

Tor, ¿la herramienta definitiva de anonimato?

Anonimato en la red

Ignacio Aguilera Martos

1. Interferencias
2. ¿Por qué es importante el anonimato?
3. Tor(The onion router)

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

Y derivados, con la idea de compartir experiencias, hacer mesas redondas y participar activamente en la defensa de los derechos en internet y la privacidad.

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

Y derivados, con la idea de compartir experiencias, hacer mesas redondas y participar activamente en la defensa de los derechos en internet y la privacidad.

Página web

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.

Ciclo de vida de un nodo

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

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: ab2dafgh1jklmi3t.onion ó facebookcorewwi.onion.

- 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.