Tor: alla scoperta dei router a cipolla

Marco Bonetti
marco.bonetti@slackware.it

22 Agosto 2008

MOCA 2008 - Pescara

Licenza

Outline

- Tor: the second-generation onion router
- Funzionamento di Tor
- Tor in pratica

- Tor: the second-generation onion router

Cronologia

- Anni '80: David Chaum teorizza e implementa le “mix networks”, catene di proxy server
- Anni '90: lo United States Naval Research Laboratory si interessa alla materia e sviluppa la tecnologia dell'onion routing
  - Onion Routing briefing slides, 1996
  - "Hiding Routing Information," Information Hiding, R. Anderson (editor), Springer-Verlag LLNCS 1174, 1996, pp. 137-150
- Oggi: “Tor: The Second-Generation Onion Router”, Venerdì 13 Agosto 2004 @ 13th USENIX Security Symposium

Cosa è Tor?

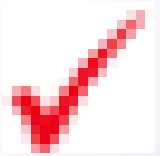
- Uno strumento per persone e organizzazioni che voglio migliorare la loro sicurezza in internet
- Un programma per anonimizzare la navigazione, la pubblicazione di contenuti, lo scambio di messaggi, IRC, SSH e altre applicazioni che usano il protocollo TCP
- Una piattaforma per sviluppare nuovi programmi dotati di caratteristiche di anonimità, sicurezza e privacy

Perchè usare Tor?

- 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 ;-)
- L'impiego di protocolli insicuri (smtp, vnc, telnet) lascia filtrare troppe informazioni
- 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

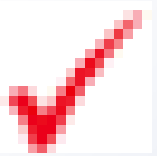
- Tor: the second-generation onion router
- Funzionamento di Tor

Una prima soluzione



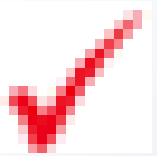
- I pacchetti che viaggiano in Internet sono composti da:
  - Header, contiene le informazioni di instradamento
  - Payload, contiene i dati

Una prima soluzione



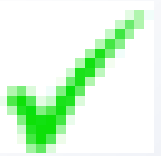
- I pacchetti che viaggiano in Internet sono composti da:
  - Header, contiene le informazioni di instradamento
  - Payload, contiene i dati
- Se riesco a criptare il payload nessuno può “leggere” il contenuto della mia sessione
- È vero, ma questa tecnica da sola non è sufficiente a proteggermi: l'header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

Una prima soluzione



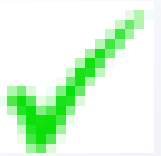
- I pacchetti che viaggiano in Internet sono composti da:
  - Header, contiene le informazioni di instradamento
  - Payload, contiene i dati
- Se riesco a criptare il payload nessuno può “leggere” il contenuto della mia sessione
- È vero, ma questa tecnica da sola non è sufficiente a proteggermi: l'header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

La soluzione proposta da Tor



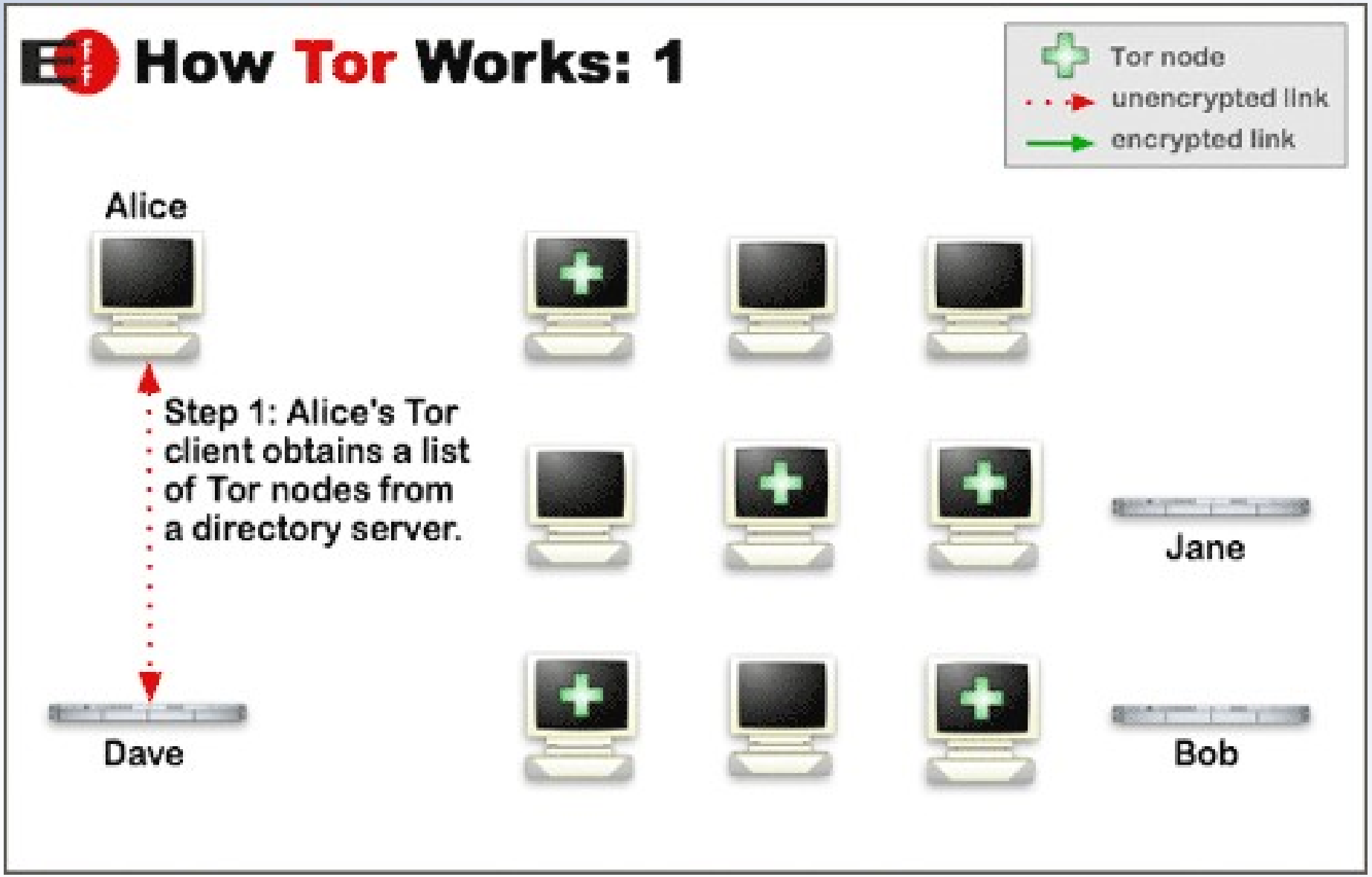
- Creiamo una rete di nodi parallela a Internet per l'instradamento dei pacchetti
- La rete di Tor funziona come una scatola nera (black box): i pacchetti che vi entrano scompaiono e appaiono “auto magicamente” all'uscita, dopo aver percorso un viaggio all'interno della rete parallela
- L'idea è quella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

La soluzione proposta da Tor

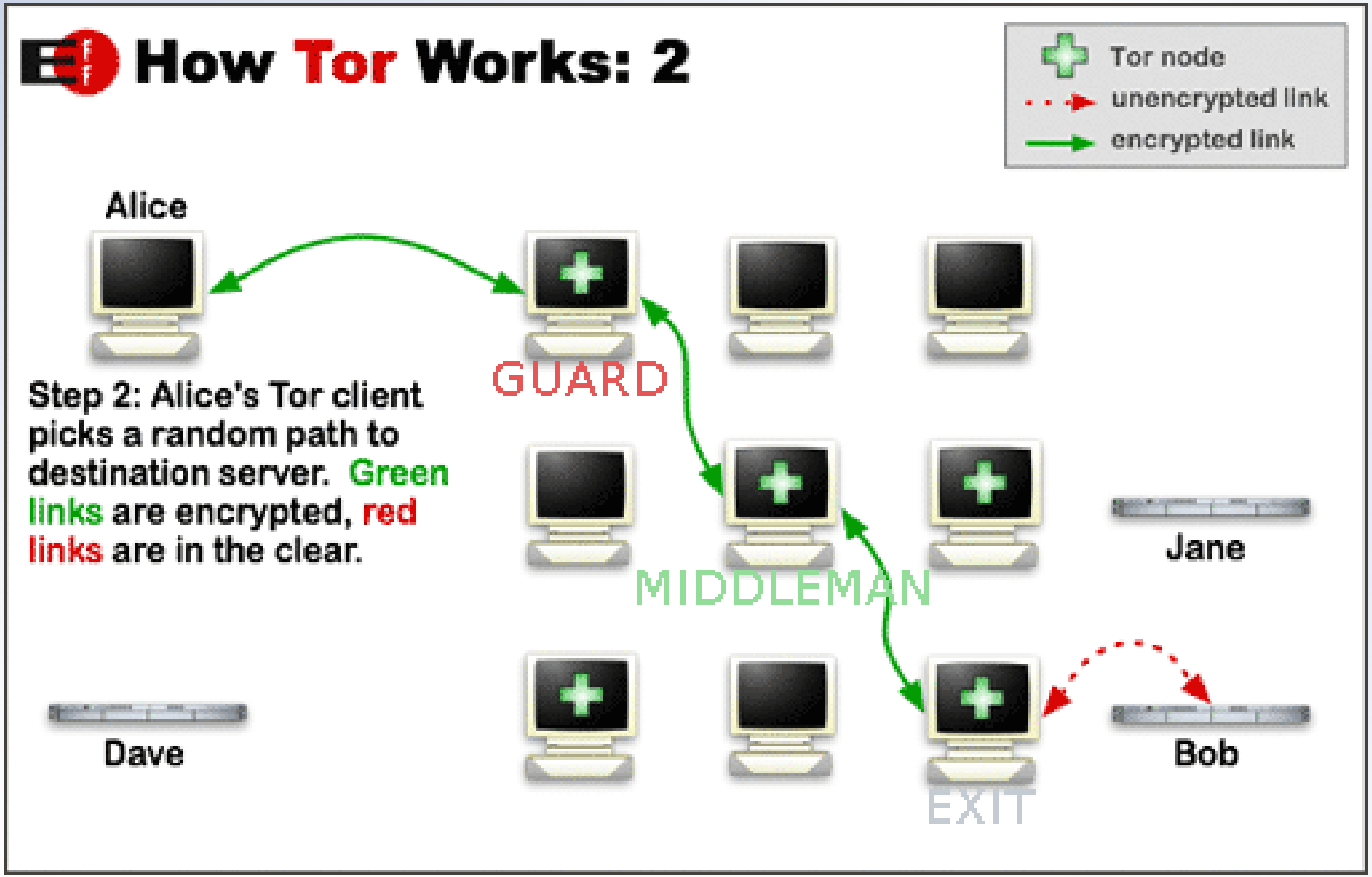


- Creiamo una rete di nodi parallela a Internet per l'instradamento dei pacchetti
- La rete di Tor funziona come una scatola nera (black box): i pacchetti che vi entrano scompaiono e appaiono “auto magicamente” all'uscita, dopo aver percorso un viaggio all'interno della rete parallela
- L'idea è quella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

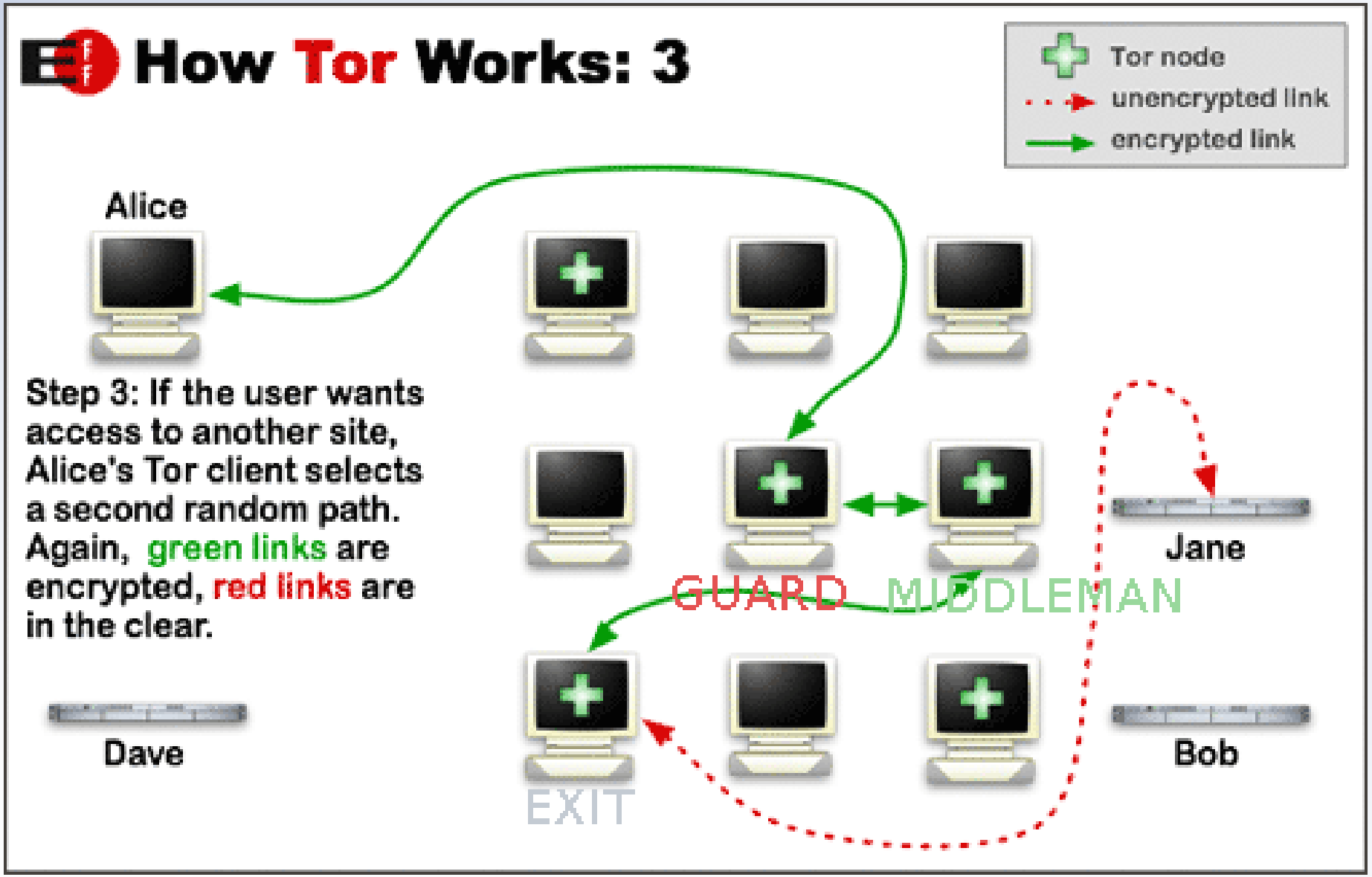
La magia – 1


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

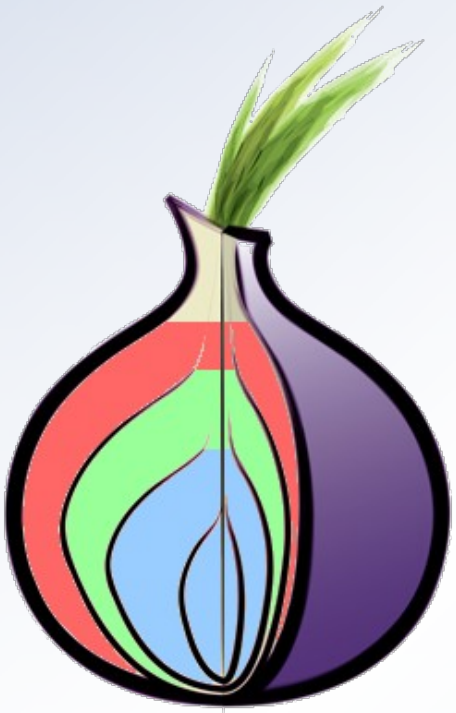
La magia – 2


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

La magia - 3

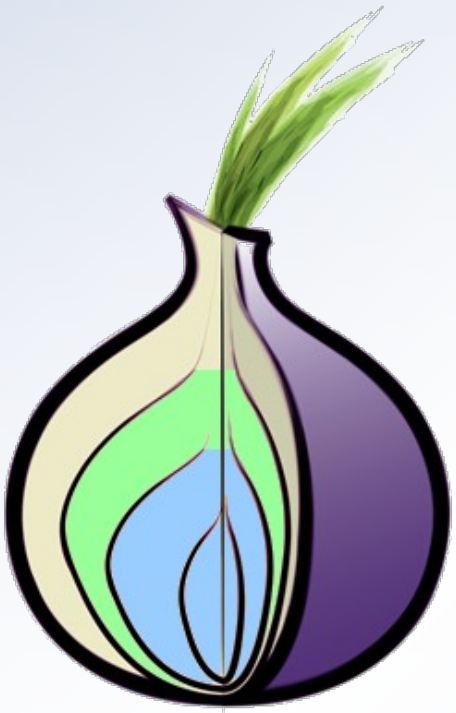

How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
GUARD
MIDDLEMAN
Dave
EXIT
Bob

Creazione di un circuito - 1



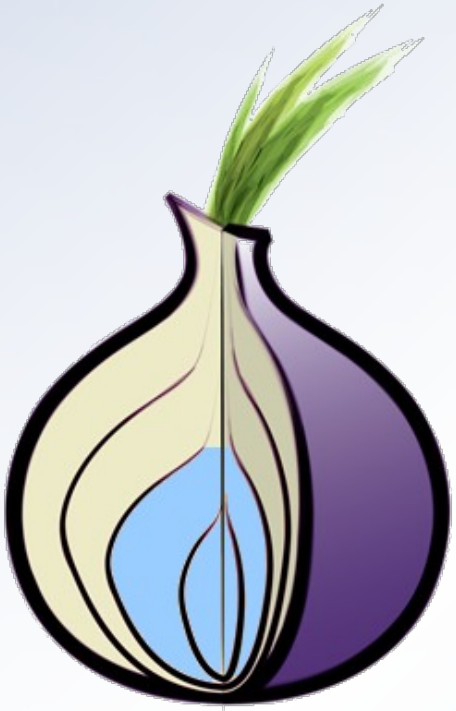
- Il client invia al nodo di guardia (GUARD) il pacchetto completo
- Il nodo di guardia decritta il primo strato e individua il nodo di transito a cui inviare il rimanente payload

Creazione di un circuito - 2



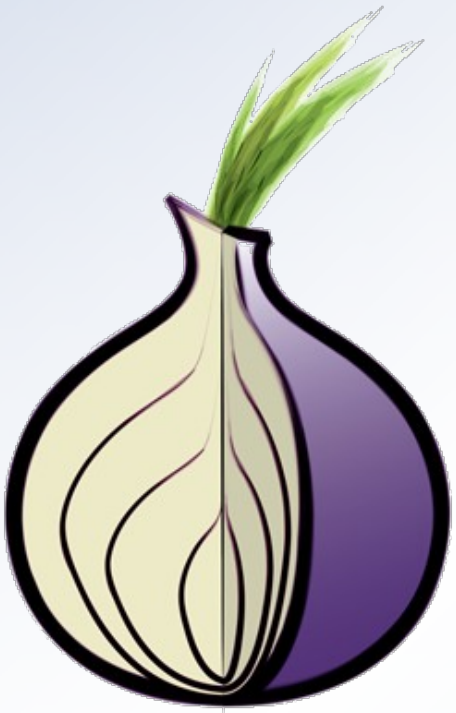
- Il nodo di transito (MIDDLEMAN) riceve dal guardiano il payload ridotto
- Come nel caso precedente, decritta lo strato di sua competenza per conoscere quale sarà il prossimo nodo a cui inviare il resto del payload

Creazione di un circuito - 3



- Il nodo di uscita (EXIT) riceve le istruzioni finali per la creazione del circuito
- Decrittando le informazioni ricevute, il nodo individua la macchina da contattare e la specifica richiesta da inviare

Creazione di un circuito - 4



- Il circuito è completo!
- Con le informazioni ottenute al passaggio precedente, il nodo di uscita si collega alla macchina finale e chiede le informazioni volute dal client di partenza
- Una volta ottenuta una risposta provvederà ad inoltrarla all'indietro, utilizzando il circuito appena stabilito

Cipolle!

- Avete capito perché si chiama “router a cipolla”?

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 destinazione
- 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

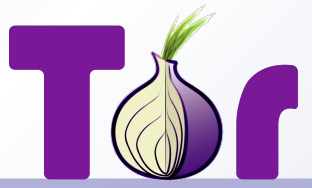
- Perché limitarsi a oscurare le comunicazioni?
- Nascondere i servizi!
- Un server Tor è in grado di pubblicare informazioni riguardanti particolari servizi (sito web, server IM) offerti esclusivamente ad altri utenti Tor
- Questi servizi (gli “hidden service”) non sono visibili dall'esterno ma solo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

- Tor: the second-generation onion router
- Funzionamento di Tor
- Tor in pratica

Installare Tor – il client

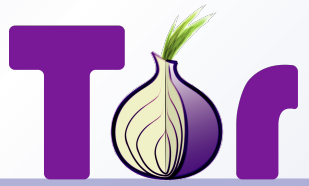
- Tor è free software rilasciato sotto la 3-clause BSD
- Liberamente scaricabile all'indirizzo https://www.torproject.org/download.html.en
- Il client ascolta su **localhost** sulle seguenti porte:
  - porta 9050 per il proxy SOCKS v. 4/4A/5
  - porta 9051 per la control port (opzionale)
- Se si è installato il bundle, ci si trova anche il proxy http Privoxy in ascolto su **localhost**:8118
- Non serve aprire porte sui router/firewall!

Installare Tor – il server



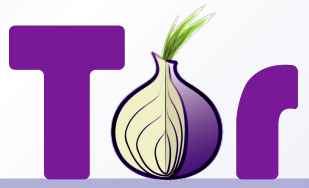
- Non c'è differenza tra il programma client e quello server, solo che il secondo caso deve essere esplicitamente configurato dall'utente
- Il server ascolta **all'esterno** su diverse porte:
  - porta 9001 (443) per la creazione di circuiti
  - porta 9030 (80) per fornire servizio directory (opzionale)
  - porta 9040 per eseguire transparent proxying (opzionale)
- Permette il relay di traffico verso e fuori dalla rete Tor
- Permette la gestione di hidden services
- Ora potete controllare le porte dei vostri firewall/router ;-)

Configurare un Tor server - 1



- 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://www.torproject.org/docs/tor-doc-relay

Configurare un Tor server - 2



- 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

Web - 1

- La navigazione via web è semplice da anonimizzare: basta selezionare 127.0.0.1:9050 come socks proxy per il proprio browser
- L'utilizzo della versione 4a rispetto alla 4 o alla 5 è importante per inteccettare le richieste DNS

Web - 2

- Tor viene distribuito accoppiato con Privoxy e TorButton
  - Privoxy è un proxy http/https
    - usato in cascata prima di Tor
    - esegue information stripping delle richieste
    - rimuove ads e simili
    - NO http pipelining :'(
      - provate Polipo ;-)
  - TorButton è un plugin per Firefox
    - imposta automaticamente il browser per l'utilizzo di Tor
    - esegue una serie di controlli aggiuntivi volti a limitare al massimo il filtraggio di informazioni
      - blocca js/plugin/updates
      - isola sessioni
      - gestisce i cookies

IM

- 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 del plugin OTR http://www.cypherpunks.ca/otr/

IRC

- 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: irc://mejokbp2brhw4omd.onion/ per l'accesso autenticato via GPG e irc://5t7o4shdbhotfuzp.onion/ per l'acceso libero (down durante i periodi di abuso)

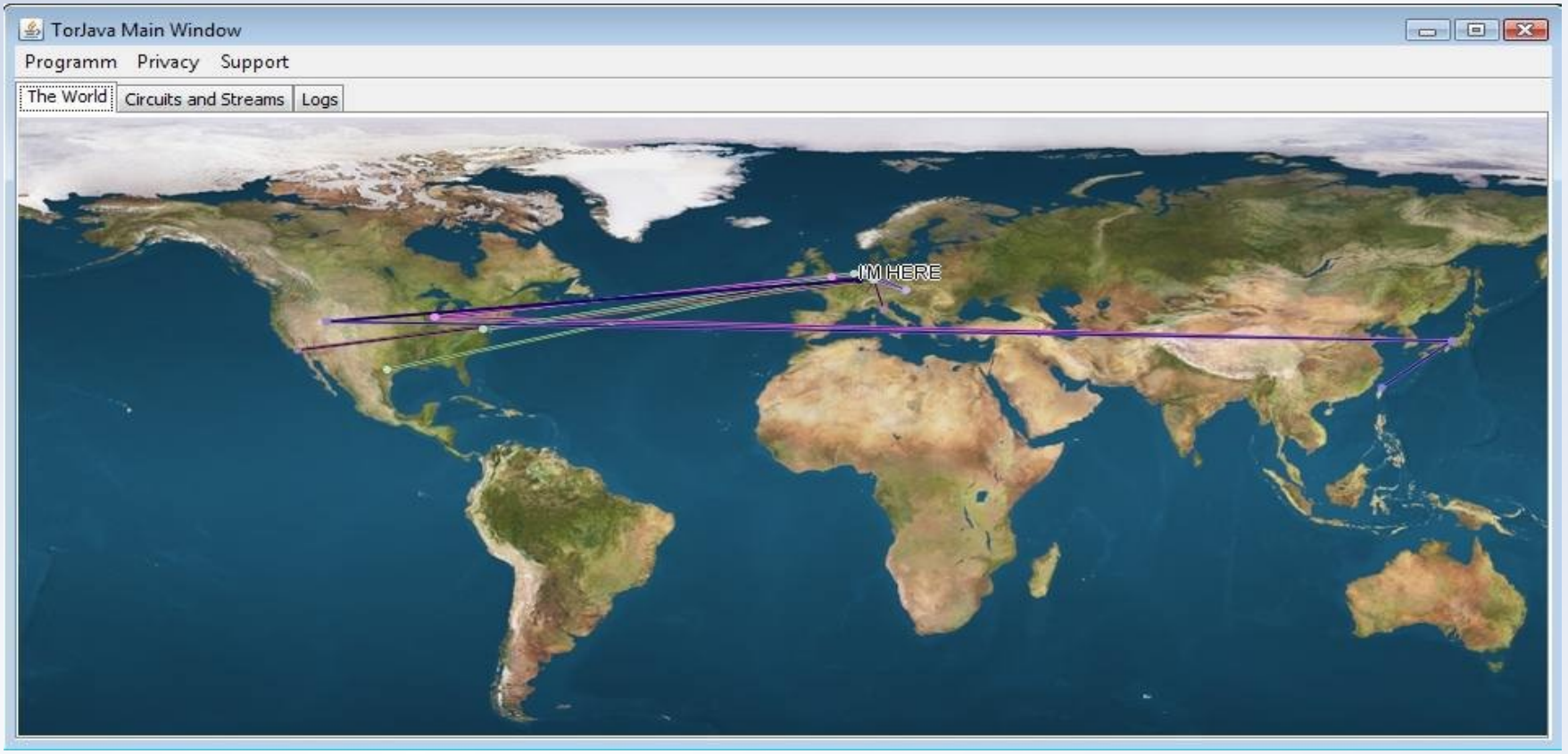
P2P

- 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

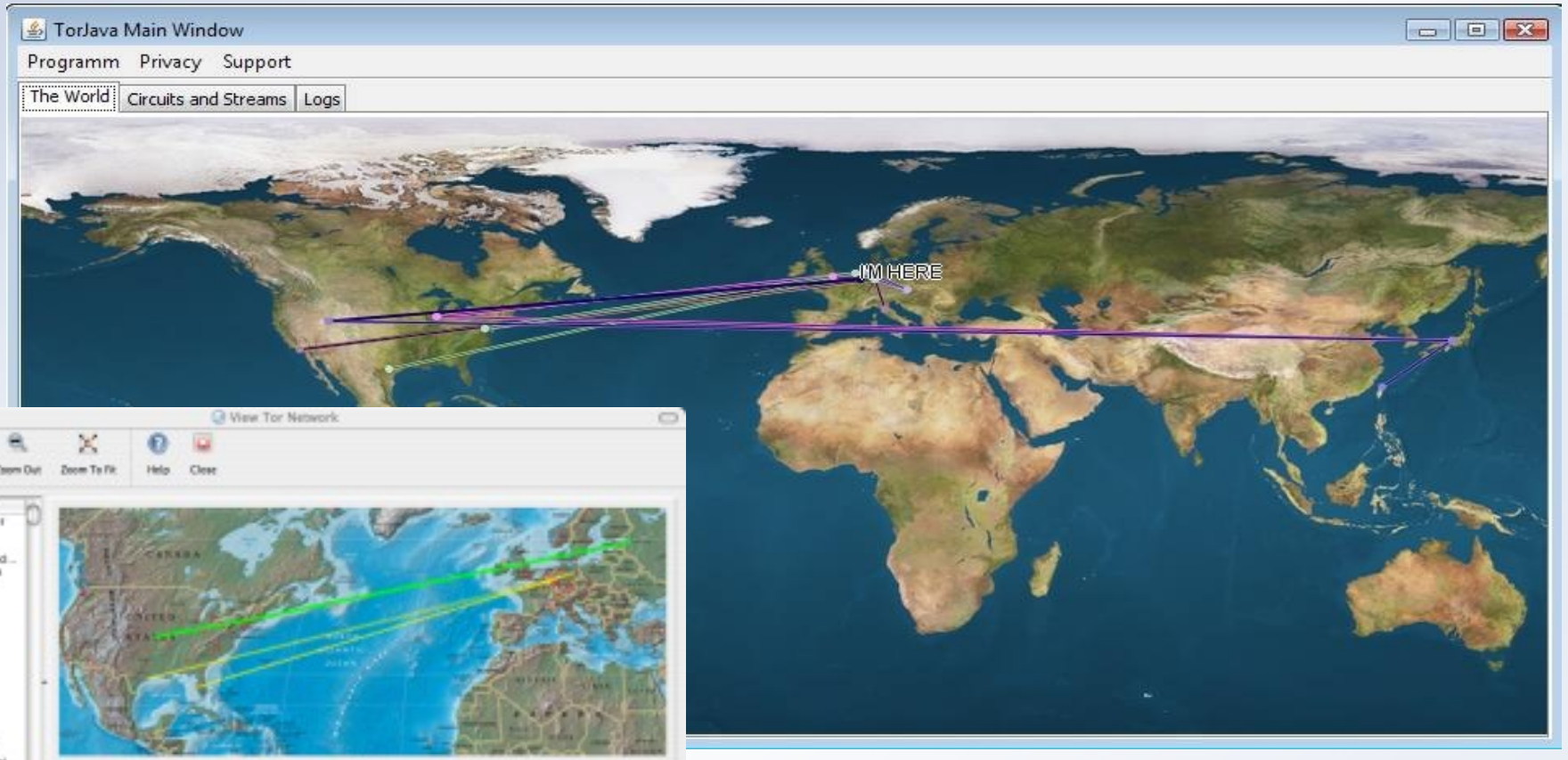
Il resto

- Il protocollo ssh prevede l'utilizzo di programmi proxy, con Tor e OpenSSH è utile impiegare un proxy command come Connect: http://www.meadowy.org/~gotoh/projects/connect
- 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://www.google.com/
- Per tutti gli altri: http://shellscripts.org/project/toraliases/

Il futuro

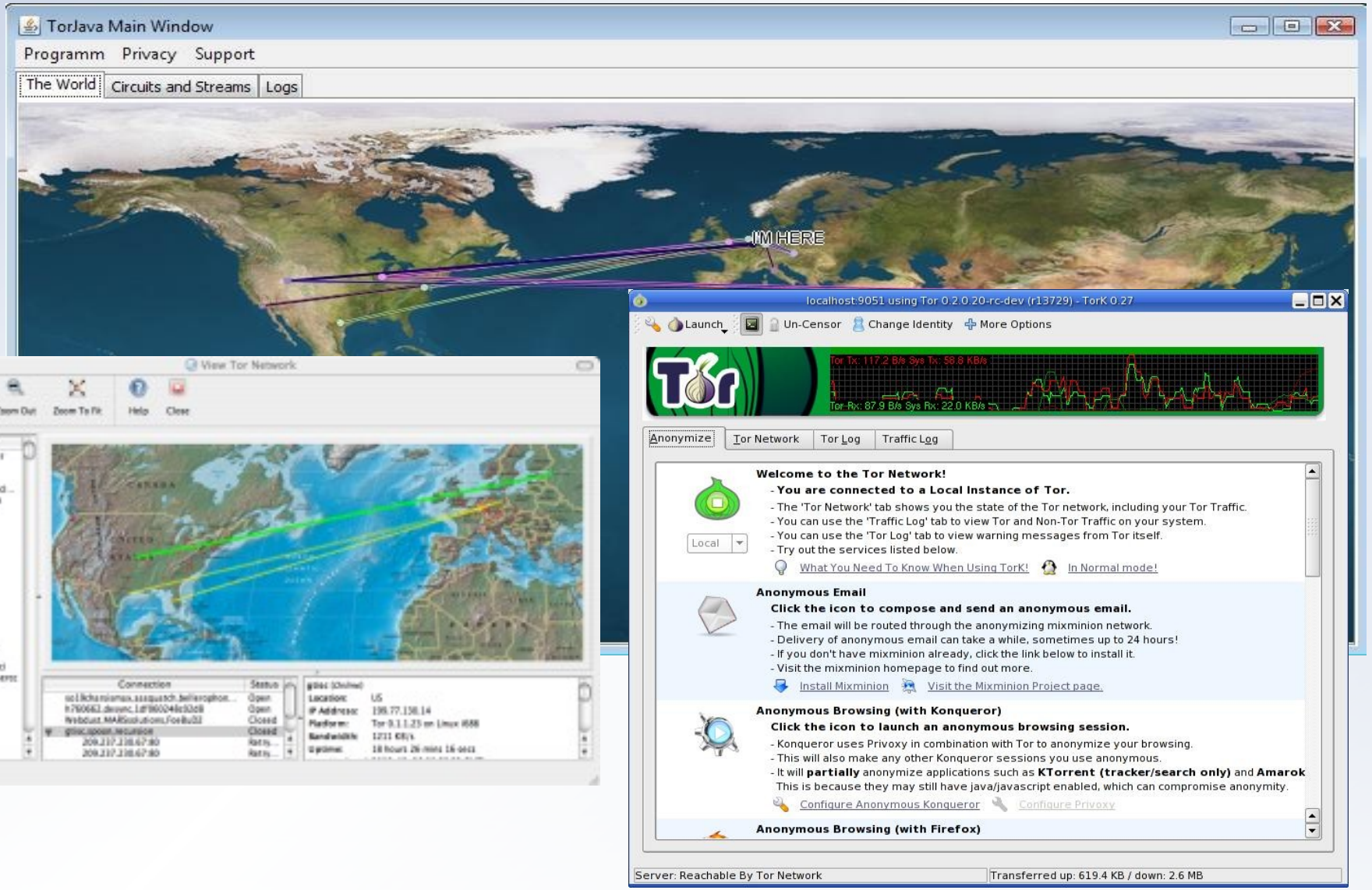

TorJava Main Window
Programm
Privacy
Support
The World
Circuits and Streams
Logs
I'M HERE

Il futuro


TorJava Main Window
Programm Privacy Support
The World
Circuits and Streams
Logs
I'M HERE

View Tor Network
Refresh
Zoom In
Zoom Out
Zoom To Fit
Help
Close
Server
Connection
Status

Il futuro


TorJava Main Window
Programm Privacy Support
The World
Circuits and Streams
Logs
I'M HERE
View Tor Network
Refresh
Zoom In
Zoom Out
Zoom To Fit
Help
Close
Server
Connection
Status
localhost:9051 using Tor 0.2.0.20-rc-dev (r13729) - TorK 0.27
Launch
Un-Censor
Change Identity
More Options
Tor Tx: 117.2 B/s Sys Tx: 58.8 KB/s
Tor Rx: 87.9 B/s Sys Rx: 22.0 KB/s
Anonymize
Tor Network
Tor Log
Traffic Log
Welcome to the Tor Network!
- You are connected to a Local Instance of Tor.
- The 'Tor Network' tab shows you the state of the Tor network, including your Tor Traffic.
- You can use the 'Traffic Log' tab to view Tor and Non-Tor Traffic on your system.
- You can use the 'Tor Log' tab to view warning messages from Tor itself.
- Try out the services listed below.
Local
What You Need To Know When Using TorK!
In Normal mode!
Anonymous Email
Click the icon to compose and send an anonymous email.
- The email will be routed through the anonymizing mixminion network.
- Delivery of anonymous email can take a while, sometimes up to 24 hours!
- If you don't have mixminion already, click the link below to install it.
- Visit the mixminion homepage to find out more.
Install Mixminion
Visit the Mixminion Project page.
Anonymous Browsing (with Konqueror)
Click the icon to launch an anonymous browsing session.
- Konqueror uses Privoxy in combination with Tor to anonymize your browsing.
- This will also make any other Konqueror sessions you use anonymous.
- It will partially anonymize applications such as KTorrent (tracker/search only) and Amarok
This is because they may still have java/javascript enabled, which can compromise anonymity.
Configure Anonymous Konqueror
Configure Privoxy
Anonymous Browsing (with Firefox)
Server: Reachable By Tor Network
Transferred up: 619.4 KB / down: 2.6 MB

Ringraziamenti

- A Roger Dingledine, Nick Mathewson, Peter Palfrader, tutti gli altri sviluppatori di Tor e la EFF per portare avanti un tale progetto
- A Ren Bucholz per le immagini di “How Tor works”
- A Mike Perry per il suo lavoro su Tor e TorButton

Fine

- Domande?