11/01/2010

Come nascondere l'identità in Rete

di Matteo Cappelli

Livello guida: Intermedio

Indice

1 Introduzione **1**
1.1 A chi è rivolto il manuale 2

2 Che cos'è l'Anonimato **3**

3 Il concetto di Anonimato in Rete **3**
3.1 Uso dell'Anonimato 5

4 Una panoramica sui software per l'Anonimato **6**

5 Server Proxy **7**
5.1 Server Proxy HTTP e strumenti web-based 8
5.2 Server SOCKS 11
5.3 Concatenazione di server proxy differenti 12
5.4 Il punto debole 12

6 VPN **13**

7 Darknet - la rete separata dalla Rete **15**
7.1 Anonet 15
7.2 Freenet 16
7.3 GNUnet 18
7.4 I2P 18
7.5 Altri sistemi interessanti 19

8 Mix Network **19**
8.1 Jap/JonDo 20
8.2 Onion Routing e Tor 22
8.3 Altri sistemi interessanti 25

9 Possibili minacce ad un sistema di Anonimato **25**

10 Le capacità reali di intercettazione **26**

11 Conclusioni **26**

1 Introduzione

L'evoluzione delle linee digitali ha portato Internet in modo continuativo e fisso, sia negli uffici, sia nelle case di molte famiglie, ma se da un lato migliorano la velocità di connessione e la potenza dei pc, dall'altro non si assiste ad un perfezionamento dei parametri di sicurezza degli utenti. Uno dei punti di forza di Internet è sempre stato l'anonimato, ma oggi è sempre

più difficile restare anonimi sulla grande Rete, in quanto gli utenti sono sempre più spiati e la loro privacy è messa a repentaglio.

Navigando in Rete, senza le dovute precauzioni, un utente lascia al suo passaggio un'infinità di informazioni, che vengono memorizzate nei siti web visitati o nelle chat. In questi ultimi anni si sono sviluppate sempre più le reti sociali, come facebook, che minacciano seriamente la privacy delle persone.

Spesso i dati di una persona vengono raccolti a sua insaputa, grazie all'utilizzo del sistema dei log e dei cookie. Ogni volta che un utente visita un sito, o comunque si collega ad Internet, il suo provider registra automaticamente ogni suo collegamento. Queste registrazioni automatiche si chiamano file di log, e normalmente hanno una funzione contabile amministrativa, in quanto forniscono ai provider i dati necessari alla fatturazione. Attraverso i log è però possibile avere accesso ad informazioni quali il sistema operativo utilizzato, il browser, il colore e la definizione dello schermo, e l'ultimo sito web visitato, con una conseguenza: possono essere creati precisi profili dell'utente. Quindi, navigare sul web è come fare una passeggiata con un cartello posto alle proprie spalle e con sopra scritta la propria identità.

Oltre ai problemi relativi alla privacy, chi almeno una volta non ha desiderato sapere come riescono i protagonisti hacker di certi film a far rimbalzare le loro connessioni in giro per il mondo? È possibile nascondere l'identità del proprio pc dietro quella di altri? Con il presente manuale si dimostrerà se tutto ciò è realtà oppure finzione.

(se trovate errori, o per qualsiasi suggerimento, potete contattarmi all'indirizzo `matcap83@libero.it`)

La guida è rilasciata con licenza CC [7].

1.1 A chi è rivolto il manuale

Il manuale è rivolto a tutti coloro che vogliono conoscere gli strumenti che permettono di nascondere in Rete la propria identità, come essi funzionano e quali funzionalità hanno. Si assume che il lettore abbia conoscenze minime del funzionamento del web e della Rete, sappia cosa sono un indirizzo IP e un protocollo di comunicazione (come HTTP o FTP), e sappia distinguere i termini client e server.

L'obiettivo di questo manuale è quello di illustrare i software e le tecniche ad oggi più diffuse che permettono di mascherare il proprio indirizzo IP, spiegando quali caratteristiche hanno i vari strumenti analizzati. Il manuale non vuole pertanto essere un semplice howto sulla configurazione/installazione dei software presentati, poiché sul web si trovano numerose guide per ogni software trattato (per ognuno si riportano i principali link a cui si possono trovare le istruzioni per una corretta configurazione). Gli strumenti presi in esame sono rivolti a più fasce di utenti: alcuni, come le darknet, sono piuttosto complessi da usare e configurare, dunque non adatti ai newbie,

mentre altri, come il sempre più diffuso Tor, sono più semplici da utilizzare e consigliati anche ad utenti con poca esperienza.

2 Che cos'è l'Anonimato

L'anonimato è lo stato di una persona anonima, ossia di una persona la cui identità è sconosciuta. Questo può succedere per diversi motivi: una persona è riluttante a farsi conoscere, oppure non lo vuole per motivi di sicurezza, come ad esempio per i testimoni di crimini, la cui identità deve essere protetta. Nascondere la propria identità può essere una scelta per legittime ragioni di privacy e, in alcune occasioni, anche per sicurezza personale. I criminali solitamente preferiscono rimanere anonimi, soprattutto quando scrivono lettere ricattatorie. In una grande città è presente più anonimato che in un piccolo paese, ed anche se alcuni possono considerarlo uno svantaggio, per altri potrebbe essere un vantaggio. Un'opera anonima non ha autori conosciuti. Lo possono essere i prodotti del folclore o della tradizione, tramandati oralmente; oppure lo sono i dati riguardanti il nome di un autore andati perduti o intenzionalmente nascosti [31].

Per quanto riguarda le reti informatiche, si consideri il seguente contesto: "*Alice usa un sistema S per interagire con Bob*", o alternativamente "*Bob mette a disposizione di Alice un servizio di rete S*". In questo scenario, esistono due tipi fondamentali di accessi anonimi [34]:

Forward Anonymity (figura 1). Nessuno può dire chi è Alice.

Reverse Anonymity (figura 2). Nessuno può dire chi è Bob.

Figura 1: Forward Anonymity.

3 Il concetto di Anonimato in Rete

L'anonimato su Internet è una proprietà comunemente identificata come la privatezza della comunicazione elettronica [33]. Da un punto di vista più ampio, le comunicazioni anonime sono studiate nell'ambito della sicurezza informatica, quando un utente tenta di proteggere la propria riservatezza da

Figura 2: Reverse Anonymity.

coloro che vogliono scoprire certe informazioni. Queste informazioni hanno un *valore* per le persone che vogliono ottenerle, e di conseguenza vi sarà un *costo* per il soggetto coinvolto, qualora le informazioni dovessero essere rivelate [39].

Un semplice esempio può essere suggerito dal mondo del commercio: per un venditore, una preziosa informazione potrebbe essere quella di tutti i precedenti acquisti fatti da un potenziale compratore; in questo modo chi vende la merce saprebbe quanti soldi è disposto a spendere l'acquirente. In questo caso il valore può essere espresso in termini monetari.

Un'altro esempio è la sorveglianza di una cellula terroristica. Se si fosse in grado di scoprire l'identità dei componenti, si potrebbe allora tracciare un quadro delle potenziali "amicizie". Inoltre, sarebbe di immenso aiuto poter osservare i dati inviati e ricevuti attraverso la rete, in particolare, analizzando l'intensità del traffico si potrebbe prevenire un eventuale attacco terroristico. In questo esempio il valore delle informazioni è collegato ad una maggiore protezione che potrebbe essere fornita, come nel caso degli attacchi terroristici, mentre il costo è dato dalla neutralizzazione delle cellula stessa.

Così come ci sono valori e costi per le informazioni estratte, così ci sono anche per le tecniche di sorveglianza, ed in modo simile per i sistemi che permettono di rendere anonime le informazioni. In questo ultimo caso i costi sono dovuti alla progettazione dei sistemi che permettono l'anonimato, alla loro operatività, ed al loro mantenimento.

A livello pratico, "anonimato in Rete" potrebbe essere definito come l'utilizzo di un particolare software in grado di nascondere l'identità di un utente in Rete. In figura 3 è possibile vedere cosa succede all'utente Alice qualora utilizzi un software per l'anonimato: su Internet non sarà più visibile il suo reale indirizzo IP (222.222.222.222), ma quello di un'altra macchina (l'indirizzo IP 123.123.123.123), e perciò Alice risulterà nascosta "dietro" a qualcuno. Bisogna precisare che questo procedimento non crea un'identità falsa ad Alice, in quanto l'indirizzo IP fornito dal software (123.123.123.123) è un indirizzo IP reale appartenente ad una macchina collegata ad Internet, e non è fittizio, quindi l'azione è del tutto lecita. Diversamente se il software assegnasse ad Alice un indirizzo IP fasullo l'azione non sarebbe più lecita, in quanto l'azione verrebbe definita *spoofing*, rappresentando un vero

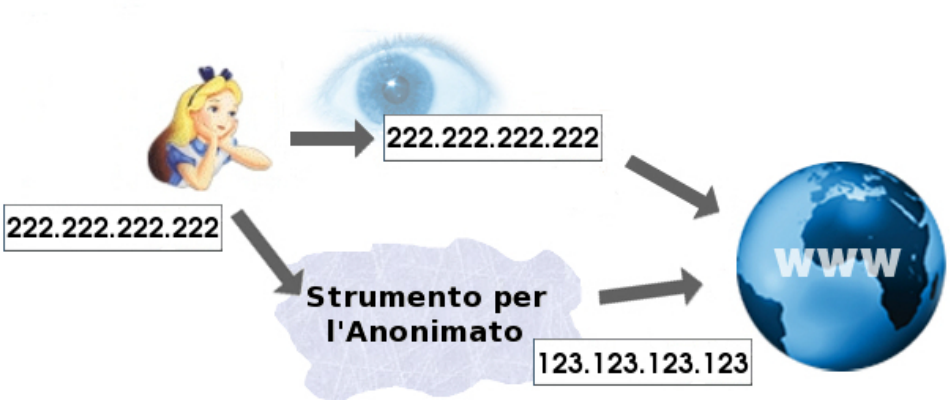

Figura 3: Mascheramento di un indirizzo IP.

e proprio attacco informatico. Il punto è questo: chi è disposto a fornire il proprio indirizzo IP affinché altri possano nascondersi dietro esso? Una bella domanda, svelata nei prossimi paragrafi.

3.1 Uso dell'Anonimato

L'uso più popolare di Internet negli ultimi anni è stato l'invio e la ricezione di mail e la navigazione sul web. Dunque, per assicurare l'anonimato nella comunicazione, dovrebbe essere costruita un'infrastruttura che permetta ad una persona di effettuare queste attività libera da intrusioni da parte di qualsiasi attaccante. Tutto questo potrebbe interessare un vasto pubblico di persone [46]:

- coloro che non vogliono farsi tracciare nella navigazione web;
- chi non vuole farsi profilare (commercialmente);
- aziende che non vogliono rendere note relazioni strategiche;
- persone soggette a restrizioni delle libertà di espressione (come in Cina o in Iran);
- autorità giudiziarie che vogliono visitare siti senza lasciare IP governativi nei log.

Oltre a questi, possono essere molti i casi in cui l'anonimato delle comunicazioni non è solamente desiderabile, ma essenziale. Per esempio, in un servizio web che tratta di argomenti quali l'alcolismo, oppure il cancro, è necessario l'anonimato di un individuo che si espone in questo servizio, in modo tale che la sua identità sia tenuta segreta a terze parti. Il fallimento di questo può danneggiare la persona, facendo diminuire ad esempio i premi delle assicurazioni, causando discriminazioni, oppure tensioni sociali.

Nel caso della posta elettronica, le persone esigono la libertà dai controlli di routine, sia in termini di contenuto che di partecipanti, come avviene attualmente nella normale corrispondenza postale. Ciò può includere messaggi mail riguardanti i familiari, il lavoro, i vantaggi/svantaggi di prodotti o servizi di varie compagnie, le orazioni politiche ed altro che potrebbe essere potenzialmente di interesse per una terza parte, che non è coinvolta nella comunicazione.

Un'altra importante applicazione delle mail anonime può essere la testimonianza di coloro che vogliono denunciare un misfatto, da parte, per esempio, di una persona potente o semplicemente una persona con autorità sul testimone. Chiaramente, una maniera per favorire le testimonianze è di istituire un servizio di posta elettronica veramente anonimo e sicuro, in modo da permettere a chiunque di mandare un messaggio in maniera relativamente facile, senza la paura di essere scoperto.

Ed ancora, sia le mail anonime, sia la navigazione anonima possono essere usate per distribuire notizie e comunicati online, senza la paura di sorveglianza in paesi con un regime repressivo.

La resistenza alla censura è l'abilità di pubblicare un documento su un sistema che assicura la sua disponibilità per un lungo lasso di tempo, malgrado potenti avversari provino a prevenirne la distribuzione. L'anonimato è uno strumento molto potente nei sistemi di resistenza alla censura, poiché impedisce di seguire le tracce dell'autore, ed in questo modo rimuove gli elementi di paura che spesso scoraggiano le persone a pubblicare documenti controversi. Ancora più importante, previene che la macchina, in cui sono memorizzati i file, sappia che contiene proprio tali file, ed in questo modo viene prevenuto un eventuale filtro messo lì da qualche organizzazione.

Di contro, l'anonimato può essere utilizzato da malintenzionati o addirittura da veri e propri criminali. Regalare anonimato e privacy a tutti costringe purtroppo a non poter escludere nessuno, nemmeno i "cattivi". Applicazioni e strumenti che garantiscono l'anonimato, infatti, possono funzionare solo se rendono impossibile qualsiasi tentativo di controllo, localizzazione o censura, e non ammettono mezze misure [39].

4 Una panoramica sui software per l'Anonimato

Al momento attuale esistono numerosi sistemi che permettono di ottenere un certo grado di anonimato, alcuni sono in via di sviluppo, altri sono già disponibili ma ancora in fase di revisione e quindi poco stabili, altri ancora sono invece pienamente funzionanti e pronti per un utilizzo di massa. Tutti questi sistemi vengono catalogati come PET [38], ossia quell'insieme composto da tutte le tecnologie che permettono il miglioramento della privacy. I più diffusi sistemi PET possono essere così catalogati:

Server Proxy. Questo insieme di strumenti è costituito dai server proxy

HTTP e SOCKS. Un proxy è fondamentalmente un intermediario che si pone tra il pc di un utente e la Rete, inoltrando per conto dell'utente tutte le richieste. I proxy garantiscono un minimo grado di anonimato, rispetto ad altri sistemi.

VPN. Una VPN crea una connessione fra il pc di un utente ed un server remoto VPN, e tutti i dati in transito attraverso Internet sono così inviati all'interno di un tunnel virtuale, criptato ed inaccessibile da chiunque. Il server remoto VPN poi si occupa di agire come server proxy, nascondendo quindi l'identità dell'utente.

Darknet. Una darknet è una rete virtuale privata, del tutto separata da Internet. Nel suo significato più generale, una darknet può essere qualsiasi tipo di gruppo chiuso e privato di persone che comunicano tra loro, ma il nome spesso è usato nello specifico per reti di condivisione di file, dette P2P. Solamente all'interno di questa rete viene garantito anonimato e privacy.

Mix Network. Questi sistemi creano tra il pc di un utente e la Rete una catena di proxy, attraverso la quale vengono inviati i dati. In aggiunta ogni messaggio inviato viene criptato da ogni proxy, il quale conosce solamente il nodo da cui il messaggio è arrivato e quello a cui deve essere trasmesso. Le mix network permettono di raggiungere un buon livello di anonimato.

Di seguito, viene discussa in modo più approfondito ogni singola categoria.

5 Server Proxy

Un server proxy è un programma che si interpone tra client e server, e può essere utilizzato sia in locale sia per l'accesso diretto ad Internet. Nel caso di una rete LAN, può essere usato in modo che più host possano accedere ai servizi della Rete attraverso una sola connessione. In questo contesto, ogni pc di un utente ha assegnato un IP privato, che viene gestito dal proxy. A sua volta il proxy ha un indirizzo IP privato, ed uno pubblico, con il quale è identificato nella rete esterna. In pratica, se un server proxy è utilizzato in una rete locale, i singoli computer non hanno accesso diretto alla rete esterna ma solo il proxy lo ha, il quale è l'unico ad essere identificato dall'esterno: i singoli utenti risultano anonimi rispetto alla rete esterna.

Estendendo il concetto ad Internet, è possibile avere alcuni client (gli utenti) con indirizzo IP pubblico che si connettono ad un server con funzione di proxy, il quale gestisce le richieste per conto loro: il risultato, osservabile in figura 4, è una connessione anonima per ogni client connesso tramite il proxy. Un noto software commerciale che usa questo sistema per garantire

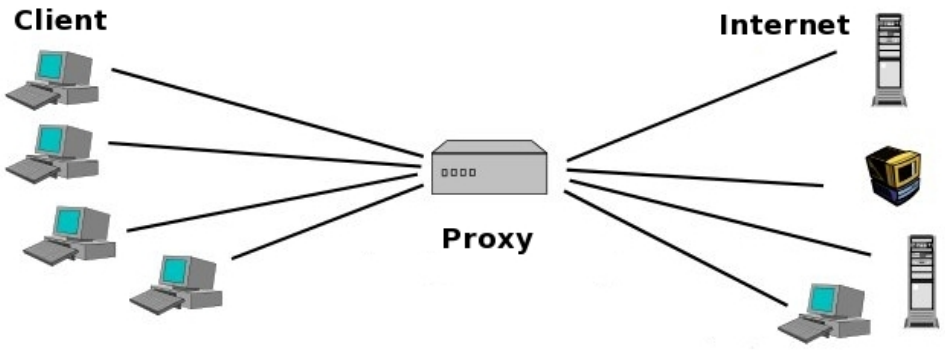

Figura 4: Comunicazione tramite proxy.

l'anonimato è Anonymizer [2]. Nel contesto di un server web, il proxy intercetta le richieste che arrivano dai client, per procurare dai vari siti web le pagine HTML, e redirigerle quindi in locale. In questo modo il server web ospitante il sito richiesto rileva l'indirizzo del proxy, e non quello reale del client.

Sono adesso trattati individualmente i server proxy HTTP e SOCKS, con una descrizione dei pro/contro di entrambi.

5.1 Server Proxy HTTP e strumenti web-based

Un server proxy (chiamato anche server proxy HTTP, server proxy web, o più semplicemente proxy) è un tipo di proxy che può essere utilizzato per la navigazione anonima sul WWW, e per l'invio di mail attraverso il web. Alcuni proxy supportano anche il protocollo sicuro HTTPS, e alle volte FTP. I proxy sono classificati, secondo [40] e [6], in base alla loro velocità e, soprattutto, al livello di anonimato che permettono di raggiungere:

Proxy di tipologia Trasparent. Sono molto veloci, ma lasciano scoprire con semplici strumenti il reale IP di un navigatore. Questi proxy modificano alcuni header trasmessi dal browser e ne aggiungono altri, tuttavia inviano al sito contattato anche l'indirizzo IP del richiedente, oltre al loro indirizzo. Questo significa che l'amministratore del sito vedrà un contatto con "doppio IP", quello del proxy e quello dell'utente. Si usano soprattutto in attività di concatenazione proxy, inserendo ovviamente un proxy Elite all'inizio della concatenazione, e solo dopo una serie di proxy Trasparent.

Proxy di tipologia Anonymous. Sono server proxy meno veloci rispetto ai precedenti, ma consentono un discreto livello di anonimato. Tuttavia, con particolari tecniche, è possibile comprendere se un utente sta utilizzando un proxy, poiché vengono modificati alcuni header dei

pacchetti inviati dal client. Dunque, si potrebbe bloccare in ogni caso l'accesso ad un sito, o risalire al mittente, anche se la procedura di identificazione dell'IP reale è ben più complessa.

Proxy di tipologia Elite. Si tratta di server proxy difficili da identificare in quanto tali, che forniscono perciò un buon ottimo livello di anonimato.

Sul web è possibile trovare intere liste di proxy, come quella visualizzabile all'indirizzo web [44] e contenente una lista completa di proxy pubblici, suddivisi per nazione e per tipologia.

Oltre ai tipi di proxy esaminati, esiste una particolare categoria di server, detti proxy CGI, i quali sono costituiti da un sito web che permette la navigazione in Rete. Molti di questi siti permettono di scegliere quali dati inviare (cookie, referer, tipo di browser, ...), e possono essere catalogati come Trasparent, Anonymous, ed anche Elite. Un proxy CGI risulta semplicissimo da utilizzare, in quanto basta collegarsi alla pagina del proxy (ad esempio [25], ed il molto valido [5]), e digitare in un campo apposito la pagina web da visitare. Ne esistono moltissimi, più o meno affidabili, ed è possibile trovarne una lunga lista all'indirizzo [10]. In figura 5 è possibile osservare la pagina principale del proxy The Cloak, usato per collegarsi al sito `www.google.com` (indicato dal cerchio rosso). The Cloak è uno dei proxy CGI migliori attualmente sul web, in quanto è possibile personalizzare la navigazione abilitando o meno numerose opzioni (cancellazione dei cookie, disabilitazione di Java, ...).

Per aumentare il grado di anonimato, è possibile concatenare più server proxy: maggiore è la lunghezza della catena di proxy usati, più difficile sarà essere rintracciati. Concatenare più server di questo tipo significa giungere al server finale attraversando ogni server proxy, e significa pure mostrare la reale identità del navigatore solamente al primo dei proxy. Una concatenazione assume la forma

```
Client >>>> Proxy-1 >>>> ... >>>> Proxy-i >>>> Internet
```

dove Proxy-i indica l'i-esimo proxy interposto tra il pc di un utente ed Internet. Non c'è alcun limite teorico al numero di proxy concatenabili, benché vi siano delle limitazioni pratiche. Una concatenazione può essere effettuata in tre modi:

1. utilizzando proxy CGI. In questo caso basta semplicemente immettere, nell'indirizzo della barra di navigazione del proxy CGI, l'indirizzo di un altro proxy CGI;

2. utilizzando un proxy standard (impostazione manuale nel browser), e quindi passando attraverso proxy CGI;

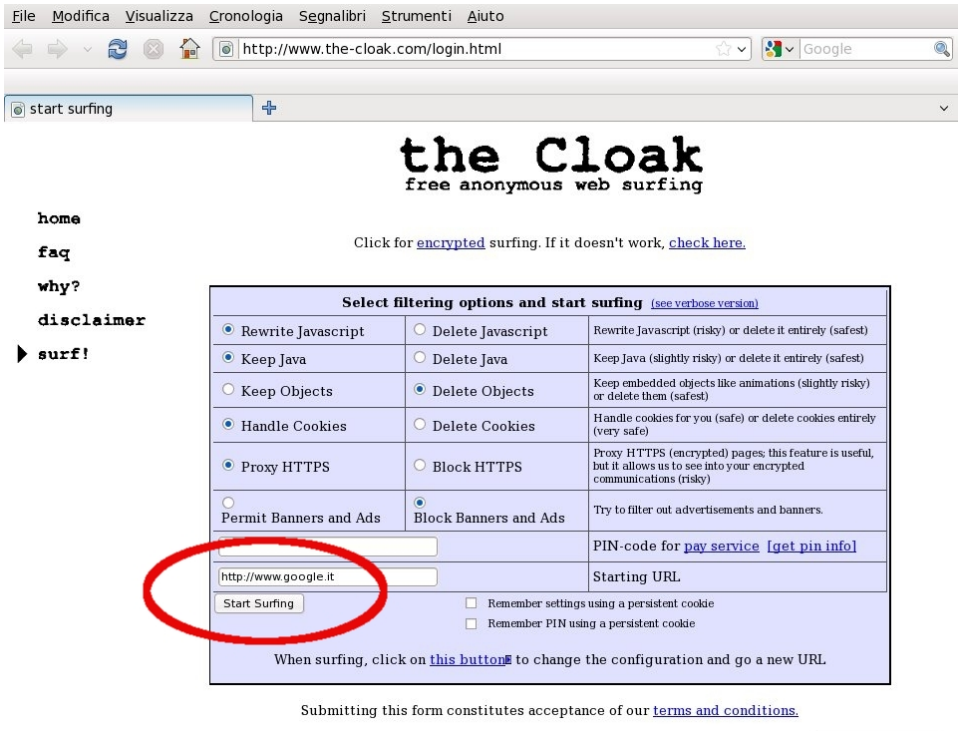

Figura 5: Proxy The Cloak.

3. utilizzando software specifici, come ad esempio SocksChain [26], oppure tramite plugin nel caso di FireFox. In questi casi, il software crea un "proxy virtuale" [10], che fisicamente corrisponde alla catena di proxy stabilita.

Sono però da considerare i pro ed i contro di questo strumento. Sicuramente l'utilizzo dei proxy CGI è relativamente semplice, dal momento che non richiedono particolari requisiti o conoscenze. Più complesso invece è l'utilizzo di proxy HTTP, poiché si deve ricercare un server funzionante, controllandone la sua tipologia. Un'altra caratteristica interessante dei proxy è la possibilità di mascherare l'IP di una persona che usa una webmail, anche se le sue azioni sono comunque tracciate attraverso l'account di posta.

Passando agli aspetti negativi, il peggiore è che alcuni proxy mantengono i file di log del traffico di rete, anche se accessibili solamente all'amministratore del sistema. Questi dati, difatti, a seguito di qualche intrusione potrebbero finire nella mani di un malintenzionato o, comunque, di qualcuno che voglia risalire all'identità del navigatore. Oltre a ciò, alcuni proxy, definiti *Hostile Proxy* [40], sono creati appositamente per spiare il traffico altrui, e carpire i dati dai client a loro connessi (password, numeri di carta di credito, informazioni personali e messaggi inviati via mail).

I server proxy possono anche essere adoperati in combinazione a software specifici, come ad esempio Multiproxy [20]. Questo programma necessita di una lista di proxy, da indicare in input, e automaticamente si connetterà al nodo più veloce della lista. Degno di nota è pure Stealther [27], un'applicazione simile alla precedente ma che dispone già di una lista di server proxy, aggiornabile e personalizzabile. Questo programma, una volta testati quali sono i proxy attivi al momento della connessione, stabilisce ad ogni nuova richiesta da parte dell'utente, o a periodi di tempo prestabiliti, una connessione con uno di essi. Con questo procedimento ogni connessione avviene attraverso un proxy differente.

In definitiva, l'anonimato che può essere raggiunto con i server proxy è in genere sufficiente qualora una persona voglia nascondersi da parenti/scuola/lavoro, ma, nel caso si desideri una garanzia elevata di anonimato, si deve optare per altre soluzioni.

5.2 Server SOCKS

I server proxy SOCKS sono una tipologia di particolari server che possono essere usati al fine di mascherare la propria identità, similmente ai proxy HTTP e CGI appena trattati.

Innanzitutto il protocollo SOCKS realizza una forma di proxy a livello di trasporto, e non a livello applicativo come nel caso precedente. Il protocollo consente, ai pc appartenenti ad una rete protetta da firewall (ad esempio in una LAN), di comunicare con l'esterno passando attraverso il firewall, senza richiedere una trasmissione diretta dell'IP. Pertanto, un singolo pc invia il suo flusso di dati verso Internet e attraverso il firewall, proprio grazie al servizio SOCKS. Sebbene un firewall blocchi tutte le connessioni dall'esterno, esistono SOCKS che possono essere attraversati in entrambi i sensi: questo è il segreto alla base di questo sistema. I dati possono attraversare il firewall dalla LAN verso l'esterno, ma anche i pacchetti di dati di utenti esterni possono sfruttare il servizio SOCKS di quella rete per navigare anonimi. In questo modo il protocollo esegue un filtro tra l'utente collegato, ed il server che si vuole raggiungere.

Adesso sono elencate le principali differenze tra i server proxy e SOCKS:

- mentre i server proxy operano principalmente sulle porte 80, 8080, 3128, 9090, i SOCKS sfruttano la porta 1080;
- un server proxy viene sfruttato soprattutto per connessioni web basate sul protocollo HTTP, i SOCKS invece possono operare con molti tipi di protocolli, tra cui FTP, IRC, POP3, ed SMTP. L'unico requisito è che il software, usato per la connessione, supporti il protocollo SOCKS;
- esistono programmi in grado di far passare tutte le connessioni attraverso un SOCKS, anche programmi come telnet, ad esempio, attraverso i quali sarebbe impossibile risultare anonimi;

- i pacchetti inviati dal client, compresi gli header, non sono modificati, a differenza di molti server proxy;
- la connessione è solitamente più lenta rispetto ai collegamenti effettuati tramite proxy.

Inoltre anche per i proxy SOCKS si possono creare concatenazioni, allo stesso modo dei server proxy HTTP, facendo uso di programmi appositi come SocksChain. Si ricorda infine che esistono tre versioni differenti del protocollo (4, 4a, e 5).

5.3 Concatenazione di server proxy differenti

Una particolarità dei server proxy HTTP, CGI e SOCKS, è di poter essere combinati nella realizzazione di una concatenazione. Per far ciò è necessario il programma SocksChain, in grado di far transitare la connessione attraverso sia proxy HTTP che proxy SOCKS. È possibile realizzare catene del tipo:

```
proxy SOCKS >>>> proxy HTTP >>>> proxy CGI
proxy SOCKS >>>> proxy HTTP
proxy HTTP >>>> proxy CGI
```

o ancora:

```
proxy HTTP >>>> proxy SOCKS
```

Non è possibile creare invece concatenazioni come le seguenti:

```
proxy CGI >>>> proxy HTTP
proxy CGI >>>> proxy SOCKS
```

5.4 Il punto debole

Il problema principale dei server proxy HTTP e SOCKS è da ricercare nell'affidabilità dei proxy adoperati. Qualora si utilizzasse anche un server di tipo Elite (caso migliore), non si ha alcuna garanzia certa sul reale grado di anonimato ottenuto. Inoltre, l'operatività di un server può non essere costante nel tempo, e costringere un utente a dover trovare ogni volta un server proxy funzionante (o aggiornare una lista di proxy, nel caso di programmi quali Multiproxy). In conclusione, il funzionamento della connessione e l'occultamento dell'identità di una persona dipendono unicamente dal proxy adoperato, e, pertanto, qualsiasi attacco portato a quell'unico punto comprometterebbe l'anonimato.

Pertanto, se si ricerca uno strumento affidabile, che permetta anche di garantire un buon livello di anonimato, è consigliabile ricorrere ad altri strumenti di anonimato.

6 VPN

Una VPN è una tecnologia che permette il collegamento fra due reti private attraverso la rete pubblica, ed è nata fondamentalmente con l'obiettivo di instaurare una connessione criptata, e di aumentare così la produttività delle aziende. Le connessioni tra le reti remote vengono stabilite attraverso i meccanismi di Internet, per permettere lo scambio di dati in modo trasparente, come se le reti fossero collegate da un linea diretta. Questa tecnica prende il nome di tunneling, ed attraverso il suo utilizzo i nodi di instradamento della rete pubblica non sono in grado di rilevare che la trasmissione è parte di una rete privata.

Dal lato consumer, lo scopo di queste reti è di trasportare i dati di un utente in un luogo geograficamente diverso da quello di partenza, soggetto nella maggior parte dei casi a leggi diverse, e di oltrepassare alcuni filtri dei provider. Queste reti necessitano di un sistema di autenticazione, ed inoltre tutti i dati vengono criptati per garantire la riservatezza delle informazioni. Qualsiasi metodo per criptare il traffico di rete fra due host remoti può essere usato per creare una VPN, anche protocolli generalmente utilizzati per altri scopi, come SSH o SSL. Questo è ciò che è una VPN.

Fondamentalmente, un software per l'anonimato basato sulla tecnologie delle VPN opera in modo simile ai proxy visti precedentemente, ed è possibile vedere un esempio in figura 6. Ogni richiesta effettua da un utente viene prima criptata, ossia resa inaccessibile da chiunque tenti di intercettarla, quindi viene inviata al server VPN. Una volta che il server VPN ha ricevuto i dati, li invierà alla destinazione (stessa funzionalità dei proxy HTTP e SOCKS), e dopo aver ricevuto la risposta dalla destinazione la invierà, criptata, indietro all'utente.

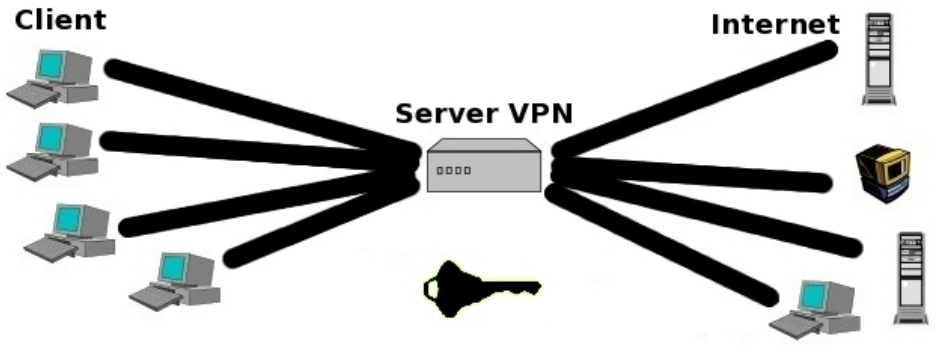

Figura 6: Comunicazione tramite VPN (tutti i dati sono criptati).

Sul mercato esistono numerose offerte di servizi basati sulla tecnologia VPN, e la maggior parte sono a pagamento, con abbonamenti di uno, due mesi, oppure un anno. Tutti questi servizi possono essere catalogati in base

al costo, al protocollo usato, al sistema di criptazione (e quindi al grado di riservatezza e anonimato ottenibile) ed alla raggiungibilità della rete [32]. Oltre a questi, esistono anche aziende che hanno prodotto vere e proprie suite di programmi per l'anonimato basate sulle reti VPN. Tra i software più famosi si citano GoTrusted [12] e SmartHide [3], la cui schermata principale è visibile in figura 7.

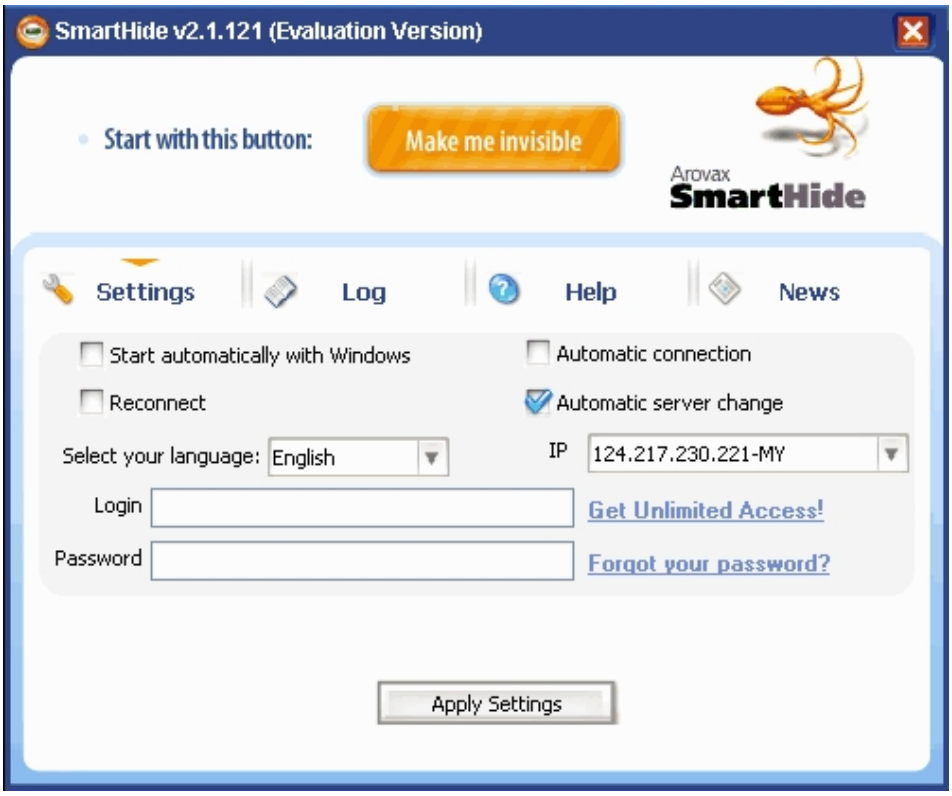

Figura 7: Interfaccia di SmartHide.

Dal punto di vista dell'anonimato i principali vantaggi di questo sistema sono:

- velocità elevata;
- non vengono mantenuti file di log (nella quasi totalità dei servizi);
- tutti i dati sono criptati;
- moltissimi servizi Internet possono essere resi anonimi, come la navigazione web, il P2P, la messaggistica istantanea (come MSN), ...

Di contro, si possono elencare i seguenti lati negativi:

- il servizio quasi sempre è a pagamento;

- la raggiungibilità di una rete VPN è variabile;
- è sempre richiesta la registrazione per l'utilizzo del servizio, e, in genere, si deve far uso di un client proprietario.

Si ricorda anche che il termine VPN è un termine generico e non un marchio. In particolare, non esiste alcun ente che regoli la denominazione di un prodotto come VPN, e dunque ogni produttore può utilizzarlo a suo arbitrio.

7 Darknet - la rete separata dalla Rete

Le caratteristiche di una darknet sono fondamentalmente due: la possibilità di immettere e fruire di informazioni con mezzi interni alla darknet stessa, questo perché spesso non è solamente un sistema di file-sharing; e la creazione di comunità di utenti logicamente separate dalla Rete. Tutti i software di tipo darknet dunque offrono sia reverse che forward anonymity (è possibile navigare ma anche pubblicare siti in modo anonimo), ma soltanto all'interno della loro rete e non di Internet.

In questa categoria i più importanti sistemi che hanno raggiunto piena maturità, e quindi liberamente utilizzabili, sono quattro:

- Anonet [8];
- Freenet [9];
- I2P [13];
- GNUnet [11].

Sono adesso illustrati singolarmente.

7.1 Anonet

Anonet è una rete "privata" di una comunità di utenti, e si tratta di una rete F2F, ossia di una rete P2P riservata ai soli soci. Come tale, non è di libero accesso per chiunque. Per collegarsi ad Anonet è necessario entrare a far parte della sua comunità di utenti ed ottenere delle apposite chiavi di autorizzazione. In altri termini, prima di collegarsi ad Anonet è necessario passare attraverso un'apposita procedura di "affiliazione". Ogni utente in Anonet è identificato solamente da un indirizzo IP anonimo, con il quale è possibile collegarsi ad un apposito server all'interno della rete e scaricare e riservare per i propri usi delle intere sottoreti TCP/IP composte ognuna di centinaia di indirizzi IP. Oltre a ciò è possibile usare ognuno degli indirizzi ottenuti per esporre su Anonet dei server web, dei server di posta o qualsiasi altro servizio. Ogni computer, e per estensione, ogni utente, forma un nodo

della rete Anonet e le comunicazioni tra nodo e nodo corrono all'interno di tunnel criptati e basati sulla tecnologia delle VPN (vedere paragrafo 6 - VPN).

Dal punto di vista tecnico, Anonet utilizza la stessa architettura e gli stessi strumenti di Internet, pertanto, su Anonet è possibile offrire o usare gli stessi servizi presenti su Internet: la posta elettronica, i siti web ed i blog, i server di chat, i server di messaggistica istantanea, FTP, le reti P2P, BitTorrent, ecc. L'unica differenza sono gli indirizzi IP.

Per evitare collisioni con gli indirizzi di Internet, Anonet usa gli indirizzi compresi tra 1.0.0.0 e 1.255.255.255, riservati in teoria dall'IANA per usi interni, e perciò non utilizzabili né su Internet né sulle LAN.

A differenza di quello che avviene su Internet, su Anonet non c'è nessun "ente superiore" che assegna gli indirizzi IP agli utenti. Ogni nuovo utente si collega ad un apposito sito web, e riserva per sé stesso almeno due diversi blocchi di indirizzi (due diverse "sottoreti"), uno per la navigazione su Anonet e l'altro per l'esposizione di servizi TCP/IP sulla rete. In questo modo, non esiste nessun legame tra l'indirizzo IP e l'identità dell'utente che lo usa. Ad esempio, è possibile sapere che l'indirizzo 1.0.0.9 viene usato dall'utente Bob, ma è impossibile sapere chi sia in realtà Bob o dove risieda.

L'uso della rete Anonet è sconsigliato agli utenti principianti, in quanto il suo utilizzo non è banale, e prima di poter effettivamente accedere ad Anonet è necessario presentarsi alla comunità degli utenti anonimi, ed essere accettati. Sul sito ufficiale [8], nella sezione **Come ci si collega**, sono riportate tutte le istruzioni per accedere alla rete di anonimato.

7.2 Freenet

Freenet è un'applicazione per la pubblicazione ed il recupero anonimo di informazioni realizzata in linguaggio Java, disponibile su praticamente tutti i sistemi operativi ed in sviluppo dal lontano 1999. Il sistema è completamente slegato dal WWW, e le sue due caratteristiche principali sono le seguenti:

- non esistono motori di ricerca, e poiché la rete è separata da Internet non è possibile ad esempio adoperare google. Dunque, il procedimento è quello di partire da una o più pagine standard, dalle quali si seguono i collegamenti in base alle descrizioni, fino a trovare ciò che si desidera;
- oltre a navigare all'interno di Freenet, è possibile eseguire l'upload di qualsiasi tipo di materiale, o addirittura di un proprio sito.

A differenza di altre applicazioni simili, che memorizzano i dati in chiaro sui dischi dei pc dei partecipanti alla rete, Freenet estende la protezione dei contenuti tramite la crittografia e la suddivisione dei dati in un "datastore" criptato, distribuito e ridondante. La pubblicazione dei materiali e la loro fruizione è permessa grazie alle risorse dei singoli utenti, poiché viene

adoperata sia la banda passante che lo spazio su disco di ogni persona collegata. Caratteristica importante di Freenet è che viene offerto l'anonimato sia a chi memorizza le informazioni, sia a chi le recupera (forward e reverse anonymity).

Freenet è una rete molto utilizzata e popolata di contenuti di ogni tipo, a differenza di Internet, in cui molti documenti possono essere censurati. Dunque il consiglio è di fare attenzione a cosa si cerca, e soprattutto agli utenti che si possono conoscere. Inoltre caratteristica di Freenet è la possibilità di creare ulteriori gruppi chiusi di utenti interni a Freenet, e con ammissione ad invito.

Sebbene molte nazioni censurino le comunicazioni per motivi diversi, hanno tutte una caratteristica comune: qualcuno deve decidere cosa tagliare e cosa mantenere, cosa considerare offensivo e cosa no. Freenet è una rete che elimina, per chiunque, la possibilità di imporre la sua scala di valore sugli altri, ed in pratica a nessuno è permesso cancellare niente (da ciò il nome Freenet, in italiano "rete libera"). La tolleranza verso le opinioni altrui è fortemente incoraggiata, agli utenti è richiesto di non prestare attenzione ai contenuti che non approvano.

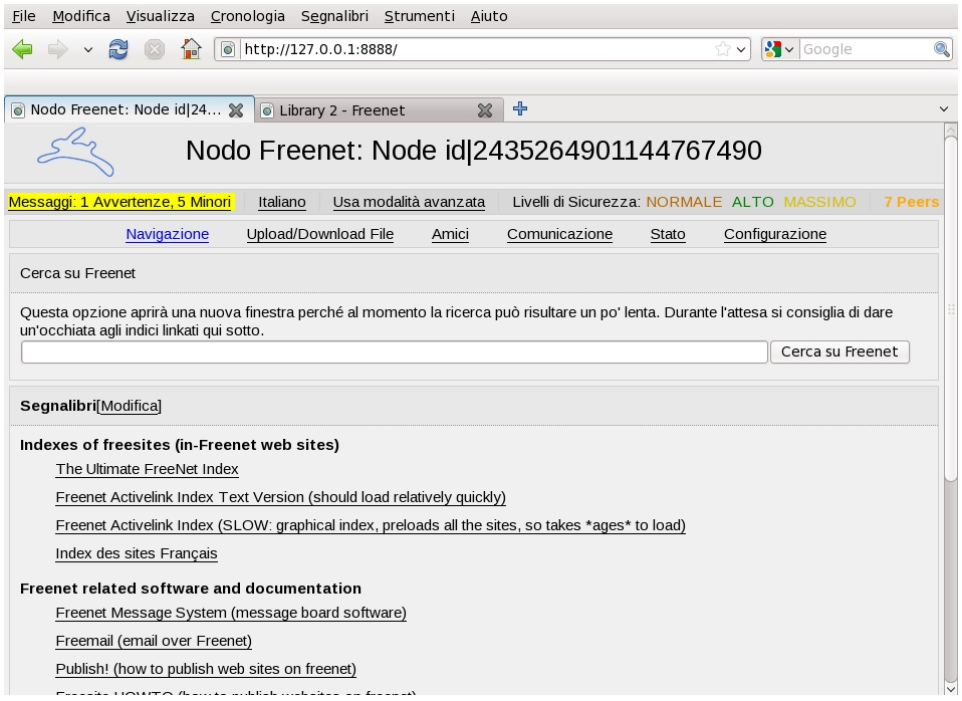

Figura 8: Schermata principale di Freenet.

Inoltre all'interno di Freenet è possibile utilizzare servizi simili a quelli presenti sul web [36], come ad esempio la messaggistica istantanea (tramite

il programma Frost, oppure con Freenet Message Board), oppure la posta elettronica.

In definitiva, come nel caso di Anonet, anche l'uso di Freenet richiede una certa esperienza nell'uso del pc, e non è consigliato agli utenti che ricercano un sistema semplice ed immediato. Infatti, l'installazione del sistema risulta semplice, ma complessa è invece la fase di configurazione (anche se è facilitata dal fatto che sono presentati all'utente una serie di step, per impostare nel migliore dei modi le opzioni).

In figura 8 è mostrata la schermata principale di Freenet, all'interno del browser Firefox. Il download dell'applicazione può essere effettuato direttamente dalla homepage del sito del progetto, mentre nella sezione **Documentation** è possibile trovare abbondante materiale per usare al meglio Freenet.

7.3 GNUnet

GNUnet può essere descritto come "l'ambiente P2P decentralizzato, anonimo e anticensura del Progetto GNU." In realtà è un sistema (attualmente alla versione beta) che va ben oltre il semplice file-sharing, in quanto mira a fornire un framework per protocolli generici di comunicazione P2P anonima e non censurabile. La sua caratteristica peculiare è la trasmissione anonima dei dati basata su source rewriting, ossia l'impossibilità di dedurre se una data richiesta è stata generata da un nodo, oppure se è stata inoltrata per conto di altri. Tutte la comunicazioni in GNUnet, sia quelle in entrata che quelle in uscita, sono autenticate e criptate nodo a nodo, in modo da evitare la censura.

Il download dell'applicazione può essere effettuato dall'apposita sezione del sito ufficiale, scegliendo il tipo di file in base al sistema operativo usato. L'utilizzo di GNUnet si consiglia solo agli utenti veramente interessati a provare il software, dal momento che il sito stesso riporta la frase "Tieni presente che si tratta di una versione beta. La rete non è ancora stata testa su larga scala e il codice ha bisogno di piccoli aggiustamenti, Ci sono diversi problemi noti di portabilità. [...] La rete è ancora abbastanza piccola ed i download potrebbero essere piuttosto lenti."

7.4 I2P

Originariamente chiamato Invisible Internet Project, è un software libero ed open source per la realizzazione di una rete anonima, in grado di offrire un livello in cui le applicazioni possono scambiarsi dati, messaggi, navigare e quant'altro. Come Freenet, anche I2P è un'applicazione scritta prevalentemente in Java, tuttavia realizza una darknet a livello applicativo. Di conseguenza, non è possibile usare applicazioni Internet standard [37], come

la posta elettronica o IRC, ed inoltre è possibile muoversi esclusivamente all'interno dell'applicazione stessa.

All'interno della rete non esiste un punto centrale su cui si potrebbe fare pressione per compromettere l'integrità, la sicurezza o l'anonimato del sistema. La rete supporta la riconfigurazione dinamica in risposta a vari attacchi, ed è stata pure progettata per far uso di risorse addizionali appena si rendono disponibili. Inoltre, le specifiche tecniche del sistema sono disponibili a tutti, e liberamente consultabili.

I2P è stato progettato per permettere agli utenti di comunicare in modo anonimo con tutti gli altri, non sono infatti identificabili da terze parti né colui che invia i dati, né cosa è stato inviato (forward e reverse anonymity). Ad esempio, è possibile sia consultare i siti web all'interno di I2P, con la possibilità di pubblicare anche in modo anonimo le informazioni, sia accedere in modo anonimo al normale web attraverso determinati proxy HTTP. Tuttavia, l'accesso ad Internet è tenuto sotto controllo, e talvolta disabilitato per prevenire eventuali attacchi.

In conclusione, I2P ha molte caratteristiche interessanti, ma si trova ancora in fase di sviluppo pre-alpha, ed è ben lontano dal poter fornire quel minimo di affidabilità che ha raggiunto, ad esempio, GNUnet.

7.5 Altri sistemi interessanti

Sono da citare anche: Mute [21], un sistema di file-sharing che protegge la privacy degli utenti; ANts [42], un progetto P2P tutto italiano; iMule [14], un sistema ottenuto dalla modifica di eMule, e realizzato appositamente per poggiarsi sulla rete I2P; ed infine Entropy, il cui sviluppo è però stato bloccato per la verifica della sicurezza degli algoritmi interni.

8 Mix Network

Oltre ai metodi presi in esame, esistono strumenti di anonimato che possono essere sfruttati come i server proxy, interponendosi tra un utente ed il servizio richiesto. Le mix network, ideate da David Chaum [39] nei primi anni 80, sono costituite da una collezione di router, chiamati *mix*, interconnessi fra loro, i quali forniscono anonimato per il transito del traffico. Con questo sistema è arduo per un malintenzionato sapere quale client comunica con quale server (analisi del traffico entrante ed uscente), grazie all'occultamento dell'indirizzo IP del mittente (forward anonymity).

Inizialmente le mix network erano stato concepite solamente per inviare messaggi anonimi, ma recentemente sono state utilizzate anche per fornire anonimato durante la navigazione in Rete. Una mix network di Chaum consiste nell'interconnessione tra loro di tutti i mix, ognuno avente una propria chiave per la cifratura sia pubblica che privata. In dettaglio, se l'utente Alice vuole inviare un messaggio, deve eseguire i seguenti passi:

- scegliere il mix di partenza;
- scegliere la sequenza di mix che il messaggio deve attraversare.

Fatto ciò, Alice deve criptare il messaggio tante volte quanti sono i mix scelti. In figura 9 si può osservare il funzionamento di questa tecnologia.

Figura 9: Funzionamento di una rete di mix.

Una variante di questo sistema è quella delle mix network in *cascata*, o *mix cascade*, in cui i mix sono appunto collegati tra loro in cascata, e gli utenti si connettono sempre al medesimo mix iniziale. Con questa variante, tutti i messaggi che attraversano i mix effettuano sempre lo stesso percorso, ovvero sono attraversati sempre gli stessi mix e nello stesso ordine.

I principali software basati sull'idea di Chaum sono:

- Jap/JonDo ([16] e [15]);
- Onion Routing [24] e Tor [29];
- i remailer Mixmaster [18] e Mixminion [19] (non trattati in questa guida).

Di seguito sono descritti in dettaglio Jap/JonDo, l'Onion Routing e Tor.

8.1 Jap/JonDo

Jap/JonDo (da ora in avanti chiamato solo Jap per brevità) è un programma scritto in Java, free, multipiattaforma ed open source, ed è stato sviluppato sull'idea dei mix cascade. Il software permette agli utenti di scegliere tra diversi percorsi (mix cascade) possibili, a differenza di altri sistemi, quali ad esempio Tor, che costruiscono ogni volta i percorsi in modo dinamico. Come appena detto, Jap è un software free, tuttavia esistono due tipologie di percorsi utilizzabili, *free* e *premium*, il cui stato è verificabile all'indirizzo [17]. La differenza tra i due tipi di servizi consiste in alcuni limiti che sono imposti ai servizi free. Nel caso dei servizi premium, la disponibilità di almeno un percorso funzionante è sempre garantita, così come la

velocità di connessione, entro determinati valori ben più elevati di quelli dei servizi free. In aggiunta, gli sviluppatori dichiarano ufficialmente che i servizi premium offrono il supporto ad un maggior numero di applicazioni, tra cui chat IRC e programmi di file-sharing, mentre i servizi free permettono unicamente di usare il software per la navigazione tramite browser.

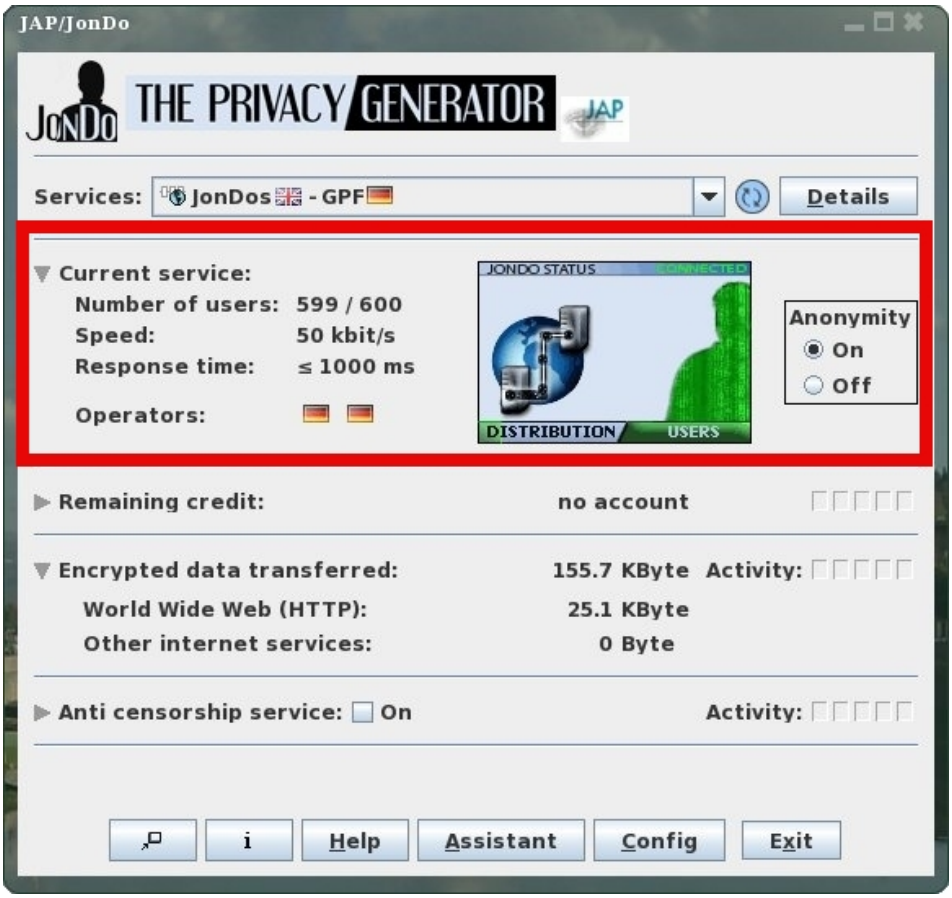

Figura 10: Interfaccia di Jap/JonDo.

Per installare e configurare correttamente il programma, ed il proprio browser, si possono trovare indicazioni direttamente sul sito ufficiale [16], o si può consultare una guida in italiano [22], davvero ben fatta. I passi base da eseguire sono tre:

1. download e installazione di Jap, dalla sezione **JonDo Program** e quindi **download** del sito ufficiale;
2. configurazione del campo "Server Proxy" sul browser, in modo che tutte le connessioni vengano inoltrate al programma Jap;
3. avvio di Jap, ed eventuale configurazione dei parametri principali.

In figura 10 è possibile vedere uno screenshot del programma, con evidenziata in rosso la sezione della finestra dalla quale è possibile facilmente attivare l'anonimato, e tenere sotto controllo la velocità della connessione.

La caratteristica principale di Jap è la sua estrema semplicità di utilizzo, difatti basta avviarlo e lasciarlo in background mentre si effettuano tutte le normali operazioni sul web, in quanto il programma stesso provvederà in modo automatico a scegliere un percorso funzionante. Inoltre, una particolarità del software è la possibilità di essere usato in congiunzione con la rete Tor, in modo da aumentare notevolmente il grado di anonimato raggiungibile.

8.2 Onion Routing e Tor

L'Onion Routing è un sistema di comunicazione flessibile e resistente sia ad osservatori esterni sia alle analisi del traffico, e il progetto originale proviene da ambienti militari americani [24]. Il sistema è basato sul principio dei mix cascade di Chaum, ma è applicato ad una struttura *circuit-based*, ossia ogni percorso utente-destinazione viene creato al momento dell'invio del primo pacchetto. Ogni messaggio viene criptato ed inviato attraverso il circuito definito in partenza, composto da una sequenza di proxy chiamati *onion router* (corrispondenti ai mix). Nello specifico, il procedimento è il seguente:

1. Alice, al momento della connessione, si collega ad uno degli onion proxy, anziché direttamente ad Internet;

2. l'onion router, a cui alice si è collegata, crea dinamicamente una connessione anonima attraverso altri onion router, fino alla destinazione.

Da notare che, prima di trasmettere ogni messaggio, il primo onion router aggiunge uno strato di cifratura per ogni onion router che deve essere attraversato (da qui il nome "onion", in italiano "cipolla"). Durante la trasmissione dei dati, ogni onion router rimuove uno strato di cifratura dal messaggio usando la propria chiave privata, fino al nodo finale su Internet, a cui il messaggio arriverà in chiaro. Questo procedimento viene effettuato anche per il messaggio di risposta, dal nodo su Internet ad Alice. Da questo sistema è stato generato Tor, denominato Onion Router di seconda generazione [41]. In figura 11 è mostrato un esempio della rete Tor, con i percorsi creati dinamicamente e differenti per ogni utente. Dalla figura si può vedere come l'indirizzo IP finale di entrambi gli utenti sia diverso da quello reale:

- l'indirizzo IP reale di Alice è 111.111.111.111, ma quello visibile su Internet corrisponde a 123.123.123.123;

- l'indirizzo IP reale di Bob è 222.222.222.222, mentre quello osservabile sul web è 190.190.190.190.

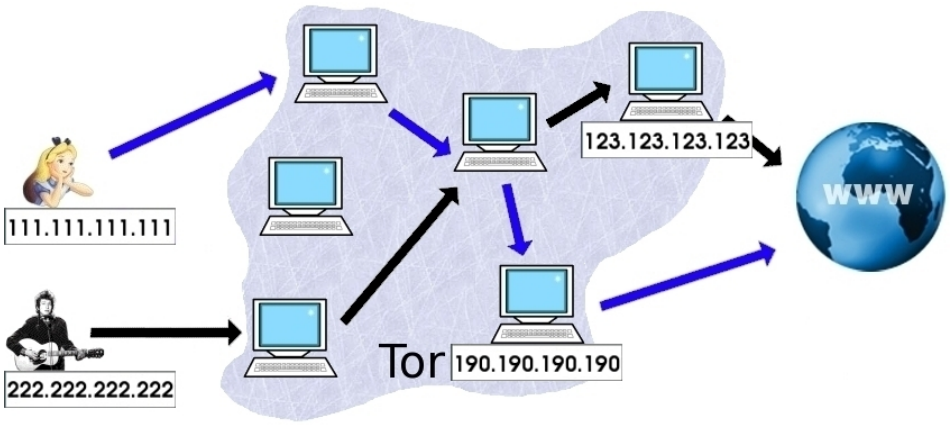

Figura 11: Percorsi dinamici di Tor.

Inoltre, una caratteristica molto importante di Tor è che permette di ottenere non soltanto forward anonymity, ma anche reverse anonymity, dal momento che chiunque può per esempio pubblicare in modo del tutto anonimo un sito web all'interno di Tor.

Due buoni punti di partenza per installare e utilizzare Tor sono il sito ufficiale [29], e la guida in italiano [23], semplice e molto esaustiva (per i più esperti invece consiglio la lettura di questo howto [43] e dell'articolo [30]). Come nel caso di Jap, i passi da eseguire sono i seguenti:

1. download e installazione di Tor, dalla sezione **Scarica** del sito ufficiale;
2. configurazione del campo "Server Proxy" sul browser, in modo che tutte le connessioni vengano inoltrate attraverso Tor;
3. avvio di Tor e configurazione dei parametri principali.

Fondamentalmente Tor è composto da tre software differenti:

- Privoxy, un proxy web che permette a Tor di essere utilizzato anche con programmi che non supportano SOCKS (Tor si basa su tale protocollo);
- Vidalia, l'interfaccia grafica;
- Tor.

L'interfaccia Vidalia permette di usare il software in modo molto semplice ed immediato, e, inoltre, a partire dall'ultimo anno è aumentata la compatibilità con le piattaforme Linux (prima durante l'installazione di Vidalia si riscontravano problemi molto frequentemente). Una delle funzionalità del programma è quella di mostrare la mappa della rete Tor, visibile in figura 12, la quale mostra il percorso fatto dai dati su scala mondiale (di default

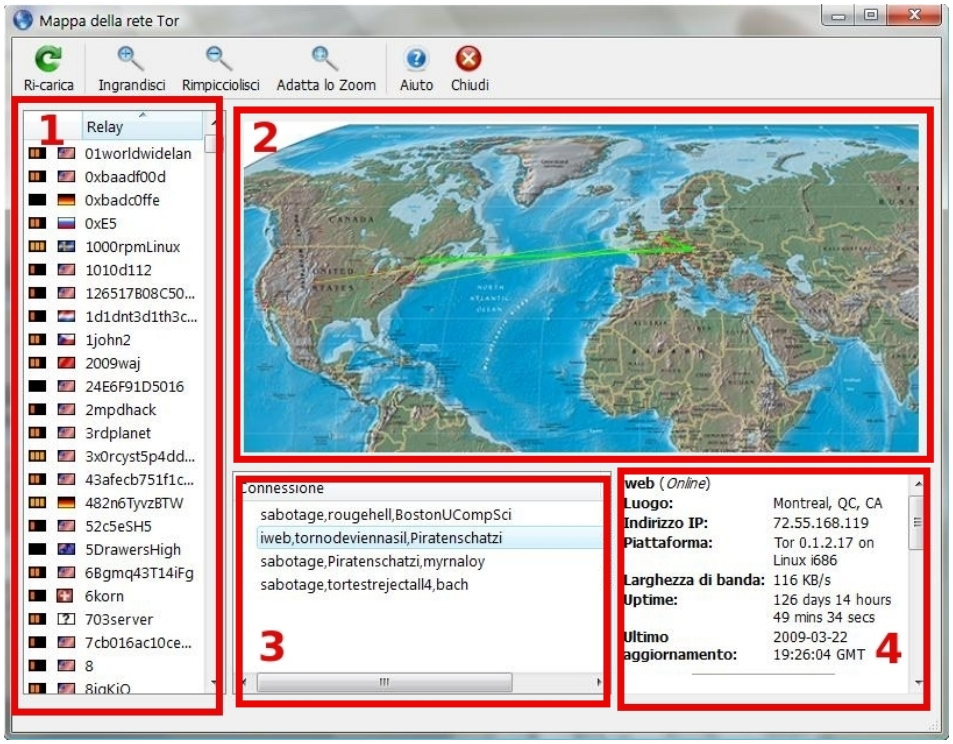

Figura 12: Mappa della rete Tor.

il percorso cambia ogni 10 minuti). La finestra è suddivisa in quattro parti principali, indicate dai numeri in rosso:

1. l'elenco di tutti i nodi della rete Tor;
2. la locazione geografica, su scala mondiale, di ogni nodo;
3. i percorsi che sono stati creati (viene mantenuto costantemente aperto più di un percorso, in modo che allo scadere dei 10 minuti l'utente non debba attendere per la creazione di un nuovo cammino);
4. i dettagli del nodo selezionato.

Inoltre, Tor non offre soltanto forward anonymity, ma anche reverse anonymity, dando la possibilità agli utenti di pubblicare un sito web (o altri servizi) all'interno della rete di computer di Tor in modo totalmente anonimo. In definitiva, Tor è un software molto completo e che ha raggiunto la sua piena maturità, liberamente utilizzabile (rispetto a Jap che nella versione free ha pesanti limitazioni), e di facile utilizzo per la navigazione tramite browser. Qualora invece si volessero rendere anonime anche altre applicazioni, come MSN, software di P2P, o torrent, allora la configurazione può richiedere qualche attenzione in più.

8.3 Altri sistemi interessanti

Oltre ai software appena citati, ne esistono molti ancora in via di sviluppo: Cebolla [4], che in italiano significa cipolla, il corrispettivo di Onion in inglese; e Tarzan [28], un sistema di file-sharing in via sperimentale, che estende la struttura delle reti di tipo mix network ad un ambiente P2P.

9 Possibili minacce ad un sistema di Anonimato

Nel contesto delle comunicazioni anonime, l'obiettivo primario di un avversario è di stabilire una corrispondenza affidabile tra un individuo e l'invio/ricezione di un particolare messaggio [39]. Un altro obiettivo potrebbe essere quello di distruggere il sistema, rendendolo inaffidabile. Questi attacchi rientrano nella categoria DoS (Denial Of Service), e sono chiamati Selective DoS qualora il target sia un utente specifico o un gruppo particolare. Un attaccante potrebbe anche tentare di ingigantire la "reputazione" degli attacchi contro il sistema di anonimato, con la speranza che il sistema venga utilizzato da meno persone. Se così dovesse essere, allora l'anonimato complessivo sarebbe ridotto, un particolare individuo non crederebbe più nel sistema, e finirebbe per usare uno strumento di comunicazione meno sicuro, o addirittura si asterrebbe dalla comunicazione [39].

Dal punto di vista della sicurezza informatica, le minacce all'anonimato possono essere suddivise a seconda delle capacità dell'avversario. Un avversario viene detto *passivo* se osserva solamente il transito dei dati sui collegamenti. Un attaccante passivo viene definito *globale* se può osservare tutti i collegamenti della rete. Gli avversari passivi e globali sono la principale minaccia per i sistemi di anonimato appartenenti alla categoria mix (vedere paragrafo 8 - Mix Network).

Un attaccante viene invece detto *attivo* se può anche inserire, modificare, o cancellare messaggi sulla rete. Una combinazione di queste capacità può essere usata per ritardare i messaggi in una rete di comunicazione anonima, o per riempire la rete di messaggi.

Inoltre, gli attaccanti possono anche arrivare a controllare un certo numero di nodi all'interno della rete anonima. In questo modo il traffico passante per questi nodi risulta trasparente all'attaccante, che può anche modificare i messaggi in transito su di essi. Il problema è di identificare tali nodi "sovvertiti", sconosciuti agli altri utenti, e questo potrebbe essere uno degli obiettivi di un protocollo di sicurezza.

Tutti i termini finora introdotti vengono solitamente usati nell'ambito della crittografia, e non permettono di identificare tutte le possibili minacce ad un sistema di comunicazione anonima. Infatti può essere definito un ulteriore tipo di attacco, tenendo conto che i sistemi di anonimato sono spesso diffusi in ambienti dove è presente un forte squilibro di potere: ogni partecipante, semplice utente o intermediario, è vulnerabile ad un attacco

di tipo *costrizione* [39]. Questi attacchi generalmente sono molti costosi per tutte le parti, e non possono essere troppo vasti o troppo numerosi.

Un esempio di tale attacco potrebbe essere quello di un tribunale che ordina di mantenere e di consegnare i file di log ad un attaccante. O ancora, un altro esempio potrebbe essere la richiesta di decriptare un particolare testo, o la richiesta dei segreti necessari a decriptarlo. Entrambi questi scenari potrebbero essere messi in atto senza alcuna autorità legale, ed adoperando unicamente la forza. Inoltre gli individui coinvolti nell'attacco potrebbero essere costretti ad eseguire determinati compiti. Come ultimo esempio consideriamo il caso in cui sia adoperato un sistema informatico per le votazioni: i partecipanti potrebbero essere costretti a votare in un certo modo.

10 Le capacità reali di intercettazione

Attualmente, le organizzazioni governative, tra cui NSA, FBI, BKA, e Polizia Postale, sono gli avversari più temibili, grazie sia ai fondi a loro disposizione, sia alla loro autorità legale al di sopra di qualsiasi giurisdizione. Molte di queste organizzazioni potrebbero essere considerate avversari passivi e globali. In aggiunta, alcune di loro hanno anche i mezzi necessari per richiedere legalmente la decriptazione di dati, o per ottenere persino le chiavi usate per la cifratura (queste considerazioni si trovano nell'UK RIP Act, ma non sono ancora effettive [35]). Spesso questi poteri sono ristretti ad una particolare area geografica e sono ancora limitati, sebbene le risorse di queste organizzazioni siano più che sufficienti.

Molto spesso anche le grandi compagnie hanno risorse paragonabili a quelle di tali organizzazioni. Tuttavia, quello che manca alle compagnie è l'autorità legale per controllare le comunicazioni, o per costringere i nodi di un sistema di anonimato a rivelare i propri segreti. Molto spesso una tecnica adottata è quella di tenere attivi alcuni nodi "sovvertiti", in modo da raccogliere informazioni sugli utenti, e in modo da poter lanciare attacchi attivi. Un esempio palese fu lo scontro tra gli utenti che scaricavano musica protetta da copyright e le compagnie discografiche: in questo caso furono inserirti alcuni nodi all'interno della rete P2P, in modo tale da conoscere quali file venivano richiesti e quali messi a disposizione. Tutte queste informazioni furono poi sfruttate per avviare numerosi processi [45].

11 Conclusioni

In definitiva, è possibile affermare che quanto visto nei film con protagonisti giovani hacker è in parte vero, anche se spesso ovviamente nei film viene tutto semplificato. Gli strumenti proposti e descritti in questa guida permettono dunque di nascondere l'identità di una persona durante le ope-

razioni in Rete, e soprattutto chiunque può raggiungere un buon livello di anonimato:

- i server proxy CGI, come The Cloak, sono consigliati a chi non ha molta dimestichezza con il pc, e a chi ricerca un sistema utilizzabile ovunque (non necessariamente sul proprio pc, ma ad esempio anche da un InternetPoint). Questa soluzione garantisce un grado di privacy piuttosto basso, ma tuttavia sufficiente per gran parte delle operazioni in Rete;

- i software basati su tecnologia VPN, come SmartHide, sono invece consigliati a chi vuole un sistema di anonimato completo, e soprattutto a chi ha intenzione di utilizzarlo frequentemente ed è disposto a pagare una quota mensile per usufruire del servizio;

- le darknet possono essere considerate il "vero" sistema di anonimato, in quanto permettono di creare una comunità di persone, separata da Internet, realmente anonime. Questo strumento è il più difficile da usare, e da configurare al meglio, e quindi è consigliato solo ad utenti che hanno bisogno di un alto livello di anonimato, e hanno le conoscenze e l'interesse per configurare correttamente il software;

- i software quali Jap/JonDo e Tor sono infine consigliati a chi vuole un sistema abbastanza semplice da usare, ma al tempo stesso dalle grandi potenzialità in termini di anonimato raggiungibile e di funzionalità (con Tor è possibile anche pubblicare siti web in modo anonimo all'interno della rete Tor, anche se questa caratteristica è consigliata agli utenti più esperti).

Concludo, come sempre, con una frase detta da Bart Simpson: "*Io non l'ho fatto, nessuno mi ha visto farlo, e non puoi provarlo in nessun modo!*"

Riferimenti bibliografici

[1] Anonymity anywhere.
`http://www.anonymityanywhere.com`.

[2] Anonymous web surfing by anonymizer.
`http://www.anonymizer.com`.

[3] Arovax smarthide.
`http://www.smarthide.com`.

[4] Cebolla - pragmatic ip anonymity.
`http://www.cypherspace.org/cebolla`.

[5] The cloak - free anonymous web surfing (server proxy cgi).
`http://www.the-cloak.com`.

[6] Come nascondere l'indirizzo ip usando http, connect, proxy cgi/php/web e sock.
`http://tools.rosinstrument.com/proxy/howto.htm`.

[7] Creative commons license.
`http://www.creativecommons.it`.

[8] Darknet anonet.
`http://anonetitalia.wordpress.com/`.

[9] The free network project.
`http://freenetproject.org`.

[10] Free proxy servers: free proxy lists, programs to work with proxies, proxy faq.
`http://www.freeproxy.info`.

[11] Gnunet - gnu's framework for secure p2p networking.
`http://gnunet.org`.

[12] Gotrusted: Secure & anonymous surfing.
`http://www.gotrusted.com/`.

[13] I2p anonymous network.
`http://www.i2p2.de`.

[14] Imule - the anonymous emule.
`http://www.imule.i2p.tin0.de`.

[15] Jap - servizio di anonimizzazione di internet.
`http://anon.inf.tu-dresden.de`.

[16] Jondonym - servizio commerciale di jap.
`http://anonymous-proxy-servers.net/`.

[17] Jondonym-status.
`http://anonymous-proxy-servers.net/en/status`.

[18] Mixmaster: A type ii anonymous remailer.
`http://www.mixmaster.it/`.

[19] Mixminion: A type iii anonymous remailer.
`http://mixminion.net/`.

[20] Multiproxy.
`http://www.multiproxy.org`.

[21] Mute: Simple, anonymous file sharing.
`http://mute-net.sourceforge.net/`.

[22] Navigazione anonima - guida di jap/jondo.
`http://proxoit.altervista.org/jap.html`.

[23] Navigazione anonima - guida di tor.
`http://proxoit.altervista.org/tor/tor.html`.

[24] Onion routing.
`http://www.onion-router.net`.

[25] Proxeasy - anonymous web proxy (server proxy cgi).
`http://www.proxeasy.com`.

[26] Sockschain.
`http://www.ufasoft.com/socks`.

[27] Stealther anonymizer.
`http://www.photono-software.de`.

[28] Tarzan - p2p anonymization.
`http://pdos.csail.mit.edu/tarzan`.

[29] Tor: anonymity online.
`http://www.torproject.org`.

[30] Tor onion routing internals: funzionamento e analisi dell'architettura.
`http://www.makeinstall.it`.

[31] Wikipedia - il concetto di anonimato.
`http://it.wikipedia.org/wiki/Anonimita`.

[32] Virtual private network, November 2008.
`http://www.p2panonimi.p2pforum.it/wiki/Virtual_Private_Network`.

[33] Carmelo Badalamenti. Tor e la sicurezza informatica, February 2007.
`http://rollsappletree.altervista.org`.

[34] Gianni Bianchini and Alessandro Lori. Tecnologie emergenti per la privacy e l'anonimato in rete. In *Smau/E-Academy*, October 2005.

[35] The Stationery Office Books. *Regulation of Investigatory Powers Act 2000*. The Stationery Office Books, August 2000. ISBN 0105423009.

[36] Marco Calamari. Freenet: 2 anni dopo. In *Linux Day*, November 2002.

[37] Marco Calamari. Cassandra crossing/ invisibile internet project, September 2006.
`http://punto-informatico.it/1659085/PI/Commenti/cassandra-crossing-invisibile-internet-project.aspx`.

[38] Marco Calamari. Cassandra crossing/ lo stato delle pet, December 2006.
`http://punto-informatico.it/1811559/PI/Commenti/cassandra-crossing-stato-delle-pet.aspx`.

[39] George Danezis. *Better Anonymous Communications*. PhD thesis, University of Cambridge, July 2004.

[40] Maurizio DelVecchio. Guida di base all'utilizzo dei proxy, December 2007.
`http://forum.zeusnews.com/viewtopic.php?t=27739`.

[41] Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *Proceedings of the 13th USENIX Security Symposium*, August 2004.

[42] Gwren. Ants p2p.
`http://antsp2p.sourceforge.net`.

[43] Uwe Hermann. Howto: Anonymous communication with tor, June 2006.
`http://www.hermann-uwe.de/blog`.

[44] Nazzareno Schettino. Proxy list navigazione anonima.
`http://www.notrace.it/proxy-list.asp`.

[45] Tony Smith. European riaa-style anti-file swap lawsuits 'inevitable', December 2003.
`http://www.theregister.co.uk/content/6/34547.html`.

[46] Paul Syverson. Making anonymous communication. In *National Science Foundation*, June 2004.