p2pdfs – peer-to-peer distributed filesystem (in userspace)

sECuRE beim NoName e.V.

6. Juni 2008

Motivation

- Verschlüsselung notwendig
- Authentifikation via bestehendem CA Cert-Web-of-trust
- Ausgleich für niedrigen Upstream bei 90% der Teilnehmer durch Caches
- Untrusted Caches bei \$billig-vserver-provider
- Tags für Dateien/Ordner (effektiv symlinks)
- Ohne Server sollen die Rechner trotzdem ein Netz bilden können
- Nicht „Yet another filesharing program“, sondern ein Filesystem in Anlehnung an NFS, CIFS oder AFS – nur besser (für uns)

Warum nicht einfach Bittorrent?

- Man müsste für jede Datei ein torrent-file erstellen, selbst bei Automation müsste man ein Programm laufen haben
- Man bräuchte einen privaten Tracker, der wiederum zentral laufen muss
- Verschlüsselung ist in den meisten Clients nur auf PREFERRED, nicht auf REQUIRED gestellt. Zudem sind die Implementationen teilweise inkompatibel.
- Man kann keine Files aus bittorrent mit mplayer öffnen (na gut, in p2pdfs momentan auch noch nicht)
- Prinzip der untrusted caches kann nicht erfüllt werden

Warum nicht einfach {N, CI, A}FS

- Ohne VPN bei NFS und CIFS schwer (sicher) einzuschränkender Benutzerkreis
- Keine Verteilung bei NFS/CIFS, wir haben weder Serverbandbreite en masse noch Storage um zentral zu lagern
- AFS für große Dateien ohne großen Cache unbrauchbar, außerdem ist das Prinzip der Lastverteilung durch Caches wie bei Bittorrent nicht möglich
- Prinzip der untrusted caches kann nicht erfüllt werden

Systemvoraussetzungen

- Nur auf Linux getestet momentan
- Mac OS X und andere BSDs haben kein %a in sscanf, daher noch nicht ganz lauffähig
- Bei NetBSD ist die FUSE-Implementation noch nicht in mainline
- Libraries: OpenSSL, eet, libuuid, libtransmission (mit Patches)

Was schon funktioniert

- Serverbetrieb. Die Dateibäume der einzelnen Clients sind auch dann verfügbar, wenn sie nicht verbunden sind.
- Austausch von Daten via Bittorrent
- Mehrere Downloads/Uploads gleichzeitig
- Verschlüsselung! AES- $\{128,192,256\}$ je nach Schlüssellänge des Netzes
- Caching der Dateibäume, damit man nicht bei jedem Start neue Hashes erstellen muss

Was noch nicht funktioniert

- Peer-only-Netze (ohne Server), da die Nachrichten momentan noch nicht eindeutig gekennzeichnet sind und somit – sobald mehrere Verbindungen auf einmal implementiert sind – potentiell im Kreis wandern würden. Milestone: 0.1-RELEASE
- Standard-libtransmission verwenden, da die Patches, die uns ein eigenes Peer-Management und **echte** trackerless torrents erlauben, noch nicht in Mainline sind
- Authentifikation via client certificate (z.B. CACert), da OpenSSL nicht ganz so einfach ist und momentan noch keine Zeit für die Implementation eines ordentlichen Prüfverfahrens der Zertifikate war. Milestone: 0.1-RELEASE
- Tags – ebenfalls aus Zeitmangel noch nicht implementiert
- Userspace-utilites zum Kopieren von Dateien (momentan „cat“), Anzeigen von Status, etc... Milestone: 0.1-RELEASE

Milestones

- 0.1-ALPHA: Erste einigermaßen stabile Testversion. Seit 21.05.2008 erreicht
- 0.1-BETA: Je nach Fehlerstatus von 0.1-ALPHA werden entweder möglichst viele Fehler behoben um sinnvolles Weitertesten zu ermöglichen, oder es werden vordergründig Features für 0.1-RELEASE implementiert, die dann getestet werden
- 0.1-RELEASE: Alle geplanten wichtigen Features sind implementiert und möglichst auch getestet

Und nun?

- Fragen?
- Testen! bitte
- <https://p2pdfs.zekjur.net/>
- SVN auf <https://p2pdfs.zekjur.net/svn>
- TRAC auf <https://p2pdfs.zekjur.net/trac>, Account gibt's bei mir
- Mailingliste p2pdfs-announce für neue Versionen