

# DATEIÜBERTRAGUNGS- PROTOKOLLE

KV Sicherheit in Applikationsprotokollen

Florian Ströbitzer



11

## Inhalt

|        |   |   |
|--------|---|---|
| 1.     | TFTP – Trivial File Transfer Protocol ..... | 2 |
| 1.1.   | Übertragungsmodi .....                      | 2 |
| 1.2.   | Das Protokoll .....                         | 3 |
| 2.     | FTP – File Transfer Protocol.....           | 4 |
| 2.1.   | Verbindungsarten.....                       | 4 |
| 2.1.1. | Aktives FTP.....                            | 4 |
| 2.1.2. | Passives FTP.....                           | 5 |
| 2.1.3. | FXP – File Exchange Protocol.....           | 5 |
| 2.2.   | Authentifizierung.....                      | 5 |
| 2.2.1. | Anonymous Login .....                       | 5 |
| 2.3.   | Bekannte Sicherheitsprobleme .....          | 6 |
| 2.4.   | Secure FTP .....                            | 6 |
| 3.     | BitTorrent .....                            | 7 |
| 3.1.   | Funktion.....                               | 7 |
| 4.     | NFS – Network File System.....              | 7 |
| 4.1.   | Sicherheit.....                             | 7 |
|        | Literaturverzeichnis.....                   | 8 |
|        | Abbildungsverzeichnis.....                  | 9 |

# 1. TFTP – Trivial File Transfer Protocol

TFTP ist eines der ersten Dateiübertragungsprotokolle und wurde 1980 entwickelt. Wie der Name sagt ist TFTP bewusst einfach entworfen, um es klein zu halten und einfach implementieren zu können. Basierend auf dem EFTP, dem Easy File Transfer Protocol, welches in den späten 70er bei XEROX Parc entwickelt wurde um den Xerox Alto, ein Rechner der in der Geschichte als einer der ersten PC's (Personal Computers) gilt (Xerox Alto - Wikipedia, the free encyclopedia), über Ethernet zu booten.

TFTP setzt auf UDP auf schließt aber die Verwendung anderer Transportprotokolle nicht aus. Mit TFTP ist es lediglich möglich Dateien (sowie E-Mails) zu lesen oder zu schreiben. Es gibt keinerlei Möglichkeiten Verzeichnisstrukturen aufzulisten oder zu manipulieren, wie dies der Fall bei FTP (siehe Kapitel 2) ist. Gegenwärtig besitzt TFTP auch keine Benutzerauthentifizierung.

## 1.1. Übertragungsmodi

TFTP unterscheidet drei Übertragungsmodi:

- Netascii: 8 Bit ASCII-Mode
- Octet: 8 Bit Raw Bite
- Mail: Kodierung wie bei Netascii, Empfänger ist Benutzer, nicht eine Datei (sollte nicht mehr implementiert werden)

## 1.2. Das Protokoll

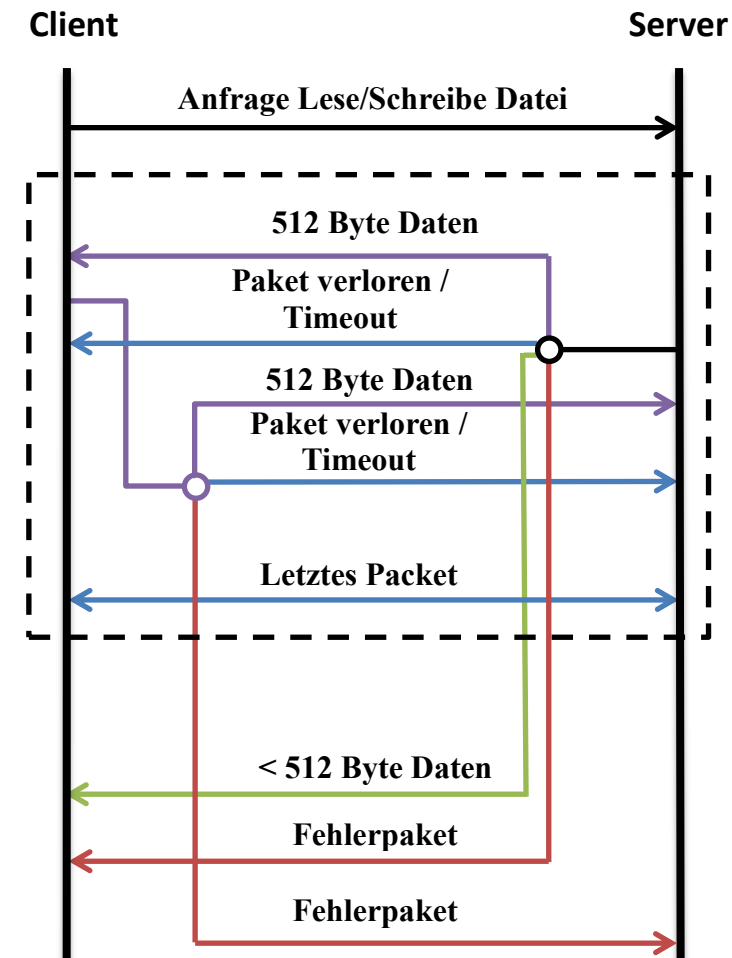


Abbildung 1 - TFTP

Jede Übertragung beginnt mit der Anfrage eine Datei zu lesen oder zu schreiben. Nimmt der Server die Verbindung an so wird eine Übertragung gestartet. Die Übertragung einer Datei erfolgt bei TFTP immer in 512 Byte großen Blöcken, sowohl das Lesen als auch das Schreiben. Der Server hat nun drei verschiedene Möglichkeiten zur Antwort:

- Ist die Antwort des Servers ein 512 Byte großes Datenpaket, wobei dieses Paket beim Schreiben einer Datei eine Bestätigung des ersten erhaltenen Datenpakets und eine fortlaufende Sequenznummer beinhaltet und beim Lesen einer Datei die ersten Daten dieser Datei beinhaltet, stellt dies den Normalfall dar und es kann der Client ebenfalls mit einem Datenpaket antworten.
- Ist die Antwort des Servers ein Datenpaket das kleiner ist als 512 Byte wird das Protokoll erfolgreich beendet und die Übertragung geschlossen.
- Der Server antwortet mit einem Fehlerpaket. Dies geschieht z.B.: beim Schreiben einer Datei sollte der Festplattenspeicher des Servers voll sein und führt unmittelbar zum Abbruch der Übertragung.

Es besteht weiters die Möglichkeit, dass das Datenpaket verloren geht, da das Übertragungsprotokoll UDP keinerlei Netzübertragungssicherheit gewährleistet. Sollte dieser

Fall eintreffen wartet der Gegenüber ein gewisse Zeitspanne ab und leitet dann eigene Schritte ein um dieses Paket zu erhalten. Er sendet das zuletzt gesendete Paket, dass dem Gegenüber anhand der beinhaltenden Sequenznummer signalisiert, dass sein Paket verloren gegangen ist und er es daraufhin erneut senden muss.

## 2. FTP – File Transfer Protocol

FTP ist wohl das bekannteste Übertragungsprotokoll für Dateien und wurde 1985 im RFC 959 spezifiziert. Es ermöglicht zusätzlich zum Datenaustausch auch das Auflisten von Verzeichnissen und Dateien und deren Änderung wie z.B.: löschen, umbenennen, etc. und benutzt das Transportprotokoll TCP.

Dazu wird eine separate Verbindung zwischen Client und Server hergestellt. FTP nutzt daher zwei Verbindungen:

- Verbindung für Datenübertragung (Port 20 oder zufälligen)
- Verbindung für Steuerung (Port 21)

Die angegebenen Ports sind serverseitig zu betrachten.

### 2.1. Verbindungsarten

#### 2.1.1. Aktives FTP

Bei der aktiven Verbindung öffnet der Client einen zufälligen Port, typischerweise jenseits von 1023, den sogenannten Well-Known-Ports. Daraufhin sendet der Client mit dem Kommando PORT seine eigene IP-Adresse und die Portnummer des geöffneten Ports an den Server auf den bekannten Port 21. Daraufhin können Client und Server zwischen dem zufälligen Port auf der Seite des Clients und den bekannten Port 20 auf Seite des Servers eine Datenübertragung aufbauen. Und zusätzlich ist es dem Client über Port 21 auf Seite des Servers möglich die Datenstruktur des Serververzeichnisses auszulesen und zu manipulieren und dies zeitgleich zur Datenübertragung.

### 2.1.2. Passives FTP

Bei der passiven Methode sendet der Client das Kommando PASV an den Server und fordert ihn auf einen zufälligen Port zu öffnen. Der Server teilt daraufhin dem Client seine IP-Adresse und den geöffneten Port mit. Der Client kann nun eine Datenübertragung aufbauen. Passiv FTP wird dann verwendet wenn der Client hinter einer Firewall sich befindet oder durch vorgeschaltetes Nating es keine Möglichkeit gibt eine einkommende TCP-Verbindung anzunehmen.

### 2.1.3. FXP – File Exchange Protocol

Das File Exchange Protocol bietet die Möglichkeit Dateien zwischen FTP-Server auszutauschen. Dabei ist es nicht nötig Datenübertragungen zwischen den Servern und dem Client aufzubauen und damit die Datenübertragung unnötig zu verlangsamen, sondern die Verbindung wird direkt zwischen den Servern erstellt und der Client steuert lediglich die Übertragung. Bei dieser Verbindungsart werden Aktiv und Passiv FTP verbunden.

Zu Beginn schickt der Client ein PASV Kommando an einen der Server und erhält dadurch einen zufälligen Port des Servers, welcher dieser geöffnet hat und auf einkommende Daten wartet. Daraufhin schickt der Client ein PORT Kommando an den anderen Server mit der IP-Adresse und dem geöffneten Port des ersten Servers. Damit besteht zwischen den zwei Servern eine Übertragungsverbindung und der Client kann nun über die beiden Steuerports der Server die Übertragung lenken.

## 2.2. Authentifizierung

Im Standard des FTP-Protokolls ist nur eine Authentifizierung mit Benutzername und Passwort vorgesehen. Diese Daten werden unverschlüsselt und im Klartext übertragen und sind ohne Probleme im Netzwerk mit zu lesen. Die Kommandos hierfür sind USER und PASS.

### 2.2.1. Anonymous Login

Einen Sonderfall stellt der sogenannte Anonymous Login dar. Bei dieser Variante ist es möglich sich mit dem Benutzer Anonymous und einem beliebigen Passwort einzuloggen. Früher wurde aus Höflichkeit als Passwort die eigene E-Mail Adresse angegeben. Da dies aber zu vermehrten Missbrauch durch Spamming führte wird dies heute nicht mehr praktiziert. Server die diese Loginmethode unterstützen werden als öffentliche Server bezeichnet.

## 2.3. Bekannte Sicherheitsprobleme

Da das FTP-Protokoll ein sehr altes Protokoll ist und zu Zeiten seiner Spezifizierung die Sicherheitsaspekte noch geringere Bedeutung besaßen sind mehrere Sicherheitsprobleme bekannt.

- FTP Bounce Attacken      Dabei wird das PORT-Kommando missbraucht um öffentliche FTP-Server zum Portscanning zu verwenden. Einem FTP-Server wird die IP-Adresse und der zu scannende Port übermittelt worauf dieser beginnt eine Verbindung mit dem Server auf zu bauen.
- Spoof Attacken      Im Kontext von Netzwerksicherheit ist eine Spoof Attacke wenn eine Person oder Programm es schafft sich als jemand anderer auszugeben und damit Zugriff auf geschützte Daten erhält.
- Brute Force Attacken      Bei Brute Force Attacken werden einfach alle potenziellen Möglichkeiten ausprobiert um damit an Benutzerzugriffsdaten zu gelangen.
- Packet Capture      Wie schon im Kapitel 2.2 erwähnt wird der Benutzername und das Passwort im Klartext übertragen und kann mit geeigneten Programmen im Netzwerk abgefangen werden.

## 2.4. Secure FTP

Um diese Sicherheitsmängel zu beheben wurden mehrere Methoden entwickelt und unter dem Begriff Secure FTP gesammelt.

- FTPS      Bei FTP über SSL wird die FTP-Verbindung selber verschlüsselt, ohne alle Daten über eine unterliegende SSH-Verbindung zu senden.
- SFTP      Oder auch SSH File Transfer Protocol genannt ist eine Datenübertragungsprotokoll von SSH und ist mit FTP nicht verwandt, besitzt aber einen ähnlichen Befehlssatz.
- FTP over SSH      Dabei wird eine normale FTP-Sitzung durch eine SSH-Verbindung getunnelt.

## 3. BitTorrent

Anders als bei herkömmlichen Dateiübertragungsprotokollen wird bei BitTorrent auch die Upload-Kapazitäten der Clients genutzt. Dateien werden also nicht nur von Servern verteilt sondern auch von Nutzer zu Nutzer (Peer-to-Peer, P2P). Dadurch teilt sich die Last auf mehrerer Rechner auf, was wiederum Einsparungen für die Betreiber von Servern heißt.

### 3.1. Funktion

Zuerst erstellt der sogenannte Initial-Seeder (Seeder sind Clients die bereits eine vollständige Kopier der Datei besitzen und nur mehr Uploaden) eine Torrent-Datei. Diese Datei besitzt lediglich beschreibenden Charakter und ist nur ein paar Kilobyte groß. In dieser befindet sich die IP-Adresse des Trackers sowie Dateiname, Größe und eine Liste von Prüfsummen von Segmenten der herunterzuladenden Daten.

Der Tracker wird benötigt um Kontakt zwischen interessierten Peers herzustellen. Er besitzt für jeden registrierten Torrent eine Liste von IP-Adressen von aktiven Peers die zur Zeit in einem sogenannten Schwarm mitwirken und die Datei verteilen.

## 4. NFS – Network File System

NFS ist ein von Sun Microsoft entwickeltes Protokoll um Benutzern oder darüber liegenden Systemen den Zugriff auf eine im Netzwerk befindliche Datei so zu ermöglichen als befinde sie sich lokal im Dateisystem.

Das Äquivalent in Windows-Umgebungen zu NFS heißt SMB (Server Message Block). Anders als bei SMB authentifiziert das populäre NFS V3 nicht den Benutzer sondern den Client-Rechner anhand seiner IP, erst NFS V4 ermöglicht die Benutzerauthentifizierung.

Ursprünglich wurde NFS mit UDP implementiert, mittlerweile sind aber auch andere Implementierungen wie TCP erhältlich.

### 4.1. Sicherheit

Ursprünglich war Sicherheit eine Sache der darunter liegenden RPC-Schicht (Remote Procedure Call). Um nun Sicherheit zu generieren wurde die RPC-Schicht durch Secure RPC ausgetauscht. Da aber Secure RPC keine weite Verbreitung erlangte und die Implementierung nicht immer möglich war wurde diese Variante nicht weiter vorangetrieben.

## Literaturverzeichnis

*BitTorrent* – *Wikipedia*. (10. 11 2011). Von Wikipedia – Die freie Enzyklopädie:  
<http://de.wikipedia.org/wiki/BitTorrent> abgerufen

*Network File System* – *Wikipedia*. (10. 11 2011). Von Wikipedia – Die freie Enzyklopädie:  
[http://de.wikipedia.org/wiki/Network\\_File\\_System](http://de.wikipedia.org/wiki/Network_File_System) abgerufen

*File Transfer Protocol* – *Wikipedia*. (kein Datum). Abgerufen am 10. 11 2011 von Wikipedia – Die freie Enzyklopädie: [http://de.wikipedia.org/wiki/File\\_Transfer\\_Protocol](http://de.wikipedia.org/wiki/File_Transfer_Protocol)

*File Transfer Protocol* - *Wikipedia, the free encyclopedia*. (kein Datum). Abgerufen am 10. 11 2011 von Wikipedia, the free encyclopedia: [http://en.wikipedia.org/wiki/File\\_Transfer\\_Protocol](http://en.wikipedia.org/wiki/File_Transfer_Protocol)

Sollins, K. (7 1992). *RFC 1350 - The TFTP Protocol (Revision 2) (RFC1350)*. Abgerufen am 10. 11 2011 von Internet FAQ Archives - Online Education - faqs.org:  
<http://www.faqs.org/rfcs/rfc1350.html>

*TFTP*. (kein Datum). Abgerufen am 10. 11 2011 von Universität Oldenburg:  
<http://einstein.informatik.uni-oldenburg.de/rechnernetze/tftp.htm>

*Xerox Alto* - *Wikipedia, the free encyclopedia*. (kein Datum). Abgerufen am 10. 11 2011 von Wikipedia, the free encyclopedia: [http://en.wikipedia.org/wiki/Xerox\\_Alto](http://en.wikipedia.org/wiki/Xerox_Alto)

## **Abbildungsverzeichnis**

|                         |   |
|-------------------------|---|
| Abbildung 1 - TFTP..... | 3 |
|-------------------------|---|