

# The Freenet Project

Anonymes Netzwerk basierend auf dem Kleine-Welt-Phänomen

Bahtiar 'kalkin' Gadimov

FrOSCon 2009

23. August 2009



The Freenet Project  
<http://freenetproject.org/>



featured by [colonne\\_idle](#)

# Was ist Freenet?

Freenet ist ein Netzwerk bzw. Datenspeicher, das Zensurresistenz und Informationsfreiheit, durch Anonymität und Dezentralisierung versucht zu erreichen.

# The Freenet Project

Anonymes Netzwerk basierend auf dem Kleine-Welt-Phänomen

Bahtiar 'kalkin' Gadimov

FrOSCon 2009

23. August 2009

# Übersicht

- 1 Motivation
- 2 Überblick über die Entstehung
- 3 Funktionsweise
  - Routing
  - Keys
  - Key Targets
  - Sicherheit
- 4 Anwendungen

# Wer bin ich?

- Java- und Phpentwickler
- Student an der RWTH-Aachen

# Wer bin ich nicht?

- Kein Freenet Developer
- AFAIK kein Terrorist

# Warum benutze ich Freenet?

- Hartes Durchgreifen der politischen Systeme im Internet
- Weil Freenet ein zensurresistentes Medium ist

# Entstehung

- 1999 Ian Clarke schreibt “Distributed Decentralised Information Storage and Retrieval System”
- Aufruf zur Umsetzung der Idee als Software
- 2000 meistzitierte Paper im Fach Computer Science
- März 2000 freenet 0.1

# The Freenet Project Inc

- Gründung als gemeinnützige Organisation
- 2002 Mathew 'toad' Toseland bezahlter Hauptentwickler
- Freenet China Projekt bis 2003

## Freenet 0.7

- 2005 auf der ML das Darknet-Konzept diskutiert
- Ende 2005 Vorstellung dieses Konzept auf der 13. DefCon und dem 22C3
- April 2006 Erste Alpha von Freenet 0.7 erreicht
- Am 8 May 2008 ist 0.7 stable released worden
- Am 12 Juni 2009 kamm die stabile Version 0.7.5 raus

# Freenet vor 0.7

- Verwendete das Opennet Konzept
- Sehr verwundbar für Harvesting
- Freenet Pakete waren erkennbar
- Folge: Chinas Firewall blockierte Freenet

# Was ist ein Darknet?

## Definition

Ein Darknet ist ein privates Peer-to-Peer-Netz, in dem sich die Nutzer nur mit den Menschen verbinden, denen sie vertrauen.

Auf P2P bezogen:

- Ein P2P Netz das nur per Einladung (Key austausch) benutzt werden kann
- Teilnehmer sind vertrauenswürdig
- Darknets sind im Regelfall sehr klein

# Kleine-Welt-Phänomen

## Hypothese

Jeder Mensch (sozialer Akteur) auf der Welt ist mit jedem anderen über eine sehr kurze Kette von Bekanntschaftsbeziehungen verbunden.

# Milgrams Experiment

- Durchgeführt vom Soziologen Stanley Milgram an der Harvard University
- Durchschnittliche Pfadlänge ist 6

# Milgrams Experiment

- Durchgeführt vom Soziologen Stanley Milgram an der Harvard University
- Durchschnittliche Pfadlänge ist **6**

# Das Konzept übertragen auf Freenet

- Ich verbinde mich mit jedem Teilnehmer über Freunde
- Harvesting nicht mehr möglich
- Mit den ausgetauschten Schlüsseln (References) wird die Verbindung vom ersten Paket an verschlüsselt

# Problematik

- Wem von seinen Freunde gibt man das Paket?
- Im Real Life betrachtet man:
  - Geographischer Standpunkt
  - Hobbys/Beruf
- Im Freenet:
  - Die gesuchte Person ist unbekannt
  - Man sucht ein File welches die Person hat

# Problematik

- Wem von seinen Freunde gibt man das Paket?
- Im Real Life betrachtet man:
  - Geographischer Standpunkt
  - Hobbys/Beruf
- Im Freenet:
  - Die gesuchte Person ist unbekannt
  - Man sucht ein File welches die Person hat

# Problematik

- Wem von seinen Freunde gibt man das Paket?
- Im Real Life betrachtet man:
  - Geographischer Standpunkt
  - Hobbys/Beruf
- Im Freenet:
  - Die gesuchte Person ist unbekannt
  - Man sucht ein File welches die Person hat

# Die Lösung

- Jeder Peer hat ein Datastore
- Jedes File hat ein entsprechendes Hash-Key
- Jeder Peer spezialisiert sich auf bestimmte Keys

# Routing Beispiel

- Alice sucht den Key BAR
- Spezialisierung der verbundenen Freunde/Peers:
  - Bobs Spezialisierung: FOO
  - Dave Spezialisierung: QUX
  - Carols Spezialisierung: BAZ
    - Gefunden? File wird an Alice geschickt
    - Nein? Anfrage gemerkt und an Freund der eine ähnliche Spez wie BAR hat weitergeschickt

# Routing Details

- Jeder Request hat eine HTL(Hops-To-Live) max 18
- Request wird nicht weitergeschickt wenn  $htl == 0$
- Wenn  $htl == maxhtl$ , dann ist Dekrementierungswahrscheinlichkeit 50%, ansonsten 100

# Keys

- CHK — Content Hash Key
- SSK — Signed Subspace Key
- USK — Updateable Subspace Key
- KSK — Keyword Signed Key

# Content Hash Key

- Beschreiben statischen Content. z.B. \*.ogg, \*.png...
- Ist ein File größer als 32kB wird es aufgespalten
- Falls File aufgespalten zeigt der Key auf Masterfile
- Masterfile enthält CHK's der Splitter

Aufbau:

CHK@FileHash,DecryptKey,CryptoEinstellungen

Beispiel:

CHK@SVbD9HM5nzf3AX4yFCBc-A4dhNUF5DPJZLL5NX5Brs,bA7qLNJR7IXRKn6uS5PaySjIM6azPFvK18kSi6bbnQ,AAEA-8

# Signed Subspace Key

- Werden für Content benutzt der sich veraendert z.B. Websites
- Basieren auf dem Public-Private Key Verfahren
- Routing Key besteht aus  $H(H(\text{PublicKey})+(\text{Name-Version}))$

Aufbau:

`SSK@PublicKeyHash,DecryptKey,CryptoEinstellungen,Name-Version`

# Erstellen eines SSK

- Man generiert ein Publik und Private Key
- Erstellt einen Symmetrischen Schlüssel
- Wählt einen Namen für den Ordner z.B. mysite-5
- Verschlüsselt die Files, signiert mit dem Public Key
- Hängt den Public Key dran

# SSK Krypto Details

- Public-Private-Key basiert auf 2048-bit DSA
- Simetrische Verschlüsselung basiert auf 256-bit Rijndael aka AES-256

# Updateable Subspace Key

- Ein Wrapper um SSK
- Es werden “/” benutzt
- Versionsnummern können negativ sein

Aufbau:

`USK@PublicKeyHash,DecryptKey,CryptoEinstellungen/Name/[-]Version`

# USK Typ 1

## Beispiel

USK@rd0SN1...ABAAE/mysite/5/

- Eine lokale Liste enthält alle besuchten USK's mit Versionsnummer
- Es wird die aktuellste USK, aber mindestens die Version 5 ausgeliefert
- Im Hintergrund wird die Liste aktualisiert

# USK Typ 1

## Beispiel

USK@rd0SN1...ABAAE/mysite/5/

- Eine lokale Liste enthält alle besuchten USK's mit Versionsnummer
- Es wird die aktuellste USK, aber mindestens die Version 5 ausgeliefert
- Im Hintergrund wird die Liste aktualisiert

# USK Type 2

## Beispiel

USK@rd0SN1...ABAAE/mysite/-5/

- Lokale Liste wird nicht konsultiert.
- Die Versionen 5 plus 4 weitere (6,7,8,9) werden gesucht
- Die Suche stoppt wenn 4 Versionsnummern nicht gefunden werden.

# USK Type 2

## Beispiel

USK@rd0SN1...ABAAE/mysite/-5/

- Lokale Liste wird nicht konsultiert.
- Die Versionen 5 plus 4 weitere (6,7,8,9) werden gesucht
- Die Suche stoppt wenn 4 Versionsnummern nicht gefunden werden.

# Keyword Signed Key

- So siehts aus: **KSK@foobar.txt**
- Aus foobar.txt wird Public, Private Key und symetrischer Schlüssel generiert
- Leicht zu merken
- Können auf CHK's weiterleiten
- Spoofbar

# Key Targets

- File
- Splitfile
- Simple Manifest
- Container

# Splitfile

- Splitfile enthält Keys für Splitter (1024B bei SSK, 32kB bei CHK)
- 2/3 der Splitter sind “data blocks”
- 1/3 “check blocks” – wird für Splitfile Healing verwendet

# Simple Manifest

- Eine Liste von Keys und Meta-Daten der Files
- Im Grunde ein Directory Listing
- Wird für freesites verwendet

# Container

- Freesite oder Sammlung von Files als ein ZIP Paket
- Inkludierte Files sind kleiner als 64KB
- Maximal 2MB gross
- Jeder der Files im Container ist durch den selben Key auffindbar

## Beispiel

```
CHK@NOSdw7FF88S...bNg7YsgM,AAEC-8/file1.txt  
CHK@NOSdw7FF88S...bNg7YsgM,AAEC-8/file2.jpg
```

# Sicherheit

- Alle Pakete sind verschlüsselt und sehen zufällig aus

# Anwendungen

# Browser!

- FProxy — HTTP Proxy
- localhost:8888
- Beispiel: `http://localhost:8888/KKS@foobar.txt`

# Freenet Console

- Ein Telnet Interface
- Erlaubt alles zu machen was mit FProxy moeglich ist

# Frost

- Wurde mit Freenet ausgeliefert
- Newsgruppen, Download- und Uploadmanager
- Newsgruppen basieren auf Public-Private-Key Verfahren
- Eine Art Web Of Trust (GOOD, CHECK, BAD, OBSERVE)
- Leidet stark unter Spam — deswegen tot.

# FMS

- Alternative zu Frost
- Lokaler Newserver
- Ein sehr ausgeklügeltes Trust System
- In C geschrieben.
- Benutzbar mit Webgui oder Newsclient

# Freemail

- lokaler IMAP/SMTP Server
- basiert wieder auf Public–Private–Key Verfahren
- Man braucht nicht dauernd Online zu sein
- Beispiel Mail: foobar@DS3FG3R...SF6FHJ8YUK.freemail

# Was fehlt

- Real Time Chat

# Wie kann ich helfen?

- Betreiben eines Nodes
- Als Developer/Tester/Übersetzer
- Spenden!

# Ende

- Noch Fragen?
- Folien unter <http://files.blase16.de/files/>
- Lizenz: Creative Commons Namensnennung



# Ende

- Noch Fragen?
- Folien unter <http://files.blase16.de/files/>
- Lizenz: Creative Commons Namensnennung

