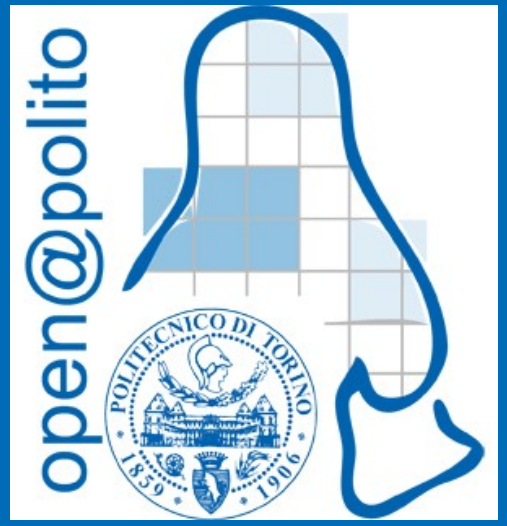
Tor

Di Andrea Gabbani

Con il supporto di:



Cosa e' Tor?

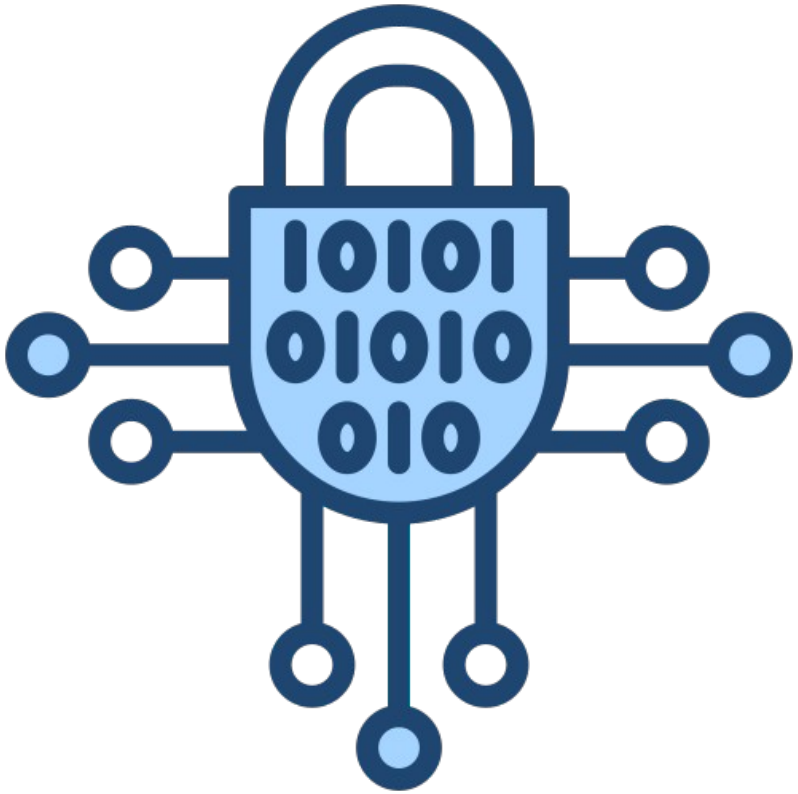
- Tor – The Onion Router (ma non scrivetelo TOR...)
- "Tor e' un programma [...] che ti protegge rimbalzando le tue comunicazioni in una **rete distribuita di relay** messi a disposizioni da volontari in tutto il mondo: impedisce a qualcuno che osserva la tua connessione internet di sapere quali siti visiti, e impedisce ai siti che visiti di sapere dove ti trovi. Questa serie di relay di volontari si chiama la **Rete Tor.**"

Threat Model

- Cosa stiamo proteggendo, e da chi?
- “Presumiamo un avversario in grado di osservare una porzione del traffico di rete, che puo’ generare, modificare, eliminare, o ritardare il traffico; che puo’ operare dei relay Tor propri; e che puo’ compromettere una frazione dei relay.”
- Confrontiamo Tor e HTTPS...

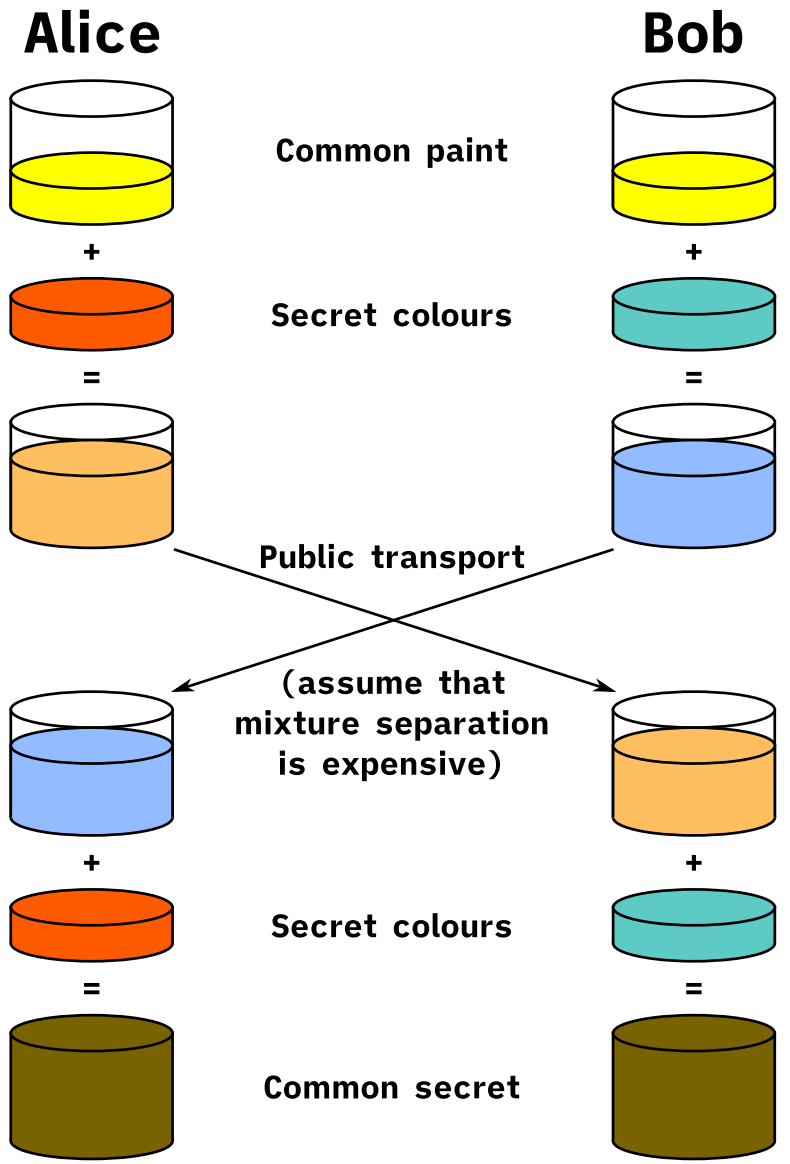
Alcune nozioni di crittografia...

- Diffie-Hellman
- AES-128
- TLS



Diffie-Hellman

- Condivisione sicura di una chiave simmetrica su canali pubblici
- Usata da Tor per lo scambio di chiavi tra il client e i relay
- Avviene in maniera “telescopica”, nessun nodo ha tutte le chiavi



AES-128

- Algoritmo di cifratura simmetrica con chiave di lunghezza variabile
- Tor usa una chiave da 128 bit
- Usata per cifrare i contenuti delle “celle”

TLS

- Lo stesso protocollo crittografico usato per le connessioni HTTPS
- Usato per cifrare le comunicazioni tra relay e relay
- Completamente indipendente dal (eventuale) TLS usato per raggiungere un sito web tramite HTTPS

Relay (o router/nodi)

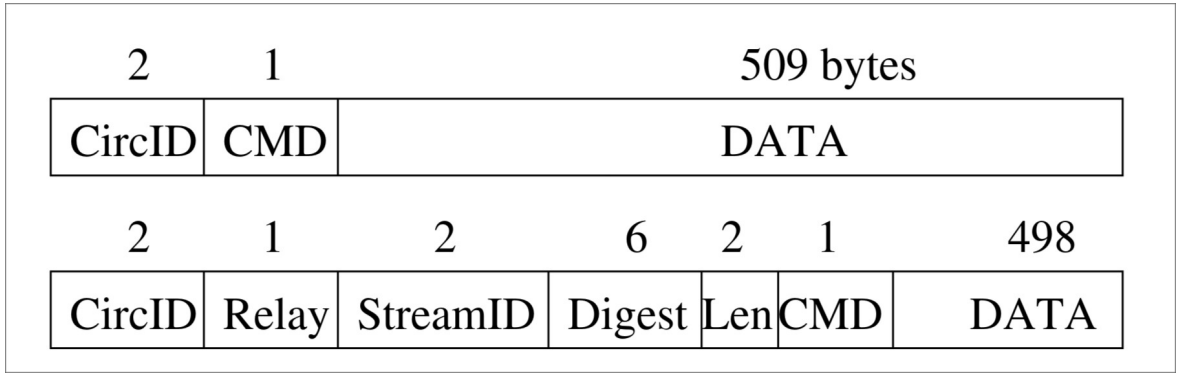
- Unita' fondamentale della rete Tor
- Operati indipendentemente da volontari in tutto il mondo
- Entry/Guard, Middle, Exit – componenti principali
- Directory – nodo speciale contenente lista dei nodi
- Bridge – relay extra che permette di nascondere l'utilizzo di Tor

Circuito

- Unione di relay che connette un client a un server
- Composto da un minimo di 3 nodi
- Ogni relay conosce solo i propri vicini, mai il percorso completo
- Ricostruito periodicamente in background per motivi di sicurezza

Cella

- Unita' fondamentale di comunicazione nella rete Tor
- Lunghezza fissa (512 Byte) – impedisce attacchi dipendenti dalla correlazione tra il contenuto e la dimensione
- Celle di controllo – usate nella gestione dei circuiti
- Celle di relay – usate nella trasmissione di flussi dati



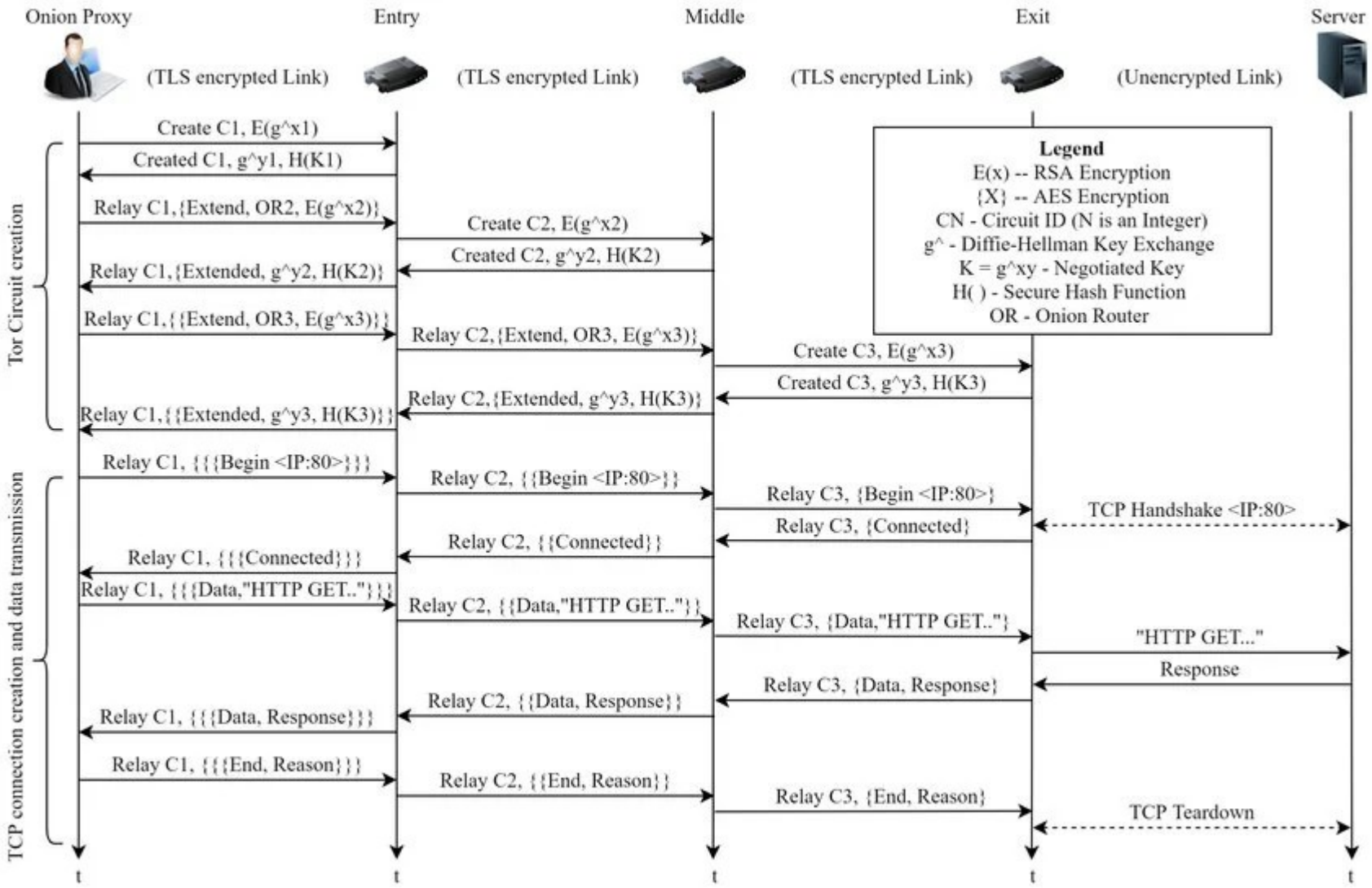
Directory

- Relay speciali che contengono una lista pubblica di relay utilizzabili per costruire i circuiti
- Attualmente 9 in tutto il mondo, gestiti da operatori fidati
- Funzionano con un sistema di Consensus – devono essere d'accordo sugli IP dei relay, le loro capacita', larghezza di banda...
- Assegnano ruoli e flag ai relay (Entry, Exit, Fast, Stable...)

Costruzione di un Circuito

- Il client sceglie i relay dalla directory, e costruisce il circuito in maniera “telescopica”
- Nessun relay ha tutte le informazioni necessarie per ricostruire il percorso completo
- Le celle con comando “CREATE” e “EXTEND” vengono usate per creare ed estendere il circuito

Costruzione di un Circuito



Bridge

- Relay non elencati nella directory disponibili su richiesta
- Molto piu' difficili da bloccare o restringere
- Strutturalmente quasi identici a un relay normale, ma con una configurazione leggermente diversa

Pluggable Transport

- La connessione verso il bridge e' sempre riconoscibile come Tor
- I Pluggable Transport mascherano il traffico Tor facendolo sembrare altro
- obfs4 – dati casuali
- snowflake – traffico WebRTC
- meek – traffico HTTPS verso un CDN (AWS o Azure)
- Non utilizzabili senza bridge – richiedono una componente server

Servizi Onion

- Permettono a un server di nascondere il proprio indirizzo IP sulla rete Tor, oltre che nascondere l'IP del client
- Cifratura end-to-end integrata e indipendente da certificati pubblici – l'indirizzo e' la chiave pubblica!
- Il traffico tra client e server non esce mai dalla rete Tor
- Come viene costruita una connessione con un servizio onion?

Software basato su Tor

- Tor Browser – Firefox modificato per l'utilizzo con Tor
- Tails – Sistema operativo "amnesico" costruito attorno a Tor fatto per non lasciare tracce sul computer usato
- Orbot – Applicazione Android per reindirizzare il traffico delle applicazioni tramite la rete Tor
- Whonix – Sistema operativo che reindirizza tutto il traffico tramite la rete Tor, con svariati miglioramenti di sicurezza

Vulnerabilita' di Tor

- Attacchi passivi – correlazione del traffico, website fingerprinting
- Attacchi attivi – relay operati o compromessi da avversari
- Livello applicazione – browser fingerprinting, leak DNS/WebRTC
- Errore umano – errori di configurazione, usare la stessa identita' dentro e fuori dalla rete Tor

Come proteggersi?

- Tor Browser e' costruito per mitigare molti attacchi a livello applicazione (se non viene modificato intenzionalmente o meno...)
- La rotazione periodica dei circuiti limita gli attacchi passivi basati sulla correlazione
- La quantita' dei relay rende inefficienti gli attacchi attivi
- Costruire un threat model adeguato e sviluppare una strategia di OPSEC (OPerational SECurity)
- Strumenti come Tails e Whonix aiutano a espandere il threat model oltre la rete

Tor + VPN?

- Client → VPN → Tor – metodo supportato, impedisce all'entry relay di vedere il tuo IP e nasconde il tuo utilizzo di Tor dal provider/rete, permettendone l'uso se bloccato o rallentato
- Client → Tor → VPN – metodo sconsigliato, il VPN agisce come "exit relay permanente", facilitando attacchi di correlazione del traffico
- In entrambi i casi, il VPN va considerato con cura (policy dei log, sicurezza, privacy del pagamento...) in quanto bisogna fidarsi di esso piu' del proprio provider/rete

Cavilli etici e legali

- Non sono un avvocato. Questi non sono consigli legali.
- Operare un relay puo' portare a seri problemi legali se fatto senza comprenderne la natura
- **ALTAMENTE SCONSIGLIATO** operare un exit relay da casa, in quanto apparente punto di origine per traffico di natura potenzialmente illegale
- Operare un relay =/= utilizzare la rete Tor

Contribuisci a Tor!

- E' estremamente facile aiutare il progetto Tor e i suoi utilizzatori
- Hosta un relay – entry, middle, e bridge portano con se' rischi minimi e sono hostabili da casa
- Contribuisci al codice – Tor e' open source, chiunque puo' aiutare
- Usa Tor – se aumentano gli utilizzatori, e' piu' difficile per un avversario monitorare la rete
- Parlane – ci sono molti miti e incomprensioni su Tor che hanno bisogno di essere sfatati

Fonti

- https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.html
- https://support.torproject.org/