The Freenet Project

Anonymes Netzwerk basierend auf dem Kleine-Welt-Phänomen

Kalkin Sam

Easterhegg 2008

21. März 2008

featured by `cologne.idle`

Was ist Freenet?

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

Übersicht

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
- Ende März 2008 soll 0.7 stable released werden (hoffentlich)

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

Allgemein kann ein Darknet eine beliebige geschlossene Gruppe von kommunizierenden Leuten sein.
Quelle: http://de.wikipedia.org/wiki/Darknet

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.

- Experimentell nachgewiesen
- Durchschnittliche Pfadlänge ist **6**

Das Konzept übertragen auf Freenet

- Ich verbinde mich mit jedem Teilnehmer über Freunde
- Harvesting nicht mehr möglich
- Mit den ausgetauschten Schluessel 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 verbunden 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

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 1kB 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

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

- Problem: Man weiß nicht ob es die aktuellste Version ist

Updateable Subspace Key

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

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

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

Browser!

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

Frost

- Wird 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

FMS

- Alternative zu Frost
- Lokaler Newserver
- Ein ausgeklügertes Trust System
- In C geschrieben.
- “Unbedienbar”

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
- Wiki (In Entwicklung)
- FMS in Java

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