

Tor: le origini...

Pierluigi Perri – Jan Reister

Andrea Trentini – Giovanni Ziccardi

Università degli Studi di Milano

Il nome “Tor” (e non TOR...)

“The name "Tor" can refer to several **different** components”.

- (1) The Tor **software**: a **program** you can run on your computer that helps keep you **safe** on the Internet. Tor protects you by **bouncing** your communications around a distributed network of **relays** run by **volunteers** all around the world: it prevents somebody watching your Internet connection from learning **what sites you visit**, and it prevents the sites you visit from learning **your physical location**.
- (2) The Tor **network**: This set of **volunteer relays** is called the Tor network.
- (3) The Tor **Project** is a **non-profit** (charity) organization that maintains and develops the Tor software.

1. Una overview

- Le origini **militari**: “Tor was originally designed, implemented, and deployed as a **third-generation onion routing project** of the U.S. Naval Research Laboratory”.
- (Anche) l’**approccio** militare e la **protezione delle comunicazioni**: “It was originally developed with the **U.S. Navy in mind**, for the primary purpose of protecting **government communications**”.
- Si è evoluto in uno **strumento duttile**: “Today, it is used every day for a wide variety of purposes **by normal people**, the military, journalists, law enforcement officers, activists, and many others”.

Onion Routing

- Cosa è: “Onion Routing is a **distributed overlay network** designed to **anonymize** TCP-based applications like web browsing, secure shell, and instant messaging”.
- “**Percorsi**” e “**circuiti**” e idea di “**conoscenza reciproca**”: “Clients choose a path through the network and build a circuit, in which each node (or “onion router” or “OR”) in the path **knows** its predecessor and successor, but no other nodes in the circuit”.

In estrema sintesi:

- Il cuore (1): un network di tunnel virtuali per privacy e sicurezza. “Tor is a **network of virtual tunnels** that allows people and groups to **improve their privacy and security** on the Internet”.
- Il cuore (2): un’ottima base per costruirci “sopra” qualcosa di sicuro con “**incorporata**” la privacy. “It also enables software developers to **create** new communication tools with **built-in privacy features**”.
- Humus per applicazioni per la condivisione di informazioni: “Tor provides the foundation for a range of applications that allow organizations and individuals to **share** information **over public networks** without compromising their privacy”.

Il primo paper

Tor: The Second-Generation Onion Router

- Roger Dingledine, The Free Haven Project, arma@freehaven.net
- Nick Mathewson, The Free Haven Project, nickm@freehaven.net
- Paul Syverson, Naval Research Lab, syverson@itd.nrl.navy.mil

Abstract del paper

We present Tor, a circuit-based low-latency anonymous communication service. This second-generation Onion Routing system addresses limitations in the original design by adding perfect forward secrecy, congestion control, directory servers, integrity checking, configurable exit policies, and a practical design for location-hidden services via rendezvous points.

Abstract

- Tor works on the real-world Internet, requires no special privileges or kernel modifications, requires little synchronization or coordination between nodes, and provides a reasonable tradeoff between anonymity, usability, and efficiency. We briefly describe our experiences with an international network of more than 30 nodes. We close with a list of open problems in anonymous communication.

I possibili usi:

- Evitare il **tracciamento** e la **profilazione** durante la navigazione o aggirare **blocchi**: “Individuals use Tor to keep websites from **tracking** them and their family members, or to connect to news sites, instant messaging services, or the like when these are **blocked** by their local Internet providers”.
- Attivazione di **servizi nascosti** anche (e soprattutto) “**geograficamente**”: “Tor's **hidden services** let users **publish web sites** and other services without needing to reveal the location of the site”.

I possibili usi:

- Trattamento di informazioni **delicate** e sensibili che richiedono **anonimato** o che non sarebbero altrimenti diffuse dai protagonisti se non ci fosse una sorta di “**scudo**”: “Individuals also use Tor for socially sensitive communication: chat rooms and web forums for **rape** and **abuse** survivors, or people with illnesses”.

I possibili usi:

- **Giornalisti, comunicazioni sicure e rapporti con fonti anonime o con detentori di informazioni riservate:** “Journalists use Tor to communicate more safely with whistleblowers and dissidents”.
- **NGO e rapporti sicuri con il Paese di origine:** “Non-governmental organizations (NGOs) use Tor to allow their workers to connect to their home website while they're in a foreign country, without notifying everybody nearby that they're working with that organization”.

I possibili usi:

- Online privacy e security: “Groups such as **Indymedia** recommend **Tor** for safeguarding their members' online privacy and security”.
- **Attivismo**: “Activist groups like the Electronic Frontier Foundation (EFF) recommend Tor as a mechanism for maintaining civil liberties online”.

I possibili usi:

- Tutela da **intercettazioni** anche a livello societario: “Corporations use Tor as a safe way to conduct competitive analysis, and to protect sensitive procurement patterns from eavesdroppers”.
- **Surrogato di VPN** anche per non rilasciare specifiche informazioni: “They (**alcune società**) also use it to replace traditional VPNs, which reveal the exact amount and timing of communication. Which locations have employees working late? Which locations have employees consulting job-hunting websites? Which research divisions are communicating with the company's patent lawyers?”.

Possibili usi:

- **OSINT:** “A branch of the U.S. Navy uses Tor for **open source intelligence gathering**, and one of its teams used Tor while deployed in the Middle East recently”.
- **Indagini senza lasciare tracce e azioni sotto copertura:** “Law enforcement uses Tor for visiting or surveilling web sites without leaving government IP addresses in their web logs, and for security during sting operations”.

In (prima) conclusione

- Strumento **versatile** e **multi-purpose**.
- Strumento chiaramente orientato **all'attivismo**, a **nascondere**, a **non lasciare tracce** e ad **aggirare**, quindi non ben visto in molti Paesi e ambiti.
- Strumento **sicuro** anche per la **varietà** dei suoi utilizzatori: “The variety of people who use Tor is actually part of what makes it so secure. Tor hides you among the other users on the network, so the more **populous** and **diverse** the user base for Tor is, the more your anonymity will be protected”.

Un secondo passo tecnico:

- Essenziale è comprendere il “rapporto” tra Tor e un’azione/forma di **sorveglianza** su Internet che si chiama “analisi del traffico”: “Using Tor protects you against a common form of Internet surveillance known as "traffic analysis.”
- Serve a cercare di capire il “**chi**” o anche il “**dove**” o il “**verso chi o cosa**” delle comunicazioni su reti pubbliche: “Traffic analysis can be used to infer who is talking to whom over a public network. Knowing the source and destination of your Internet traffic allows others to track your behavior and interests”.

Perché analizzare il traffico?

- Per comprendere **da quale Paese navighi**, anche a soli fini **commerciali**, per fornirti o meno un **servizio** o per **discriminarti** sul prezzo finale del prodotto.
- Per comprendere, se sei all'estero, dov'è la tua “nave madre” o la società o il Paese verso il quale ti colleghi (“professional affiliation”).

Come funziona l'analisi del traffico:

- Comprendere il concetto di **pacchetti di dati**, di **payload** e di **header (intestazione)**: “Internet data packets have **two parts**: a data **payload** and a **header** used for routing”.
- Il “corpo/contenuto” (**payload**): “The data payload is whatever is being sent, whether that's an email message, a web page, or an audio file”.
- Gli “indizi” dati dagli header: “Even if you **encrypt** the data payload of your communications, traffic analysis still reveals a great deal about what you're doing and, possibly, what you're saying. That's because it focuses on the header, which discloses **source, destination, size, timing**, and so on”.

Cosa si vede...

- Il problema di base in un'ottica di privacy: chi riceve una tua informazione può sapere qualcosa di te “semplicemente” **analizzando** gli header “A basic problem for the privacy minded is that the recipient of your communications can see that you sent it by looking at headers”.
- Anche “**terzi**” possono vedere: “So can authorized intermediaries like Internet service providers, and sometimes unauthorized intermediaries as well.
- Ci si “**siede**” nel mezzo e si osserva, o si applicano tecniche più sofisticate: “A very simple form of traffic analysis might involve sitting somewhere between sender and recipient on the network, looking at headers”.

L'idea di Tor per risolvere:

A distributed, anonymous network

La soluzione:

- **Riduzione dei rischi di sorveglianza e distribuzione del rischio:** “Tor helps to reduce the risks of both simple and sophisticated traffic analysis by **distributing your transactions** over several places on the Internet, so **no single point** can link you to your destination”.

Un percorso “tortuoso”

- Simile all’idea dell’utilizzo di un percorso “tortuoso” e **imprevedibile** per confondere qualcuno che ci stia seguendo a piedi e **cancellazione** delle tracce: “The idea is similar to using a twisty, hard-to-follow route in order to throw off somebody who is tailing you – and then periodically erasing your footprints”.

No a percorsi “diretti”

- Percorsi casuali dei pacchetti che circolano e concetto di relay anche al fine di confondere o ingannare un potenziale osservatore (o ascoltatore...): “Instead of taking a direct route from source to destination, data packets on the Tor network take a random pathway through several relays that cover your tracks so no observer at any single point can tell where the data came from or where it's going”.

Necessità di un client

- Creazione di un percorso privato sulla rete: “To create a private network pathway with Tor, the user's **software** or client incrementally builds a circuit of encrypted connections through relays on the network”.
- Si crea un vero e proprio **circuito** dentro la rete, con precise caratteristiche.
- L'idea di **relay** e di **connessioni cifrate**.

Il circuito

- Concetto di **hop** (“salti” o “punti di passaggio”) e di “**conoscenza**” e riconoscimento tra i vari relay: “The circuit is extended one hop at a time, and each relay along the way knows only which relay gave it data and which relay it is giving data to”.
- “Ignoranza” volontaria dell’intero percorso dei pacchetti: “No individual relay ever knows the **complete path** that a data packet has taken. The client negotiates a **separate set of encryption keys** for each hop along the circuit to ensure that each hop can't trace these connections as they pass through”.

L'ecosistema di Tor

- I tipi di dati e di servizi all'interno dell'ecosistema una volta che il circuito sicuro è stato allestito: Once a circuit has been established, many kinds of data can be exchanged and several different sorts of software applications can be deployed over the Tor network”.

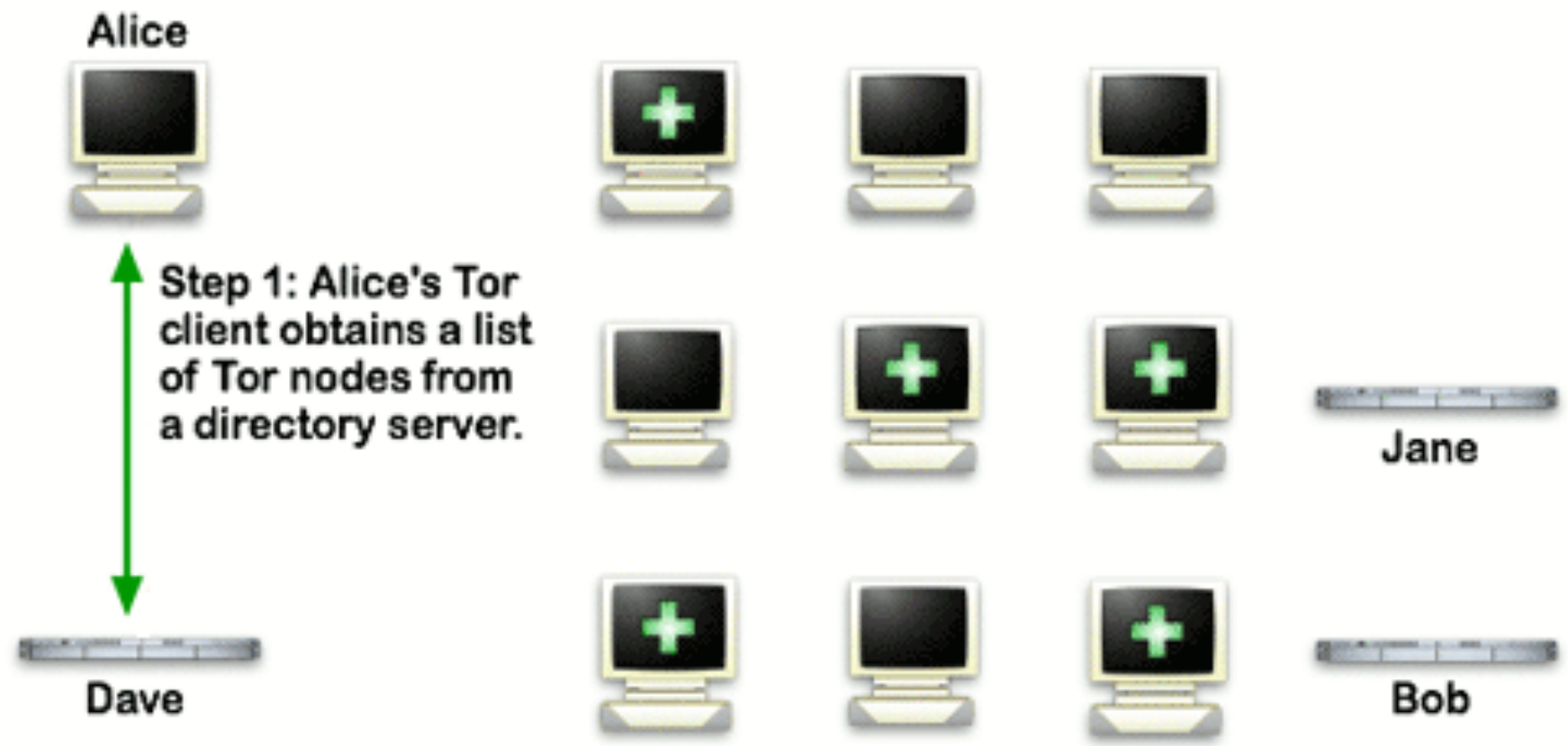
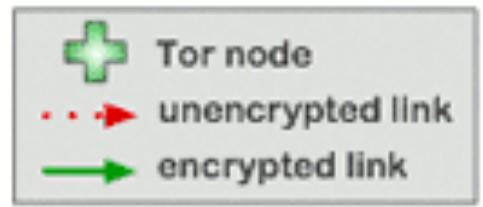
Chi vede chi? (e cosa?)

- Inutilità dell'analisi del traffico per il link dei vari passaggi: “Because each relay sees no more than one hop in the circuit, neither an eavesdropper nor a compromised relay can use traffic analysis to link the connection's source and destination. Tor only works for TCP streams and can be used by any application with SOCKS support”.

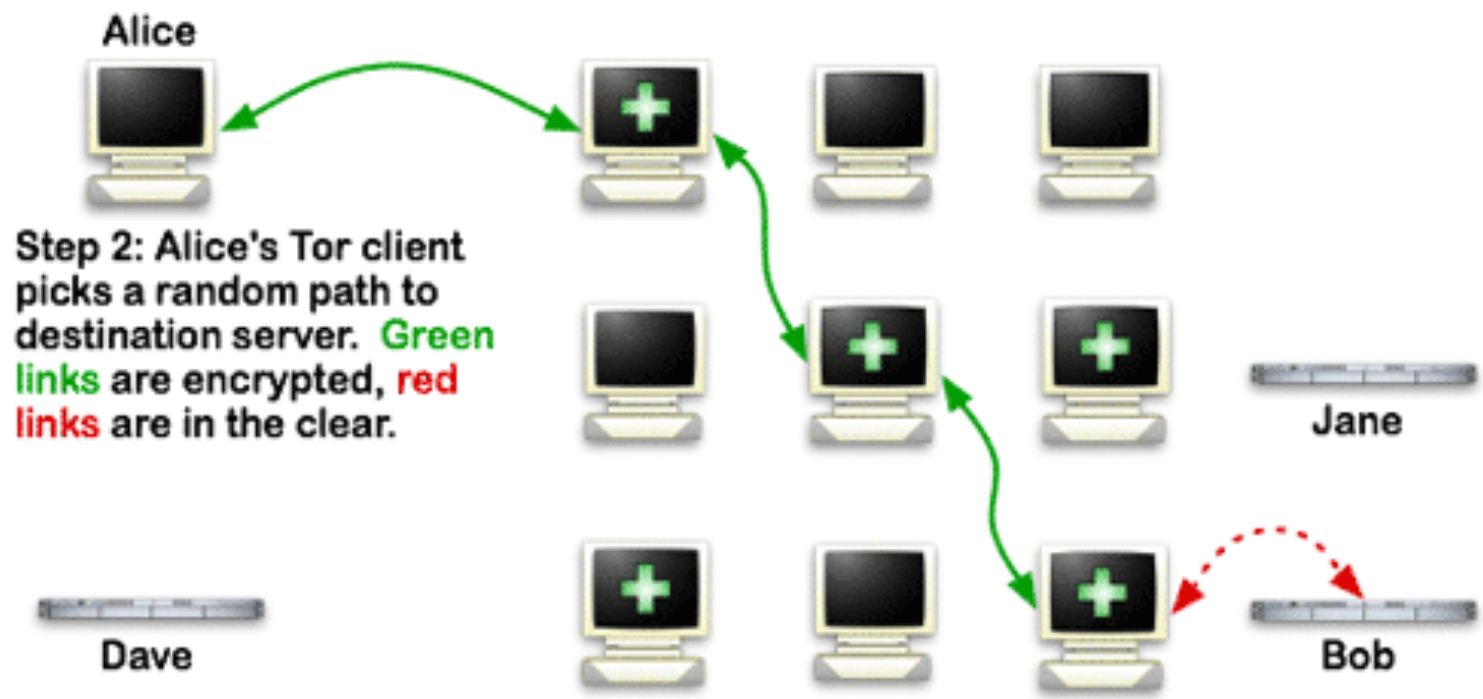
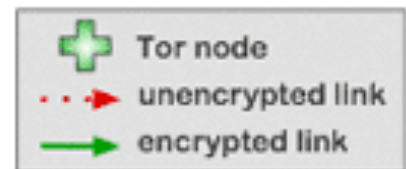
Strategie intelligenti:

Attenzione ai **collegamenti temporali** delle varie attività:
“For efficiency, the Tor software uses the same circuit for connections that happen within the same ten minutes or so. Later requests are given a new circuit, to keep people from linking your earlier actions to the new ones”.

How Tor Works: 1



2 How Tor Works: 2



Il servizio nascosto

- Il concetto di “servizio nascosto”: “Tor also makes it possible for users to **hide** their locations while offering various kinds of services, such as web publishing or an instant messaging server”.
- Non si conosce l’identità altrui: “Using Tor “rendezvous points,” other Tor users can connect to these hidden services, each without knowing the other's network identity”.

A che serve:

- Per siti Web, Blog, e altri tipi di servizi: “This hidden service functionality could allow Tor users to set up a website where people publish material without worrying about censorship. Nobody would be able to determine who was offering the site, and nobody who offered the site would know who was posting to it”.

Non è la panacea...

- Rimanere realmente anonimi è difficile: “Tor can't solve all anonymity problems. It focuses only on protecting the transport of data”.
- Occorre altro: “You need to use protocol-specific support software if you don't want the sites you visit to see your identifying information. For example, you can use web proxies such as Privoxy while web browsing to block cookies and withhold information about your browser type”.

Be smart...

- Occorre sempre essere svegli: “Also, to protect your anonymity, be smart. Don't provide your name or other revealing information in web forms. Be aware that, like all anonymizing networks that are fast enough for web browsing, Tor does not provide protection against end-to-end timing attacks: If your attacker can watch the traffic coming out of your computer, and also the traffic arriving at your chosen destination, he can use statistical analysis to discover that they are part of the same circuit”.

L'idea di “Tor Bundle”

- Una prima “avvertenza” importante: non basta il bundle di software Tor ma occorre anche attenzione alla corretta configurazione e ai propri comportamenti e abitudini in rete.

“Want Tor to really work?...then please don't just install it and go on. You need to change some of your habits, and reconfigure your software! Tor by itself is NOT all you need to maintain your anonymity. Read the full list of warnings”.

Esempio per Windows:

The Tor Software for Windows comes bundled in **four** different ways:

- The **Tor Browser Bundle** contains everything you need to safely browse the Internet. This package requires no installation. Just extract it and run.
- The **Vidalia Bundle** contains Tor, Vidalia, Polipo, and Torbutton for installation on your system. You need your own Firefox, and you'll need to configure other applications if you want them to use Tor.

Esempio per Windows

- The **Bridge-by-Default** Vidalia Bundle is a Vidalia Bundle which is configured to be a bridge in order to help censored users reach the Tor network.
- The **Expert Package** contains just Tor and nothing else. You'll need to configure Tor and all of your applications manually.

Esempio per Apple OSX

The Tor Software for OS X comes bundled in two different ways:

- The Tor Browser Bundle contains everything you need to safely browse the Internet. This package requires no installation. Just extract it and run. [Learn more »](#)
- The Vidalia Bundle contains Tor, Vidalia, Polipo, and Torbutton for installation on your system. You need your own Firefox, and you'll need to configure other applications if you want them to use Tor.

Esempio per GNU/Linux

- Linux/Unix
- The Tor Software comes bundled in two different ways:
- The Tor Browser Bundle contains everything you need to safely browse the Internet. This package requires no installation. Just extract it and run. [Learn more »](#)
- [Read how to use our repositories for the Tor software.](#)

Esempio per smartphone

- Android-based phones, tablets, computers
Android Bundle Android Instructions
- iPhone, iPod Touch, iPad Test packages by Marco
- Nokia Maemo/N900 Experimental
instructions

Le avvertenze perché funzioni bene

- Tor only protects Internet applications that are configured to send their traffic through Tor – it doesn't magically anonymize all your traffic just because you install it. We recommend you use Firefox with the Torbutton extension.

- Torbutton blocks browser plugins such as Java, Flash, ActiveX, RealPlayer, Quicktime, Adobe's PDF plugin, and others: they can be manipulated into revealing your IP address. For example, that means Youtube is disabled. If you really need your Youtube, you can reconfigure Torbutton to allow it; but be aware that you're opening yourself up to potential attack. Also, extensions like Google toolbar look up more information about the websites you type in: they may bypass Tor and/or broadcast sensitive information. Some people prefer using two browsers (one for Tor, one for non-Tor browsing).

- Beware of cookies: if you ever browse without Tor and a site gives you a cookie, that cookie could identify you even when you start using Tor again. Torbutton tries to handle your cookies safely. CookieCuller can help protect any cookies you do not want to lose.

- Tor anonymizes the origin of your traffic, and it encrypts everything between you and the Tor network and everything inside the Tor network, but it can't encrypt your traffic between the Tor network and its final destination. If you are communicating sensitive information, you should use as much care as you would on the normal scary Internet – use HTTPS or other end-to-end encryption and authentication. HTTPS Everywhere is a Firefox extension produced as a collaboration between The Tor Project and the Electronic Frontier Foundation. It encrypts your communications with a number of major websites.

- While Tor blocks attackers on your local network from discovering or influencing your destination, it opens new risks: malicious or misconfigured Tor exit nodes can send you the wrong page, or even send you embedded Java applets disguised as domains you trust. Be careful opening documents or applications you download through Tor, unless you've verified their integrity.

- Tor tries to prevent attackers from learning what destinations you connect to. It doesn't prevent somebody watching your traffic from learning that you're using Tor. You can mitigate (but not fully resolve) the risk by using a Tor bridge relay rather than connecting directly to the public Tor network, but ultimately the best protection here is a social approach: the more Tor users there are near you and the more diverse their interests, the less dangerous it will be that you are one of them.

- Do not use BitTorrent and Tor together unless you are using a system like TAILS.

- Be smart and learn more. Understand what Tor does and does not offer. This list of pitfalls isn't complete, and we need your help identifying and documenting all the issues.

Tor vs. proxies

- How is Tor different from other proxies?
- A typical proxy provider sets up a server somewhere on the Internet and allows you to use it to relay your traffic. This creates a simple, easy to maintain architecture. The users all enter and leave through the same server. The provider may charge for use of the proxy, or fund their costs through advertisements on the server. In the simplest configuration, you don't have to install anything. You just have to point your browser at their proxy server. Simple proxy providers are fine solutions if you do not want protections for your privacy and anonymity online and you trust the provider from doing bad things. Some simple proxy providers use SSL to secure your connection to them. This may protect you against local eavesdroppers, such as those at a cafe with free wifi Internet.

- Simple proxy providers also create a single point of failure. The provider knows who you are and where you browse on the Internet. They can see your traffic as it passes through their server. In some cases, they can even see inside your encrypted traffic as they relay it to your banking site or to ecommerce stores. You have to trust the provider isn't doing any number of things, such as watching your traffic, injecting their own advertisements into your traffic stream, and recording your personal details.

- Tor passes your traffic through at least 3 different servers before sending it on to the destination. Because there's a separate layer of encryption for each of the three relays, Tor does not modify, or even know, what you are sending into it. It merely relays your traffic, completely encrypted through the Tor network and has it pop out somewhere else in the world, completely intact. The Tor client is required because we assume you trust your local computer. The Tor client manages the encryption and the path chosen through the network. The relays located all over the world merely pass encrypted packets between themselves.

Chi vede chi...

- Doesn't the first server see who I am?
- Possibly. A bad first of three servers can see encrypted Tor traffic coming from your computer. It still doesn't know who you are and what you are doing over Tor. It merely sees "This IP address is using Tor". Tor is not illegal anywhere in the world, so using Tor by itself is fine. You are still protected from this node figuring out who you are and where you are going on the Internet.

Chi vede chi...

- Can't the third server see my traffic?
- Possibly. A bad third of three servers can see the traffic you sent into Tor. It won't know who sent this traffic. If you're using encryption, such as visiting a bank or e-commerce website, or encrypted mail connections, etc, it will only know the destination. It won't be able to see the data inside the traffic stream. You are still protected from this node figuring out who you are and if using encryption, what data you're sending to the destination.

Quali programmi?

- There are two pieces to "Torifying" a program: connection-level anonymity and application-level anonymity. Connection-level anonymity focuses on making sure the application's Internet connections get sent through Tor. This step is normally done by configuring the program to use your Tor client as a "socks" proxy, but there are other ways to do it too.

Application level

- For application-level anonymity, you need to make sure that the information the application sends out doesn't hurt your privacy. (Even if the connections are being routed through Tor, you still don't want to include sensitive information like your name.) This second step needs to be done on a program-by-program basis, which is why we don't yet recommend very many programs for safe use with Tor.

Firefox

- “Most of our work so far has focused on the **Firefox** web browser. The bundles on the download page automatically install the Torbutton Firefox extension if you have Firefox installed. As of version 1.2.0, Torbutton now takes care of a lot of the connection-level and application-level worries”.

Il concetto di “torify”

- “There are plenty of other programs you can use with Tor, but we haven't researched the application-level anonymity issues on them well enough to be able to recommend a safe configuration.”
- “Our wiki has a list of instructions for **Torifying** specific applications. There's also a list of applications that help you direct your traffic through Tor”.

Il nome

- Why is it called Tor? Because Tor is **the onion routing network**. When we were starting the new next-generation design and implementation of onion routing in 2001-2002, we would tell people we were working on onion routing, and they would say "Neat. Which one?" Even if onion routing has become a standard household term, Tor was born out of the actual onion routing project run by the **Naval Research Lab**.
- Note: even though it originally came from an acronym, Tor is not spelled "TOR". **Only the first letter is capitalized**. In fact, we can usually spot people who haven't read any of our website (and have instead learned everything they know about Tor from news articles) by the fact that they spell it wrong.

Tor è lento?

Se lo domandano anche i creatori: “Why is Tor so slow?”

“There are **many reasons** why the Tor network is currently slow”.

“Tor is never going to be **blazing fast**. Your traffic is **bouncing** through volunteers' computers in various parts of the world, and some **bottlenecks** and **network latency** will always be present. You shouldn't expect to see university-style bandwidth through Tor.

But that doesn't mean that it can't be **improved**. The current Tor network is quite small compared to the number of people trying to use it, and many of these users don't understand or care that Tor can't currently handle file-sharing traffic load.