

Gradivo iz vaj pri predmetu “Odprta koda in informacijska varnost”

Izbirni seminar na Fakulteti za družbene vede, Univerza v Ljubljani v študijskem letu 2007/2008.

~ izbrana poglavja ~

Navodila so namenjena študentom kot učni pripomoček.
V navodilih je obravnavanih samo del tem, ki so bila predstavljena na predavanjih.

(CC) Matej Kovačič, 2008

Delo je izdano pod Creative Commons licenco: “Priznanje avtorstva-Nekomercialno-Deljenje pod enakimi pogoji 2.5 Slovenija”.
Celotno pravno besedilo licence je dostopno na spletni strani: <<http://creativecommons.org/licenses/by-nc-sa/2.5/si/legalcode>>, ali na
poštnem naslovu: Inštitut za intelektualno lastnino, Streliška 1, 1000 Ljubljana.

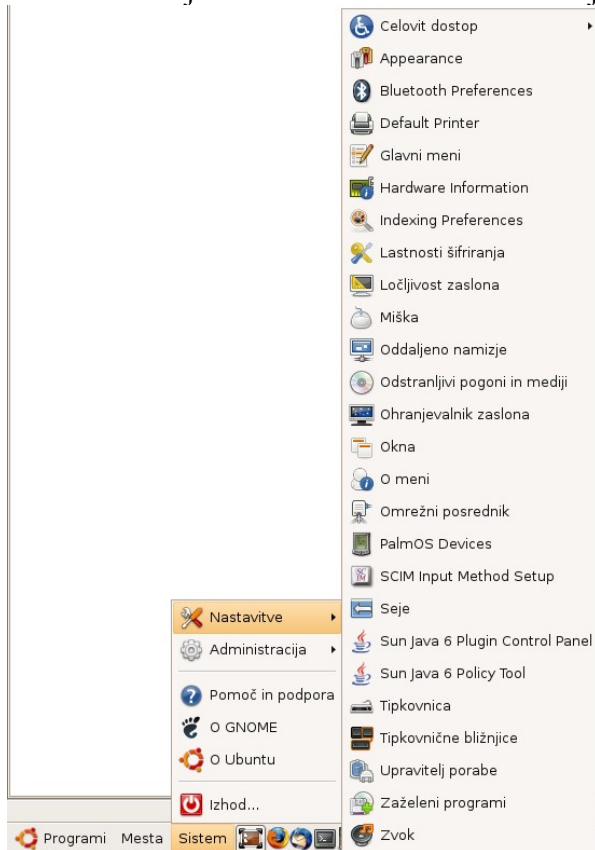
Kazalo vsebine

| | |
|--|----|
| Nastavitve namiznega okolja v Ubuntu Linuxu..... | 3 |
| Spreminjanje elementov pulta (“opravilne vrstice”) in prilagoditev izgleda okolju Windows..... | 4 |
| Ostale pomembnejše nastavitve..... | 5 |
| Sinhronizacija časa..... | 6 |
| Nameščanje programskih paketov..... | 7 |
| Seznami skladišč programskih paketov..... | 7 |
| Nameščanje programskih paketov s pomočjo orodja Synaptic..... | 9 |
| Delo z datotekami..... | 10 |
| Ukaz sudo (in gksu)..... | 11 |
| Sprememba gesla..... | 12 |
| Dodajanje uporabnikov in nastavljanje pravic uporabnikom..... | 13 |
| Zagonski nalagalnik GRUB..... | 14 |
| Optimizacija sistema..... | 16 |
| Razdelki (particije)..... | 17 |
| Pisarniški paket OpenOffice.org..... | 19 |
| Delo z besedilom (OpenOffice.org Word processor)..... | 19 |
| Delo s preglednicami (OpenOffice.org Spreadsheet)..... | 20 |
| Predstavitve (OpenOffice.org Presentation)..... | 20 |
| Pretvornik za docx datoteke..... | 20 |
| Uporaba črkovalnika..... | 20 |
| Odpiranje multimedijskih datotek..... | 22 |
| Pisanje na NTFS razdelke..... | 23 |
| Povezovanje med sistemi..... | 24 |
| Emulacija..... | 25 |
| Virtualizacija..... | 28 |
| Namestitev VirtualBoxa..... | 28 |
| Nastavitev virtualnega stroja..... | 29 |
| Varnost informacijskih sistemov..... | 31 |
| Varno uničevanje podatkov..... | 32 |
| Prepisovanje podatkov v okolju Windows..... | 32 |
| Uporaba orodja za preverjanje slabih sektorjev na disku v Linuxu..... | 32 |

| | |
|--|----|
| Brisanje "praznega" prostora na disku in uporaba ukaza shred..... | 32 |
| Uporaba orodja dd (disk dump) v Linuxu..... | 33 |
| Uporaba orodja DBAN..... | 34 |
| Obnavljanje podatkov..... | 35 |
| Šifriranje..... | 36 |
| Šifrirni algoritmi..... | 36 |
| Varnost zgoščenih algoritmov..... | 37 |
| Napredni matematični napadi na kriptografijo..... | 37 |
| Steganografija..... | 38 |
| Šifrirne nastavitve in šifrirna programska oprema v Ubuntu Linuxu..... | 38 |
| Povezovanje s ssh..... | 40 |
| Avtentikacija oddaljenega računalnika..... | 40 |
| Avtentikacija (prijava) uporabnika..... | 41 |
| Priprava ključev za avtentikacijo s ključem..... | 41 |
| Sprememba imena gostitelja oz. naslova oddaljenega računalnika..... | 41 |
| Izstop iz ssh seje..... | 42 |
| Grafični dostop do aplikacij preko ssh tunela..... | 42 |
| Reverzni ssh tunel..... | 43 |
| Povezovanje na alternativna vrata..... | 43 |
| Varnostne kopije..... | 44 |
| Požarni zid..... | 46 |
| Samodejni zagon požarnega zidu Firestarter ob zagonu računalnika..... | 52 |
| Povezovanje v VPN omrežja..... | 54 |
| Nastavitev odjemalca..... | 54 |

Nastavitve namiznega okolja v Ubuntu Linuxu

Grafično okolje Ubuntu Linuxa lahko nastavljamo v meniju *Sistem – Nastavitve*:



Nekatere podrobnejše možnosti nastavitvev:

- izgled oken, ozadja in vklop učinkov namizja (razni vizualni efekti oken, plapolajoča okna, itd.): *Sistem – Nastavitve – Appearance*.
- Nastavitvev tipkovnice in nastavitvev razporeditve tipkovnice (izbira slovenske, angleške, itd. tipkovnice): *Sistem – Nastavitve – Tipkovnica*. Če želimo, da se na okenskem pultu pojavi indikator tipkovnice (za preklapljanje med različnimi razporeditvami tipkovnic), moramo v pult vključiti poseben gradnik (*applet*).
- Nastavitvev ločljivosti zaslona in zasuk zaslonske slike (zrcalno, rotirano): *Sistem – Nastavitve – Ločljivost zaslona*.
- Nastavitvev obnašanja oken (načina preklapljanja med okni, načina aktiviranja oken): *Sistem – Nastavitve – Okna*.
- Nastavitve miške (občutljivost, obnašanje): *Sistem – Nastavitve – Miška*.
- Vklop, izbira in nastavitvev ohranjevalnika zaslona: *Sistem – Nastavitve – Ohranjevalnik zaslona*.
- Nastavitvev zvočnega sistema (priporočena je uporaba privzetega zvočnega sistema ALSA) ter nastavitvev sistemskih zvokov: *Sistem – Nastavitve – Zvok*.
- Če želimo lahko nastavimo privzete samodejne akcije ob priklopu odstranljivih pogonov ali vstavitvi CD/DVD plošč v računalnik: *Sistem – Nastavitve – Odstranljivi pogoni in mediji*. Nastavimo lahko ali naj se USB ključki samodejno priključijo, kateri naj bo privzeti predvajalnik za video DVD-je, itd.
- Nastavimo lahko privzeti spletni brskalnik in privzeti odjemalec elektronske pošte: *Sistem – Nastavitve – Zaželeni programi*.
- Vnos podatkov o uporabniku: *Sistem – Nastavitve – O meni*.

- Pregled strojne opreme: *Sistem – Nastavitve – Hardware information*.
- Pregled informacij o sistemu (procesor, pomnilnik, diskovni pogoni, pregled delujočih procesov, obremenitev sistema,..): *Sistem – Administracija – Nadzornik sistema*
- Nastavimo lahko kateri programi se bodo samodejno zagnali ob uspešni prijavi uporabnika v sistem: *Sistem – Nastavitve – Seje*
- Če želimo lahko uredimo sistemski meni (meni Programi): *Sistem – Nastavitve – Glavni meni*. Dodajamo ali odstranjujemo lahko posamezne vnose (programe) v meniju.

Spreminjanje elementov pulta (“opravilne vrstice”) in prilagoditev izgleda okolju Windows

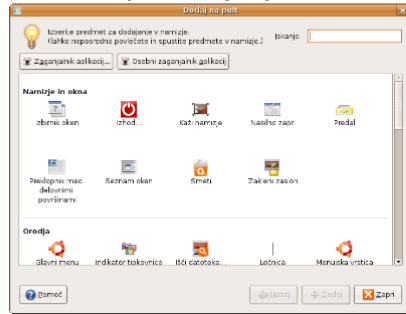
Ubuntu ima v privzetem okolju na vrhu in na dnu zaslona dve “opravilni vrstici” (podobno kot Start opravilna vrstica v okolju Windows). Tej “opravilni vrstici” se v Ubuntu Linuxu reče *pult*. Če želimo, da bo Ubuntu izgledal podobno kot Okna, lahko zgornji pult odstranimo. Z desnim miškinim gumbom kliknemo na zgornji pult in izberemo *Odstrani ta pult*.

Nato prilagodimo še spodnji pult. Z desnim miškinim gumbom kliknemo manj in izberemo *Dodaj na pult*. Odpre se okno iz katerega na pult vlečemo posamezne elemente. Obstoječe elemente lahko odstranimo z desnim klikom in izbiro *Odstrani iz pulta*. Če želimo, jih lahko premaknemo, vendar jih je potrebno najprej odkleniti (desni klik - odstranimo kljukico iz *Prikljeni na pult*). Predmet premaknemo tako, da z desnim miškinim gumbom kliknemo nanj ter izberemo *Premakni*. Izbrani element sedaj z miško premikamo levo ali desno in ko nastavimo željeni položaj kliknemo z miškinim levim gumbom in predmet fiksiramo. Če želimo, ga sedaj lahko ponovno priklenemo na izbrano mesto.

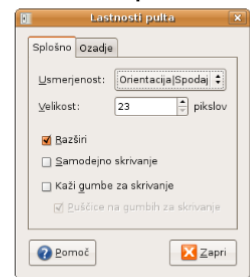
Ubuntu ima na voljo številne elemente pulta, ena izmed možnih razporeditev je prikazana na spodnji sliki:

Kako pult v Ubuntu približati opravilni vrstici v Windows?

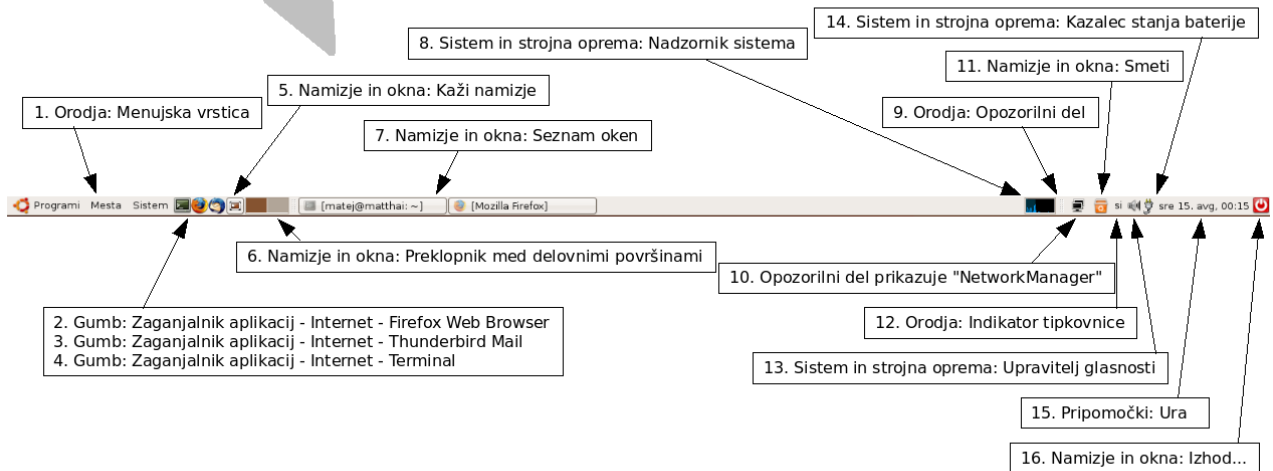
Desni klik na pult - Dodaj na pult



Desni klik na pult - Lastnosti



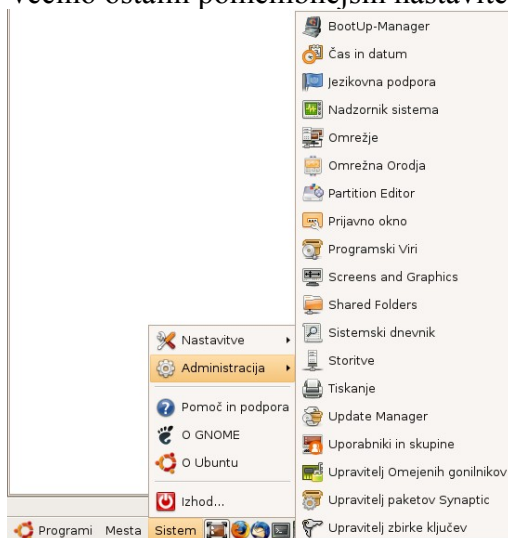
Usmerjenost:
Orientacija | Spodaj
Velikost:
lahko pomanjšamo debelino vrstice



Z desnim klikom na pult in izbiro *Lastnosti*, lahko določimo še širino in mesto pulta ter nekatere druge lastnosti. Pri nekaterih elementih lahko podobno kot pri pultu izberemo in nastavimo lastnosti.

Ostale pomembnejše nastavitve

Večino ostalih pomembnejših nastavitvev opravimo v meniju *Sistem – Administracija*.



Opomba: na sliki so vključene možnosti dodatnih nastavitvev, ki niso del privzete namestitve sistema,

pač pa so bile dodane kasneje.

- Jezikovne pakete za dodatno jezikovno podporo namestimo preko menija: *Sistem – Administracija – Jezikovna podpora*. Nastavimo tudi privzeti jezik. Razporeditev tipkovnice je potrebno nastaviti posebej. Jezikovne nastavitve se uveljavijo po odjavi in ponovni prijavi v sistem.
- Nastavitve omrežja (Network Manager): *Sistem – Administracija – Omrežje*.
- Na voljo so tudi nekatera omrežna orodja (npr. ping, skeniranje vrat, pot sledenja (*traceroute*), Whois, itd.): *Sistem – Administracija – Omrežna orodja*.
- Nastavitve prijavnega okna (pred vstopom v sistem): *Sistem – Administracija – Prijavno okno*.
- Ubuntu 7.10 sicer sam zazna USB tiskalnice, ko jih priključimo na računalnik in samodejno namesti (aktivira) ustrezne gonilnike. Tiskalnice vezane na paralelna vrata (LPT) in omrežne tiskalnice pa nastavimo v meniju: *Sistem – Administracija – Tiskanje*. Privzeti tiskalnik določimo v meniju: *Sistem – Nastavitve – Default printer*.

Sinhronizacija časa

Z desnim gumbom miške kliknemo na uro na menujski vrstici in izberemo *Nastavi datum in uro*. Pri *Nastavitve* izberemo *Keep synchronized with Internet servers*. Po potrebi pod *Časovni strežniki* izberemo še slovenske časovne strežnike (*ntp1.arnes.si*, *ntp2.arnes.si* in/ali *goodtime.ijs.si*). Preverimo še, če imamo nastavljen ustrezen časovni pas. Sedaj se bo čas na računalniku samodejno sinhroniziral oz. nastavil na točen čas.

Nameščanje programskih paketov

Ubuntu omogoča preprosto nameščanje programske opreme. To lahko storimo na več načinov:

- pomočjo programa Synaptic: *Sistem – Administracija – Upravitelj paketov Synaptic*,
- tako, da iz interneta prenesemo ustrezeni programski paket (s končnico .deb) in dvokliknemo nanj,
- iz ukazne vrstice,
- ročno prevedemo izvorno kodo programa (razmeroma zapleten način, ki ga običajni uporabniki praviloma ne uporabljajo).

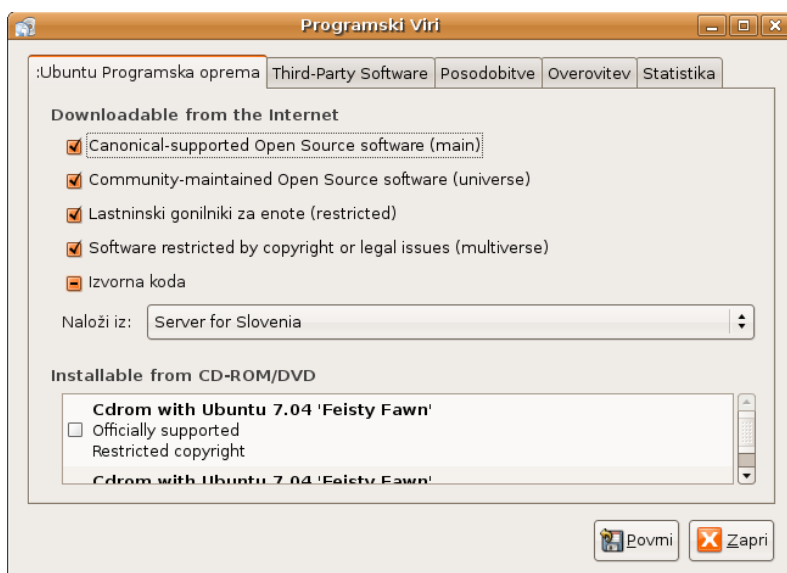
Za nameščanje nove programske opreme ali nadgrajevanje sistema je seveda potrebno imeti administratorske pravice zato orodja za nameščanje programskih paketov ob zagonu zahtevajo administratorsko geslo.

Programski paketi se nahajajo v obliki posebnih datotek s končnico .deb, oz. tim. deb paketkov. Sistem poišče ustrezen deb paketek, ga prenese iz interneta in namesti. Deb paketi vsebujejo opis programa, vendar so opisi razmeroma kratki, enovrstični.

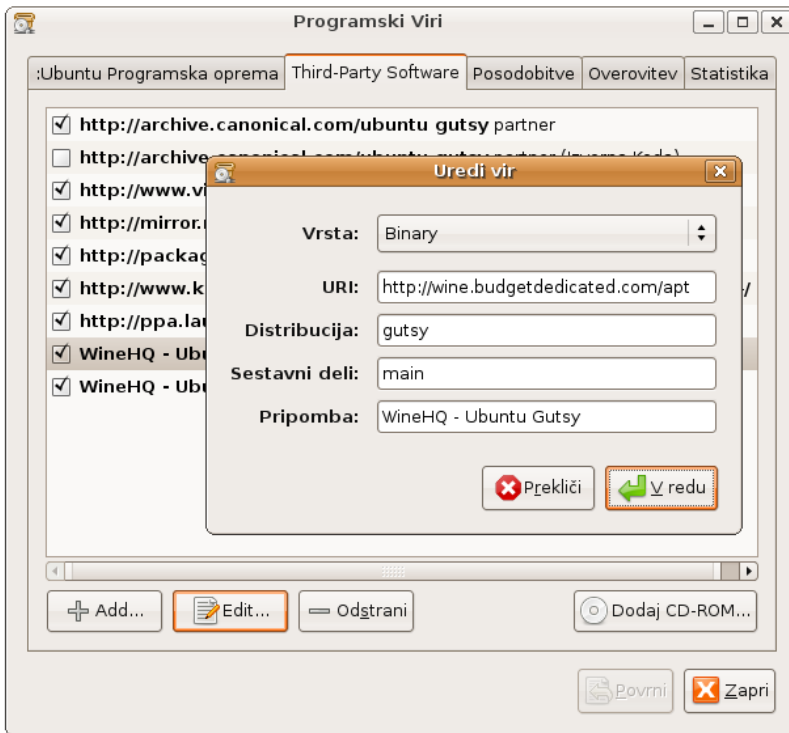
Seznami skladišč programskih paketov

Programske pakete dobimo v posebnih skladiščih (v angleščini jim rečemo *repository*). Skladišča vzdržujejo in dopolnjujejo razvijalci oz. vzdrževalci (ang. *maintainers*).

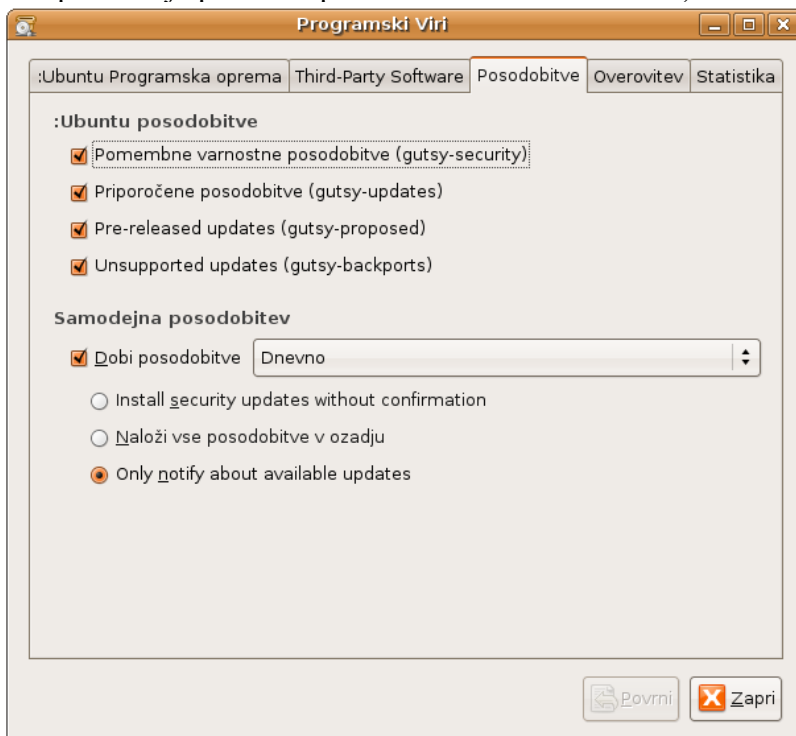
Uradna distribucija Ubuntu v svojih skladiščih nudi le omejen nabor programskih paketov, saj podpirajo le strogo odprtokodne pakete in pakete brez licenčnih omejitev. Če torej želimo nameščati dodatno programsko opremo (npr., dodatne pisave in kodeke), je treba v lokalni seznam skladišč, ki jih bomo uporabljali vključiti dodatna skladišča, ki vsebujejo programske pakete. To storimo v meniju: *Sistem – Administracija – Programski viri*. V meniju označimo tudi katere programske posodobitve želimo sprejemati.



V zavihku *Third-Party Software* lahko s klikom na gumb *Add* dodamo skladišče oz. vir programskih paketov:



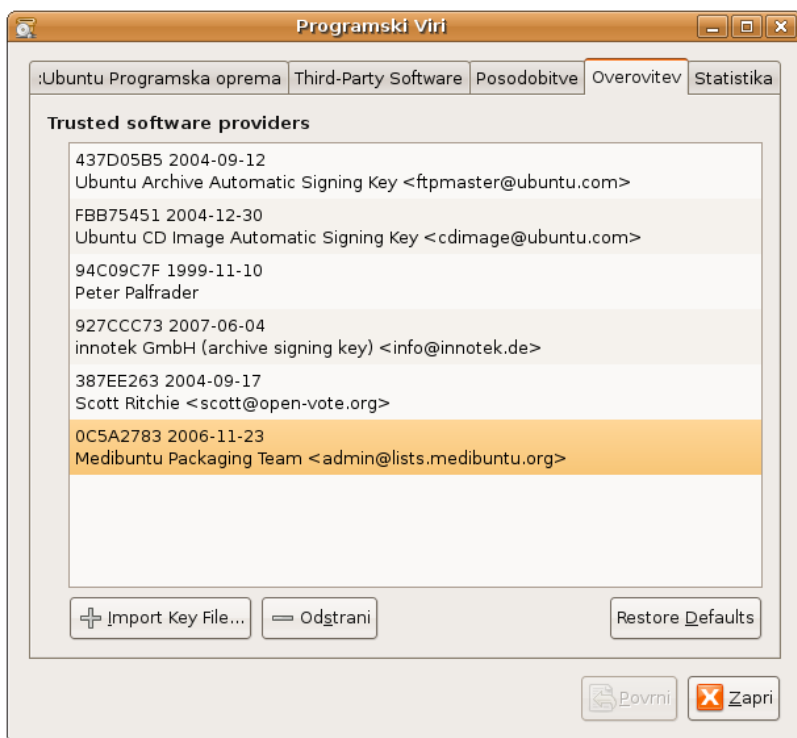
V zavihku *Posodobitve* obkljukamo katere posodobitve želimo prejemati in kako pogosto (npr. dnevno ali redkeje) naj Ubuntu preverja ali so v skladiščih s posodobitvami na voljo kakšne nove posodobitve. Označimo tudi ali naj sistem samodejno namesti nove posodobitve, ali posodobitve v ozadju prenese in pred namestitvijo vpraša ali pa naj o posodobitvah samo obvesti uporabnika (v tem primeru je potrebno posodobitve namestiti ročno).



Zaradi varnosti so programski paketi v skladiščih digitalno podpisani s šifrnimi ključi vzdrževalcev skladišč. Ta varnostni mehanizem omogoča, da operacijski sistem preveri pristnost programskih paketov, ki jih prenese iz interneta. S tem preveri če ni morda napadalec izvedel tim.

napad s posrednikom, torej se nam na internetu lažno predstavlja kot eno izmed veljavnih skladišč programskih paketov in nam nato podtakni lažni programski paket.

Da bi sistem lahko preveril pristnost digitalno podpisanih programskih paketov mora imeti shranjene javne šifrirne ključe vzdrževalcev skladišč, ki so te programske pakete podpisali. Šifrirne ključe, ki jih navadno dobimo na spletnih straneh vzdrževalcev ali skladišč programskih paketov v sistem upravljanja s paketi uvozimo s klikom na gumb *Import Key file*:



Nameščanje programskih paketov s pomočjo orodja Synaptic

Grafična namestitev poteka tako, da najprej zaženemo Synaptic, ki se nahaja v meniju: *Sistem – Administracija – Upravitelj paketov Synaptic*. Program nas najprej vpraša za administratorsko geslo.

Nato v orodni vrstici kliknemo na *Iskanje...* in vnesemo ime programskega paketa, ki ga želimo namestiti. Pred tem seveda moramo v naš lokalni seznam skladišč programskih paketov vključiti skladišče, ki želeni programski paket vsebuje.

Program označimo za namestitev (desni klik in izbira iz menija) nato pa kliknemo gumb *Uveljavi*. Če ga želimo odstraniti, ga označimo za odstranitev ali popolno odstranitev.

Ubuntu nas sam opozarja na čakajoče posodobitve sistema (prikaže obvestilo na pultu). Ročno jih preverimo iz menija: *Sistem – Administracija – Update Manager*. Na *Sistem – Administracija – Programski viri* pa določimo interval v katerem naj sistem preverja za nove posodobitve.

Delo z datotekami

Seznam uporabniških map ter izmenljivih nosilcev se nahaja na Mesta – Home Folder. Za delo z datotekami skrbi program *Nautilus* (podobno kot v okolju windows File Explorer).

- Ustvarjanje, kopiranje, brisanje (v koš), trajno brisanje: z desnim klikom na datoteko ter tipkami *delete* (brisanje v koš), *shift-delete* (trajno brisanje), premikanje v drugo mapo, z miško, kopiranje v drugo mapo z miško in držanjem tipke *Ctrl*, povezovanje v drugo mapo (premik z miško ter držanje *Ctrl-shift*). Če datoteko permaknemo z miško in držimo *Alt*, se po tek, ko datoteko izpustimo odpre meni z možnimi akcijami.
- Lastniške pravice nad datotekami: desni klik na datoteko. Nastavimo lahko dovoljenja za lastnika, skupino ter ostale.
- Če je datoteka označena za branje jo ne moremo spreminjati, lahko pa jo izbrišemo!

Ukaz sudo (in gksu)

Ukaz sudo sistemu pove, da želimo nek ukaz pognati z administratorskimi pravicami. Seveda moramo v naslednjem koraku vpisati administratorsko geslo. Ker si sistem za nekaj časa (seveda samo v isti seji) zapomni sistemsko geslo, nam ga v primeru da ukaz sudo uporabimo večkrat v kratkem času ni treba kar naprej vpisovati. Sudo seveda ni treba vpisovati če smo že prijavljeni kot korenski uporabnik, vendar pa je Ubuntuju iz varnostnih razlogov korenski uporabnik onemogočen.

Gksu je grafični ekvivalent ukaza sudo. Ko nek ukaz zaženemo v gksu načinu, se zaslon potemni in odpre se okno za vnos gesla.

Primer: odpremo ukazno vrstico: *Programi – Pripomočki – Terminal* in vnesemo ukaz: “gksu nautilus”.

Sprememba gesla

Lastno geslo spremenimo v meniju: *Sistem – Nastavitve – O meni*. Sistem iz varnostnih razlogov ne dovoli imeti kratkega gesla. Če kljub temu želimo nastaviti krajše (in manj varno geslo), v ukazno vrstico (*Programi – Pripomočki – Terminal*) vnesemo ukaz: “`sudo passwd ime_uporabnika`”. Najprej vnesemo trenutno geslo, nato pa sledimo navodilom na zaslonu.

V primeru, da geslo pozabimo, računalnik zaženemo v varnem načinu (v zagonskem meniju, tim. zagonskem nalagalniku – ang. *boot loader GRUB*) izberemo *recovery mode*, sistem se zažene v ukazni vrstici, kjer vnesemo ukaz “`sudo passwd ime_uporabnika`” nato pa računalnik ponovno zaženemo z ukazom “`sudo reboot`”.

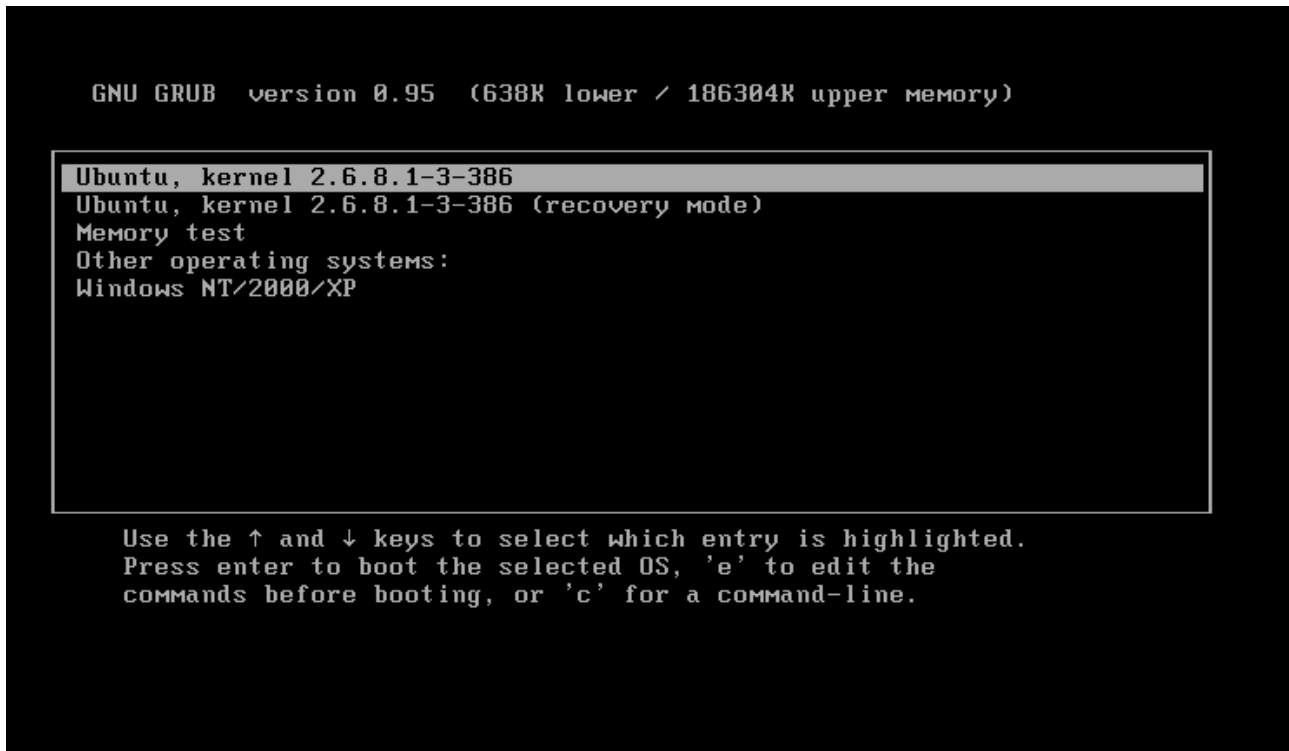
Dodajanje uporabnikov in nastavljanje pravic uporabnikom

Uporabimo meni: *Sistem – Administracija – Uporabniki in skupine*.

Zagonski nalagalnik GRUB

Zagonski nalagalnik GRUB (ang. *boot loader* GRUB) je program, ki omogoča zagon različnih operacijskih sistemov. Uporabjen je primeru, če imamo na računalniku poleg Linuxa nameščen še kakšen drug operacijski sistem.

V tem primeru bo Ubuntu kot privzeti operacijski sistem nastavil sebe, če pa želimo zagnati npr. Windows, pa bo potrebno ob zagonu računalnika izbrati ustrezen vnos v GRUB meniju.



```
GNU GRUB version 0.95 (638K lower / 186304K upper memory)

Ubuntu, kernel 2.6.8.1-3-386
Ubuntu, kernel 2.6.8.1-3-386 (recovery mode)
Memory test
Other operating systems:
Windows NT/2000/XP

Use the ↑ and ↓ keys to select which entry is highlighted.
Press enter to boot the selected OS, 'e' to edit the
commands before booting, or 'c' for a command-line.
```

Če v določenem času (tim. *timeout*) ne izberemo ničesar, se samodejno naloži privzeti operacijski sistem.

V Grub meniju lahko zaženemo Ubuntu v varnem načinu (*recovery mode*), poženemo test pomnilnika RAM (*Memory test*) ali izberemo kakšen drug, neprivzeti operacijski sistem (npr. Windows).

Če želimo spremeniti privzeti operacijski sistem in in *timeout*, je potrebno urediti datoteko z menijskimi vnosi. To storimo tako, da v ukazni vrstici (*Programi – Pripomočki – Terminal*) vnesemo naslednji ukaz: “`gksu gedit /boot/grub/menu.lst`”.

Odpre se tekstovna doteka, ki jo lahko urejamo. Pri urejanju je seveda potrebna previdnost.

Na začetku (nekje okrog vrstice 14) poiščemo vrstico:

```
default 0
```

S spremembo številke 0 nastavimo zagon privzetega operacijskega sistema v GRUB meniju. Grub vrstice šteje od 0 dalje. Če torej želimo privzeto zagnati Windows na 5. mestu, vnesemo 4.

Okrog vrstice 19 pa poiščemo vrstico:

```
timeout          10
```

Število 10 pomeni 10 sekund "timeouta". Čas lahko poljubno spreminjamo.

Optimizacija sistema

Namestimo programski paket Boot-Up Manager (ime programskega paketa je *bum*). Program se pojavi v meniju: Sistem – Administracija – Boot-Up Manager.

V programu izključimo storitve, ki jih ne potrebujemo (npr. Bluetooth, če nimamo Bluetooth naprave, itd.). Previdno pri izklapljanju, da sistema ne “onemogočimo”!

Razdelki (particije)

Razdelek (oz. particija, angleško *partition*) je del diska, ki ga operacijski sistem upravlja kot ločeno enoto. Vsak disk lahko razdelimo na največ štiri primarne razdelke, če jih želimo imeti več, pa lahko uporabimo tim. *razširjeni razdelek*, ki služi kot neke vrste okvir za nadaljnje logične razdelke.

Vsak razdelek je potrebno pred uporabo še *formatirati* - s tem postopkom na razdelek namestimo *datotečni sistem*. Šele ko je na razdelku datotečni sistem, nanj lahko zapisujemo datoteke. Najbolj znani datotečni sistemi so npr. FAT in NTFS (v okolju Windows) ter ext3 (v okolju Linux).

V okolju Windows različne razdelke vidimo kot različne "diske", npr. C:, D:, itd., ki pa se fizično lahko nahajajo na istem disku. Sicer velja omeniti, da Windows različne razdelke na različnih ali istih diskih ne prikazuje ločeno, pač pa enotno. Tako imamo lahko en sam trdi disk, ki je razdeljen na dva razdelka (C: in D:), ali pa imamo dva trda diska, od katerih vsak vsebuje en sam razdelek (prvi disk C:, drugi disk D:).

Pod Linuxom se diski in razdelki označujejo ločeno. Tako je na primer prvi trdi disk označen z `/dev/hda` (če gre za IDE disk) oz. `/dev/sda` (če gre za SCSI disk), prvi razdelek na tem disku pa je označen s številko - torej `/dev/hda1`.

Če je v računalniku nameščenih več operacijskih sistemov (npr. Windows, Linux, itd.), je potrebno imeti več razdelkov (lahko na istem, ali pa na različnih diskih). Vsak operacijski sistem je namreč potrebno namestiti in zagnati iz svojega razdelka.

V praksi to pomeni, da bo v primeru, če imate računalnik, ki ima nameščen operacijski sistem Windows in ima na disku en sam razdelek (npr. C:), potrebno poleg tega razdelka ustvariti še enega.

To storimo tako, da obstoječi razdelek zmanjšamo. Seveda pa tak razdelek ne sme biti polno zaseden s podatki – torej mora biti na npr. C: dovolj praznega prostora.

Ravno to manjšanje obstoječega razdelka je kritična operacija, saj v primeru napake lahko na razdelku, ki ga manjšamo pride do izgube podatkov.

Spreminjanje velikosti razdelkov ni vsakdanja operacija, zato obstaja posebna programska oprema, ki je namenjena delu z razdelki. Eden bolj znanih plačljivih programov je npr. *Partition Magic*, pod Linuxom pa (med drugim) lahko uporabimo brezplačen program *GParted*. Tudi Ubuntu namestitveni program zna krčiti razdelke.

Pri tem je potrebno v okolju Windows najprej pognati program "*Check disk*", dobro pa je tudi, če disk *defragmentiramo*. Zelo priporočljivo je tudi ustvariti varnostno kopijo obstoječih podatkov, saj bomo v primeru napake pri spreminjanju razdelka izgubili vse podatke, potrebno pa bo tudi na novo namestiti Windows!

Ko je to opravljeno se lahko lotimo razdeljevanja diska. Kot rečeno zna to narediti namestitveni program Ubuntuja. Med razdeljevanjem diska računalnika ne smemo ugasniti, saj lahko to privede do izgube podatkov!

Ko je disk razdeljen, bo v okolju Windows edina razlika v tem, da bo razdelek C: nekoliko manjši, poleg njega pa se bo "pojavi" nov razdelek (ki ga operacijski sistem Windows v primeru, da ni formatiran z njem znanim (npr. NTFS ali FAT) datotečnim sistemom niti ne prikazuje). Ob prvem

zagonu operacijskega sistema Windows se bo verjetno zagnal "Check disk" nato pa bo Windows zaznal "novo" strojno napravo (nov razdelek), za katerega bo tudi "namestil" gonilnike.

Ko potem Linux namestimo na ta novo ustvarjeni prazni razdelek, bo Ubuntu namestitveni program ustvaril tudi posebni zagonski meni (praviloma GRUB, lahko pa tudi kakšnega drugega, recimo LILO), ki se prikaže takoj po tem, ko zaženemo računalnik. V tem meniju nato izberemo kateri operacijski sistem želimo zagnati.

Ker so operacijski sistemi na ločenih razdelkih, se med seboj ne "motijo". Vse kar dela operacijski sistem Windows, dela samo znotraj "svojega" razdelka, enako pa velja tudi za Linux.

Velja pa dodati še to, da Windows druge razdelke, formatirane z njemu neznanimi datotečnimi sistemi sicer vidi, vendar "misli", da so prazni in neformatirani. Če torej v okolju Windows skušamo priklopiti tak razdelek, bo operacijski sistem Windows predlagal, da razdelek formatira.

Linux pa razdelke formatirane z datotečnim sistemom FAT ali NTFS tudi vidi, privzeto pa zna pisati samo na FAT razdelke. Za pisanje na NTFS je potrebno namestiti dodatno programsko opremo.

Seveda je potrebno biti pri pisanju na razdelke drugih operacijskih sistemov previden, da kaj ne izbrišemo oz. česa ne uničimo. Operacijski sistem Windows namreč med tem ko je aktiven ne dovoli spreminjanja in brisanja sistemskih datotek, če pa je računalnik zagnan v okolju Linux, pa omejitve, ki jih postavi okolje Windows seveda ne veljajo.

Pisarniški paket OpenOffice.org

Priročnik za uporabo Pisarniškega paketa OpenOffice.org:

http://openoffice.lugos.si/knjiga/Hitri_vodnik_po_OpenOffice.org_FDL.pdf

- Osnovno seznanjanje z OpenOffice.org: *Programi – Pisarna – OpenOffice.org Presentation* (izdelava prosojnic), *OpenOffice.org Spreadsheet* (tabele in izračuni), *OpenOffice.org Word processor* (urejanje besedil).

Delo z besedilom (OpenOffice.org Word processor)

- Odpiranje različnih formatov datotek (*Datoteka – Odpri*). Shranjevanje v različne formate datotek (*Datoteka – Shrani kot – Vrsta datoteke*).
- V OpenOffice.org lahko urejamo obstoječe MS Office datoteke.
- Nastavitev privzetega formata za shranjevanje: *Orodja – Možnosti – Nalaganje, shranjevanje – Splošno* (kot privzeti format za shranjevanje dokumentov lahko nastavimo MS Office format zapisa).
- Zamenjava privzetih pisav (npr. Times New Roman – to pisavo je potrebno predhodno namestiti): *Orodja – Možnosti – OpenOffice.org Writer – Osnovne pisave*.
- Nastavitev samopopravkov: *Orodja – Samopopravki*.
- Nastavitev lastnega privzetega sloga (če npr. želimo, da se ob odprtju novega praznega dokumenta odpre dokument z določeno poravnavo, določeno vsebino (npr. da vsebuje glavo z logotipom podjetja, itd.).
 1. Odpremo prazen dokument v OOO in v njem določimo tisto, kar želimo imeti spremenjeno. Odpremo slogovnik (F11), ki bo že imel izbran slog odstavka *Privzeto*. kliknemo nanj z desnim gumbom miške in izberemo *Spremeni...*
 2. Določimo spremembe, npr. na zavihku *Poravnava* izberemo *Obojestransko*, na zavihku *Pisava* izberemo pisavo, itd. Kliknemo *V redu*.
 3. Sedaj novo predlogo shranimo: *Datoteka - Predloge – Shrani*.
 4. Damo ji ime, npr. *MojaPredloga*.
 5. Nastavimo jo za privzeto predlogo: *Datoteka - Predloge - Organiziraj*. Kliknemo na svojo predlogo in izberemo *Ukazi - Nastavi za privzeto predlogo*. Kliknemo *V redu*.
 6. Ponovno zaženemo OpenOffice.org.
- Izdelava preprostega kazala: za naslove in besedilo uporabimo različne sloge, nato kliknemo: *Vstavi – Kazala vsebine – Kazala vsebine*.
- Če je potrebno nastaviti Javansko okolje: *Orodja – Možnosti – OpenOffice.org – izberemo ustrezno Javansko okolje*.
- Izvažanje v različne formate datotek, npr. v MediaWiki format (zahteva nameščeno Javansko okolje): *Datoteka – Izvozi – MediaWiki*.
- Izvoz v PDF: klik na ikono za izvoz v PDF ali *Datoteka – Izvozi v PDF*, kjer lahko nastavimo podrobne nastavitve, npr. nastavitev gesla za odpiranje ter omejitev pravic.
- Tiskanje: *Datoteka – Natisni* ali klik ikone tiskalnika.
- Vstavljanje posebnih znakov (*Vstavi – Poseben znak*), glav in nog (*Vstavi – Glava / Noga*) opomb pod črto (*Vstavi – Sprotna opomba*).
- Delo s tabelami.
- Barvno označevanje besedila.

Delo s preglednicami (OpenOffice.org Spreadsheet)

- Preprosti izračuni v in (večkriterijsko) sortiranje podatkov.
- Risanje grafov (grafe lahko prenašamo - kopiramo v urejevalnik besedila ali predstavitev).

Predstavitve (OpenOffice.org Presentation)

- Izdelava preproste predstavitve z nekaj slikami.
- Uporabimo lahko proste sličice iz *Open Clip Art Library*, <http://www.openclipart.org/> - Download Files.

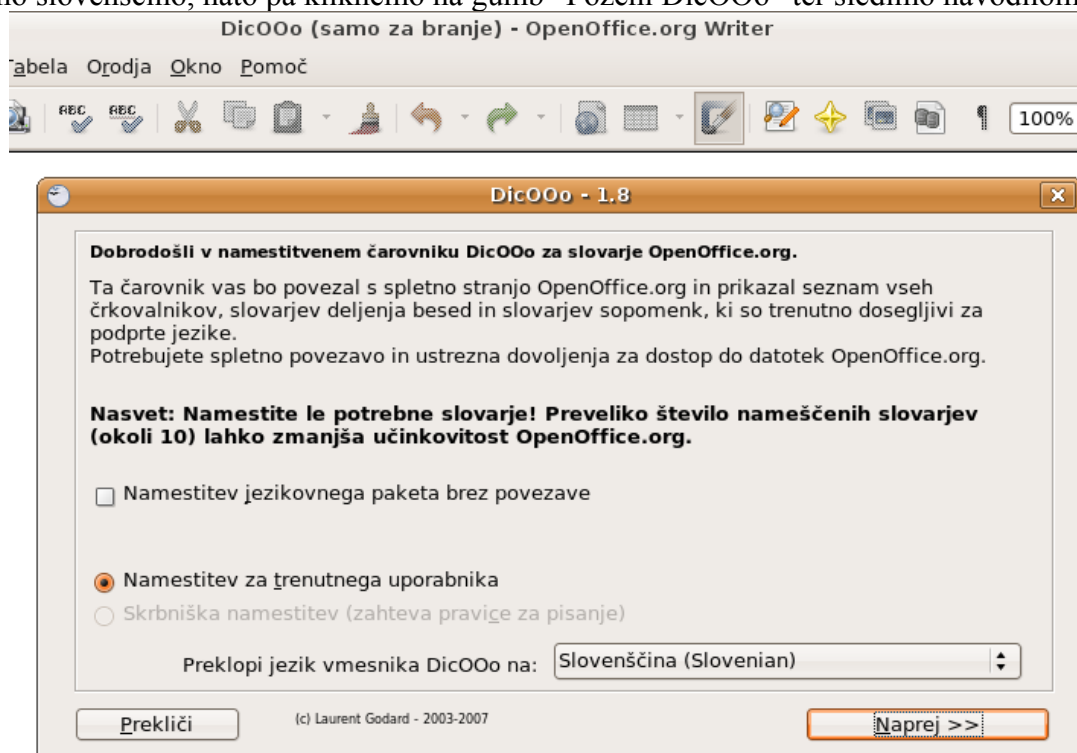
Pretvornik za docx datoteke

Docx pretvornika (iz MS Open Dokument formata) se nahaja v programskem paketu odff-converter.). Programski paket dobimo na spletišču *Getdeb.net*.

Uporaba črkovalnika

Linux uporablja sistemski črkovalnik (deluje v vseh programih, npr. OpenOffice.org, Firefoxu, itd.). Nepravilne besede so rdeče podčrtane, če kliknemo nanje z desnim gumbom, se odpre meni in na vrhu lahko izberemo med pravilnimi besedami.

Dodatne slovarje za preverjanje črkovanja in deljenje besed namestimo s pomočjo čarovnika, ki ga najdemo na: *Datoteka – Čarovniki – Namestitev slovarjev*. Odpre se nov dokument, kjer najprej izberemo slovenščino, nato pa kliknemo na gumb “Poženi DicOOo” ter sledimo navodilom.

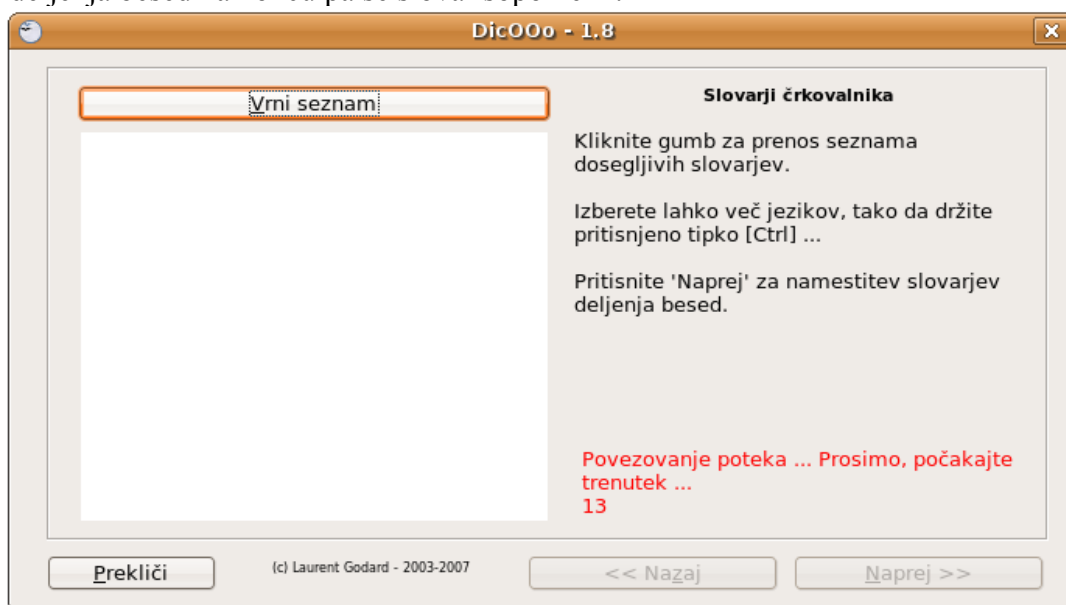


Ta čarovnik je licenciran pod pogoji LGPL, ki je dostopna na:

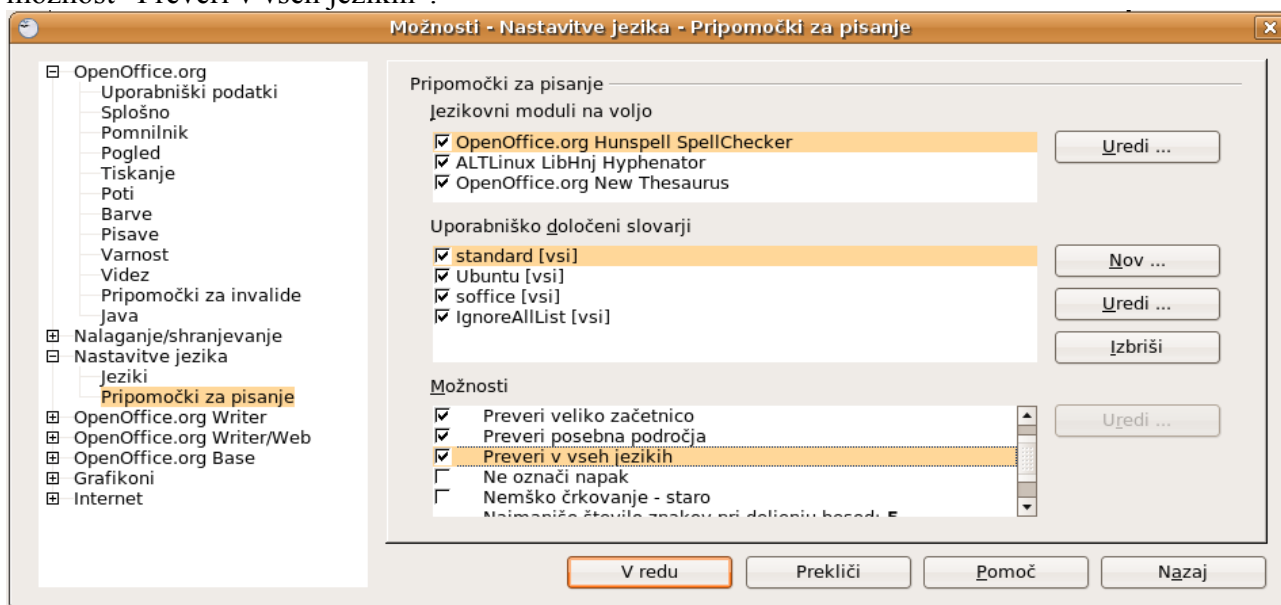
<http://www.opensource.org/licenses/lgpl-license.php>

Avtor: Laurent Godard – © 2003-2005 – LaurentGodard@openoffice.org

Najprej izberemo slovarje črkovalnika (seznam slovarjev dobimo s klikom na “Vrni seznam”), nato slovarje deljenja besed na koncu pa še slovar sopomenk.



Po končani namestitvi ponovno zaženemo OpenOffice.org nato pa v meniju Orodja – Možnosti - Nastavitve jezika - Pripomočki za pisanje izberemo nove slovarje ter med “Možnosti” obkljukamo možnost “Preveri v vseh jezikih”.



Odpiranje multimedijskih datotek

Najprej je potrebno namestiti ustrezne kodeke. Namestimo lahko tudi alternativne predvajalnike, npr. VLC (programski paket *vlc*, lahko namestimo tudi *mozilla-plugin-vlc* ter *vlc-plugin-**). Program najdemo pod *Programi - Zvok in video - VLC media player*.

Namestitev predvajalnika VLC za privzeto predvajanje DVD plošč: *Sistem - Nastavitve - Odstranljivi pogoni in mediji - Večpredstavnost - Video DVD-ji - Ukaz: vlc %m*.

Pisanje na NTFS razdelke

Privzeto Ubuntu ne omogoča pisanja na NTFS razdelke (namestitveni CD pa to omogoča!). Za pisanje na NTFS razdelke potrebujemo naslednja dva programska paketa: *ntfsprogs* ter *ntfs-config*.

Podporo za pisanje na NTFS vključimo v sistemskem meniju: *Programi - Sistemska orodja - NTFS Configuration Tool*).

Povezovanje med sistemi

Povezujemo se lahko na namizje (v tem primeru mora biti uporabnik prijavljen v sistem) ali na računalnik (v tem primeru je dovolj, da je računalnik prižgan in povezan v internet). Pri povezovanju je potrebno vedeti IP ali internetni naslov računalnika, včasih pa tudi uporabniško ime in geslo. Pazimo, da požarni zid ne blokira povezovanja!

- **Povezovanje iz Linux namizja na oddaljeno Linux ali Windows namizje:** Sistem – Nastavitve – Oddaljeno namizje ter Programi – Internet – Terminal Server Client (za na Linux namizje uporabimo protokol VNC, za na Windows namizje pa protokol RDP).
- **Sprejemanje povezav iz oddaljenega sistema:** Sistem – Nastavitve – Oddaljeno namizje (nastavimo ali je za povezovanje potrebna potrditev, geslo ali nič o d tega, ali dovolimo samo ogled namizja, ali pa omogočamo upravljanje z namizjem).
- **Povezovanje na Linux namizje iz okolja Windows:** s pomočjo odjemalca *Tight VNC viewer* (<http://www.tightvnc.com/download.html> – izberemo “viewer executable, does not require installation”).
- **Povezovanje iz Linux namizja na oddaljeni Linux sistem s pomočjo “X-odpošiljanja” (X-forwarding):** na oddaljenem Linux sistemu mora biti nameščen ssh strežnik (namestimo programski paket *ssh*). V ukazni vrstici (*Programi – Pripomočki – Terminal*) vnesemo ukaz “ssh -X uporabniško_ime@naslov_racunalnika” (npr. `ssh -X matej@192.168.1.2`). Po vnosu gesla za *oddaljeni sistem*, smo preko ukazne vrstice povezani na ta sistem. Sedaj lahko zaženemo grafični program, ki se bo zagnal na oddaljenem sistemu, njegovo okno pa bomo videli na našem sistemu. Npr. za zagon brskalnika Firefox vnesemo ukaz “firefox”.
- **Povezovanje iz Windows sistema na Linux sistem preko ukazne vrstice:** v okolju Windows uporabimo program *putty*, ki ga dobimo na <http://portableapps.com>. Na Linux sistemu mora biti nameščen ssh strežnik.
- **Povezovanje iz Windows sistema na Linux sistem – oddaljena mapa:** v okolju Windows uporabimo program *WinSCP*, ki ga dobimo na <http://portableapps.com>. Na Linux sistemu mora biti nameščen ssh strežnik.
- **Povezovanje iz Linux sistema na Linux sistem – oddaljena mapa:** v meniju *Mesta – Poveži se s strežnikom* izberemo tip povezave *SSH*, vnesemo IP ali internetni naslov in uporabniško ime ter geslo, lahko pa tudi ciljno mapo. Lahko pa v programu za delo z datotekami *Nautilus* ročno vnesemo lokacijo: pritisnemo *Ctrl-L* in vnesemo: `ssh://uporabniško_ime@internetni_naslov`.
- **Povezovanje iz Linux sistema na Windows sistem (preko SMB protokola) – oddaljena mapa:** v meniju *Mesta – Poveži se s strežnikom* izberemo tip povezave *Skupna raba Windows*. Lahko pa v programu za delo z datotekami *Nautilus* ročno vnesemo lokacijo: `smb://192.168.1.3/mapa`.
- **Povezovanje iz Windows sistema na Linux sistem (preko SMB protokola) – oddaljena mapa:** najprej namestimo podporo za SMB protokol (Samba) ter določimo deljene mape: *Sistem – Administracija – Shared Folders*. Nato se iz Windows omrežja povežemo na Linux deljeno mapo.
- Samba je odprtokodna implementacija SMB/CIFS omrežnega protokola. Ime Samba izvira iz imena SMB (Server Message Block), ki je standardni protokol v Windows omrežjih oz. Windows omrežnem datotečnem sistemu.

Emulacija

Emulacija je posnemanje delovanja operacijskega sistema (ali naprave) na nekem drugem sistemu. Programi za emulacijo (emulatorji) omogočajo poganjanje programov pisanih za en operacijski sistem (npr. Windows) v drugem operacijskem sistemu (npr. Linux).

Eden izmed programov, ki omogočajo poganjanje programov pisanih za Windows okolje na Linuxu je tudi Wine, ki je junija 2008 izšel v različici 1.0.

Projekt Wine se je pričel leta 1993. Avtorji Wine-a sicer trdijo, da njihov program ni emulator, pač pa API vmesnik, ki omogoča poganjanje Windows programov na Linuxu pa tudi na nekaterih drugih operacijskih sistemih (Mac OS X, FreeBSD in Solaris). Wine tako skuša v Linux in ostala podprta okolja prinesiti Windows DLL funkcije in procese Windows NT jedra. Žal podpora zaradi pomanjkanja dokumentacije zaprtokodnega operacijskega sistema Windows ni popolna, kljub temu pa Wine, ki je bil razvit predvsem z reverznim inženiringom, danes omogoča poganjanje številnih programov in iger pisanih za okolje Windows.

Pri razvoju Wine-a je v preteklosti precej pomagalo podjetje Corel (ki je želelo na Linux prenesti svoj pisarniški paket WordPerfect Office), vendar je podpora podjetja presahnila, ko ga je kupil Microsoft.

Wine omogoča poganjanje 16- in 32-bitnih Windows programov. Wine ne vsebuje podpore za 64-bitne Windows programe, vendar pa zato sam Wine lahko teče tudi na 64-bitnih sistemih. Raziskave so pokazale, da Wine uporablja okrog tretjina Linux uporabnikov.

Poleg Wine-a so za Linux na voljo tudi nekatere bolj "komercialne" aplikacije, ki temeljijo na Wineu. Najbolj znana je aplikacija CrossOver Office, ki jo trži podjetje CodeWeavers (ki so tudi razvijalci Winea). CrossOver Office omogoča enostavno poganjanje Microsoft Office aplikacij in nekaj iger. Bolj igričarsko usmerjena je aplikacija Cedega (včasih znano pod imenom WineX), ki jo trži podjetje (TransGaming Technologies). Poleg tega obstaja še nekaj aplikacij, ki uporabljajo Wine kodo, npr. Darwine (prenos Wine na Mac okolje), ReactOS (operacijski sistem, ki naj bi bil kompatibilen z Windows NT), E/OS (univerzalen operacijski sistem, kjer bi bilo mogoče poganjati katerikoli program, pisan za katerikoli operacijski sistem), itd.

Namestitev Wine je mogoča na dva načina – iz uradnih skladišč programskih paketov, ali pa iz Wineovih razvojnih skladišč. V drugem primeru je potrebno v seznam skladišč programskih paketov dodati Wine skladišča (navodila so na <http://www.winehq.org/>) ter uvoziti GPG šifrirne ključe vzdrževalca Wine skladišča. To storimo z ukazom (v ukazni vrstici):

```
wget -q http://wine.budgetdedicated.com/apt/387EE263.gpg -O- |  
sudo apt-key add -
```

Seznam podprtih Windows aplikacij se nahaja na spletni strani projekta Wine:

- <http://appdb.winehq.org/>

Aplikacije so razvrščene glede na stopnjo podprtosti na Platinum, Gold in Silver.

Navodila za uporabo Wine:

- <http://www.winehq.org/site/howto>

Po namestitvi (program se namesti v meni Programi – Wine) Windows programe zaženemo iz konzole ali s klikom na .exe datoteko. Pri zaganjanju Windows programov iz konzole je potrebno

upoštevati pravilno uporabo poti. Uporabiti je potrebno tim. "windows poti" in ne pot v Linuxu.

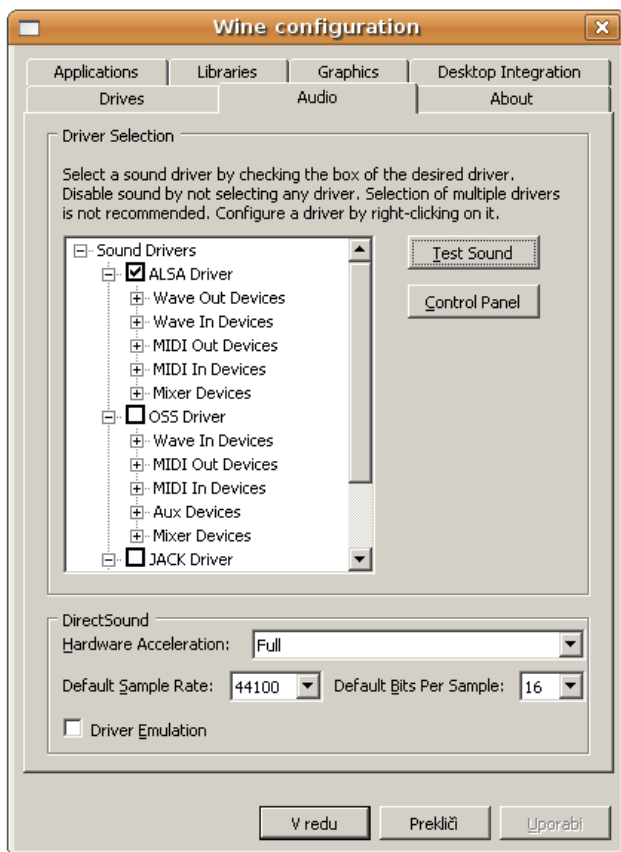
Primer za zagon programa CorelDraw:

```
wine "C:\Corel\DRAW~ICK\programs\coreldrw.exe"
```

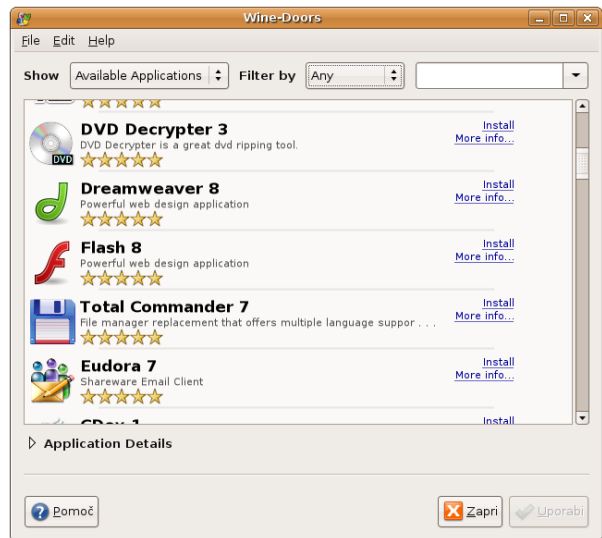
ali:

```
cd ~/.wine/drive_c/Corel/Draw\ Select/programs/  
wine coreldrw.exe
```

Za nastavitve Winea lahko uporabimo program winecfg:



Nekoliko več predvsem pa bolj enostavnih nastavitvev nam ponuja aplikacija Wine-Doors (<http://www.wine-doors.org>). Namestimo jo s pomočjo deb paketa, ki ga najdemo na spletni strani razvijalcev Wine-Doors.



Opisi ostalih pripomočkov za Wine se nahajajo na spletni strani:

- <http://wiki.winehq.org/ThirdPartyApplications>

Primer: namestitev in zagon SPSS 10.0 preko Wine:

The screenshot displays the SPSS Data Editor window with a dataset named 'Datafile_al_Blondel.sav'. The data includes columns for 'coucode', 'v001', 'inone', and 'out'. The SPSS Viewer window shows the 'Regression' output for 'v060 quality'. The 'Variables Entered/Removed' table indicates that variables v069, v073, v070, and v070 were entered, while v060 was the dependent variable. The 'Model Summary' table shows an R value of .111, an R Square of .012, an Adjusted R Square of .003, and a Std. Error of the Estimate of .69.

| Model | Variables Entered | Variables Removed | Method |
|-------|--|-------------------|---------|
| 1 | v069 reasons, v073 influence (decisions), v070 briefing ^a | | , Enter |

a. All requested variables entered.
b. Dependent Variable: v060 quality

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|-------|-------------------|----------|-------------------|----------------------------|
| 1 | .111 ^a | .012 | .003 | .69 |

a. Predictors: (Constant), v069 reasons, v073 influence (decisions), v070 briefing
b. Dependent Variable: v060 quality

Naloga: namestitev programov Pajek ter WinZip, zagon programov ter ustvarjanje menujskega vnosa.

Virtualizacija

Pri virtualizaciji gre za abstrakcijo računalniških zmogljivosti in naprav. Virtualizacija omogoča, da na enem računalniku hkrati poganjamo različne operacijske sisteme. Sistemi za virtualizacijo omogočajo ustvarjanje virtualnega računalnika oz. virtualnega stroja, v katerem lahko zaganjamo operacijski sistem in znotraj njega programe neodvisno od strojne opreme in operacijskega sistema, na kateri teče virtualizacijska programska oprema. Virtualne stroje lahko (nekatero celo med delovanjem!) selimo med različnimi fizičnimi stroji. V virtualnem okolju lahko izvajamo programe, ki v gostiteljskem operacijskem sistemu niso podprti, v virtualnem okolju pa lahko izvajamo tudi nevarno programsko kodo in preskušamo programsko opremo. Dobri virtualizacijski programi so hitri in imajo le nekaj odstotkov počasnejše izvajanje kot izvajanje neposredno v gostiteljskem sistemu.

Med bolj znanimi virtualizacijskimi programi je tudi VMware, ki ponuja nekatere brezplačne virtualizacijske produkte., npr. VMware Player in VMware Server, vendar je pod Linuxom po vsaki menjavi Linux jedra potrebno program VMware ponovno namestiti. V zadnjem času se je na tem področju uveljavilo tudi podjetje innotek, ki razvija program VirtualBox. Podjetje innotek je sredi februarja 2008 kupilo podjetje SUN. Programsko orodje VirtualBox ustvari virtualni računalnik, znotraj katerega lahko poganjamo poljuben operacijski sistem (npr. Windows NT 4.0, 2000, XP, Server 2003, Vista, DOS/Windows 3.x, Linux 2.4 in 2.6, OpenBSD,...). Program je na voljo pod dvema licencama: VirtualBox Open Source Edition je na voljo pod GNU GPL licenco, vendar ne vključuje nekaterih možnosti, ki se uporabljajo predvsem v poslovnem okolju. polna VirtualBox različica pa je na voljo brezplačno za osebno in akademsko rabo, za "neosebno" uporabo v podjetjih pa je potrebno plačati (VirtualBox Personal Use and Evaluation License). Prav tako distribucija te različice ni dovoljena.

6. What exactly do you mean by personal use and academic use in the Personal Use and Evaluation License?

Personal use is when you install the product on one or more PCs yourself and you make use of it (or even your friend, sister and grandmother). It doesn't matter whether you just use it for fun or run your multi-million euro business with it. Also, if you install it on your work PC at some large company, this is still personal use. However, if you are an administrator and want to deploy it to the 500 desktops in your company, this would not qualify as personal use. Well, you could ask each of your 500 employees to install VirtualBox but don't you think we deserve some money in this case? We'd even assist you with any issue you might have.

Use at academic institutions such as schools, colleges and universities by both teachers and students is covered. So in addition to the personal use which is always permitted, academic institutions may also choose to roll out the software in an automated way to make it available to its students and personnel.

http://www.virtualbox.org/wiki/Licensing_FAQ

Namestitev VirtualBoxa

Najprej uvozimo šifrirne ključe:

```
wget http://www.virtualbox.org/debian/innotek.asc
sudo apt-key add innotek.asc
rm innotek.asc
```

Nato v seznam skladišč programskih paketov dodamo VirtualBoxovo skladišče programskih paketov (navodila na spletni strani <http://www.virtualbox.org>) ter namestimo programski paket

virtualbox.

Vsakega uporabnika, ki bo želel poganjati virtualne stroje, npr. uporabnika *fdv*, dodamo v skupino *vboxusers*, uporabnik pa se mora nato ponovno prijaviti: *Sistem – Administracija – Uporabniki in skupine – Uredi skupine* – izberemo skupino *vboxusers* in izberemo *Lastnosti* ter dodamo člana skupine.

Program najdemo pod *Programi - Sistemska orodja - innotek VirtualBox*.

Nastavitev virtualnega stroja

Novi virtualni stroj ustvarimo s klikom na *New*, kjer nastavimo virtualno strojno opremo. VirtualBox omogoča uvoz oz. uporabo VMware virtualnega diska. Prav tako lahko namesto pravih CD/DVD nosilcev ali disket uporabljamo njihove ISO slike. Nastaviti je potrebno tudi kateri operacijski sistem bo tekel na virtualnem računalniku.

Za komunikacijo med gostiteljem in virtualnim strojem lahko namestimo dodatke, tim. VirtualBox addons, ki omogočajo boljšo resolucijo zaslona in intergracijo miške in tipkovnice z gostiteljskim sistemom (omogočajo tudi *copy-paste* funkcijo).

VirtualBox omogoča tudi povezovanje med operacijskim sistemom Windows v virtualnem stroju in gostiteljskim računalnikom preko Windows omrežja. Privzemamo, da je ime virtualnega stroja "*Windows 2000*", uporabnik *fdv*, deljeno mapo v operacijskem sistemu Windows na virtualnem stroju bomo poimenovali *LinuxMapa*.

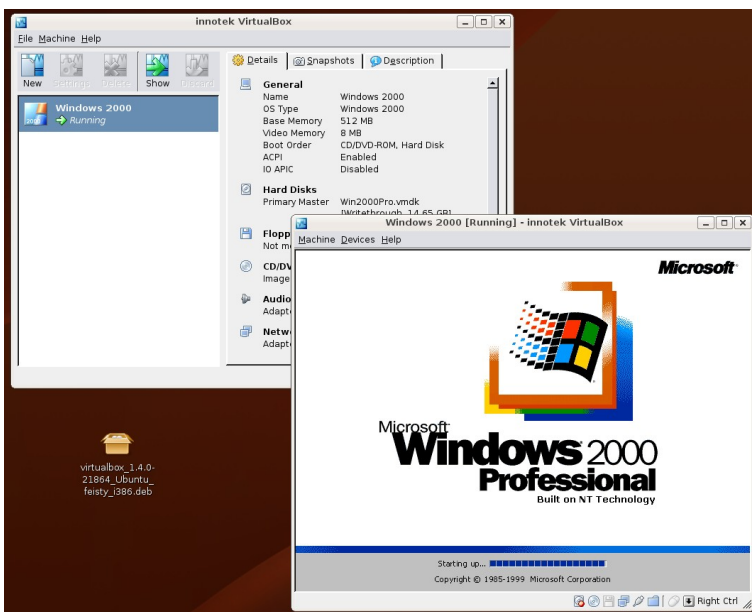
V Linuxu v ukazno vrstico napišemo ukaz:

```
VBoxManage sharedfolder add "Windows 2000" -name LinuxMapa -hostpath "/home/fdv"
```

V virtualnem stroju v operacijskem sistemu Windows odpremo ukazno vrstico in napišemo:

```
net use E: \\vboxsvr\LinuxMapa
```

LinuxMapa (/home/fdv) bo v Windows računalniku sedaj vidna kot disk E:.



Prikaz prenašanja virtualnih strojev iz enega gostitelja na drugega med delovanjem

Dell VMware Storage VMotion Demo:

<http://www.youtube.com/watch?v=7EfGJaYnQjM>

Naloga: iz računalnika na katedru je potrebno prenesti ISO sliko Helix CD-ja ter jo zagnati v virtualnem stroju v programu VirtualBox. Lahko tudi namestitev programa VMware.

Varnost informacijskih sistemov

Informacijski napadi (klasifikacija) in zaščita pred njimi. Upravljanje z varnostnimi tveganji. Razpoložljivost, celovitost in zaupnost informacijskega sistema.

- Prosojnice: varnost_IS.pdf.

Varno uničevanje podatkov

Stare (izbrisane) podatke je z nekaterimi programsko forenzičnimi tehnikami mogoče obnoviti, poleg tega znajo sodobni trdi diski slabe sektorje zamenjati z rezervnimi dobrimi sektorji, kar pomeni, da podatki ostanejo "skriti" na tim. slabih sektorjih od koder jih je mogoče obnoviti. Zato je v nekaterih primerih (npr. pred nadaljnjo prodajo) dobro podatke na nosilcih podatkov trajno uničiti. To storimo s prepisovanjem (npr. naključnih) podatkov čez stare podatke. Prepisovanje diska z naključnimi podatki pa je koristno tudi zato, ker na tako prepisanem disku ni mogoče (oz. je to izredno težko) ugotoviti koliko podatkov je bilo na disku in koliko je bilo praznega prostora.

Slaba stran postopka pa je, da je prepisovanje z naključnimi podatki precej dolgotrajno. Na računalniku s procesorjem Pentium 4 prepisovanje 500 Gb razdelka preko USB 2.0 s pomočjo psevdonaključnega generatorja števil traja dobrih 29 ur, prepisovanje 320 Gb diska pa dobrih 19 ur. Za prepisovanje diska ali razdelka z naključnimi podatki imamo sicer na voljo več metod. V nadaljevanju si jih bomo nekaj ogledali, pod Linuxom pa je priporočljivo uporabiti orodje dd s psevdonaključnim generatorjem ali orodje DBAN.

Prepisovanje podatkov v okolju Windows

V okolju Windows lahko za prepisovanje oz. brisanje podatkov uporabimo formatiranje (vendar ne tim. "hitro formatiranje"), ki pa ni preveč zanesljivo. Uporabimo lahko tudi kakšno namensko orodje, npr. Clean Disk Security (<http://www.theabsolute.net/sware/clndisk.html>) ali SDelete (<http://www.microsoft.com/technet/sysinternals/utilities/SDelete.mspx>). Žal je v okolju Windows varno oz. zanesljivo brisanje NTFS razdelkov nekoliko težavno, zato se je potrebno zavedati, da uporaba teh orodij ni vedno optimalna.

Primerjavo nekaterih namenskih orodij za brisanje podatkov v okolju Windows si je mogoče ogledati na spletni strani Sarah Dean (http://www.sdean12.org/Comparison_Shredders.htm).

Uporaba orodja za preverjanje slabih sektorjev na disku v Linuxu

Precej hitrejša metoda je uporaba orodja za preverjanje slabih sektorjev na disku v Linuxu - *badblocks*. Predpostavimo, da je diskovni razdelek na USB disku, ki ga želimo šifrirati /dev/sdc3. USB disk najprej programsko odklopimo - z desnim klikom na disk izberemo možnost Izvrzi oz. Odklopi. Disk naj ostane fizično priključen. Sledi ukaz v ukazni vrstici:

```
badblocks -c 10240 -s -w -t random -v /dev/sdc3
```

in počakamo nekaj ur. Med tem se nam izpisuje približno takle izpis:

```
Checking for bad blocks in read-write mode
From block 0 to 97530615
Testing with random pattern:          30720/          97530614
```

Brisanje "praznega" prostora na disku in uporaba ukaza shred

Znotraj aktivnega sistema lahko ustvarimo veliko datoteko (z imenom bigfile) s katero zapolnimo celoten prostor na disku, nato pa to datoteko izbrišemo z ukazom shred:

```
dd if=/dev/zero of=bigfile
sync
shred -u -v -n 5 bigfile
sync
```

Stikalo `-u` povzroči, da program datoteko po uničenju odstrani, stikalo `-v` pomeni naj program prikazuje napredek, stikalo `-n` pa določi število prepisov (v našem primeru 5).

Pri tem je potrebno vedeti, da nekateri datotečni sistemi (npr. ext3) del prostora na disku namenijo administratorju sistema (običajno je to 5% tim. superuser blocks). Običajni uporabnik ima torej na voljo 95% sistema in ko ga porabi sistem prične javljati, da je disk zapolnjen – kljub temu pa ima administrator sistema na voljo še nezapolnjenih 5% diska.

Uporaba orodja dd (disk dump) v Linuxu

Verjetno najbolj optimalna metoda glede na razmerje med varnostjo in hitrostjo je uporaba orodja *dd* (disk dump). Mimogrede, orodje je del vsakega standardnega živega CDja (live CD). V našem primeru je torej diskovni razdelek, ki ga želimo šifrirati `/dev/sdc3`. USB disk najprej programsko odklopimo ter izvedemo ukaz:

```
dd if=/dev/urandom of=/dev/sdc3 bs=16M
```

Ukaz *dd* (disk dump), bo razdelek `/dev/sdc3` (ki je v našem primeru tim “izhodna datoteka” output file (odtod v ukazu `of=...`) prepisal s podatki, ki jih dobi na tim. “vhodni datoteki” (input file, oziroma `if=...`). Kot “vhodna datoteka” je nastavljen psevdonaključni generator števil `/dev/urandom`.

Če želimo doseči večjo stopnjo varnosti lahko namesto psevdonaključnega generatorja števil `/dev/urandom` uporabimo naključni generator števil `/dev/random` in celo večkratno prepisovanje. V primerjavi uporabe naključnega generatorja števil pa je dobro imeti dober vir entropije, kar lahko dosežemo z naključnim “tipkanjem” po tipkovnici ali z vklopom mikrofona, ki ga postavimo nekam na prosto. Se pa čas prepisovanja v primeru naključnega generatorja števil še podaljša.

Prepišemo lahko tudi celoten disk (v tem primeru uporabimo napravo `/dev/sdc` - brez številke), vendar bo v tem primeru potrebno na povsem izbrisanem disku kasneje ustvariti nov razdelek. Parameter `blocksize (bs=16M)` pri ukazu je precej pomemben, saj zelo pohitri prepisovanje diska. Po vnosu ukaza počakajmo nekaj časa (precej časa, npr. prepisovanje 500 Gb diska na USB 2.0 in z Intel Pentium 4 procesorjem je trajalo dobrih 29 ur, prepisovanje 320 Gb diska pa dobrih 19 ur), da se disk v celoti prepiše z naključnimi podatki.

Ker je prepisovanje z *dd* dolgotrajno, *dd* pa ne izpiše napredka, lahko napredek pogledamo z naslednjim ukazom, ki procesu *dd* pošlje `USR1` signal. Ukaz povzroči izpis statusa delovanja programa, izvajanja procesa pa ne prekine:

```
sudo killall -USR1 dd
```

Dobimo približno takle izpis, ki v našem primeru kaže, da smo prepisali že 1,9 Gb podatkov:

```
116+1 zapisov na vhodu
116+0 zapisov na izhodu
1946157056 bytes (1,9 GB) copied, 426,526 sekunde, 4,6 MB/s
```

Uporaba orodja DBAN

Lahko pa uporabimo tudi orodje DBAN (Darik's Boot and Nuke, <http://dban.sourceforge.net/>), s katerim stare podatke na disku učinkovito uničimo z večkratnim prepisovanjem, na izbiro pa imamo več metod. DBAN je potrebno najprej zapisati na disketo od koder računalnik tudi zaženemo in nato izberemo razdelek ali disk, ki naj ga program izbriše. Uporaba tega orodja je najbolj zanesljiva, vendar pa tudi najbolj dolgotrajna, če izberemo najbolj varno metodo brisanja.

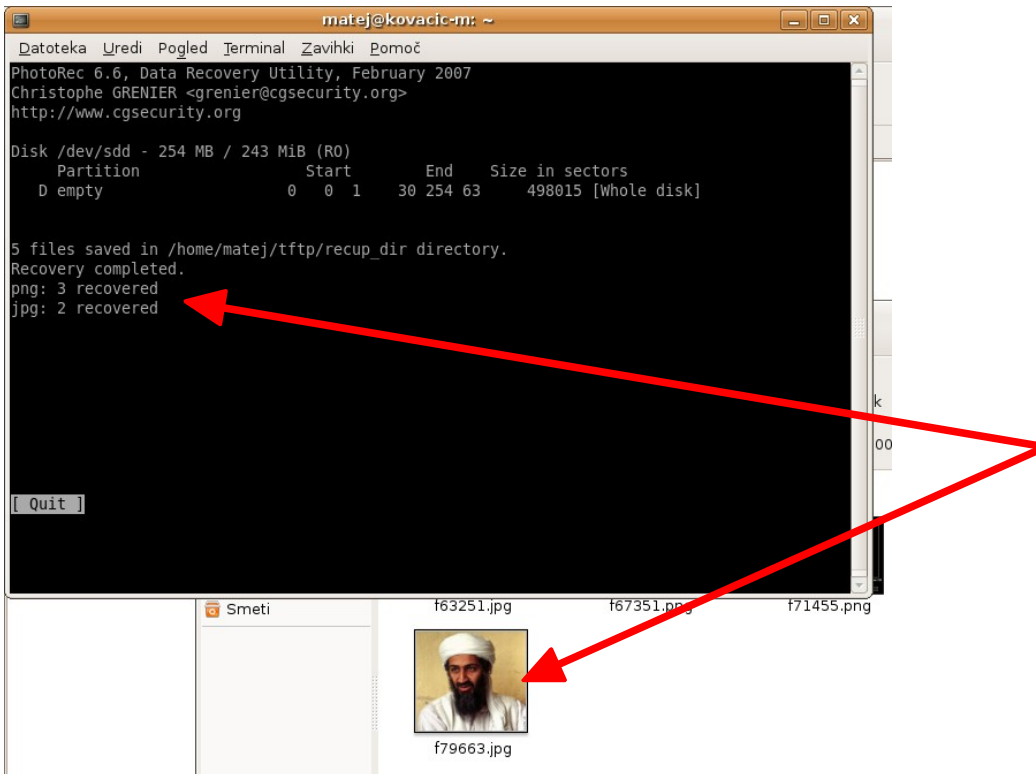
```
Darik's Boot and Nuke 1.0.7
----- Options -----
Entropy: Linux Kernel (urandom)
PRNG:    Mersenne Twister (mt19937ar-cok)
Method:  DoD Short
Verify:  Last Pass
Rounds:  1
----- Statistics -----
Runtime:    00:00:11
Remaining:  00:00:19
Load Averages: 0.33 0.09 0.02
Throughput: 10260 KB/s
Errors:     0

(SCSI 1,0,0,0,-) VMware, VMware Virtual S
[34.01%, round 1 of 1, pass 2 of 3] [writing] [10260 KB/s]
```

Obnavljanje podatkov

Obnavljanje izbranih podatkov je mogoče z orodji iz programskega paketa testdisk. Paket vsebuje orodji:

- *TestDisk*, ki je prosto orodje namenjeno obnavljanju izgubljenih razdelkov, deluje v več operacijskih sistemih in pozna številne datotečne sisteme (<http://www.cgsecurity.org/wiki/TestDisk>)
- *PhotoRec*, ki je prosto orodje namenjeno obnavljanju izgubljenih datotek. Deluje tudi v primeru poškodbe datotečnega sistema ter pozna več datotečnih sistemov (<http://www.cgsecurity.org/wiki/PhotoRec>).



Šifriranje

Kriptografija - metode za zaščito vsebine (kodiranje) sporočil. S pomočjo kriptografije onemogočimo prisluškovanje elektronskim ali zvočnim komunikacijam.

Verodostojna zatajitev (ang. *plausible deniability*) omogoča uporabo več šifrnih ključev za isti kontejner podatkov. Z prvim ključem odklenemo prve podatke, z drugim ključem druge, itd. v primeru, da smo prisiljeni razkriti svoje šifrne ključe, lahko razkrijemo samo prvi ključ, ključ, ki skriva podatke, ki jih ne želimo razkriti pa ostane skrit. Praviloma naj z običajno kriptozo ne bi bilo mogoče ugotoviti koliko nivojev skritih podatkov obstaja v kontejnerju.

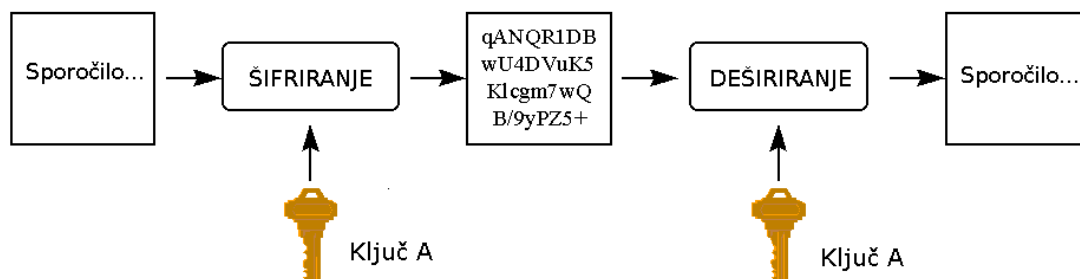
Generator naključnih števil je funkcija, ki vrne neko naključno število. Večina (to velja predvsem za programske generatorje) vrne psevdo-naključna števila torej so to psevdonaključni generatorji.

Generatorji naključnih števil so zelo pomembni za varno delovanje kriptografskih aplikacij, zato je zelo pomembno, da le-ti generirajo čimbolj naključna števila. Varnost kriptografije je namreč odvisna tudi od varnosti generatorjev naključnih števil.

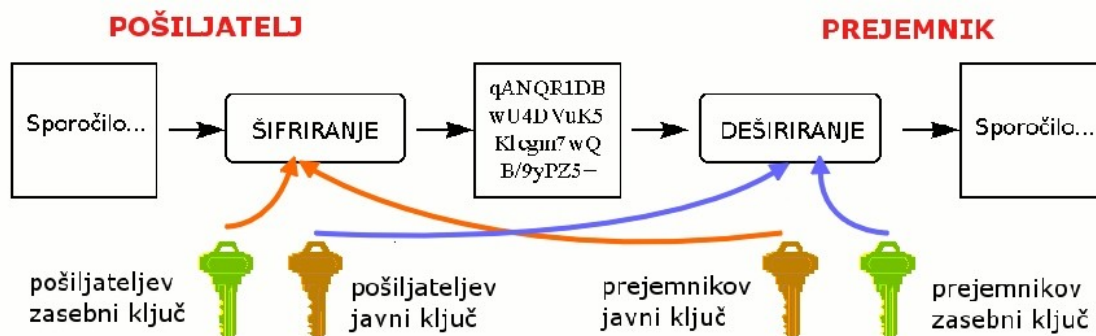
Šifrirni algoritmi

Pri varovanju podatkov uporabljamo simetrične, asimetrične in zgostitvene algoritme.

Simetričnimi algoritmi ali algoritmi z zasebnim ključem: imamo samo en ključ, s katerim zašifriramo in dešifriramo sporočilo. Običajno so ti algoritmi hitri, težko pa je varno izmenjati ključ. Problem predstavlja tudi število ključev - vsak uporabnik mora imeti za vsakega dopisovalca svoj ključ.



Asimetrični algoritmi ali algoritmi z javnim ključem: uporabnik ima dva ključa, enega objavi, drugi ostane tajen. Vsi, ki mu hočejo poslati sporočilo, bodo uporabili njegov javni ključ za šifriranje sporočila. Dešifriral pa ga bo lahko le on sam s svojim tajnim ključem in javnim ključem pošiljatelja. Te metode so računsko bolj zahtevne in zato počasnejše kot simetrične.



Zgostitveni algoritmi poljubno dolg tekst preslikajo v število fiksne dolžine (izračunajo tim. kontrolno vsoto, ang. *hash*), kar je uporabno za implementacijo digitalnega podpisa in preverjanje integritete datotek. Najbolj znana algoritma sta MD5 in SHA.

Varnost zgostitvenih algoritmov

Zgostitveni algoritmi morajo zagotavljati:

- enosmernost (da je iz kontrolne vsote nemogoče nazaj izračunati originalen podatek)
- odsotnost kolizije (da ne obstajata dva različna niza znakov, ki vrmeta isto kontrolno vsoto)

Avgusta 2004 so na konferenci Crypto '04 v Kaliforniji predstavili uspešno razbitje zgostitvenega algoritma SHA-0. Raziskovalci so namreč našli dve različni sporočili, za kateri SHA-0 vrne isto vrednost, torej isti "prstni odtis" dveh različnih sporočil. Gre za odkritje tim. kolizije v funkciji. Februarja 2005 so trije kitajski raziskovalci uspeli najti tudi kolizijo v SHA-1 funkciji.

Napredni matematični napadi na kriptografijo

Na konferenci Crypto leta 1996 in Eurocrypt leta 1997 sta raziskovalca Adam Young in Moti Yung prvič predstavila zamisel o kleptografiji. V članku "*Mitigating Insider Threats to RSA Key Generation*", objavljenem v reviji Cryptobytes, je Young opisal metodo SETUP (secretly embedded trapdoor with universal protection – tajno vključena stranska vrata z univerzalno zaščito), ki s pomočjo prirejenega algoritma zgenerira tak par šifrnih ključev (pri asimetrični kriptografiji), da je na videz (matematično) povsem enak kakor navaden par ključev, poleg tega pa je tudi enako varen, razen pred napadalcem, saj tajno vključena stranska vrata predstavljajo napadalčev javni ključ. Young pravi, da napad SETUP oziroma kleptografija napadalcu daje ekskluzivno prednost, saj je zaradi lastnosti prirejenih ključev le-te nemogoče ločiti od neprirejenih. To pomeni, da je nemogoče ugotoviti, ali je bil napad SETUP izveden ali ne. Young in Yung sta pokazala, da je napad mogoče implementirati v RSA, DSA (Digital Signature Algorithm) ter Diffie-Hellmanovo izmenjavo ključev. Bistvo njunih ugotovitev pa je v tem, da so takšna stranska vrata mogoča pri t. i. kriptografskih napravah black-box, torej pri napravah, katerih delovanje ni transparentno.

(Več o tem v knjigi *Nadzor in zasebnost v informacijski družbi*, <http://matej.owca.info/knjiga2/>)

~ ~ ~

Nekatere raziskave so tudi pokazale, da generatorji naključnih števil v nekaterih operacijskih sistemih niso dovolj zanesljivi. Raziskava Dorrendorfa, Guttermana in Pinkasa iz novembra 2007 je pokazala, da generator naključnih števil v Windows 2000 ni varen. Algoritem, ki se uporablja tudi za generiranje SSL ključev namreč ni bil javno objavljen, analiza pa je pokazala, da je mogoče z razmeroma preprostimi napadi predvideti prihodnje "naključne" vrednosti in s tem uganiti npr. SSL šifrirne ključe.

Seveda pa niti uporabniki operacijskega sistema Linux niso varni. Raziskava iz marca 2006 je namreč odkrila številne ranljivosti tudi v generatorju naključnih števil v tem operacijskem sistemu.

Ameriški National Institute of Standards and Technology je leta 2007 pripravil nov standard za generiranje naključnih števil. Pripravili so štiri standardizirane tehnike oz. algoritme, med katerimi se eden imenuje Dual_EC_DRBG.

Algoritem je sicer najpočasnejši med vsemi štirimi, Bruce Schneier pa je na svojem blogu zapisal,

da je postal standard izključno zato, ker ga je priporočila tajna služba NSA.

V začetku leta 2006 so v algoritmu sicer opazili nekaj pomanjkljivosti (algoritem proizvaja nekaj tim. pristranosti), leta 2007 pa sta na konferenci Crypto 2007 Shumow in Ferguson iz Microsofta pripravila predstavitev, v kateri se sprašujeta, če algoritem Dual_EC_DRBG ne vsebuje tim. "stranskih vrat".

Raziskovalca sta namreč ugotovila, da algoritem uporablja konstante za definiranje eliptične krivulje, ki pa so povezane z nekim naborom skritih števil. Kdor pozna, ali bi poznal te številke, bi lahko s pomočjo poznavanja prvih 32 naključno generiranih znakov algoritma Dual_EC_DRBG uganil vse naslednje "naključno" generirane znake. Povedano drugače: v algoritmu je morda vrinjen "tajni ključ" napadalca, saj konstante morda predstavljajo javni ključ napadalca, skrito število pa predstavlja napadalčev tajni ključ, kar napadalcu omogoči uspešen napad na sam algoritem.

S tem bi bilo mogoče razmeroma enostavno razbiti praktično vsak kriptografski algoritem, ki bi temeljil na generatorju naključnih števil Dual_EC_DRBG.

Sicer ni znano, ali NSA oziroma kdorkoli drug v resnici poseduje omenjene skrite številke. A dejstvo, da ji bi kdo utegnil posedovati je verjetno dovolj močan argument proti uporabi tega algoritma.

(Vir: spletna stran Slo-Tech)

Steganografija

Steganografija je skupek metod za skrivanje sporočil. Steganografija nam omogoča izmenjavo nevidnih sporočil, nevidno kodiranje, označevanje datotek z tim. elektronskim vodnim tiskom ter označevanje datotek z elektronskimi serijskimi številkami.

Program S-Tools 4 za Windows 95 (zagon preko Wine) nam omogoča da neko poljubno datoteko skrijemo v sliko ali zvočno datoteko. Program lahko sporočila skriva v BMP, GIF ali WAV datoteke.

Program deluje v tim. "drag-and-drop" (*povleci-in-spusti*) načinu. Ko program požemo se samodejno odpre okno Actions. Edine možne nastavitve so v File, Properties, kjer lahko vklopimo ali izklopimo kompresijo ter nastavimo stopnjo kompresije (čim boljša je kompresija, tem počasneje poteka sam postopek skrivanja). Slikovno ali zvočno datoteko povlečemo v program, nato pa na to datoteko povlečemo še datoteko z elektronskim sporočilom. Odpre se okno, kamor vpišemo geslo in izberemo šifrirni algoritem. Ko se skrivanje konča dobimo novo datoteko, ki jo shranimo na disk (na datoteko kliknemo z levim gumbom miške in izberemo možnost Save).

Odkrivanje poteka tako, da datoteko s skritim sporočilom povlečemo v program. Na datoteko kliknemo z levim gumbom miške ter izberemo možnost Reveal. Izberemo dešifrirni algoritem, vtipkamo pravo geslo in odpre se novo okno z odkrito datoteko, ki jo je potrebno še shraniti na disk in postopek je končan.

Šifrirne nastavitve in šifrirna programska oprema v Ubuntu Linuxu

- Sistem – Nastavitve – Lastnosti šifriranja (nastavitev privzetega ključa, predpomnjenje šifrirne faze,...)

- Programski paket *seahorse*: Programi – Pripomočki – Gesla in šifrirni ključi (lastnosti iz izvažanje ključev,...)
- FireEncrypter: dodatek za brskalnik Firefox, ki omogoča prikaz različnih načinov šifriranja ter generiranja gesel v brskalniku Firefox (<https://addons.mozilla.org/en-US/firefox/addon/3208>).
- FireGPG: dodatek za Firefox, ki omogoča uporabo PGP/GPG šifriranja na spletnih straneh (<http://firepgg.tuxfamily.org/>)
- Enigmail: dodatek za poštni odjemalec Mozilla Thunderbird za šifriranje e-pošte programski paket *mozilla-thunderbird-enigmail*).

Ostale teme:

- gesla (izbira varnih gesel, uporaba različnih gesel za različne sisteme, zakaj je pri spremembi gesla potrebno dvakrat vnesti isto geslo, spreminjanje gesel)
- nastavljanje in spreminjanje gesel šifrirnih ključev
- delo z javnimi ključi (iskanje po strežnikih s ključi, uvoz ključev, izvoz ključev, preklic ključa), potrebno je imeti dostop do izhodnih vrat (ang. *port* 11371).

Naloga: študentje namestijo programsko opremo za šifriranje in delo s šifrirnimi ključi, ter si izmenjajo nekaj šifriranih e-sporočil. Preskusijo tudi delovanje programa S-Tools.

Povezovanje s ssh

Ssh ali varna lupina (Secure SHell) omogoča varno povezovanje med Linux (pa tudi Unix in BSD) računalniki. Omogoča prenos datotek in izvajanje ukazov na oddaljenem računalniku. ssh so razvili v 1990-tih letih kot alternativo ostalim, ne-varnim protokolom za povezovanje na oddaljene sisteme (telnet, rlogin), ki pri povezovanju niso uporabljali šifriranja.

Ssh je na voljo kot odjemalec (omogoča povezovanje na sisteme) in kot strežnik (omogoča, da se odjemalci povezujejo na sistem). V Ubuntuju je ssh odjemalec že privzeto nameščen, strežnik pa namestimo z namestitvijo programskega paketa *ssh* (gre za metapaket, ki vsebuje tako odjemalec, kot tudi strežnik). Po namestitvi ssh strežnik zažene proces *sshd*, ki na privzetih vratih 22 posluša za dohodnimi "ssh klici".

Povezovanje na oddaljene sisteme s ssh poteka ukazne vrstice, ki jo odpremo s klikom na: *Programi – Pripomočki – Terminal*.

Povezovanje poteka z ukazom *ssh*, ki mu podamo uporabniško ime in naslov strežnika ali IP naslov. Primer: "ssh uporabnik@moj.streznik.net" ali "ssh uporabnik@192.168.1.2". Če se želimo povezati na lasten lokalni računalnik, vpišemo ukaz "ssh localhost".

Avtentikacija oddaljenega računalnika

Ssh omogoča tudi avtentikacijo oddaljenega računalnika. Ko se namreč poskusimo povezati na oddaljeni računalnik, si ssh odjemalec in strežnik izmenjata javne ključ. Ko ssh odjemalec od nekega oddaljenega računalnika prvič prejme njegov javni ključ, uporabnika vpraša ali naj ključu zaupa in ali naj ga doda v svojo lokalno zbirko javnih ključev. Lokalna zbirka javnih ssh ključev se nahaja v datoteki ".ssh/known_hosts", zaradi varnosti pa v tej datoteki niso zapisani naslovi oddaljenih računalnikov, pač pa njihove kontrolne vsote.

```
The authenticity of host 'cryptobox (192.168.1.2)' can't be established.  
RSA key fingerprint is c5:dd:0b:ae:de:d1:dd:e2:07:9b:92:dd:11:4b:a7:6d.  
Are you sure you want to continue connecting (yes/no)? yes
```

Ko se na oddaljeni računalnik povežemo naslednjič, ssh odjemalec od oddaljenega računalnika ponovno pridobi njegov javni ključ, vendar pa preveri ali se le-ta ujema z javnim ključem, ki ga je v svojo lokalno zbirko javnih ključev shranil prvič. Če se ključa ujemata, povezovanje omogoči, sicer pa povezovanje prekine in nas opozori na možnost napada s posrednikom.

Ob prvem poskusu povezave na oddaljeni računalnik nam ssh izpiše prstni odtis njegovega javnega ključa, ki zglada npr. takole: "1d:67:eb:42:08:92:11:22:11:7a:a0:de:79:49:6f:a6". Na tej točki imamo uporabniki možnost preveriti istovetnost oddaljenega računalnika. Seveda pa moramo pred tem na oddaljenem računalniku izpisati prstni odtis njegovega javnega ključa in potem tisti izpis primerjati z izpisom ko ga dobimo od povezovanju.

Na Linux računalnikih prstni odtis javnega ssh ključa izpišemo z ukazom:
ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key

Avtentikacija (prijava) uporabnika

Ko je oddaljeni računalnik avtenticiran odjemalcu, sledi avtentikacija uporabnika oddaljenemu računalniku. Avtentikacija oz. prijava je mogoča z geslom ali s šifrnim ključem. V primeru prijave z geslom (ki je privzeta) vpišemo geslo, v primeru prijave s ključem, pa moramo na svojem računalniku imeti nameščen šifirni ključ, prijava pa steče samodejno.

Primer prijave z geslom:

```
matej@kovacic-m:~$ ssh matej@www.nekstreznik.si
matej@www.nekstreznik.si's password:
Linux cryptobox 2.4.29-rc2 #1 Thu Jan 13 14:20:11 CET 2005 i686 unknown
matej@cryptobox:~$
```

Priprava ključev za avtentikacijo s ključem

Za avtentikacijo s šifrnim ključem je na oddaljenem računalniku potrebno najprej ustvariti ssh ključ. Ssh ključ ustvarimo na lokalnem računalniku, iz katerega se bomo povezovali na oddaljeni računalnik.

V danem primeru bomo uporabili algoritem je RSA, velikost ključa pa bo 3072 bitov. Vnesemo ukaz:

```
ssh-keygen -t rsa -b 3072
```

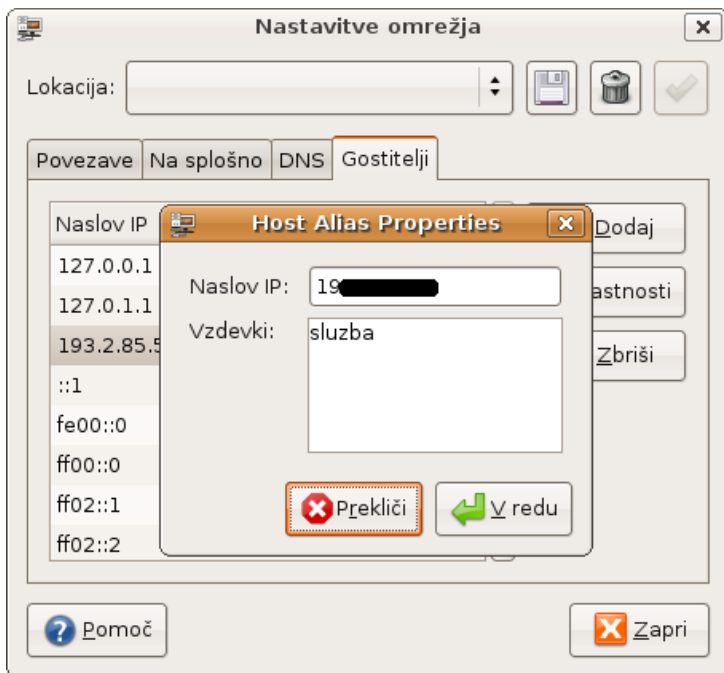
Za geslo (*passphrase*) pritisnemo “*enter*” (pustimo prazno), nakar se ustvari par javni in zasebni ključ, ki se v podimeniku `.ssh` shranita v datoteki `id_rsa` in `id_rsa.pub`. `id_rsa` vsebuje zasebni ključ in ga je treba varno hraniti. `id_rsa.pub` pa vsebuje javni ssh ključ.

Vsebino javnega ključa `id_rsa.pub` prekopiramo v datoteko `.ssh/authorized_keys` **na oddaljenem računalniku** na katerega se želimo povezovati brez gesla.

Sedaj se lahko brez gesla (s ključem) povežemo na oddaljeni strežnik.

Sprememba imena gostitelja oz. naslova oddaljenega računalnika

Če želimo še hitrejšo prijavo na oddaljeni sistem (z manj tipkanja) lahko naslove oddaljenih računalnikov zapišemo s skrajšanimi oz. nam domačimi imeni. Odpremo program za nastavitev omrežja: *Sistem – Administracija – Omrežje*, ter izberemo zavihek “*Gostitelji*”. Kliknemo gumb “*Add*” ter vpišemo IP naslov oddaljenega računalnika ter mu določimo lokalno ime.



Sedaj se bomo na oddaljeni računalnik lahko povezali z ukazom:

```
ssh uporabnik@sluzba
```

Pri tem je dobro tudi vedeti, da ime uporabnika na oddaljenem sistemu lahko izpustimo, če je ime enako imenu trenutno prijavljenega uporabnika.

Uporaba prijave s ključem nam omogoči enostavno zaganjanje programov oz. izvajanje ukazov (npr. skript) na oddaljenem računalniku. Primer za samodejni zagon programa "calendar" na oddaljenem računalniku (brez vpisovanja gesla):

```
ssh sluzba /usr/bin/calendar
```

Izstop iz ssh seje

Iz ssh seje izstopimo z ukazom exit ali s pritiskom na Ctrl-D.

Grafični dostop do aplikacij preko ssh tunela

Če želimo zagnati neko aplikacijo na oddaljenem računalniku v grafičnem načinu, torej tako, da se program zažene na oddaljenem računalniku, okno programa pa vidimo na lokalnem računalniku, se povežemo z vključenim posredovanjem ukazov grafičnega strežnika X:

```
ssh -X uporabnik@sluzba.si
```

Nato v ukazni vrstici (na oddaljenem računalniku) vpišemo ukaz za zagon aplikacije, če želimo, pa dodamo še znak &, da se program zažene v ozadju (v tem primeru za zagon novega programa ni potrebno odpirati nove ukazne vrstice, pač pa iz iste ukazne vrstice zaganjamo več programov, vsi pa tečejo v ozadju). Primer za oddaljeni zagon brskalnika Firefox:

```
firefox &
```

Na podoben način lahko zaženemo npr. odjemalec pošte Thunderbird na lokalnem računalniku, vendar kot drug uporabnik, kot tisti, ki je trenutno prijavljen v sistem. V tem primeru vnesemo ukaz:

```
ssh -X localhost
```

in potem zaženemo Thunderbird, ali pa to storimo neposredno:

```
matej@sluzba:~$ ssh -X janez@localhost /usr/bin/thunderbird
```

Reverzni ssh tunel

Včasih oddaljeni računalnik na katerega se želimo povezati ni neposredno dostopen, ker je “skrit” v internem omrežju (npr. za domačim usmerjevalnikom, za NAT-om ali za požarnim zidom).

Predpostavimo, da se preko ssh želimo od doma povezati na službeni računalnik, ki ni neposredno dosegljiv. Rešitev je uporaba tim. reverznega ssh tunela.

Najprej se iz službenega računalnika povežemo na domači računalnik. Povežemo se z uporabniškim imenom “janez”, povezavo pa bomo preusmerjali na lokalna vrata 2048 (izberemo lahko katerakoli vrata, le da so prazna):

```
ssh -R 2048:localhost:22 janez@doma.si
```

Ko pridemo domov, se na službeni računalnik povežemo z ukazom (v primeru smo uporabili službeno uporabniško ime fdv):

```
ssh -p 2048 fdv@localhost
```

Pomembno je, da prve povezave iz službenega računalnika na domači ne prekinemo. V nasprotnem primeru se namreč reverzni ssh tunel prekine.

Povezovanje na alternativna vrata

ssh privzeto deluje na vratih 22. Nekateri požarni zidovi ta vrata blokirajo (npr. v podjetjih, kjer ne želijo, da bi se uporabniki preko ssh tunela povezovali na domače računalnike in med delovnim časom brskali po spletu brez omejitev ali brali domačo elektronsko pošto). V takem primeru lahko ssh strežnik nastavimo tako, da bo poslušal na drugih, ne-privzetih vratih.

Najprej na oddaljenem računalniku odpremo konfiguracijsko datoteko sshd_config:

```
sudo gedit /etc/ssh/sshd_config
```

in v njej poiščemo nastavitve dohodnih vrat:

```
# What ports, IPs and protocols we listen for
Port 22
```

Vrstico *Port 22* spremenimo v npr. *Port 80* (80 so privzeta vrata za spletne strežnike).

Nato ponovno zaženemo ssh strežnik:

```
sudo /etc/init.d/ssh restart
```

Sedaj se lahko na oddaljeni računalnik povežemo z ukazom:

```
ssh -p 80 uporabnik@doma.si
```

Varnostne kopije

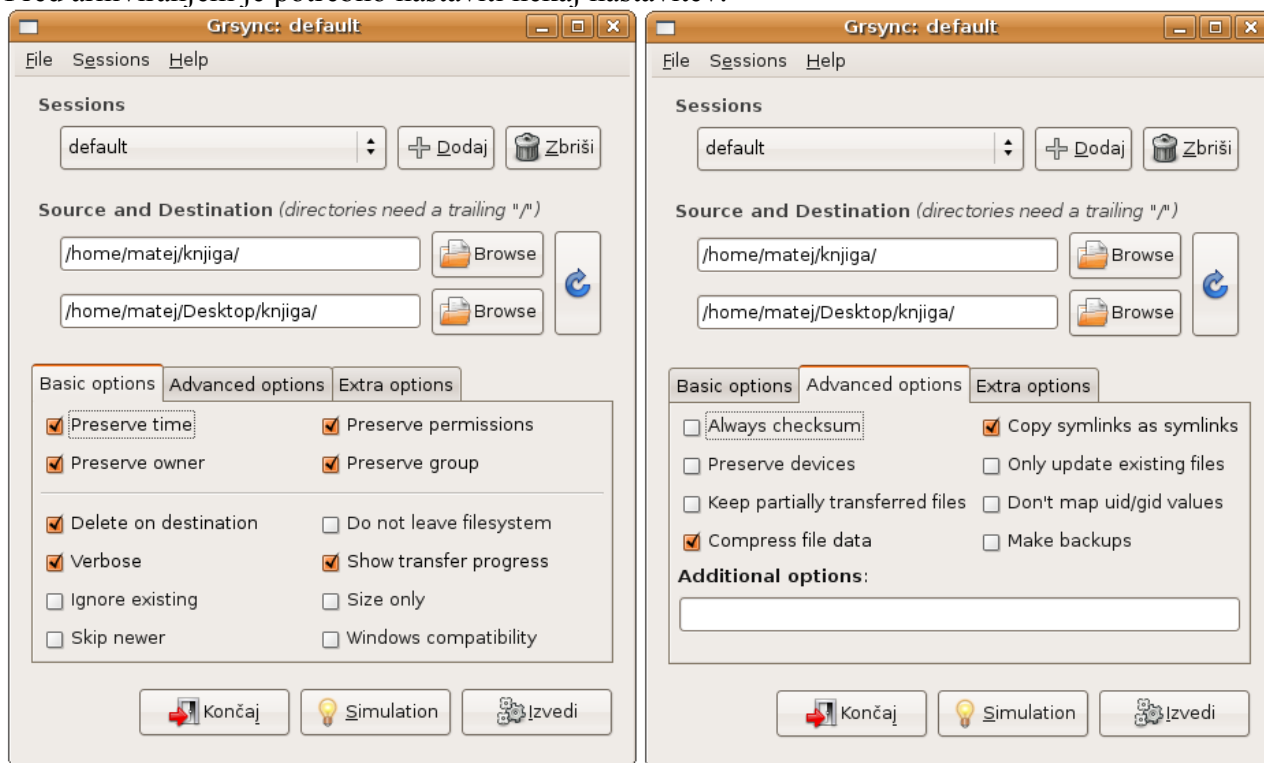
Varnostne kopije (ang. *backup* oz. arhiviranje) izdelujemo z namenom obnove podatkov v primeru okvare ali poškodbe trdega diska oz. računalnika. Omogočajo nam tudi obnovitev podatkov na nove sisteme (npr. ob zamenjavi računalnika).

Vse uporabniške nastavitve in vsi uporabniški podatki se v Linuxu praviloma nahajajo v podimeniku oz. na razdelku `/home` in sicer na podimeniku vsakega posameznega uporabnika (`/home/fdv` za uporabnika `fdv`, itd.). Nastavitve se praviloma nahajajo v skritih datotekah in mapah, ki imajo na začetku imena piko (npr. `“.mozilla-thunderbird”`). Brskalnik datotek Nautilus prikaže skrite datoteke če pritisnemo `Ctrl-H` ali v meniju *“Pogled”* izberemo *“Skrite datoteke”*.

Pod Linuxom lahko varnostne kopije izdelamo z orodjem Rsync. Rsync je orodje, ki ga uporabljamo iz ukazne vrstice, obstajajo pa tudi nekateri grafični vmesniki za Rsync. Eden izmed njih je `grsync` (namestiti je potrebno programski paket `grsync`, program pa zaženemo iz *Programi – Internet – Grsync*).

Rsync omogoča izdelavo popolne varnostne kopije datotek in imenikov, ohrani lahko tudi datume in lastniške pravice. Program `rsync` lahko zaženemo kot navadni uporabnik, če pa mu podamo parametre za ohranitev lastništva nad datotekami, je potrebno `rsync` oz. `grsync` pognati z administratorskimi privilegiji (iz ukazne vrstice z ukazom *“gksu grsync”*).

Pred arhiviranjem je potrebno nastaviti nekaj nastavitvev:



Osnovne možnosti *“Preserve time”*, *“Preserve permissions”*, *“Preserve owner”* in *“Preserve group”* omogočajo, da se pri arhiviranju ohrani lastništvo nad datotekami. Napredna možnost *“Copy simlinks as symlinks”* omogoča ohranitev simbolnih povezav, možnost *“Compress file data”* pa omogoča uporabo kompresiranja pri arhiviranju preko omrežja. Med osnovnimi možnostmi velja omeniti še možnost *“Delete on destination”*, ki omogoča sinhronizacijo arhiva z originalno lokacijo

(datoteke, ki so bile izbrisane na originalni lokaciji iz katere ustvarjamo arhiv, se izbrišejo tudi v arhivu). Pri tej možnosti je potrebno biti previden – če so namreč v ciljnim arhivskem imeniku še kakšne druge ne-arhivske datoteke, jih bo program ob vklopu tega parametra izbrisal, saj bo skušal arhivski imenik sinhronizirati z originalnim!

Določiti je potrebno še izvorni imenik, ki ga želimo arhivirati (*source*) ter lokacijo arhiva (*destination*). Kot lokacijo lahko nastavimo tudi oddaljeno lokacijo, npr.: “uporabnik@streznik.si:/home/uporabnik/arhiv”. V tem primeru je seveda potrebno vpisati geslo za dostop do oddaljenega sistema ali pa uporabiti ssh avtentikacijo s ključem.

Možnost “*Size only*” je uporabna pri prenosu preko omrežja; v tem primeru rsync ne prenaša datotek, ki sta enake velikosti, saj privzame, da sta datoteki enaki.

Možnosti “*Verbose*” in “*Show transfer progress*” povzročita, da program izpisuje vsa sporočila o svojem delovanju ter prikazuje napredek pri prenosu datotek.

Med dodatnimi parametri lahko navedemo še parameter “*–exclude*” kjer določimo podimenik/e, ki ga/jih ne želimo arhivirati (npr. *exclude=*”/home/matej/zacasno”).

Nastavitve lahko shranimo v profil, program pa nam omogoča, da imamo različne profile za različne vrste arhiviranja.

Rsync zna prenašati samo spremenjene dele datotek, kar zelo pohitri proces arhiviranja. Prvi prenos datotek v arhiv zato traja dolgo, kasneje pa se sinhronizirajo samo spremembe datotek. Pri arhiviranju preko omrežja lahko na ciljnim sistemu (kamor se zapisuje arhiv) uporabimo Rsync strežniški program, ki prenašanje datotek preko omrežja še optimizira.

Rsync lahko zaženemo tudi iz ukazne vrstice (npr. preko ssh povezave ali v primeru uporabe Linux strežnika). Primer ukaza za arhiviranje vsebine uporabniškega imenika /home/fdv na prenosni USB disk priključen na /media/backup (podani so parametri za ohranitev pravic in lastništva nad datotekami):

```
sudo rsync --verbose --progress --stats --compress --recursive --times -perms --links --owner --group --delete /home/fdv /media/backup
```

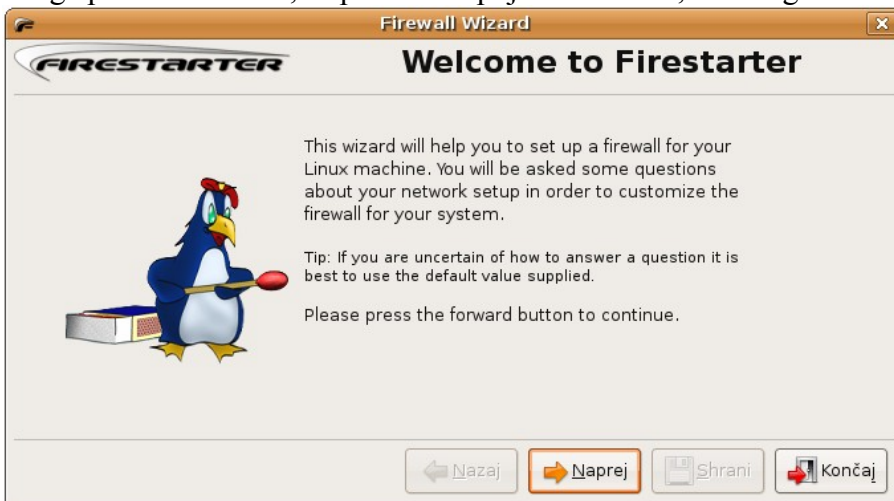
Požarni zid

Če želimo računalnik dodatno zaščititi pred nepooblaščenimi dostopi preko omrežja, je potrebno namestiti požarni zid. Nekateri uporabniki so sicer mnenja, da uporaba požarnega zidu ni potrebna, če skrbno omejimo število procesov, ki omogočajo povezovanje na računalnik. Vseeno pa velja, da je uporaba požarnega zidu za povprečnega namiznega uporabnika zelo priporočljiva.

Linux ima v ta namen vgrajen program *iptables*, s katerimi lahko uporabniki sestavljajo pravila za filtriranje mrežnega prometa, dovoljevanje ali prepovedovanje vhodnih oziroma izhodnih povezav, skratka nadzorujejo mrežni promet računalnika. *Iptables* omogočajo tudi napredno usmerjanje omrežnega prometa (izdelavo NAT – *Network Address Translation* in napredno usmerjanje (routing)). Ker je neposredno delo z *iptables* za začetnike precej težavno (gre pravzaprav za nekakšen skriptni jezik, ki zahteva tudi nekoliko bolj poglobljeno poznavanje delovanja računalniških omrežij), je priporočljiva uporaba grafičnega vmesnika za nastavljanje požarnega zidu. Eno izmed uporabniku zelo prijaznih orodij je program *Firestarter*.

Najprej namestimo programski paket “*firestarter*”. Program zaženemo iz menija *Programi – Internet – Firestarter*.

Ko ga prvič zaženemo, se pred nami pojavi čarovnik, ki omogoča osnovno nastavljanje:



V uvodnem oknu še ničesar ne nastavljamo, zato kliknemo na gumb *Naprej*.



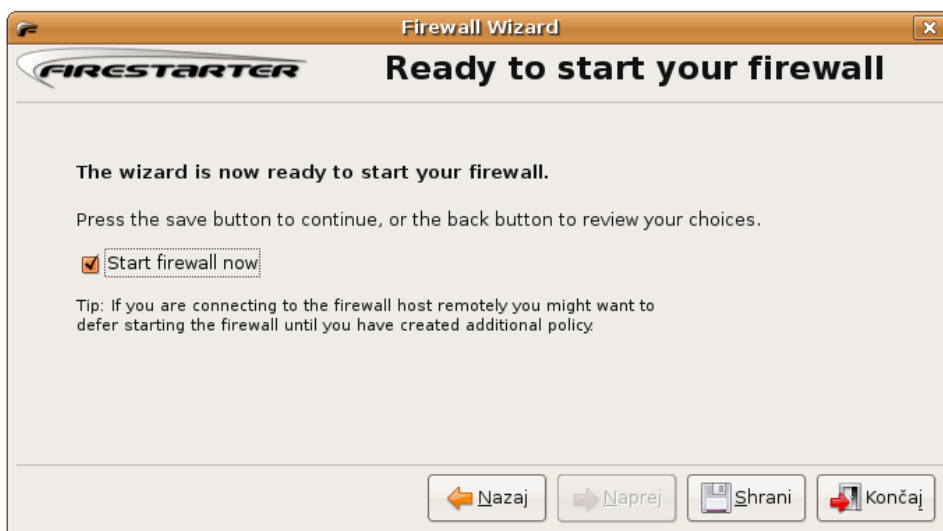
V naslednjem oknu izberemo omrežni vmesnik, ki ga želimo s požarnim zidom nadzorovati. Omrežni vmesniki so v Linuxu označeni z imeni (navedenih je le nekaj najpogostejših):

- lo (lokalni loopback vmesnik, gre za neke vrste virtualni omrežni vmesnik, ki je vedno prisoten);
- eth0,... (ime izvira iz *ethernet*, eth0 je prvi omrežni vmesnik, eth1, drugi, itd.);
- ppp0,... (PPP (*Point-to-Point Protocol*) vmesnik, ki omogoča prenos podatkov preko serijske povezave, ppp0 je prvi omrežni vmesnik, ppp1, drugi, itd.);
- tun0,... (ime izvira iz *network tunnel*, je virtualni omrežni vmesnik, ki se navadno uporablja pri VPN omrežjih, pa tudi pri virtualizaciji).

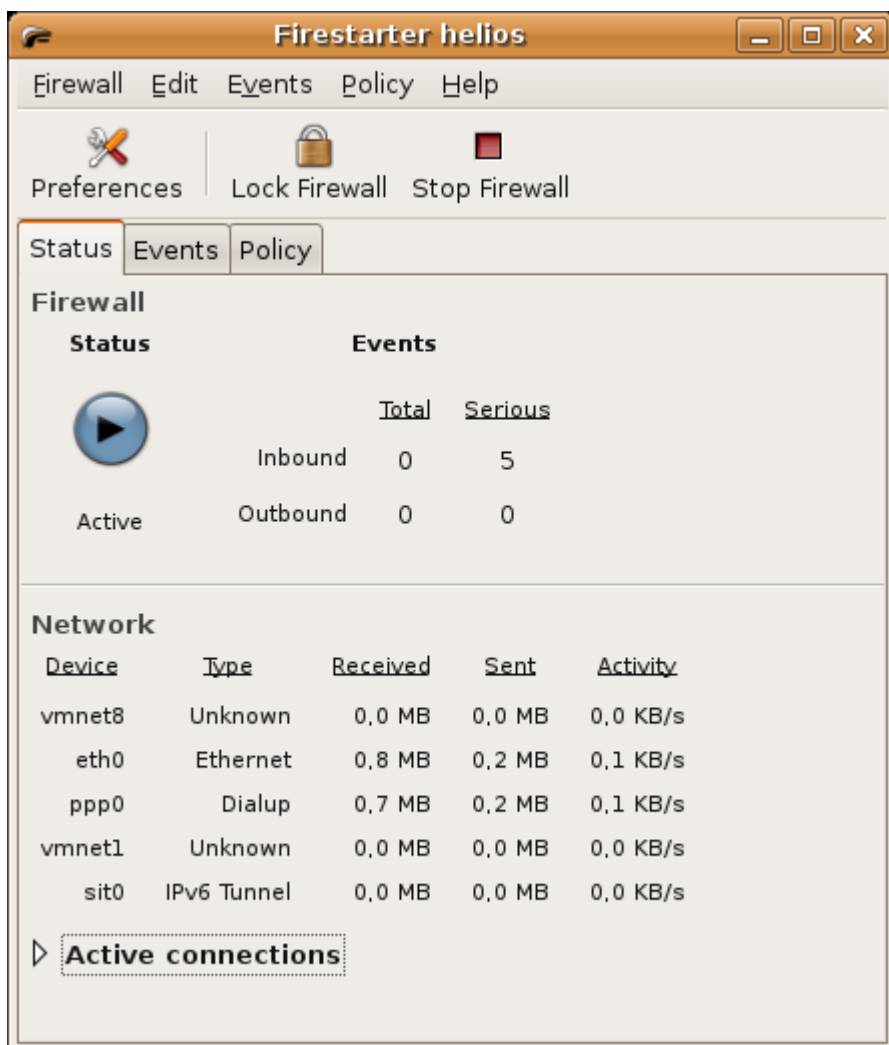
Uporabniki klicne povezave (tudi ADSL) izberejo *ppp0*, tisti, ki pa uporabljajo VDSL, kabelski dostop ali pa so priključeni na usmerjevalnik pa *eth0*. Če nimamo fiksnega IP naslova, obkljukamo tudi možnost “*IP address is assigned via DHCP*”, za aktiviranje požarnega zidu ob aktiviranju izhodne klicne povezave pa še “*Start the firewall on dial-out*”.



Naslednje okno ponuja možnost aktiviranja deljenja internetne povezave. V poštev seveda pride, če imamo več omrežnih vmesnikov. V kolikor želimo povezavo deliti izberemo omrežni vmesnik, na katerega bomo povezali ostale računalnike (običajno eth1) in vklopimo samodejno dodeljevanje IP naslovov (“*Enable DHCP for local network*”).

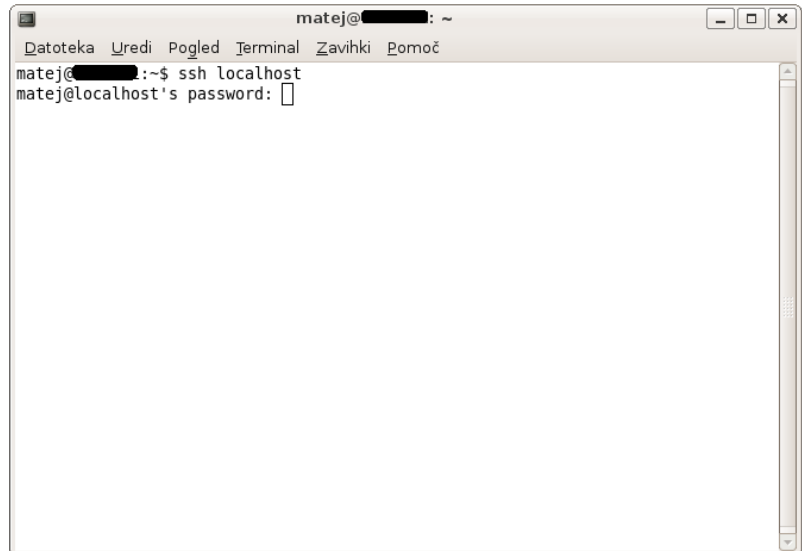
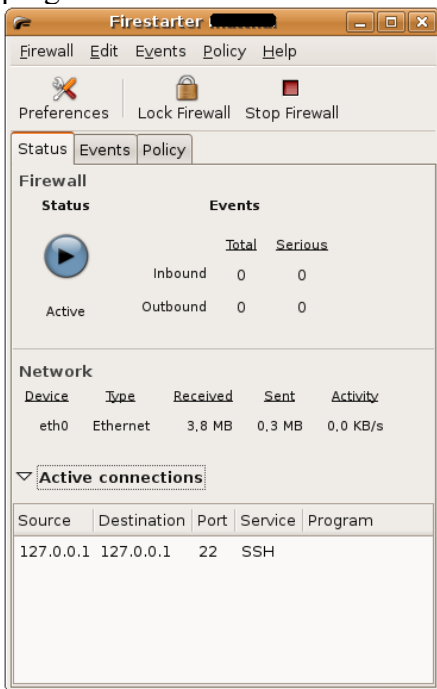


Po potrditvi izbire s klikom na *Naprej* se pojavi zadnje okno čarovnika, kjer izberemo možnost "Start firewall now" in potrdimo s pritiskom na gumb *Shrani*.

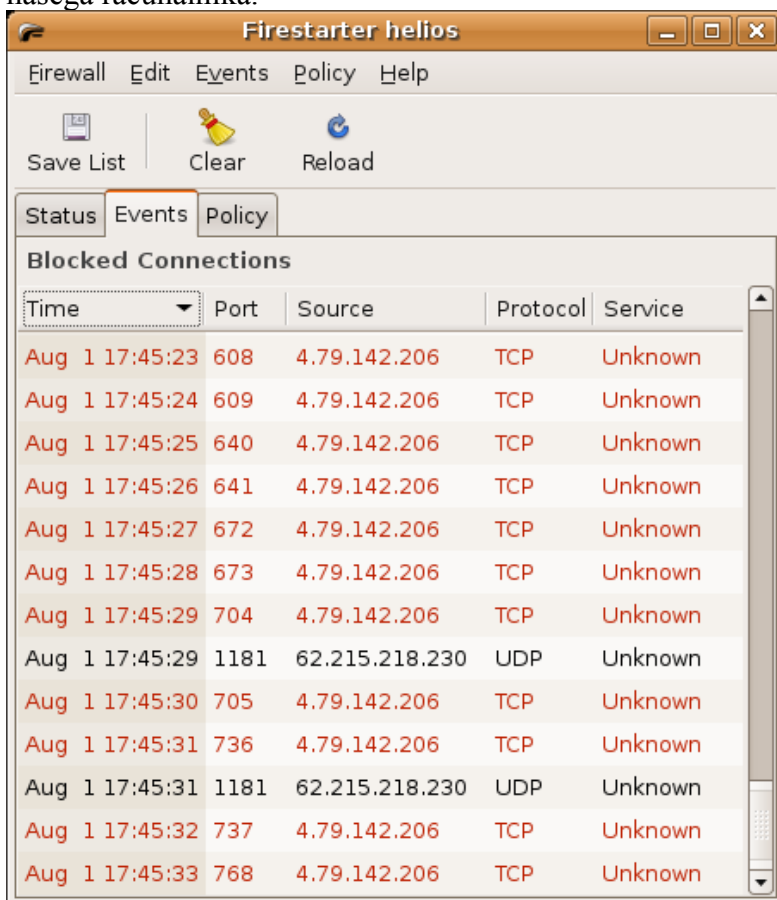


V oknu glavnega vmesnika najdemo tri gumbе in tri zavihke. Gumb *Preferences* omogoča dostop do možnosti požarnega zidu, *Lock Firewall* blokira ves omrežni promet (dohodne in odhodne omrežne povezave), *Stop firewall* pa zaustavi požarni zid.

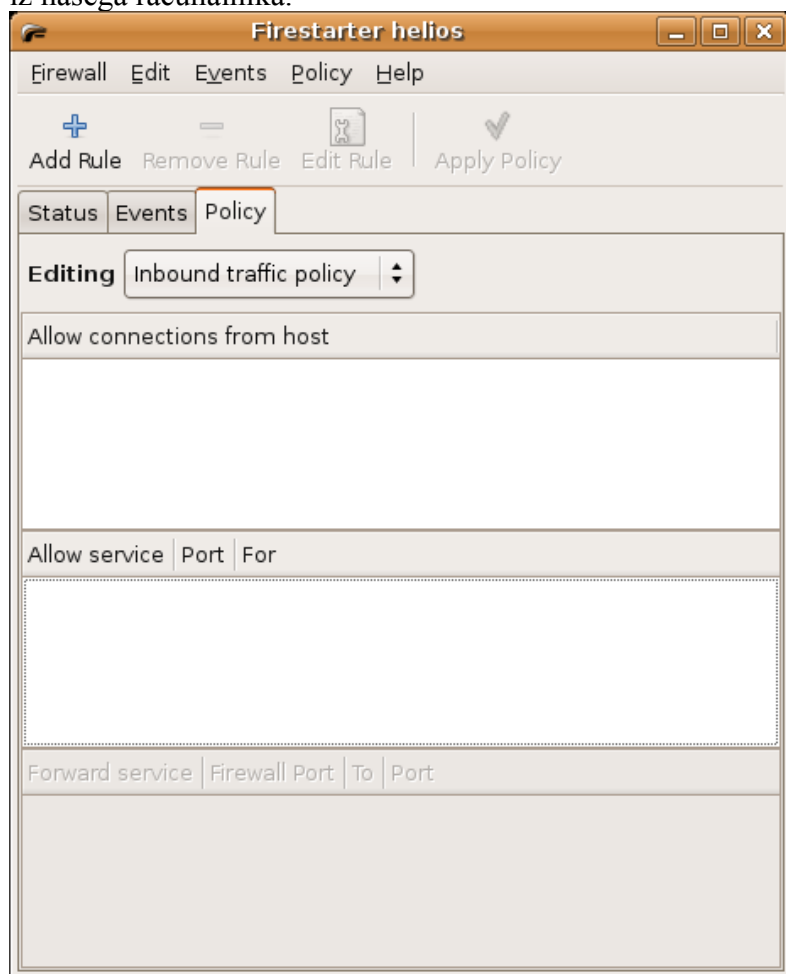
Zavihek *Status* nam prikazuje stanje in promet preko mrežnih vmesnikov in aktivne povezave programov na računalniku. Lahko si ogledamo tudi aktivne povezave.



Zavihek *Events* nam omogoča spremljanje delovanja požarnega zidu. Prikazuje blokirane vhodne povezave. Tako lahko “v živo” vidimo, od kod vse poskušajo različni računalniki dostopati do našega računalnika.



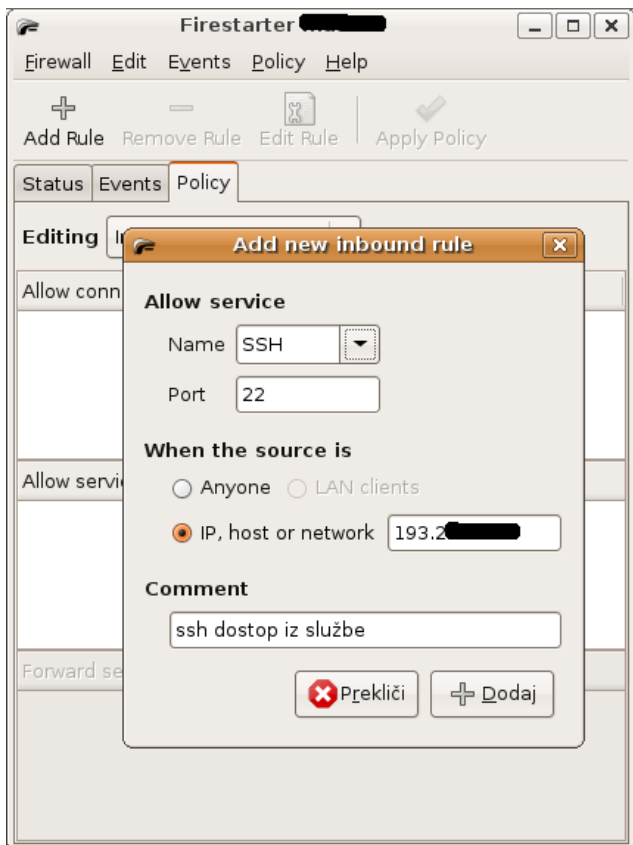
Zavihek *Policy* pa se uporablja za vnašanje pravil, ki dovoljujejo ali prepovedujejo povezave na in iz našega računalnika.



Nastavimo lahko pravila za vhodni ali izhodni promet. Pravila za izhodni promet so privzeto permissivna (dovoljujejo vse povezave, razen prepovedanih), lahko pa nastavimo, da so restriktivna (dovoljujejo samo izrecno določene povezave).

Z desnim klikom na polje pod *Allow connections from host* odpremo novo pogovorno okno ter izberemo *Add rule*, kjer lahko določimo IP naslov, ime gostitelja ali omrežje iz katerega dovolimo dostope na naš računalnik.

Če želimo omogočiti dostop do posamezne storitve, npr. oddaljen dostop do našega računalnika preko ssh, z desnim klikom na polje pod *Allow service* odpremo novo pogovorno okno, izberemo *Add rule*, nato pa pri polju *Name* iz menija izberemo *SSH*, pri čemer se polje *Port* (vrata) izpolni samo (glede na običajne privzete vrednosti, ssh običajno posluša na vratih 22). Pod *When source is* lahko omogočimo dostop do ssh vrat komerkoli, ali pa dodelimo dostop glede na IP naslov, ime gostitelja ali omrežje. V polje *Comment* lahko vpišemo opombo po želji. Če zelene storitve ni na seznamu, lahko vsa polja izpolnimo ročno.

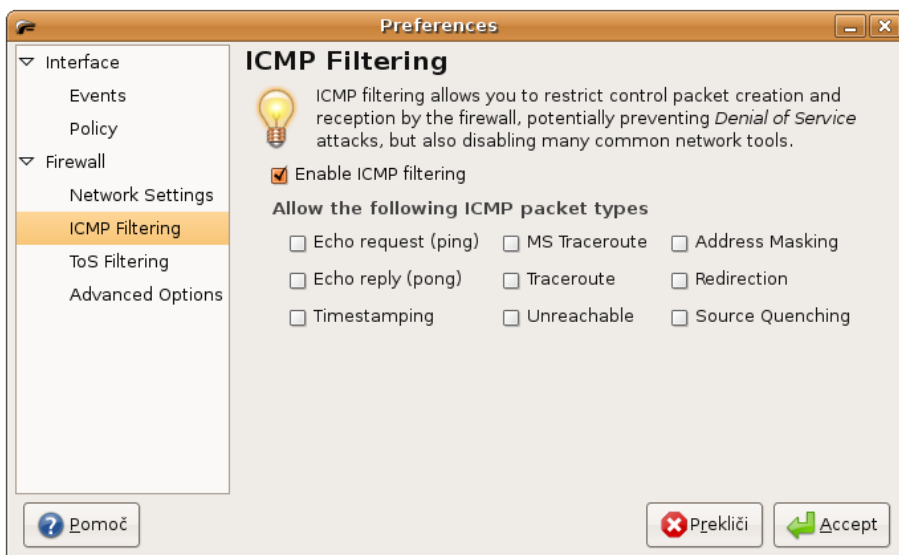


S klikom na *Apply Policy* pravilo uveljavimo.

Na zavihku *Status* lahko kliknemo na gumb *Preferences*, kjer lahko dodatno nastavljamemo požarni zid.

Pod *Interface – Policy* lahko določimo, da se spremembe uveljavijo takoj, ko je novo pravilo ustvarjeno. Pod *Firewall* lahko nastavimo kdaj se požarni zid zažene oz. ponovno zažene. Po ponovnem zagonu računalnika se požarni zid praviloma sam aktivira, kar sicer ni vidno nikjer na zaslonu. Program namreč ob ponovnem zagonu računalnika zažene ustrezno iptables skripto z našimi pravili.

Pod *Firewall – ICMP filtering* lahko vključimo dodatno filtriranje ICMP prometa, med ostalimi nastavitvami pa lahko tudi določimo obnašanje požarnega zidu ob blokiranju povezav ter nastavimo filtriranje glede na prioriteto omrežnega prometa,



Dodatna pravila, ki smo jih napisali z *iptables* lahko shranimo v datoteko */etc/firestarter/user-pre* ali v datoteko */etc/firestarter/user-post*. V prvem primeru jih bo *Firestarter* zagnal začetku, v drugem pa ob koncu izvajanja svojih pravil.

Samodejni zagon požarnega zidu Firestarter ob zagonu računalnika

Ob (ponovnem) zagonu računalnika se požarni zid sam zažene (to sicer za nekatere distribucije Linuxa ne velja), saj program ob ponovnem zagonu računalnika zažene ustrezno *iptables* skripto z našimi pravili.

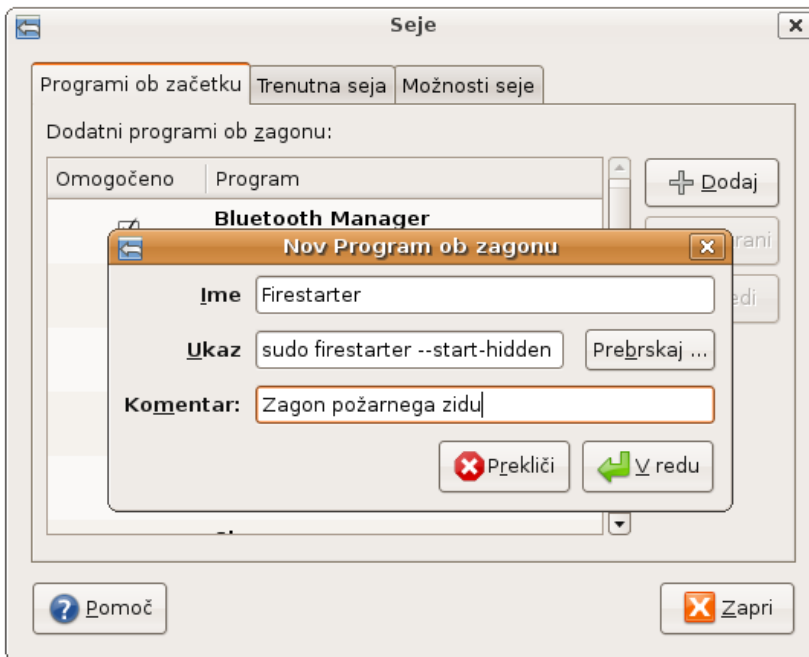
Če želimo ob ponovnem zagonu sistema samodejno zagnati *Firestarter*, najprej določimo, da ob zagonu *Firestarterja* ni potrebno vpisovati gesla za vstop v administratorski način. To storimo tako, da v datoteko */etc/sudoers* dodamo pravilo, kateri uporabniki lahko zaženejo *Firestarter* brez gesla.

V ukazni vrstici vnesemo ukaz “`sudo gedit /etc/sudoers`” in na konec datoteke dodamo pravilo:

```
uporabnik ALL= NOPASSWD: /usr/bin/firestarter
```

Namesto *uporabnik* vnesemo ime ustreznega uporabnika, npr. *matej*. Uporabnik bo sedaj lahko zagnal *Firestarter* z administratorskimi privilegiji ne da bi mu bilo potrebno vnesti geslo za vstop v administratorski način.

Na koncu je potrebno nastaviti še samodejni zagon *Firestarterja* ob prijavi v sistem. V *Sistem – Nastavitve – Seje* kliknemo na gumb *Dodaj* ter v polje Ukaz vnesemo “`sudo firestarter –start-hidden`”.



Ob naslednjem zagonu se bo *Firestarter* samodejno zagnal in prikazal v statusni vrstici.

Uporabniški priročnik za požarni zid *Firestarter* je mogoče dobiti na naslovu:

- <http://www.fs-security.com/docs/fs-manual.pdf>

Dodatni omrežni triki (ukaze vnesemo v ukazno vrstico):

- izpis aktivnih omrežnih povezav: `netstat --inet -p`
- izpis aktivnih omrežnih povezav brez DNS preverjanja: `netstat --inet -pn`
- izpis vzpostavljenih omrežnih povezav `netstat -an | grep EST`
- identifikacija aplikacije, ki je povezana na določenih vratih: `lsof -nP | grep 37174`

Povezovanje v VPN omrežja

VPN (Virtual Private Networking) nam omogoča varno povezovanje različnih omrežij med seboj z uporabo šifriranih tunelov. Prek takšnega tunela lahko dostopamo do oddaljenega omrežja na podoben način, kot bi bili fizično prisotni v omrežju ali celo speljemo ves internetni promet iz našega računalnika preko tunela do oddaljenega računalnika ter tako dostopamo do interneta preko oddaljenega omrežja. VPN se tako uporablja za oddaljen dostop do računalnikov v internih omrežjih in njihovih storitev (interni spletni strežniki, interni datotečni strežniki), varno uporabo brezžičnih omrežij (preusmeritev internetnega prometa od našega računalnika prek tunela do varne izhodne točke na ožičenem omrežju), itd. VPN sicer omogoča povezovanje med različnimi sistemi (Windows, Linux,...).

Za vzpostavitev VPN povezav obstaja več različnih odjemalcev. Eden izmed bolj uporabljanih je *OpenVPN*. *OpenVPN* pod Linuxom teče kot *demon* (ang. *daemon*, proces, ki teče v ozadju), upravljamo pa ga iz ukazne vrstice. Programski paket, ki ga je potrebno namestiti se imenuje *openvpn*. Na voljo pa je tudi grafični upravljavski vmesnik *Open VPN Admin*.

Neposredno z Open VPN omrežji zna delati tudi Ubuntujev upravitelj omrežja, vendar njegovo delovanje ni zanesljivo (v trenutni različici ga včasih ni mogoče zagnati). Če ga vseeno želimo uporabiti je potrebno namestiti dodatek za upravitelj omrežja, paket z imenom *network-manager-openvpn*.

Če želimo postaviti Open VPN strežnik moramo postaviti svojo lastno infrastrukturo javnih ključev (tim. PKI infrastrukturo - *public key infrastructure*). PKI infrastruktura vsebuje javni ključ (certifikat) in zasebni ključ VPN strežnika in vseh odjemalcev ter glavni CA certifikat (Certificate Authority) namenjen digitalnemu podpisovanju javnih ključev (certifikatov) strežnika in odjemalcev. To je pomembno zato, ker OpenVPN podpira dvosmerno avtentikacijo – strežnik se avtentificira odjemalcu, odjemalec pa strežniku. Pri vzpostavitvi povezave se strežnik in odjemalec drug drugemu avtentificirata tako, da najprej preverita ali je bil certifikat drugega podpisan s strani CA certifikata.

Na strežniku zato potrebujemo samo CA javni ključ, strežniški certifikat in strežniški zasebni ključ, ne pa tudi certifikatov odjemalcev. Strežnik pa bo tudi sprejel samo tiste certifikate odjemalcev (oz. dovolil samo tiste VPN povezave s strani odjemalcev), ki so bili podpisani s strani CA certifikata. Strežnik pri tem potrebuje samo CA javni ključ, ne pa tudi CA zasebnega ključa. CA zasebni ključ lahko zato zaradi varnosti odstranimo iz računalnika (ga arhiviramo, ne izbrišemo!). Brez CA zasebnega ključa namreč ni mogoče ustvarjati oz. podpisovati novih ključev za odjemalce. V primeru kraje odjemalčevega certifikata je mogoče posamezni kompromitirani certifikat preklicati, hkrati pa je mogoče za vsakega odjemalca posebej nastaviti dostopne pravice.

Nastavitev odjemalca

Za povezovanje v VPN omrežje potrebujemo:

- CA certifikat
- odjemalčev javni ključ (odjemalčev certifikat)
- odjemalčev zasebni ključ
- po možnosti pa še *tls-auth* ključ, ki še poveča varnost VPN povezave

Vse omenjene ključe in ustrezno konfiguracijsko datoteko nam dodeli upravitelj VPN strežnika. Ključe in konfiguracijsko datoteko shranimo v podimenik `/etc/openvpn` in sicer po naslednjem

dogovoru: (primer za povezavo z imenom "Sluzba"):

- Podimenik /etc/openvpn:
 - Sluzba.conf
- Podimenik /etc/openvpn/Sluzba
 - ca.crt (CA certifikat)
 - odjemalec1.crt (odjemalčev javni ključ)
 - odjemalec1.key (odjemalčev zasebni ključ)
 - ta.key (tls-auth ključ)

VPN povezavo sedaj zaženemo iz ukazne vrstice z ukazom:

```
sudo /etc/init.d/openvpn start Sluzba
```

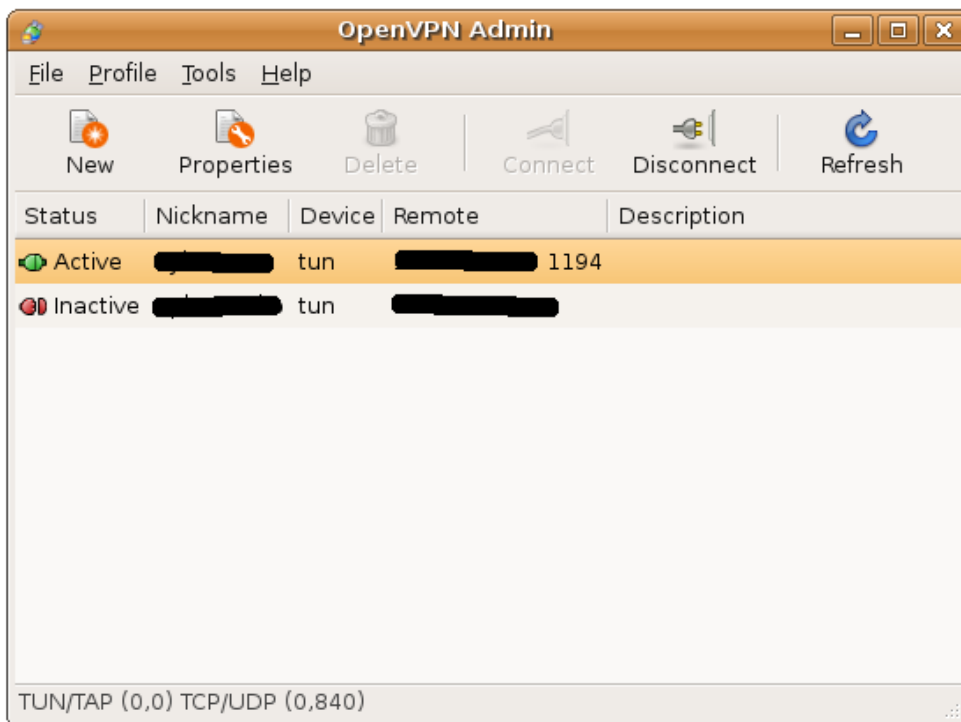
Povezavo pa zaustavimo z ukazom:

```
sudo /etc/init.d/openvpn stop Sluzba
```

Če želimo, da se VPN povezava samodejno vzpostavi ob zagonu računalnika je potrebno popraviti konfiguracijsko datoteko /etc/default/openvpn. Na začetek dodamo vrstico:

```
AUTOSTART="Sluzba"
```

Če želimo pa lahko uporabimo grafični upravljalni vmesnik *Open VPN Admin*. *Open VPN Admin* je potrebno namestiti iz deb paketa, ki ga najdemo na spletni strani <http://sourceforge.net/projects/openvpnadmin>.



Po namestitvi program *OpenVPN Admin* najdemo v meniju *Programi - Sistemsko orodja - OpenVPN Administrator*. Po zagonu se naseli v sistemsko vrstico, iz njega pa je mogoče enostavno upravljati (zaganjati in zaustavljati) ter urejati VPN povezave.

Navodila za postavitve OpenVPN strežnika ter nastavitve odjemalcev je mogoče dobiti na naslovu:

- <http://openvpn.net>
- <http://wiki.cybersoc.info/doku.php/debian:openvpn>

Ukazna vrstica

Ukazno vrstico odpremo s klikom na: *Programi – Pripomočki – Terminal* oziroma z vstopom v virtualno konzolo s pritiskom na Ctrl-F1 do Ctrl-F6 (na Ctrl-F7 se nahaja grafična virtualna konzola). V ukazno vrstico lahko vnašamo ukaze s tipkovnico. Načeloma lahko z ukazno vrstico postorimo vse, kar lahko postorimo tudi v grafičnem vmesniku (to velja za sistemske nastavitve, pa tudi za nekatere grafične programe).

Osnovni ukazi

Seznam nekaj najpogostejših osnovnih ukazov:

| <i>ukaz</i> | <i>razlaga</i> |
|--|--|
| ls | ang. <i>list</i> , pregled vsebine imenika. Z dodatnimi parametri <i>-lh</i> dobimo uporabniško prijazen izpis datotek z njihovimi velikostmi, parameter <i>-a</i> doda izpis vseh, tudi skritih datotek. Iz izpisa je razvidno tudi lastništvo datotek (uporabnik: matej, skupina video) ter pravice dostopa (uporabnik in skupina imata pravico datoteko brati in vanjo pisati, ostali pa samo brati): -rw-rw-r-- 1 matej video 16 2008-04-22 15:17 test.txt |
| cd <ime> | ang. <i>change directory</i> , vstopimo v imenik z imenom <ime>. Z ukazom <i>cd ..</i> se vrnemo v nadrejeni imenik. |
| mkdir <ime> | ang. <i>make directory</i> , ustvarimo imenik z imenom <ime>. |
| rm <ime> | ang. <i>remove</i> , odstranimo datoteko z imenom <ime>. Če želimo odstraniti podimenik, dodamo parameter <i>-r</i> , ki rekurzivno odstrani imenik in celotno njegovo vsebino. Parameter <i>-f</i> izvede prisilno odstranitev (brez spraševanja). Ukaz <i>rm -rf <ime></i> uporabljajmo s skrajno previdnostjo! |
| mv <ime> <cilj> | ang. <i>move</i> , ukaz premakne datoteko ali imenik na ciljno lokacijo. Kot ciljno lokacijo navedemo podimenik ali piko (.) za trenutni podimenik. |
| cp <ime> <cilj> | ang. <i>copy</i> , ukaz je namenjen kopiranju datotek na cilj. Če dodamo parameter <i>-r</i> je kopiranje rekurzivno. |
| scp <ime> <cilj> | ang. <i>secure copy</i> , ukaz je namenjen kopiranju datotek preko omrežja, pri kopiranju se uporablja šifrirana povezava. Če dodamo parameter <i>-r</i> je kopiranje rekurzivno. |
| chmod <kdo><+/-><pravice> <datoteka> <parametri> | ang. <i>change mode</i> , nastavljanje pravic dostopa do datotek ali imenikov. Pravice nastavljamo za lastnika, skupino, druge ali za vse, nastavimo pa lahko pravico do branja, pisanja ali izvajanja (programa). Pravice podamo v obliki: <kdo><+/-><pravica>. Če dodamo parameter <i>-R</i> se ukaz izvede za imenik, njegovo vsebino in vse podimenike. <kdo> je lahko "u" (<i>user</i> – uporabnik), "g" (<i>group</i> – skupina), "o" (<i>other</i> – ostali) ali "a" (<i>all</i> – kdorkoli). |

| | |
|--------------------------------------|--|
| | <p>Z oznako + ali – označimo ali bomo določeno pravico dodali ali odvzeli.</p> <p><pravice> so lahko “r” (<i>read</i> – pravica branja), “w” (<i>write</i> – pravica pisanja) ter x (<i>execute</i> – pravica izvajanja).</p> <p>Primer (na datoteki test.txt skupini in uporabniku podelimo pravico branja in pisanja):</p> <pre>chmod ug+rw test.txt</pre> |
| chown <uporabnik.skupina> <datoteka> | <p>ang. <i>change owner</i>, sprememba lastništva nad datoteko ali imenikom (sprememba lastnika in skupine).</p> <p>Ukaz chown fdv.fdv test.txt bo spremenil lastništvo datoteke test.txt tako, da bo lastnik postal uporabnik fdv ter skupina fdv.</p> |
| cat <ime> | ang. <i>concatenate</i> , izpiše vsebino datoteke na zaslon. |
| ps -A | ang. <i>process</i> , ukaz s podanim parametrom -A izpiše seznam aktivnih procesov (programov). |
| killall <ime_procesa> | Ukaz ubije (ugasne) aktiven proces (program). |
| top | Ukaz prikaže koliko sistemskih sredstev (procesorske moči in pomnilnika) porabijo procesi in programi. S pritiskom na M se prikažejo procesi sortirani glede na porabo pomnilnika. Pregled zapustimo s pritiskom na tipko q. |
| htop | Program htop je ravno tako namenjen prikazu porabe sistemskih sredstev, le da ima dodatne možnosti izpisov in je enostavnejši za uporabo. Ker ni vključen v sistem, ga je potrebno najprej namestiti. Program krmilimo s pritiski na tipke F1 do F10, zapustimo pa s pritiskom na tipko q. |
| sudo <ukaz> | Ukaz omogoča izvajanje podanega ukaza (<ukaz>) z administratorskimi privilegiji oziroma kot nek drug uporabnik. Uporabnik, ki želi izvesti ta ukaz mora imeti ustrezne privilegije (navedene v datoteki /etc/sudoers). ukaz sudo su omogoča prijavo trenutnega uporabnika kot administratorja (root) sistema. |
| su <uporabnik> | Trenutni uporabnik se v sistem prijavi kot upoabnik z imenom <uporabnik>. |
| w | ang. <i>who</i> , ukaz izpiše uporabnike, ki so prijavljeni v sitem ter ukaze, ki jih izvajajo (v primeru uporabnikov, ki so prijavljeni v grafično okolje je izpisan samo podatek, da uporabnik poganja grafično okolje (x-session-manager). |
| pwd | ang. <i>print working directory</i> , ukaz izpiše v katerem imeniku se trenutno nahajamo. |
| man <ime_ukaza> | ang. <i>manual</i> , ukaz prikaže kratek uporabniški priročnik oziroma opis ukaza in njegovih parametrov. |
| nano <ime_datoteke> | Nano je preprost urejevalnik teksta. Ko končamo s pisanjem besedila program zapustimo s pritiskom na Ctrl-X. Program nas vpraša ali naj shrani spremembe (odgovorimo Y- Yes) ter vpišemo ime datoteke, kamor želimo shraniti besedilo (oz. pritisnemo enter za uporabo privzete vrednosti). |

Nameščanje in odstranjevanje programov iz ukazne vrstice

Za nameščanje programov v okolju Ubuntu uporabljamo orodje apt. Seznam programskih skladišč lahko dodamo z urejanjem datoteke `/etc/apt/sources.list`. Ukaz je potrebno zagnati z administratorskimi privilegiji (torej s `sudo`).

| <i>ukaz</i> | <i>razlaga</i> |
|---|--|
| <code>apt-get update</code> | Iz seznama programskih skladišč osvežimo seznam programskih paketov, ki se nahajajo v teh skladiščih. |
| <code>apt-get upgrade</code> | Namestimo posodobitve sistema. |
| <code>apt-cache search <ime></code> | Iščemo med programskimi paketi, ki so nam na voljo. Iskanje poteka po imenu in opisu. |
| <code>apt-get install <ime_paketa></code> | Namestimo programski paket. |
| <code>apt-get install --reinstall <ime_paketa></code> | Ponovno namestimo programski paket. |
| <code>apt-get remove <ime_paketa></code> | Odstranimo programski paket. |
| <code>apt-get remove --purge <ime_paketa></code> | Popolnoma odstranimo programski paket. |
| <code>dpkg -i <ime paketa></code> | Namestimo .deb paket, ki smo ga prenesli v trenutni imenik. |
| <code>dpkg -l</code> | Izpišemo seznam vseh nameščenih in ne popolnoma odstranjenih programskih paketov v sistemu. |
| <code>dpkg-reconfigure xserver-xorg</code> | Ponovno nastavimo grafični strežnik X, ukaz je uporaben kadar želimo odpraviti težave z gonilniki za grafično kartico oz. nastavitvami grafične kartice ali monitorja. |

Delo z omrežjem

Pri delu z omrežjem je potrebno najprej nastaviti IP naslov in podomrežno masko (maska razdeli omrežje na podomrežja in določa, koliko IP številk premore dano omrežje).

Fiksni IP naslov nastavimo z ukazom `ifconfig`, dinamičnega pa preko DHCP pridobimo z ukazom `dhclient`. Sledi nastavitvev poti (ang. *route*) na koncu pa nastavimo še IP naslove DNS strežnikov.

| <i>ukaz</i> | <i>razlaga</i> |
|---|--|
| <code>ifconfig <omrežni_vmesnik> <ukaz></code> | Ukaz <code>ifconfig</code> je namenjen nastavljanju omrežnih vmesnikov. Najpogosteje ima računalnik en sam ethernet omrežni vmesnik, ki se imenuje <code>eth0</code> . |
| <code>ifconfig eth0 down</code> | Ukaz deaktivira in odstrani vse IP naslove na omrežnem vmesniku <code>eth0</code> , prav tako se prekinejo vse omrežne povezave in poti (ang. <i>route</i>). |
| <code>ifconfig eth0 192.168.1.166 netmask 255.255.255.0 up</code> | Priklop omrežnega vmesnika – dodelili smo mu IP naslov 192.168.1.166 na podomrežni maski 255.255.255.0. |
| <code>ifconfig eth0</code> | Izpis nastavitvev omrežnega vmesnika <code>eth0</code> . Če želimo izpisati nastavitve vseh omrežnih vmesnikov vpišemo samo ukaz <code>ifconfig</code> . |
| <code>ifconfig eth0:1 192.168.1.167 up</code> | Vzpostavitev virtualnega mrežnega vmesnika <code>eth0:1</code> z IP naslovom 192.168.1.167. |

| | |
|---|--|
| <code>sudo ifconfig eth0 hw ether 00:01:10:00:01:10</code> | Sprememba MAC naslova mrežne kartice (v 00:01:10:00:01:10). |
| <code>route add default gw 192.168.1.1</code> | Z ukazom smo v omrežne nastavitve dodali privzeti prehod, (ki povezuje naše omrežje z nekim drugim, npr. internetom) ki se nahaja na IP naslovu 192.168.1.1. |
| <code>route -n</code> | Izpis omrežnih poti. |
| <code>iwconfig <omrežni_vmesnik> <ukaz> <parameter></code> | Ukaz iwconfig je namenjen nastavljanju brezžičnih omrežnih vmesnikov. |
| <code>iwconfig wlan0 essid <ESSID_omrežja></code> <code>iwconfig wlan0 channel <kanal></code> <code>iwconfig wlan0 ap <BSSID_dostopne_točke></code> | Prvi ukaz brezžični omrežni vmesnik poveže na omrežje z ESSID (ime omrežja, ki ga oddaja brezžična dostopna točka). Z drugim ukazom lahko določimo na kateri brezžični kanal se bomo povezali (od 1 do 14, praviloma se povezujemo na kanal 11, vsi kanali pa niso v uporabi v vseh državah). S tretjim ukazom pa se priključimo na brezžično dostopno točko z danim BSSID-jem (strojnim naslovom brezžičnega omrežnega vmesnika) omrežja, npr.: <code>iwconfig wlan0 ap 02:ca:ff:ee:ba:be</code> |
| <code>dhclient <omrežni_vmesnik></code> | Z ukazom preko DHCP pridobimo omrežne nastavitve na omrežnem vmesniku. |

IP naslove DNS strežnikov vpišemo v datoteko `/etc/resolv.conf` in sicer v obliki `nameserver <IP_naslov>`, primer za DNS strežnike Arnesa:

```
nameserver 193.2.1.72
nameserver 193.2.1.66
```

Razno

| <i>ukaz</i> | <i>razlaga</i> |
|---|--|
| <code>lspci</code> | Iang. <i>list PCI</i> , izpiše seznam vseh PCI naprav (PCI kartic) v računalniku. |
| <code>dmesg</code> | ang. <i>diagnostic message</i> , izpiše sporočila Linux jedra, izpis se pogosto uporablja za odpravljanje napak. |
| <code>df -h</code> | ang. <i>disk free</i> , izpiše zasedenost posameznih razdelkov na disku oz. diskov. |
| <code>du -h <imenik></code> | ang. <i>disk space usage</i> , izpiše zasedenost imenika in vseh njegovih podimenikov. |
| <code>tail -f <datoteka></code> | Izpisuje konec datoteke. Uporabno za izpisovanje sistemskih sporočil. Izpisovanje prekinemo s pritiskom na Ctrl-C. Primer: <code>tail -f /var/log/messages</code> <code>tail -f /var/log/syslog</code> |
| <code>sudo /etc/init.d/<ime_storitve> start stop restart</code> | S parametri start, stop ali restart zaganjamo, ugašamo ali ponovno zaganjamo storitve (ang. <i>service</i>) sistema. Če želimo npr. ponovno zagnati omrežje (torej izključiti omrežni vmesnik, ga ponovno vključiti ter nastaviti IP |

| | |
|------------------------------------|--|
| | naslov in ostale omrežne nastavitve vnesemo ukaz: sudo /etc/init.d/networking restart |
| sudo mount <razdelek> <lokacija> | Ukaz se uporablja za ročno priklopljanje razdelkov na dano lokacijo. Primer: sudo mount /dev/sda1 /mnt Ukaz sudo mount -a ponovno priklopi vse razdelke, ki se avtomatično priklopijo ob zagonu računalnika (in so navedeni v datoteki /etc/fstab) |
| sudo umount <lokacija> | Z ukazom ročno odklopimo razdelek, priključen an dano lokacijo. Primer: sudo umount /mnt |
| sudo sfdisk -l | Ukaz izpiše vse razdelke v sistemu. |
| mkfs.<datotečni_sistem> <razdelek> | Ukaz formatira dani razdelek z podanim datotečnim sistemom. Primer (formatiramo razdelek hda1 z datotečnim sistemom ext3): sudo mkfs.ext3 /dev/hda1 Nekateri datotečni sistemi: mkfs.ext2, mkfs.ext3, mkfs.ntfs, mkfs.vfat , mkfs.reiserfs. Previdnost pri uporabi ukaza! |

Naloge:

- brskanje po imenikih na disku,
- pregled vsebine tekstovne datoteke,
- urejanje tekstovne datoteke z urejevalnikom nano,
- napisati skripto ter jo zagnati,
- zagon brskalnika Firefox iz ukazne vrstice,
- pregled aktivnih procesov,
- nasilno ugašanje programa (Firefox).

Vaje:

- varnost brezžičnih omrežij
- ogledal nekaj kratkih filmov o varnosti brezžičnih omrežij
- prikaz uporabe ukazov v ukazni vrstici v operacijskem sistemu BusyBox na brezžični dostopni točki.