Fundamentos de Redes

Redes anónimas: I2P

Alberto Jesús Durán López
Antonio Coín Castro

Grupo 5

27 de noviembre de 2017

Privacidad en la red

"[Privacy] can be defined as an individual's claim to control the terms under which personal information – information identifiable to the individual – is acquired, disclosed, and used."

Anonimato en el acceso corriente a Internet

- Identificación de forma unívoca por la **dirección IP**
- Geolocalización
- Rastreo de datos personales (*tracking*)
- Cookies
- Anuncios dirigidos

Métodos para mantener el anonimato

- Proxy
- VPN
- Redes anónimas
- Otros

Proxy

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

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

VPN

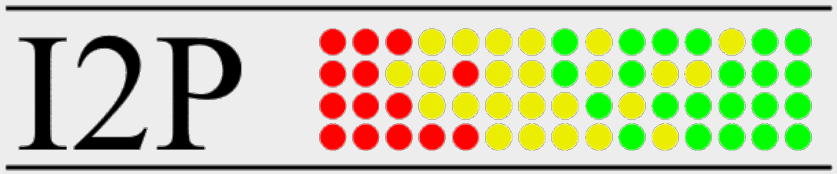
Acrónimo de *Virtual Private Network*. Es un medio de extender una red privada a través de una red pública.

- Acceso remoto a una red privada (UGR)
- Dirección IP camuflada
- Confidencialidad garantizada: paquetes encriptados
- Sistema de autentificación para conectarse
- Mecanismos para mantener integridad de mensajes

Otros...

- Buscadores que no te rastrean (e.g. DuckDuckGo)
- Sistemas operativos específicos (e.g. TAILS)
- HTTPS

Redes anónimas
Invisible Internet Project



I2P es una herramienta de **software libre** que ofrece una capa de red de abstracción distribuida para comunicaciones entre ordenadores, la cual permite a las aplicaciones que la utilizan transmitir mensajes de forma anónima y segura.

Invisible Internet Project

Estructura

Se trata de una red superpuesta (*overlay network*) basada en el intercambio de paquetes.

- Los paquetes están dirigidos a direcciones criptográficas.
- Emisor y receptor no pueden identificarse mutuamente.
- Comunicaciones ocultas a terceros (encriptadas)
- Funcionamiento P2P

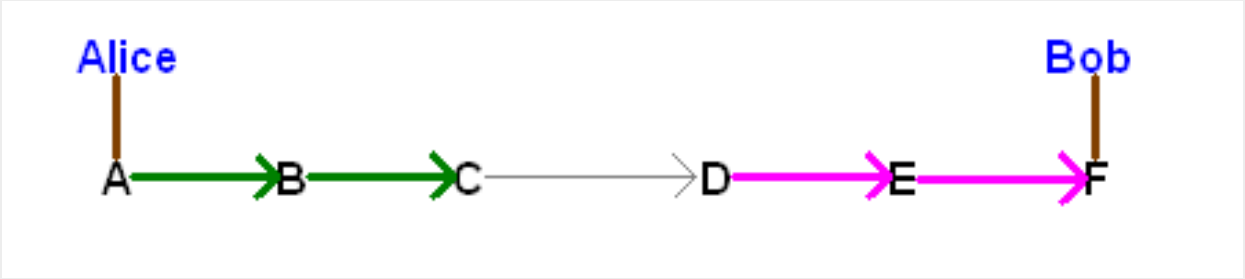
Invisible Internet Project

Estructura

- Un **nodo** es un ordenador conectado a I2P.
- Un **túnel** es una secuencia de nodos que forman camino temporal, unidireccional y seguro por el que viajan los mensajes.

Invisible Internet Project
Funcionamiento

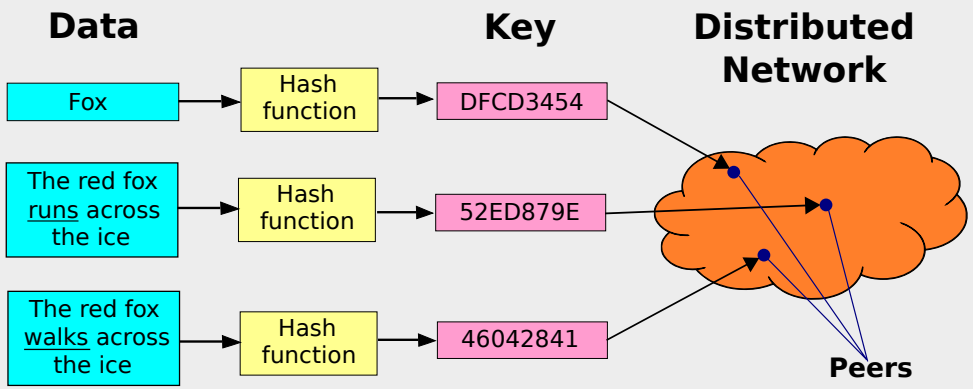
Cada cliente construye una serie de túneles de entrada (*inbound*) y de salida (*outbound*).



Se elige la longitud del túnel para encontrar un equilibrio entre el anonimato, la latencia y el *throughput*.

Invisible Internet Project
netDB

La base de datos en red está completamente distribuida. En cada instante, hay un subconjunto de nodos especiales (*floodfill nodes*) encargados de mantenerla.



Cuando se envía un mensaje, se buscan en la tabla los túneles de entrada del nodo destino (*LeaseSet*).

Invisible Internet Project

Algoritmo Kademlia

Los accesos y consultas a la base de datos se realizan al nodo *floodfill* más cercano. La medida de cercanía se computa utilizando la métrica XOR sobre el ID de los nodos.

- $A \oplus B \geq 0$, y $A \oplus B = 0 \iff A = B$
- $A \oplus B = B \oplus A$.
- $A \oplus B \leq (A \oplus C) + (C \oplus B)$

I2P, Invisible Internet Project

Enrutamiento tipo garlic:

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

I2P, Invisible Internet Project

gonna study topología, see ya I2P!