Navigazione anonima con TOR

Tails TorBrowser Orfox, VPN, SSH anti tracking

Tails TorBrowser Orfox

Montebelluna Linux Users Group (MontelLUG)

LinuxDay2k17 - 28 ottobre 2017
c/o FabLab Castelfranco Veneto

Licenza d'utilizzo

Sommario

Anonimato, privacy, riservatezza, ...

per quale motivo usare questi strumenti?

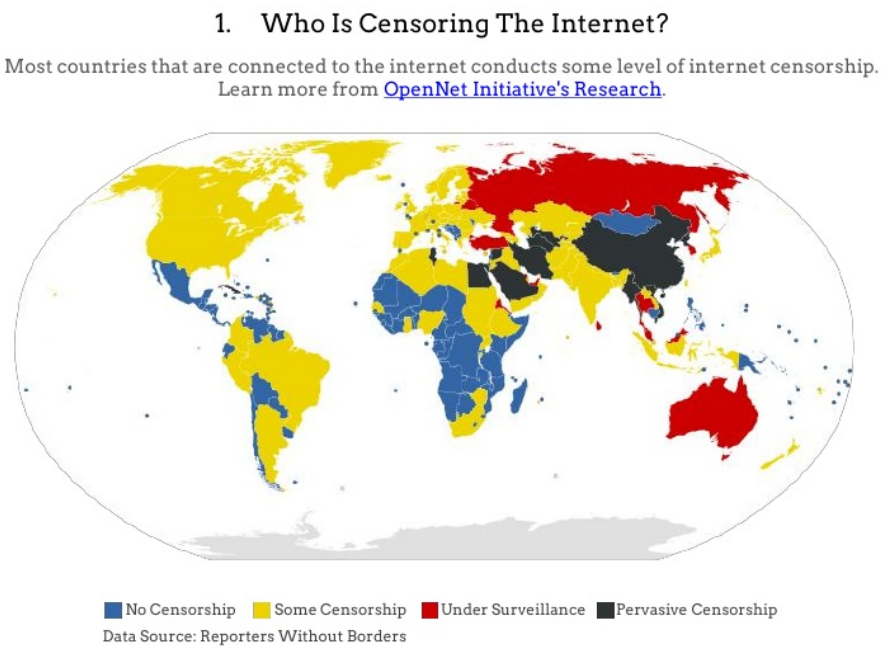
- per tutelare la nostra privacy ed evitare di essere profilati
- per tutelare la libertá di espressione ed evitare la censura
- per tutelare la democrazia
- per evitare le discriminazioni e le persecuzioni

`https://spreadprivacy.com/is-private-browsing-really-private/`

Anonimato, privacy, riservatezza, ...

La censura

Il numero degli attacchi della censura alla libertá e alla privacy su internet nel 2017 é stato senza precedenti (fonte torproject.org)



Anonimato, privacy, riservatezza, ...

La censura

Paesi in tutto il mondo cercano di limitare l'accesso al web, soffocare il dissenso e ridurre la privacy personale. Esempi:

- l'Egitto nel 2011
- il Venezuela a seguito dei disordini
- In Turchia si sta censurando internet
- Negli Stati Uniti, il Congresso ha consentito agli ISP di tenere traccia degli utenti e di vendere i loro dati

`https://it.wikipedia.org/wiki/Censura_di_Internet`

Anonimato, privacy, riservatezza, ...

La profilazione

La profilazione degli utenti non serve solo al marketing ed ad offrire i prodotti piú adatti agli utenti.
I dati sulla profilazione potrebbero esser utilizzati illegalmente per:

- discriminare i diritti fondamentali degli individui
- influenzare le scelte e le decisioni (anche democratiche) e la percezione della realtá (la bolla informativa)

Le soluzioni disponibili

Oggi parleremo di:

- TOR: se il nostro obiettivo é l'anonimato
- VPN e SSH: se il potenziale rischio si trova tra il nostro computer e internet (ISP, WiFi libere, censura, filtraggio)

Tor: sommario

3. TOR
   - Cos'é TOR
   - La distribuzione TAILS
   - Torbrowser: browser per computer
   - Orfox/Orweb con Orbot: per la navigazione sotto Android
   - Vidalia/Torsocks: per tutte le altre applicazioni

Cos'é TOR

Tor é l'acronimo di The Onion Router. É un sistema di comunicazione anonima per Internet basato su un particolare protocollo di rete.
Tor rende molto piú difficile (ma non impossibile) tracciare l'attivitá Internet dell'utente. (fonte Wikipedia.org)

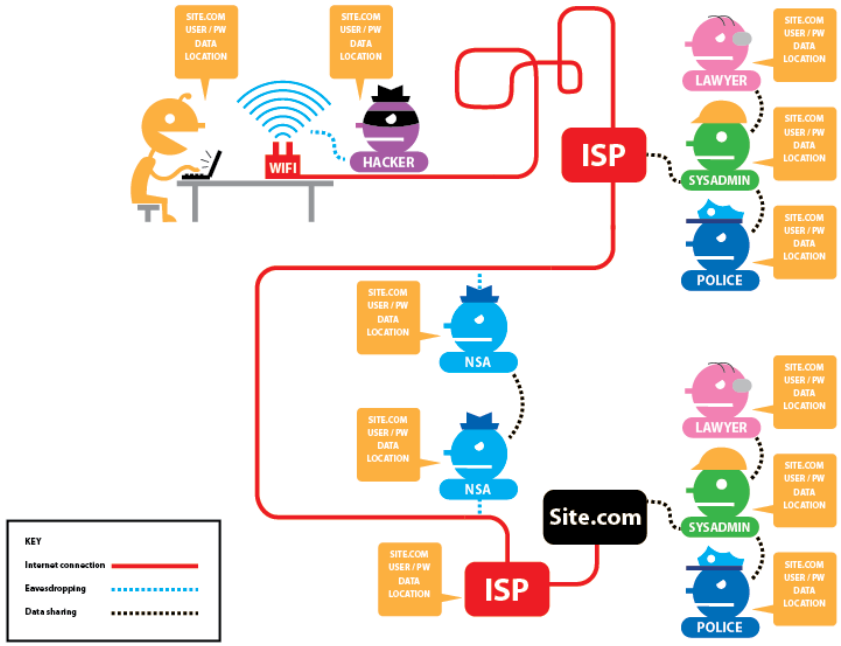
TorProject.org

torproject.org

Cos'é TOR

Come funziona: in estrema sintesi

Vediamo una rappresentazione grafica
Le comunicazioni **senza SSL e senza TOR**



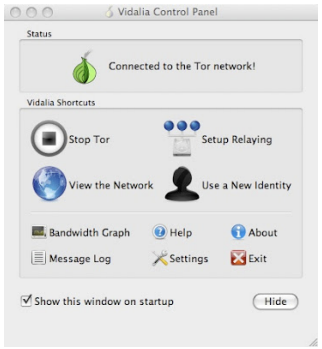
CON SSL ma senza TOR

Cos'é TOR

Soluzioni software disponibili:

TorBrowser

la Distribuzione
GNU/Linux Tails



il pacchetto
tor/Vidalia

Orfox

La distribuzione GNU/Tails

https://tails.boum.org/

- É una distribuzione GNU/Linux SOLO live CD/USB
- progettata per preservare la privacy
- per usare Internet in modo anonimo ed aggirare la censura
- forza ogni tipo di connessione ad Internet tramite la rete Tor
- non lascia tracce sul computer usato
- sfrutta gli ultimi tools criptografici disponibili per criptare files, emails e instant messaging

Torbrowser

https://www.torproject.org/

- é un Browser preimpostato per navigare tramite TOR
- sviluppato con Mozilla, basato su Firefox, Open Source
- utilizzabile in Microsoft Windows, Apple MacOS o GNU/Linux
- é portabile: non necessita di installazione

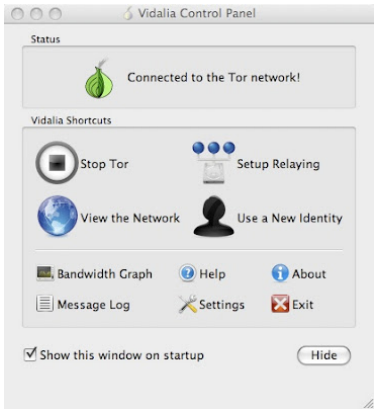
Orfox/Orweb con Orbot: per la navigazione sotto Android

https://www.torproject.org/

- riguardano gli smartphone ed in particolare Android
- Orfox e Orweb sono browser preimpostati per usare TOR
- Orbot é lo strumento tramite cui i browser si collegano alla rete TOR
- si installa tramite repositori di Google Play (o meglio) F-Droid

Vidalia/Torsocks: per fare altro

https://www.torproject.org/



- sconsigliato se si deve usare per navigare
- serve a consentire ad altre applicazioni di utilizzare la rete Tor tramite Socket
- puó servire per creare un nuovo Relay "The Tor network relies on volunteers to donate bandwidth"
- puó servire per fornire un "hidden service" ovvero un server che funziona nella rete Tor: es. `https://3g2upl4pq6kufc4m.onion/`

TOR non é del tutto sicuro!

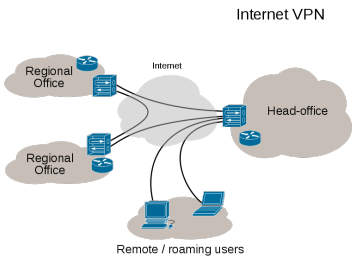
TOR funziona e rende anonima la navigazione, ma dei comportamenti errati possono render vano lo strumento. Si devono prendere determinate precauzioni:

- Per navigare é meglio usare Tor Browser che il tuo browser con Vidalia
- Non scaricare torrent tramite Tor (applicazioni insicure, rallentamento della rete)
- Se si usa un proprio browser disattivate i plugins (Flash, RealPlayer, Quicktime, ecc...)
- Usare sempre la versione HTTPS dei websites
- Non aprire i documenti scaricati mentre si é online
- In determinati casi usare i bridges (nel punto di accesso é identificabile il collegamento a Tor)

Altre soluzioni VPN e SSH: sommario

Altre soluzioni: VPN e SSH

VPN

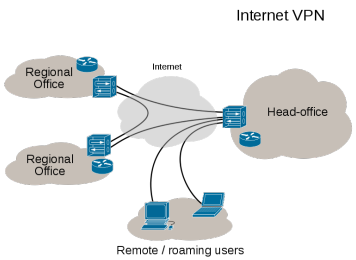


Una VPN (virtual private network) é una rete di telecomunicazioni privata, tra soggetti che utilizzano un protocollo di trasmissione pubblico e condiviso (Internet ad esempio)

Altre soluzioni: VPN e SSH

VPN

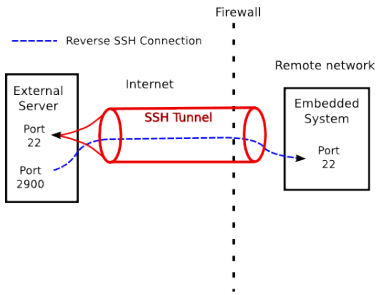
Scopi di una VPN:



- offrire alle aziende, a un costo minore, le stesse possibilitá delle linee private a noleggio, ma sfruttando reti condivise pubbliche
- trasmettere dati ed informazioni in modo riservato attraverso Internet tra soggetti tra loro distanti
- ottenere un maggiore grado di riservatezza, mascherando il proprio IP o i dati di navigazione al proprio ISP, attraverso un VPN provider (attenzione al rischio)
- collegarsi in modo sicuro ad internet anche da un punto di accesso non sicuro

Altre soluzioni: VPN e SSH

SSH



SSH é un File Transfer Protocol o SFTP ovvero un protocollo di rete che prevede il trasferimento dei dati e funzionalitá di manipolazione.

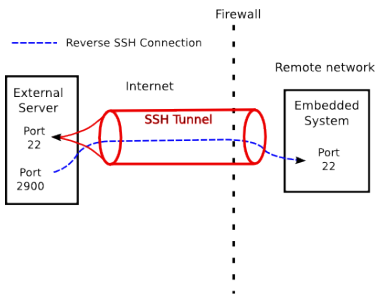
Una VPN si puó realizzare con questo protocollo

Altre soluzioni: VPN e SSH

SSH

Scopi per usare SSH:

- creare una VPN veloce (anche con il router di casa)
- collegarsi in modo sicuro ad un server
- trasmettere dati ed informazioni in modo riservato attraverso Internet (anche l'intera interfaccia di un computer remoto)
- superare un firewall, ottenendo mascheramento del proprio IP o i dati di navigazione al proprio ISP
- collegarsi in modo sicuro ad internet anche da un punto di accesso non sicuro (wifi libero)



Raccomandazioni: sommario

5. Raccomandazioni contro il tracciamento e la profilazione

Raccomandazioni contro il tracciamento e la profilazione

Se la nostra preoccupazione non é la navigazione anonima, la censura, la privacy in senso esteso, possiamo anche evitare di utilizzare TOR; con alcune piccole attenzioni possiamo ridurre il rischio di profilazione

- Utilizzare Firefox in modalitá anonima + estensioni HTTPS Everywhere, uBlock Origin, Ghostery, NoScript
- Effettuare le proprie ricerche su Internet con motori di ricerca che non ci tracciano: esempio `https://duckduckgo.com/`

Raccomandazioni contro il tracciamento e la profilazione

- Impostare il router o il computer con dei DNS specifici: esempio `http://www.fooldns.com/`
- Limitare l'uso dei software di Google (Gmail,Drive,Calendar) e socialnetwork (Facebook) `https://spreadprivacy.com/how-to-remove-google/`
- Usare la testa

DOMANDE???

Linkografia:

- https://www.eff.org/
- https://guardianproject.info/
- https://prism-break.org/
- https://myshadow.org/browser-tracking
- http://www.fooldns.com/
- https://spreadprivacy.com/
- https://protonmail.com/

Ringraziamenti

Da parte di tutto il MontelLUG, ringrazio in particolar modo Gloria e Mirco ed il FabLab di Castelfranco Veneto per la disponibilitá degli spazi, la cortesia e l'impegno dimostrato per la realizzazione del LinuxDay 2017.

Grazie