Petr Krčmář

Zapomeňte už na FTP a přenášejte soubory bezpečně

8. listopadu 2009

LinuxAlt, Brno

ROOT.CZ

O čem to bude?

- Proč říct „ne“ protokolu FTP
- Jak si FTP trochu vylepšit

ROOT.CZ

Co máš proti FTP?

- FTP je bohužel velmi oblíbené
  - U uživatelů a tím pádem i webhosterů
  - Ani porovnávací služby obvykle neřeší
- Poprvé v roce 1971 (RFC 114), aktuálně 959
  - Naprosto žádné zabezpečení
  - Jméno, heslo, příkazy i data jdou nešifrovaně
  - Stejně nebezpečné jako telnet
- Lze jednoduše odposlechnout a zneužít

Nepoužívejte FTP!

ROOT.CZ

Jak FTP vylepšit?

- Existují bezpečnostní rozšíření (RFC 2228)
- FTPS – balí klasické FTP do SSL (přidává TLS)
  - Stejné jako HTTPS
  - Neplést s SFTP!
  - Bohužel zůstávají nevýhody (třeba porty)
- FTP over SSH
  - Tunelování klasického FTP přes SSH
  - Neplést s SFTP! (to pořád ještě není ono)
  - Komplikované, SSH klient musí znát FTP (porty)

Tak znova a tentokrát lépe

- Protokol SCP
  - Nahrazuje zastaralé a nebezpečné rcp
  - Používá pro šifrování SSH na portu 22
  - Neřeší autentizaci a ověřování klíčů
- Na rozdíl od FTP umí přenášet i práva
- Řádkový klient je součástí OpenSSH (i jiných)
- Má řadu grafických klientů

Jak se SCP používá

- Úplně stejně jako cp
- Pro kopírování pryč:

```
$ scp data.txt pepa@server:texty/data.txt
```

- Pro kopírování k nám:

```
$ scp pepa@server:data/text.txt text.txt
```

- Zeptá se na heslo nebo lépe ověří klíče
  - Vysvětlíme si dále

SCP není ideální

- SCP se rychle rozšířilo
- Objevily se brzy jeho slabiny
- Je to stále jenom cp
- Chceme další operace se soubory, adresáři...
- Vznikl nový protokol SFTP jako reakce na SCP
  - Neplést s dříve zmíněným FTPS (jako HTTPS)
  - A neplést s FTP over SSH
  - Umí toho více, dnes se používá téměř výhradně

Co umí SFTP

- Přenášet soubory i s právy
- Navazovat spojení při přenosu souborů
- Vypisovat adresáře
- Mazat soubory
- Je navrženo multiplatformně
  - wildcards expanduje server dle svých zvyklostí
- SCP server obvykle na unixech, SFTP kdekoliv
- SFTP je komplexní vzdálený souborový systém

Co SFTP neřeší a co výkon

- SFTP opět neřeší bezpečnost
  - Nechává ji na SSH
- SFTP je obvykle pomalejší než SCP
  - SCP například nečeká na potvrzování paketů
  - Sype se plnou rychlostí na druhou stranu
  - SCP se ale proto nedá zastavit (není kontrola)
    - Musí se sejmout celé spojení
- U SFTP není problém zastavit konkrétní přenos

ROOT.CZ

Klienti pro SFTP

- scp2 – ačkoliv vypadá jako SCP, používá SFTP
- WinSCP – pro Windows
  - Překvapení: i WinSCP používá SFTP :-)
- gFTP (GTK klient)
- FileZilla (multiplatformní, velmi univerzální)
- FireFTP – rozšíření pro Firefox
- a halda dalších...

Jak to funguje ve zkratce

- Pomocí SSH klienta se otevře spojení
- Proběhne autorizace a autentizace obou stran
- Otevře se spojení
- Uvnitř spojení se otevře nové sezení
- V něm se požádá o SFTP server
- Obě strany spolu komunikují jak je třeba
- Zavře se sezení a případně celý tunel

Stůj! Heslo nebo klíč

- Heslo se dá odkoukat
- Mělo by být pro každý server jiné
- Je třeba ho zadávat pořád dokola
- Autorizace pomocí RSA je bezpečnější
- A taky rychlejší a pohodlnější
- Využívá jak terminál SSH, tak i SCP a SFTP
- Už není třeba zadávat heslo

Jak na RSA aneb rychlokurs

- Vygenerujeme si u sebe oba klíče:

```
$ ssh-keygen -t rsa -b 2048 -f ~/.ssh/muj_rsa_klic
```

- Klientovi oznámíme, že ho má použít
- Do souboru `~/.ssh/config` zapíšeme:

```
Host data.root.cz
        User petr
        IdentityFile ~/.ssh/muj_rsa_klic
```

… a na serveru

- Veřejný klíč má klient v `~/.ssh/muj_rsa_klic.pub`
- Obsah se musí přidat na server do

  `~/.ssh/authorized_keys`
- Například:

```
$ ssh petr@data.root.cz 'cat >> ~/.ssh/authorized_keys'
< ~/.ssh/muj_rsa_klic.pub
```

- Naposledy zadáme heslo a je to

ROOT.CZ

A jak to funguje

- Zero-knowledge proof
  - Důkaz bez předání znalosti
  - Klíče neputují mezi servery
- Server vygeneruje náhodný řetězec
- Zašifruje veřejným klíčem klienta a pošle
- Klient privátním klíčem dešifruje a vrátí
- Pokud se vrácený řetězec shoduje = OK
- Stejný veřejný klíč na více serverech

Proč to webhosteři nenabízejí?

- Bojí se dát lidem přístup na SSH terminál
  - Naprosto zbytečně
  - Je možno SSH omezit jen na SFTP!
- Alternativní shell scponly
  - Nedovolí jiné příkazy než pro přenos souborů
  - Omezí uživatele
- Nebo ještě lépe...

Zablokování jen na SFTP

- Nastavíme sftp-server jako standardní shell:

```
# usermod -s /usr/lib/sftp-server petr
```

- Povolíme ho mezi shelly
- Do `/etc/shells` přidáme řádek:

```
/usr/lib/sftp-server
```

- A je vyřízeno, uživatel může pouštět jen SFTP
- Nedostane se ke klasické konzoli

Otázky na závěr

- Kdo to...?
- Co to...?
- Je to pravda...?
- Proč je to...?
- A jak je to s...?
- Komu je...?
- S kým je to...?
- Proč proboha...?
- Kdo to má...?
- To už vážně tohle...?
- Na mou duši...?
- Žádná legrace...?
- A proč bych měl...?
- Nebo neměl...?

ROOT.CZ

Děkuji za pozornost

Petr Krčmář
www.root.cz, www.debian-linux.cz
petr.krcmar@iinfo.cz
GPG: 9FBEA4F5

ROOT.CZ