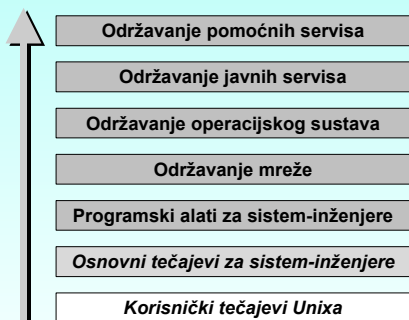


Održavanje javnih servisa

autori: Dinko Korunić (@srce.hr), Denis Stančer (@srce.hr) i Bojan Ždrnja (@fer.hr)

mentor: Miroslav Milinović (@srce.hr)
recenzent: Hrvoje Stipetić (@zv.hr)

(c) 2001-04 - 2001-10, CARNet & SRCE. Sva prava pridržana.
<http://sistemac.carnet.hr/nts/copyright.html>



Ciljevi tečaja

- Obučavanje o konceptu, instalaciji i konfiguraciji javnih servisa:
 - elektroničke pošte i mailing lista
 - weba i cachinga
 - imeničkih servisa
 - FTP-a, mrežnih novina (News), IRC-a
- Obučavanje o sigurnosti i zaštiti privatnosti krajnjeg korisnika

Potrebno predznanje

- Osnove Unixa
- Rad s nekim od tekst editora (vi, joe, ...)
- Osnove programiranja
- Osnove održavanja Unix operacijskog sustava
- Poznavanje načina rada i instalacije CARNetovih paketa (pkg)
- Osnove kompiliranja (configure, gcc, make) i instaliranja programa (make install)

Dio I Elektronička pošta i mailing liste

priredio Bojan Ždrnja

Sadržaj (1. dan)

Koncept elektroničke pošte - MTA, MUA, protokoli, raspoloživi programi, CARNetov izbor	10 min
Sendmail - instalacija, konfiguracija, logovi, dopunske mogućnosti, tuning	130 min
Pristup elektroničkoj pošti za korisnike - koncept, POP3, IMAP	65 min
Mailing liste - koncept, Majordomo, otvaranje i administracija lista, veza s MTA	65 min

Koncept elektroničke pošte

Općenito

- Mailbox (poštanski sandučić)
 - datoteka ili direktorij gdje se pohranjuju poruke elektroničke pošte
- Agenti
 - MUA (Mail User Agent)
 - korisnikova aplikacija
 - upotrebljava se za čitanje i slanje elektroničke pošte
 - podjela prema pristupu mailboxu: lokalni pristup i pristup putem računalne mreže

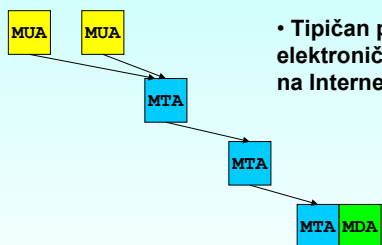
Koncept elektroničke pošte

Općenito (2)

- Agenti
 - MTA (Mail Transfer Agent)
 - prenose poruke elektroničke pošte između računala
 - poruke elektroničke pošte dobivaju od MUA
 - poruke se predaju drugim MTA
 - MTA su odgovorni za pravilnu isporuku elektroničke pošte
 - MDA (Mail Delivery Agent)
 - stavljaju dobivenu poruku elektroničke pošte u korisnikov mailbox
 - kada poruka elektroničke pošte stigne na ciljno računalo, MTA je predaje MDA

Koncept elektroničke pošte

Općenito (3)



- Tipičan put poruke elektroničke pošte na Internetu.

Koncept elektroničke pošte

Raspoloživi programi

- Svaka kategorija ima (naravno) puno raspoloživih programskih paketa
- MUA
 - Pine najpoznatiji na Unixima (jednostavna upotreba)
 - POP3 i IMAP omogućavaju čitanje elektroničke pošte sa poslužitelja, radne stanice ili osobnog računala
 - najčešći POP3/IMAP klijenti su Microsoft Outlook, Qualcomm Eudora i Netscape Messenger

Koncept elektroničke pošte

Raspoloživi programi (2)

- MTA
 - Sendmail (najpoznatiji i najozloglašeni)
 - Qmail
 - Exim
- MDA
 - mail.local kod Sendmail paketa
 - deliver (Cygnus)
 - Procmal

Koncept elektroničke pošte

CARNetov odabir

- CARNet je izabrao pakete koji su podržani
- Paketi se mogu skinuti prevedeni za CARNetove platforme (Solaris, Debian Linux) u binarnom obliku
- MUA: ostavlja se korisniku na izbor
- MTA: Sendmail
- MDA: mail.local (dolazi sa Sendmail paketom)

Sendmail

Općenito

- Najrašireniji MTA
- Najstariji i najpoznatiji
- Dolazi sa većinom operacijskih sustava
- Sa Solaris 7 operacijskim sustavom dolazi stara inačica Sendmaila
- Preporuka je instalirati najnoviju inačicu

Sendmail

Općenito (2)

- Inačica 8 Sendmaila je aktualna inačica
- Od 8.9.x inačice pojednostavljena instalacija prevođenjem konfiguracijskih datoteka pomoću m4 prevodioca
- CARNetovi paketi su trenutno inačica 8.9.3-1
- Najnovija inačica uvijek dostupna na <http://www.sendmail.org>

Sendmail

Princip rada

- Konfiguracijska datoteka Sendmaila .cf opisuje što Sendmail radi sa adresama elektroničke pošte
- Sendmail prepisuje adrese prema pravilima u konfiguracijskim datotekama
- Pravila su organizirana po skupovima (*ruleset*) koji se izvode propisanim redom
- Danas se koristi prevodilac m4 jer je .cf datoteka jako komplicirana

Sendmail

Potrebni paketi

- Uska integracija SMTP-a s DNS poslužiteljem (najčešće BIND)
- Baza podataka s korisničkim aliasima
 - koristi se `makemap` program
 - različite baze podataka (dbm, newdbm)
 - moguće je definirati koja se baza podataka koristi
- m4 prevodilac konfiguracijske datoteke

Sendmail

Instalacija

- Dohvaćanje paketa (izvorni kod)
- Postojanje već prevedenog paketa na CARNetovom poslužitelju
- Zadnja inačica uvijek dostupna na Sendmail web poslužitelju
- Raspakiranje tar.gz arhive

Sendmail

Instalacija (2)

- Hijerarhija direktorija Sendmail paketa
- U src direktoriju nalazi se izvorni kod
- Sendmail **NE** koristi make za prevođenje
- Umjesto make programa koristi se skripta koja dolazi sa Sendmailom, Build
- Pokretanje: `sh ./Build`

Sendmail Instalacija (3)

- Na Solaris operacijskom sustavu prevođenje treba proći bez problema ("out-of-the-box")
- Prilikom prevođenja stvara se unutar src/ direktorija pripadajući obj.* direktorij
- Direktorij obj ovisi o platformi na kojoj se prevodi paket
- U obj.*/ direktoriju biti će izvršna datoteka Sendmaila



Sendmail Instalacija (4)

- Za spremanje različitih podataka Sendmail koristi novu Berkeley bazu podataka (NEWDB)
- Ova baza podataka nije potrebna tijekom prevođenja, ali se koristi kasnije za pohranjivanje različitih podataka
- Moguće je koristiti i druge načine zapisa podataka
- NewDB je na <http://www.sleepycat.com>



Sendmail Instalacija i pokretanje (5)

- Nakon što je prevođenje i instalacija gotova, izvršna datoteka Sendmaila se na Solaris operacijskom sustavu nalazi u /usr/lib direktoriju
- Sendmail je potrebno pokretati u *daemon* načinu rada (zasebni servis), što govori -bd opcija prilikom pokretanja
- Moguće dati vrijednost provjere liste čekanja, -q opcija (-q15m npr.)

Sendmail Konfiguracija

- Tradicionalno vrlo komplicirana konfiguracijska datoteka (`sendmail.cf`)
- Razlog ove kompliciranosti je jednostavnost koda unutar čitanja za Sendmail
- Lokacija ove datoteke je uvijek `/etc/mail/sendmail.cf`



Sendmail Konfiguracija (2)

- Od inačice 8 Sendmaila koristi se m4 prevodilac za generiranje `sendmail.cf` datoteke
- Prevođe se `.mc` datoteke u kojima se ključnim riječima definiraju željene mogućnosti Sendmaila
- Općenite `.mc` datoteke dolaze sa Sendmailom, sve se nalaze unutar `cf/` direktorija



Sendmail Konfiguracija (3)

- Potrebno je napraviti glavnu `.mc` datoteku pomoću koje m4 prevodilac stvara `sendmail.cf` konfiguracijsku datoteku
- Prevođenje se zadaje jednostavno i na svim platformama je isto
- Potrebno je biti u `cf/` direktoriju:

```
$ m4 ../m4/cf.m4 datoteka.mc >  
sendmail.cf
```



Sendmail Konfiguracija (4)

- Prevođenje .mc datoteke može se alternativno izvesti i sa:

```
./Build config.cf
```

- Potrebno je u glavnoj .mc datoteci definirati sve potrebe na Sendmailu
- Sve potrebe definiraju se ključnim riječima koje mogu imati (ali ne moraju) i neki parametar



Sendmail Konfiguracija (5)

- Preporučljivo je uzeti opću .mc datoteku i nju promijeniti po potrebama
- U cf/cf direktoriju nalaze se primjeri .mc datoteka
- Za potrebu tipičnog CARNet računala potrebno je uzeti generic-solaris2.mc datoteku



Sendmail Konfiguracija (6)

- Vrlo jednostavna datoteka, početak uvijek isti (divert ključna riječ)
- Definirana vrsta operacijskog sustava
- Definirana domena (generička, nije potrebno mijenjati)
- Definirani MAILER programi (za normalnu upotrebu u CARNet ustanovi isto nije potrebno mijenjati)

Sendmail Domene

- Potrebno je definirati domene za koje će Sendmail na lokalnom računalu prihvaćati elektroničku poštu
- Domene se definiraju u datoteci `/etc/mail/local-host-names`
- Sintaksa datoteke je jednostavna, samo se upisuju imena domena

Sendmail Domene (2)

- Primjer datoteke s domenama:
`zesoi.fer.hr`
`zesoi.etf.hr`
- Nakon upisanih promjena, potrebno je restartati Sendmail ili mu poslati SIGHUP signal
- Ovo je potrebno napraviti uvijek kada se mijenjaju datoteke sa klasama (poput ove)

Sendmail Relay poruka

- Relaying predstavlja prijenos poruke preko pojedinog poslužitelja
- Konfiguracija automatski zabranjuje relay sa svih računala
- Ukoliko se želi dodati relay, to je potrebno napraviti u posebnoj datoteci `/etc/mail/relay-domains`
- U datoteku se mogu upisati puna imena računala ili IP adrese

Sendmail

Relay poruka (2)

- Za lokalnu domenu u kojoj se nalazi poslužitelj može se koristiti ključna riječ:
`FEATURE(relay_entire_domain)`
- Lokalna domena predstavlja onu koja je definirana u M klasi Sendmaila (obično u `local-host-names` datoteci)
- Alternativno relay se može podešavati u datoteci sa pravima pristupa,
`/etc/mail/access`

Sendmail

Aliasi korisnika

- Korisnici mogu imati alias adrese
- Alias adrese mogu se usmjeravati bilo gdje (ne moraju ostajati na lokalnom računalu)
- Aliasi se mogu iskoristiti kao jednostavne distribucijske liste za više korisnika
- Nedostatak ovakvih lista je otežano administriranje (sve mora administrator ručno raditi)

Sendmail

Aliasi korisnika (2)

- Aliasi se definiraju u datoteci:
`/etc/mail/aliases`
- Aliasi su jednostavnog oblika:
`alias: adresa`
- Obavezno moraju biti definirani aliasi za korisnike:
`postmaster`
`MAILER_DAEMON`

Sendmail

Aliasi korisnika (3)

- Na postmaster adresu usmjeravaju se poruke elektroničke pošte koje su se vratile greškom
- Poruke se vraćaju greškom na ovu adresu ako su i To: i From: polja upisana krivo
- Ako ne postoji postmaster alias, doći će do petlje u slanju poruka s jednog računala na drugo

Sendmail

Aliasi korisnika (4)

- Nakon mijenjanja datoteke sa aliasima potrebno ju je prevesti u pripadajuću bazu podataka radi bržeg pristupa Sendmaila do traženih podataka

```
$ newaliases
```

Sendmail

Pravo pristupa

- Pravo pristupa određuje se u datoteci /etc/mail/access
- Potrebno je uključiti mogućnost definiranja prava pristupa ključnom riječi:
FEATURE (access_db)
- Pomoću prava pristupa može se definirati i relay za neke domene

Sendmail Pravo pristupa (2)

- Pravo pristupa koristi se kada se želi kontrolirati pristup sa neke adrese ili mreže
- Sintaksa je jednostavna:

```
spammer@nesto.hr REJECT  
korisnik@srce.hr OK  
hacke@hack.hr ERROR:"550 Ne  
prihvacamo mail od hackera"
```

Sendmail Pravo pristupa (3)

- Nakon promjene datoteke prava pristupa (izvorne datoteke), potrebno je također obnoviti datoteku s bazom podataka
- Baza podataka s pravom pristupa drži se u hash formatu

```
$ makemap hash /etc/mail/access < \  
source_datoteka
```

Sendmail Korištenje virtual hostinga

- Omogućava mapiranje različitih (virtualnih) domena na korisnike na lokalnom računalu ili na drugim računalima
- Osim Sendmaila, potrebna je i konfiguracija DNS poslužitelja, te izrada baze podataka s korisnicima i pripadajućim domenama za koje se radi virtual hosting

Sendmail

Korištenje virtual hostinga (2)

- Na DNS poslužitelju potrebno je postaviti MX zapise tako da za virtualnu domenu pokazuju na pravi poslužitelj:

```
virthost.com. IN MX 10 nashost.hr  
virthost.com. IN MX 20 second.hr
```



Sendmail

Korištenje virtual hostinga (3)

- Potrebno je uključiti virtual hosting u .mc datoteci i prevesti je u pripadajuću .cf datoteku:

```
FEATURE(`virtusertable', `dbm  
/etc/mail/virtusertable')dnl
```



Sendmail

Korištenje virtual hostinga (4)

- Ova ključna riječ koristi bazu podataka koja se nalazi u /etc/mail/virtusertable
- Baza podataka je po navedenom u dbm obliku
- Ukoliko je Sendmail preveden sa NEWDB, a ne sa NDBM opcijom, potrebno je umjesto dbm koristiti hash



Sendmail

Korištenje virtual hostinga (5)

- Nakon upisanih promjena u .mc datoteci potrebno ju je prevesti u pripadajuću .cf datoteku
- Da bi Sendmail bio uspješno pokrenut potrebno je napraviti i pripadajuću virtusertable datoteku u kojoj su opisi virtualnih poslužitelja – u protivnom se prilikom pokretanja javlja greška

Sendmail

Korištenje virtual hostinga (6)

- Sintaksa virtusertable datoteke je jednostavna:

```
korisnik@virthost.com    localuser
```

- Ovaj oblik mapira prikazanu adresu na lokalnog korisnika

Sendmail

Korištenje virtual hostinga (7)

- Moguće je preusmjeravanje na drugo računalo:

```
korisnik@virthost.com    \  
    korisnik@drugoracunalo.com
```

- Ovaj oblik mapira prikazanu adresu na adresu korisnika na drugom računalu

Sendmail

Korištenje virtual hostinga (8)

- Preusmjeravanje kompletne elektroničke pošte za jednu domenu na jednog korisnika:

```
@virthost.com    localuser
```

- Sva dolazeća pošta na domenu virthost.com ide lokalnom korisniku

Sendmail

Korištenje virtual hostinga (9)

- Pregledavanje `virtusertable` datoteke od strane Sendmaila izvodi se po redu
- Koristi se prvo pravilo na koje se naiđe
- Potrebno je voditi računa o tome što se dešava u pojedinim slučajevima i napisati pravilo koje prihvaća sve slučajeve (kao zadnje pravilo)

Sendmail

Korištenje virtual hostinga (10)

- Primjer `virtusertable` datoteke

```
bojan@dom1.com    bzdrnja  
error@dom1.com    error:nouser Ne\  
                  postoji korisnik  
list@dom1.com     nasa-lista  
@dom1.com         %1@drugadomena.hr
```

Sendmail

Korištenje virtual hostinga (11)

- Prethodni primjer sadrži tipične primjere virtual hostinga
- Elektronička pošta za korisnika `bojan@dom1.com` usmjeruje se na lokalnog korisnika
- Naveden je korisnik koji ne postoji, `error@dom1.com`



Sendmail

Korištenje virtual hostinga (12)

- Navedena je lista koju Sendmail zapravo dohvaća iz datoteke sa aliasima – `nasa-lista` je alias definiran na nekoliko korisnika u `/etc/mail/aliases` datoteci
- Na kraju se sva elektronička pošta koja nije zadovoljila prethodna pravila, šalje na korisnika sa istim imenom na `drugadomena.hr`



Sendmail

Korištenje virtual hostinga (13)

- Nakon izvedenih promjena na `virtusertable` datoteci, potrebno je napraviti bazu podataka koju će Sendmail koristiti:

```
$ makemap dbm \  
  /etc/mail/virtusertable < \  
  izvorna_datoteka
```



Sendmail

Korištenje virtual hostinga (14)

- Također je potrebno dodati i ime virtualne domene za koju će se primati elektronička pošta u `/etc/mail/local-host-names` datoteci
- Nakon provedenih promjena, potrebno je restartati Sendmail ili mu poslati SIGHUP signal

Sendmail

Prepisivanje odlazeće adrese

- Vrlo korisna opcija, omogućuje da sva elektronička pošta ima istu adresu s koje odlazi
- Ne vidi se adresa računala već je moguće staviti bilo koju drugu adresu

```
MASQUERADE_AS(`carnet.hr')
```

Sendmail

Direktorij sa listom čekanja (queue)

- Određuje se sa operacijskim sustavom na kojem je instaliran Sendmail
- Obično se nalazi u:
`/var/spool/mqueue`
- Simbolička imena datoteka, povezana s logovima

Sendmail

Pokretanje Sendmaila

- Potrebno je napraviti skriptu za pokretanje Sendmaila koja će ga pokrenuti prilikom svakog *reboota* računala
- Pokretanje s komandne linije je jednostavno, zadaju se parametri za rad kao servis i za provjeru liste E-mail poruka na čekanju (queue)

Sendmail

Pokretanje Sendmaila (2)

- Prilikom svakog pokretanja Sendmail provjerava *queue* listu i pokušava poslati poruke koje su imale grešku (npr. nedostupno računalo)
- Karakteristično pokretanje:

```
$ /usr/lib/sendmail -bd -qlh
```

Sendmail

Sigurnost

- Potrebno je obratiti pažnju na datoteke u */etc/mail* direktoriju i prava čitanja, odnosno pisanja na njima
- Niti u jednu datoteku ne smije biti omogućeno pisanje od strane korisnika na sustavu
- Sendmail ovakvu grešku javlja prilikom pokretanja

Sendmail

Anti-spam mogućnosti

- Automatski ugrađeno odbijanje relaya za druge domene, obično je potrebno eksplicitno dodati relay za vlastitu domenu
- Provjera domene korisnika koji šalje elektroničku poštu iz MAIL FROM: polja

```
MAIL FROM: test@test.hr
501 5.1.8 test@test.hr... Sender
domain must exist
```

Sendmail

Anti-spam mogućnosti (2)

- Provjera korisnika koji prima elektroničku poštu iz RCPT TO: polja

```
MAIL FROM: test@carnet.hr
250 2.1.0 test@carnet.hr... Sender ok
RCPT TO: test@test.hr
550 test@test.hr... Relaying denied
```

Sendmail

Logovi

- Sve informacije o radu Sendmaila nalaze se u logovima
- Logovi su u `/var/log/syslog` datoteci
- Moguće je vidjeti korisnike koji su slali i dobivali elektroničku poštu kao i greške u radu

Sendmail Logovi (2)

- Puno nivoa opsežnosti zapisivanja logova
- Standardni nivo uključuje samo adrese pošiljaoca i primatelja te greške

```
Jun 16 15:54:13 branka sendmail[23839]:  
f5GDsDR23839: from=<hwdad2001@yahoo.com>,  
size=1251, class=0, nrcpts=1,  
msgid=<200106161400.QAA16283@labs3.cc.fer.hr>,  
proto=ESMTP,daemon=Daemon0,  
relay=labs3.cc.fer.hr [161.53.72.21]
```

Sendmail Logovi (3)

- Nastavak loga pokazuje kome je bila namijenjena dotična poruka elektroničke pošte

```
Jun 16 15:54:15 branka sendmail[23840]:  
f5GDsDR23839: to=bzdrnja@maja,  
delay=00:00:02, xdelay=00:00:02,  
mailer=esmtplib, pri=30657,  
relay=maja.zesoi.fer.hr. [161.53.64.3],  
dsn=2.0.0, stat=Sent (f5GDuu628097 Message  
accepted for delivery)
```

Sendmail Logovi (4)

- Greške u logovima se lako vide i objašnjenja su razumljiva

```
Jun 16 15:55:12 diana.zesoi.fer.hr  
sendmail[8343]: f5GDtCp08343:  
ruleset=check mail, arg1=<nobody>,  
relay=[202.96.176.236],  
reject=553 5.5.4 <nobody>... Domain name  
required
```

Sendmail Vježba I

- Napraviti .mc datoteku s:
 - korištenjem relayinga za domenu
 - korištenjem virtualhost tablice
- Prevesti .mc datoteku u .cf datoteku za Sendmail
- Pokrenuti Sendmail

Sendmail Vježba I (2)

- Provjeriti ispravnost pregleda domena Sendmaila u SMTP-u:

```
telnet localhost 25  
helo localhost  
mail from: test@test.hr
```

- Ovakav mail treba biti odbijen

Sendmail Debug

- Postoji nekoliko načina na koje se može provjeravati ispravnost rada Sendmaila
- U logovima se mogu vidjeti nastali problemi na višim razinama kao što je npr. zabranjen relaying
- Problemi u konfiguracijskim datotekama i bazama podataka prijavljuju se prilikom pokretanja Sendmaila

Sendmail Debug (2)

- Sendmail ima *verify* način rada u kojem se samo provjeravaju adrese
- Ovaj način rada je koristan za provjeravanje korisnika ili lista

```
$ /usr/lib/sendmail -bv bzdrnja  
bzdrnja... Deliverable: mailer local,  
user bzdrnja
```

Sendmail Debug (3)

- Sendmail je moguće pokrenuti u test načinu rada sa *-bt* opcijama
- U test načinu rada moguće je provjeriti izvođenje pravila (*rulesetova*) u Sendmailu

```
$ /usr/lib/sendmail -bt  
> 3,0 bojan.zdrnja@carnet.hr
```

Sendmail Vježba II

- Napraviti alias za neku listu korisnika
- Pokrenuti Sendmail u test načinu rada
- Provjeriti ispisivanje zadane lokalne adrese liste korisnika

Sendmail

Sažetak

- Vrlo moćan i kompleksan MTA
- Najrašireniji MTA danas
- Komplicirana konfiguracijska datoteka, prevođenje sa višeg nivoa korištenjem m4 prevodioca
- Mogućnosti definiranja aliasa, prava pristupa, virtualnih hostova ...

Sendmail

Literatura

- CF-README.txt datoteka sa opisom mogućnost m4 prevodioca i .mc datoteka
- <http://www.sendmail.org> - glavna web stranica s najnovijim inačicama
- "Sendmail (The Bat Book)", O'Reilly & Associates
- comp.mail.sendmail news grupa

Pristup elektroničkoj pošti za korisnike

Općenito

- Omogućava pristup sa udaljenog računala (radne stanice korisnika)
- Korisnik ima neku inačicu MUA na svom računalu
- Vrlo popularno zbog korištenja MUA na Windows operacijskim sustavima

Pristup elektroničkoj pošti za korisnike

Općenito (2)

- Pristup s dva poznata protokola:
 - POP3 (engl. *Post Office Protocol*)
 - IMAP (engl. *Internet Message Access Protocol*)
- Najpoznatiji MUA (Outlook i Eudora) pristupaju ovim protokolima
- Potrebno imati pripadajuće servise na poslužitelju

POP3

Općenito

- Najpoznatiji i najprihvaćeniji protokol za čitanje elektroničke pošte sa udaljenog računala
- POP3 servis je na portu 110
- CARNet podržava Qpopper paket od Qualcomm

Qpopper

Princip rada

- Servis očekuje zahtjeve na portu 110
- Pokreće se iz Inetd-a, što preko TCP wrappers paketa omogućava određivanje prava pristupa
- Prilikom čitanja elektroničke pošte kopira sadržaj u istoimenu `.korisnik.pop` datoteku (npr. mailbox `bzdrnja` kopira u `.bzdrnja.pop`)

Qpopper Instalacija

- Dohvaćanje paketa (izvorni kod)
- Postojanje već prevedenog paketa na CARNetovom poslužitelju
- Zadnja inačica uvijek dostupna na Qualcommovom web poslužitelju
- Raspakiranje tar.gz arhive

Qpopper Instalacija (2)

- Qpopper koristi GNU konfiguraciju
- Konfiguracija se pokreće s:

```
./configure
```
- Nakon što završi proces konfiguracije potrebno je prevesti izvorni kod s:

```
make
```

Qpopper Instalacija (3)

- Na operacijskim sustavima koje podržava CARNet, proces prevođenja trebao bi proći bez greške
- Instalacija na sustav provodi se s:

```
Make install
```
- Izvršna datoteka uvijek se zove `popper`

Qpopper Konfiguracija

- Preporučuje se pokretanje iz Inetd-a
- Potrebno dodati konfiguracijsku liniju u /etc/inetd.conf:

```
pop3 stream tcp nowait root \  
/usr/local/lib/popper -s
```

- I liniju za servis u /etc/services:

```
pop3 110/tcp# Post Office
```

Qpopper Konfiguracija (2)

- Postoji puno parametara koji se zadaju s komandne linije
- Obično se koristi samo -s koji omogućava zapisivanje statistike korištenja:

```
bzdrnja 0 0 1 385 test.carnet.hr  
192.168.2.4
```

- Korisnik je obrisao 0 poruka i 0 okteta, 385 okteta je ostalo na poslužitelju

Qpopper Konfiguracija (3)

- Prava pristupa na direktorijima moraju biti ispravno postavljena
- /var/spool/mail direktorij treba biti u vlasništvu korisnika root i grupe mail
- Sticky bit treba biti postavljen da onemogući brisanje ili promjenu imena korisnika nad tuđim datotekama

Qpopper Ostalo

- Qpopper koristi autentifikaciju operacijskog sustava (/etc/passwd i /etc/shadow)
- Prilikom pokretanja kopira se datoteka u .user.pop.
- Ukoliko je mailbox jako velik, ovo može potrajati i uzrokovati timeout grešku kod korisnikovog MUA!

Qpopper Debug

- Ispravnost rada Qpoppera je vrlo lako provjeriti preko porta 110
- Telnetom na port 110 poslužitelja mora se vidjeti QPOP banner poruka
- Ukoliko se ne može uspostaviti komunikacija s poslužiteljem i portom 110, potrebno je provjeriti logove od TCP wrappers paketa

Qpopper Debug (2)

- Najčešća greška je da se zaboravi poslati SIGHUP signal Inetd-u nakon promjene /etc/inetd.conf datoteke
- Ako je sve postavljeno dobro, treba se dobiti poruka slična:

```
+OK QPOP (version 4.1) at host
starting <13625.811191280@host>
```

Qpopper Debug (3)

- Za bilo kojeg korisnika može se provjeriti ispravnost s:
USER bzdrnja
- Treba se dobiti:
+OK Password required for bzdrnja
- Nakon čega se može upisati zaporka:
PASS zaporka

Qpopper Debug (4)

- Unošenjem zaporka Qpopper odgovara s:
+OK bzdrnja has 2 message(s) (4123 octets).
- Sada se može provjeriti stanje poštanskog sandučića korisnika s komandom:
LIST
- Komunikacija se završava s QUIT

Qpopper Vježba

- Prevesti izvorni kod u izvršni
- Instalirati Qpopper na sustav
- Konfigurirati Inetd
- Konfigurirati TCP wrappers paket
- Provjeriti ispravnost rada telnetiranjem

Qpopper

Literatura

- http://www.eudora.com/qpopper_general/ - glavna web stranica s najnovijim inačicama Qpoppera
- Qualcomm: Qpopper Administrator's Guide
- <http://www.eudora.com/qpopper/faq.html> - FAQ o instalaciji i konfiguraciji Qpoppera

IMAP

Općenito

- IMAP omogućava pristup elektroničkoj pošti na udaljenom računalu kao da je pohranjena lokalno
- Vrlo korisno kada korisnici čitaju elektroničku poštu s različitih računala
- Sprema poruke na poslužitelju u različite mail datoteke što ubrzava pristup i poboljšava performanse

UW IMAP Server

Princip rada

- Servis očekuje zahtjeve na portu 143
- Pokrenut je iz Inetd-a, što preko TCP wrappers paketa omogućava određivanje prava pristupa
- Datoteke drži u korisničkim direktorijima, potrebno obratiti pažnju na zauzeće diska (quota)

UW IMAP Server Instalacija

- Dohvaćanje paketa (izvorni kod)
- Zadnja inačica uvijek dostupna na University Of Washington web poslužitelju
- Raspakiranje tar.gz arhive
- Sa IMAP paketom dolaze i poslužiteljski programi za POP, ali ih CARNet ne podržava/preporuča



UW IMAP Server Instalacija (2)

- IMAP ne koristi GNU autoconf
- Potrebno je pokrenuti prevođenje Imapd servisa u direktoriju:

```
imap-2000/imapd
```

- Koristi se *shadow* datoteka sa zaporkama na Solaris operacijskom sustavu:

```
make sol
```



UW IMAP Server Instalacija (3)

- Nakon uspješnog prevođenja dobiva se izvršna datoteka
- Izvršna datoteka je uvijek:

```
imap-2000/imapd/imapd
```
- Potrebno je izvršnu datoteku kopirati na mjesto gdje se nalaze poslužiteljski programi (npr.

```
/usr/local/sbin
```

)



UW IMAP Server Instalacija (4)

- Preporučuje se pokretanje iz Inetd-a
- Potrebno dodati konfiguracijsku liniju u
- /etc/inetd.conf:

```
imap stream tcp nowait root \  
/usr/local/sbin/imapd imapd
```

UW IMAP Server Instalacija (5)

- Potrebno je dodati i liniju za servis u
- /etc/services datoteci:

```
imap 143/tcp # IMAP
```

- Ovom linijom registramo servis IMAP-a

UW IMAP Server Konfiguracija

- Na od CARNeta podržanim Unix operacijskim sustavima IMAP ispravno radi "out-of-the-box"
- Uopće ne koristi konfiguracijsku datoteku
- Konfiguracija nije potrebna!

UW IMAP Server

Karakteristike

- Nije moguće čitati poštu od administratorskog korisničkog računa (`root`), odnosno računa sa UID-om 0
- Moguće je dodati podršku za SSL, čime se kriptira promet
- Moguće je dodati podršku i za Kerberos v5

UW IMAP Server

Vježba

- Prevesti izvorni kod u izvršni
- Instalirati IMAP na sustav
- Konfigurirati Inetd
- Konfigurirati TCP wrappers paket
- Provjeriti ispravnost rada telnetiranjem na port 143

UW IMAP Server

Literatura

- <http://www.imap.org> - glavna web stranica s najnovijim inačicama IMAP-a
- <ftp://ftp.cac.washington.edu/imap> – lokacija najnovije inačice IMAP-a
- <http://www.isi.edu/in-notes/rfc2060.txt> - specifikacija IMAP protokola
- BUILD, CONFIG - datoteke koje dolaze s paketom i u kojima je objašnjen postupak instalacije i konfiguracije

Mailing liste

Koncept

- Distribucija poruka elektroničke pošte između velikog broja korisnika
- Jednostavno rješenje bez posebnih mogućnosti je zapravo alias kod MTA (Sendmail)
- Alias nema napredne mogućnosti administriranja i drugih stvari koje pružaju programski paketi za mailing liste (MLM – *Mailing List Manager*)

Mailing liste

Koncept (2)

- MLM omogućavaju moderiranje poruka
- Najpoznatiji MLM danas su Listserv i Majordomo paketi
- Listserv se preporučuje za mailing liste sa vrlo velikim prometom (preko 200.000 poruka dnevno)
- CARNet podržava Majordomo paket

Mailing liste

Koncept (3)

- Više načina slanja poruka koje stižu na mailing listu:
 - trenutno slanje poruka
 - digest (slanje više poruka u jednoj – korisno kod mailing lista sa velikim brojem poruka po danu)
 - indexi (slanje samo podataka o autorima i naslovima poruka po danu)

Mailing liste

Koncept (4)

- Mogućnosti arhiviranja mailing lista
- Mogućnosti pretraživanja GET naredbom
- Pristup preko web sučelja (moguće je integrirati sa MLM)
- "Pametno" pregledavanje poruka da ne bi došlo do petlje ili ponavljanja poruka

Majordomo

Instalacija

- Dohvaćanje paketa (izvorni kod)
- Zadnja inačica uvijek dostupna na GreatCircle web poslužitelju
- Raspakiranje tar.gz arhive
- Sa IMAP paketom dolaze i poslužiteljski programi za POP, ali ih CARNet ne podržava/preporuča

Majordomo

Instalacija (2)

- Majordomo treba imati korisnički račun
- Obično se uzima majordomo i ista grupa
- Korisnik koji upravlja listama trebao bi biti isto u ovoj grupi, tada ne mora raditi su na majordomo korisnički račun
- Potrebno je odabrati direktorij za instalaciju (npr. /home/mlm)

Majordomo Instalacija (3)

- Potrebno je postaviti ispravnu lokaciju Perl interpretera i C prevodioca u `Makefile` datoteku
- Potrebno je postaviti lokaciju za manual, korisnika i prava pristupa
- Wrapper će biti pokrenut sa `setuid root` pravima



Majordomo Instalacija (4)

- Potrebno je napraviti `majordomo.cf` konfiguracijsku datoteku
- Prilikom prve instalacije preporučljivo je kopirati `sample.cf` u `majordomo.cf` datoteku koja se zatim može mijenjati po potrebama
- Konfiguracijska datoteka mora biti ispravna po Perl sintaksi



Majordomo Instalacija (5)

- U konfiguracijskoj datoteci potrebno je unijeti ispravne vrijednosti za:
 - `$whereami` – računalo na kojem je instalirano
 - `$whoami` – kako korisnici šalju zahtjeve
 - `$whoami_owner` – vlasnik liste
 - `$homedir`
 - `$listdir` – gdje su mailing liste
 - `$sendmail_command` – gdje je Sendmail



Majordomo Instalacija (6)

- Potrebno je prevesti wrapper program
- Ovo se izvodi naredbom:
`$ make wrapper`
- Sada se mogu instalirati Majordomo programi
- Ovo se izvodi naredbom:
`$ make install`



Majordomo Instalacija (7)

- Nakon što su instalirani Majordomo programi, potrebno je instalirati i njegov wrapper:
`$ make install-wrapper`
- Ovim postupcima završena je instalacija Majordoma, međutim potrebno je još postaviti konfiguraciju za Sendmail



Majordomo Instalacija (8)

- U alias datoteku od Sendmaila potrebno je dodati Majordomo aliase
- Potrebno je dodati aliase:
`majordomo: "|/home/mlm/wrapper \
majordomo"`
`owner-majordomo: bzdrnja`
`majordomo-owner: bzdrnja`



Majordomo Instalacija (9)

- Na kraju, da bismo provjerili je li konfiguracija Majordoma ispravna, to možemo napraviti s:

```
$ cd /home/mlm  
$ ./wrapper config-test
```

- Ovo je potrebno pokrenuti kao običan korisnik (ne kao administrator)
- Trebali bismo vidjeti ispravnu konfiguraciju Majordomo programa

Majordomo Provjera s listom

- Konfiguracija se može provjeriti i stvaranjem prazne datoteke "test" u direktoriju za liste i zatim zadavanjem komande lists:

```
$ touch /home/mlm/lists/test  
$ echo 'lists' | mail majordomo
```

- Ako sve radi ispravno, trebali bismo dobiti poruku od Majordomo programa

Majordomo Otvaranje nove liste

- Imena lista mogu imati bilo koje znakove iz skupa [a-z0-9_-]
- Ime liste može se sastojati od velikih i malih znakova
- Sva imena liste prilikom konfiguracije MORAJU biti upisana malim slovima OSIM za -l argument resend i majordomo programa!

Majordomo

Otvaranje nove liste (2)

- Da bi se otvorila nova lista prvo je potrebno napraviti praznu datoteku sa imenom liste u direktoriju za liste
- Pravila pristupa svim datotekama trebaju biti 664
- U istom direktoriju treba se nalaziti i .info datoteka sa kratkim opisom mailing liste za korisnike



Majordomo

Otvaranje nove liste (3)

- Konfiguracija glavnih parametara liste nalazi se u aliases datoteci Sendmaila
- Svaka lista treba imati barem sljedeće aliase:
 - test (alias same liste)
 - owner-test (vlasnik liste koji dobija poruke o greškama)
 - test-request (adresa za administrativne zahtjeve)
 - test-approval (adresa moderatora)



Majordomo

Otvaranje nove liste (4)

- Za sve aliase treba dodati pripadajuće opise u aliases datoteci Sendmaila
- U većini slučajeva odlazeće poruke predaju se resend programu koji hvata Majordomo komande
- Specijalne mogućnosti su arhiva i digest koje također treba specijalno definirati



Majordomo

Otvaranje nove liste (5)

- Tipični set aliasa je:

```
test: "/home/mlm/wrapper resend -l test
test-list"
test-list: :include:/home/mlm/lists/test
owner-test: bzdrnja
test-owner: bzdrnja
test-request: "/home/mlm/wrapper majordomo -
l test"
```

Majordomo

Otvaranje nove liste (6)

- Nakon unošenja aliasa u `/etc/aliases` datoteku potrebno je izvesti `newaliases`
- Sve datoteke Majordomo poslužitelja trebaju biti u vlasništvu korisnika majordomo i grupe majordomo
- Vlasnik i grupa trebaju imati pravo pisanja po svim datotekama i direktorijima

Majordomo

Administracija nove liste

- Nakon što su aliasi uneseni, potrebno je konfigurirati novu listu slanjem komande:

```
config test test.admin
```
- Ovo uzrokuje stvaranje početne konfiguracije za listu koja se šalje elektroničkom poštom natrag pošiljaocu
- Sada se može promijeniti zaporka i administrirati lista

Majordomo

Administracija nove liste (2)

- Odmah nakon otvaranja nove liste preporučuje se mijenjanje početne zaporka
- Početna zaporka napisana je u poruci koja se dobiva od Majordomo programa
- Zaporka se mijenja slanjem poruke elektroničke pošte sa sljedećim sadržajem:

```
passwd <lista> <stara_zaporka>  
<nova_zaporka>
```

Majordomo

Administriranje liste

- Dodavanje korisnika na listu ne zahtjeva akciju administratora
- Korisnik sam šalje poruku elektroničke pošte na adresu Majordomo programa
- Dvije mogućnosti

```
test-request@carnet.hr - Message:  
subscribe
```

```
majordomo@carnet.hr - Message:  
subscribe test
```

Majordomo

Intro datoteka

- Intro datoteka šalje se korisnicima koji zadaju intro ili subscribe komandu
- Nova intro datoteka postavlja se komandom:

```
newintro <lista> <zaporka>
```
- Nakon ove linije sav tekst do kraja stavlja se u intro datoteku

Majordomo

Info datoteka

- Info datoteka šalje se korisnicima koji zadaju info komandu
- Nova info datoteka postavlja se komandom:
`newinfo <lista> <zaporka>`
- Nakon ove linije sav tekst do kraja stavlja se u info datoteku

Majordomo

Podešavanje konfiguracije

- Konfiguracijsku datoteku moguće je dobiti i postaviti preko elektroničke pošte
`config <lista> <zaporka>`
- Ova naredba šalje korisniku konfiguracijsku datoteku sa ubačenim komentarima
- Zaporka može biti ona u datoteci `<lista>.passwd` ili administratorska zaporka iz konfiguracijske datoteke

Majordomo

Podešavanje konfiguracije (2)

- Nova konfiguracijska datoteka postavlja se naredbom:
`newconfig <lista> <zaporka>`
- Nakon ove linije sav tekst do kraja stavlja se u konfiguracijsku datoteku
- Konfiguracijska datoteka mora biti kompletna, kao ona dobivena u prethodnom koraku

Majordomo Sigurnost

- Ovakva postavka Majordomo programa nije sigurna
- Bilo koji korisnik na sustavu može mijenjati konfiguracijske datoteke Majordomo programa
- Promjena prava pristupa Majordomo direktorija iziskuje i promjenu konfiguracije Sendmaila!

Majordomo Vježba

- Instalirati Majordomo paket
- Napraviti sve konfiguracijske datoteke
- Provjeriti instalaciju
- Napraviti test mailing listu
- Dodati jednog korisnika na test mailing listu

Majordomo Literatura

- INSTALL.txt datoteka koja dolazi s Majordomo paketom
- <http://www.greatcircle.com/majordomo> - glavna web stranica Majordomo paketa
- <http://www.cis.ohio-state.edu/~barr/majordomo-faq.html> - FAQ

Sažetak Sendmail

- Build datoteka za prevođenje
- m4 prevodilac za konfiguracijsku datoteku
- Aliasi korisnika
- Relay
- Virtualni hostovi



Sažetak POP-3

- Qpopper – CARNetov izbor
- GNU autoconf paket
- Pokretanje iz Inetd-a
- Port 110
- Koristi .user.pop datoteke prilikom rada



Sažetak IMAP

- University Of Washington IMAPD
- Koristi se poseban direktorij za držanje korisničkih E-mail poruka
- Ne treba konfiguracija
- Pokreće se iz Inetd-a
- Port 143



Sažetak Majordomo

- Napisan u Perlu
- Integracija sa Sendmailom
- Administracija lista preko poruka elektroničke pošte

Dio II Apache Web poslužitelj i caching

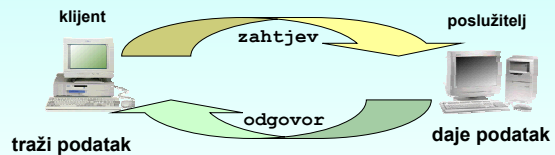
priređio Denis Stančer

Sadržaj (2. dan)

Koncept Weba	20 min
Anonimni FTP	160 min
- instalacija i standardna konfiguracija	30 min
- autentifikacija	30 min
- virtualni web poslužitelj	20 min
- logovi i tuning	40 min
- moduli i dodaci na osnovni poslužitelj	40 min
Caching	90 min
- koncept (proxy, cache, raspoloživi alati)	10 min
- Apache kao proxy cache	40 min
- Squid (instalacija, podešavanje)	40 min

Koncept Weba Model

- Poznati model klijent-poslužitelj



Koncept Weba HTTP protokol

- HyperText Transfer Protocol
- Opisan u RFC 1945
- Trenutna inačica je 1.1 (RFC 2068)
- Jezik kojim komuniciraju web poslužitelj i web preglednik [\[browser\]](#)
- Služi za razmjenu podataka [\[resources\]](#)
- Podrazumijevani port za HTTP je 80
- Zahtjevi su neovisni [\[stateless\]](#)

Koncept Weba HTTP protokol (2)

- HTTP upit se sastoji:
 - metode (velika slova)
 - zaglavnih polja [\[header fields\]](#)
 - praznog reda
- Metode: GET, HEAD, POST
- HTTP 1.0 definira 16 zaglavnih polja

Koncept Weba HTTP protokol (3)

- S klijentske strane se podrazumijevaju:
GET <URI> HTTP/1.1
Host: <ime_poslužitelja>
User-agent: <naziv_klijenta/x.xx>
- S poslužiteljske strane se podrazumijevaju:
HTTP/1.x <KÔD> <POJAŠNJENJE>
Server: <naziv_poslužitelja/x.xx>
Last-Modified: <ddd>, <dd> <MM> <YYYY>
HH:mm:ss GMT
Content-Type: <MIME_tip>

Koncept Weba HTTP protokol (4)

- Povratni kodovi:
 - 1xx razne obavijesti
 - 2xx neka vrsta uspjeha
 - 3xx preusmjerenje klijenta na drugi URL
 - 4xx greška na klijentskoj strani
 - 5xx greška na poslužiteljskoj strani
- Npr:
200 OK
404 Not Found

Koncept Weba HTTP 1.1 poboljšanja

- Brži odziv uporabom jedne TCP veze [[persistent connection](#)] što omogućuje slanje više zahtjeva i odgovora
- Brži odziv i ušteda u propusnosti podrškom za cache
- Brži odziv za dinamički generirane stranice uporabom komadnog pakiranja, što dozvoljava početak slanja odgovora prije nego se zna njegova duljina
- Štednja na IP adresama jer omogućava posluživanje web stranica za više domena s istog poslužitelja (jedne IP adrese)

Koncept Weba

HTTP 1.1 poboljšanja (2)

- Dodaje još 4 metode: PUT, DELETE, OPTIONS i TRACE
- Definiira 46 zaglavnih riječi i jednu obaveznu (Host:)

Koncept Weba

HTTP primjer

- Upit

```
$ telnet regoc.srce.hr 80
Trying 161.53.2.69...
Connected to regoc.srce.hr.
Escape character is '^]'.
GET /index.html HTTP/1.1
Host: regoc.srce.hr
User-Agent: By Hand/1.0
<prazan_red>
```

Koncept Weba

HTTP primjer (2)

- Odgovor

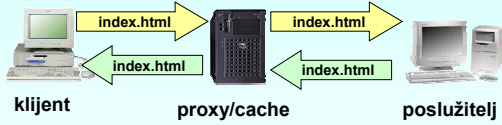
```
HTTP/1.1 200 OK
Date: Sun, 30 Sep 2001 15:19:19 GMT
Server: Apache/1.3.20 (Unix) PHP/4.0.6
Last-Modified: Wed, 12 Sep 2001 08:24:56 GMT
Content-Length: 5792
Content-Type: text/html
```

```
<html>
<head><title>SRCE</title>
...
```

Koncept Web

Model poslužitelj-proxy/cache-klijent

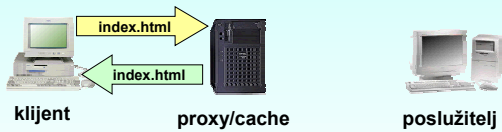
- Mnogi korisnici pregledavaju iste stranice
- Prvi put kada se zatraži dokument



Koncept Web

Model poslužitelj-proxy/cache-klijent (2)

- Svaki sljedeći put kada se zatraži dokument



Apache Instalacija

- Dohvat distribucije s URLa
<http://www.apache.org/dist/httpd/>
- Kraj posljednje inačice piše
Current release
- Moguće je snimiti
 - izvorni kod: za integraciju s raznim proširenjima (npr. PHP, Perl ...), složenija konfiguracija i potrebno prevođenje
 - binarnu distribuciju: samo osnovni poslužitelj, jednostavna instalacija

Apache Instalacija (2)

- Obavlja se u nekoliko koraka
 - moduli se kompiliraju
 - moduli se pretvaraju u *libraryje*
 - svi *libraryji* linkaju u jednu izvršnu datoteku
- Izuzetak su moduli koji su proglašeni dijeljenima (`mod_so`)

Apache Instalacija (3)

- Najjednostavnija instalacija:
`./configure`
- Nakon pripreme je potrebno kompilirati:
`make`
- Nakon 3-5 minuta je moguće instalirati:
`make install`
- Instalacija traje još kraće

Apache Instalacija (4)

- Prilikom pripreme Apache nas upozorava:
Configuring for Apache, Version 1.3.12
+ Warning: Configuring Apache with **default settings**.
+ This is probably **not** what you really want.
+ Please read the **README.configure** and **INSTALL** files
+ first or at least run '`./configure --help`' for
+ a compact summary of available options.
- Apache omogućava detaljnu kontrolu nad pripremom i na taj način omogućava fino podešavanje poslužitelja

Apache Instalacija (5)

- Prilikom instalacije Apache rasporedi svoje datoteke (izvršne, konfiguracijske, logove ...) u razne direktorije. Gdje?

```
# ./configure --show-layout
```

- Sve to možemo promijeniti:

```
--sysconfdir=<dir>   konfiguracijske datoteke
--htdocsdir=<dir>    HTML dokumenti
--logfiledir=<dir>   log datoteke
--bindir=<dir>       izvršne datoteke
```

- Detalji:

```
# ./configure --help
```

Apache Konfiguracija

- U direktoriju `/usr/local/apache/conf` se nalazi glavna (i jedina) konfiguracijska datoteka `httpd.conf`
- Potrebno je postaviti neke parametre prije pokretanja samog poslužitelja

Apache Konfiguracija (2)

- Obavezno provjeriti i promijeniti ako je potrebno:

Port	port na kojemu poslužitelj "sluša" [80]
User	korisničko ime poslužitelja [apache]
Group	korisnička grupa poslužitelja [apache]
ServerAdmin	E-mail adresa administratora
ServerName	puno (FQDN) ime poslužitelja

Apache Konfiguracija (3)

- Detaljnije podešavanje
- DocumentRoot direktorij HTML dokumenata
[`/usr/local/apache/htdocs`]
- UserDir direktorij u kojemu su osobne stranice
svakog korisnika [`public_html`]
- DirectoryIndex naziv defaultne datoteke koja se
prikazuje za URLove koji završavaju s /
[`index.html`] (možda dodati `index.htm`)
- AccessFileName naziv datoteke u kojoj se nalaze podaci potrebni
za kontrolu pristupa [`.htaccess`]
- CustomLog datoteka i format zapisa pristupa poslužitelju
[`/usr/local/apache/logs/access_log`
`common`] (možda promijeniti u `combined`)

Apache Pokretanje i zaustavljanje

- Pokretanje
`/usr/local/apache/bin/apachectl start`
- Zaustavljanje
`/usr/local/apache/bin/apachectl stop`
- Zaustavljanje i ponovno pokretanje
`/usr/local/apache/bin/apachectl restart`
- Ponovno pokretanje ili samo pokretanje ako ne radi
`/usr/local/apache/bin/apachectl graceful`

Apache Pokretanje i zaustavljanje (2)

- Najzanimljivije opcije za `httpd`:
 - d `<put>` alternativni korijen poslužitelja
 - f `<datoteka>` alternativna konfiguracijska datoteka
 - T ispitaj je li konfiguracijska datoteka u redu
 - t kao -T uz provjeru svakog `DocumentRoot` direktorija (da li je direktorij i da li postoji)

Apache Kontrola pristupa

- Pristup određenim dijelovima weba se može kontrolirati
 - iz središnje konfiguracijske datoteke
 - iz lokalnih (`.htaccess`) konfiguracijskih datoteka (ako je to omogućeno u središnjoj konfiguracijskoj datoteci)
- U oba slučaja se koristi jednaka sintaksa, osim što se u središnjoj datoteci mora navesti direktorij (`<Directory>`)
- Za lokalne datoteke potrebno je u središnjoj konfiguracijskoj datoteci naći `<Directory "/usr/local/apache/htdocs">`:

```
AllowOverride None      =>
AllowOverride All
```

Apache Kontrola pristupa (2)

- Autentifikacija putem korisničkog imena i lozinke:

```
AuthType Basic
AuthName "<naslov>"
AuthUserFile <datoteka_s_lozinkama>
Require valid-user
```
- Uputno je sve datoteke za kontrolu pristupa nazivati `.ht*` jer ih poslužitelj ne prikazuje

```
<Files ~ "^\.ht"> Order allow,deny
Deny from all </Files>
```
- Lozinke se dodjeljuju putem programa `/usr/local/apache/bin/htpasswd`

Apache Kontrola pristupa (3)

- Primjer `/usr/local/apache/htdocs/web1/.htaccess`:

```
AuthType Basic
AuthName "Restricted Directory"
AuthUserFile /usr/local/apache/htdocs/web1/.htusers
Require valid-user
```
- Dodijelimo lozinke (`-c` ako datoteka ne postoji)

```
cd /usr/local/apache/htdocs/web1
/usr/local/apache/bin/htpasswd -c -b .htusers user1
pwdABC1
Adding password for user user1
/usr/local/apache/bin/htpasswd -b .htusers user2
pwdABC2
Adding password for user user2
```

Apache Kontrola pristupa (4)

- Autentifikacija putem korisničkog imena i lozinke te pripadnosti grupi:

```
AuthType Basic
AuthName "<naslov>"
AuthUserFile <datoteka_s_lozinkama>
AuthGroupFile <datoteka_s_grupama>
Require Group <grupa>
```



Apache Kontrola pristupa (5)

- Primjer /usr/local/apache/htdocs/web2/.htaccess:

```
AuthType Basic
AuthName "Restricted Directory"
AuthUserFile /usr/local/apache/htdocs/web2/.htusers
AuthGroupFile /usr/local/apache/htdocs/web2/.htgroups
Require group admin
```

- Stvorimo /usr/local/apache/htdocs/web2/.htgroups
admin: user1
- Ponovimo dodjelu lozinke za user1 i user2



Apache Kontrola pristupa (6)

- Autentifikacija putem IP adrese ili imena računala klijenta:

```
Order deny,allow
Deny from all
Allow from adresa
```

- Ako adresa nije u popisu, javi se greška 403

Forbidden:

```
You don't have permission to access /web3 on this
server
```



Apache

Kontrola pristupa (7)

- Autentifikacija putem IP adrese ili imena računala klijenta i para korisničko ime/lozinka:

```
Order deny, allow
Deny from all
Allow from adresa
AuthType Basic
AuthName "<naslov>"
AuthUserFile <datoteka_s_lozinkama>
Require valid-user
Satisfy any
```

Apache

Virtualni poslužitelji

- Nekoliko načina
 - više IP adresa za više imena (ili domena)
 - jedna IP adresa za više imena (ili domena)
 - kombinacija gore navedenog
- Najčešće korišteno rješenje
 - jedna IP adresa za više imena (ili domena)

Apache

Virtualni poslužitelji (2)

- U `httpd.conf`

```
<VirtualHost new-name.dot.com>
    direktive
</VirtualHost>
```
- Direktive mogu sve koje se koriste kod konfiguracije "normalnog" poslužitelja

Apache Virtualni poslužitelji (3)

- Što nam sve treba:
 - nova direktiva `VirtualHost` u `httpd.conf`
 - novo ime registrirano u DNS-u kao alias na postojeći poslužitelj
 - novi direktorij u kojemu će biti dokumenti
 - novi direktorij u kojemu će biti logovi

Apache Virtualni poslužitelji (4)

- U `httpd.conf` (obično se pišu na kraju):

```
<VirtualHost virtual03.unix.srce.hr>
ServerAdmin webmaster@tecaj03.unix.srce.hr
DocumentRoot /usr/local/apache/htdocs/virtual
ServerName virtual03.unix.srce.hr
ErrorLog /usr/local/apache/logs/v_error_log
CustomLog /usr/local/apache/logs/v_access_log
common
</VirtualHost>
```

Apache Logovi

- U `httpd.conf` se definira nekoliko formata zapisa
`LogFormat "%h %l %u %t \"%r\" %>s %b" common`
- Nakon toga se uz određenu log datoteku veže određeni format
`CustomLog /usr/local/apache/logs/access_log common`
- Greške se zapisuju u (definirano s `ErrorLog`)
`/usr/local/apache/logs/error_log`
- Formati se definiraju:
`LogFormat "definicija" naziv`
`LogFormat "%h %l %u %t \"%r\" %>s %b" common`

Apache Logovi (2)

- Pojašnjenje:

- %h remote host
- %l remote logname (from identd)
- %u remote user (authenticated)
- %t time
- %r first line of request
- %s original request status
- %>s last request status (if redirected)
- %b bytes sent

Apache Logovi (3)

- Ostali korisni formati:

- %a remote IP address
- %{FOO}e contents of environment varibale FOO
- %f filename
- %H the request protocol
- %{FOO}i contents of FOO header sent to server
- %q query string

Apache Tuning

- Apache je u podrazumijevanoj konfiguraciji postavljen da radi prvo sigurno pa tek onda brzo
- Web poslužitelj mora imati dovoljno RAM-a
- U konfiguraciji s dozvolama pristupa koristiti IP adrese radi izbjegavanja nepotrebnih DNS upita

Apache Tuning (2)

- Prilagoditi direktive u `httpd.conf`:
 - isključiti (po defaultu već je isključena):
`HostNameLookups off`
 - za web s puno posjeta povećati na 250 (ili više):
`MaxClients 250`
- Ne pokretati poslužitelj iz `tcpd` wrappera
- Ne pokretati X Windowse uz poslužitelj
- Zabraniti SSI
- Ako ima puno CGI skripti, koristiti `mod_perl`



Apache Tuning (3)

- Najčešći problem, npr. za:

```
DocumentRoot /www/htdocs
<Directory />
AllowOverride all
</Directory>
```

je zatražen dokument `/index.html`. Apache pokušava otvoriti `/.htaccess`, `/www/.htaccess` i `/www/htdocs/.htaccess` što opterećuje poslužitelja



Apache Tuning (4)

- Rješenje:

```
DocumentRoot /www/htdocs
<Directory />
AllowOverride None
</Directory>
<Directory /www/htdocs>
AllowOverride all
</Directory>
```



Apache Tuning (5)

- Performanse poslužitelja se najbolje popravljaju isključivanjem/uključivanjem modula prilikom kompilacije
- Pomoću `./configure --help` se dobije popis svih modula koji dolaze s poslužiteljem

Apache Sigurni Web

- Apache ne dolazi sa SSL (port 443) podrškom zbog zakonskih ograničenja vezanih uz enkripciju
- SSL podrška se dodaje prilikom kompiliranja (20 min):

```
Tar xzf openssl-x.xx.xx.tar.gz
cd openssl-x.xx.xx
./config no-idea -fPIC
make
make test
make install
```

Apache Sigurni Web (2)

- Konfiguracija `mod_ssl`:

```
tar xzf mod_ssl-x.x.x-x.x.xx.tar.gz
cd mod_ssl-x.x.x-x.x.xx
./configure --withapache=../apache_x.x.xx/
```
- Konfiguracija Apache poslužitelja:

```
cd ../apache_x.x.xx
SSL_BASE=../open_ssl-x.x.x ./configure --enable-module=ssl [drugi_moduli]
```
- Kompiliranje Apache poslužitelja (priprema 3-5 min):

```
make
```

Apache Sigurni Web (3)

- Izrada (generičkog) certifikata (3 min):
`make certificate`
- Instaliranje (3-5 min):
`make install`
- Skripta `apachectl` sada ima dodatni argument `startssl` kojim se pokreće SSL poslužitelj:
`/usr/local/apache/bin/apachectl startssl`

Apache Moduli

- Apache dolazi s 38 modula
- Uglavnom su to moduli za:
 - autentifikaciju
 - proxy
 - radnje vezane uz datoteke na disku
 - logove

Apache Moduli (2)

```
[access=yes      actions=yes      alias=yes       ]
[asis=yes        auth_anon=no     auth_dbm=no    ]
[auth_db=no      auth_digest=no  auth=yes       ]
[autoindex=yes   cern_meta=no    cgi=yes        ]
[digest=no       dir=yes         env=yes        ]
[example=no      expires=no      headers=no     ]
[imap=yes        include=yes     info=no        ]
[log_agent=no    log_config=yes  log_referer=no]
[mime_magic=no   mime=yes        mmap_static=no]
[negotiation=yes proxy=no        rewrite=no     ]
[setenvif=yes    so=no          spelling=no    ]
[status=yes      unique_id=no    userdir=yes    ]
[usertrack=no    vhost_alias=no ]
```

Apache Moduli (3)

cgi=yes izvršavanje CGI skripti
dir=yes posluživanje URL-ova s posljednjim /
env=yes prosljeđivanje ENV varijabli CGI skriptama
imap=yes podrška za .map datoteke (zamjena za
imagemap CGI program)
include=yes podrška za SSI
log_config=yes podrška za Common Log Format
mime_magic=no čita prvih nekoliko byteova kako bi se
odredio tip datoteke (poput file
programa)
proxy=no pretvara Apache i u proxy-cache poslužitelj

Apache Moduli (4)

rewrite=no podrška prepisivanju URL-ova (kod DNS
aliasa)
so=no podrška za dijeljene datoteke ([shared
objects])
speling=no podrška za ispravljanje URL-ova (velika i
mala slova i do jedne pogreške u URL-u)
userdir=yes omogućuje podršku za osobne URL-ove
oblika `http://site.com/~user/`

Apache Moduli (5)

- Da bi se neki modul uključio u izvršni kod potrebno je
./configure dati argument
`--enable-module=<ime>`
gdje je <ime> jedan od naziva modula:
`--enable-module=proxy`
- Ako je modul dijeljeni, treba još dodati
`enable-shared npr:`
`--enable-module=proxy --enable-shared=proxy`

Apache Moduli (6)

- Najpoznatija proširenja putem vanjskih modula:
 - Perl (`mod_perl` – <http://perl.apache.org/>)
 - SSL (`mod_ssl` – <http://www.modssl.org/>)
 - FrontPage dodaci
- Svaki od ovih modula je potrebno kompilirati

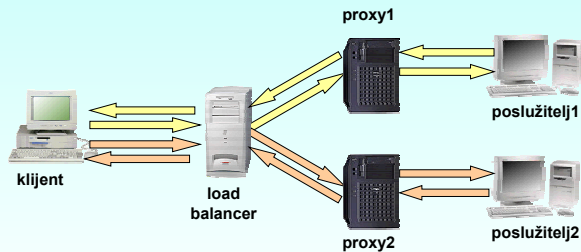
Apache Dodaci

- Najpoznatiji dodaci na Apache:
 - PHP (Preprocessed HTML Pages) moćan skriptni jezik koji se interpretira prije nego se stranica pošalje klijentu (<http://www.php.net/>)
 - MySQL baza podataka usko vezana s PHP-om (<http://www.mysql.com/>)
 - sve što može Perl (putem `mod_perl-a`)

Cache Proxy i cache

- Proxy
 - poslanik koji radi nešto u tuđe ime
- Cache
 - odlagalište stvari i vrijednosti koje su trenutno suviše ili neugodne za nositi
- Danas kada se govori o proxyju ili o cachingu, onda se prešutno misli o paru proxy/cache

Cache Caching u CARNetu



Cache Apache

- Apache dolazi s modulom `mod_proxy` koji omogućuje:
 - standardni proxy/cache promet
 - prosjeđivanje zahtjeva drugim proxy/cache poslužiteljima
 - blokiranje određenih (IP) adresa za proxy promet
 - blokiranje zahtjeva za proxy prometom s određenih (IP) adresa

Cache Apache (2)

- Da bi se omogućila podrška za proxy, potrebno je ponovo kompilirati poslužitelj s novom konfiguracijom:

```
# ./configure --enable-module=proxy
# make
# make install
```

Cache Apache (3)

- Da bi se proxy aktivirao, potrebno je u središnjoj konfiguracijskoj datoteci naći i odkomentirati retke:

```
<IfModule mod_proxy.c>
ProxyRequests On
ProxyVia On
CacheRoot /usr/local/apache/cache
CacheSize 5
CacheGoInterval 4
CacheMaxExpire 24
CacheLastModifiedFactor 0.1
CacheDefaultExpire 1
NoCache .hr
</IfModule>
```

Cache Squid instalacija

- Snimanje Squida:
<ftp://www.squid-cache.org/pub/>
- Najjednostavnija instalacija:

```
# tar xzf squid-2.x.RELEASE-src.tar.gz; cd ...
# ./configure
```
- Nakon 2-3 minute je potrebno kompilirati:

```
# make
```
- Nakon 3-5 minuta je moguće instalirati:

```
# make install
```
- Instalacija traje još kraće

Cache Squid podešavanje

- Nakon instalacije se u squid.conf datoteci postavi:
 - http_port port na koji klijenti šalju svoje zahtjeve
 - lcp_port port na kojemu međusobno komunicira više poslužitelja
 - no_cache zabranjuje ili dozvoljava pohranu dokumenata koji u svom URL-u imaju imenovani uzorak, npr:

```
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
```

Cache

Squid podešavanje (2)

- Pokretanje
 - squid -z (prvi put)
 - squid
- Mogući su
- Zaustavljanje
 - squid -k shutdown
 - squid -k kill
- Zaustavljanje i ponovo pokretanje
 - squid -k reconfigure

Sažetak

- Koncept Weba
 - HTTP
- Apache
 - instalacija i konfiguracija
 - autentifikacija
 - virtualni poslužitelji
 - logovi
 - tuning
 - SSL
 - moduli i dodaci
- Cache
 - Apache
 - Squid
 - *instalacija
 - *konfiguracija

Literatura

- Apache 1.3 dokumentacija
- Apache FAQ
- Squid 2.4s4 dokumentacija
- Squid FAQ
- James Marshal: "HTTP Made Really Easy"
- Brendan Cassida: "Apache tutorial"

Dio III

Imenički servisi, FTP, News, sigurnost i zaštita privatnosti

priređio Dinko Korunić

Sadržaj (3. dan)

Imenički servisi	50 min
- koncept imeničkih servisa u CARNetu	10 min
- LDAP - koncept/podatkovni model	20 min
- LDAP - instalacija, konfiguracija, uporaba	20 min
Anonimni FTP	60 min
- instalacija, konfiguracija, uporaba	
IRC	30 min
- instalacija, konfiguracija, uporaba	
News	30 min
- instalacija, konfiguracija, uporaba	
Sigurnost i zaštita privatnosti	80 min
- Ssh - instalacija, konfiguracija, uporaba	30 min
- Skey - instalacija, konfiguracija, uporaba	20 min
- Pgp - instalacija, konfiguracija, uporaba	30 min

Imenički servisi

Općenito

- **LDAP** (Lightweight Directory Access Protocol) je klijent-poslužitelj protokol za pristup imeničkom servisu ([directory service](#)) inicijalno zamišljen kao frontend za **X.500**, ali može služiti i za druge imeničke servise
- **WHOIS++** je jednostavni tekstualni upit za pretraživanjem preko kojeg se može konstruirati dijeljeni imenik ([distributed directory](#)) – specificiran u RFC 1835
- Za izmjenu podatka između WHOIS++ i LDAP imeničkih servisa (atribut-vrijednost bazirani) služi **CIP** (Common Indexing Protocol)

Imenički servisi

WHOIS++ - osnove

- Originalni WHOIS model 1985 – imenički servis sa samo jednom bazom
- WHOIS++ - više baza povezanih **indeksirajućim** servisom
- Sadrži niz **individualnih zapisa** koji sadržavaju aktualne informacije
- Zapisi podijeljeni u više tipova (npr. Person, Domain, itd.)
- Za svaki tip postoji definiran različit tip atributa koje zapis može poprimiti – set atributa je predložak (**template**) identičan klasi objekta u X.500



Imenički servisi

WHOIS++ - osnove (2)

- Primjer zapisa temeljenog na predlošku "osoba":

```
Template: Person
First-Name: Peter
Last-Name: Jurg
Favourite-Drink: Milk
```

- Zapis temeljen na predlošku "domena":

```
Template: Domain
Domain-Name: stratix.nl
Contact-Name: Mark Jacobs
```

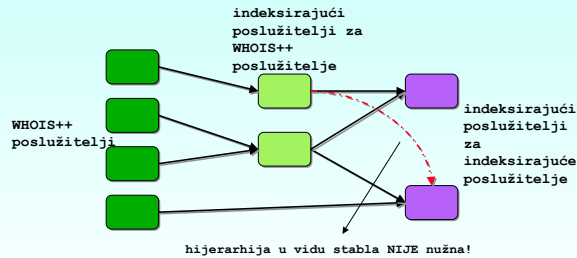


Imenički servisi

WHOIS++ - osnove (3)

- WHOIS++ je bitno različit od X.500 – ne definira hijerarhijsku imeničku strukturu već prostor za indeksirajuće poslužitelje
- Za svaki WHOIS++ poslužitelj postoji barem jedan indeksirajući poslužitelj koji drži informacije o sadržaju tog poslužitelja u posebnom formatu
- Taj format je **centroid** i drži informacije o predlošcima i atributima te listi vrijednosti koje se mogu pojaviti za bilo koji atribut, kao i pokazivač na WHOIS++ poslužitelj od kojega dolaze početne informacije
- Servis za pretraživanje klijent pretražuje radi stvaranja listi podataka

Imenički servisi WHOIS++ - dijagram hijerarhije



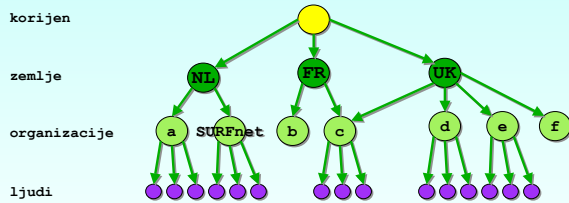
Imenički servisi X.500 - osnove

- X.500 je standard za imeničke servise kompanije ITU (International Telecommunications Union)
- X.500 koristi **distribuirani pristup** za stvaranje globalnog imeničkog servisa:
 - lokalne informacije o organizacijama se čuvaju lokalno u DSA (Directory System Agent)
 - moguć odnos: jedna organizacija u više DSA, više organizacija u jednom DSA

Imenički servisi X.500 – osnove (2)

- DSA je baza podataka:
 - sadrži informacije u strukturi opisanoj X.500 informacijskim modelom
 - ima mogućnost razmjene (ako je potrebno!) s drugim DSA preko DSP (Directory System Protocol)
 - svi DSA u X.500 imeničkom servisu su povezani u predefiniрани model DIT (Directory Information Tree) – hijerarhijski strukturiran, ima čvor i listove: zemlje, organizacije, pojedince

Imenički servisi X.500 – dijagram hijerarhije



napomena: DNS – LDAP korelacije

Imenički servisi X.500 – osnove (3)

- Svaki DSA drži dio **globalnog imenika** te preko DIT strukture može pronaći koji DSA drži određeni dio imenika
- **Informacijski model:**
 - sve informacije u imeniku su **zapisi (entries)**
 - svaki od njih pripada u barem jednu **klasu objekata (object class)**
 - stvarna informacija u zapisu je određena sa tzv. **atributima** koji su sadržani u tom zapisu

Imenički servisi X.500 – osnove (4)

- **Informacijski model (nastavak)**
 - **klase objekata** (kojima zapis pripada) određuju kakve **tipove atributa** može imati zapis
 - odnosno kakve informacije su specifične za tu klasu objekata
 - atribut može imati **jednu i više vrijednosti**
 - barem jedna vrijednost atributa se koristi kao **ime cijelog zapisa**
 - ime zapisa mora biti **jedinstveno** u toj grani DIT

Imenički servisi

LDAP – osnove

- LDAP služi za pristup X.500 baziranim imeničkim servisima preko TCP/IP
- Detalji definirani u **RFC2251** (LDAPv3)
- Za izgradnju hijerarhijskog stabla može se koristiti:
 - opisani geografsko/organizacijski model
 - DNS model – LDAP poslužitelj je moguće naći koristeći DNS
- Kontrola atributa (dozvoljeni, obvezni) preko specijalnog atributa: **objectClass** (definira shemu koja će se poštovati)



Imenički servisi

LDAP – osnove (2)

- Svaki zapis ima jedinstveno ime **DN** (Distinguished Name) = ime samog zapisa **RDN** (Relative Distinguished Name) zajedno sa ostalim zapisima:
 - RDN: uid=miro@regoc.srce.hr
 - DN: uid=miro@regoc.srce.hr, dc=srce, dc=hr
 - ovaj način određivanja je specificiran u RFC2253
- Informacije/zapisi/itd. mogu biti:
 - dodane, promijenjene, obrisane, pročitane



Imenički servisi

LDAP – osnove (3)

- 1990. – pojava LDAPv3:
 - "jaka" autentifikacija preko SASL
 - integritet i zaštita podataka preko TLS (SSL)
 - internacionalizacija – Unicode
 - refereri i sl.
 - dodatne ekstenzije, otkrivanje šeme i sl.
- Istovremena podrška za LDAPv2 i LDAPv3 se **ne** preporuča!

Imenički servisi LDAP i WHOIS - sažetak

- WHOIS++
 - više baza povezanih **indeksirajućim** servisom odnosno poslužiteljem
 - **za svaki** poslužitelj postoji još jedan indeksirajući
 - indeksirajući podaci u **centroidu** koji može sadržavati pokazivače na druge poslužitelje ili podatke
 - hijerarhija **nije nužna**
- LDAP
 - **nužna** hijerarhija, **distribuirani** pristup
 - **frontend** za X.500
 - čvor, listovi: **globalni imenik**

Imenički servisi OpenLDAP - općenito

- OpenLDAP je slobodna implementacija LDAP poslužitelja:
 - **slapd** – samostojeći LDAP poslužitelj
 - podržava LDAPv2 i LDAPv3
 - IPv4 i IPv6
 - SASL – DIGEST-MD5, GSSAPI, EXTERNAL
 - TLS/SSL
 - Berkeley DB ili GDBM
 - threading, replikacija, generički moduli, više baza odjednom
 - **slurpd** – samostojeći LDAP replikacijski poslužitelj
- CARNet paket u izradi, izvorni kod se nalazi na <http://www.openldap.org>

Imenički servisi OpenLDAP – slapd.conf

- U priloženi primjer dodati:

```
include /staza/cosine.schema
include /staza/inetorgperson.schema
```
- Ovisno o korištenoj bazi podataka:

```
moduleload back_idbm.la
```
- Podesiti suffix:

```
dc=srce, dc=hr
```
- Administrativni DN, lozinke kao i indeksiranje:

```
rootdn ([BN])
rootpw lozinka
index objectClass,uid eq
```

Imenički servisi

OpenLDAP – postavljanje

- Pokrene se slapd
- Dodaju se informacije o organizaciji sa:

```
ldapadd -x -D "[BN]" -W -f ime_datoteke.ldif
```
- Datoteka srce.ldif:

```
dn: dc=srce, dc=hr
dc: srce
o: University Computing Center - SRCE
objectclass: organization
objectclass: dcObject
```

Imenički servisi

OpenLDAP – postavljanje (2)

- Pomoću iste naredbe dodaju se i podaci za pretraživanje:

```
dn: uid=miro@regoc.srce.hr, dc=srce, dc=hr
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
cn: Miroslav Milinovic
sn: Milinovic
ou: SRCE
mail: miro@regoc.srce.hr
```

Imenički servisi

OpenLDAP – postavljanje (3)

- **dn** = distinguished name
- **cn** = common name
- **rdn** = relative distinguished name
napomena: *rdn* tvori *dn* zajedno sa svim svojim precima
- **sn** = surname
- **ou** = organisation unit
- **c** = country
- **o** = organisation

FTP

Uvod

- FTP protokol – definiran u RFC959 i RFC1579
- Inicijalni RFC vrlo rano definiran (RFC959 sredinom 1985. koji je nadgradio dotadašnji 765)
- Komunikacija poslužitelj – klijent se odvija pomoću FTP naredbi uz odgovarajuće parametre:
 - USER, PASS, ACCT, CWD, CDUP, SMNT, QUIT, REIN, PORT, PASV, itd.
- Protokol ima niz propusta:
 - autorizacija čistim tekstom
 - mogući "man-in-the-middle" napadi jer nema enkripcije veze

FTP

Uvod (2)

- Tipični način rada:
 - poslužitelj sluša na određenom portu
 - korisnik inicira **full-duplex** vezu te se klijent i poslužitelj međusobno spajaju prema konvencijama **telnet** protokola i ostvaruju **kontrolnu vezu**
 - korisnik sluša na vlastitom FTP-**podatkovnom** portu, a poslužitelj pri prijenosu inicira vezu sa vlastitog podatkovnog porta na korisnikov
 - pri završetku prvo se zatvara podatkovna veza, a zatim i kontrolna

FTP

Osnovna sigurnost

- Sve lozinke se prenose u vidu **čistog teksta**
- Moguće rješenje: preko korištenja PAM modula (npr. S/Key) ili već gotove S/Key biblioteke
- Danas se FTP protokol **sve manje koristi**
- Uspješno ga zamjenjuju (u općem slučaju)
 - klijenti: SFTP (SSH2), Scp (SSH1 i SSH2), Nc
 - protokoli: HTTP, HTTPS ...
- Ostaje slučaj potrebe **anonimnih FTP poslužitelja** – lozinka je E-mail adresa, login je "ftp" ili "anonymous"

FTP

Wuftp - uvod

- Wuftp spada među najraširenije i najpoznatije FTP poslužitelje uz Proftpd
- Dostupan na adresi <http://www.wuftp.org>
- Wuftp dodaje niz funkcionalnosti osnovnom protokolu:
 - logiranje prijenosa i naredbi, kompresiranje i arhiviranje u letu, klase korisnika i limiti na klase, guest korisnici, aliasovi, virtualni poslužitelji
- CARNet Debian paket – na [ftp://ftp.carnet.hr/pub/packages/...](ftp://ftp.carnet.hr/pub/packages/)

FTP

Wuftp - osnovna konfiguracija

- **ftppass** – opće konfiguriranje poslužitelja:
 - određivanje pristupa (klasa):

```
class all real *
```
 - ponašanje klase:

```
limit all 32 Any /usr/local/etc/msg.dead
```
 - ovlasti klase:

```
delete no guest,anonymous
```
 - ponašanja anonimnog poslužitelja:

```
passwd-check rfc822 enforce
```



FTP

Wuftp - osnovna konfiguracija (2)

- **ftppass** (nastavak):
 - opće ponašanje poslužitelja:

```
message /welcome.msg login  
compress yes all  
noretrieve .notar core /etc /bin /dev /usr  
/incoming
```
 - logiranje

```
log commands real
```
 - mogućnosti "upload" direktorija:

```
upload /home/ftp * no
```



FTP

Wuftpd - osnovna konfiguracija (3)

- **ftpusers**
 - **zabrana** pristupa poslužitelju korisnicima
 - zabranjeni korisnici su slijedno navedeni (najčešće root, daemon, nobody, bin, sys, itd.)
- **ftphosts**
 - dozvola ili zabrana pristupa korisnicima i/ili poslužiteljima
 - ključne riječi allow/deny i hostmaske

FTP

Wuftpd - osnovna konfiguracija (4)

- **ftpconversions**
 - popisi konverzija između datoteka koje Ftpd poznaje i njihovi atributi
 - datoteka koju u većini slučajeva ne treba konfigurirati:

```
..gz: : /bin/gzip -cd
%s:T_REG|T_ASCII:O_UNCOMPRESS:GUNZIP
: : /bin/gzip -9 -c %s:T_REG:O_COMPRESS:GZIP
: :
..tar:/bin/tar -c -f - %s:T_REG|T_DIR:O_TAR:TAR
```

FTP

Wuftpd - napredno konfiguriranje

- **ftpservers**
 - datoteka koja se brine za **virtual hosting**, odnosno tzv. virtualne poslužitelje
 - slušanje više mrežnih interfaceova, konfiguracijske datoteke su svaka u **zasebnom** direktoriju:

```
10.196.145.10 /etc/ftpd/ftpd1/
10.196.145.200 /etc/ftpd/ftpd2/
neka.domena INTERNAL
```
 - ključna riječ INTERNAL - glavna konfiguracija

FTP

Wuftp - anonimni poslužitelj

- Wuftp pruža tri moguće usluge:

- anonimni FTP

- login = anonymous/ftp
- nepostojeći korisnik
- home direktorij mu je najčešće ~ftp

- guest FTP – login = guest

- stvarni korisnik
- ima vlastiti direktorij
- u `chroot()` okruženju

- stvarni korisnici

- imaju vlastite home direktorije, itd.

FTP

Wuftp - postavljanje anonFTP

- Kreiranje korisnika i direktorija:

- stvoriti korisnika ftp i staviti ga u kakvu zasebnu grupu

- korisnička lozinka treba biti nevaljana (ili zaključan account):

```
ftp:*:400:400:Anonymous FTP:/home/ftp:/bin/true
```

- napraviti direktorij ~ftp čiji je isključivi vlasnik root, a grupa ona od samog ftp korisnika

- dozvole za direktorij trebaju biti 555 (rx, ne w)

FTP

Wuftp - postavljanje anonFTP (2)

- Stvaranje izvršnih datoteka:

- stvoriti ~ftp/bin; vlasnik root, mod 111 = x

- kopirati ls u ~ftp/bin (po mogućnosti statički!), opet sa dozvolama 111

- svi dodatni programi tipa tar i slični, trebaju također biti identično konfigurirani

- najčešće se dodatno stavljaju gzip, tar, uncompress, itd.

- ako nisu statički linkani potrebno je iskopirati i nužne biblioteke rutina (ldd)

FTP

Wuftp - postavljanje anonFTP (3)

- Priređivanje sistemskih konfiguracijskih datoteka:
 - napraviti ~ftp/etc direktorij
 - napraviti datoteke passwd i group iz početka (ne kopirati postojeće!) s dozvolama 444 – najčešće sadržavaju samo root, daemon, uucp i ftp korisnike, služe za ispis ls naredbe, shadow nije potreban jer sve lozinke trebaju biti obrisane ili zaključane (najčešće zvjezdica umjesto lozinke)

FTP

Wuftp - postavljanje anonFTP (4)

- Stavljanje sadržaja:
 - napraviti direktorij ~ftp/pub; vlasnik je ftp administrator, a dozvole su 555 (preporučljivije: 2555 – setgroupid)
 - svi direktoriji ispod također trebaju biti isti (rekurzivno)
 - niti jedan direktorij ili datoteka ne smiju biti vlasništvo korisnika ftp
 - potrebno je zabraniti chmod, delete, overwrite, rename, chmod i umask naredbe za anonymous

FTP

Wuftp - postavljanje anonFTP (5)

- upload direktorij
 - mjesto na kojem korisnici anonimnog ftp poslužitelja mogu ostavljati datoteke
 - ~ftp/incoming direktorij, vlasnik root, s dozvolama 733
- ```
upload /var/spool/ftp * no
upload /var/spool/ftp /incoming yes ftp
staff 0600 nodirs
path-filter anonymous /etc/path.msg ^[-A-Za-z0-9\._]*$ ^\.\ ^-
```

---

---

---

---

---

---

---

---

## FTP

### Wuftp - postavljanje anonFTP (6)

- Biblioteke rutina i ostale Solaris specifičnosti:
  - direktoriji ~ftp/usr i ~ftp/usr/lib (root, 555)
  - snimiti libc.so.\* i libdl.so.\* u ~ftp/usr/lib (root, 555)
  - snimiti ld.so (dinamički loader) u ~ftp/usr/lib (root, 555)
  - napraviti ~ftp/dev direktorij (root, 111) i ondje stvoriti zero uređaj  
mknod zero c 3 12
  - napraviti direktorij ~ftp/usr/share/lib/zoneinfo i snimiti ondje  
/usr/share/lib/zoneinfo/localtime
  - uključiti sistemsko logiranje u /etc/syslog.conf:  
daemon.\* /var/adm/daemonlog

---

---

---

---

---

---

---

---

## FTP

### Wuftp - dodatna sigurnost

- Dodatna sigurnost:
  - touch ~ftp/.rhosts
  - touch ~ftp/.forward
  - chmod 400 ~ftp/.rhosts
  - chmod 400 ~ftp/.forward
- Opcionalna mogućnost je i korištenje FTP poslužitelja pod **chroot()** okolinom – preporučljivo jer smanjuje opasnost od provale cijelog stroja ako dođe do kompromitiranosti Wuftp
- Za testiranje Wuftp može se koristiti debugiranje preko **-d** i/ili **-v** opcija prosljeđenih Ftpd

---

---

---

---

---

---

---

---

## FTP

### Wuftp - chroot

- **chroot()** sistemski (Libc) poziv:
  - mijenja pokazivač root datotečnog sustava (/) tekućem procesu i svima koji ga nasljeđuju
  - ovo znači da proces ne može više pronaći "/" ako nema referenci na njega
  - rezultat: proces/daemon koji je "provaljiv" ne predstavlja problem za sigurnost sistema jer osoba koja je provalila ne može doći do /
  - ali: ako postoji koji otvoreni fd prije chroot() moguće je doći do inode od /

---

---

---

---

---

---

---

---

## FTP

### Wuftp - logovi

- Primjer **xferlog** (xferstats za statistiku):  
Wed Aug 1 06:46:40 2001 1 L155075.ppp.dion.ne.jp 6627  
/home/ftp/pub2/wget/wget-1.5.2-1.5.3.diff.gz b \_ o a  
mozilla@ ftp 0 \* c
- Izvadak iz **authlog**:  
Aug 21 08:38:06 gnjilux ftpd: hosted-by.mainserver.nl:  
anonymous/aa@bb.nl[1346]: ANONYMOUS FTP LOGIN FROM  
hosted-by.mainserver.nl [213.207.35.2], aa@bb.nlAug 21  
08:38:49 gnjilux ftpd: hosted-by.mainserver.nl:  
anonymous/aa@bb.nl: QUIT[1346]: FTP session closed
- Direktive za logiranje u **ftppassess**:  
log transfers anonymous,guest,real inbound,outbound

---

---

---

---

---

---

---

---

---

---

## FTP

### Wuftp - sažetak

- Konfiguracijske datoteke:
  - **ftppassess** – opće konfiguriranje, klase, logiranje, upload direktorij
  - **ftpusers** – zabrana pristupa određenim korisnicima
  - **ftphosts** – zabrana/dozvola pristupa određenim računalima i/ili korisnicima (podržava hostmaske!)
  - **ftpconversions** – konverzije među datotekama
  - **ftpservers** – virtualni poslužitelji
- 3 načina rada:
  - **obični korisnici** – svaki obični korisnik s poslužitelja
  - **guest korisnici** – 1 stvarni korisnik na više njih
  - **anonimni ftp** – chroot okruženje, ograničenja, itd.

---

---

---

---

---

---

---

---

---

---

## IRC

### Uvod

- **Internet Relay Chat** – komunikacija između korisnika u **stvarnom vremenu**
- Osnovni protokol specificiran 1988. godine za RT komunikaciju između korisnika na **BBS**-ovima (Bulletin Board System)
- Kasnije dorađen u RFC 1459 (IRC2 protokol)
- IRC protokol:
  - čisti tekst!
  - bilo koji socket bazirani klijent, uključujući i telnet

---

---

---

---

---

---

---

---

---

---

## IRC Uvod (2)

- Danas prilično usavršen:
  - podržava "klijent – poslužitelj" model
  - server-master (**hub**) – server-slave (**leaf**)
  - enkripcija
  - kompresija podataka } binarni prijenos!
  - TS (**timestamp**) protokol – vremenska sinkronizacija podataka
  - autorizacija korisnika
  - provjera korisnika: **iauth**, **proxy**, **openSOCKS**

---

---

---

---

---

---

---

---

## IRC Uvod (3)

- Različiti IRC poslužitelji namijenjeni različitim IRC mrežama:
  - IRCNet – više od 80 000 korisnika u svakom trenutku, irc2.10.\*
  - EFNet – oko 60 000 korisnika ..., Hybrid, Comstud
  - Undernet, Dalnet, EFNOW, Hybnet, itd.
- Razlike u softveru velike, neki se čak ne drže originalnih specifikacija, tj. RFC-a
- Postoje IRC3 specifikacije (A. Church) u nastajanju:
  - audio, video, binarni prijenos, bolja vremenska sinkronizacija, cikličke mreže, rješavanje aktualnih problema

---

---

---

---

---

---

---

---

## IRC Osnovni pojmovi

- Korisničko ime = **nickname**
- Mjesto (kanal) za javnu komunikaciju = **channel**
- Poruka = **message**, možete poslati:
  - na kanal (jedan ili više)
  - individualnom korisniku ili više njih
- Čuvar kanala = **channel operator**
- IRC administrator = **ircop**

---

---

---

---

---

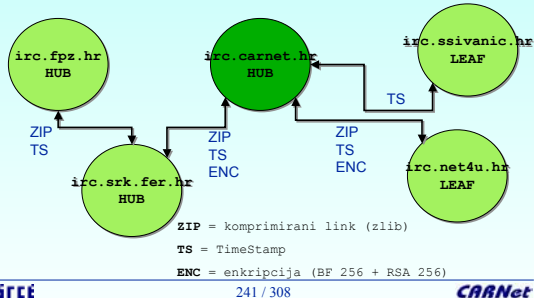
---

---

---



## IRC Aktualna hijerarhija



---

---

---

---

---

---

---

---

## IRC Naša implementacija

- CARNet koristi Hybrid6:
  - enkripcija (256bit BF, 2048bit RSA ključevi), kompresija podataka (Zlib - level 4)
- Dodatni patchevi: CCIT CRC16 kodiranje adresa zbog zaštite korisnika:
  - ICMP host unreachable
  - death ping
  - nuke
  - UDP flood
- Izvorni kod poslužitelja i servisa dostupan na <ftp://ftp.carnet.hr/pub/misc/irc>

---

---

---

---

---

---

---

---

## IRC Naša implementacija (2)

- Dodatni servisi – HybServ2:
  - rezervacija: NickServ – [nickname](#), ChanServ - [channel](#)
  - ostavljanje offline poruka – MemoServ
  - mrežne statistike – StatServ
  - opće informativne poruke – Global
- Implementirani u vidu "virtualnog poslužitelja" koji djeluje zasebno i posve automatski (samostojeći)
- Riješili probleme:
  - otklanjanje kanala, nickova, poruka dok ljudi nisu online, itd.
  - nadziranje mogućih problema

---

---

---

---

---

---

---

---

## IRC

### Konfiguriranje i korištenje

- Složeno konfiguriranje: puno predradnji (analiza korisnika, popisi modemskih ulaza), analiza topologije IRC mreže, komplicirana konfiguracijska datoteka
- Korištenje pak vrlo jednostavno:
  - /msg nick poruka
  - /msg #kanal poruka
  - /join #kanal
  - /leave
  - /quit
  - pisanje poruke bez "/" prefiksa
- <http://irc.carnet.hr>

---

---

---

---

---

---

---

---

## IRC

### Hybrid6 – konfiguriranje poslužitelja

M:irc.srk.fer.hr:161.53.70.132::6667

P:::6667:

Y:51:90:1:100:80000

Y:0:90:1:100:40000

Y:30:190::500:100000

I:NOMATCH::\*@\*:51

I:161.53.0.0/16::x:30

I:NOMATCH::\*@\*.hr::30

O:kreator@\*.srk.fer.hr:070v1FfQliJgs:kreator:KORUGNHD:10

H::\*:irc.carnet.hr

N:irc.carnet.hr:@irc.carnet.hr:pubkey:irc.carnet.hr:0:2

C:irc.carnet.hr:@irc.carnet.hr:pubkey:irc.carnet.hr:9999:2

klase korisnika

dodjeljivanje klase adresama

administratorska linija

spajanje na drugi poslužitelj

---

---

---

---

---

---

---

---

## News

### Općenito

- NNTP specficiran u RFC1036 i RFC977
- Niz protokola za razmjenu poruka između (obično) decentralizirane mreže news poslužitelja
- Članci (**news articles**) organizirani u grupe (**newsgroups**) koje imaju hijerarhiju (geografsku, tematsku, lokalnu, itd.)
- Svi članci se lokalno spremaju na **svakom** poslužitelju – propagiraju se dalje, čineći pristup svim člancima vrlo brzim
- Ukupni skup članaka - **Usenet**

---

---

---

---

---

---

---

---

## News Općenito (2)

- Najpoznatiji i navodno najčešći news poslužitelj - INN
- Trenutni razvoj je prešao na 2.3.1:
  - novi načini zapisivanja članaka
  - izmijenjene konfiguracijske datoteke, poboljšani i ubrzan rad, itd.
- Kod nas se pretežno i dalje koristi 2.2 serija:
  - kompatibilnosti i nekompatibilnosti sa 2.3
  - gotove konfiguracije
  - problematični upgrade
  - navodne nestabilnosti u 2.3 seriji
- Adresa izvornog koda: <http://www.isc.org/inn>

---

---

---

---

---

---

---

---

---

---

## News Hijerarhija grupa

- Hijerarhija članaka (glavnih 8):
  - comp.\*, humanities.\*, misc.\*, news.\*, rec.\*, sci.\*, soc.\*, talk.\*
- Alternativno:
  - alt.\* - alternativa, sve dozvoljeno
- Geografski određeno:
  - de.\*, hr.\*
- Dodatne ili komercijalne:
  - bionet.\*, compuserve.\*
- Profesionalne:
  - microsoft.\*, borland.\*

---

---

---

---

---

---

---

---

---

---

## News Klijenti

- Unix:
  - Xemacs+Gnus
  - Slim
  - Tin
  - Trn ...
- Windows:
  - Netscape Navigator
  - MS Outlook ...

---

---

---

---

---

---

---

---

---

---

## News INN

- INN – rješen u vidu različitih skripti (Perl, Sh) i programa koji međusobno komuniciraju
- Tri standardne arhitekture i jedna vrlo rijetka:
  - centralizirana
  - distribuirana – dijeljeni **news article spool**
  - distribuirana – replikacija članaka
  - distribuirana – news cache
- Posve različiti načini funkcioniranja, otpornosti na greške, hardverski zahtjevi, itd.

---

---

---

---

---

---

---

---

---

---

## News

### INN – centralizirana arhitektura

- **Centralizirana arhitektura:**
  - jedan news poslužitelj koji prima članke i poslužuje članke kao i obrađuje ulazni promet (**incoming feed**) te šalje te članke dalje
  - primjena: male mreže i mali poslužitelji
  - prednosti:
    - lako održavanje – jedan jedinstveni sistem
    - mali zahtjevi – ako je mali news promet, može služiti i za drugo
  - mane:
    - ograničena nadogradivost – dodavanje samo CPU/memorije ...
    - neotpornost na greške – u slučaju greške ostaje se bez servisa

---

---

---

---

---

---

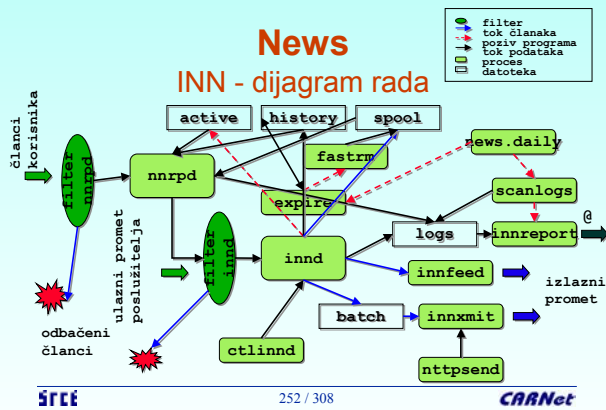
---

---

---

---

## News INN - dijagram rada




---

---

---

---

---

---

---

---

---

---

## News

### INN – centralizirana arhitektura (2)

- Centralni dio sistema:
  - **innd** proces koji prima ulazni tok podataka (feed), barata sa **active** i **history** datotekama kao i samim article spoolom, sluša na portu 119 i prima ulazne konekcije (korisnike)
  - za svaku ulazni konekciju podiže se **nnrpd** proces koji služi za interakciju s korisnikom
  - konfiguracijske datoteke: readers.conf, inn.conf
- Komunikacija s korisnikom:
  - svaki nnrpd proces također čita active i history datoteke da nađe informacije o člancima, uzima iz spoola tražene članke, šalje ih klijentu te prima članke od korisnika
  - konfiguracijske datoteke: active, history

---

---

---

---

---

---

---

---

## News

### INN – centralizirana arhitektura (3)

- Komunikacija s korisnikom (nastavak):
  - svaki poslani članak se provuče kroz **filter\_nnrpd** (Perl ili TCL/Tk skripta koja filtrira samo poslane članke)
  - u slučaju detektiranih grešaka, članak se odbija uz poruku u greški
  - ako prođe, šalje se innd-u koji to provuče kroz **filter\_innd** (skenira **sav** ulazni promet – dakle i **feed**) i vraća u slučaju greške (nnrpd vraća nazad članak), a ako prođe innd, sprema u spool
  - moguće dodati **anti-spam** filtere

---

---

---

---

---

---

---

---

## News

### INN – centralizirana arhitektura (4)

- Dodatni detalji:
  - **news.daily** se brine za brisanje članaka koji duže stoje u spoolu (**article expiration**) – konfiguracijska datoteka je expire.ctl
  - logovi – news.daily poziva **scanlogs** koji rotira log datoteke i poziva **innreport** za procesiranje istih, te stvara izvještaj i šalje administratoru
  - nadgledanje samog procesa – **innwatch** (innwatch.ctl)
  - kontrola innd-a – **ctlinnd** (control.ctl)

---

---

---

---

---

---

---

---

## News

### INN – distribuirana arhitektura

- **Distribuirani poslužitelj s dijeljenim spoolom (shared article spool):**

– primjena: veliki sistemi i mrežni poslužitelji

– prednosti:

- jedinstvena kopija – članci se ne dupliciraju, samo jedan (zajednički) niz diskova dovoljan
- sinkroniziranje podataka – svi vide isti spool, nepotrebno dodatno sinkroniziranje
- robusnost - ako jedan poslužitelj prestane raditi, servis svejedno ostaje na drugom
- skalabilnost – moguće dodavati nove poslužitelje u slučaju rasta broja čitatelja

---

---

---

---

---

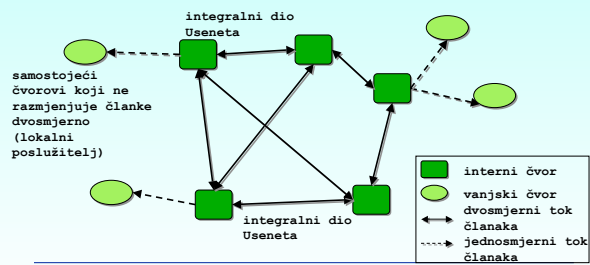
---

---

---

## News

### Distribuirana mreža



---

---

---

---

---

---

---

---

## News

### INN – distribuirana arhitektura (2)

- **Distribuirani poslužitelj s dijeljenim spoolom (nastavak):**

– mane:

- povećana složenost: teže održavati, potrebno osigurati ispravno dijeljenje
- točka loma: u slučaju kvara na article spoolu, kompletan news servis (oba poslužitelja) prestaju raditi (ako nije RAID)

- **Distribuirani s keširanjem:**

– centralizirana arhitektura i polje news cacheova (nntpcache) koji ne čitaju direktno centralni spool već vrše upite samom centralnom poslužitelju

---

---

---

---

---

---

---

---

## News

### INN – distribuirana arhitektura (3)

- **Distribuirani s replikacijom članaka:**
  - primjena: veliki sistemi i veliki zahtjevi
  - prednosti:
    - robusnost i skalabilnost (kao kod dijeljenog spoola)
    - nema zajedničke točke loma
  - mane:
    - održavanje: vrlo teško zbog potrebe za inteligentnom sinkronizacijom članaka
    - povećani downtime: u startu nakon pada servisa u pravilu potrebno duže vrijeme za početnu sinkronizaciju
    - polja diskova: povećana cijena zbog povećane potrebe za diskovnim prostorom (razlog je replikacija)

---

---

---

---

---

---

---

---

## News

### INN – sažetak

- Konfiguriranje INN2 izuzetno složeno
- Konfiguracijskih datoteka vrlo mnogo:
  - newsfeeds = gdje se šalju članci
  - overview.fmt = format overview baze
  - expire.ctl = kontrola expireanja članaka
  - inn.conf = konfiguracija samog poslužitelja
  - hosts.nttp = hostovi kojima se šalju članci
  - server, organization = ime poslužitelja ...
  - nntp.access = pristup news serveru
  - innfeed.conf = konfiguracijska datoteka za feedanje članaka
  - innwatch.ctl = konfiguracija nadglednika daemona
  - ....

---

---

---

---

---

---

---

---

## Sigurnost i zaštita privatnosti za korisnike

- Plaintext protokoli = **čisti tekst**:
  - FTP, Telnet, HTTP, Rlogin, Rsh, SMTP
  - lozinke se prenose također kao čisti tekst
- Provaljeno računalo + sniffer = kompromitirani LAN (u većini slučajeva)
- Rješenja:
  - mail = PGP, GNUPG
  - Telnet, FTP, Rsh, Rlogin ... = SSH
  - Telnet, Dlogin, FTP ... = S/Key, OPIE
- Sigurno identificiranje korisnika (ključevi, autorizacija)

---

---

---

---

---

---

---

---

## Sigurnost i zaštita privatnosti za korisnike (2)

- Što služi čemu:
  - **SSH** = sigurna zamjena za Telnet i FTP, koristiti na mjestima na kojima je polazno računalo nekompromitirano, a vaša veza do tog računala **ne** sadržava niti jedan Telnet ili sličan nesiguran protokol
  - **S/Key** = koristi se kad je vaša veza do računala "nesigurna" (Telnet i sl.)
  - **PGP** = koristi se za zaštitu E-maila i podataka, baziran na principu javnih i tajnih ključeva

---

---

---

---

---

---

---

---

## Zaštita privatnosti SSH – općenito

- Mogućnosti:
  - tuneliranje, X11 forwarding
  - enkripcija + kompresija + provjera jedinstvenosti komunikacije
  - SFTP, Scp
  - Kerberos, PAM, OTP, OpenSSL, ...
  - izvođenje naredbi na udaljenom računalu
- Rasprostranjenost, dostupnost, stabilnost
- Uspješno zamjenjuje Telnet, FTP, Rlogin, Rsh

---

---

---

---

---

---

---

---

## Zaštita privatnosti SSH – općenito (2)

- Dva protokola:
  - SSH1 – 1.3 i 1.5
  - SSH2 – 2.0
- RFC još uvijek neobjavljen, ali postoje 2 drafta
- Komercijalne (ssh-nonfree) i slobodne (BSD) inačice (OpenSSH)
- OpenSSH klijent – na adresi <http://www.openssh.com>
  - podržava protokol 1 i 2 kao i SFTP
  - vrlo rasprostranjen, aktivna podrška
  - potekao sa OpenBSD platforme

---

---

---

---

---

---

---

---



## Zaštita privatnosti SSH – protokol 1

- Svaki poslužitelj ima **1024-bitni RSA** ključ na disku
- Svaki sat - novi **768-bitni RSA** ključ (ne na disku!)
- Poslužitelj pošalje klijentu oba ključa, ovaj generira **256-bitni** "slučajni" broj (svoj ključ) kriptiran pomoću prva dva i šalje nazad
- Nakon uspješnog **handshakinga** se taj broj koristi za daljnju enkripciju veze pomoću 3DES ili Blowfish algoritama
- Zatim **slijedi autorizacija** ...
- Paketi se konstantno provjeravaju CRC sumama (**man-in-the-middle** napad)

---

---

---

---

---

---

---

---

---

---

## Zaštita privatnosti SSH – protokol 2

- U osnovi sličan SSH1 protokolu
- Svaki poslužitelj ima vlastiti **DSA ključ**
- **Ne** generira se dodatan ključ
- **Razmjena ključeva** ide preko standardiziranog Diffie-Hellman algoritma
- Daljnja veza se kriptira Blowfish, 3DES, CAST128, Arcfour, 128-bitnim AES ili 256-bitnim AES algoritmima
- **Integritet poruka** - preko hmacsha1 ili hmacmd5 koda, (to nedostaje SSH1 protokolu)

---

---

---

---

---

---

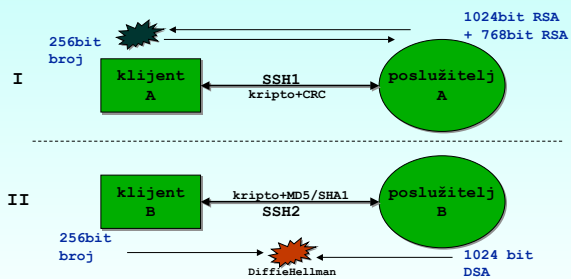
---

---

---

---

## Zaštita privatnosti SSH – dijagram




---

---

---

---

---

---

---

---

---

---

## Zaštita privatnosti

### OpenSSH – instalacija

- CARNet SSH paketi za Solaris:
  - ssh\_1.2.27-1\_solaris2.7.pkg
  - ssh\_1.2.31\_solaris2.7.pkg
  - openssh\_2.1.0\_solaris2.7.pkg
- Analogno i za Digital Unix (OSF)
- Preporučljivo uvijek koristiti **posljednju** inačicu
- OpenSSH kompatibilan sa SSH1 i SSH2 protokolima kao i **svim** klijentima

---

---

---

---

---

---

---

---

## Zaštita privatnosti

### OpenSSH – instalacija (2)

- Standardna instalacija CARNet paketa:  
`dpkg -i openssh_2.1.0_solaris2.7.pkg`
- Automatski se izvršava postinstall skripta:
  - zapis za Ssh servis u `"/etc/inet/services"`
  - zapis za Ssh autoriziranje u `"/etc/pam.conf"`
  - kreira se `"/var/run"` direktorij za `"sshd.pid"` datoteku sa PID Ssh daemona
  - generiraju se RSA i DSA ključevi za poslužitelj
  - starta se sshd proces

---

---

---

---

---

---

---

---

## Zaštita privatnosti

### OpenSSH – instalacija (3)

- Izvršne datoteke na sistemu
  - scp – kopiranje datoteka preko SSH
  - slogin, rsh, rlogin – obično symlinkovi na ssh datoteku
  - ssh – klijent
  - ssh-add – skripta za dodavanje ključeva
  - ssh-agent – za čuvanje ključeva
  - ssh-keygen – generator ključeva
  - sshd – SSH daemon odnosno poslužiteljski proces

---

---

---

---

---

---

---

---

## Zaštita privatnosti OpenSSH – konfiguriranje

- Konfiguriranje:
  - klijenta = `ssh_config`
  - poslužitelja = `sshd_config`
- Dodatne mogućnosti (nisu u ovom paketu, vjerojatno će biti u 2.5.0):
  - `sshd_prng_cmds` – PRNG (ili kako zaobići nepostojeći `"/dev/random"` uređaj)
  - `sshd_primes` – prosti brojevi za PRNG
- U pravilu **ne treba** ništa dodatno konfigurirati!

## Zaštita privatnosti OpenSSH – konfiguriranje (2)

- Klijent:
  - CARNet paket koristi postavljene standarde
  - ove postavke osiguravaju dodatnu sigurnost korisnika, ali **ne** i cjelokupnog sistema
  - iznimka:  
Host \*  
ForwardAgent no  
ForwardX11 no  
FallbackToRsh no

## Zaštita privatnosti OpenSSH – konfiguriranje (3)

- Poslužitelj - opcije od **vrlo velike važnosti** i treba se osigurati da uvijek budu postavljene:  
PermitRootLogin no  
IgnoreRhosts yes  
StrictModes yes  
X11Forwarding no  
KeepAlive yes  
RhostsAuthentication no  
PermitEmptyPasswords no  
UseLogin no

## Zaštita privatnosti SSH – upotreba

- Spajanje na poslužitelj:  
`ssh -l kreator@regoc.srce.hr -v -C`
- Kopiranje datoteke:  
`scp .zshrc kreator@fly.srk.fer.hr:~/tmp/`
- Generiranje vlastitog ključa:  
`ssh-keygen`
- Kontrolni znakovi Ssh procesu:  
`~^Z ili ~. ili pak ~~.`

## Zaštita privatnosti SSH – upotreba (2)

- Navodimo SSH klijente za Windows OS:
  - PuTTY – SSH1 i SSH2:  
<http://www.chiark.greenend.org.uk/~sgtatham/putty/>
  - TTSSH – SSH1: <http://www.zip.com.au/~roca/tssh.html>
  - OpenSSH pomoću Cygwin projekta: <http://www.cygwin.com>
  - MSSH – SSH1: <http://cs.mscd.edu/MSSH/>
  - SecureCRT – SSH1 i SSH2:  
<http://www.vandyke.com/products/SecureCRT/>
  - F-Secure SSH – SSH1 i SSH2: <http://www.datafellows.com/f-secure/>
  - FISSH – SSH1 i SSH2: <http://www.massconfusion.com/ssh/>
  - MacSSH, NiftyTelnet 1.1

## Zaštita privatnosti OpenSSH – sažetak

- “Sigurna” zamjena za Telnet
- OpenSSH – besplatna zamjena, podržava SSH1 i SSH2 protokol
- Konfiguracija:
  - klijent – ssh:
    - ssh\_prng\_cmds, primes, ssh\_config
  - poslužitelj – sshd:
    - sshd\_config
- Omogućava i FTP i X11 forwarding

## Zaštita privatnosti S/Key – teorija

- Original **Mink** - tvrtka Bellcore sredinom 90-ih
- Kasnije preuzeo Wietse Venema u paketu Logdaemon
- Olaf Kirch (Linux S/Key); Wyman Miles (Pam\_secuid)
- Danas evoluiralo u više pravaca – **OTP, OPIE**
- Specifikacije:
  - RFC1760 - S/KEY One Time Password System
  - RFC2289 - A One-Time Password System
  - RFC2243 - OTP Extended Responses
  - RFC2444 - The One-Time-Password SASL Mechanism



---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – teorija (2)

- Prisluškivanje mreže → dobiveno korisničko ime i lozinka
- Rješenje: **jednokratne lozinke** ⇒ privatne informacije su dostupne – ali ne i sam pristup!
- Zahtjevi za OTP:
  - generator određenih ključeva na osnovu tajne lozinke i informacije s poslužitelja unaprijed generira određen broj ključeva
  - program koji na osnovu unesenog ključa daje pristup i smanjuje redni broj dozvoljenog ključa



---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – teorija (3)

- **Seed, challenge** = **jedinstveni** string za svako novo generiranje niza ključeva, npr. dk3455
- **Sequence number** = **redni broj** S/Key ključa
- **Pass-phrase** = **tajna lozinka** (ne smije se unositi preko Telnet!)
- **Secure hash function** = funkcija koja omogućava **jednosmjerno** kriptiranje tajne lozinke (npr. MD5, SHA1, MD4)

---

---

---

---

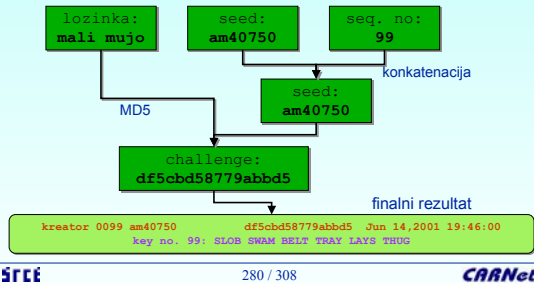
---

---

---

---

## Zaštita privatnosti S/Key – primjer



---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – opći algoritam

- Korak 1 - generiranje:
  - proizvoljan niz znakova kao tajna lozinka (> 10, obično do 63 znaka), najčešće tekst
  - spaja se sa "seedom" od poslužitelja (nije tajni!)
  - prolazi kroz hash funkciju i smanjuje na 64 bita
- Korak 2 - proračun:
  - na izlaz 1 koraka S primjenjuje se **hash** funkcija točno N puta (specificira korisnik)
  - svaki slijedeći OTP se generira provođenjem S kroz hash funkciju N-1 puta

---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – opći algoritam (2)

- Korak 3 – izlaz:
  - sve jednokratne lozinke ovako generirane su **64-bitne dužine**
  - lozinka se pretvara u niz od **šest kratkih engleskih riječi** izabranih iz rječnika od 2048 engleskih riječi:
    - 11 bitova po riječi = svi OTP se mogu enkodirati
    - 2 bita zaalosti = checksum, 64 bita je raspodijeljeno na parove te se sumiraju zajedno, 2 bita najmanje važnosti su ukodirani u zadnju riječ (najmanje važni bit sume je zadnji bit riječi)
    - riječi su predočene velikim slovima sa razmacima između
    - rječnik je standardiziran u RFC 1760 (kasnije i u RFC 2289)

---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – opći algoritam (3)

- Korak 4 – provjera:
  - poslužitelj ima u bazi podataka OTP od zadnjeg uspješnog logiranja ili prvi OTP svježe generirane sekvence
  - dekodira se OTP od generatora u 64-bitni ključ i provede kroz hash funkciju jednom
  - ako rezultat odgovara onome u bazi, korisniku je dozvoljeno logiranje, a u bazu se snima iskorišteni OTP

---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – implementacija

- CARNet S/Key paket:
  - nekad - Skey izvađen iz Logdaemon paketa
  - danas - samostojeći PAM (Pluggable Authentication Module)
    - integracija u postojeći sistem bez modifikiranja login binarne datoteke
    - jednostavna nadogradivost i izmjenjivost
    - jednostavno isključiti
    - jednostavna konfiguracija za sve servise odjednom, zasebne servise, itd.
    - prenosivost – radi na BSD, Linux i Solaris

---

---

---

---

---

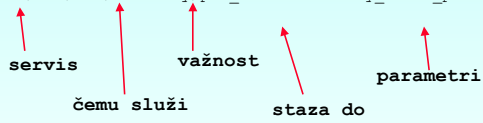
---

---

---

## Zaštita privatnosti S/Key – instalacija u pam.conf

```
login auth sufficient /usr/lib/security/pam_skey.so.1
login auth required
 /usr/lib/security/pam_unix.so.1 try_first_pass
```



- Konfiguracija PAM modula – razlikuje se od verzije do verzije PAM biblioteke; nema na Digital Unixu

---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – primjer

```
UNIX(r) System V Release 4.0
(fly)login:kreator
challenge s/key 64 f10328002
password:

amanda:~ $ keyinit %23:10
Adding kreator:
Reminder - Only use this method if you are directly
connected. If you are using telnet or rlogin exit with no
password and use keyinit -s.
Enter secret password:
Again secret password:
ID kreator s/key is 99 am53046
LUNG SUNK FOLD CARE BEER DOOR
```

---

---

---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – klijenti i alternative

- OTP generatori:
  - SkeyCalc - <http://www.orange-carb.org/SkeyCalc>
  - WinKey - <ftp://ftp.msri.org/pub/skey/winkey.exe>
  - DosKey - <ftp://ftp.msri.org/pub/skey/doskey.exe>
  - JOTP - <http://www.cs.umd.edu/users/harry/jotp/>
  - OpieCalc - <http://www.scs.carleton.ca/skey/opiecalc.sit.hqx>
- Alternative za Unixe:
  - PAM OPIE
  - Linux S/Key

---

---

---

---

---

---

---

---

---

---

## Zaštita privatnosti S/Key – sažetak

- S/Key – jednokratne lozinke
- PAM – vlastiti moduli za vlastite vrste autorizacije, platformski nezavisno:
  - Linux, BSD, Solaris
- Konfiguracija za S/Key:
  - lozinke (MD4/MD5) se nalaze u:
    - /etc/skeykeys
  - dodatna autorizacije za S/Keyeve:
    - /etc/keyaccess

---

---

---

---

---

---

---

---

---

---



## Zaštita privatnosti

### PGP – uvod

- Pretty Good Privacy = softver za "jaku" enkripciju (**strong encryption**) autora Philipa Zimmermanna
- Aktualna verzija – PGP 6.5.8 na <http://www.pgpi.com>
- Koristi enkripciju na temelju **javnih ključeva** za zaštitu E-mailova kao i raznih vrsta podataka
- Omogućava **sigurnu razmjenu podataka** preko inače nesigurnih "kanala", odnosno tipova prijenosa
- Brzina, kompresija, **digitalno potpisivanje**

---

---

---

---

---

---

---

---

## Zaštita privatnosti

### PGP – teorija

- Standardni kriptosistemi (npr. DES): jedan ključ za kriptiranje i dekriptiranje – inicijalno ga je potrebno "sigurno" prenijeti
- Kriptosistemi bazirani na javnim ključevima
  - **javni ključ** (**public key**): isključivo služi za kriptiranje poruke osobi čiji je taj ključ
  - **tajni ključ** (**secret key, private key**): služi za dekriptiranje te iste poruke, bez njega je to nemoguće!

---

---

---

---

---

---

---

---

## Zaštita privatnosti

### PGP – teorija (2)

- Tajni ključ služi i za "potpisivanje" poruka (**digital signature**) – primatelj pomoću javnog ključa osobe može provjeriti validnost (točnost izvora i sadržaja)!
- Za samo kriptiranje poruke se **ne** koristi algoritam za enkripciju poruke preko javnih ključeva zbog sporosti
- Umjesto toga se koriste "single-key" enkripcijski algoritmi (brzi i pouzdani) pomoću privremeno generiranog ključa (nepoznat korisniku)!

---

---

---

---

---

---

---

---

## Zaštita privatnosti

### PGP – teorija (3)

- Taj ključ se zatim kriptira pomoću javnog ključa primatelja i šalje zajedno s kriptiranim tekstom (ciphertext)
- Primatelj pomoću tajnog ključa odkriptira takav ključ i zatim pomoću njega samu poruku
- Javni ključevi se drže u certifikatima ključeva (key certificate) koji sadržavaju user ID (ime osobe ili login), vremensku oznaku kada je stvoren (timestamp) i sam materijal ključa



---

---

---

---

---

---

---

---

## Zaštita privatnosti

### PGP – teorija (4)

- Tajni ključevi su sami kriptirani samom tajnom lozinkom (passphrase) u slučaju da budu ukradeni
- Kolekcija više certifikata ključeva je tzv. key ring – očito ih dijelimo na tajne i javne
- Svaki ključ ima svoju jedinstvenu oznaku "key ID" što je 64 bitova najmanje važnosti, ali se prikazuje u radu samo donjih 32 bita



---

---

---

---

---

---

---

---

## Zaštita privatnosti

### PGP – teorija (5)

- Digitalni potpis je 128-bitni ključ koji nastaje prolaskom teksta kroz jednosmjernu hash funkciju, koji je dodatno kriptiran tajnim ključem
- Potpisani dokumenti dobivaju na početak key ID i takav potpis zajedno sa vremenom stvaranja potpisa
- Kriptirane datoteke na početak dobivaju key ID od javnog ključa kojim je kriptirano

---

---

---

---

---

---

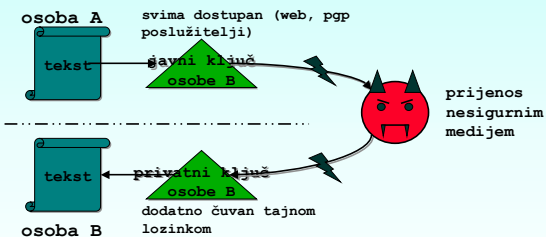
---

---

## Zaštita privatnosti PGP – sigurnost sigurnosti

- Do danas **nije** pronađen efektivni način **kako provaliti** PGP poruku u **razumnoj** količini vremena
- Jedini načini su:
  - ukrasti lozinku
  - nadgledati proces enkripcije uz pomoć najviših ovlasti
  - brute force napad
  - trojan napadi: lažni ključevi, lažni programi, itd.
  - prisluškivanje računala - Van Eck zračenje
- Složene matematičke analize: brute force napad na IDEA (simetrični cipher) praktički **nemoguć**

## Zaštita privatnosti PGP – shema rada



## Zaštita privatnosti PGP – sigurnost sigurnosti (2)

- Napad na RSA (simetrični cipher koji se čini sigurnim zbog teškoća faktoriranja jako velikih brojeva)
- Potrebno vrijeme za faktoriranje pomoću NFS algoritma (Number Field Sieve, najbrži postojeći algoritam za brojeve >110):
  - 512bit : 30,000 MIPS-godina
  - 768 bit : 200,000,000 MIPS-godina
  - 1024 bit : 300,000,000,000 MIPS-godina
  - 2048 bit : 300,000,000,000,000,000,000,000 ...

## Zaštita privatnosti PGP – kriptiranje

- CARNet paket - PGP 2.6.3
- Kriptiranje datoteke pomoću tuđeg javnog ključa:  
`pgp -e tekst_dat korisnicki_ID`
- Kao rezultat dobivamo: `tekst_dat.pgp`
- Za stvaranje tekstualne verzije:  
`pgp -a -e tekst_dat korisnicki_ID`
- Ili za slanje odjednom više osoba:  
`pgp -e tekst_dat k_ID1 k_ID2 ...`

---

---

---

---

---

---

---

---

## Zaštita privatnosti PGP – potpisivanje

- Za potpisivanje teksta ili poruke (stvara `tekst_dat.pgp` potpisanu poruku i komprimira je nakon potpisivanja):  
`pgp -s tekst_dat [-u vas_kljuc]`
- Drugi dio omogućava odabir ključa (ako ih imate više)
- Za potpisivanje poruke kao tekst (stvara `tekst_dat.asc`) uz pomoć CLEARSIG metode:  
`pgp -sta tekst_dat`

---

---

---

---

---

---

---

---

## Zaštita privatnosti PGP – korištenje

- Za potpisivanje i kriptiranje:  
`pgp -es tekst tudji_ID [-u vas_ID]`
- Za "jednostavno" kriptiranje  
`pgp -c tekst_datoteka`
- Dekriptiranje:  
`pgp kript_dat [-o dekript_dat]`
- Generiranje vlastitih ključeva:  
`pgp -kg`

---

---

---

---

---

---

---

---

## Zaštita privatnosti PGP – korištenje (2)

- Dodavanje tuđeg ključa u kolekciju ključeva:  
`pgp -ka kljuc_dat [keyring]`
- Micanje ključa iz kolekcije ključeva:  
`pgp -kr kor_ID [keyring]`
- Ekstrakcija određenog ključa iz kolekcije:  
`pgp -kx kor_ID kljuc_dat [keyring]`
- Pregled sadržaja kolekcije:  
`pgp -kv[v] [kor_ID] [keyring]`



---

---

---

---

---

---

---

---

## Zaštita privatnosti PGP – korištenje (3)

- Provjera vlastitih ključeva:  
`pgp -kc [kor_ID] [keyring]`
- Pregled 16-bajtnog "izvatka" (fingerprint) za (najčešće!) usmenu provjeru validnosti ključa:  
`pgp -kvc kor_ID [keyring]`
- Primjer:  
UserID: "Philip R. Zimmermann <prz@acm.org>"  
Key Size: 1024 bits; Creation date: 21 May 1993;  
KeyID: C7A966DD  
Key fingerprint: 9E 94 45 13 39 83 5F 70 7B E7 D8 ED C4  
BE 5A A6



---

---

---

---

---

---

---

---

## Zaštita privatnosti PGP – korištenje (4)

- PGP se lako integrira u mail klijente pod Unix ili Windows operacijskim sustavima:
  - Mutt
  - Pine – PGP4Pine
  - Xemacs – mailcrypt
  - MS Outlook – preko PGPTray-a
  - MS Eudora – preko PGPTray-a
- Windows verzije PGP sadržavaju GUI koji vrlo olakšava te pojednostavljuje rad

---

---

---

---

---

---

---

---

## Zaštita privatnosti PGP – sažetak

- Standardni kriptografski sistemi:
  - jedan ključ za enkripciju + dekripciju = nesigurno, ali brzo
- Kriptografski sistemi bazirani na javnim i tajnim ključevima:
  - jaka enkripcija
  - **javni ključ**: provjera potpisa, enkripcija
  - **tajni ključ**: potpisivanje, dekripcija, zaštićen tajnom lozinkom

---

---

---

---

---

---

---

---

## Literatura

- Dokumentacija uz programske pakete  
praktički obvezno pročitati
- OpenLDAP dokumentacija i FAQ:  
<http://www.openldap.org/>  
<http://www.openldap.org/doc/admin/quickstart.html>  
<http://www.openldap.org/faq/>
- SurfNet x.500 projekt:  
<http://www.surfnet.nl/innovatie/afgesloten/x500/eindverslag.html>
- Wu-FTPD dokumentacija i FAQ:  
<http://www.wuftp.org/wu-ftp-faq.html>  
<http://www.wuftp.org/HOWTO/>  
<http://www.wuftp.org/rfc/>
- "Setting Up Secure FTP"



---

---

---

---

---

---

---

---

## Literatura (2)

- Anonymous FTP FAQ:  
<http://www.landfield.com/wu-ftp/docs/anonymous-ftp-faq.html>
- Guest HOWTO:  
<http://www.wu-ftp.org/HOWTO/guest.HOWTO>
- Setting Up wuftp for Non-Anonymous Accounts:  
[http://glennf.com/writing/wuftp\\_setup.html](http://glennf.com/writing/wuftp_setup.html)
- INN Cookbook, INN Architecture, INN Implementation:  
<http://web.inter.NL.net/users/Elena.Samsonova/unix/inn.shtml>
- INN dokumentacija i FAQ:  
<http://www.eyrie.org/~eagle/faqs/inn.html>  
<http://www.isc.org/inn>
- Hybrid6 i Hybrid7 dokumentacija, Hybserv dokumentacija:  
<http://irc.carnet.hr/docs.htm>

---

---

---

---

---

---

---

---

## Literatura (3)

- **PGP Attacks:**  
<http://axion.physics.ubc.ca/pgp-attack.html>
- **Practical Attacks on PGP:**  
<http://www.eskimo.com/~joelm/pgpatk.html>
- **PGP Intro:**  
<http://umbc7.umbc.edu/pgp/pgpintro.html>  
<http://www.fiji.org/~phm/pgphtmlpen.html>
- **Secret key protection:**  
<http://senderek.de/security/secret-key.protection.html>
- **PassPhrase FAQ:**  
<http://www.stack.nl/~galactus/remailers/passphrase-faq.html>  
<http://www.unix-ag.uni-kl.de/~conrad/krypto/passphrase-faq.html>

---

---

---

---

---

---

---

---

## Literatura (4)

- Svi odgovarajući i spomenuti RFC-ovi:  
<http://www.compsci.bristol.ac.uk/~henkm/rfc.html>  
<http://www.AntiOnline.com/archives/text/rfc/>
- Raznu dodatnu literaturu moguće je dobiti upisivanjem relevantnih izraza u koju web tražilicu:
  - <http://www.google.com>
  - <http://www.meta360.com>
  - <http://www.hotbot.com>

---

---

---

---

---

---

---

---