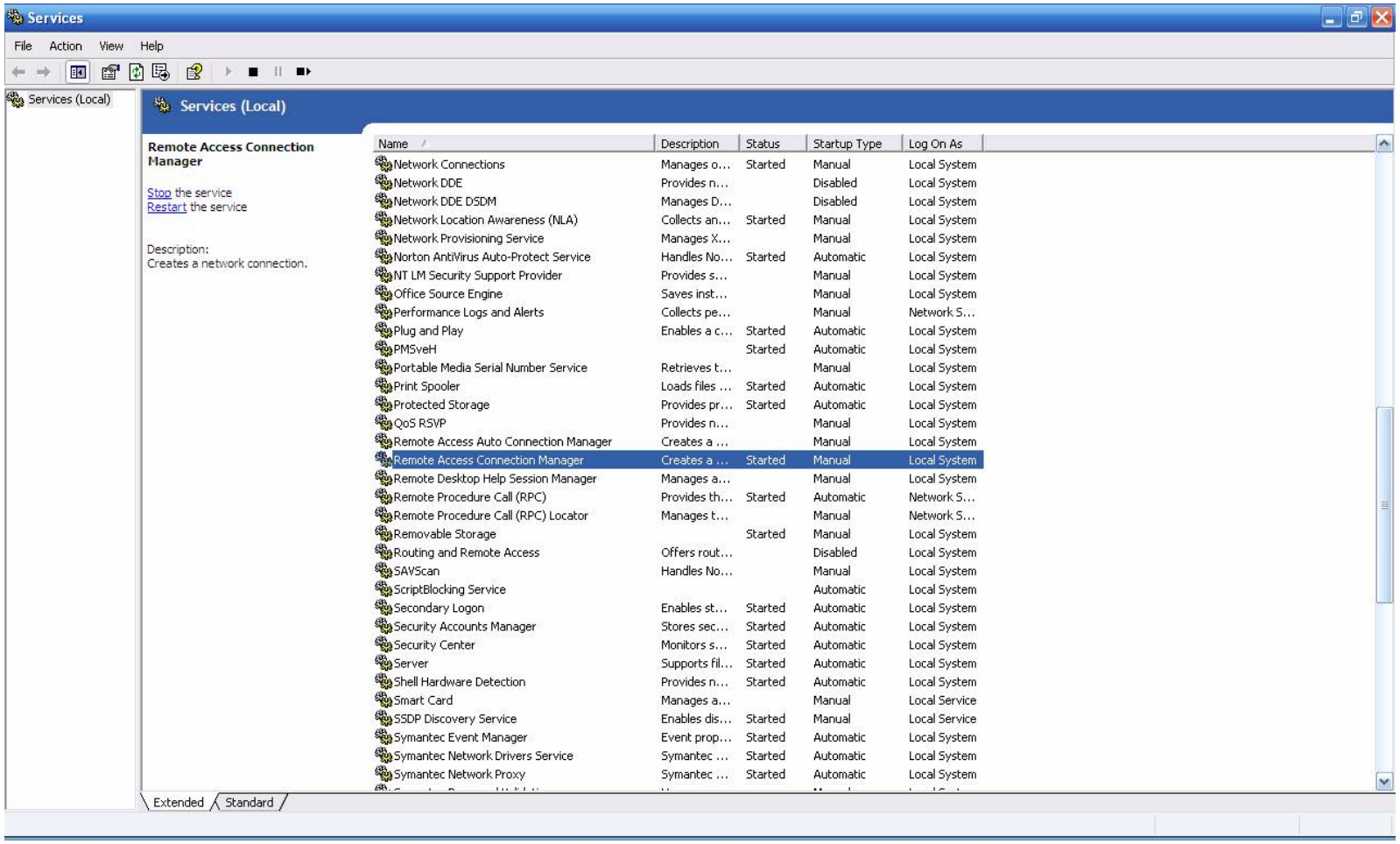
Izgled evidencije bezbednosti u Event Vieweru



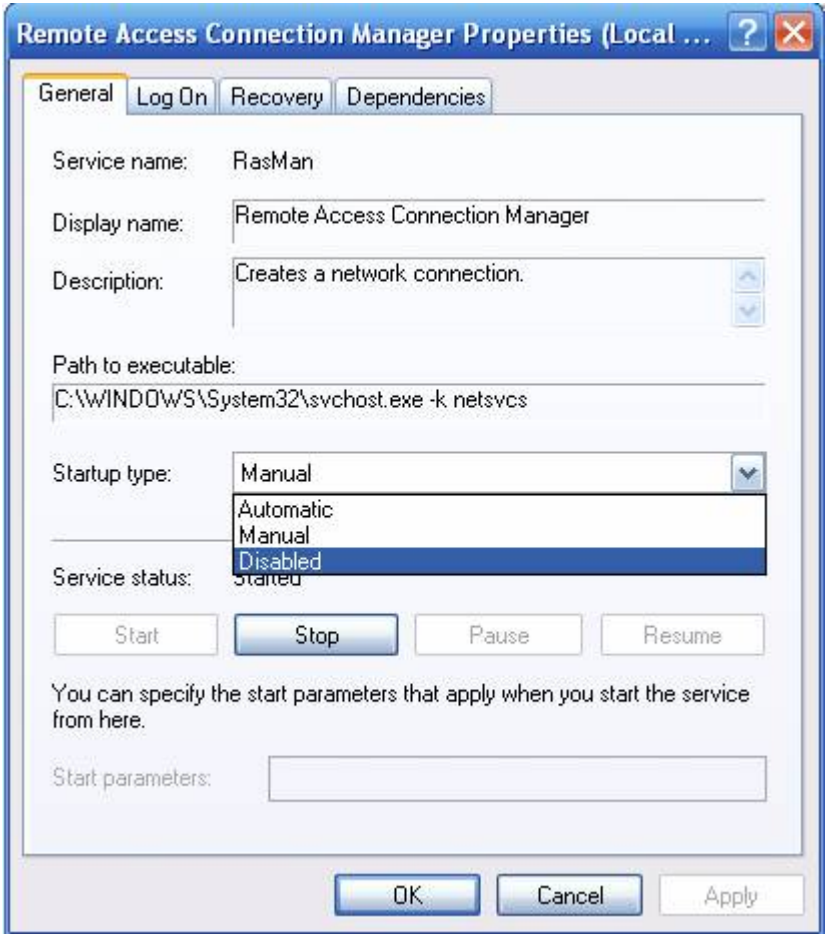
Onemogućavanje daljinskih usluga

- Mnoge Web lokacije dozvoljavaju korisnicima da se prijave na mrežu sa udaljenih mesta
- Ako to lokaciji nije potrebno, trebalo bi onemogućiti daljinske usluge da bi se smanjio rizik od hakerske zloupotrebe usluga za pristupanje sistemu
- Zavisno od operativnog sistema koji je pokrenut, razlikuju se koraci koji se moraju izvesti da bi se sprečio daljinski pristup
- U nastavku je dat prikaz onemogućavanja daljinskih usluga u Windowsu
- **Start|Settings|Control Panel|Administrative Tools|Services**

Prozor Services



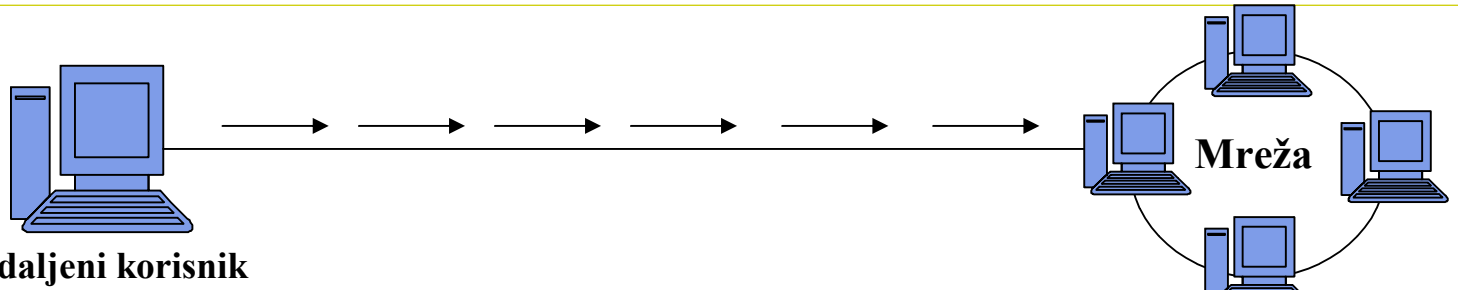
Onemogućavanje daljinskih usluga



Onemogućavanje daljinskih usluga

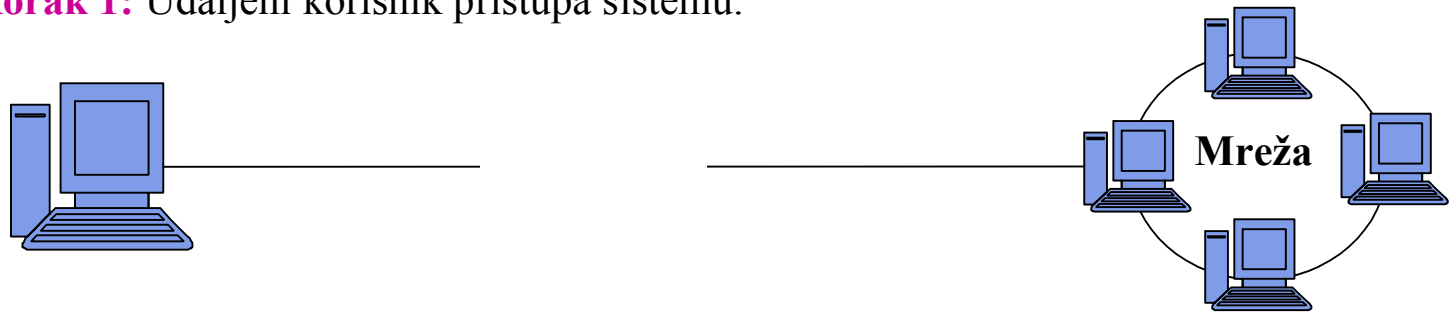
- U nekim trenucima korisnici imaju opravdanu potrebu da pristupe mreži iz daljine
- Ako postoje jedan ili više korisnika koji pristupaju mreži preko modema, može se povećati bezbednost sistema korišćenjem sistema sa povratnim pozivom
  - Udaljeni korisnik pristupa sistemu preko svog modema
  - Zavisno od softvera za povratni poziv, korisnik može da pozove određeni broj ili se od korisnika može tražiti da nakon biranja broja dostavi korisničko ime i lozinku ili digitalni sertifikat
  - Sistem sa povratnim pozivom zatim će prekinuti poziv i ponovo pozvati korisnika na unapred određeni broj – kao što je broj telefona modema u korisnikovoj udaljenoj kancelariji ili kući
- Na ovaj način haker na bilo kom drugom mestu ne može daljinski da pristupi sistemu, zato što sistem s povratnim pozivom neće uputiti povratni poziv hakerovom modemu

Sistem sa povratnim pozivom

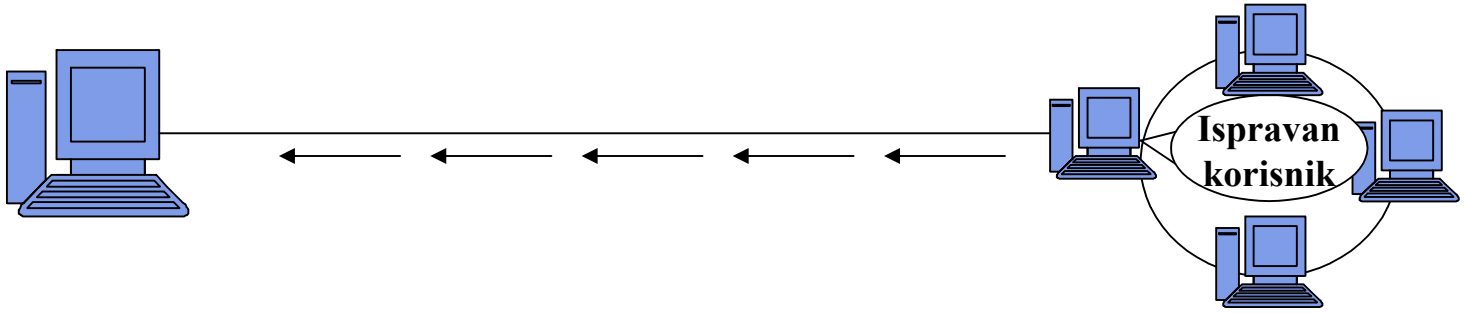


Udaljeni korisnik

Korak 1: Udaljeni korisnik pristupa sistemu.

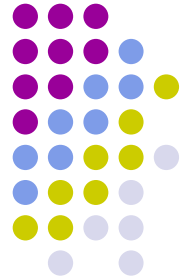


Korak 2: Server proverava identitet korisnika i prekida modemsku vezu.



Korak 3: Ako je udaljeni korisnik ispravan, server ga poziva na unapred određen broj.

Analiziranje ranjivosti sistema



- Postoji nekoliko Web lokacija na kojima se može proveriti koliko je lokacija ranjiva
- Većina provera koje obavljaju ove lokacije odnose se na probleme karakteristične za mrežu, za razliku od ranjivosti operativnog sistema
- Postoji nekoliko uslužnih programa koji se mogu preuzeti i pokrenuti radi obavljanja tih posebnih provera
- Na lokaciji http://www.insecure.org/tools.html može se pregledati lista najefikasnijih bezbednosnih alata

Bezbednost Web aplikacija