FTP-SSL

http://ftp-ssl.sf.net

Martin Dušek

Martin Fúsek

Josef Vlček

Zadání

- FTP server
- SSL
- OS Windows a Linux
- webová administrace
- implementace ACL na adresáře
- podpora pro virtuální adresáře a cesty

http://www.sourceforge.net

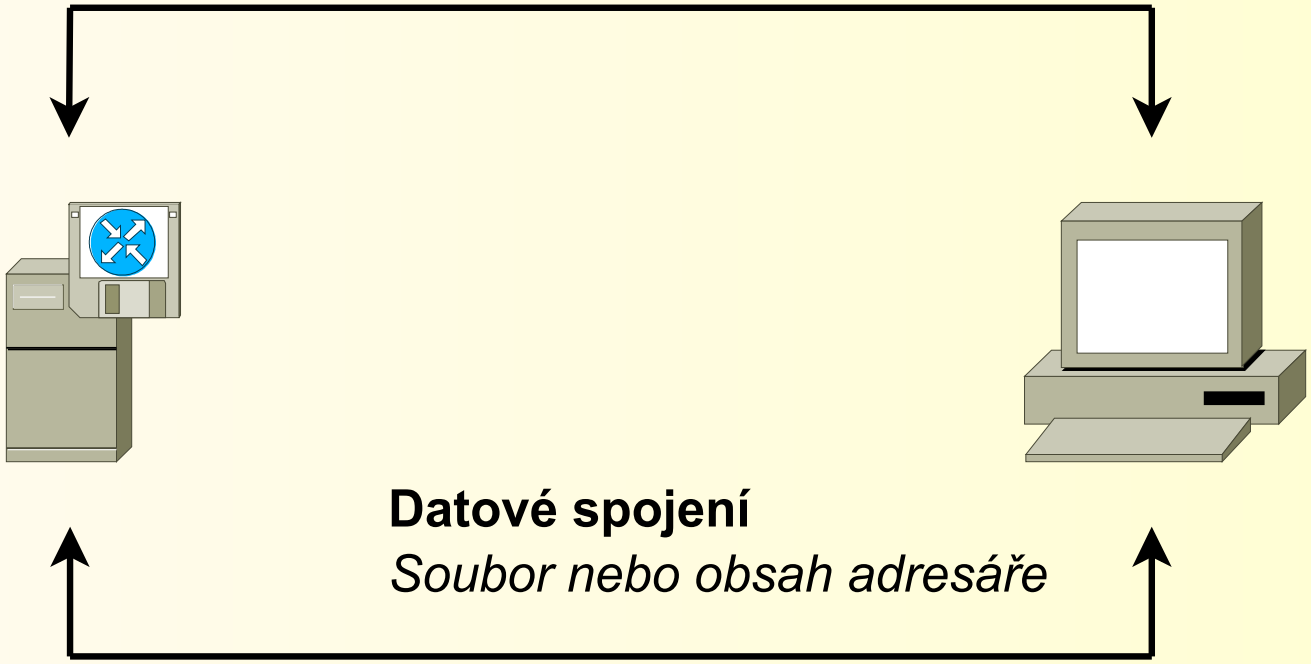
- registrace uživatele zdarma
- opensource projekty - registrace je “formalita”
- Subversion i CVS
- webové stránky projektu
- správa release verzí

FTP

- RFC 959 - File Transfer Protocol (FTP)
  - norma z roku 1975 (starý protokol!)
- RFC 2228 - FTP Security Extensions
- RFC 4217 - Securing FTP with TLS
  - SSL 3.0, TLS 1.0
  - explicitní FTPS – preferovaná metoda (port 21)
  - implicitní FTPS – jen šifrované spojení (port 990)

FTP komunikace

Řídící spojení
FTP příkazy (CWD, LIST, atd.)



Datové spojení
Soubor nebo obsah adresáře

FTP komunikace

- Server naslouchá na portu 21 (řídící spojení)
- Datové spojení nemusí existovat celou dobu:
  - STREAM
    - tok bajtů
    - zavření datového spojení znamená konec souboru
- Reprezentace dat:
  - ASCII
    - přenos textových souborů (např.: výpis adresáře)
  - IMAGE
    - binární data (přenosy souborů)

FTP komunikace

- Aktivní spojení
  - klient pošle příkaz PORT s adresou, kde naslouchá
  - server se připojí ke klientovi
- Pasivní spojení
  - klient pošle příkaz PASV
  - server odpoví adresou, kde naslouchá
  - klient se připojí k serveru
  - důvod: firewally

Architektura serveru

- vícevláknový server
- jedno vlákno čeká na příchozí spojení
- jedno vlákno čte standartní vstup (ukončení serveru)
- při přijetí spojení se vytvoří dvě nová vlákna:
  - řídící spojení
  - datové spojení - “čeká na příkazy z řídícího vlákna”
- ve vláknech použita blokující volání

ACL (Access control lists)

- Každý uživatel má svůj seznam
- implementace jen na adresáře
  - dědičnost
  - priority: pořadí
- práva:
  - R = read
  - W = write
  - L = list

Virtuální cesty

- Obdoba symbolických odkazů
- Výpis pomocí LIST podobný příkazu ls
- Práva se kontrolují jen pomocí ACL
- Problém: fyzické cesty na serveru
- ACL i virtuální cesty se spravují pomocí webového rozhraní

Webové rozhraní

- Používá soubor ftp.ini
  - globální nastavení serveru (ssl-certifikát, politika, ...)
  - uživatelé (login, heslo, home, acl, virtuální cesty, ...)
  - lze editovat i ručně

```
[USER4]
Enable = 1
Name = martin
Password = 925d7518fc597af0e43f5606f9a51512
Homedir = c:/web/martin/
access1 = c:/web/martin/>RL
virpath1 = d:/books/>c:/home/martin/>books
```

- OVERVIEW
- SERVER
- NEW USER
- Users
  - pepak
  - martin
  - maruska
  - fanda

User detail

Disable this account : ☐
Name : martin
Password : *******
Retype Password : *******
Home Directory: c:/web/martin/

Access control item 1

Access Priority : 1
Access control : c:/web/martin/
READ ☑
WRITE ☐
LIST ☑

ADD new Access control

Virtual path definition 1

Phisical Path : d:/books/
Mapped to : c:/home/martin/
Directory name : books

ADD new Virtual path

SAVE

Delete

Bezpečnost

- Šifrování datového a řídícího spojení
- Bezpečnostní politiky:
  - Žádná = šifrování SSL je volitelné, klient jej nemusí použít
  - ForceSSL = první příkaz klienta musí být AUTH TLS, jinak je klient odmítnut. Šifrované musí být i datové spojení (STOR, RETR, ...), jinak se příkaz neprovede

Použité knihovny

- Pthreads
  - POSIX threads – Linux i Windows
  - Pro Win32: http://sourceware.org/pthreads-win32/
- OpenSSL
  - http://www.openssl.org
  - nejpoužívanější knihovna
  - Podporuje SSL i TLS, lze využít s BSD sockety
  - špatná dokumentace (chybí tutoriály)

OpenSSL

- recv = SSL_read
- send = SSL_write
- handshake
  - spojeni se socketem: SSL_set_fd
  - vlastní handshake: SSL_accept
- Network buffer + SSL buffer
  - problémy s funkcí select
  - vypnutí serveru?

Závěr

- Pro skutečné nasazení serveru by bylo nutné:
  - více testovat funkčnost příkazů (různí ftp klienti)
  - více testovat bezpečnost a stabilitu
  - logy
  - přemapování fyzických cest
- bude někdo pokračovat ve vývoji?
  - http://ftp-ssl.sf.net