Tor

Navigare, hidden service e configurare un relay

Politecnico Open unix Labs

Corsi Linux Avanzati 2012

Indice

Tor: cos'è?

- Tor è:
  - un software open-source e multipiattaforma
  - una rete
  - un protocollo
- Permette di navigare in maniera anonima
- In breve: nasconde il vostro indirizzo IP
- Apparentemente è un normale proxy

Chi lo usa?

- Si usa laddove Internet è sottoposto a censura
- Attivisti in Cina, Iran, Corea e altri paesi
- Fondamentale nella Primavera Araba (Egitto, Libia...)

Anche persone ordinarie

- In Cina Facebook non è raggiungibile
- Giovani ragazzi utilizzano Tor
- Permette di rimanere in contatto con il resto del mondo

In Italia?

- Internet viene oscurato anche in Italia
- Il caso più lampante è The Pirate Bay

Chi finanzia il progetto?

- Electronic Frontier Foundation
- Human Rights Watch
- Dipartimento della Difesa Statunitense
- Google
- Altre organizzazioni non-governative

Come funziona?

- Il concetto alla base di Tor è l'onion routing
- Gli attori sono
  - Mittente
  - Un entry-node
  - Alcuni nodi intermedi (tipicamente 1)
  - Un exit-node
  - Il destinatario

Onion routing

1. Il mittente crittografa 3 volte il suo messaggio
2. L'entry node riceve il messaggio
3. L'entry node rimuove il primo strato di crittografia
4. Il messaggio viene inoltrato ad un nodo intermedio
5. Il nodo intermedio rimuove un altro strato di crittografia
6. Il messaggio viene inoltrato all'exit-node
7. L'exit-node rimuove l'ultimo strato di crittografia
8. Il messaggio in chiaro raggiunge il destinatario

Vantaggi rispetto ad un normale proxy

- Un comune proxy conosce:
  - il vostro IP
  - il destinatario
  - il contenuto del messaggio
- Con Tor invece:

Conosce...	Entry-node	Nodo intermedio	Exit-node
il tuo IP?	×		
il destinatario?			×
il contenuto?			×

Quindi?

- Compromettere l'anonimato è molto più difficile
- Tutti i 3 nodi dovrebbero essere complici e coordinati
- I nodi sono scelti a caso tra gli attuali 2300
- Per creare un nodo basta una normale installazione

Come lo uso?

- Vedremo tre modi in cui si può usare Tor:
  - Navigare sul web in maniera anonima
  - Offrire un servizio (web) anonimo
  - Configurare un nodo della rete Tor

Indice

Navigare anonimi

- L'uso più frequente è la navigazione sul web
- Ci sono due metodi per fare navigare dietro Tor:
  - Usare il browser tramite un proxy SOCKS sulla porta 9050[1]
  - Servirsi del TBB (Tor Browser Bundle)

[1] Altre informazioni su questo metodo nel GiornaLinux di giugno 2011, disponibile all'indirizzo http://www.poul.org/progetti/giornalinux/

Il Tor Browser Bundle

- Il TBB è il metodo raccomandato per navigare con Tor
- Integra Firefox e un client Tor
- Firefox è stato patchato per massimizzare l'anonimato
- Semplice da usare e funziona out-of-the-box
- https://www.torproject.org/projects/torbrowser.html.en

Demo

Indice

Offrire un servizio anonimo

- È possibile esporre un servizio in maniera anonima su Tor
- Ovvero potete offrire un contenuto senza rivelare chi siete
- In concreto l'indirizzo IP del vostro server rimarrà celato
- Un siffatto servizio è detto hidden-service

Gli hidden-service

- Gli hidden-service sono raggiungibili solo tramite Tor[2]
- Un hidden-service è identificato da un dominio .onion
- Ad esempio eqt5g4fuenphqinx.onion

[2] A meno di utilizzare servizi come tor2web, con serie implicazioni a livello di sicurezza, in particolare per il client

Come funzionano?

- Il collegamento client-server è complicato
- https://www.torproject.org/docs/hidden-services.html.en
- Per l’anonimato di entrambi si usano 6 nodi intermedi

Let’s do it!

- Configurare un hidden-service è piuttosto semplice:
  1. Installare Tor e assicurarsi che funzioni correttamente
  2. Mettere un webserver in ascolto su 127.0.0.1, porta 80[3]
  3. Creare la directory “/var/lib/tor/mio_hiddenservice/”:

```
mkdir -p /var/lib/tor/mio_hiddenservice/
```

[3] O in alternativa, usare Netcat per accogliere le richieste:
nc -l -p 80 -s 127.0.0.1

Let’s do it!

4. Assicurarsi che l’utente di Tor possa scriverci:

```
chown tor:tor /var/lib/tor/mio_hiddenservice/
```

5. Aggiungere al file torrc (tipicamente in /etc/tor):

```
HiddenServiceDir /var/lib/tor/mio_hiddenservice/
HiddenServicePort 80 127.0.0.1:80
```

6. Riavviare il servizio di Tor

Fatto!

- A questo punto l'hidden service è pronto
- L'indirizzo .onion tramite il quale è raggiungibile si trova in:

/var/lib/tor/mio_hiddenservice/hostname

- In alcuni minuti sarà raggiungibile dagli utenti Tor
- Per testare la raggiungibilità si può usare tor2web.org:

http://eqt5g4fuenphqinx.tor2web.org/

- Altrimenti con un client Tor (ad esempio il TBB) andare a:

http://eqt5g4fuenphqinx.onion/

Demo

Indice

Perché creare un nodo Tor?

- Per mantenere viva e neutrale la rete Tor
- Per aiutare tutti coloro che hanno necessità
- Per sperimentare!

Tipi di nodo Tor

- Il normale client Tor permette di configurarsi come un nodo
- Entry-node e nodi intermedi sono in realtà la stessa cosa
- Gli exit-node permettono l'uscita del traffico verso Internet

I bridge

- I bridge sono entry-node “segreti”[4]
- Servono per evitare che Tor venga bloccato dagli ISP
- Senza bridge basterebbe fare una blacklist dei nodi Tor
- Un utente ne può ottenere pochi alla volta:

https://bridges.torproject.org/

[4] Ovvero non esiste una lista completa pubblica di bridge

Rischi?

- Entry-node, bridge e nodi intermedi non corrono rischi
- Solo gli exit-node rischiano di trovarsi in guai legali
- Infatti dal loro IP potrebbe partire qualunque cosa:
  - spam
  - pirateria
  - pedopornografia
- È una scelta che va ponderata con il proprio ISP!

Come si configura?

- Modifichiamo il file torrc[5]:

```
# Disabilitiamo l'uso di Tor come client
SocksPort 0
# Impostiamo IP e porta per il nostro nodo
ORListenAddress 1.2.3.4
ORPort 443
# Non vogliamo essere un exit-node
Exitpolicy reject *:*
```

[5] Si consiglia di usare una porta raggiungibile da tutti, 443 è un'ottima scelta, se già occupata anche 563 è in genere raggiungibile

Bridge e limitazione di banda

- Se si vuole configurare un bridge:

```
BridgeRelay 1
```

- Limitiamo la banda a 250 kB/s e massimo 10 GB al giorno:

```
AccountingStart day 5:00
AccountingMax 10 GB
BandwidthRate 250 KB
```

Quasi fatto!

- Riavviare il servizio Tor
- Ricordarsi di aprire la porta designata sul firewall
- Per verificare il funzionamento consultare i log:

  /var/log/tor/tor.log

- Se contiene un messaggio del tipo:

  Self-testing indicates your ORPort is reachable from the outside...

  Tutto sta funzionando correttamente