e-privacy: **riservatezza e diritti individuali in rete**

difendersi dal Grande Fratello nel terzo millennio

Firenze - 27 Aprile 2002

Freenet: un cammino di libertà

Marco A. Calamari - **marcoc@firenze.linux.it**

The Freenet Project

Firenze Linux User Group

Di cosa parleremo ?

- Cosa è Freenet ?
- Meccanismi crittografici
- Come funziona Freenet
- Client ed applicazioni
- Prospettive future
- Bibliografia

Cosa è Freenet ?

Cosa è Freenet

“Freenet è una rete adattativa di nodi peer-to-peer che si interrogano reciprocamente per immagazzinare e recuperare file di dati identificati da nomi (chiavi) indipendenti dalla locazione.”

Freenet è formata da server (nodi) paritetici; i nodi normalmente includono un proxy che permette di accedere al server con un form, utilizzando il protocollo HTTP.

“Freenet :
A Distribuited Anonymous Information Storage and Retrieval System”
I.Clarke et al.

… e tradotto in italiano ?

“Freenet è un sistema per scrivere e leggere file da Internet senza che si possa risalire a chi li ha scritti, chi li conserva sul disco e chi li recupera.”

Questo scopo viene raggiunto utilizzando il client (nodo) Freenet, che spezzetta, crittografa, duplica, disperde i contenuti del file, e riesce ad eseguire l’operazione inversa per recuperarli.

Freenet non permette di cancellare niente e non conserva informazioni su dove un file si trova.

Modelli Peer-to-peer

- Modello centralizzato
  - Esempio : Napster
  - indice mantenuto da un autorità centrale - conoscenza globale dei dati (single point of failure)
  - contatto diretto tra richiedente e fornitore
- Modello decentralizzato
  - Esempio : Freenet, Gnutella
  - nessun indice globale – conoscenza locale dei dati (approximate answers)
  - contatti mantenuti da una “catena” di intermediari

Obbiettivi da raggiungere

- Anonimato sia per il produttore che per il fruitore dell’informazione
- Il sistema non deve avere elementi di controllo centralizzati o di amministrazione
- Il sistema deve essere robusto rispetto ai problemi hardware/software
- Il sistema deve “adattarsi” e mutare nel tempo
- Le performance devono essere paragonabili ad altri sistemi (web)

Caratteristiche dell'attuale implementazione

- Versione 0.3.9.2
- Realizzata in linguaggio java - portabile su differenti architetture
- Sono disponibili protocolli e librerie per un'agevole implementazione di programmi client che usino Freenet come meccanismo di trasporto.
- Anonimità del contenuto del datastore di un nodo - non è possibile cercare una categoria di contenuti, ma solo identificare un certo file

Caratteristiche dell'attuale implementazione

- Adattività della rete - il grafo delle connessioni logiche tra i nodi evolve nel tempo verso una stabilità ed efficienza maggiore.
- Non responsabilizzazione del gestore del nodo - il sistema non è completamente deterministico, e non consente di provare che un certo file presente nel datastore proviene dal nodo locale e non da un altro nodo della rete

Caratteristiche dell'attuale implementazione

- Resilienza della rete - l'informazione non puo' essere rimossa da Freenet ma solo lasciata "morire" di morte naturale.
- Comportamento "ecologico" della rete - l'informazione che viene richiesta si moltiplica su più nodi e si "avvicina" ai nodi che la richiedono

Caratteristiche dell'attuale implementazione

- Anonimità sia di chi memorizza informazioni che di chi le recupera - nel caso si prevedano attacchi con memorizzazione del traffico sono necessarie cautele aggiuntive (tunnel SSL).
- Mancanza della possibilità di indicizzare le chiavi in modo da operare una ricerca intelligente. Il problema non è risolto a livello di protocolli, e soluzioni parziali sono demandate a programmi applicativi

Caratteristiche della versione 0.4/0.5

- Meccanismo di split files con ridondanza
- Autenticazione crittografica tra nodi
- Chiavi ARK (Addres Resolution Key)
  SSK@<node key>/<node address> - the content is the new node address.
- Routing migliorato
- Datastore indipendente dal filesystem
- Modifiche ai protocolli incompatibili con la 0.3.x.x

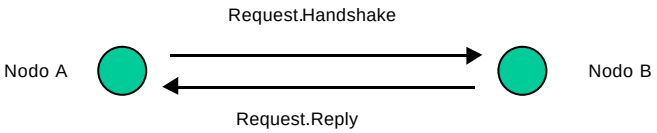
Come funziona Freenet

Come funziona Freenet

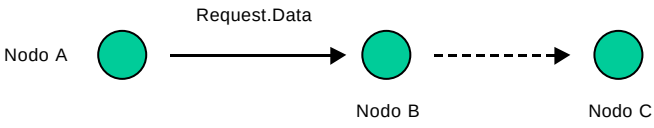
- I nodi comunicano tra loro con un semplice protocollo connection-oriented chiamato FNP (Freenet Network Protocol)
- I client applicativi che vogliono utilizzare i servizi Freenet di un nodo locale utilizzano un altro protocollo chiamato FCP (Freenet Client Protocol)

Come funziona Freenet

Fase di Handshake



Fase di richiesta dati

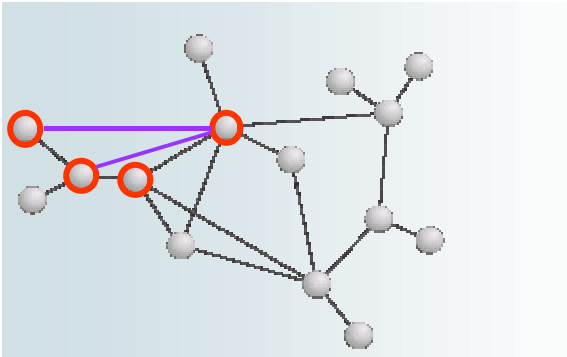


Come funziona Freenet

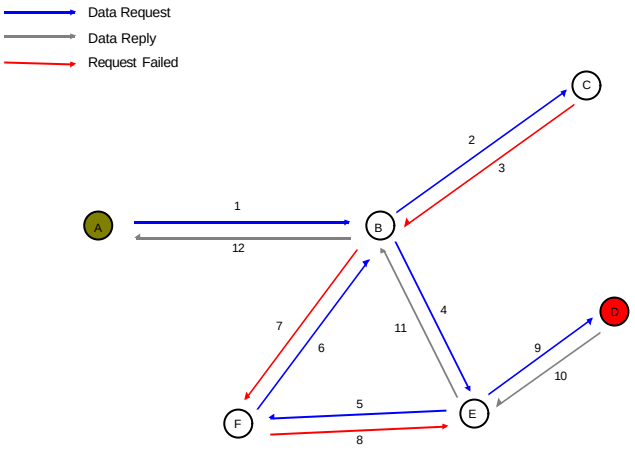
- Il nodo che effettua il boot deve conoscere almeno un nodo già in rete tramite un metodo out-of-band.
- Il problema del boot di un nodo (conoscenza di un altro nodo affidabile a cui connettersi) non è risolto. Attualmente si utilizza una pagina web del Progetto Freenet o si fornisce un nodo manualmente
- I nodi “scoprono” altri nodi durante il funzionamento.

Come funziona Freenet

- I nodi comunicano tra loro sulla base di una conoscenza locale dinamica dei nodi limitrofi
- Ogni nodo richiede una chiave, nell’ordine, ai nodi limitrofi



Come funziona Freenet



Come funziona Freenet

- Un nodo che riceve da un confinante la richiesta di una chiave che ha precedentemente cercato e non trovato la rigetta immediatamente.
- Un nodo che deve inserire una chiave, prima la ricerca per evitare una collisione, e successivamente la inserisce
- La “profondità” della ricerca o dell’inserimento di una chiave è data dall’HTL (hops to live)
- Ogni nodo che deve passare una richiesta decrementa l’HTL di 1

Come funziona Freenet

- **Un “rumore di fondo probabilistico” viene inserito in tutte le decisioni di routing (variazione dell’HTL, possesso della chiave, etc.) per impedire che un eventuale registrazione del traffico possa far risalire al nodo che ha effettuato la richiesta o l’inserimento originali e permettere all’operatore del nodo la ripudiabilità di un’eventuale attribuzione.**

Come funziona Freenet

- Ogni nodo memorizza le chiavi “alla rinfusa” in un database che viene denominato “datastore
- Una chiave esiste in più copie, dipendenti dalla profondità di inserimento della richiesta originale
- Ogni nodo che, dopo aver trasmesso una richiesta che ha avuto successo riceve la chiave da ripassare al nodo richiedente se ne fa una copia in locale

Come funziona Freenet

- I singoli datastore vengono gestiti con un watermark, sulla base della data e del numero degli accessi alle singole chiavi
- Le chiavi “popolari” si moltiplicano e si spostano “vicino” a chi le richiede
- Le chiavi “impopolari” scompaiono
- Si tratta di un comportamento “ecologico” che permette di realizzare un sistema in cui non esiste il comando “delete”

Come funziona Freenet

- I singoli nodi si “specializzano” nel memorizzare alcune chiavi, basandosi su una “distanza lessicale” che viane calcolata utilizzando un hash del contenuto della chiave, e specializzandosi in un segmento di essa
- Le decisioni di routing delle richieste vengono fatte in maniera intelligente, poiché i server pubblicizzano il segmento di spazio delle chiavi in cui sono “specializzati”

Meccanismi crittografici

Le chiavi di Freenet

- I file in Freenet sono associati e memorizzati utilizzando oggetti detti "chiavi" :

  CHK (content hash key)

  KSK (keyword signed key)

  SSK (signed subspace key)

  MSK (map space key)

- Nota : la funzione hash utilizzata è lo SHA-1 a 160 bit mentre l'algoritmo asimmetrico di cifratura è il DSA

La chiave CHK

- è il “cavallo da tiro di Freenet
- è derivata dall’hash del contenuto del file corrispondente. Tutti i file sono chiavi CHK
- file che hanno la stessa chiave sono uguali; file anche solo leggermente diversi hanno chiavi diverse
- il nome della chiave è ben poco mnemonico

La chiave CHK

- Il file viene inoltre criptato utilizzando una chiave generata in modalità random
- Vengono pubblicati sia l’hash che la chiave di decrittazione
  - Esempio inserisci in Freenet foto.gif
  - hash(foto.gif) = zdfaGTjIYUTiuyIUTiugu
  - chiave di crittazione rgenerata a caso = fpR12gfadghgfhf
  - Una volta inserito, il dato potrà essere richiesto fornendo la seguente stringa :

    CHK@ zdfaGTjIYUTiuyIUTiugu , fpR12gfadghgfhf

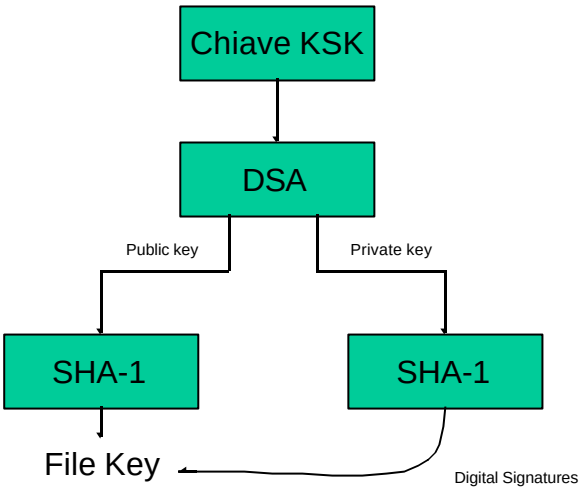
La chiave KSK

- è la chiave più semplice e user-friendly
  - Esempio -> freenet:KSK@foto_di_marco
  - La stringa descrittiva (foto_di_marco) viene utilizzata per generare una coppia di chiavi pubblica/privata (algoritmo DSA)
  - La chiave pubblica viene utilizzata per produrre l'hash associato al file inserito (SHA-1)
  - La chiave privata viene utilizzata per "firmare" il file inserito.

La chiave KSK

- con il contenuto del file foto_di_marco viene prodotta una chiave CHK
- il nome della chiave CHK viene inserito come contenuto della chiave KSK@ foto_di_marco
- le due chiavi vengono separatamente inserite in Freenet
- per recuperare il file, si richiede la chiave KSK@ foto_di_marco, si estrae da essa il nome della chiave CHK@zdfaGTjIYUTiuyIUTiugu,fpR12gfadghgfhf, si recupera quest'ultima, si estrae da essa il contenuto e lo si decritta.

La chiave KSK



E' affidabile la chiave KSK ?

- I file in Freenet sono associati solo a chiavi CHK.
- La chiave KSK e' solo un segnalibro che permette di recuperare piu' facilmente il contenuto di una chiave CHK
- Aspettando che una chiave KSK svanisca, si puo' reinserirla, faccendola puntare ad una chiave CHK diversa
- Un esempio clamoroso è stato quando un burlone ha modificato la chiave KSK di test di freenet, gpl.txt, sostituendola in modo che puntasse al contenuto della licenza BSD

La chiave SSK

- Costruzione di un “namespace” personale
  - Creiamo una coppia di chiavi pubblica/privata di tipo SSK
  - Utilizzeremo la chiave privata per inserire documenti “sotto” il nostro namespace
  - Pubblicheremo la nostra chiave pubblica per rendere accessibili i file pubblicati
  - Esempio -> SSK@public_key/musica/song1.mp3 SSK@public_key/musica/song2.mp3

La chiave MSK

- Risolve il problema di aggiornare contenuti che non possono essere cancellati (freesite)
- Viene utilizzata come home page di un freesite
- Può essere acceduta direttamente ...
  - freenet:MSK@SSK@11…11/nomesito//
- … od indirettamente, e Freenet seleziona quella che si riferisce alla data corrente
  - freenet:MSK@SSK@11…11/yyyyyymmddhhmmss-nomesito//

La chiave MSK

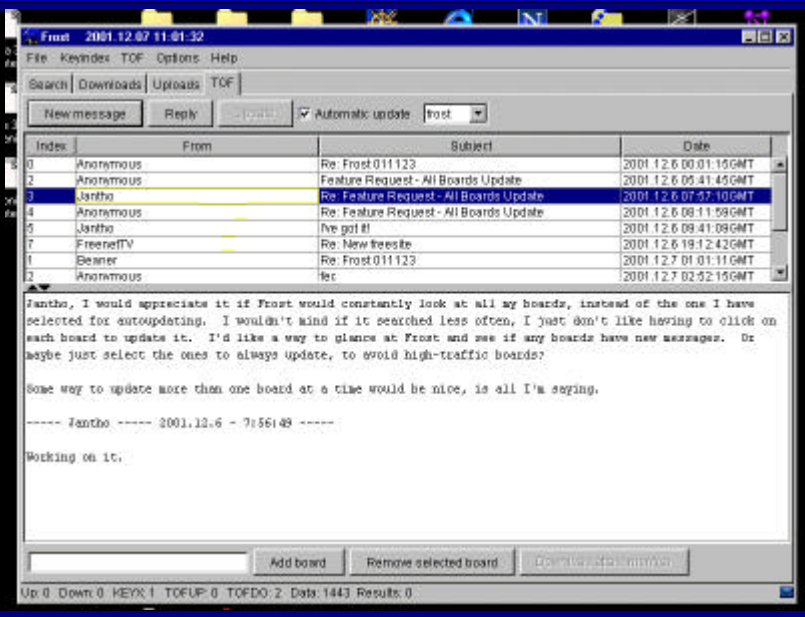
- Le chiavi MSK vengono inserite in batch prima della data a cui si riferiscono
- Il meccanismo cosi creato si chiama DBR - date base redirect (date, non data !)
- Le chiavi MSK ormai vecchie e che non vengono più richieste “muoiono” di morte naturale
- La chiave MSK di un freesite contiene gli “indirizzi” delle chiavi CHK a cui i link di tutto il freesite si riferiscono

Client ed applicazioni

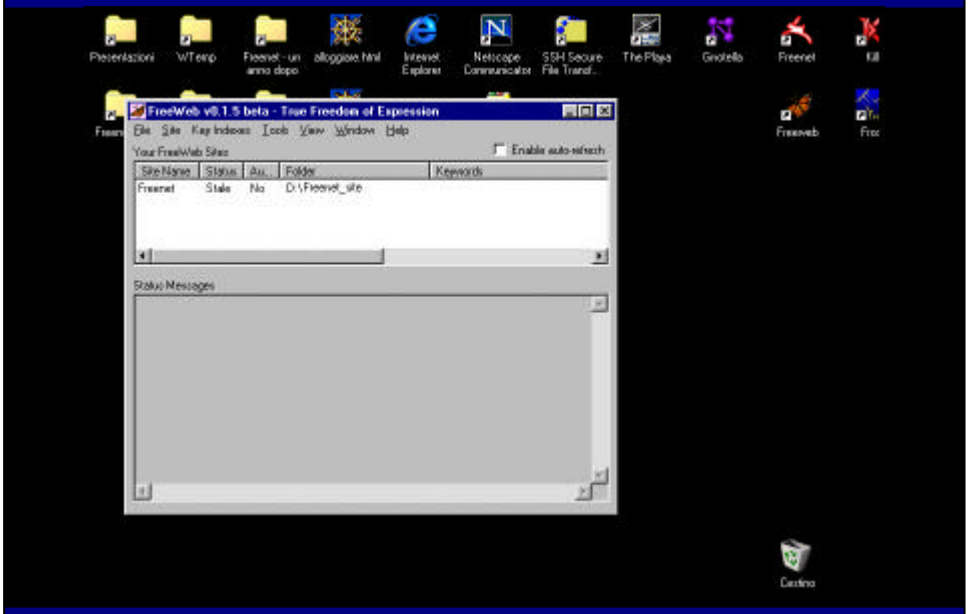
Client ed applicazioni

- Frost - client grafico per la ricerca di chiavi ed il chat (windows)
- Freeweb - client grafico per l'inserimento di freesite
- Espra - creazione e gestione di cataloghi
- Manifest - client a linea comandi per la gestione di chiavi e freesite
- FCPtools - client a linea comandi per la gestione di chiavi e freesite

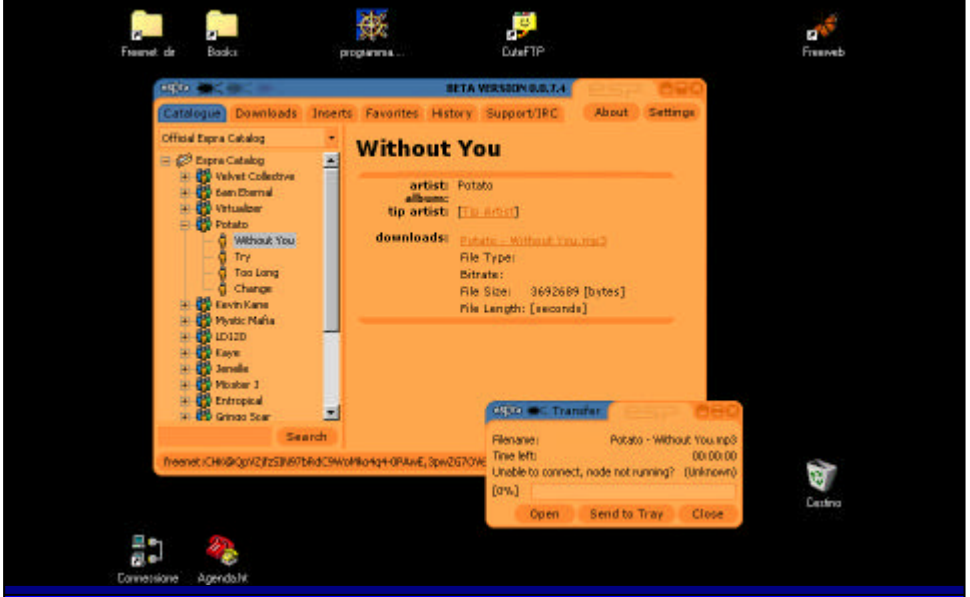
Frost



FreeWeb



Espra



Prospettive future

Prospettive future

- Formazione di un gruppo di sviluppo più grande e più strutturato, che applichi metodi di sviluppo più formalizzati (ci vuole poco!)
- Documentazione esaustiva di protocolli, API e metodi di routing
- Studio sistematico delle metodologie di attacco alla rete Freenet
- Diffusione dell'utilizzo di Freenet e sviluppo di nuovi client che la utilizzino come mezzo di trasporto e/o memorizzazione.

Aspetti legali

- **ITAR** (International Traffic in Arms Regulations)
- **DMCA** (Digital Millennium Copyright Act)
- **P.A.T.R.I.O.T Act** (Provide Appropriate Tools Required to Intercept and ObstructTerrorism)
- **Convenzione U.E. contro il cybercrime**
- **EUCD** (European Union Copyright Directive)

Bibliografia

Bibliografia

- “Freenet : A Distribuited Anonymous Information Storage and Retrieval System” - I.Clarke et al.
- Performance in Decentralized Filesharing Networks” - T. Hong
- Advanced Routing on Freenet: (Serapis) - Shu Yan Chan

I documenti sono reperibili sul sito del progetto
http://freenet.sourceforge.net
disponibile anche in italiano
http://freenet.sourceforge.net/lang/it

Grazie a tutti per l’attenzione

per maggiori informazioni:

marcoc@firenze.linux.it

mail list su Freenet in italiano
http://lists.firenze.linux.it/mailman/listinfo/freenet-list

Sito ufficiale Freenet in italiano
http://freeenet.sourceforge.net/lang/it

Il progetto Winston Smith
freenet:MSK@SSK@4YqXGejNt1zwoCXo23fCYeVH~lwQAgE/20011118000000-pws//