File Transfer Protocol

Ingo Blechschmidt
<iblech@web.de>

LUGA

25. Januar 2006

Inhalt

Geschichte

- Erste Definition in RFC 114 (April 1971)
- Hervorhebung des Unterschieds zwischen „direkter“ und „indirekter Nutzung“ durch den RFC:

  Direkte Nutzung: Einloggen via Telnet o. Ä.
  Indirekte Nutzung: Abstraktion durch ein Protokoll
- Probleme bei direkter Nutzung
  („wie listet man unter $OS nochmal Dateien auf?“)
- FTP als Möglichkeit indirekter Nutzung;
  große Vereinfachung
- Kontinuierliche Weiterentwicklung
  (u. a. RFC 959 (Oktober 1985))

Geschichte

- Erste Definition in RFC 114 (April 1971)
- Hervorhebung des Unterschieds zwischen „direkter“ und „indirekter Nutzung“ durch den RFC:

  Direkte Nutzung: Einloggen via Telnet o. Ä.
  Indirekte Nutzung: Abstraktion durch ein Protokoll
- Probleme bei direkter Nutzung
  („wie listet man unter $OS nochmal Dateien auf?“)
- FTP als Möglichkeit indirekter Nutzung;
  große Vereinfachung
- Kontinuierliche Weiterentwicklung
  (u. a. RFC 959 (Oktober 1985))

Aufbau

- ASCII-Basierung ($\rightarrow$ einfaches manuelles Testen; ähnlich wie bei POP3 oder NNTP)
- Multi-User-Fähigkeit
- Strukturierung der Dateien in Verzeichnisse
- Trennung in Kontroll- und Datenkanäle:

  Kontrollkanal: Default-TCP-Port 21; Kommandoaustausch
  Datenkanäle: dynamische Portaushandlung;
  nur Datenaustausch

Aufbau

- ASCII-Basierung ($\rightarrow$ einfaches manuelles Testen; ähnlich wie bei POP3 oder NNTP)
- Multi-User-Fähigkeit
- Strukturierung der Dateien in Verzeichnisse
- Trennung in Kontroll- und Datenkanäle:

  Kontrollkanal: Default-TCP-Port 21; Kommandoaustausch
  Datenkanäle: dynamische Portaushandlung;
  nur Datenaustausch

Typischer Ablauf

1. Einloggen
2. Holen des Dateilistings, Holen einer bestimmten Datei
3. Ausloggen

Einloggen

```
$ telnet FTP-Server 21
Trying a.b.c.d...
Connected to FTP-Server.
Escape character is '^]'.
220 Banner
USER Benutzername
331 Password required for Benutzername.
PASS Passwort
230-Willkommensnachricht
230-Willkommensnachricht
230-Willkommensnachricht
230-Willkommensnachricht
230 User logged in.
```

Live-Demo

Einloggen

```
$ telnet FTP-Server 21
Trying a.b.c.d...
Connected to FTP-Server.
Escape character is '^]'.
220 Banner
USER Benutzername
331 Password required for Benutzername.
PASS Passwort
230-Willkommensnachricht
230-Willkommensnachricht
230-Willkommensnachricht
230-Willkommensnachricht
230 User logged in.
```

Live-Demo

Einloggen

```
$ telnet FTP-Server 21
Trying a.b.c.d...
Connected to FTP-Server.
Escape character is '^]'.
220 Banner
USER Benutzername
331 Password required for Benutzername.
PASS Passwort
230-Willkommensnachricht
230-Willkommensnachricht
230-Willkommensnachricht
230-Willkommensnachricht
230 User logged in.
```

Live-Demo

Einloggen

```
$ telnet FTP-Server 21
Trying a.b.c.d...
Connected to FTP-Server.
Escape character is '^]'.
220 Banner
USER Benutzername
331 Password required for Benutzername.
PASS Passwort
230-Willkommensnachricht
230-Willkommensnachricht
230-Willkommensnachricht
230-Willkommensnachricht
230 User logged in.
```

Live-Demo

Dateilisting – passiv

```
PASV
227 Entering Passive Mode (a,b,c,d,x,y)
LIST
125 Data connection open; Transfer starting.
226 Transfer complete.
```

Übermittlung der Daten im *Datenkanal*

```
$ telnet a.b.c.d $((x*256 + y))
Trying a.b.c.d...
Connected to FTP-Server.
Escape character is '^]'.
drwxr-xr-x 1 Nutzer Gruppe 0 Nov 25 2002 bussys
drwxr-xr-x 1 Nutzer Gruppe 0 May 21 2001 deskapps
[...]
Connection closed by foreign host.
```

Live-Demo

Dateilisting – passiv

```
PASV
227 Entering Passive Mode (a,b,c,d,x,y)
LIST
125 Data connection open; Transfer starting.
226 Transfer complete.
```

Übermittlung der Daten im *Datenkanal*

```
$ telnet a.b.c.d $((x*256 + y))
Trying a.b.c.d...
Connected to FTP-Server.
Escape character is '^]'.
drwxr-xr-x 1 Nutzer Gruppe 0 Nov 25 2002 bussys
drwxr-xr-x 1 Nutzer Gruppe 0 May 21 2001 deskapps
[...]
Connection closed by foreign host.
```

Live-Demo

Dateilisting – passiv

```
PASV
227 Entering Passive Mode (a,b,c,d,x,y)
LIST
125 Data connection open; Transfer starting.
226 Transfer complete.
```

Übermittlung der Daten im *Datenkanal*

```
$ telnet a.b.c.d $((x*256 + y))
Trying a.b.c.d...
Connected to FTP-Server.
Escape character is '^]'.
drwxr-xr-x 1 Nutzer Gruppe 0 Nov 25 2002 bussys
drwxr-xr-x 1 Nutzer Gruppe 0 May 21 2001 deskapps
[...]
Connection closed by foreign host.
```

Live-Demo

Dateilisting – passiv

```
PASV
227 Entering Passive Mode (a,b,c,d,x,y)
LIST
125 Data connection open; Transfer starting.
226 Transfer complete.
```

Übermittlung der Daten im *Datenkanal*

```
$ telnet a.b.c.d $((x*256 + y))
Trying a.b.c.d...
Connected to FTP-Server.
Escape character is '^]'.
drwxr-xr-x 1 Nutzer Gruppe 0 Nov 25 2002 bussys
drwxr-xr-x 1 Nutzer Gruppe 0 May 21 2001 deskapps
[...]
Connection closed by foreign host.
```

Live-Demo

Übertragungsarten

Passive Übertragung

- `PASV`:
  Öffnung eines Ports auf dem FTP-Server durch den FTP-Daemon
- `LIST`, `RETR`, `STOR`:
  Übertragung der Daten in einer TCP-Verbindung *vom* Client *zum* mitgeteilten Port des Servers
- Durchlassen der Verbindung durch die Firewall des Servers (!)

Aktive Übertragung

- `PORT` *i*`,`*j*`,`*k*`,`*l*`,`*x*`,`*y*:
  Öffnung eines Ports auf dem Client durch den FTP-Client
- `LIST`, `RETR`, `STOR`:
  Übertragung der Daten in einer TCP-Verbindung *vom* Server *zum* mitgeteilten Port des Clients
- Durchlassen der Verbindung durch die Firewall des Clients (!)

Dateilisting – aktiv

```
PORT i,j,k,l,x,y
200 PORT command successful.
LIST
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
```

Übermittlung der Daten im *Datenkanal*

```
$ netcat -vlp $((x*256 + y))
Listening on [i.j.k.l] [Port] ...
connect to [i.j.k.l] from (UNKNOWN) [a.b.c.d] 20
drwxr-xr-x 1 Nutzer Gruppe 0 Nov 25 2002 bussys
drwxr-xr-x 1 Nutzer Gruppe 0 May 21 2001 deskapps
[...]
 sent 0, rcvd 809
```

Live-Demo

Dateilisting – aktiv

```
PORT i,j,k,l,x,y
200 PORT command successful.
LIST
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
```

Übermittlung der Daten im *Datenkanal*

```
$ netcat -vlp $((x*256 + y))
Listening on [i.j.k.l] [Port] ...
connect to [i.j.k.l] from (UNKNOWN) [a.b.c.d] 20
drwxr-xr-x 1 Nutzer Gruppe 0 Nov 25 2002 bussys
drwxr-xr-x 1 Nutzer Gruppe 0 May 21 2001 deskapps
[...]
 sent 0, rcvd 809
```

Live-Demo

Dateilisting – aktiv

```
PORT i,j,k,l,x,y
200 PORT command successful.
LIST
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
```

Übermittlung der Daten im *Datenkanal*

```
$ netcat -vlp $((x*256 + y))
Listening on [i.j.k.l] [Port] ...
connect to [i.j.k.l] from (UNKNOWN) [a.b.c.d] 20
drwxr-xr-x 1 Nutzer Gruppe 0 Nov 25 2002 bussys
drwxr-xr-x 1 Nutzer Gruppe 0 May 21 2001 deskapps
[...]
 sent 0, rcvd 809
```

Live-Demo

Dateilisting – aktiv

```
PORT i,j,k,l,x,y
200 PORT command successful.
LIST
150 Opening ASCII mode data connection for /bin/ls.
226 Transfer complete.
```

Übermittlung der Daten im *Datenkanal*

```
$ netcat -vlp $((x*256 + y))
Listening on [i.j.k.l] [Port] ...
connect to [i.j.k.l] from (UNKNOWN) [a.b.c.d] 20
drwxr-xr-x 1 Nutzer Gruppe 0 Nov 25 2002 bussys
drwxr-xr-x 1 Nutzer Gruppe 0 May 21 2001 deskapps
[...]
 sent 0, rcvd 809
```

Live-Demo

Übertragungsarten

Passive Übertragung

- `PASV`:
  Öffnung eines Ports auf dem FTP-Server durch den FTP-Daemon
- `LIST`, `RETR`, `STOR`:
  Übertragung der Daten in einer TCP-Verbindung *vom* Client *zum* mitgeteilten Port des Servers
- Durchlassen der Verbindung durch die Firewall des Servers (!)

Aktive Übertragung

- `PORT` *i*`,`*j*`,`*k*`,`*l*`,`*x*`,`*y*:
  Öffnung eines Ports auf dem Client durch den FTP-Client
- `LIST`, `RETR`, `STOR`:
  Übertragung der Daten in einer TCP-Verbindung *vom* Server *zum* mitgeteilten Port des Clients
- Durchlassen der Verbindung durch die Firewall des Clients (!)

Oft genutzte FTP-Befehle

`USER`, `PASS`	Authentifizierung
`QUIT`	Ausloggen
`DELE`	Löschen einer Datei
`RNFR`, `RNTO`	Umbennung (rename *from*, rename *to*)
`MKD`, `RMD`	Erzeugen, Löschen eines Verzeichnis
`CWD`	Verzeichniswechsel
`PORT`	Auswählen von aktivem FTP
`PASV`	Auswählen von passivem FTP
`LIST`	Verzeichnislisting
`RETR`	Herunterladen einer Datei
`STOR`	Hochladen einer Datei

Direkte Server-zu-Server-Übertragung

- Wunsch:
  Kopie einer Datei von FTP-Server *A* zum FTP-Server *B*
- Problem:
  Herunterladen von *A* auf den lokalen Rechner langsam
  Hochladen auf *B* vom lokalen Rechner aus langsam
- Abhilfe: Kombination von aktivem und passivem FTP
- Problem: Weigerung vieler Daemonen, beliebige Rechner zu kontakten

Vermittlung zwischen *A* und *B*

Zu *A*	Zu *B*
`PASV`	`PORT A,x,y`
`227 Entering Passive Mode (A,x,y)`	`200 PORT command successful.`

Direkte Server-zu-Server-Übertragung

- Wunsch:
  Kopie einer Datei von FTP-Server *A* zum FTP-Server *B*
- Problem:
  Herunterladen von *A* auf den lokalen Rechner langsam
  Hochladen auf *B* vom lokalen Rechner aus langsam
- Abhilfe: Kombination von aktivem und passivem FTP
- Problem: Weigerung vieler Daemonen, beliebige Rechner zu kontakten

Vermittlung zwischen *A* und *B*

Zu *A*	Zu *B*
PASV	*PORT A,x,y*
227 Entering Passive Mode (*A*,*x*,*y*)	200 PORT command successful.

Direkte Server-zu-Server-Übertragung

- Wunsch:
  Kopie einer Datei von FTP-Server *A* zum FTP-Server *B*
- Problem:
  Herunterladen von *A* auf den lokalen Rechner langsam
  Hochladen auf *B* vom lokalen Rechner aus langsam
- Abhilfe: Kombination von aktivem und passivem FTP
- Problem: Weigerung vieler Daemonen, beliebige Rechner zu kontakten

Vermittlung zwischen *A* und *B*

Zu *A*	Zu *B*
PASV	*PORT A,x,y*
227 Entering Passive Mode (*A*,*x*,*y*)	200 PORT command successful.

FTP als Einweg-Proxy – Spoofing mit FTP

- Wunsch: Anonymes Senden von beliebigen Daten M an $B:p$
  (wobei $p = 256\,x + y$ mit $x, y \in \{0, 1, 2, \ldots, 255\}$)
- Realisierung durch
  1. Deponieren von M als Datei `datei` auf liberalem FTP-Server A
  2. `PORT` B`,`x`,`y
  3. `RETR` *`datei`*
- Problem nur wieder: Weigerung vieler Daemonen, beliebige Rechner zu kontakten

FTP als Einweg-Proxy – Spoofing mit FTP

- Wunsch: Anonymes Senden von beliebigen Daten M an $B:p$
  (wobei $p = 256\,x + y$ mit $x, y \in \{0, 1, 2, \ldots, 255\}$)
- Realisierung durch
  1. Deponieren von M als Datei `datei` auf liberalem FTP-Server A
  2. `PORT` B`,`x`,`y
  3. `RETR` *`datei`*
- Problem nur wieder: Weigerung vieler Daemonen, beliebige Rechner zu kontakten

Benutzernamen/Passwörter

- Übertragung von Benutzernamen und Passwörtern im Klartext
- Übertragung der Nutzdaten im Klartext
- Daher erfolgreiches Sniffen problemlos möglich

Separater Datenkanal

- Dynamische Portaushandlung;
  je nach FTP-Typ Lücken in entweder der Server- (passives FTP) oder der Client-Firewall (aktives FTP) nötig
- FTP durch NAT-Router „schwierig“

Austricksen von Firewalls

1. Firewall belauscht FTP-Kontrollkanal nach `PASV`-Rückmeldungen
2. `aaaaaaaaa[...]aaa227 Entering Passive Mode (a,b,c,d,x,y)`
3. `500 Unknown command: aaaaaaaaa[...]aaa227 Entering Passive Mode (a,b,c,d,x,y)`
4. Wählen der Länge der as so, dass `227 Entering[...]` in ein eigenes TCP-Paket fällt (Fragmentierung!)
5. „Oh, der FTP-Daemon will gleich Daten ausliefern, schnell den Weg freimachen“

Lücken im FTP-Daemon

- FTP-Daemonen müssen/können/sollten können...
  - ...auf Port 21 lauschen
  - ...den aktuellen Nutzer wechseln („`su`“)
  - ...Logs führen
  - ...FTP-spezifische Quotas beachten
- Daher: Notwendigkeit des Laufens einiger Komponenten mit root-Rechten
- Bei Sicherheitslücke nicht nur Erhalt von Nutzer-Rechten, sondern root-Rechten!

Sicherer: Privilege Separation

- Start des Daemons als root
- Öffnen des Port-21-Sockets als root
- Abarbeiten von allgemeinen Kommandos (`USER`, `PASS`) als nobody
- Nach korrekter `USER`/`PASS`-Kombination weiteres Arbeiten als *nutzer*

Alternativen

- FTPS (FTP-SSL und FTP-TLS):
  Absicherung von FTP mit SSL (vgl. HTTPS)
- SFTP (Subsystem von SSH)
- SCP
- HTTPS, WebDAV
- Subversion