Tor: attacchi al protocollo e tecniche di difesa

Marco Bonetti
marco.bonetti@slackware.it

5 Febbraio 2008

Infosecurity 2008 - Milano

Parte 1

Funzionamento di Tor

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
- Uno strumento per proteggersi dall'analisi del traffico

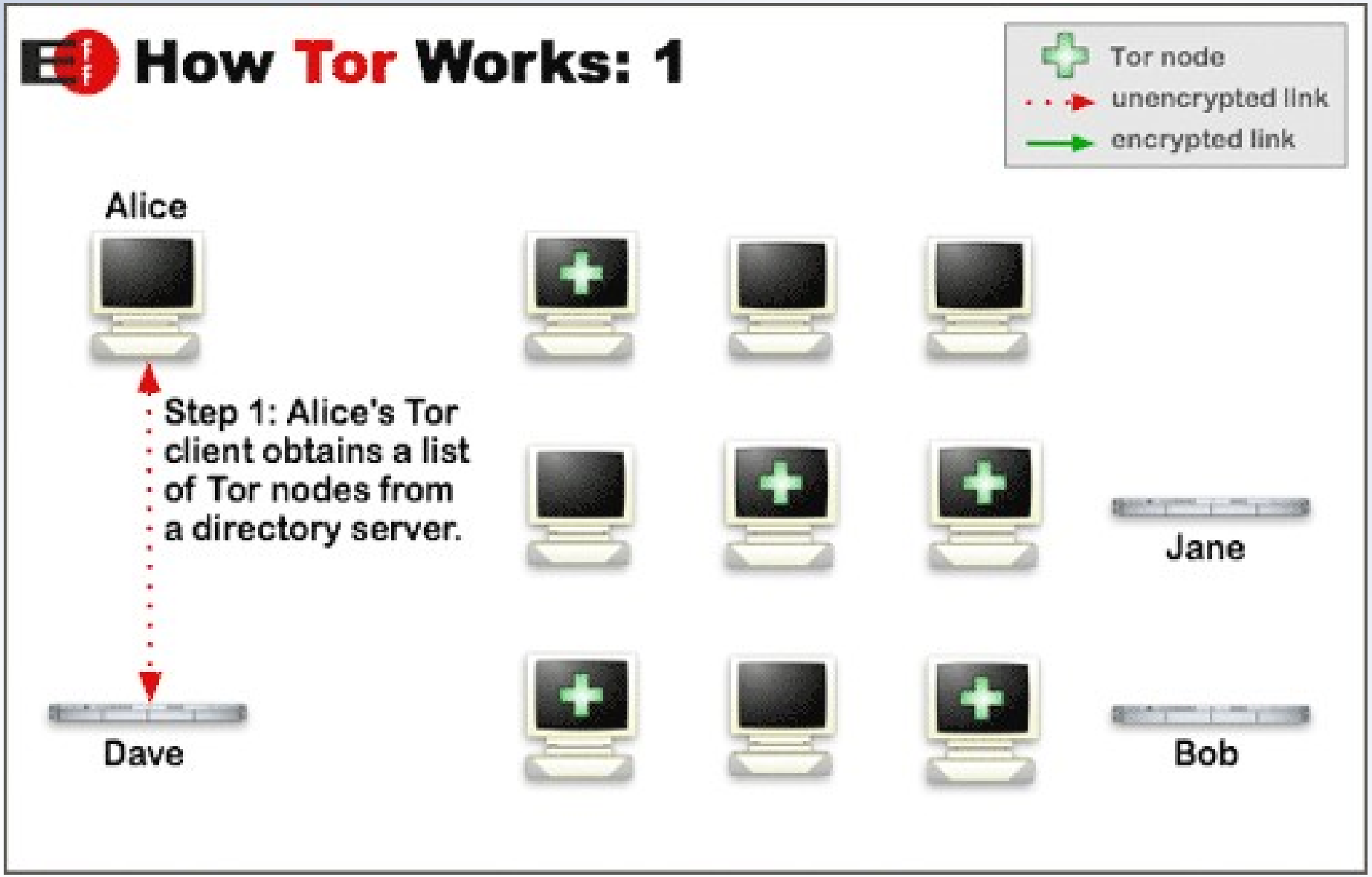
Analisi del traffico

- 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 ;-)
- 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

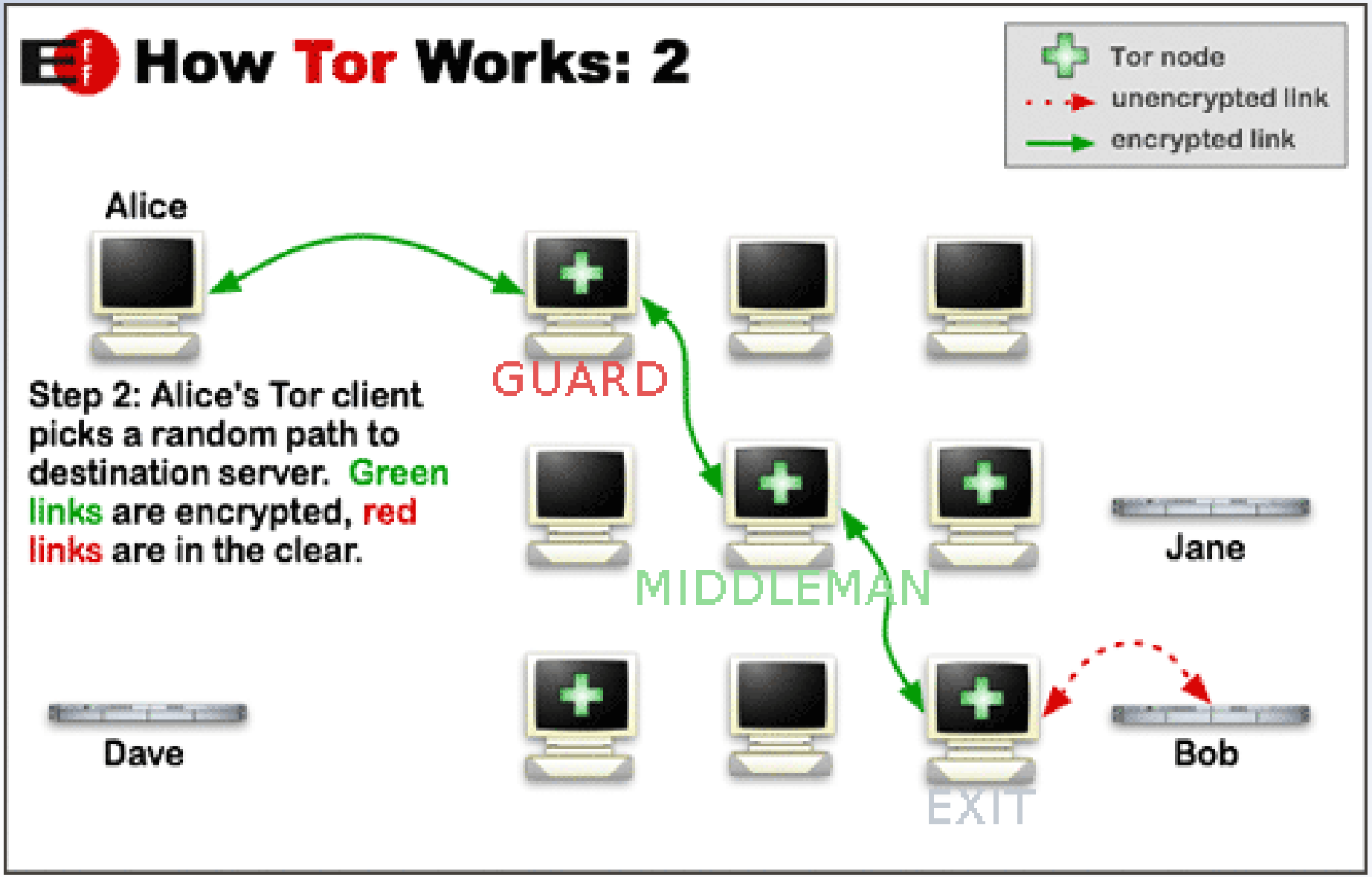
La soluzione proposta da Tor

- 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?

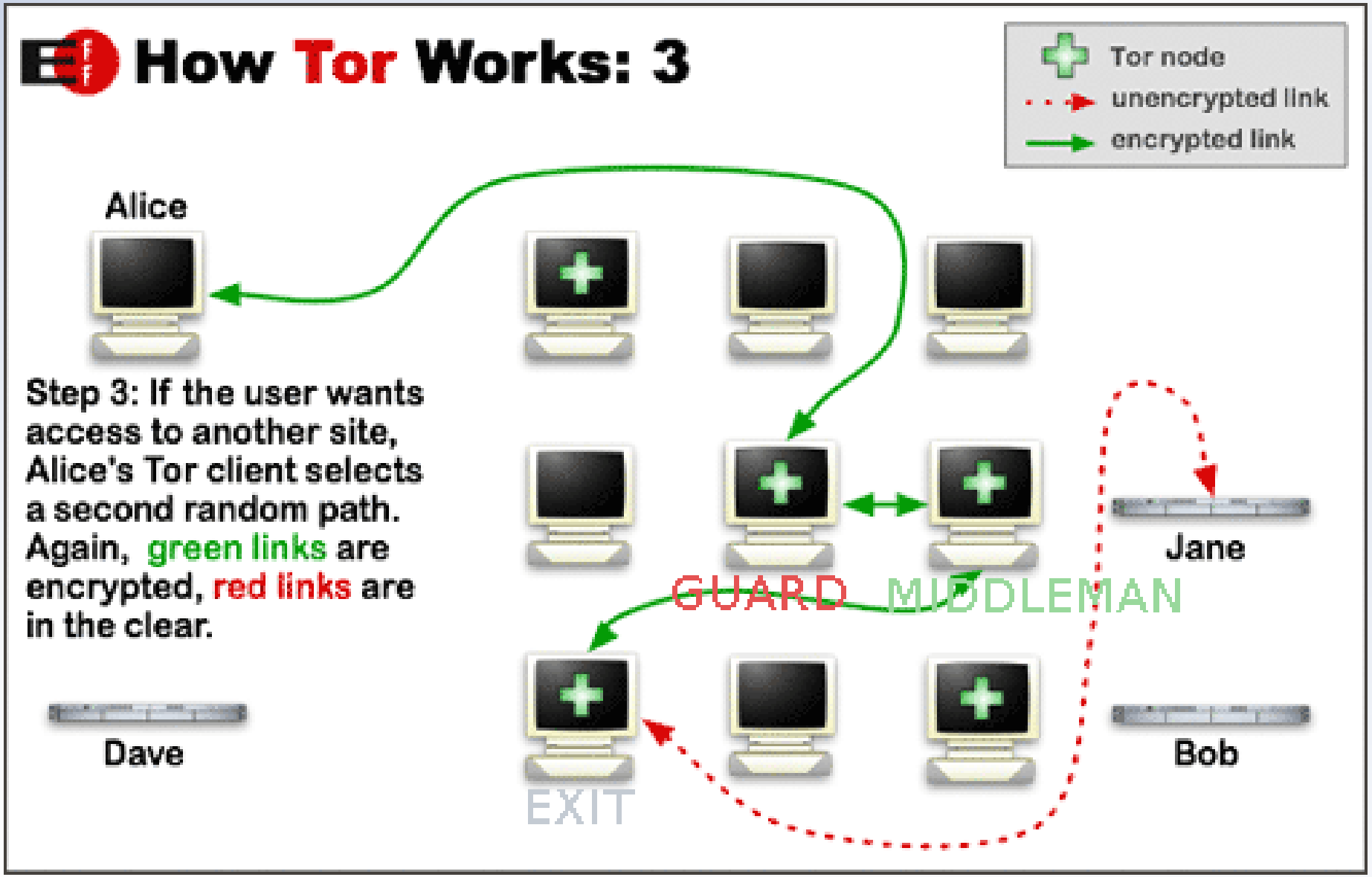
La magia – 1


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

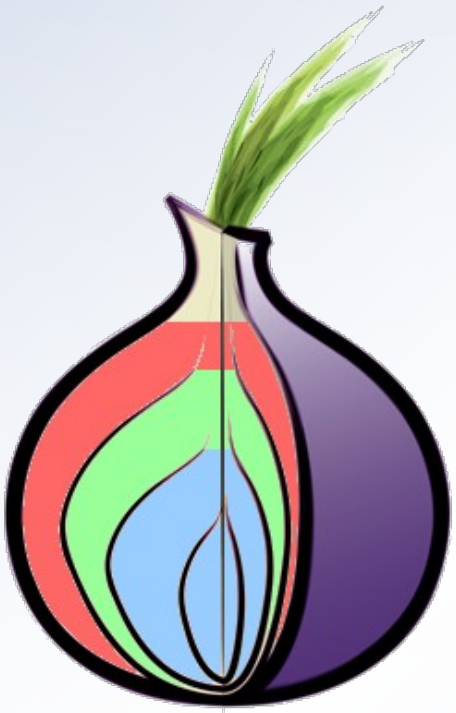
La magia – 2


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

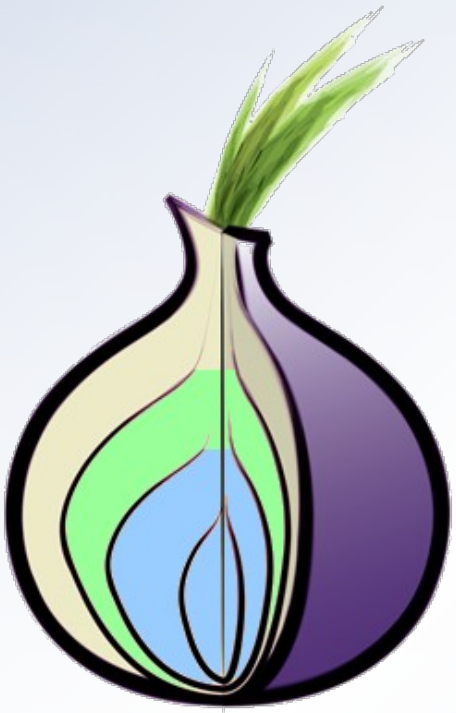

How Tor Works: 3
Tor node
unencrypted link
encrypted link
Alice
Step 3: If the user wants access to another site, Alice's Tor client selects a second random path. Again, green links are encrypted, red links are in the clear.
Jane
GUARD
MIDDLEMAN
Dave
Bob
EXIT

Creazione di un circuito - 1



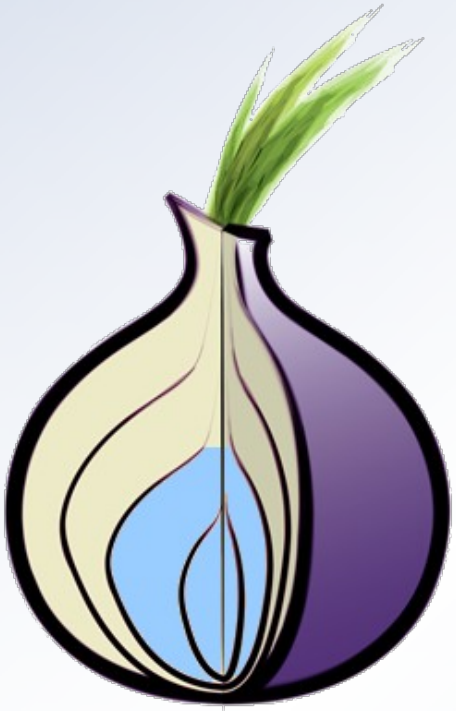
- Il client invia al nodo di guardia (GUARD) il pacchetto completo
- Il nodo di guardia decritta il primo strato e individua il nodo di transito a cui inviare il rimanente payload

Creazione di un circuito - 2



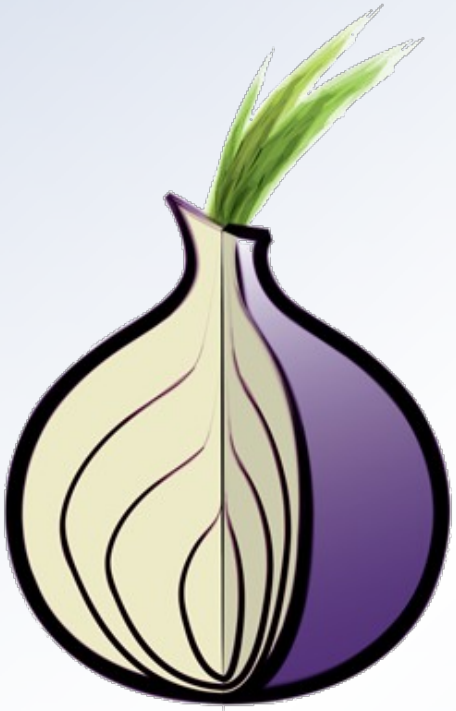
- Il nodo di transito (MIDDLEMAN) riceve dal guardiano il payload ridotto
- Come nel caso precedente, decritta lo strato di sua competenza per conoscere quale sarà il prossimo nodo a cui inviare il resto del payload

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”?
- 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

Installare Tor

- Tor è free software rilasciato sotto la 3-clause BSD e liberamente scaricabile all'indirizzo https://www.torproject.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 v. 4/4A/5 (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
- 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)

Attacchi al protocollo

Tipologie di attacchi

- Passivi, alla rete
  - analisi del traffico
  - correlazione
- Attivi, alla rete
  - impedire connessioni dalla rete Tor ai propri servizi
  - impedire connessioni verso la rete Tor
- Attivi, da parte di nodi di uscita “malvagi”
  - MITM
  - configurazioni volutamente errate
- Attivi, diretti verso i nodi e gli utilizzatori stessi
  - filtraggio di informazioni
  - dirottamento della ControlPort
  - autoconnessione dei nodi di uscita

Attacchi passivi alla rete - Problemi

- Mirano a scoprire l'identità dei partecipanti ad una comunicazione torificata
- Nascono dall'analisi del traffico della rete Tor
- Correlazione tra connessioni generate e pacchetti ricevuti
- Identificazione di “pattern” nel traffico creato e nell'utilizzo della rete

Attacchi passivi alla rete - Soluzioni

- Gli attacchi necessitano di grandi risorse e soffrono di alcuni problemi
- L'attaccante deve poter monitorare l'intera rete e tutto il traffico in ingresso e in uscita (chi ha detto echelon? ;-))
- Abilitare l'utilizzo di Tor come server vanifica gran parte di queste tecniche, mescolando il proprio traffico all'interno di quello generato dal nodo è più difficile capire chi ha generato cosa (blending)
- Uniformare l'identità presentata al momento della richiesta di un servizio permette di confondere il traffico comune da quello anonimo (pensate all'user-agent di un browser)

Attacchi attivi alla rete - Problemi

- Nascono da due esigenze diverse: bloccare le connessioni DALLA rete Tor e bloccare le connessioni VERSO la rete Tor
- Il primo caso è di semplice implementazione, esiste addirittura un progetto ufficiale: http://exitlist.torproject.org/ che fornisce la lista di indirizzi IP dei nodi di uscita attivi in stile DNSBL
- Il secondo è più complesso, alcune idee:
  - regole Snort bleeding-edge sulla morfologia dei pacchetti inviati
  - blocco dell'accesso agli indirizzi IP dei nodi server

Attacchi attivi alla rete - Soluzioni

- A volte il primo problema è una soluzione temporanea necessaria, la soluzione migliore rimane educare utenti e amministratori del servizio offerto
  - Chi ha seguito il recente IRC bot abuse su freenode?
  - Risolto con doppio hidden server: uno di libero accesso, offline durante i periodi di abuso, uno solo per utenti autenticati via chiave gpg, sempre online
- Il secondo problema è di più facile aggiramento:
  - server in ascolto su porte non standard (80 e 443)
  - blending dell'handshake delle connessioni crittate
  - richieste crittate di dati directory
  - utilizzo di bridge relay, via https://bridges.torproject.org/ oppure via gmail (Tor 0.2.0.13-alpha e successivi)

Attacchi attivi dei nodi di uscita - Problemi

- Puntano a rivelare l'identità del nodo di ingresso, sfruttando la posizione avvantaggiata dei nodi di uscita
- Pensate a un nodo di uscita “rogue” come a un ISP che vi fornisce connettività, ma molto, molto, più malvagio
- Può leggere e alterare il traffico in chiaro richiesto dal nodo client
- Può leggere e alterare il traffico cifrato usando un proprio certificato digitale
- Può pubblicizzare maggior banda di quella che ha a disposizione per ricevere più richieste da analizzare
- Può decidere quali richieste servire e quali no
- A volte è “solo” colpa della rete di appartenenza del nodo di uscita (registrati casi di ISP cinesi che eseguono html injection!)

Attacchi attivi dei nodi di uscita - Soluzioni

- La difesa è semplice, ma richiede il vostro intervento!
- NON inviate login/password a siti web che mostrano un certificato non valido
- NON eseguite login se la chiave del vostro servizio ssh è cambiata
- Seguite la mailing list or-talk e blacklistate le uscite segnate come “rogue” dai vostri nodi
- Usare un proxy http come Privoxy o Polipo a monte di Tor permette di ripulire quello che arriva al vostro browser

Attacchi attivi ai nodi e ai client – Problemi 1

- Puntano a rivelare l'identità di un nodo attaccandone l'ambiente circostante
- L'utilizzo di plugin per i browser web permette di bypassare l'utilizzo di Tor:
  - Java, Javascript, Actionscript permettono tutti di eseguire connessioni, ignorando totalmente il proxy configurato
  - I plugin multimediali soffrono di problemi simili, inoltre possono filtrare informazioni eseguendo risoluzioni dns dirette, bypassando le impostazioni del browser
- Perdita di informazioni
  - ipv6
  - connessione fallita al proxy
  - generazione di traffico attraverso canali differenti

Attacchi attivi ai nodi e ai client – Problemi 2

- Il browser fornisce troppe informazioni
  - cache
  - sessioni e cookie
  - user agent, timezone e locale
- Un sito o un nodo di uscita maligni possono ritornare un pacchetto malformato per attaccare la ControlPort usata per pilotare il comportamento del nodo di ingresso
- Un aggressore può selezionare quale nodo di uscita prendere e connettersi all'indirizzo IP esterno di quel nodo, in modo da accedere a servizi adiacenti al nodo Tor, sfruttando le credenziali di accesso del nodo stesso

Attacchi attivi ai nodi e ai client - Soluzioni

- Utilizzo dell'estensione TorButton (versione in sviluppo) per Firefox permette di ridurre i rischi:
  - Disabilita i plugins
  - Isola le sessioni di navigazione
  - Ripulisce le informazioni sensibili registrate
  - Esegue spoofing di user agent, locale e timezone
- JanusVM, una virtual machine da usare via vpn
- Incognito LiveCD
- Proxy trasparente delle connessioni
- Disabilitare la ControlPort se non sono impiegati programmi di controllo come Vidalia, Tork o Torctl
- Aggiornare sempre all'ultima versione di Tor rilasciata dal sito ufficiale: https://www.torproject.org/

Fine

- Ringraziamenti in ordine sparso:
  - 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, TorButton e il materiale di “Securing The Tor Network”, presentato a Black Hat USA 2007
  - A Roger Dingledine (di nuovo!) per il materiale di “Current events in Tor development”, presentato al CCC n. 24
- Domande?