Fundamentos de Redes

Redes anónimas: I2P

Alberto Jesús Durán López
Antonio Coín Castro

Grupo 5

27 de noviembre de 2017

Anonimato en el acceso corriente a internet

Hableremos sobre distintas formas de obtener anonimato:

- Proxy, VPN...
- I2P, Invisible Internet Project

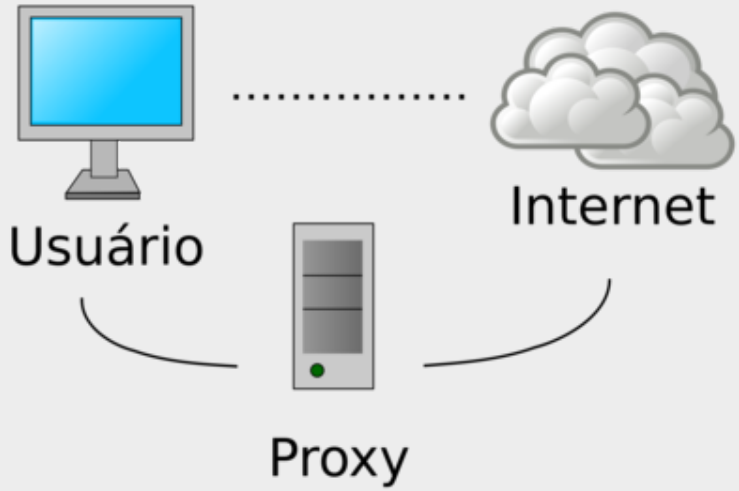
Podemos poner una diapos. con una foto introductoria para el simil de cuando nos conectamos a la red - plaza , if u want it would be great

Métodos para mantener el anonimato

- Proxy
- VPN - Virtual Private Network
- Otros

Proxy

Servidor intermediario entre las conexiones de un cliente y un servidor.



- Dirección IP camuflada
- Acceso a contenido bloqueados de algunos países

VPN

VPN

Medio de extender una red privada a través de una red pública

- Se puede acceder a una red privada remotamente
- Dirección IP camuflada
- Confidencialidad garantizada - Paquetes encriptados
- Sistema de autentificación para conectarse
- Mecanismos para mantener integridad de mensajes

Otros...

- Tails
- DuckDuckGo

I2P, Invisible Internet Project

Se puede poner diapositiva introductoria a I2P con foto

I2P, Invisible Internet Project

- Nodos y túneles
- Enrutamiento tipo garlic
- Encriptación de la información

I2P, Invisible Internet Project

Nodos y túneles for you and kademlia too

Enrutamiento tipo garlic

- Cifrado por capas
- Agregación de múltiples mensajes juntos
- Cifrado ElGamal/AES

Enrutamiento tipo garlic

Cifrado por capas:

- Comunicación de dos usuarios mediante túneles
- La información viaja desde el primer nodo del túnel hasta el último
- El 'gateway' fragmenta mensajes I2P en mensajes de túnel
- En cada salto se envía: {ID del túnel, IV, mensaje del túnel}

Enrutamiento tipo garlic

Agregación de múltiples mensajes juntos juntos para aumentar velocidad de transferencia de datos y aumentar seguridad

Enrutamiento tipo garlic

Mensajes cifrados usando ElGamal/AES

Encriptación de la información

- ElGamal
- AES: Cifrado simétrico por bloques de 128 bits
- Procedimiento aplicado a los mensajes:
  - Se cifra el IV recibido con AES
  - Usa el IV obtenido para cifrar los datos
  - Cifra de nuevo el IV usando AES
  - Envía {ID del túnel, IV, mensaje del túnel} al siguiente nodo

Software I2P

- Susimail: Interfaz web para emails
- Syndie: blogs, noticias y foros para I2P
- I2P Messenger: Cliente de mensajería instantánea
- Navegación web mediante webs anónimas
- Compartición de archivos mediante el uso de BitTorrent dentro de la red I2P
- (Android) Nightweb, aplicación que usa I2P y BitTorrent para compartir entradas de blogs, fotos y otros contenidos similares