



Interferencias

Tor, ¿la herramienta definitiva de anonimato?

Ignacio Aguilera Martos

1. Interferencias
2. ¿Por qué es importante el anonimato?
3. Tor(The onion router)
4. Tor Browser
5. Enlaces de Interés

GNU GENERAL PUBLIC LICENSE

Version 3, 29 June 2007

Copyright (C) 2007 Free Software Foundation, Inc. <http://fsf.org/>

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.

www.github.com/nacheteam/Charla-sobre-Tor

Interferencias

Interferencias

Interferencias es un grupo sin ánimo de lucro que pretende reunir a una serie de personas interesadas en:

- Privacidad
- Vigilancia masiva
- Derechos en internet
- Seguridad

Twitter: @Inter_ferencias

E-mail: interferencias@protonmail.com
interferencias.github.io

¿Por qué es importante el anonimato?

- Debemos ser dueños de nuestra información.

- Debemos ser dueños de nuestra información.
- No somos manipulados en función de nuestros datos si permanecemos anónimos.

- Debemos ser dueños de nuestra información.
- No somos manipulados en función de nuestros datos si permanecemos anónimos.

Privacidad en Internet

- Debemos ser dueños de nuestra información.
- No somos manipulados en función de nuestros datos si permanecemos anónimos.

Privacidad en Internet

La privacidad en Internet se refiere al derecho de la privacidad personal en relación con el almacenamiento, la reutilización, la provisión a terceros y la exhibición de información relativa a uno mismo a través de Internet.

- Debemos ser dueños de nuestra información.
- No somos manipulados en función de nuestros datos si permanecemos anónimos.

Privacidad en Internet

La privacidad en Internet se refiere al derecho de la privacidad personal en relación con el almacenamiento, la reutilización, la provisión a terceros y la exhibición de información relativa a uno mismo a través de Internet.

Charla de Introducción a la privacidad

[https : // bitbucket.org / josealberto4444 / charla_introduccion_privacidad](https://bitbucket.org/josealberto4444/charla_introduccion_privacidad)

Tor(The onion router)

- Comunicaciones anónimas.

- Comunicaciones anónimas.
- **NO** se pretende respaldar a delincuentes.

Propósito de Tor

- Comunicaciones anónimas.
- **NO** se pretende respaldar a delincuentes.
- Es una red compleja de analizar.

Las entidades básicas de Tor son:

Las entidades básicas de Tor son:

- Nodos.

Las entidades básicas de Tor son:

- Nodos.
- Usuarios.

Las entidades básicas de Tor son:

- Nodos.
- Usuarios.
- Autoridades de Directorio.

Las entidades básicas de Tor son:

- Nodos.
- Usuarios.
- Autoridades de Directorio.

Proxys y Tor

La relación entre nodos es similar a los proxys pero no es la misma.

Nodos y sus tipos

Los nodos son las piezas fundamentales de Tor.

Nodos y sus tipos

Los nodos son las piezas fundamentales de Tor.

Tipos:

Nodos y sus tipos

Los nodos son las piezas fundamentales de Tor.

Tipos:

Nodos Guard o Nodos de entrada

Son los nodos que ocupan el primer lugar en los circuitos. Son críticos ya que conocen la identidad del usuario.

Nodos y sus tipos

Los nodos son las piezas fundamentales de Tor.

Tipos:

Nodos Guard o Nodos de entrada

Son los nodos que ocupan el primer lugar en los circuitos. Son críticos ya que conocen la identidad del usuario.

Middle Nodes o Relay

Son los nodos intermedios dentro de los circuitos. Son los más básicos.

Nodos y sus tipos

Los nodos son las piezas fundamentales de Tor.

Tipos:

Nodos Guard o Nodos de entrada

Son los nodos que ocupan el primer lugar en los circuitos. Son críticos ya que conocen la identidad del usuario.

Middle Nodes o Relay

Son los nodos intermedios dentro de los circuitos. Son los más básicos.

Exit Nodes o Nodos de salida

Son los nodos que ocupan el último lugar de los circuitos. Estos nodos tienen la información sin encriptar para enviarla al servidor de destino.

Circuito

Es un camino de nodos dentro del grafo de la red Tor. Incluye un nodo de entrada, varios nodos intermedios y un nodo de salida.

Circuito

Es un camino de nodos dentro del grafo de la red Tor. Incluye un nodo de entrada, varios nodos intermedios y un nodo de salida.

Los circuitos tienen una caducidad (modificable por el usuario) por motivos de seguridad.

Flags de calificación de nodos

- BadExit.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.
- HSDir: Hidden Service Directory.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.
- HSDir: Hidden Service Directory.
- Named o Unnamed.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.
- HSDir: Hidden Service Directory.
- Named o Unnamed.
- Running: 45 minutos en ejecución.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.
- HSDir: Hidden Service Directory.
- Named o Unnamed.
- Running: 45 minutos en ejecución.
- Stable: 7 días en ejecución.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.
- HSDir: Hidden Service Directory.
- Named o Unnamed.
- Running: 45 minutos en ejecución.
- Stable: 7 días en ejecución.
- Valid: lista negra y versión de Tor sin alterar.

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.
- HSDir: Hidden Service Directory.
- Named o Unnamed.
- Running: 45 minutos en ejecución.
- Stable: 7 días en ejecución.
- Valid: lista negra y versión de Tor sin alterar.
- V2Dir

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.
- HSDir: Hidden Service Directory.
- Named o Unnamed.
- Running: 45 minutos en ejecución.
- Stable: 7 días en ejecución.
- Valid: lista negra y versión de Tor sin alterar.
- V2Dir

Flags de calificación de nodos

- BadExit.
- Fast : 100KB/s.
- Guard: 250KB/s.
- Authority.
- Exit.
- HSDir: Hidden Service Directory.
- Named o Unnamed.
- Running: 45 minutos en ejecución.
- Stable: 7 días en ejecución.
- Valid: lista negra y versión de Tor sin alterar.
- V2Dir

Gracias a estos flags los nodos quedan valorados para saber su posición en los circuitos y su validez como nodo en general.

Ocurre en 4 fases:

Ocurre en 4 fases:

- Fase 1(0-3): Comprobaciones básicas. Tests de seguridad y velocidad.

Ocurre en 4 fases:

- Fase 1(0-3): Comprobaciones básicas. Tests de seguridad y velocidad.
- Fase 2(3-8): Nodo intermedio. Comprobaciones sobre Guard y Exit.

Ocurre en 4 fases:

- Fase 1(0-3): Comprobaciones básicas. Tests de seguridad y velocidad.
- Fase 2(3-8): Nodo intermedio. Comprobaciones sobre Guard y Exit.
- Fase 3(8-68): Nodo Guard. Comprobaciones de estabilidad y Exit.

Ocurre en 4 fases:

- Fase 1(0-3): Comprobaciones básicas. Tests de seguridad y velocidad.
- Fase 2(3-8): Nodo intermedio. Comprobaciones sobre Guard y Exit.
- Fase 3(8-68): Nodo Guard. Comprobaciones de estabilidad y Exit.
- Fase 4(68-...): Nodo Exit. Comprobaciones esporádicas generales.

Ocurre en 4 fases:

- Fase 1(0-3): Comprobaciones básicas. Tests de seguridad y velocidad.
- Fase 2(3-8): Nodo intermedio. Comprobaciones sobre Guard y Exit.
- Fase 3(8-68): Nodo Guard. Comprobaciones de estabilidad y Exit.
- Fase 4(68-...): Nodo Exit. Comprobaciones esporádicas generales.

Los integrantes de esta comunicación son:

Los integrantes de esta comunicación son:

- Usuario.

Los integrantes de esta comunicación son:

- Usuario.
- Servicio Oculto.

Los integrantes de esta comunicación son:

- Usuario.
- Servicio Oculto.
- Puntos Introdutorios.

Los integrantes de esta comunicación son:

- Usuario.
- Servicio Oculto.
- Puntos Introdutorios.
- Nodo Rendezvous.

Los integrantes de esta comunicación son:

- Usuario.
- Servicio Oculto.
- Puntos Introdutorios.
- Nodo Rendezvous.

Los integrantes de esta comunicación son:

- Usuario.
- Servicio Oculto.
- Puntos Introdutorios.
- Nodo Rendezvous.

Diagrama de Comunicación

Usuario ⇔ Guard ⇔ Relay ⇔ Rendezvous ⇔ Relay ⇔ Guard ⇔ Servicio oculto

Servicios Ocultos

Los integrantes de esta comunicación son:

- Usuario.
- Servicio Oculto.
- Puntos Introdutorios.
- Nodo Rendezvous.

Diagrama de Comunicación

Usuario ⇔ Guard ⇔ Relay ⇔ Rendezvous ⇔ Relay ⇔ Guard ⇔ Servicio oculto

Direcciones Onion

Los servicios ocultos tienen URLs con el dominio onion y contienen 16 caracteres.

Por ejemplo: ab2dafgh6jklmi3t.onion ó facebookcorewwi.onion. Deben ser caracteres entre la 'a' y la 'z' y números entre el '2' y el '7'.

- Server Descriptor: IP, ORPort, ...

- Server Descriptor: IP, ORPort, ...
- ExtraInfo Descriptor: Información completa del nodo.

- Server Descriptor: IP, ORPort, ...
- ExtraInfo Descriptor: Información completa del nodo.
- Micro Descriptor: Información reducida del nodo.

- Server Descriptor: IP, ORPort, ...
- ExtraInfo Descriptor: Información completa del nodo.
- Micro Descriptor: Información reducida del nodo.
- Network Status Document: fichero de consenso.

- Server Descriptor: IP, ORPort, ...
- ExtraInfo Descriptor: Información completa del nodo.
- Micro Descriptor: Información reducida del nodo.
- Network Status Document: fichero de consenso.
- Router Status Entry: Información completa de nodos incluyendo flags y cálculos heurísticos.

- Server Descriptor: IP, ORPort, ...
- ExtraInfo Descriptor: Información completa del nodo.
- Micro Descriptor: Información reducida del nodo.
- Network Status Document: fichero de consenso.
- Router Status Entry: Información completa de nodos incluyendo flags y cálculos heurísticos.
- Hidden Service Descriptor: Información del servicio oculto.

- Server Descriptor: IP, ORPort, ...
- ExtraInfo Descriptor: Información completa del nodo.
- Micro Descriptor: Información reducida del nodo.
- Network Status Document: fichero de consenso.
- Router Status Entry: Información completa de nodos incluyendo flags y cálculos heurísticos.
- Hidden Service Descriptor: Información del servicio oculto.

Puente

Nodos ocultos usados para impedir las prohibiciones de uso de Tor por gobiernos o cualquier otra entidad.

Autoridad de Directorio

Nodo con permisos totales en la red. Son los únicos nodos de confianza. Tienen como misión controlar los nodos, valorarlos y administrar la red en general.

- Correlación punto a punto.

- Correlación punto a punto.
- Pérdida de información del nodo de salida.

- Correlación punto a punto.
- Pérdida de información del nodo de salida.
- Bloqueo de los nodos de salida.

- Correlación punto a punto.
- Pérdida de información del nodo de salida.
- Bloqueo de los nodos de salida.
- Ataque DDOS a Tor.

- Correlación punto a punto.
- Pérdida de información del nodo de salida.
- Bloqueo de los nodos de salida.
- Ataque DDOS a Tor.
- HeartBleed.

- Correlación punto a punto.
- Pérdida de información del nodo de salida.
- Bloqueo de los nodos de salida.
- Ataque DDOS a Tor.
- HeartBleed.
- DNS Leak.

- Correlación punto a punto.
- Pérdida de información del nodo de salida.
- Bloqueo de los nodos de salida.
- Ataque DDOS a Tor.
- HeartBleed.
- DNS Leak.
- Clogging(Saturación de nodos).

- Correlación punto a punto.
- Pérdida de información del nodo de salida.
- Bloqueo de los nodos de salida.
- Ataque DDOS a Tor.
- HeartBleed.
- DNS Leak.
- Clogging(Saturación de nodos).
- Round Trip Travel Time.

- Correlación punto a punto.
- Pérdida de información del nodo de salida.
- Bloqueo de los nodos de salida.
- Ataque DDOS a Tor.
- HeartBleed.
- DNS Leak.
- Clogging(Saturación de nodos).
- Round Trip Travel Time.

Tor Browser

¿Cómo obtener el Tor Browser?

¿Cómo obtener el Tor Browser?

Tor Project

www.torproject.org



[Home](#) [About Tor](#) [Documentation](#) [Press](#) [Blog](#) [Contact](#)

[Download](#) [Volunteer](#) [Donate](#)

Anonymity Online

Protect your privacy. Defend yourself against network surveillance and traffic analysis.



- Tor prevents people from learning your location or browsing habits.
- Tor is for web browsers, instant messaging, clients, and more.
- Tor is free and open source for Windows, Mac, Linux/Unix, and Android.

What is Tor?

Tor is free software and an open network that helps you defend against traffic analysis, a form of network surveillance that threatens personal freedom and privacy, confidential business activities and relationships, and state security.

[Learn more about Tor »](#)

Why Anonymity Matters

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.

[Get involved with Tor »](#)

Our Projects

**Tor Browser**

Tor Browser contains everything you need to safely browse the internet.

**Orbot**

Tor for Google Android devices.

**Tails**

Live CD/USB operating system preconfigured to use Tor safely.

**Arm**

Terminal (command line) applications for monitoring and configuring Tor.

**Atlas**

Site providing an overview of the Tor network.

**Pluggable Transports**

Pluggable transports help you circumvent censorship.

**Stem**

2 libraries for python scripts and

**OONI**

Cloud-based network monitoring for

Recent Blog Posts

Tor 0.3.3.8-alpha is released
Fri, 03 Feb 2017
[Tor browser in numbers](#)
Thu, 02 Feb 2017
Tor at the Heart Security in a Box
Tue, 31 Jan 2017
Tor Browser 7.0.0.10 is released
Wed, 25 Jan 2017
Tor Browser 7.0.0.10 is released
Wed, 25 Jan 2017

[View all blog posts »](#)

Who Uses Tor?

**Family & Friends**

People like you and your family use Tor to protect themselves, their children, and their dignity while using the Internet.

**Businesses**

Businesses use Tor to research competition, keep business strategies confidential, and facilitate internal accountability.

**Activists**

Activists use Tor to anonymously report abuses from danger zones. Whistleblowers use Tor to safely report on companies.

**Media**

Journalists and the media use Tor to protect their research and sources online.

**Military & Law Enforcement**

Military and law enforcement use Tor to protect their communications, investigations, and intelligence gathering online.

17

- Utilizar el Tor Browser para navegar por Internet.

- Utilizar el Tor Browser para navegar por Internet.
- Utilizar Tails.

- Utilizar el Tor Browser para navegar por Internet.
- Utilizar Tails.
- Navegar por webs https siempre que sea posible.

- Utilizar el Tor Browser para navegar por Internet.
- Utilizar Tails.
- Navegar por webs https siempre que sea posible.
- No introducir credenciales salvo en webs https.

- Utilizar el Tor Browser para navegar por Internet.
- Utilizar Tails.
- Navegar por webs https siempre que sea posible.
- No introducir credenciales salvo en webs https.
- No montar un nodo de salida si no sabes cómo hacerlo bien.

- Utilizar el Tor Browser para navegar por Internet.
- Utilizar Tails.
- Navegar por webs https siempre que sea posible.
- No introducir credenciales salvo en webs https.
- No montar un nodo de salida si no sabes cómo hacerlo bien.

Facebook no es tu amigo

Aunque Facebook tenga su web en Tor (facebookcorewwwi.onion) no lo hagáis...

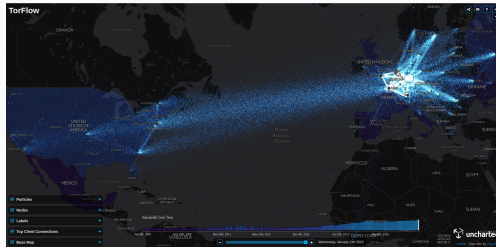
Enlaces de Interés

Tor flow

Tor flow es una web que muestra información del tráfico de la red Tor sobre un mapa del mundo interactivo.

Tor flow

Tor flow es una web que muestra información del tráfico de la red Tor sobre un mapa del mundo interactivo.



Tor Metrics

Tor metrics es una web que nos da información estadística acerca de la red tor.

Tor Metrics

Tor metrics es una web que nos da información estadística acerca de la red tor.

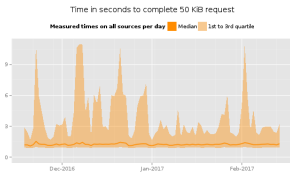
Performance

We use **Torperf** to run performance measurements. It works by fetching files of different sizes over Tor and measuring how long that takes.

Time to download files over Tor

Timeouts and failures of downloading files over Tor

Fraction of connections used uni-/bidirectionally



The Tor Project - <https://metrics.torproject.org/>

This graph shows overall performance when downloading static files of different sizes over Tor. The graph shows the range of measurements from first to third quartile, and highlights the median. The slowest and fastest quarter of measurements are omitted from the graph.

Start date: 2016-11-18

End date: 2017-02-16

Source: ☒ all ☐ torperf ☐ moria ☐ silv

File size: ☒ 50 KiB ☐ 1 MiB ☐ 5 MiB

Update graph

Download graph as PDF or SVG.

Download underlying data:

- CSV (format)

¿Preguntas?

