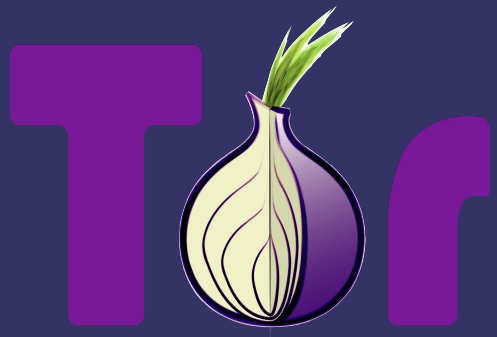
TOR – Anonimato in rete



Andrea Franchi

05092007

Anonimato?

Poter mantenere anonimi i propri dati personali e correlati è un diritto dell'utente!

Spesso non è così -> *Analisi del traffico* <- La crittografia non è sufficiente

Anonymity + Security = Privacy

L'anonimato è anche fondamentale per organizzazioni, industrie e dove manca la libertà

Analisi del Traffico?

L'analisi del traffico è una tecnica che permette di dedurre informazioni analizzando i flussi di pacchetti

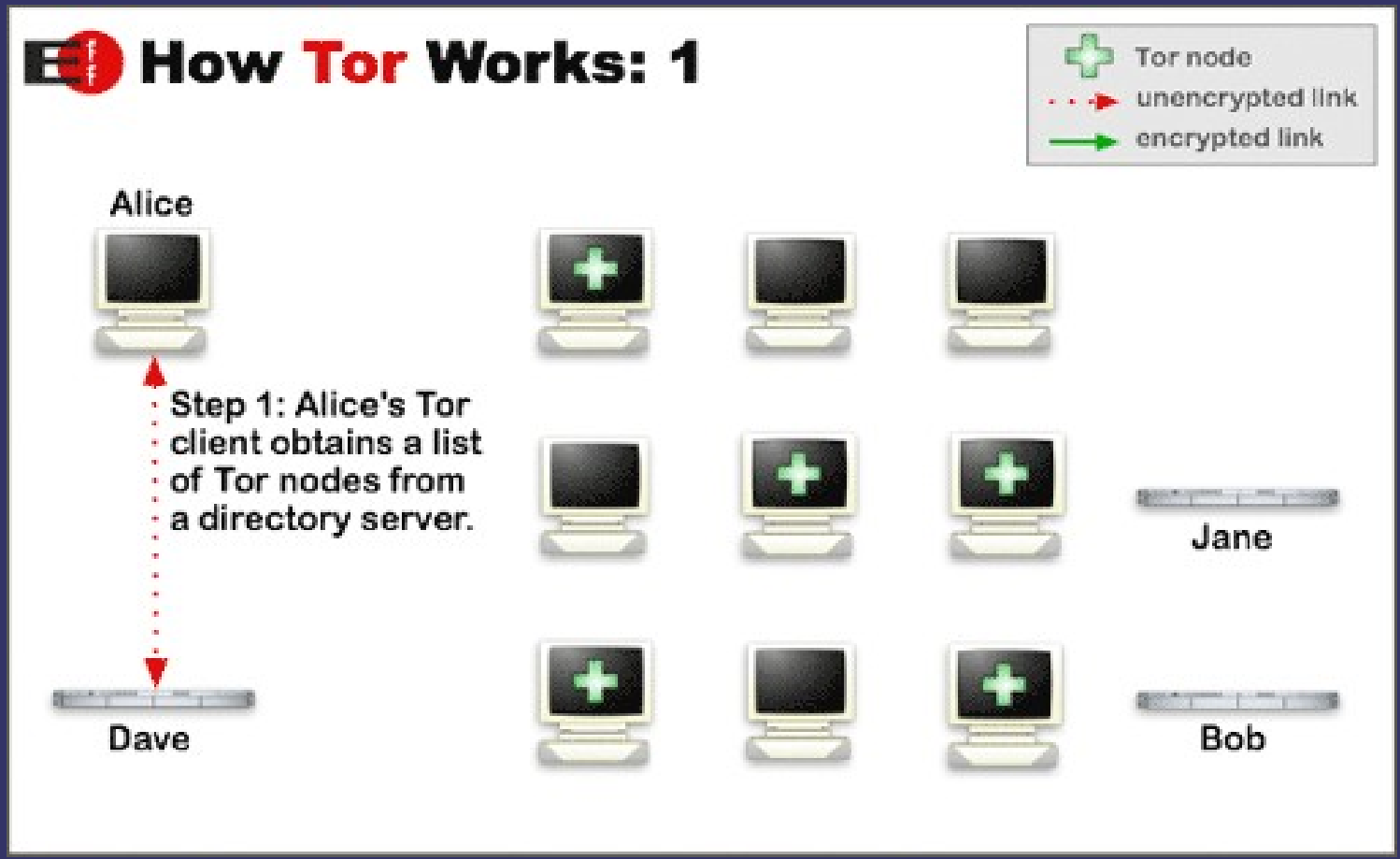
- I pacchetti che viaggiano in Internet sono composti da:
  - Header: contiene le informazioni di instradamento
  - Payload: contiene i dati
- Criptando il payload nessuno può “leggere” il contenuto della sessione. L'header però contiene informazioni altrettanto utili e non si può criptare!

Come Funziona

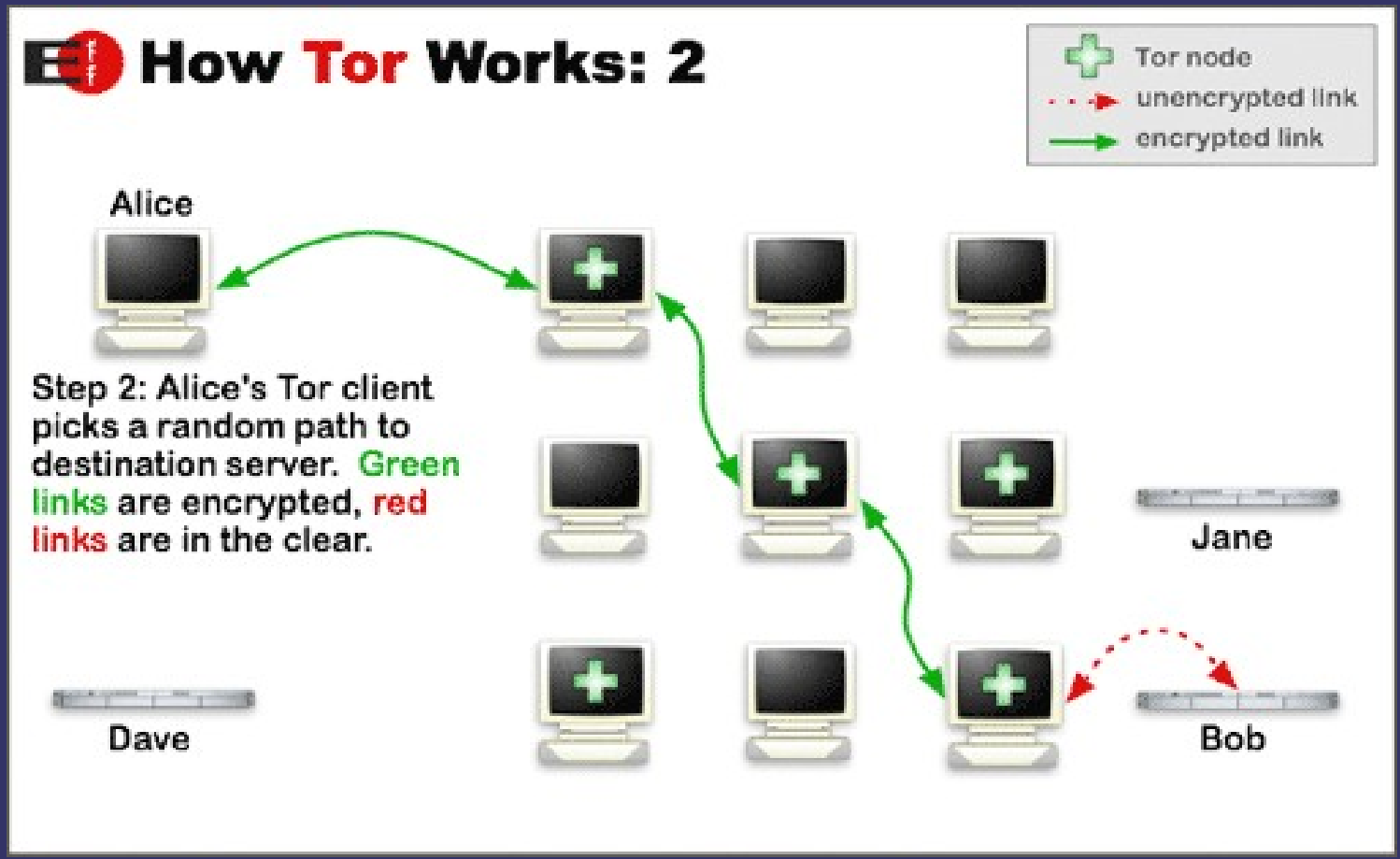
- Crea una sottorete ad internet: i pacchetti che entrano escono da tutt'altra parte attraverso circuiti variabili tra i server

- Esistono 2 tipi di host: Client e Server (exit server e interni)
- One-hop routing: ogni nodo conosce solo che un pacchetto gli arriva da un nodo e deve consegnarlo ad un'altro nodo
- I nodi intermedi non possono leggere il contenuto del payload di partenza

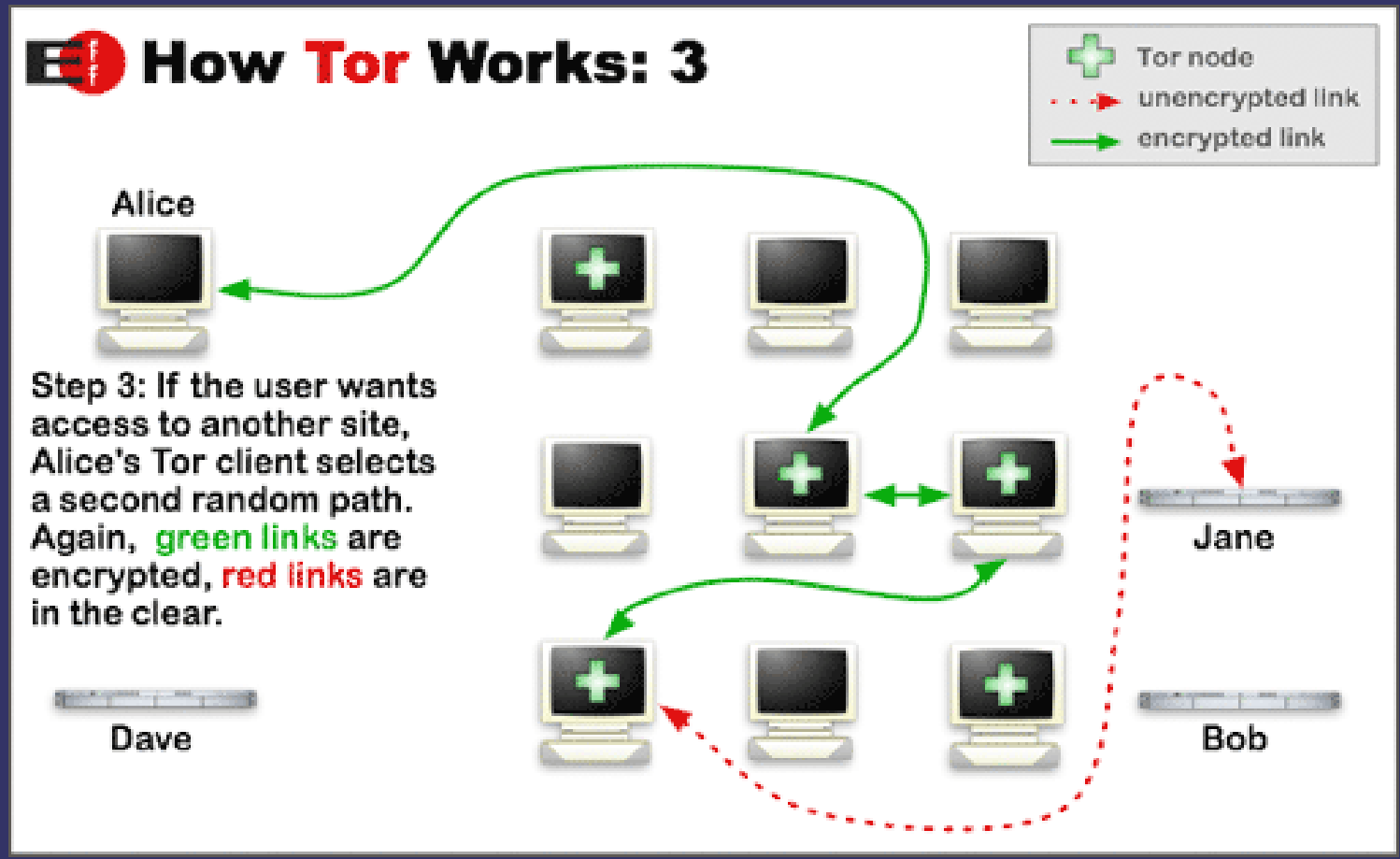
Come Funziona - 1



Come Funziona - 2



Come Funziona - 3



Hidden Services

- Sono servizi disponibili internamente alla rete Tor che permettono di pubblicare un servizio (es web server) senza rendere nota la sua posizione (anonimato all'indietro)
- Sono nella forma: http://6sxoyfb3h2nvok2d.onion
- Non è richiesto un ip pubblico quindi funzionano anche dietro nat o firewall e possono essere realizzati anche dai client
- Posso realizzare hidden services portabili ad esempio su live-cd o usb pen

Pregi

- Infrastruttura sicura contro (quasi) ogni tipo di attacco
- Progetto attivo, sviluppato e documentato
- Semplicità d'uso
- Multipiattaforma (Linux, OsX, Windows)

Problemi

- Lentezza -> non è un problema dell'onion routing
- Bisogna “torificare” le applicazioni
- Eavesdrop connections sugli exit nodes -> usare la crittografia
- Qualche malfunzionamento/falsi positivi (es. Google)

Installare Tor&c.

- Gentoo: # emerge tor privoxy Howto
- Debian: # apt-get install tor privoxy
- Slackware: # installpkg tor privoxy

oppure compilare i relativi sorgenti

GUI:

-> Vidalia (QT4)

-> TorK (Kde Tor Manager: control+configure + torify+log)

Funziona anche sotto Mac OSX e Windows

Torify

Significa configurare un'applicazione perchè utilizzi Tor

Se non si “torifica” l'applicazione funzionerà normalmente ma in maniera “non anonima”

Per la maggior parte dei programmi si specifica il proxy nella configurazione

Per alcuni esistono plugin o estensioni come TorButton per Firefox

http://wiki.noreply.org/noreply/TheOnionRouter/TorifyHOWTO

Note

Non è bene intasare la rete Tor col traffico P2P o files di grandi dimensioni

Per evitare lo spam via mail anonime, la porta 25 (smtp) è bloccata di default sui server

Tor funziona grazie al contributo dei suoi utenti che condividono la banda -> mettete su un server!

Links Utili

http://wiki.noreply.org/noreply/TheOnionRouter - Risorse e links su Tor

https://torcheck.xenobite.eu - Verifica se si sta usando Tor

https://torstat.xenobite.eu/ - Statistiche dei nodi della rete

http://gentoo-wiki.com/HOWTO_Anonymity_with_Tor_and_Privoxy