Dio III

Imenički servisi, FTP, News, sigurnost i zaštita privatnosti

priredio Dinko Korunić
verzija 2.0

Sadržaj (3. dan)

Imenički servisi
Općenito

- **LDAP** (Lightweight Directory Access Protocol) = klijent-poslužitelj protokol za pristup imeničkom servisu (directory service); zamišljen kao frontend za **X.500,** može služiti i za *druge* imeničke servise
- **WHOIS++** = jednostavni tekstualni upit za pretraživanjem; može se 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
- Više baza povezanih **indeksirajućim** servisom
- Sadrži niz **individualnih zapisa** sa stvarnim informacijama
- Zapisi podijeljeni u više tipova (npr. Person, Domain, itd.)
- Za svaki tip postoji definiran različit tip atributa koje bilo koji zapis može poprimiti
- Set atributa = **predložak** (template); u X.500 je to **klasa** objekta

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”:

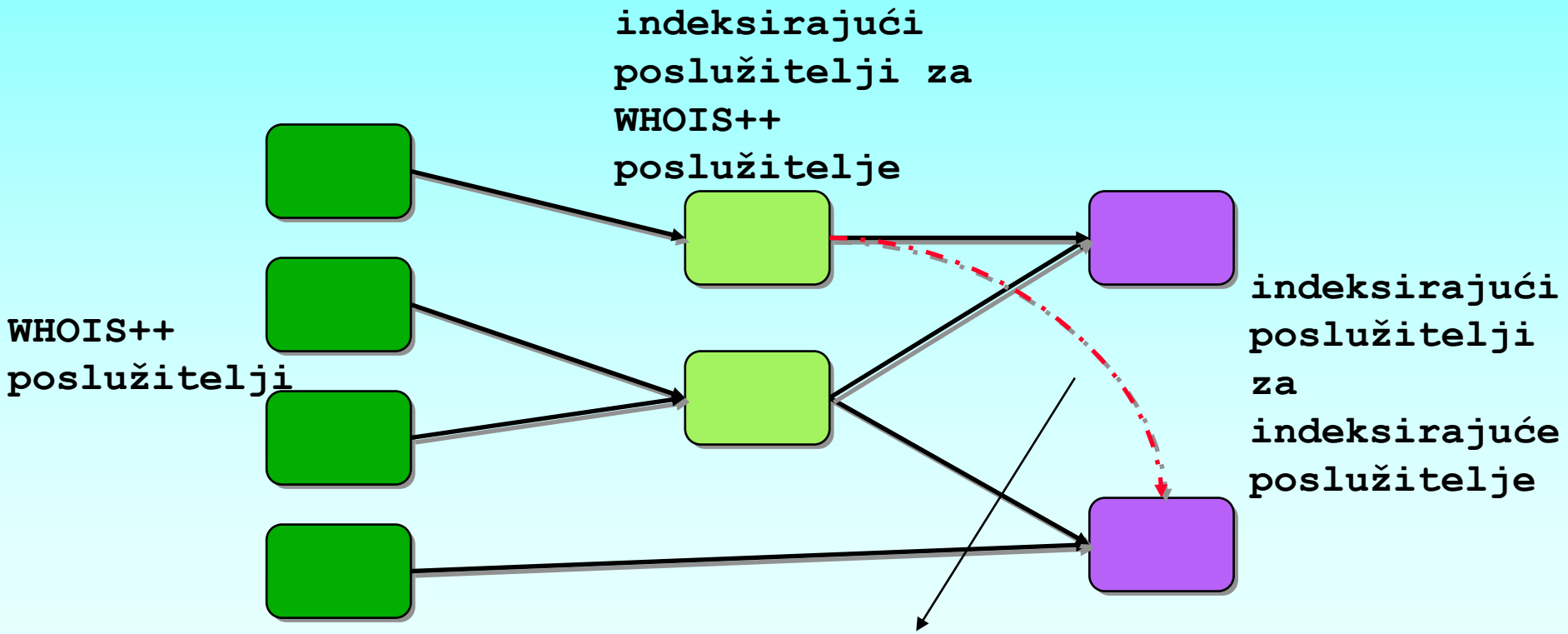
```
Template: Domain
Domain-Name: stratix.nl
Contact-Name: Mark Jacobs
```

Imenički servisi
WHOIS++ - osnove (3)

- WHOIS++ 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: drži informacije o predlošcima i atributima te listi vrijednosti (koje može poprimiti bilo koji atribut), kao i pokazivač na WHOIS++ poslužitelj sa početnim informacijama
- Servis za pretraživanje klijent pretražuje radi stvaranja listi podataka

Imenički servisi

WHOIS++ - dijagram hijerarhije



Imenički servisi
X.500 - osnove

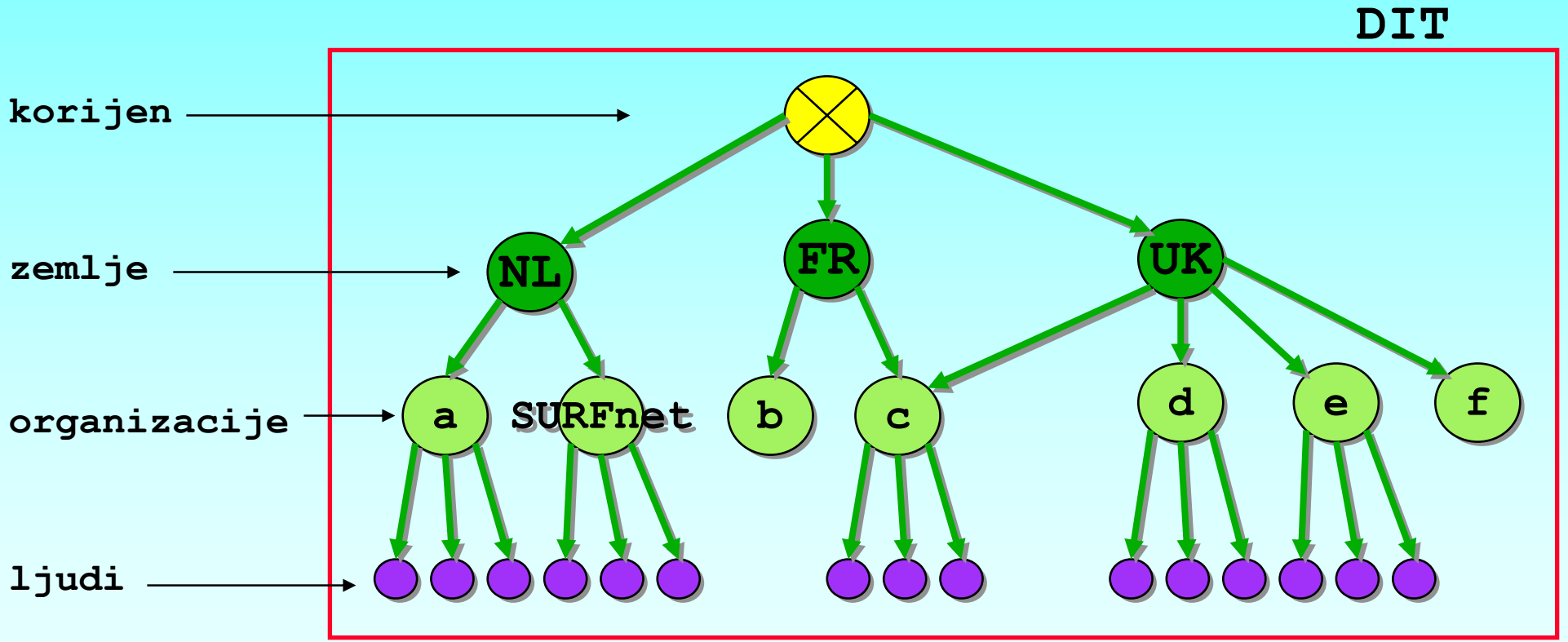
- Standard za imeničke servise kompanije ITU (International Telecommunications Union)
- Koristi **distribuirani pristup** za stvaranje globalnog imeničkog servisa:
  - Lokalne informacije o organizacijama se čuvaju lokalno u DSA (Directory System Agent)
  - Moguć odnos: jedna organizacija u više DSA, više organizacija u jednom DSA

Imenički servisi
X.500 – osnove (2)

- DSA je **baza podataka**:
  - Sadrži informacije u strukturi opisanoj X.500 informacijskim modelom
  - Mogućnost razmjene (ako je potrebno!) s drugim DSA preko DSP (Directory System Protocol)
  - Svi DSA u X.500 imeničkom servisu su povezani u predefinirani 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 poslužitelje je moguće naći koristeći DNS
- Kontrola atributa (dozvoljeni, obvezni) preko specijalnog atributa: objectClass (definira **shemu** koja će se poštovati)
- nepoštivanje sheme = ??!!

Imenički servisi
LDAP – osnove (2)

- DN (Distinguished Name) = jedinstveno ime svakog zapisa/sloga
  - omogućava jedinstveno "adresiranje" podataka
- RDN (Relative Distinguished Name) = DN 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
  - zapisa sa istim podacima može biti više!

Imenički servisi
LDAP – osnove (3)

- Informacije/zapisi/itd.
  - mogu biti dodane, promijenjene, obrisane, pročitane
  - pridržavaju se unaprijed definiranih **predložaka/shema**
- Sheme
  - popis dozvoljenih podataka
  - mogući savjeti o vrijednostima, zapisivanju i sl.
- LDAPv3 (1990 god):
  - "jaka" autentifikacija preko SASL, integritet i zaštita podataka preko TLS (SSL), internacionalizacija – Unicode, refereri, dodatne ekstenzije, otkrivanje sheme i sl.

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 postoji za Debian Linux i Solaris
- izvorni kod se nalazi na http://www.openldap.org

Imenički servisi
OpenLDAP – slapd.conf (1)

- Konfiguracija treba imati standardne sheme:
  - moguće dodati i opcionalne (npr. za DNS, sendmail, etc.)

```
include /staza/cosine.schema
include /staza/inetorgperson.schema
```

- Uključiti podršku za baze podataka:

```
moduleload back_ldbm.la
database ldbm
```

- Domena za koju dajemo LDAP informacije:

```
suffix "dc=domena1,dc=domena2,dc=hr"
```

- Administrativni DN (administrator):

```
rootdn "cn=ldapmanager,dc=vaša_domena,dc=hr"
rootpw lozinka_kakva_god
```

Imenički servisi
OpenLDAP – slapd.conf (2)

- Alternativno - DES:

```
rootpw {crypt}s4L9sOIJo4kBM
```

- Provjera rada:

```
ldapsearch -x -b '' -s base '(objectclass=*)'
  namingContexts
dn: namingContexts: dc=vaša_domena,dc=hr
```

- Dodavanje podataka:
  - offline: ldif2ldbm
  - online: ldapadd

Imenički servisi
OpenLDAP – CARNet paket

- specifičnosti:
  - Berkeley DB
  - BN (BaseName) je DNS tipa:
    dc=dns_tip, itd.
  - DN je UID tipa:
    uid=user_id,dc=domena,dc=hr
  - standardne sheme: core, inetorgperson, cosine, nis
- ldap://ds.carnet.hr/dc=hr
- http://ds.carnet.hr/ldap

Imenički servisi
OpenLDAP – postavljanje

- Pokrene se slapd
- Informacije se dodaju preko LDIF datoteka:

```
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

Imenički servisi
OpenLDAP – upotreba danas

- imenički servis - adress book (XEmacs, Netscape, Outlook, Eudora, etc.)
- konfiguracijske datoteke:
  - /etc direktorij - postoje migracijske skripte
  - sendmail conf
- autorizacija:
  - http - apache
  - YP/NIS zamjena - skripte + NSS

Imenički servisi
OpenLDAP – Sendmail (1)

- obavezne sheme:
  - include /usr/local/etc/openldap/slapd.at.conf
    include /usr/local/etc/openldap/slapd.oc.conf
- nova shema:
  - include /usr/local/etc/openldap/mail-routing.oc.conf
  - mora sadržavati:
    - attribute mailRoutingAddress cis
      attribute mailHost cis
      objectClass inetLocalMailRecipient
      requires objectClass
      allows mailLocalAddress, mailRoutingAddress, mailHost

Imenički servisi
OpenLDAP – Sendmail (2)

- prilikom kompiliranja (APPENDDEF):
  - confMAPDEF, confINCDIRS, confLIBSDIRS,confLIBS
- konfiguracija - ldap.mc
  - FEATURE(ldap_routing)
    LDAPROUTE_DOMAIN(foo.com)
    define(confLDAP_DEFAULT_SPEC, -h ldap.domena.hr -b dc=domena,dc=hr)
- test:
  - sendmail -bt
  - mailer esmtp, host mailhost1.domena.hr, user korisnik@domena.hr

FTP
Uvod

- FTP protokol – definiran u RFC959 i RFC1579
- Inicijalni RFC vrlo rano definiran (RFC959 sredinom 1985. koji je nadogradio 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
Wuftpd - uvod

- Wuftpd spada među najraširenije i najpoznatije FTP poslužitelje uz Proftpd
- Dostupan na adresi http://www.wuftpd.org
- Wuftpd 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
Wuftpd - osnovna konfiguracija

- ftpaccess – 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
Wuftpd - osnovna konfiguracija (2)

- ftpaccess (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
:   : :.gz:/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
Wuftpd - anonimni poslužitelj

- Wuftpd 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
Wuftpd - 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
Wuftpd - 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
Wuftpd - 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
Wuftpd - 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

Wuftpd - 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/paths.msg ^[-A-
  Za-z0-9\._]*$ ^\. ^-
```

FTP
Wuftpd - 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
Wuftpd - 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 Wuftpd
- Za testiranje Wuftpd može se koristiti debugiranje preko **–d** i/ili **–v** opcija proslijeđenih Ftpd

FTP
Wuftpd - 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 **ftpaccess**:

```
log transfers anonymous,guest,real inbound,outbound
```

FTP
Wuftpd - sažetak

- Konfiguracijske datoteke:
  - **ftpaccess** – 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.

FTP
ProFTPd - uvod

- Wuftpd - loš omjer kvalitete/sigurnosti
  - niz propusta u sigurnosti i dizajnu - dnevni exploiti
- ProFTPd:
  - http://www.proftpd.org/
  - kvaliteta, brzina, sigurnost
  - modularnost:
    - između ostaloga i PAM podrška
    - S/KEY mehanizam za FTP
  - jednostavno konfiguriranje i individualni .ftpaccess
  - samostojeći servis - daemon

FTP
ProFTPd - moduli (1)

- Glavni moduli:
  - mod_auth = autentifikacija
  - mod_core = konfiguracija i RFC-959 FTP naredbe
  - mod_ls = interni(!!) *listing* datoteka na sistemu
  - mod_site
  - mod_unixpw = *password* sistem
  - mod_xfer = FTP transfer naredbe
- OS ovisni modul:
  - mod_pam = PAM autentifikacija

FTP
ProFTPd - moduli (2)

- Razni dodatni moduli:
  - mod_readme = ispis readme datoteka
  - mod_ldap
  - mod_sql, mod_sql_mysql, mod_sql_postgres
- Moduli posebne namjene:
  - mod_linuxprivs, libcap
  - mod_quota
  - mod_ratio
  - mod_wrap

FTP
ProFTPd - konfiguriranje (1)

- `ServerName "ime posluzitelja"`
- `ServerType standalone`
- `Port 21`
- `#<Limit LOGIN>`
  `#  DenyAll`
  `#</Limit>`
- `User  nobody`
  `Group nogroup`
- `MaxInstances 30`
- `Umask  022`
- `TimeoutLogin  120`
- `TimeoutIdle  300`
- `TimeoutNoTransfer 600`
- `TimeoutStalled  900`
- `UseReverseDNS  on`
- `ScoreboardPath /var/run/proftpd`
- `TransferLog /var/log/xferlog`
- `<Global>`
  `DisplayLogin welcome.msg`
  `DisplayFirstChdir readme`
  `AllowOverwrite yes`
  `IdentLookups  off`
  `</Global>`

FTP
ProFTPd - konfiguriranje (2)

- virtualni poslužitelji:

```
<VirtualHost www.domena.hr>
 ServerAdmin ftp@domena.hr
 ServerName "ime"
 MaxLoginAttempts 2
 RequireValidShell no
 TransferLog
   /var/log/xferlog.nesto
 MaxClients 50
 DefaultServer on
 DefaultRoot ~ !staff
 AllowOverwrite yes
/VirtualHost>
```

- anonimni ftp:

```
<Anonymous ~ftp>
MaxClients 5 "Sorry, max %m
   users -- try again later"
User ftp
Group ftp
UserAlias anonymous ftp
<Limit WRITE>
  DenyAll
</Limit>
... itd ...
</Anonymous>
```

FTP
ProFTPd - konfiguriranje (3)

- limiti logiranja:

```
<Limit LOGIN>
  Order deny,allow
  Deny from 161.53.70.,
   .evil.net
  Allow from all
</Limit>
```

- guest korisnik:

```
<Anonymous ~guest>
User  guest
Group nobody
AnonRequirePassword on
```

- filesystem limiti i modifikacije:

```
<Limit READ DIRS>
 AllowAll
 IgnoreHidden on
</Limit>
HideUser root
<Directory negdje/public>
 <Limit STOR MKD RMD>
  AllowAll
 </Limit>
</Directory>
```

FTP
Libc: 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 /

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

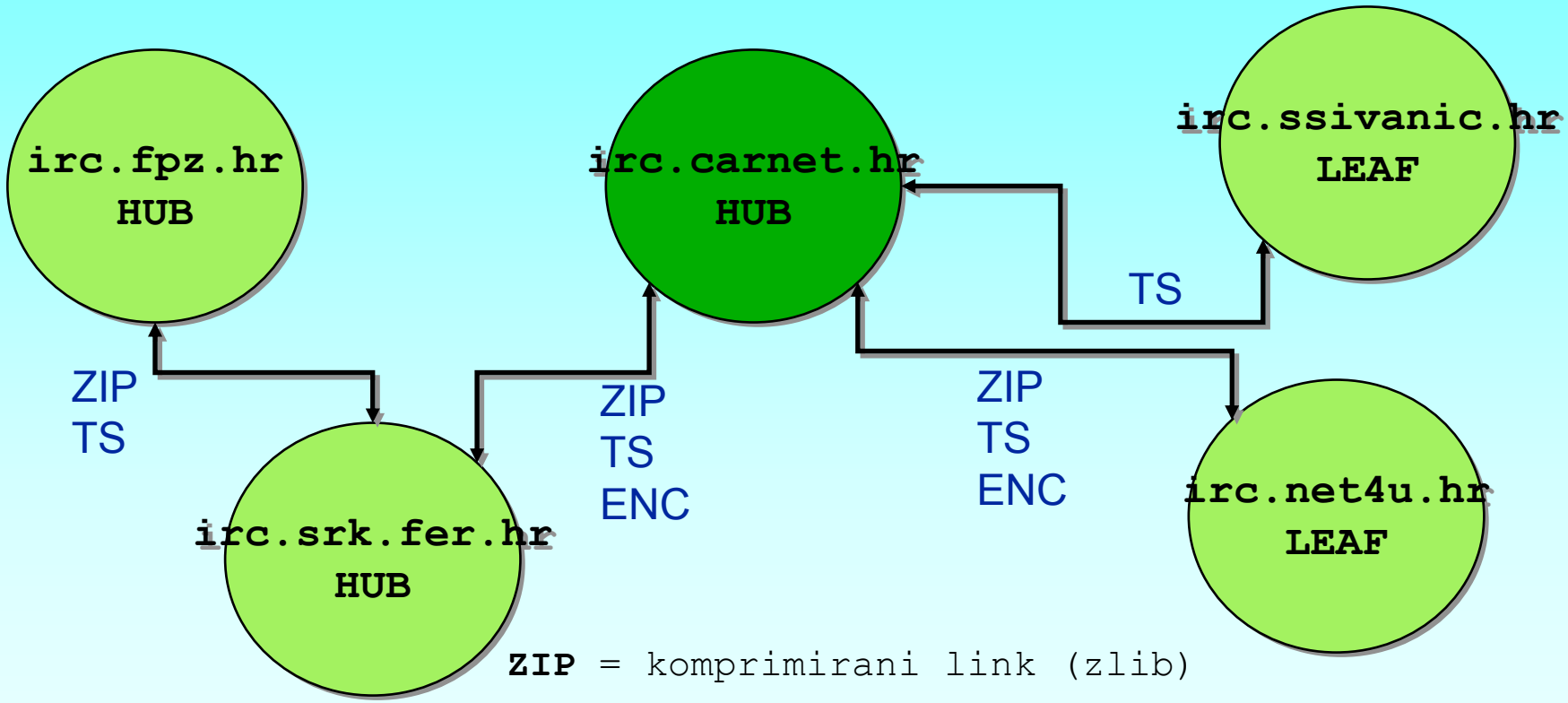
IRC
Uvod (3)

- 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



ZIP = komprimirani link (zlib)

TS = TimeStamp

ENC = enkripcija (BF 256 + RSA 256)

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:
  - otimanje 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, kompliciranа 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:070v1FfQIiJgs: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 specificiran 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, poboljšan 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
  - Slrn
  - Tin
  - Trn ...
- Windows:
  - Netscape Navigator
  - MS Outlook ...

News
INN

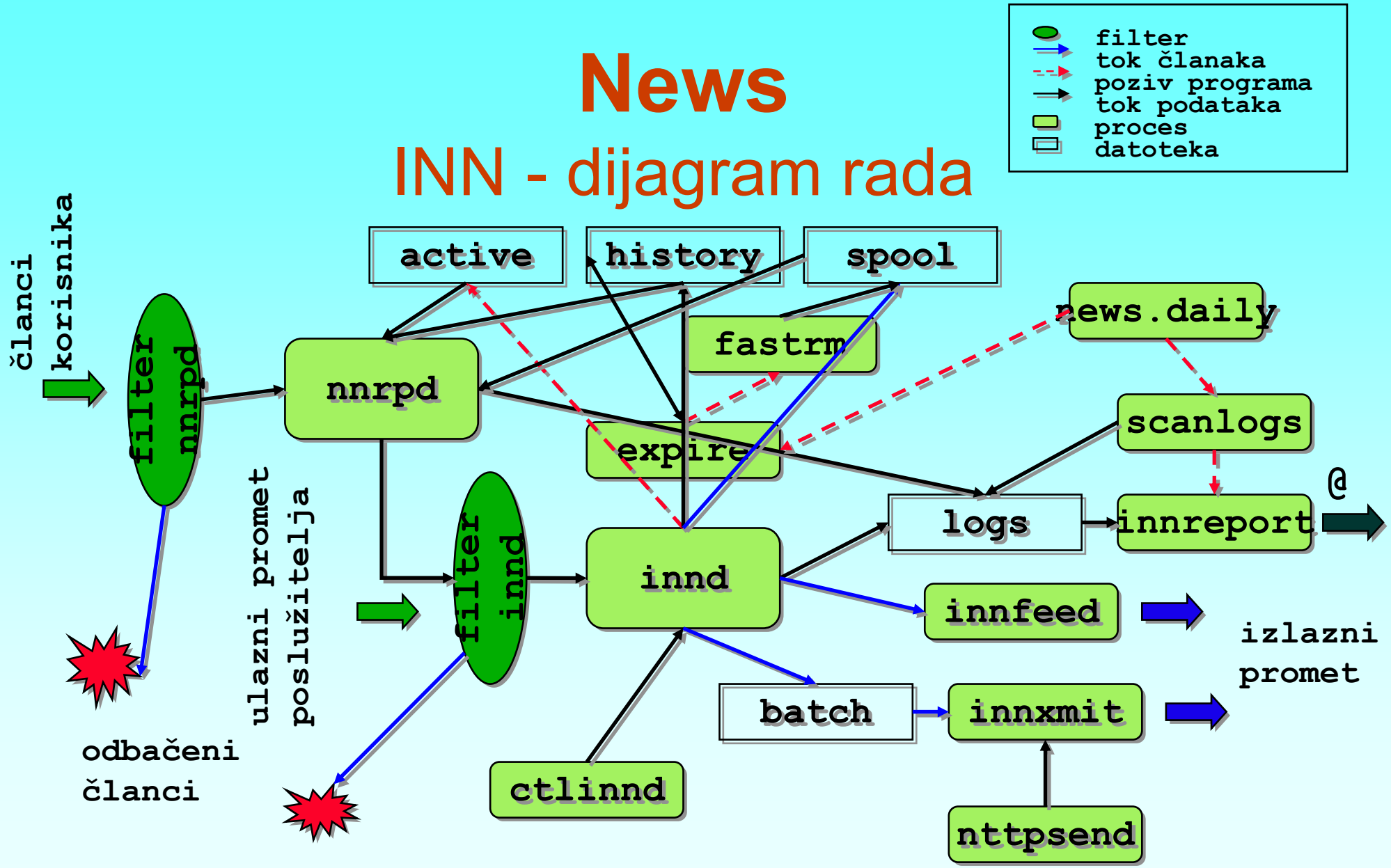
- INN – rješen u vidu različitih skripti (Perl, Sh) i programa koji međusobno komuniciraju
- Tri standardne arhitekture i jedna vrlo rijetka:
  - centralizirana
  - distribuirana – dijeljeni news article spool
  - distribuirana – replikacija članaka
  - distribuirana – news cache
- Posve različiti načini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

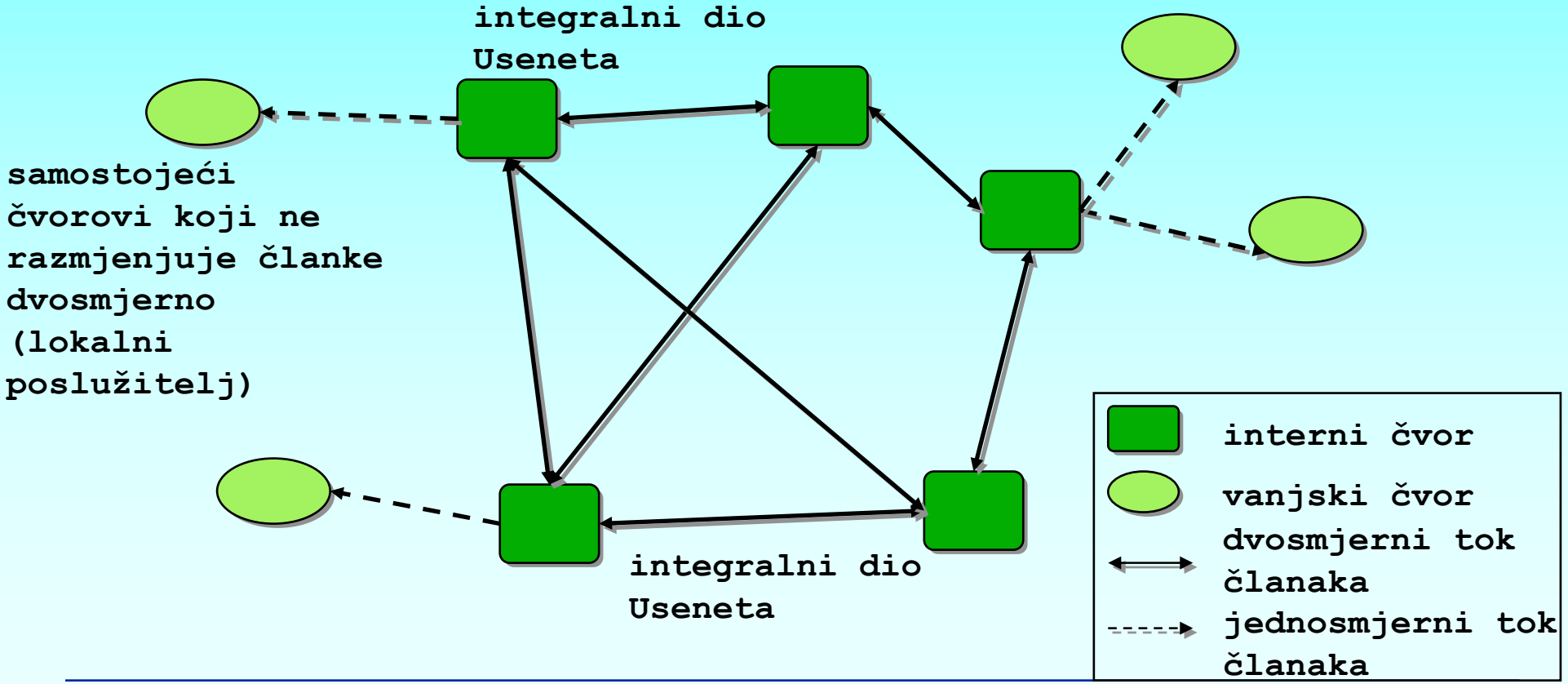
News
INN – centralizirana arhitektura (4)

- 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 zajednike 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

- Konfiguranje 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.nntp = hostovi kojima se šalju članci
  - server, organization = ime poslužitelja ...
  - nnrp.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, Dtlogin, 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

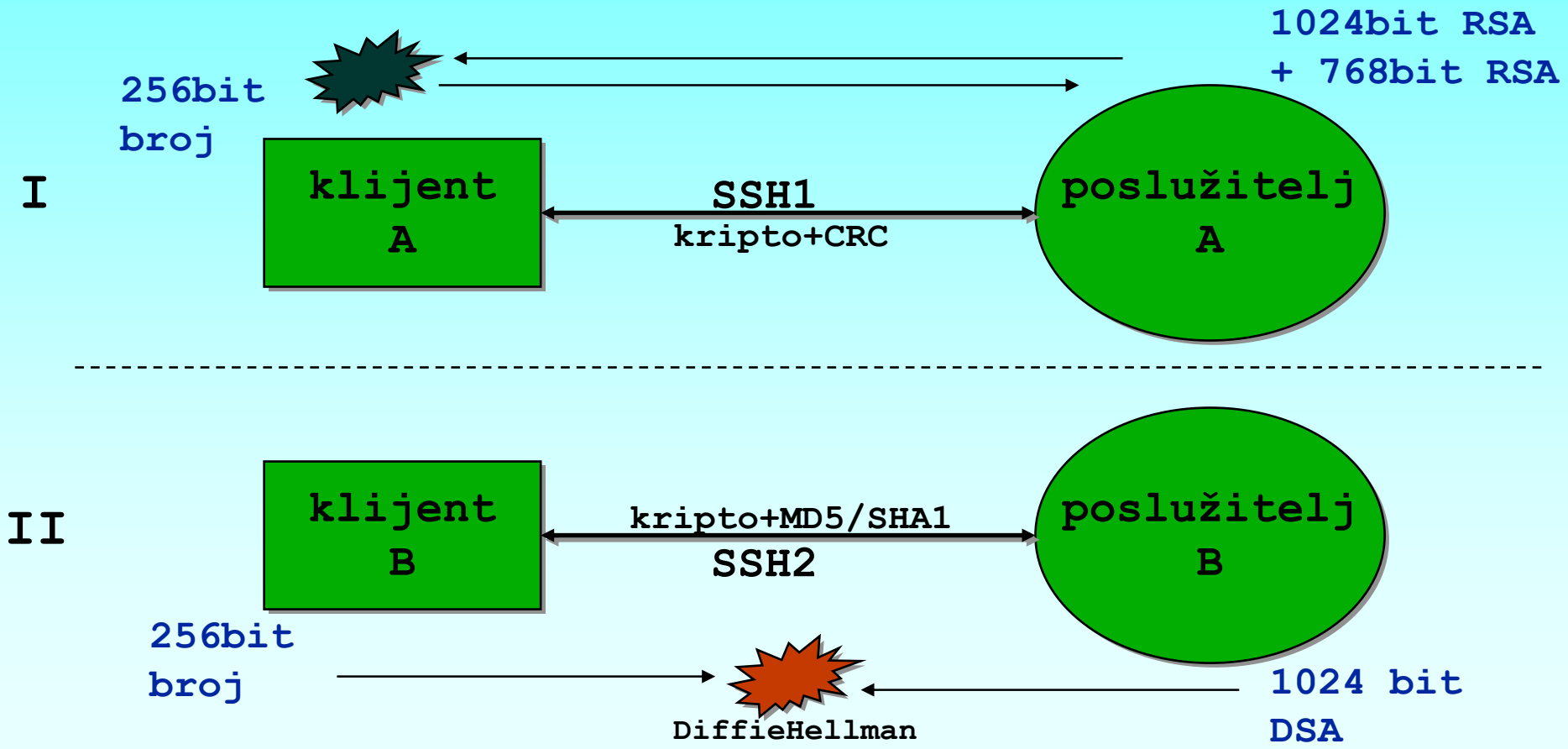
- Svaki poslužitelj ima **1024-bitni RSA** ključ na disku
- Svaki sat - novi **768-bitni RSA** ključ (ne na disku!)
- Poslužitelj pošalje klijentu oba ključa, ovaj generira **256-bitni** "slučajni" broj (svoj ključ) kriptiran pomoću prva dva i šalje nazad
- Nakon uspješnog handshakinga se taj broj koristi 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 hmcsha1 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 `~~.`
- SFTP subproces:
  `sftp kreator@malik.srce.hr`

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/ttssh.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_securid)
- 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)

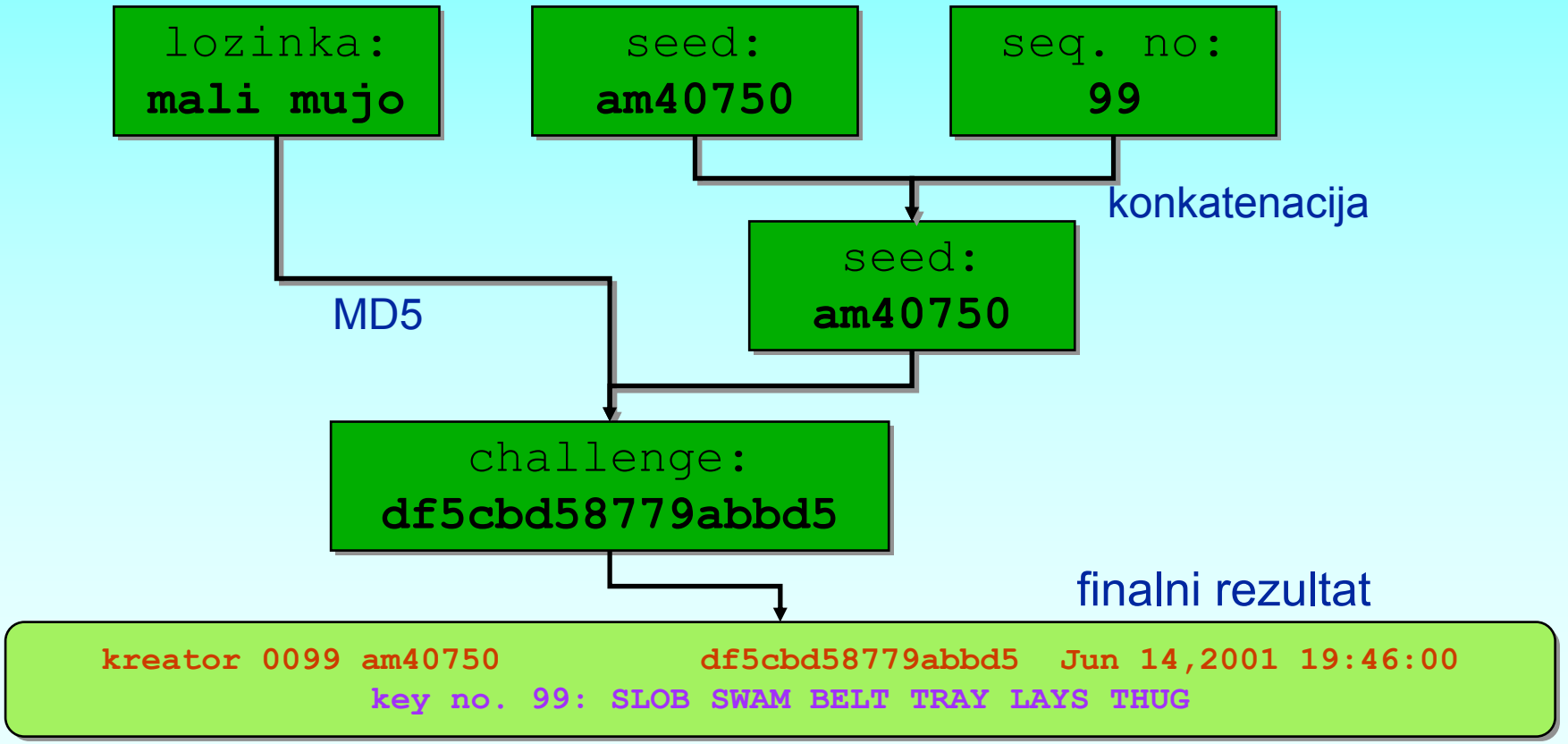
- Prisluškivanje mreže → dobiveno korisničko ime i lozinka
- Rješenje: jednokratne lozinke ⇒ privatne informacije su dostupne – ali ne i sam pristup!
- Zahtjevi za OTP:
  - generator određenih ključeva na osnovu tajne lozinke i informacije s poslužitelja unaprijed generira određen broj ključeva
  - program 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 Telneta!)
- 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 zalihosti = 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

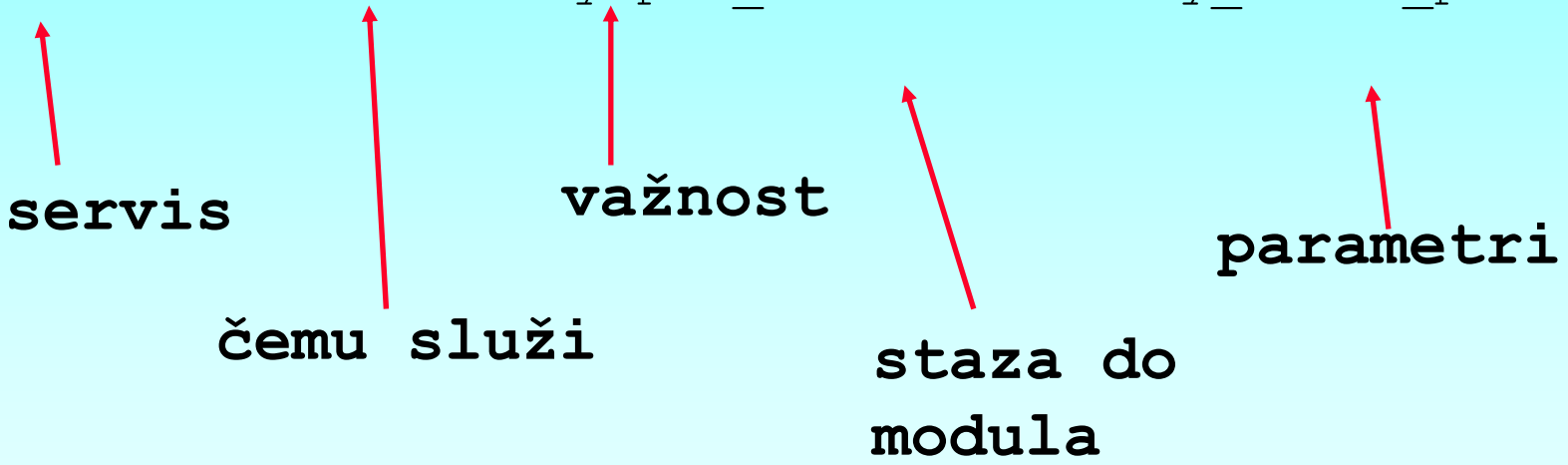
Zaštita privatnosti
S/Key – implementacija

- CARNet S/Key paket:
  - nekad - Skey izvađen iz Logdaemon paketa
  - danas - samostojeći PAM (Pluggable Autentification Module)
    - integracija u postojeći sistem bez modificiranja 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 fl0328002
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

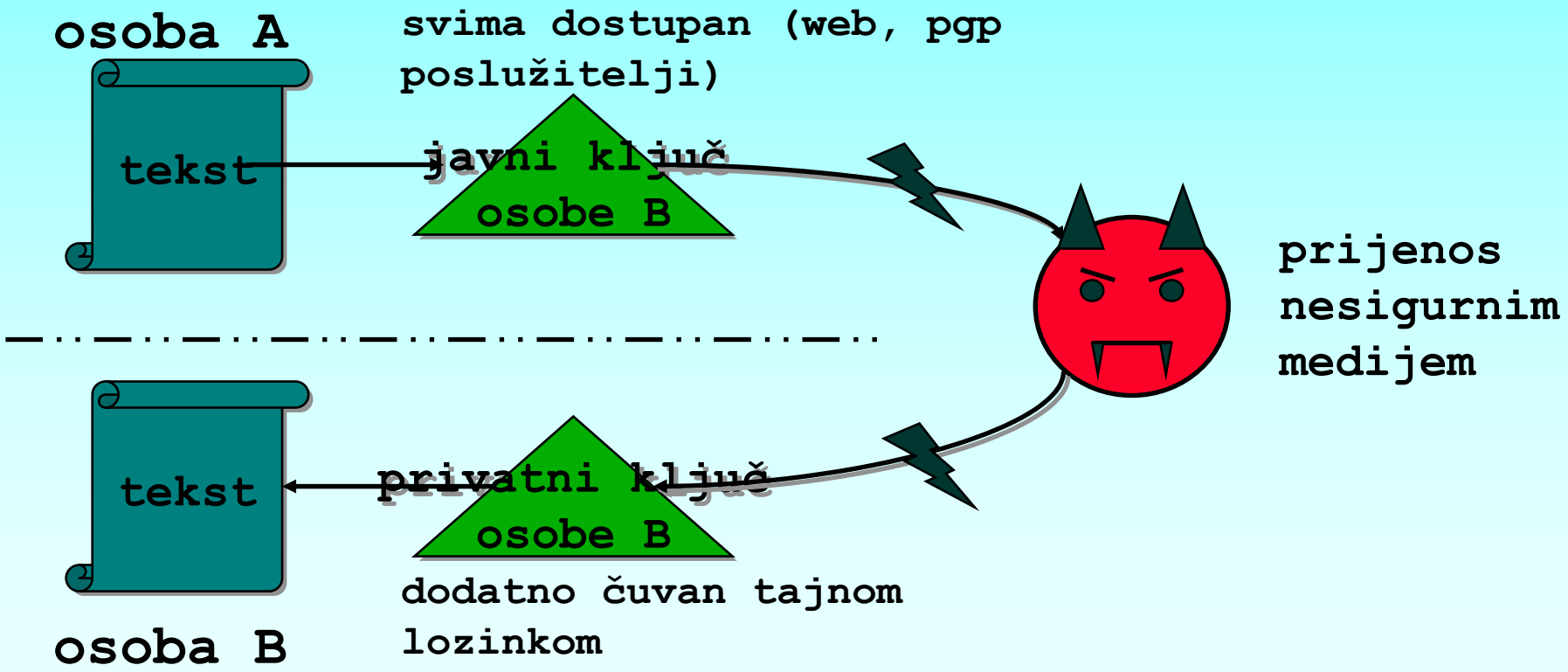
Zaštita privatnosti
PGP – teorija (5)

- 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 ...

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.wuftpd.org/wu-ftpd-faq.html
  http://www.wuftpd.org/HOWTO/
  http://www.wuftpd.org/rfc/
- "Setting Up Secure FTP"

Literatura (2)

- **Anonymous FTP FAQ:**
  http://www.landfield.com/wu-ftpd/docs/anonymous-ftp-faq.html
- **Guest HOWTO:**
  http://www.wu-ftpd.org/HOWTO/guest.HOWTO
- **Setting Up wuftpd for Non-Anonymous Accounts:**
  http://glennf.com/writing/wuftpd.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.ffii.org/~phm/pgphlpen.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