TOR: Privacy e Anonimato in rete

Marco Bonetti

28 Ottobre 2006

http://www.lugpiacenza.org/
http://www.linux.it/LinuxDay/main.shtml

Benvenuti

- *“There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files. This book is about the latter.”* Bruce Schneider, Applied Cryptography
  http://www.schneier.com/book-applied-2preface.html
- *“Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet. It also enables software developers to create new communication tools with built-in privacy features. Tor provides the foundation for a range of applications that allow organizations and individuals to share information over public networks without compromising their privacy.”* Tor: Overview
  http://tor.eff.org/overview.html

Perché tor?

- Maggiore sicurezza della trasmissione dei dati su TCP
- Maggiore privacy durante le comunicazioni interpersonali
- Tecniche di fuga
- Maggiore robustezza della connessione a Internet
- Protezione dall'analisi del traffico

Analisi del traffico

- La raccolta di dati riguardanti le comunicazioni permette di ricostruire il profilo degli interessi e dei gusti dei partecipanti
- Dimmi dove vai e ti dirò chi sei ;-)
- Esempi di analisi del traffico:
  - Un sito di e-commerce può applicare prezzi differenti a seconda del paese di origine del visitatore
  - Controllare la posta dall'estero permette di scoprire da dove si proviene o chi si è
- L'impiego di protocolli insicuri (smtp, vnc, telnet) lascia filtrare troppe informazioni

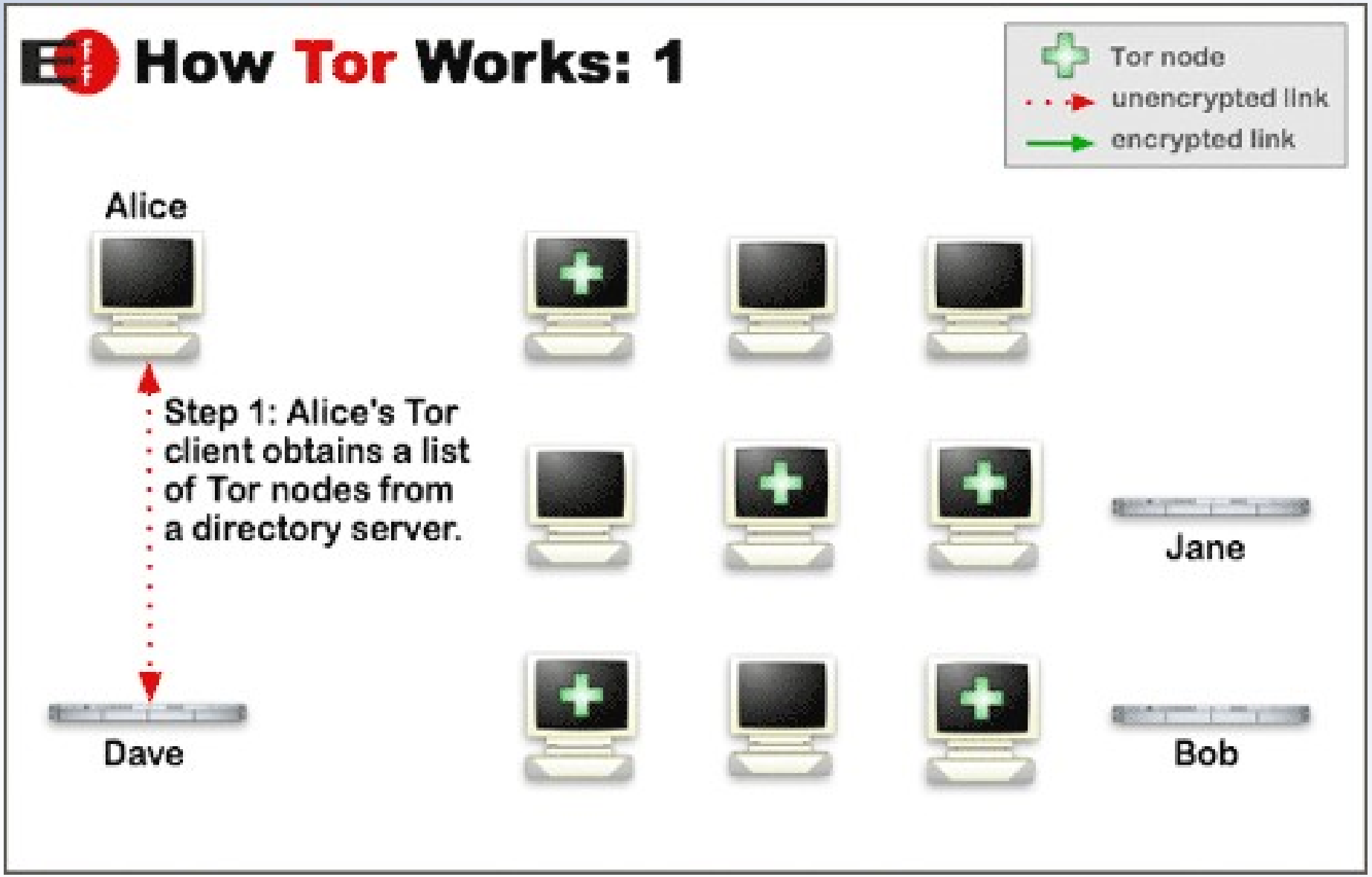
Una prima soluzione

- I pacchetti che viaggiano in Internet sono composti da:
  - Header, contiene le informazioni di instradamento
  - Payload, contiene i dati
- Se riesco a criptare il payload nessuno può “leggere” il contenuto della mia sessione
- È vero, ma questa tecnica da sola non è sufficiente a proteggermi: l'header contiene ancora troppe informazioni
- Allora cripto anche l'header!
- Provateci... ;-)

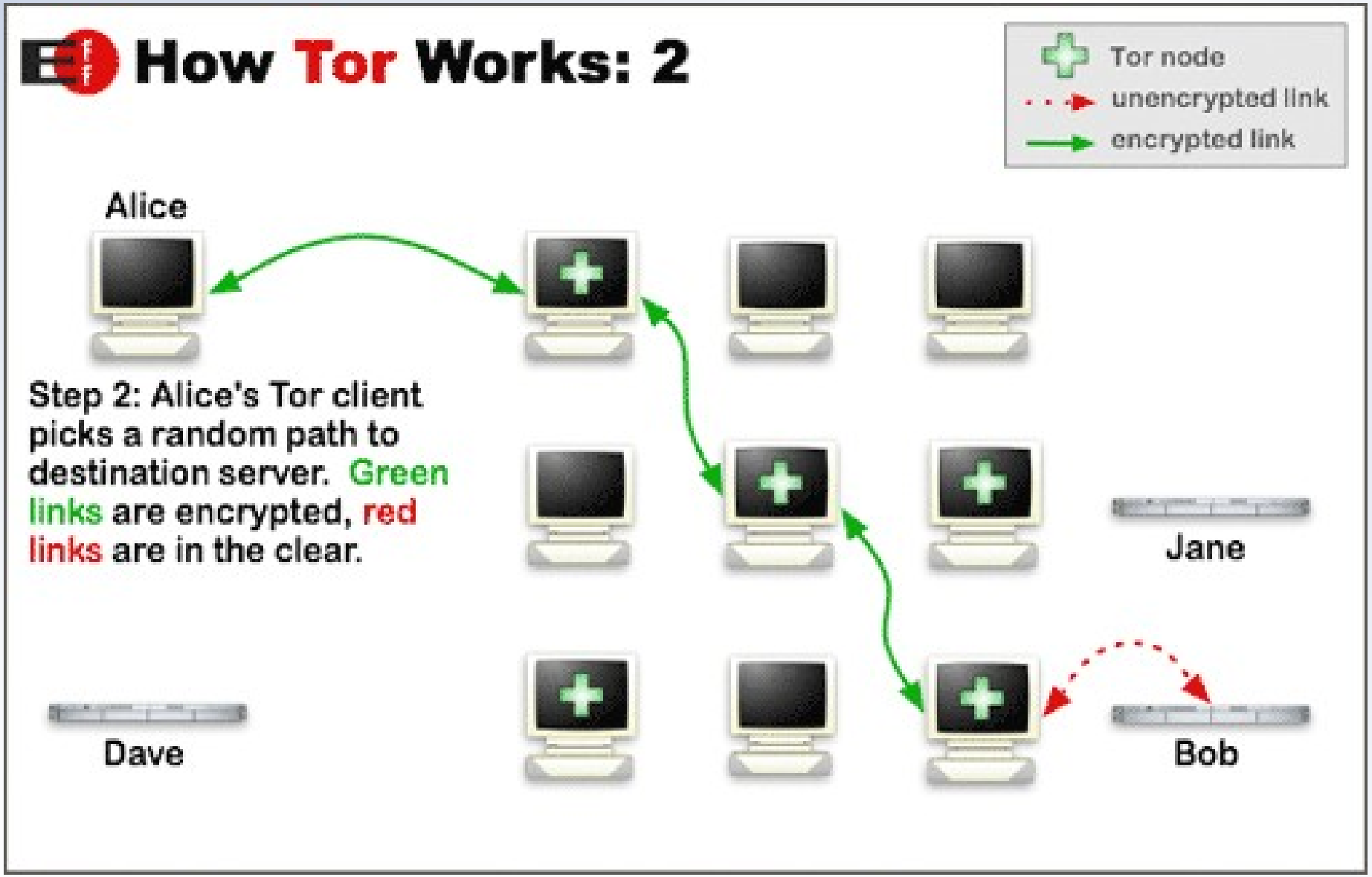
La soluzione proposta da tor

- Creiamo una rete di nodi parallela a Internet per l'instradamento dei pacchetti
- La rete di tor funziona come una scatola nera (black box): i pacchetti che vi entrano scompaiono e appaiono “auto magicamente” all'uscita, dopo aver percorso un viaggio all'interno della rete parallela
- L'idea è quella di raggiungere la destinazione cancellando le tracce che ci lasciamo dietro, in modo da rendere impossibile l'analisi del traffico
- Come accade la magia?

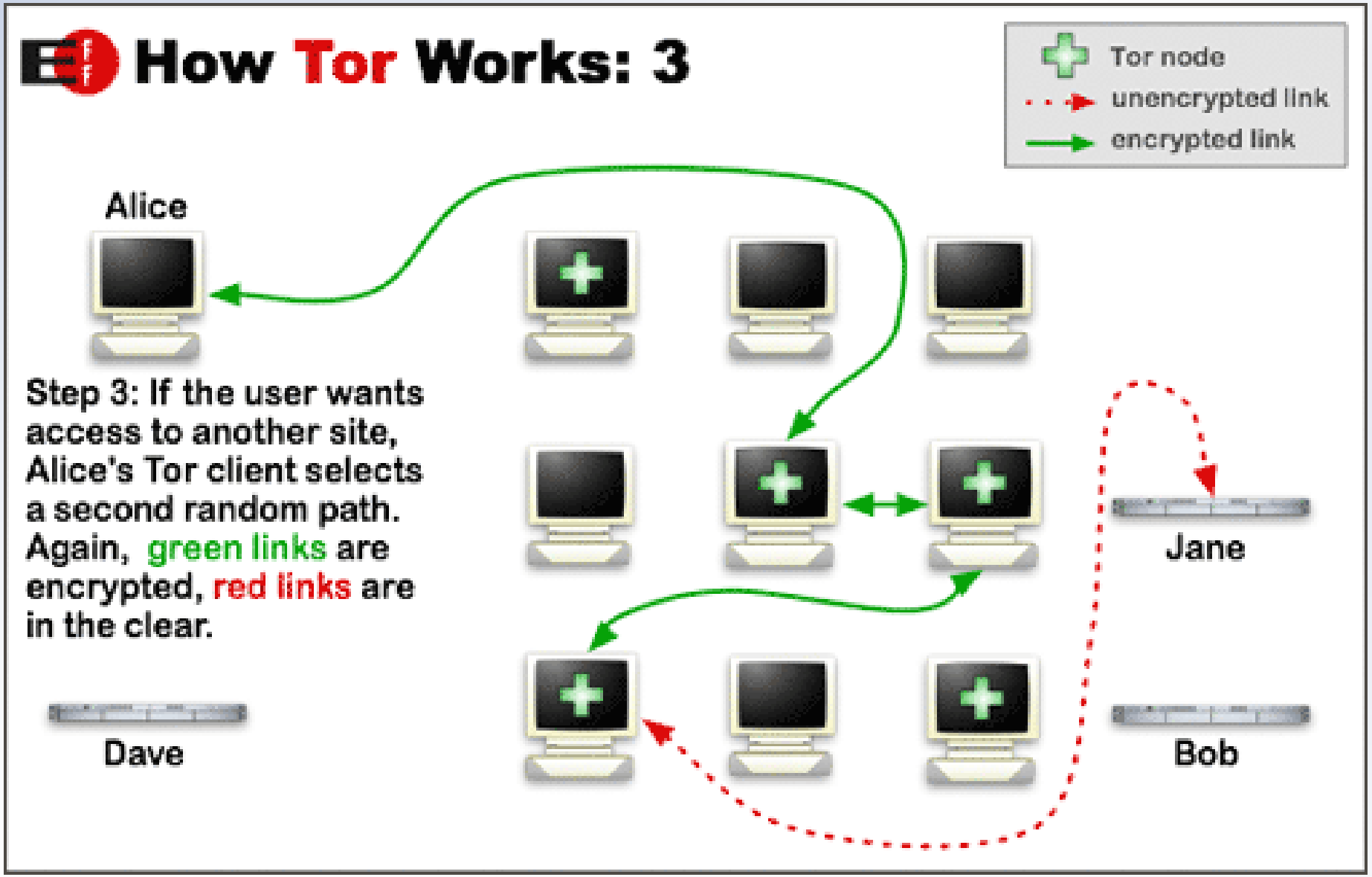
La magia -1


How Tor Works: 1
Tor node
unencrypted link
encrypted link
Alice
Step 1: Alice's Tor client obtains a list of Tor nodes from a directory server.
Dave
Jane
Bob

La magia - 2


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

La magia - 3


How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Cipolle!

- Avete capito perché si chiama “router a cipolla”?
- One-hop routing: ogni nodo conosce solo che un pacchetto gli arriva dal nodo a monte e devo consegnarlo al nodo a valle
- I nodi intermedi non possono leggere il contenuto del payload di partenza
- In questo modo riusciamo a fuggire dalle tecniche di analisi del traffico in quanto non è possibile risalire agli attori del dialogo senza riuscire a leggere TUTTO il traffico che viaggia all'interno della rete di tor e, anche in questo malaugurato caso, non si avrebbe la certezza matematica dell'individuazione dei partecipanti ma solo una approssimazione.

Spingersi oltre

- Perché limitarsi a oscurare le comunicazioni?
- Nascondere i servizi!
- Un server tor è in grado di pubblicare informazioni riguardanti particolari servizi (sito web, server IM) offerti esclusivamente ad altri utenti tor
- Questi servizi (gli “hidden service”) non sono visibili dall'esterno ma solo dalla rete torificata

Installare tor

- Tor è free software sotto la 3-clause BSD e liberamente scaricabile all'indirizzo http://tor.eff.org/download.html.en
- Il sito fornisce anche chiare e approfondite spiegazioni sull'installazione per ogni architettura supportata
- Tor viene installato come un socks proxy (127.0.0.1:9050) lanciato automaticamente all'avvio
- Non c'è differenza tra il programma client e quello server, solo che il secondo caso deve essere esplicitamente configurato dall'utente

Tor in pratica -web

- La navigazione via web è semplice da anonimizzare: basta selezionare 127.0.0.1:9050 come socks proxy v4a oppure v5 per il proprio browser
- Tor viene distribuito accoppiato con Privoxy, un proxy http/https che esegue information stripping delle richieste del browser in modo da aumentare la confidenza della propria sessione e diminuire le informazioni raccolte dal server finale

Tor in pratica – IM e IRC

- I maggiori protocolli di instant messagging forniscono la possibilità di utilizzare proxy http e /o socks per la comunicazione, basta utilizzarli attraverso tor o privoxy
- Un buon compagno di tor+IM è l'utilizzo dei plugin OTR http://www.cypherpunks.ca/otr/ in modo di accertarsi dell'identità dell'altro interlocutore
- Purtroppo non è così semplice utilizzare tor+IRC, la maggior parte dei server blocca l'accesso via proxy dei client per motivi di ordine pubblico
- Freenode fornisce ben due hidden server per la propria rete: mejokbp2brhw4omd.onion per l'accesso libero e 5t7o4shdbhotfuzp.onion per quello autenticato, entrambi sulla porta 6667

Tor in pratica - P2P

- Non ha molto senso torificare il flusso di informazioni di un programma P2P, effetto leech.
- Il protocollo più flessibile è BitTorrent
  - Il metodo più comune è torificare le informazioni scambiate con il tracker e lasciare in chiaro le connessioni ai peer, sia bittorrent (l'originale) che Azureus e gli altri client supportano l'impiego di socks e http proxy
  - Il secondo metodo è impiegare una rete di filesharing completamente torificata, con il tracker come hidden service, funziona ma impatta negativamente sulle performance globali della rete

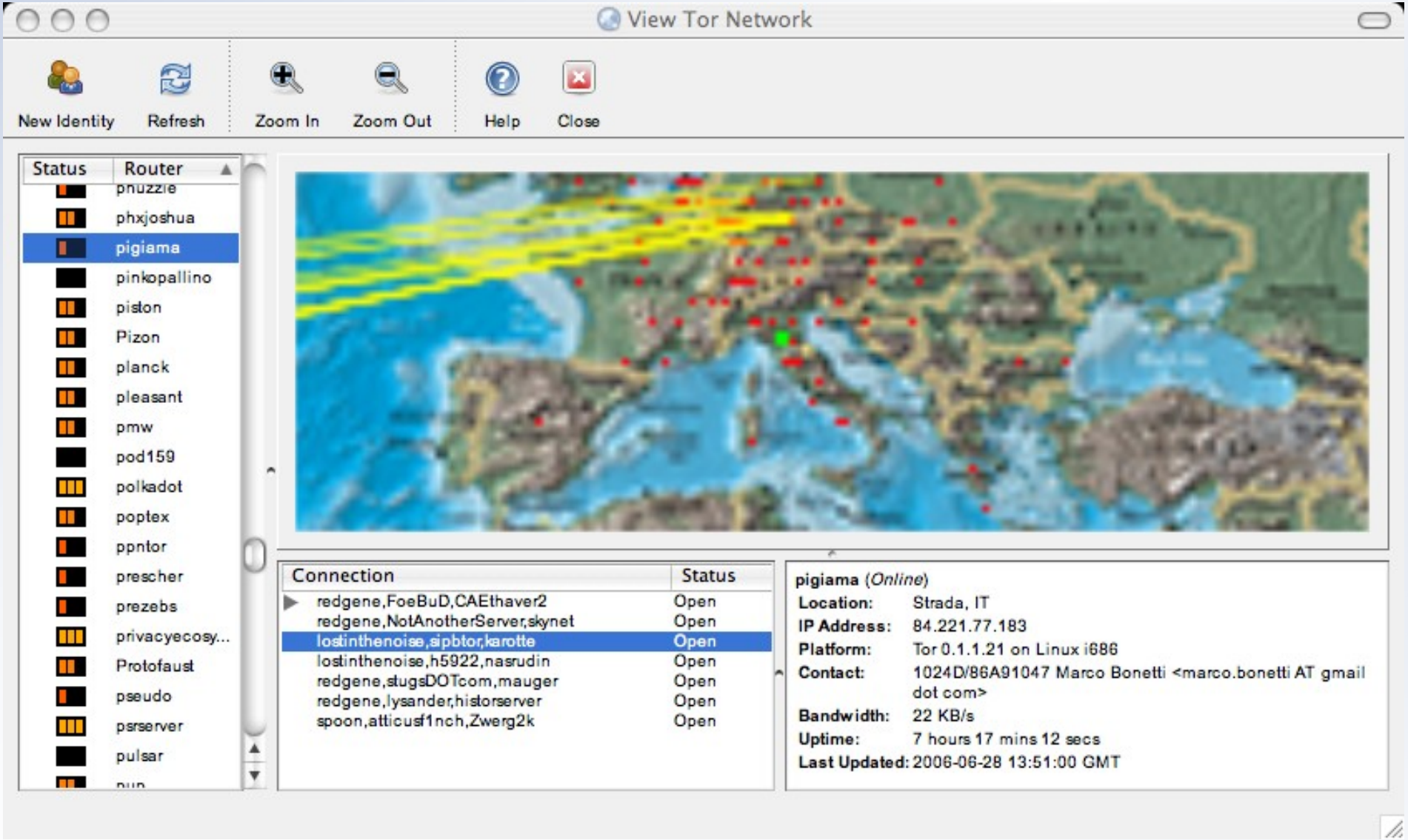
Tor in pratica – il resto

- I client openssh supportano nativamente l'utilizzo di programmi proxy, con tor è utile impiegare http://zippo.taiyo.co.jp/~gotoh/ssh/connect.html
- Non tutti i programmi supportano nativamente l'utilizzo di proxy
- Tsocks (linux e *bsd) permette di wrappare le chiamate di sistema alla funzione connect() in modo da instradarla attraverso un socks proxy, è un metodo brutale ma funziona
  - tsocks nc $IP $PORT
  - tsocks links http://serifos.eecs.harvard.edu/cgi-bin/ipaddr.pl?tor=1
- http://shellscripts.org/project/toraliases/

Tor server

- La rete tor funziona solamente grazie alla buona volontà degli utilizzatori che decidono di impiegare la propria macchina anche come server
- Se si hanno almeno 20KB di banda in upload e download è consigliabile settare un server tor
- Le istruzioni si trovano all'indirizzo http://tor.eff.org/docs/tor-doc-server.html.en
- Si può scegliere quale porte permettere in uscita dalla propria macchina
- Per chi non ha un abbonamento flat è possibile selezionare le finestre orarie di utilizzo della banda oppure una quota di banda totale mensile
- Per non incidere troppo sulle performance della rete locale si possono settare i picchi di utilizzo

Un nuovo nato



Attacchi alla rete

- **This is not a "crackdown on Tor"**, as has been widely reported. This seems to be part of a wide sweep on computers associated by IP address with a large child porn bust. There does not seem to be any specific targeting of Tor — Tor is used by journalists, human rights activists, dissident bloggers, and a vast array of blameless users. http://tor.eff.org
- Tor <= 0.1.22 dossabile
- Rogue nodes
- Phoning home http://wiki.noreply.org/noreply/TheOnionRouter/TorFAQ#he

Fine