Peeling the Onion: Attacchi alla rete Tor

Marco Bonetti
marco.bonetti@slackware.it

15 Ottobre 2008

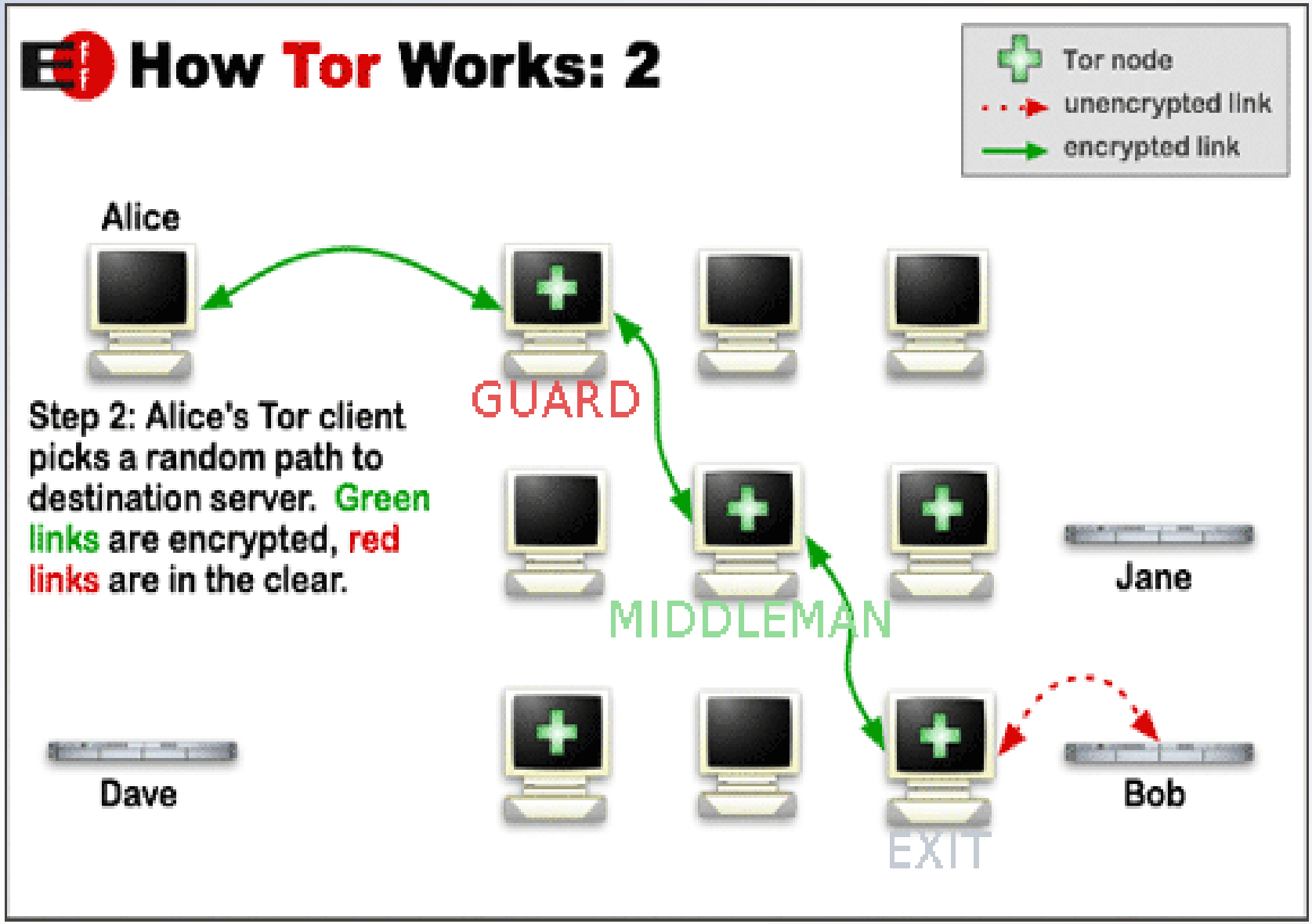
SMAU eAcademy – Milano

Licenza

Outline

- ***Tor (in 2 minuti)***
- Attacchi Passivi
- Attacchi Attivi
- Attacchi alle autorità di directory
- Conclusioni

Tor (in 2 minuti)



- Tor (in 2 minuti)
- ***Attacchi Passivi***
- Attacchi Attivi
- Attacchi alle autorità di directory
- Conclusioni

Osservazione dei pattern di traffico - Attacco

- Se osserviamo il traffico in uscita da un utente Tor non possiamo ricavarne la destinazione ne il contenuto
- Possiamo, però, profilare l'azione compiuta dall'utente
  - il traffico di un torrent è voluminoso e continuo
  - Il traffico http è intervallato

Osservazione dei pattern di traffico - Difesa

- Non è un attacco facile da portare a termine (mai dire mai!)
- Tor accorpa più flussi di dati in un singolo circuito

Estrazione contenuti (leaking) - Attacco

- Mentre il traffico viaggia attraverso la rete Tor viene cifrato
- Non è detto che lo sia anche all'uscita!
- Un attaccante può osservare il traffico in chiaro in uscita da un exite node e inferire sul client che ha inoltrato la richiesta
- Pensiamo al protocollo http:
  - User agent
  - Cookies
  - Parametri GET e POST

Estrazione contenuti (leaking) - Difesa

- Il filtering non è proprio l'obiettivo di Tor...
- Ci pensano Privoxy o Polipo (information stripping)
- Ci pensa TorButton (blending)
  - User agent
  - Linguaggio
  - Time zone
  - Dimensione della finestra (!!!)
- E il resto? Usare protocolli cifrati :)

Estrazione comportamentale (clustering) - Attacco

- Tor è altamente configurabile
  - Differenti tempi di rotazione dei circuiti
  - Differente scelta dei nodi
- Un attaccante può clusterizzare gruppi di utenti osservandone il comportamento
- I gruppi con minor numero di individui sono facilmente identificabili

Estrazione comportamentale (clustering) - Difesa

- Attenersi quanto più possibile alla configurazione di default, specialmente per la creazione dei circuiti
- Settare il comportamento di Tor per bypassare un firewall è ok
- Farlo quando non ce ne è bisogno no!

Correlazione temporale - Attacco

- Un attacco dei più effettivi
- Un attaccante che è in grado di osservare sia il traffico del nodo di ingresso alla rete che quello del nodo di uscita è in grado di correlare i tempi di invio e ricezione dei pacchetti
- Sapendo chi ha inviato cosa si può capire a cosa fosse interessata la vittima
- Se il protocollo era in chiaro l'attaccante ha pure il contenuto

Correlazione temporale - Difesa

- Impedire all'attaccante di distinguire chi genera una connessione verso la rete Tor
  - Più client dietro un firewall/router sembrano uno solo
  - Elevare il ruolo del proprio client anche solo a quello di relay permette di generare diverse connessioni
- Evitare di scegliere guardia ed uscita nella stessa sottorete o in reti molto vicine tra loro (fix recente)

Correlazione sulla dimensione dei pacchetti - Attacco

- Simile al precedente
- Invece che osservare i tempi di risposta tra ingresso e uscita, l'attaccante controlla i volumi di traffico scambiati: se riesce a inferire pattern comportamentali simili allora è possibile correlare i due nodi

Correlazione sulla dimensione dei pacchetti - Difesa

- L'utilizzo del padding delle connessioni sarebbe ottimo
- Non è ancora utilizzato per evitare di impattare sulle performance di rete
- L'attacco viene mitigato dalla comportamento stesso dei nodi:
  - Accorpano più flussi di informazione nei circuiti che costruiscono
  - Volumi di traffico differenti tra pacchetti in ingresso e in uscita

Fingerprinting - Attacco

- Simile al precedente ma elimina la necessità di osservare l'uscita
- L'attaccante conosce un set di dati e pattern di accesso
- Confronta queste informazioni con il traffico generato da un nodo client
- Se la generazione di traffico combacia con i pattern, ha correlato l'ingresso con l'uscita

Fingerprinting - Difesa

- Stessa del punto precedente

- Tor (in 2 minuti)
- Attacchi Passivi
- ***Attacchi Attivi***
- Attacchi alle autorità di directory
- Conclusioni

Compromissione chiavi - Attacco

- Se un attaccante conosce la chiave di sessione di un nodo è in grado di controllare la sessione a proprio piacimento
- Se un attaccante conosce la chiave di un nodo, può impersonare quel nodo a tempo indefinito
- A seconda di quali/quanti nodi vengono compromessi, l'attacco può variare da quasi inutile (middleman) a catastrofico (metà delle directory)
- Hello, Debian RNG!

Compromissione chiavi - Difesa

- Rotazione rapida delle chiavi di sessione
- Blacklisting delle chiavi generate con l'RNG compromesso

Tagging - Attacco

- Un attaccante può modificare il traffico generato dai propri nodi inserendo dei tag arbitrari nei flussi di informazione scambiati
- La registrazione e ricerca dei tag permette di svelare il cammino di un client

Tagging - Difesa

- Sempre siano lodati i check di integrità!
- Amen ;-)

Nodi di uscita “rogue” - Attacco 1

- 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

Nodi di uscita “rogue” - Attacco 2

- 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 di ads pubblicitari!)

Nodi di uscita “rogue” - Difesa

- 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

Nodi e client – Attacco 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

Nodi e client – Attacco 2

- 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

Nodi e client - Difesa

- 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/

Blocco delle connessioni - Attacco

- 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: https://www.torproject.rg/tordnsel/ 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

Blocco delle connessioni - Difesa

- A volte il primo problema è una soluzione temporanea necessaria, la soluzione migliore rimane educare utenti e amministratori del servizio offerto
  - Chi si ricorda dell'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 o yahoo! mail (Tor 0.2.0.13-alpha e successivi)

- Tor (in 2 minuti)
- Attacchi Passivi
- Attacchi Attivi
- ***Attacchi alle autorità di directory***
- Conclusioni

Search & Destroy - Attacco

- Il consenso sullo stato della rete viene generato dalle autorità di directory votando in base alla loro visione della rete
- L'obiettivo dell'attaccante è abbattere alcune di queste autorità per indurre la pubblicazione di uno stato non valido o non funzionante

Search & Destroy - Difesa

- Moria1 e Moria2 sono ospitate al MIT...
- ...Dannenberg è hostata dal CCC!
- Le autorità sono hardcodate nel client
- Se più della metà cade è necessario un intervento manuale dell'operatore del client per accettare il consenso

Poisoning - Attacco

- No, Kaminsky non c'entra ;-)
- Un attaccante può compromettere una o più autorità per pubblicare informazioni errate
- Ok... magari c'entra come vettore di attacco... :-P

Poisoning - Difesa

- Indipendenza degli operatori di autorità
- Diffusione geografica
- Resistenza agli attacchi, hardening
- Rete di fiducia

Splitting (Social Engineering) - Attacco

- L'attaccante mira a raggirare uno o più operatori in modo che tolgano la fiducia verso un terzo (o terzi)
- Così facendo si ottiene uno split del consenso generato dalle autorità
- Si possono isolare gli utenti a seconda di quale consenso abbiano ricevuto

Splitting (Social Engineering) - Difesa

- Nessuna :'(
- Numero limitato di autorità (7)
- Rete di fiducia

Tricking - Attacco

- L'attaccante convince un autorità a listare come non validi uno o più nodi perfettamente funzionanti
- O viceversa

Tricking - Difesa

- Il blacklisting è attualmente manuale
- Si sta sviluppando un modo per la ricerca automatica di nodi di uscita malfunzionanti (GSoC 2008)
  - Speriamo sia robusto :-P

- Tor (in 2 minuti)
- Attacchi Passivi
- Attacchi Attivi
- Attacchi alle autorità di directory
- ***Conclusioni***

Conclusioni

- *“This is experimental software. Do not relay on it for strong anonimity.”*
- L'onion routing è un protocollo robusto
- Un attaccante globale forte e motivato è in grado di scardinare il protocollo via attacchi statistici
- Per uno scenario molto meno pericoloso, gli attacchi più efficaci sono quelli che *aggirano* l'uso di Tor

Ringraziamenti

- A Roger Dingledine, Nick Mathewson, Peter Palfrader, tutti gli altri sviluppatori di Tor per portare avanti un tale progetto
- A Ren Bucholz per l'immagine 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 e per quello di “Vulnerabilities in Tor: past, present, future”, presentato all'ultimo Defcon

Fine

- Domande?