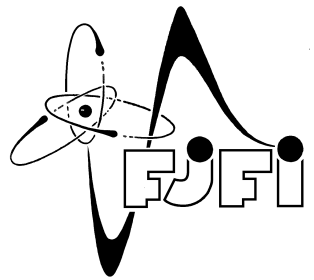
Úvod do Unixu

4. cvičení

Jan Nikl

2021



Obsah

- opakování
- autentizace SSH
- síťové nástroje
- textové editory
- e-mail
- úvod do Vim

Opakování

- archivace, komprimace – `tar`, `gzip`, `gunzip`, `...`
- vzdálené připojení – `ssh`, `logout`
  - připojení zvenčí – `kelvin`, `raman`
  - složka `~user/public_html/` dostupná přes `http://kfe.fjfi.cvut.cz/~user/`
- přenos souborů – `scp`, `sftp`, `mc`, `...`

Autentizace SSH

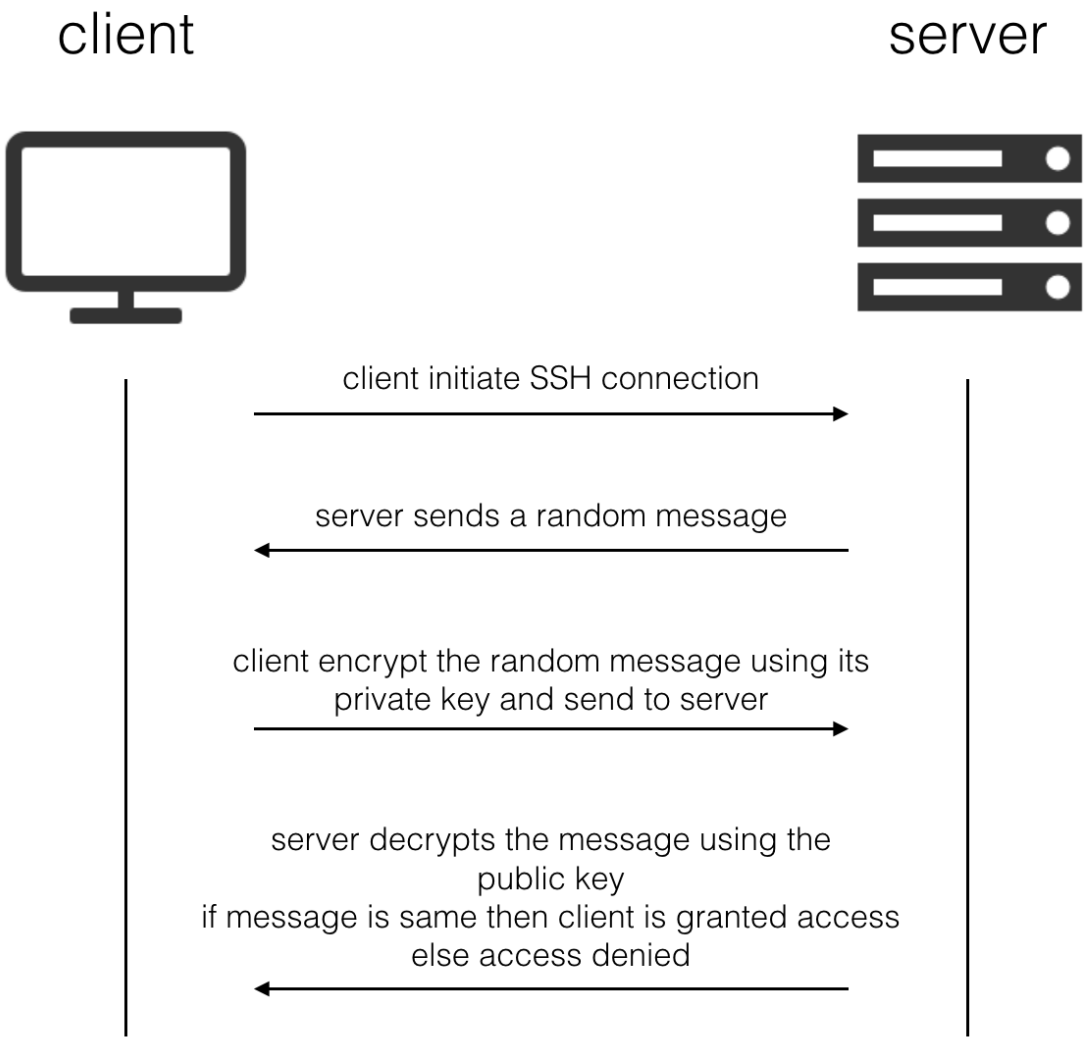
šifrování:

- symetrické – obě strany šifrují společným klíčem (AES, Twofish, Blowfish, RC4, 3DES, ...)
- asymetrické – jedna strana používá veřejný klíč, druhá strana privátní klíč (DSA, RSA, eliptické křivky, ...)

autentizace SSH:

- heslem – (ne)interaktivně zadané heslo
- klíčem – kombinací veřejný–soukromý klíč (DSA, RSA, X.509)
- (GSSAPI – přes autorizační server)

Autentizace SSH



https://www.dyclassroom.com/reference-server/how-to-setup-ssh-key-based-authentication-on-linux-server

Autentizace SSH

lokální postup:

1. vygenerování páru veřejný + privátní klíč
2. přenos veřejného klíče na server*
3. přidání soukromého klíče přihlašovacímu agentovi

```
ssh-keygen -t dsa
```

```
scp ~/.ssh/id_dsa.pub
uzivatel@server.domena:~/
```

```
ssh-add ~/.ssh/id_dsa
```

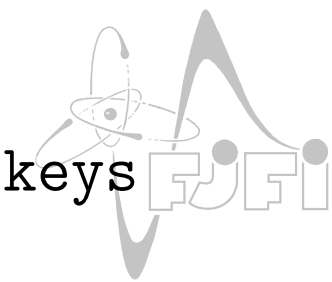
postup na serveru:

4. přidání veřejného klíče mezi akceptované
5. úklid
6. zabezpečení

```
cat ~/id_dsa.pub »
~/.ssh/authorized_keys
```

```
rm ~/id_dsa.pub
```

```
chmod 600
~/.ssh/authorized_keys
```



*Místo kroků 2,4–6 můžete použít `ssh-copy-id`

Autentizace SSH

postup na KFE:

1. vygenerování páru veřejný + privátní klíč

```
cd ~/.ssh/
ssh-keygen -t dsa
```

2. (zapnutí ssh agenta)

```
eval $(ssh-agent)
```

3. přidání soukromého klíče přihlašovacímu agentovi

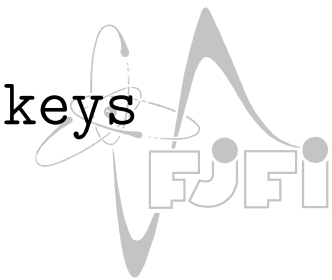
```
ssh-add id_dsa
```

4. nastavení veřejného klíče jako akceptovaného

```
cp id_dsa.pub
authorized_keys
```

5. zabezpečení

```
chmod 600
~/.ssh/authorized_keys
```



Síťové nástroje

- `ping` – testování spojení, odezvy
- `nslookup` – DNS překlad adresy
- `traceroute` (`tracert`) – sledování cesty paketu
- `dig` – DNS záznam serveru
- `write`(`, mesg, talk`) – psaní zpráv jiným uživatelům
- `netstat` – otevřená spojení
- `ifconfig` – nastavení síťových rozhraní
- `ip addr show` – nastavení sítě
- (`finger` – informace o uživateli)

Vyzkoušejte

`traceroute -n 8.8.8.8`

sledování cesty paketu na veřejné DNS Googlu bez překladu IP adres

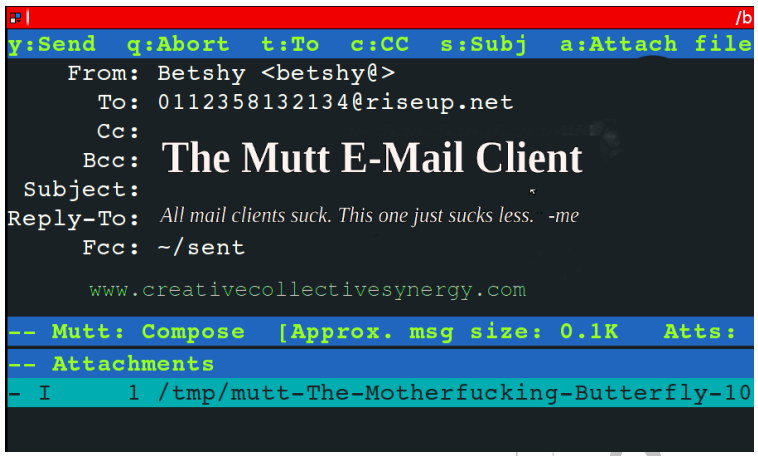
E-mail

- od počátku Unixu, původně lokálně (/var/mail)
- zcela nešifrované!
- přes Internet funguje pouze na `newtonovi`

klienti

- `mail` – původní, bez uživatelského rozhraní
- `sendmail` – přeposílání, `.forward` adresy pro přeposílání
- `pine`, `alpine`, `mutt`, ... – konzolové
- Mozilla Thunderbird, eM Client, Outlook, Windows Mail, The Bat!, SeaMonkey, ... – s GUI

*



*Pantherfly / CC BY-SA (`https://creativecommons.org/licenses/by-sa/4.0`)

Textové editory

- s GUI – `gedit`, `kedit`, `kate`, `mousepad`, `geany`, ...
- konzolové – `nano`, `vim`, `emacs`, ...

Vi(m):

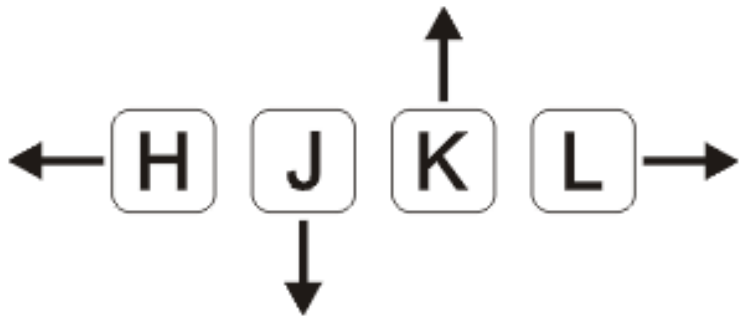
- rozšiřitelný, dostupný
- vysoce funkční, programovatelný
- GUI – `gVim`
- ed → ex → vi → vim
- mody: insert, normal, visual
- normal: *Esc*, insert: `i`, visual: `v`

*By User:D0ktorz (reworked in SVG) [GPL (http://www.gnu.org/licenses/gpl.html)], via Wikimedia Commons

Vim

- uzavření/otevření – `:w`, `:q`, `:e`
- vyhledávání – `/`, `?`, `n`, `N`
- pohyb kurzoru – `w/W`, `b/B`, `e/E`, `0/^/$`, `gg/G`, `}/{`, `:<číslo>`
- vkládání – `i/I`, `a/A`, `o/O`, `cc/ce/...`, `dd/de/...`
- označení (visual mode) – `v/V`, `y/yy`, `d/dd`, `p`
- undo/redo – `u`/*Ctrl* + *r*
- nahrazení – `:%s/text1/text2/g`

*



*Chase Lambert, online from `http://vimsheet.com/` (cit. 24.2.2018), under MIT licence