Security Summit
Milano, 24-26 marzo 2009

L'evoluzione di Tor

uno sguardo al futuro della privacy

Marco A. Calamari
Progetto Winston Smith – Sikurezza.org
marcoc@{winstonsmith.info|sikurezza.org}

Pubblicita'

Il ***Progetto Winston Smith*** e' una organizzazione informale di persone preoccupate per la privacy in Rete.

Realizza iniziative di tipo tecnologico, legale e formativo per favorire l'uso delle tecnologie di comunicazione privata e sicura, e gestisce numerosi remailer, router Tor ed altri server per la privacy. Organizza annualmente il convegno **e-privacy**.

E' una organizzazione “ricorsiva”, infatti fornisce una prova di fattibilita' del completo anonimato raggiungibile con la tecnologia realizzandosi tramite una personalita' virtuale, collettiva ed anonima, che, citando il lungimirante ed attualissimo romanzo “*1984*” prende il nome dal protagonista, *Winston Smith*.

Maggiori informazioni: *https://www.winstonsmith.info*

Sommario

- Il manifesto
- Le origini
- Anonymous proxy
- Crowds
- Una pillola di Tor
- Una storia “esemplare”
- I punti di forza
- I punti deboli
- Tor oggi
- Un piano triennale

Manifesto ...

Tor (The Onion Router) e' il software per la privacy piu' diffuso nella storia dei sistemi crittografici.

Permette di utilizzare le normali applicazioni per la comunicazione senza modifiche, e' di semplice installazione ed utilizzo, ed ha una base installata stimata a 400.000 utenti.

Questo successo che dura ormai da anni e' frutto anche di un lavoro di coordinamento e di pianificazione della sua evoluzione, e di una gestione del gruppo di sviluppo che collega gli sviluppatori con la realta' dei loro utenti e con la societa'.

L'intervento fornira' alcuni cenni sulle problematiche e le prospettive di sviluppo di Tor nei prossimi anni.

... Manifesto

Fornire una rete anonima funzionante in Internet oggi e' una sfida continua.

Noi vogliamo un software che soddisfi le necessita' degli utenti. Vogliamo anche mantenere la rete attiva e funzionante in modo da poter soddisfare piu' utenti possibili.

Sicurezza e usabilita' non devono escludersi a vicenda: se l'usabilita' di Tor aumenta, attrarra' piu' utenti, che aumenteranno le possibili sorgenti e destinazioni di ogni connessione, aumentando di conseguenza la sicurezza di ciascuno. Le attuali tendenze nel mondo legale, politico e tecnologico minacciano l'anonimato come mai prima d'ora, minando la possibilita' di leggere e parlare liberamente online. Questa situazione mina anche la sicurezza nazionale e delle infrastrutture critiche, rendendo le comunicazioni tra persone, organizzazioni, aziende e governi piu' vulnerabili all'analisi.

Le origini

Nel **1981** David Chaum introdusse e sistematizzo' il concetto di **Mix-net** **[1]** .

Nel **1986** una famosa querelle giuridica, suscitata da una iniziativa della religione di Scientology provoca l'inizio della **reazione del gruppo Cypherpunks** (niente piu' di una maillist dell'epoca) e la nascita dei sistemi crittografici di comunicazione moderni, implementando per la prima volta in maniera crittograficamente robusta il meccanismo delle **Mix-net** (maggiori particolari nel seguito).

Negli **anni '90** Paul Syverson ed altri estesero l'applicazione delle Mixnet all'incapsulamento crittografico per il routing di pacchetti di informazioni, il cosiddetto **Onion Routing** **[2]** .

Tutto e' partito dal lavoro di Chaum; da allora pare che nessuno abbia avuto idee radicalmente nuove, ma che tutti abbiano costruito PET (Privacy Enhancing Technologies) sempre migliori, edifici tecnologici sempre piu' complessi ed efficaci continuando a basarsi sulla solida fondazione delle Mixnet.

Anonymous proxy ...

All'inizio degli **anni '90** il web fa “esplodere” internet, e la navigazione web supera la posta elettronica come strumento di scambio delle informazioni. Immediatamente i ricercatori che si occupano di privacy in Rete percepiscono che la navigazione via web, oltre ad essere facilmente intercettabile presso i provider, lascia informazioni personali sui log dei server web, e che la profilazione degli utenti diventa semplice ed economica se si utilizzano metodi tipici del protocollo HTTP quali referral e cookie.

Una risposta parziale viene dallo sviluppo del protocollo SSL che permette di criptare end-to-end le sessioni di navigazione e risolve almeno il problema dell'intercettazione da parte degli ISP, ma non gli altri.

Il concetto di proxy anonimizzante, cioe' di una terza parte fidata che agisce “navigando al tuo posto” senza tenerne traccia sui suoi log risolve in buona parte il problema della profilazione (ma non quella fatta con i cookies). Gestire problemi di privacy tramite l'uso di terze parti fidate e' pero' **solo un tappabuchi, ma non una soluzione reale**.

... Anonymous proxy ...

Nel **1997** Michael K. Reiter e Aviel D. Rubin pubblicano un **[4]** documento fondamentale *"**Crowds**: Anonymity for Web Transactions"* in cui descrivono un approccio P2P al problema, che non necessita di terze parti fidate, ma della collaborazione paritaria di molti interessati.

Crowds, che deriva il suo nome dalla descrizione *"...blending into a crowd" - "scomparire in mezzo alla folla"* prevede la creazione di una rete di client con funzioni di proxy pubblici, che possono essere utilizzati come proxy locali dei normali browser web.

Il proxy Crowds locale cripta end2end la sessione e la indirizza non verso la destinazione ma verso un altro proxy scelto a caso.

Il processo si ripete fino a quando uno dei proxy decide di mettere in chiaro la comunicazione e spedirla al server web a nome suo.

... Anonymous proxy

Se molte persone usano contemporaneamente Crowds, e prendono precauzioni elementari come disabilitare i cookies ed i contenuti attivi, la privacy della navigazione e' garantita.

All'epoca pero' la ricerca sull'analisi statistico/temporale del traffico non era avanzata come ai nostri giorni, e non era pensabile, come e' oggi, un avversario di alto profilo che potesse intercettare una grossa frazione del traffico di Internet.

Ci sarebbe quindi da essere piuttosto pessimisti sull'efficacia di un sistema cosi' semplice e senza nessun meccanismo di difesa contro nodi rogue se, come vedremo piu' avanti, anche la ricerca sui proxy anonimizzanti non avesse conosciuto grossi avanzamenti.

Una Pillola di Tor

Tor ...

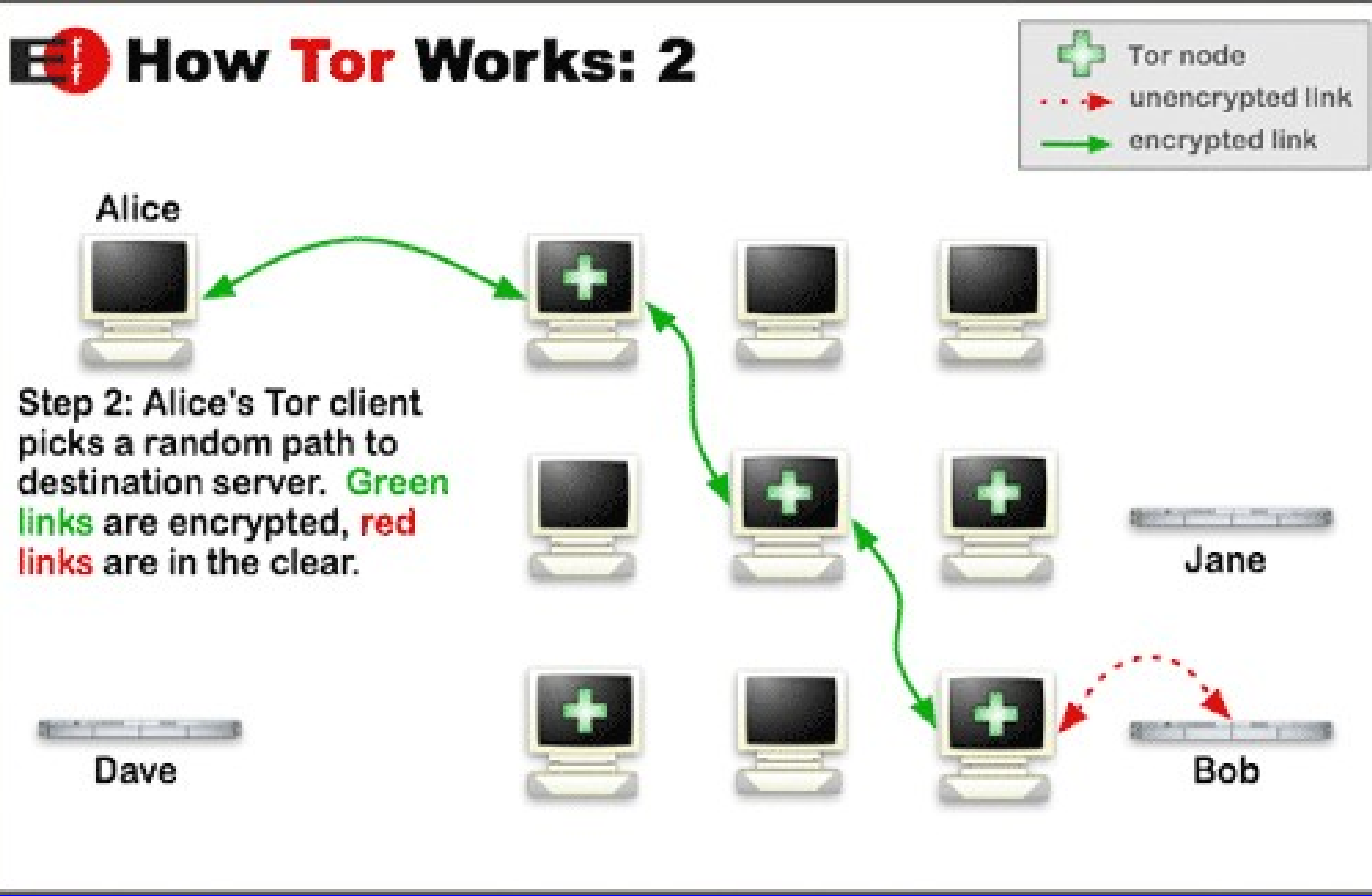
Tor - The second generation Onion Routing **[3]** e' una rete anonimizzante di proxy criptati che permette di rendere anonima qualunque comunicazione avvenga tramite l'utilizzo di TCP.

Implementata come proxy SOCKS, permette di usare tutti i piu' comuni programmi per l'accesso ad internet quali browser web, chat, posta elettronica, newsgroup e qualunque applicazione utilizzi solo circuiti TCP (niente UDP, quindi niente streaming).

Tor e' una PET di seconda generazione, sviluppata con particolare cura e che pone a livello di progettazione la difesa anche legale (plausible deniability) del degli utenti e dei gestore di router Tor.

Possiede una struttura basata su quattro tipi di nodi: **client, relay, router** e **directory server**

... Tor


How Tor Works: 2
Tor node
unencrypted link
encrypted link
Alice
Step 2: Alice's Tor client picks a random path to destination server. Green links are encrypted, red links are in the clear.
Jane
Dave
Bob

Una storia “esemplare”

Senza la pretesa di tracciare nei dettagli la storia del progetto Tor, elenchiamo alcuni avvenimenti importanti in una primitiva timeline:

• l'idea originale di Onion Routing concepita' da Syverson e' di un programmatore professionista che la realizza in un ambiente di lavoro altamente formalizzato (laboratori di ricerca della marina militare degli Stati Uniti)

• questa idea ha attratto l'attenzione di alcuni dei maggiori (giovani) esperti nella ricerca sulle reti anonime, che ne hanno fatto il loro cavallo di battaglia professionale ed accademico, con un circolo virtuoso vantaggioso sia per loro che per l'applicazione.

• l'efficacia crittografica ha attratto finanziamenti militari che ne hanno permesso uno sviluppo non basato solo sul puro volontariato.

• l'efficacia come strumento di difesa dei diritti civili in Rete ha attratto altri finanziamenti da EFF che ne intende(va) promuovere gli effetti virtuosi per la privacy delle persone.

I punti deboli

Tor anonimizza la vostra connessione TCP, facendola uscire attraverso un router Tor scelto a caso, **MA** da solo .....

NON nasconde l'appartenenza alla mixnet TOR

NON protegge l'ultima parte della connessione dal router Tor di uscita fino al server di destinazione

NON protegge le informazioni trasmesse

NON impedisce alle applicazioni di far uscire informazioni rivelatrici attraverso la normale Rete (es. richieste DNS)

NON impedisce a contenuti passivi od attivi di rivelare l'identita' del mittente (cookies, javascript) su un canale esterno nascosto.

NON impedisce l'**harvesting** (spigolatura) di informazioni da parte di un router di uscita malizioso

I punti di forza ...

Tor implementa sofisticati sistemi atti a resistere agli attacchi classici alle mixnet in generale, a quelli noti ai sistemi di routing a pacchetto ed a quelli specifici contro l'onion routing e l'applicazione stessa. Probabilmente questa continua attenzione verso la resilienza ad attacchi dell'applicazione portata, avanti senza perdere di vista gli obbiettivi di usabilita' e scalabilita', e' il punto di forza del progetto.

Altro punto di forza e' la struttura di fiducia del directory server; ciascun directory server possiede le proprie informazioni e le mantiene e le aggiorna autonomamente. Durante questo processo confronta le sue informazioni con quelle degli altri directory server e se queste sono abbastanza simili alle proprie li certifica. Il processo e' mutuo, quindi a regime ogni dirserver (attualmente 6) e' certificato dagli altri. Se avvenisse un tentativo di sovversione di un server alterando le informazioni che contiene quest verrebbe escluso dagli altri in maniera automatica, ed il fatto sarebbe rilevabile da tutti I nodi.

... I punti di forza

Il progetto Tor ha incoraggiato/supportato lo sviluppo di:

- **interfacce grafiche (Vidalia)**
- **applet, (Torbutton)**
- **proxy (Polipo)**
- **bundle (Torbrowser bundle)**
- **distribuzioni live e VM (Incognito)n**
- **nodi informativi.**

Tor oggi

Tor e' ormai da tre anni l'unica applicazione crittografica per la privacy ampiamente diffusa in Rete con numeri che lo pongono allo stesso livello delle piu' diffusa applicazioni sia commerciali che libere. Solo Freenet la segue faticosamente in questa “classifica”, ma con un distacco che pare incolmabile

Mantiene un'alta usabilita' e facilita' di installazione che lo rende adatto anche per utenti occasionali e senza particolari skill informatici.

Nella sua evoluzione ha seguito quella del quadro legale della privacy e dell'intercettazione in Rete, cercando di fronteggiarne o mitigarne, per quanto possibile, gli effetti negativi per la privacy e la riservatezza in Rete.

Ha affrontato inoltre, finora con notevole successo, I problemi legati alla scalabilita' durante una crescita che continua senza sosta.

Un piano triennale ...

Tor e' l'unica applicazione per la privacy che possieda un chiaro, dettagliato, aggiornato e condiviso piano di sviluppo.

Questa Roadmap 2008-2011 **[5]**, realizzata da uno degli autori originali, Roger Dingledine, definisce gli itinerari di sviluppo del progetto confrontandoli ed ordinandoli con le priorita' e la dimensione delle risorse necessarie.

Non dobbiamo dimenticare che le risorse del progetto Tor, grandi se paragonate a quelle di un tipico progetto di FOSS, sono poca cosa rispetto a quelle di una applicazione commerciale di successo.

Gli obbiettivi sono ambiziosi e complessi, e vanno ben oltre il tempo disponibile oggi.

Per questo motivo ci limiteremo ad elencare I principali, riservando alla sessione Q&A gli approfondimenti su alcuni di essi.

... Un piano triennale

- Supporto del protocollo UDP per funzionare in modalita' connectionless e massimizzare le possibilita' di utilizzo attraverso proxy, router e NAT

- Supporto avanzato dell'utilizzo dei nodi bridge per permetterne un efficace utilizzo per gli utenti che temano attacchi di tipo legale (e.g. Cina).

- Normalizzazione del fingerprinting della rete Tor per contrastare attacchi di analisi del traffico rivolti contro singoli nodi

- Nuove strategie di distribuzione degli indirizzi dei bridge con l'uso di canali atipici (SMS, World of Warcraft, radio)

- Miglioramento della gestione dei nodi relay da parte delle dirserver

- Supporto di ambienti destinati alle applicazioni mobili (Android)

Grazie a tutti per l'attenzione

ci sono domande ?

Potete contattarmi qui: ***marcoc@winstonsmith.info***

Il Progetto Winston Smith

mail: ws@nym.panta-rhei.eu.org

web: http://www.winstonsmith.info/pws

tor: http://5zaspldty2calvcq.onion/

freenet: **USK@RU-C2q5kN7K62WO3seMMjSTUY8izF2vCFyVFOnLf~Q0,wxvGO2QMT6IN9c7dNUhHeHnXVVwhq8YLbQL~DlMA7YE,AQACAAE/pws/4**

Letture suggerite

- [1] **Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms** - *David L. Chaum, 1981* http://www.weidai.com/mix-net.txt
- [2] **Hiding Routing Information -** *David M. Goldschlag, Michael G. Reed, and Paul F. Syverson*, 1996 - Workshop on Information Hiding, Cambridge – http://www.onion-router.net/Publications/IH-1996.pdf
- [3] **Tor: The Second-Generation Onion Router** – *R. Dingledine et al., 2004* – http://www.torproject.org/svn/trunk/doc/design-paper/tor-design.pdf
- [4] **Crowds: Anonymity for Web Transactions -** *Michael K. Reiter, Aviel D. Rubin, 1997* ACM Transactions on Information and System Security
- [5] **Tor Development Roadmap, 2008-2011** - Roger Dingledine
- **Tor** http://tor.eff.org
- **Biografia onnicomprensiva sull'anonimato** http://freehaven.net/anonbib/full/date.html
- **Progetto Winston Smith** http://www.winstonsmith.info