Creazione di servizi di rete anonimi con l'uso di Tor

Gianni Bianchini <giannibi@winstonsmith.info>

E-Privacy 2006, Firenze, 20 Maggio 2006

Copyright

Typeset using LaTeX

Sommario

Sommario

Sommario

Sommario

Motivazioni

- Senza opportuni accorgimenti, l'origine e la destinazione di ogni comunicazione in Rete, così come il relativo contenuto, sono identificabili presso ogni nodo intermedio con tecniche elementari
- Il mittente ed il destinatario di ogni messaggio di posta elettronica, così come gli utenti di un sistema di messaggistica convenzionale, sono facilmente tracciabili ed i messaggi scambiati, se non cifrati, sono palesi
- La pubblicazione sul web è facilmente censurabile attaccando, per via informatica o legale, un singolo server

Motivazioni

- Un servizio di rete è tipicamente ospitato da un singolo server o da gruppi di server di cui è nota la collocazione fisica o nella topologia della rete
- Un server costituisce tipicamente un *single point of failure*: se esso viene attaccato, isolato, rimosso o distrutto, contenuti e servizi non sono più disponibili
- Ogni host presente sulla rete, ma anche l'attività temporanea su una risorsa pubblica (ad es. un internet point), è riconducibile ad una persona o ragione sociale
- La conoscenza della collocazione di un server e dell'insieme dei servizi da esso offerti aumenta notevolmente la probabilità di successo in un attacco

Hidden services: obiettivi

- Resistenza alla censura
  - Il servizio deve rimanere accessibile in presenza di provvedimenti (filtraggio del traffico, redirezione DNS) atti ad impedirne la fruizione
- Resistenza alla violazione fisica e logica
  - Impossibilità di conoscere sia l'ubicazione del server sia l'insieme delle sue funzionalità
- Minima necessità di ridondanza per ottenere un servizio resiliente in caso di attacchi *denial of service* distribuiti *(DDoS)*
- Impossibilità di risalire a chi fornisce il servizio e/o pubblica le informazioni
- Impossibilità di risalire a chi fruisce del servizio

Accesso anonimo ad un servizio di rete

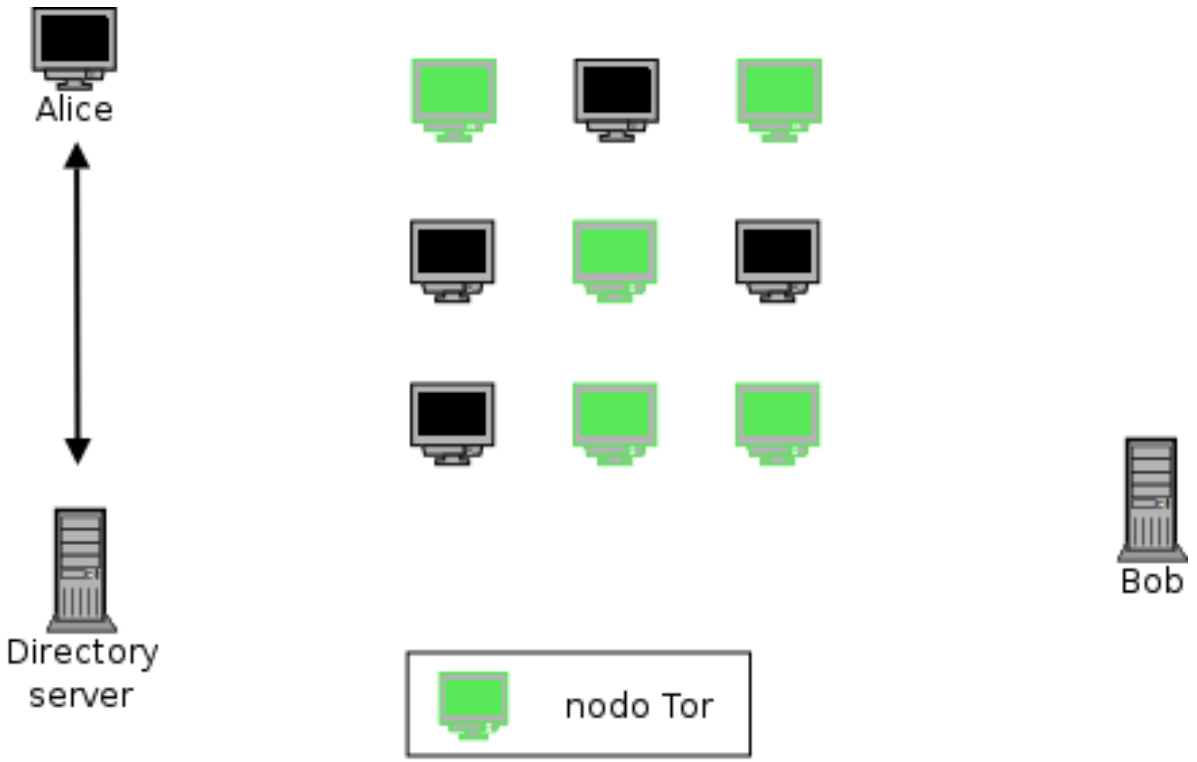
Bob fornisce un servizio di rete *S* (sito web/blog, file system condiviso, sistema di messaggistica...). *Alice* accede a tale servizio.

- Accesso *anonimo in avanti*: Alice accede a *S* senza che nessuno possa risalire all'indirizzo IP da cui ella ha generato la richiesta
- Accesso *anonimo all'indietro*: Alice accede a *S* senza che nessuno possa risalire all'indirizzo IP del server che ospita *S*

- L'accesso a servizi di rete ordinari attraverso Tor realizza l'anonimato in avanti, gli hidden services l'accesso anonimo all'indietro.

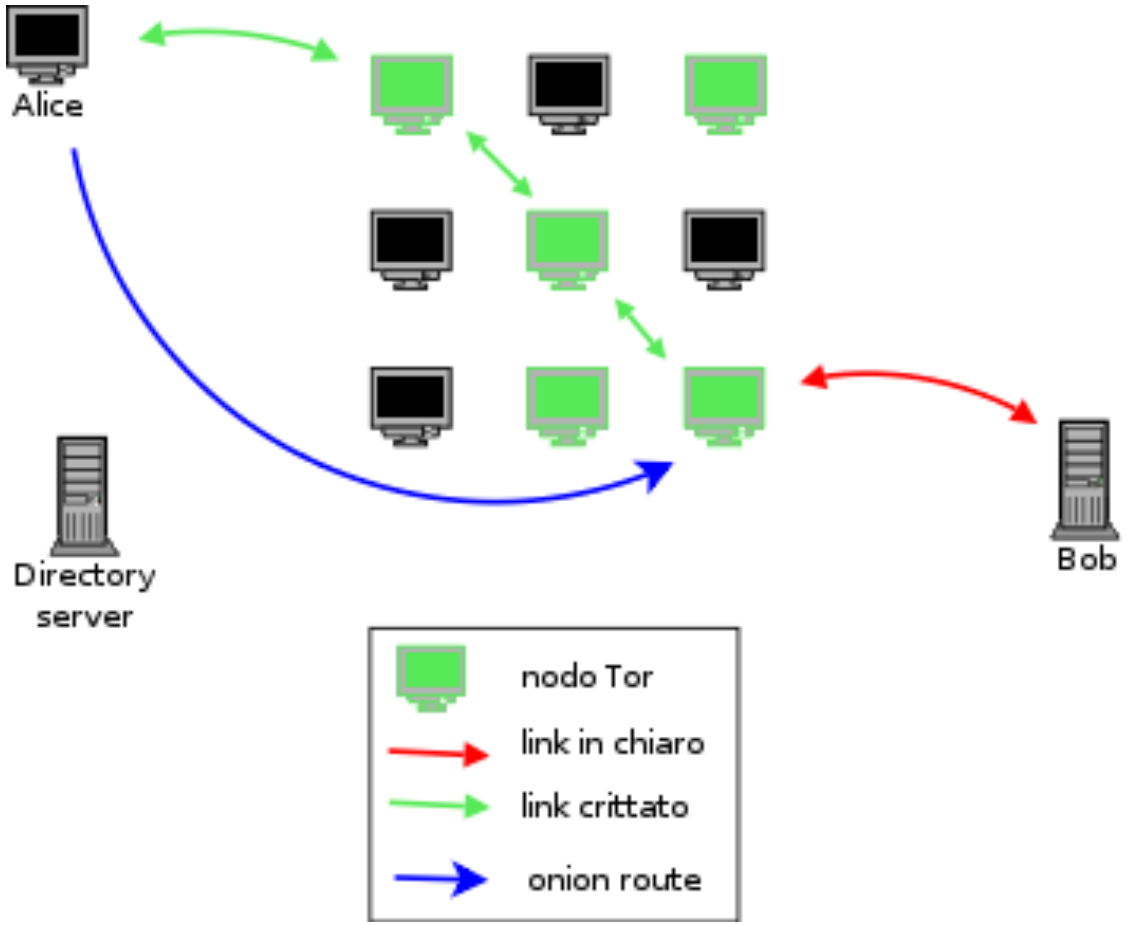
Tor: costruzione dell'onion route

1. Alice riceve una lista di nodi dai directory server e stabilisce il percorso



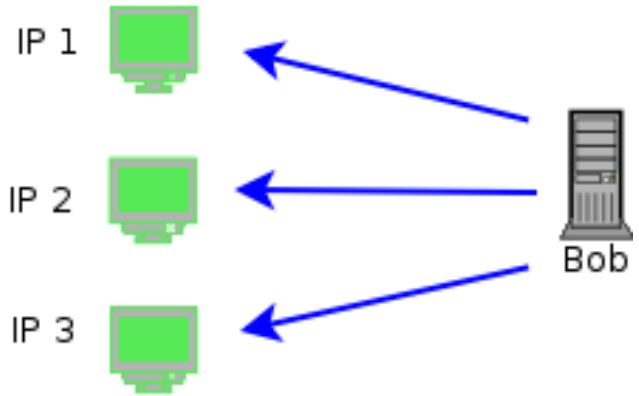
Tor: costruzione dell'onion route

2 Il percorso viene costruito



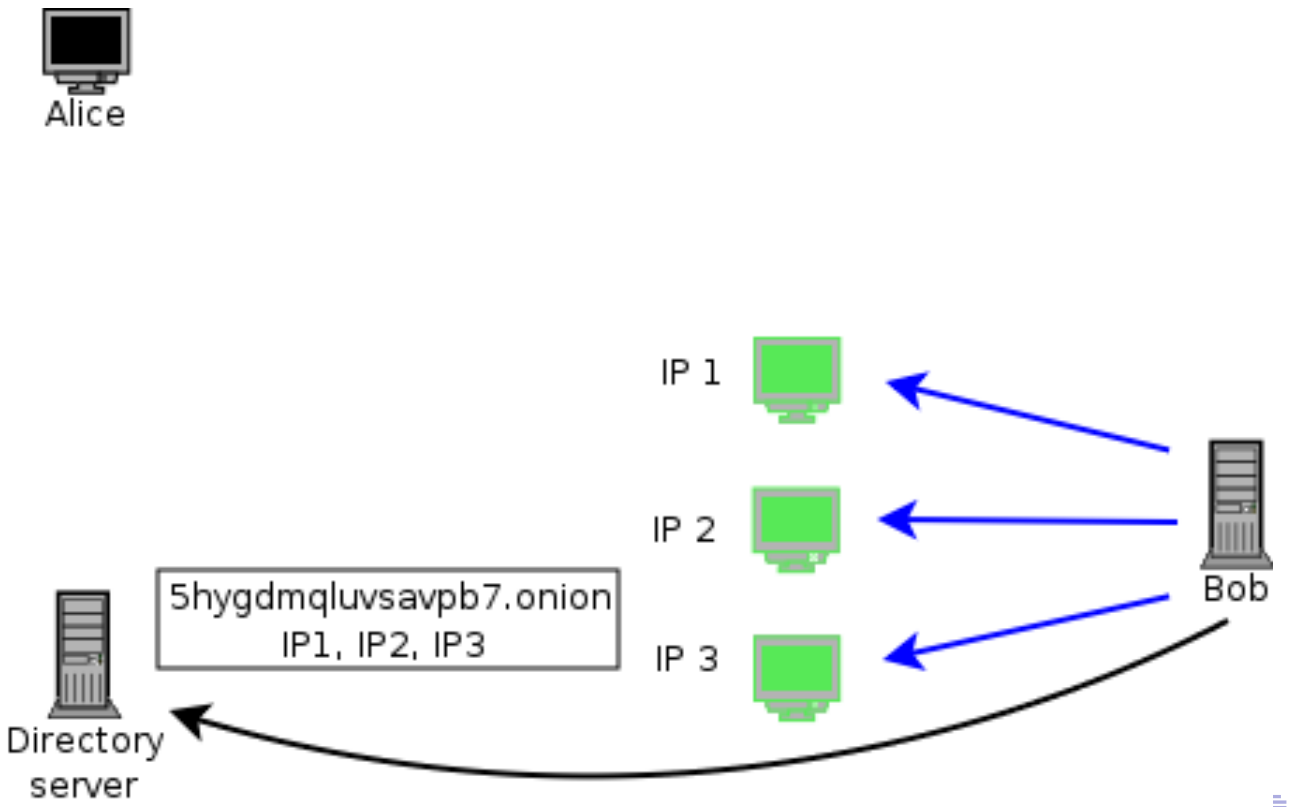
Hidden services: funzionamento

1. Bob, che intende fornire un hidden service, seleziona alcuni nodi come *introduction points (IP)* e stabilisce onion routes verso di essi



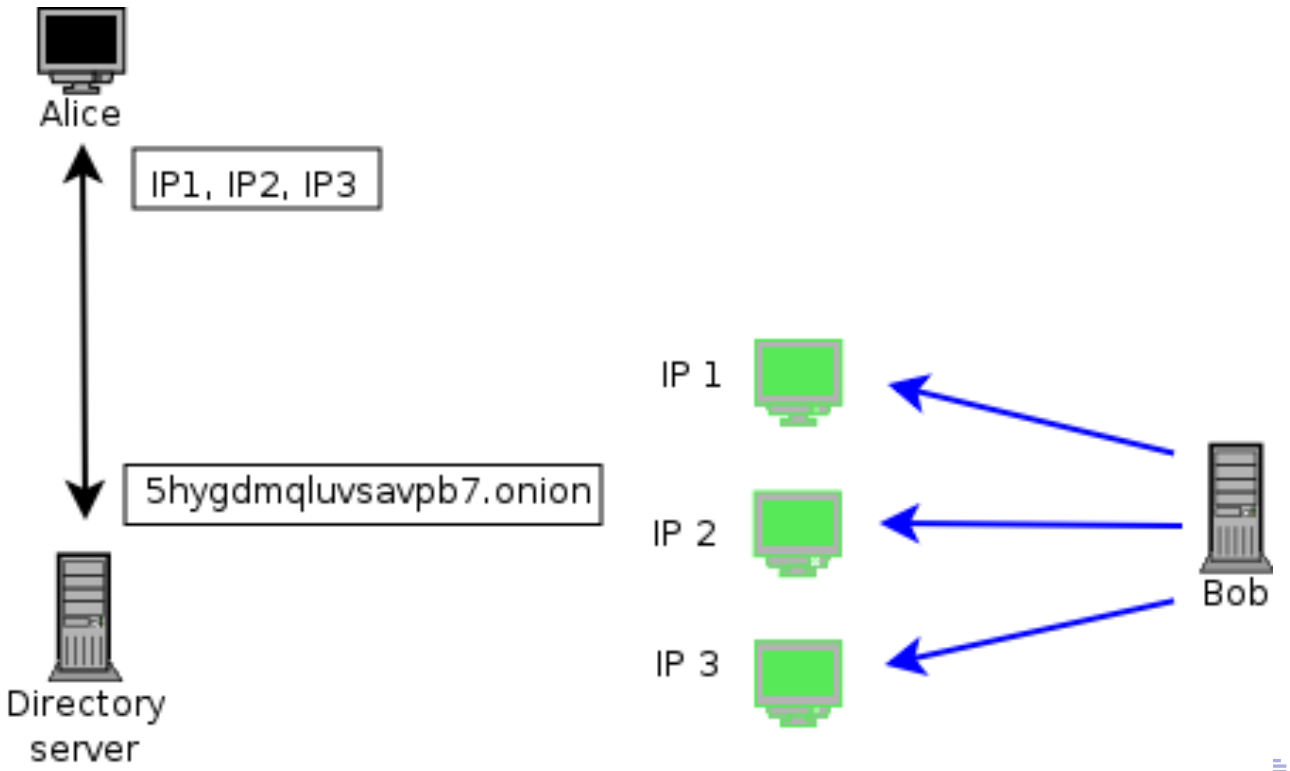
Hidden services: funzionamento

2. Bob genera una coppia di chiavi ed una *handle* per il servizio della forma `5hygdmqluvsavpb7.onion`
3. Bob comunica la handle ed i relativi IP ai directory server



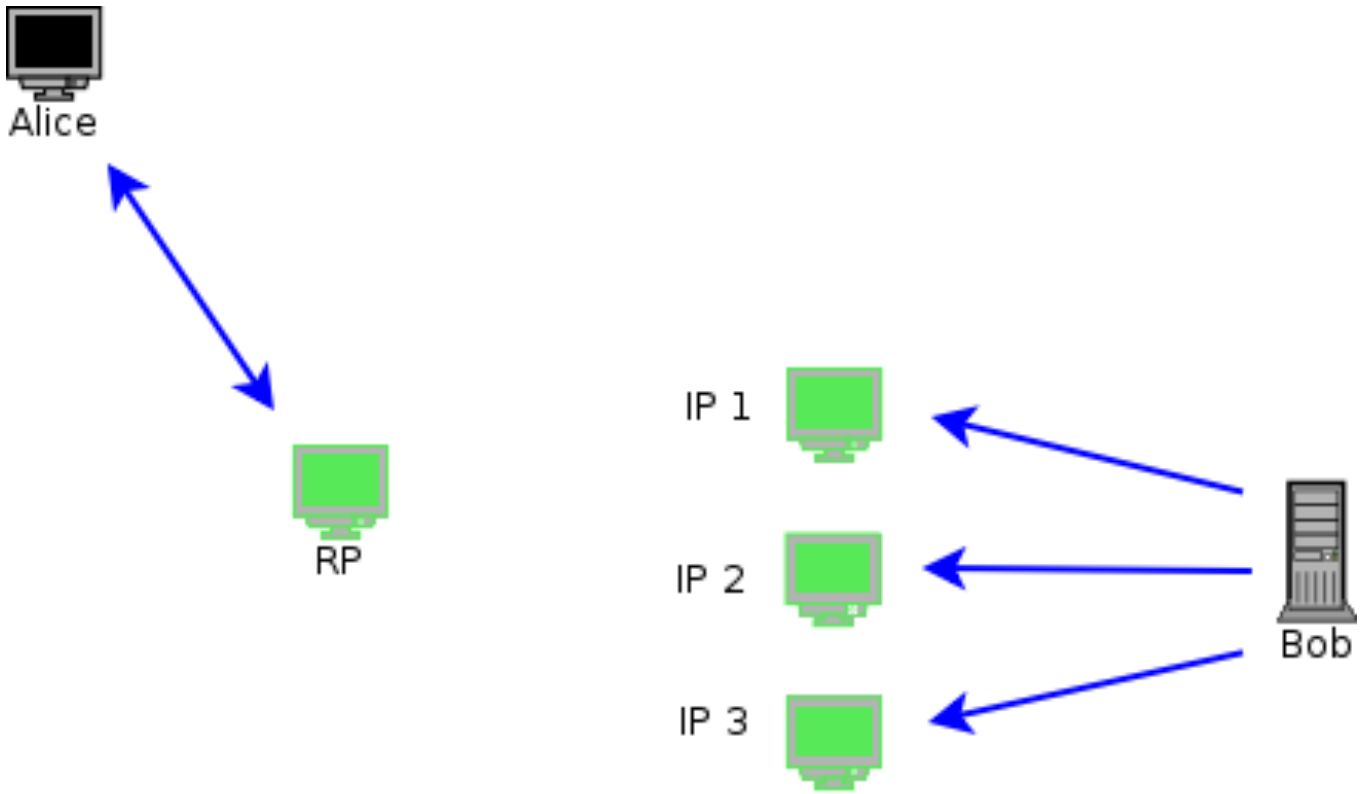
Hidden services: funzionamento

4 Alice ottiene *out of band* la handle del servizio offerto da Bob `5hygdmqluvsavpb7.onion`
5 Alice ottiene gli indirizzi dei relativi IP dai directory server



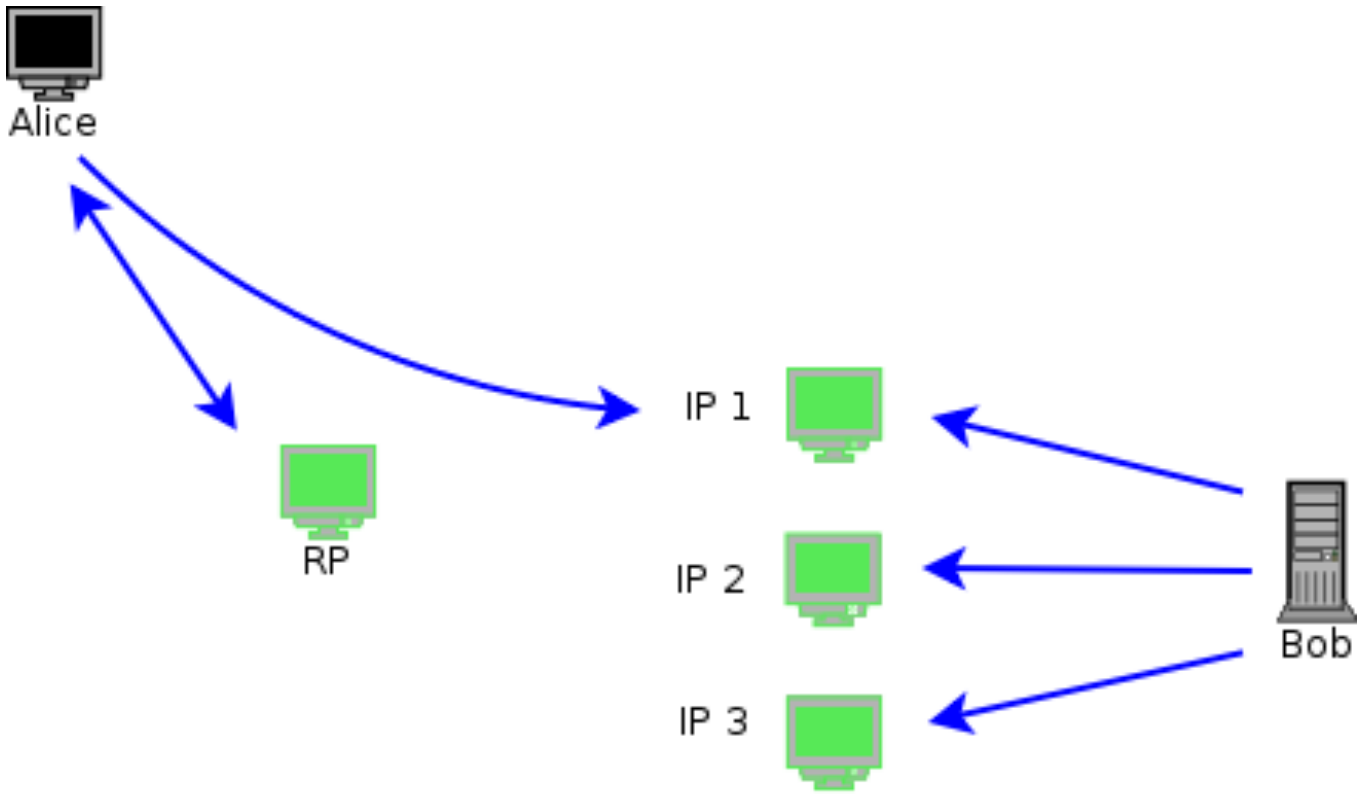
Hidden services: funzionamento

6 Alice seleziona un nodo come *rendez-vous point (RP)* e stabilisce una onion route verso di esso



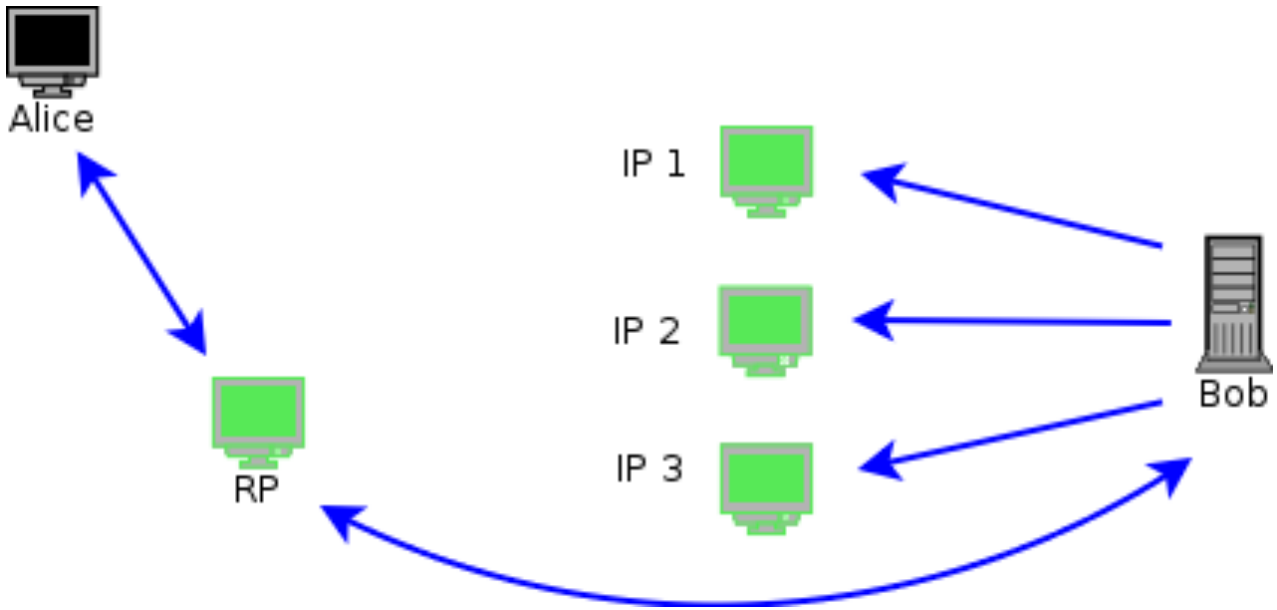
Hidden services: funzionamento

7 Alice crea una onion route verso uno degli IP e comunica attraverso di esso a Bob il nodo che funziona da RP



Hidden services: funzionamento

8 Se Bob desidera parlare con Alice, allora crea una onion route verso il RP. Il circuito si chiude attraverso il RP e risulta quindi stabilita una onion route tra Alice e Bob. Alice e Bob possono comunicare rimanendo "anonimi" l'una all'altro



Hidden services: configurazione

- È necessario disporre di un nodo Tor funzionante, *non necessariamente in modalità server*
- La configurazione di un hidden service avviene mediante redirezione di indirizzi fittizi `[indirizzo.onion:porta]` verso indirizzi fisici `[indirizzoIP:porta]`, locali o remoti, su cui "ascoltano" i servizi di rete
- Se il servizio è correttamente configurato, Tor genera automaticamente l'indirizzo `.onion`, che rappresenta anche la chiave pubblica del servizio, e la relativa chiave privata

Hidden services: configurazione

```
# File di configurazione di Tor:  /etc/tor/torrc

...
HiddenServiceDir /var/lib/tor/hidden/
HiddenServicePort 80 127.0.0.1:80 # HTTP
HiddenServicePort 22 127.0.0.1:22 # SSH
...
```

E ora si spippola!

Vediamo se funziona...

Caveat

- Servizi ospitati su host diversi dal nodo Tor generano traffico in chiaro tra host e nodo
- Il web server che fornisce un sito anonimo deve rispondere solo alle richieste provenienti da Tor (locali!) e non essere altrimenti accessibile
- Non deve essere usato lo stesso programma server per fornire sia servizi ordinari sia anonimi
- Il web server deve essere minimale (THTTPD, PublicFile). Software plurifunzionali (Apache, IIS, etc.) possono fornire informazioni che compromettono l'anonimato (stringhe di versione, hostname, ecc.)
- Si dovrebbero eliminare le estensioni di scripting e tutto quanto possa generare fughe di informazioni in merito alla macchina ospite

Altre caratteristiche

- Grazie al meccanismo dei RP, un hidden service può essere ospitato su server che non dispongono di indirizzo IP pubblico.
- Non è necessario che il nodo Tor ospite sia un server della rete Tor.
- Ogni servizio è identificato solo dalla sua chiave privata e può cambiare ubicazione fisica ad arbitrio senza vincoli di indirizzo IP o FQDN: è sufficiente trasportare le chiavi
- Si può pensare a hidden services "portatili"
  - Tor, Privoxy e chiavi su dispositivo USB: da "Privacy-box" a "Privacy-stick"! :-)

Impieghi creativi

- *Internet Relay Chat (IRC)* anonimo (centralizzato)
- Messaggistica istantanea *(IM)* anonima (decentralizzata)
  - Jabber over Tor. Configurazione di un server per utente.
- Reti private virtuali in cui ogni host è anonimo agli altri
  - OpenVPN over Tor
- Creazione di identità di posta elettronica pseudonime della forma `user@5hygdmqluvsavpb7.onion`
  - Configurazione immediata lato server
  - Non è necessario un server di posta pubblicamente accessibile, quindi niente blacklisting!
  - Meno sicure dei reply-block o Mixminion, che non hanno vincoli di temporizzazione. Necessaria installazione di Tor lato mittente più gateway SMTP o plugin per client di posta

Accesso agli hidden services

- HTTP
  - Client Tor + Privoxy
  - Configurazione di Privoxy per inoltrare le richieste attraverso Tor via SOCKS4A
  - Tor emula la risoluzione di nomi DNS via protocollo SOCKS4A, trattando opportunamente i suffissi `.onion`
- Servizi generici
  - Uso di programmi client che supportano il tunneling su HTTP (via Privoxy) o SOCKS4A. SOCKS4 non supporta la risoluzione dei nomi DNS
  - Redirezione di una porta locale su SOCKS4A tramite `socat`

Fine

Grazie per l'attenzione!

/giannibi

Bibliografia

- Tor website, http://tor.eff.org/
- Roger Dingledine, Nick Mathewson, Paul Syverson, *Tor: The Second-Generation Onion Router*.
- Roger Dingledine, *Tor Hidden Services*, Proc. What the Hack, 2005
- Privoxy website, http://www.privoxy.org/
- P. Biddle, P. England, M. Peinado, B. Willman, *The Darknet and the Future of Content Distribution*, proc. ACM Workshop on Digital Rights Management, 2002.