

Modelización del protocolo Tor y extracción de características de servicios ocultos

Jorge García de Quirós

Ricardo J. Rodríguez



Universidad
Zaragoza

Universidad de Zaragoza, Spain

28 de mayo de 2019

Agenda

- 1 **Introducción**
- 2 Modelización
- 3 Extracción de características
- 4 Análisis de los servicios ocultos
- 5 Conclusiones y trabajo futuro

Introducción

¿Qué es Tor?



- **Servicio para mejorar el anonimato y la privacidad en Internet**
- **Tor: The Onion Router**
 - Aplicación Tor
 - La red Tor, formada por dispositivos de voluntarios
 - Organización Tor Project

Introducción

¿Cómo funciona?

- **Comunicación anónima de baja latencia basada en circuitos**

- **Circuitos virtuales:** garantizan que no hay conexión directa entre cliente y servidor.
- **Salto intermedios:** cada salto es un nodo. Cada router sólo conoce al siguiente y al anterior
- **Tráfico cifrado por capas** → encaminamiento cebolla

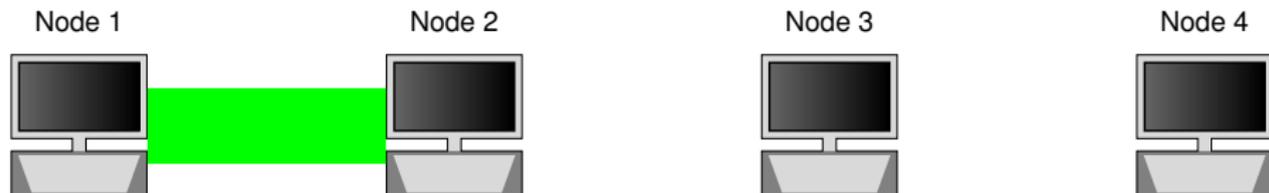


Introducción

¿Cómo funciona?

- **Comunicación anónima de baja latencia basada en circuitos**

- **Circuitos virtuales:** garantizan que no hay conexión directa entre cliente y servidor.
- **Salto intermedios:** cada salto es un nodo. Cada router sólo conoce al siguiente y al anterior
- **Tráfico cifrado por capas** → encaminamiento cebolla



Introducción

¿Cómo funciona?

- **Comunicación anónima de baja latencia basada en circuitos**

- **Circuitos virtuales:** garantizan que no hay conexión directa entre cliente y servidor.
- **Salto intermedios:** cada salto es un nodo. Cada router sólo conoce al siguiente y al anterior
- **Tráfico cifrado por capas** → encaminamiento cebolla



Introducción

¿Cómo funciona?

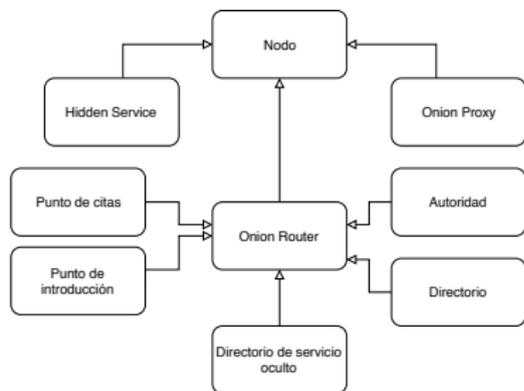
- **Comunicación anónima de baja latencia basada en circuitos**

- **Circuitos virtuales:** garantizan que no hay conexión directa entre cliente y servidor.
- **Salto intermedios:** cada salto es un nodo. Cada router sólo conoce al siguiente y al anterior
- **Tráfico cifrado por capas** → encaminamiento cebolla



Introducción

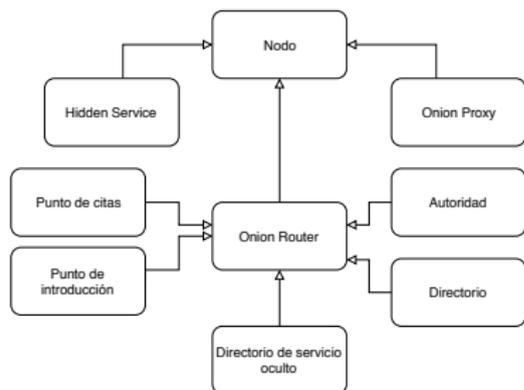
Tipos de nodos



- **Onion Proxy (OP): cliente Tor**
- **Onion Router (OR)**
 - **Elemento básico de la red Tor**
 - Mantenidos por voluntarios, establecen los circuitos para conectarse
- **Hidden Service (HS)**
 - **Proveen servicios únicamente accesibles a través de Tor**

Introducción

Tipos de nodos



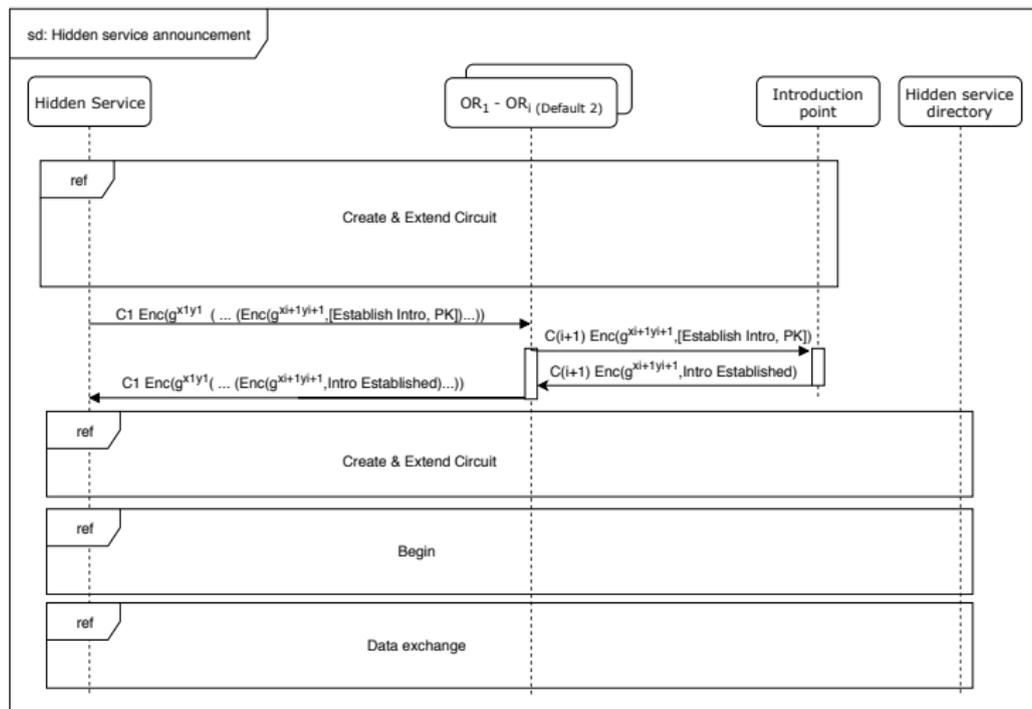
- **Directorio (Dir)**: Suministra información del estado de red
- **Autoridad (Auth)**: Genera el estado consensuado de la red
- **Directorio de servicio oculto (HsDir)**: Almacena descriptores de HS
- **Punto de Introducción (IP) y Citas (RV)**
- **Puente**
- **Puente autoridad**

Agenda

- 1 Introducción
- 2 Modelización**
- 3 Extracción de características
- 4 Análisis de los servicios ocultos
- 5 Conclusiones y trabajo futuro

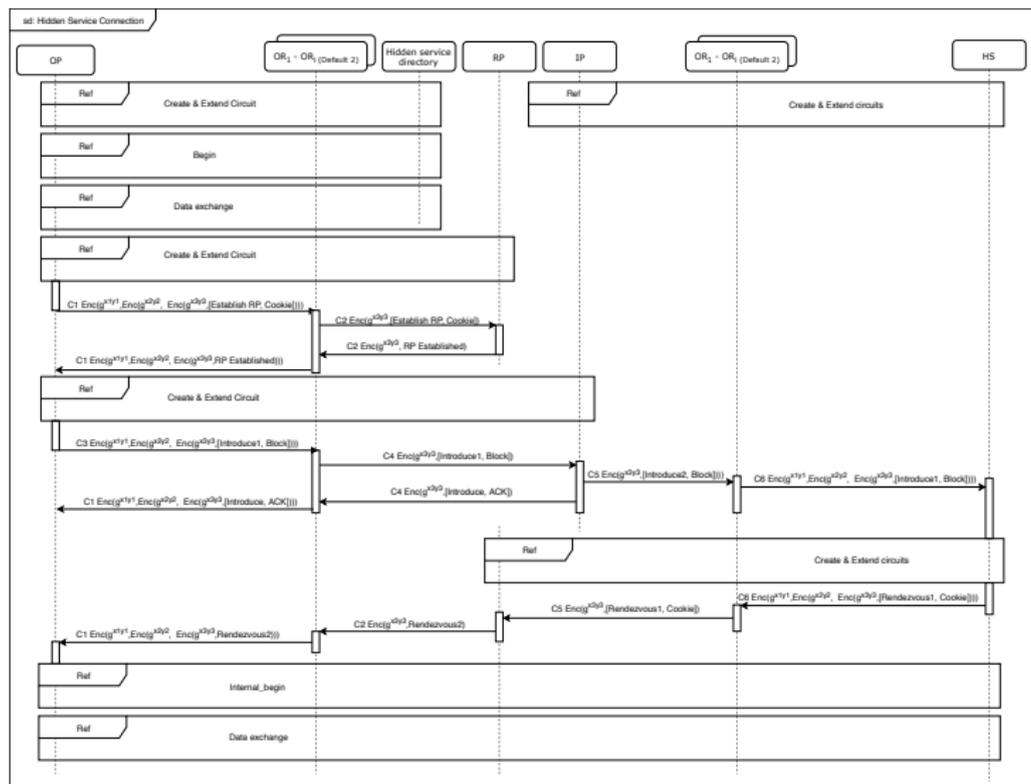
Diagramas de secuencia

Conexión a servicios ocultos – anuncio del HS

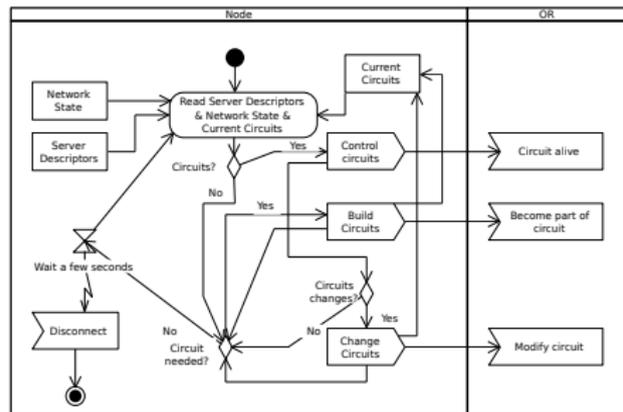
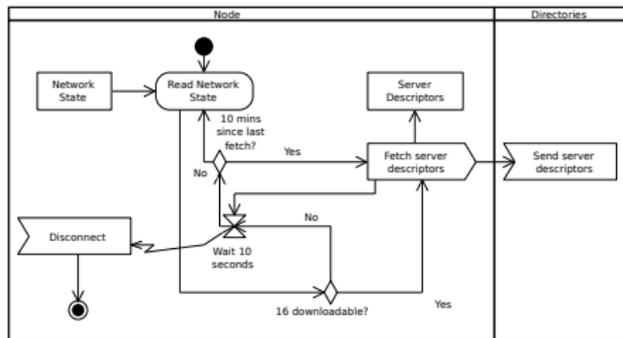
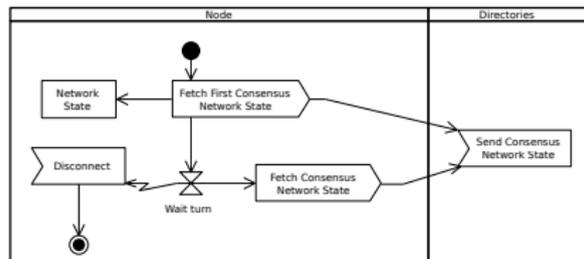
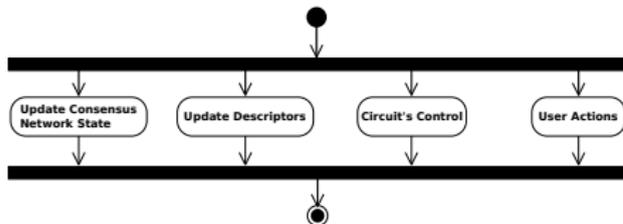


Diagramas de secuencia

Conexión a servicios Circuit – conexión al HS



Diagramas de actividad



Agenda

- 1 Introducción
- 2 Modelización
- 3 Extracción de características**
- 4 Análisis de los servicios ocultos
- 5 Conclusiones y trabajo futuro

Usos de Tor

- **Usos legítimos: defensa de derechos y libertades del individuo**
 - Acceso a contenidos prohibidos en el país de origen del usuario
 - Denuncia anónima de violaciones de derechos por parte de empresas o estados

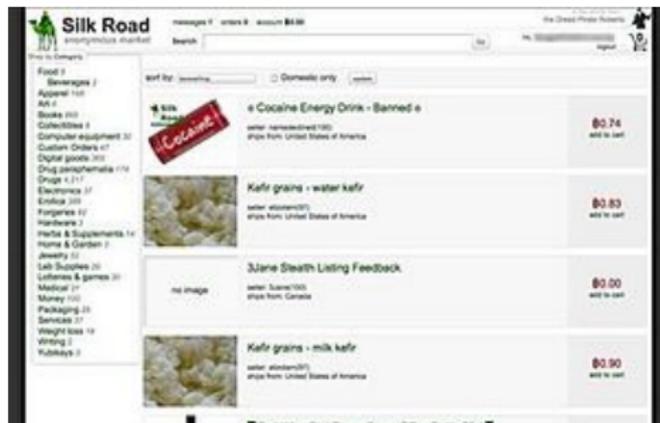
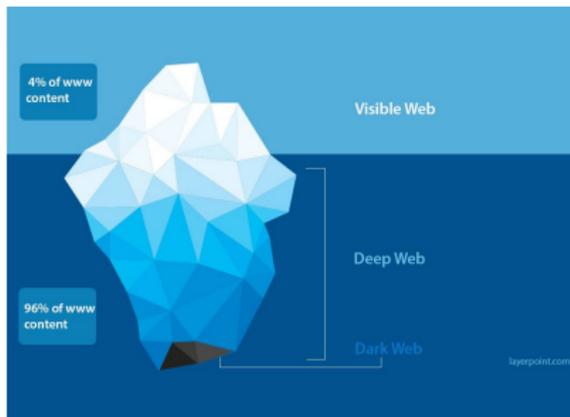
Usos de Tor

● Usos legítimos: defensa de derechos y libertades del individuo

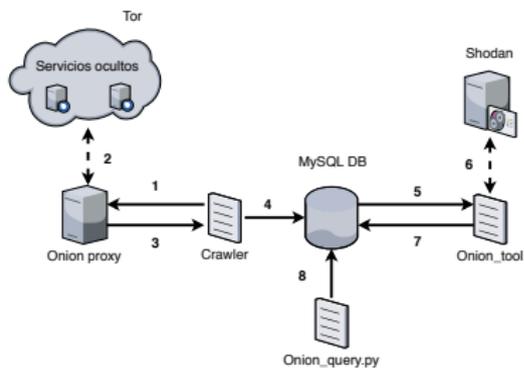
- Acceso a contenidos prohibidos en el país de origen del usuario
- Denuncia anónima de violaciones de derechos por parte de empresas o estados

● Usos ilegítimos: aprovechamiento por parte de delincuentes

- Servicios ocultos: *dark web*
- Caso más famoso: *Silk Road* (mercado online para compra de drogas). Creado en 2011, clausurado en 2013 por el FBI



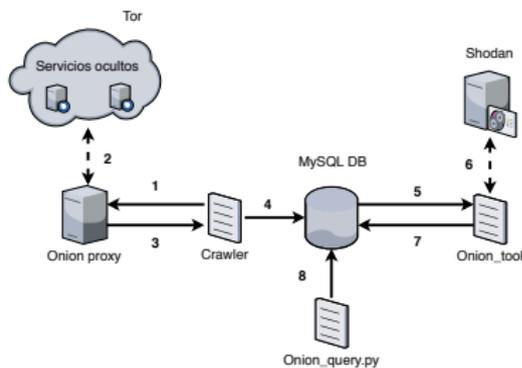
Descripción de TorHSScanner



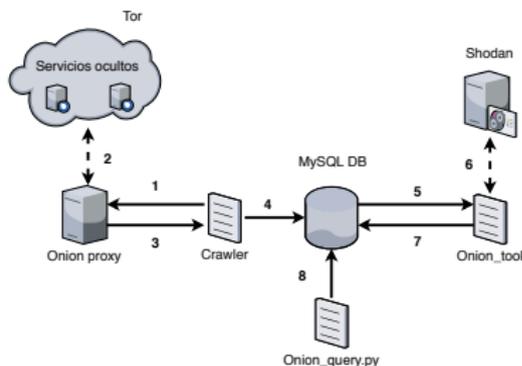
Descripción de TorHSScanner

1 Recopilación de direcciones .onion

- HTTP + HTTPS requests
- HTML del index y HTTP headers



Descripción de TorHSScanner



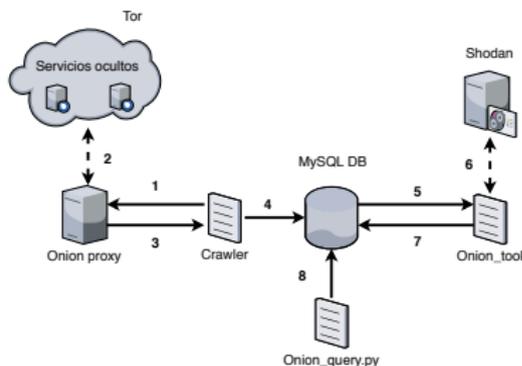
1 Recopilación de direcciones .onion

- HTTP + HTTPS requests
- HTML del index y HTTP headers

2 Desanonimización

- Metadatos de Internet (**Shodan**)
- Algoritmo voraz para encontrar similitudes

Descripción de TorHSScanner



1 Recopilación de direcciones .onion

- HTTP + HTTPS requests
- HTML del index y HTTP headers

2 Desanonimización

- Metadatos de Internet (**Shodan**)
- Algoritmo voraz para encontrar similitudes

3 Categorización

- **Categorías:** drogas, contenido-sexual, terrorismo y criptomonedas
- **Diccionarios**

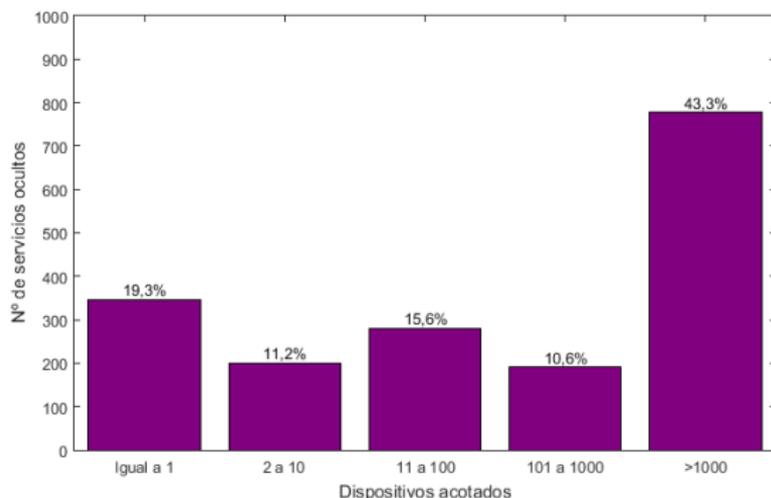
Agenda

- 1 Introducción
- 2 Modelización
- 3 Extracción de características
- 4 Análisis de los servicios ocultos**
- 5 Conclusiones y trabajo futuro

Análisis de los servicios ocultos

Resultados

- Resumen de resultados
 - 17328 direcciones .onion
 - 1796 accesibles mediante HTTP/HTTPS
- **Acotación de dispositivos**
 - 346 servicios acotados a un único dispositivo



Análisis de los servicios ocultos

Ejemplos de desanonimización

Tactical technology collective - Mozilla Firefox

Tactical technology collective x +

https://tacticaltech.org

TACTICAL TECHNOLOGY COLLECTIVE

PRIVACY

DIGITAL SECURITY

INFO-ACTIVISM

About

Contact

Disclaimer

Glossary

Twitter

Blog

CC BY SA

This work is licensed under a [Creative Commons Attribution-Share Alike 3.0 Unported License](#).

Security-in-a-Box is a project of [Tactical Technology Collective](#) and [Front Line Defenders](#)

TACTICAL TECHNOLOGY COLLECTIVE

FRONT LINE DEFENDERS

Análisis de los servicios ocultos

Ejemplos de desanonimización

The image displays two side-by-side screenshots of the Pirate Bay website, illustrating a process of de-anonymization. Both screenshots show the homepage with the iconic pirate ship logo and the text "The Pirate Bay".

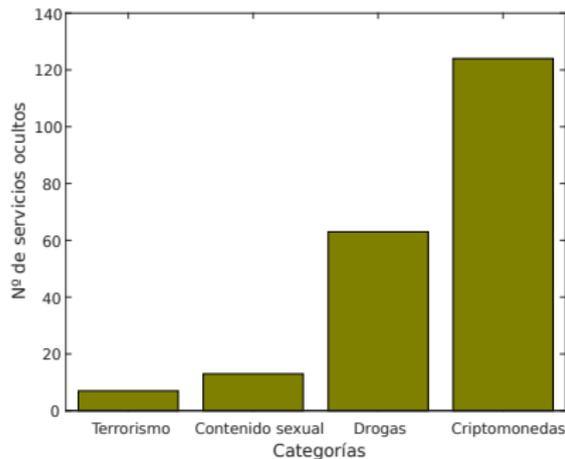
Left Screenshot: The search filter is set to "Pirate Search". Below the search bar, there are checkboxes for "All", "Audio", "Video", "Applications", "Games", "Porn", and "Other". The "All" checkbox is checked. Below these are buttons for "Pirate Search" and "I'm Feeling Lucky". A section titled "List of Pirate Bay proxies" is visible, along with links for "Login", "Register", "Language", "Select language", "About", "Blog", "Usage policy", "TOR", "Doodles", and "Forum".

Right Screenshot: The search filter is set to "Pirate Search". The "All" checkbox is checked, and the "Pirate Search" button is highlighted. The "How do I download?" section is visible, along with links for "Login", "Register", "Language", "Select language", "About", "Blog", "Usage policy", "TOR", "Doodles", and "Forum".

At the bottom of both screenshots, there are Bitcoin (BTC) and Litecoin (LTC) addresses, and a XMRR address. The addresses are identical in both screenshots, indicating that the de-anonymization process is successful in identifying the same user or service across different instances of the website.

Análisis de los servicios ocultos

Categorización



Idioma	# Num	Idioma	# Num
English	1313	Romanian	4
German	54	Turkish	4
Danish	38	Welsh	3
Portuguese	33	Slovak	3
Spanish	25	Swedish	3
French	19	Swahili	3
Italian	8	Tagalog	3
Norwegian	8	Vietnamese	3
Afrikaans	7	Indonesian	2
Dutch	7	Bulgarian	1
Somali	7	Estonian	1
Finish	6	Lithuanian	1
Polish	5	Albanian	1
Catalan	4	Unknown	229

Agenda

- 1 Introducción
- 2 Modelización
- 3 Extracción de características
- 4 Análisis de los servicios ocultos
- 5 Conclusiones y trabajo futuro**

Conclusiones y trabajo futuro

- **Diagramas UML cubriendo diferentes aspectos de la red Tor**
 - Elementos que la componen (nodos, mensajes)
 - Comunicación
 - Comportamiento de los nodos
- **Importante cantidad de datos de servicios ocultos**
 - Direcciones .onion
 - Información de su contenido, cabeceras y protocolo
- **Herramienta de desanonimización y categorización**

Trabajo futuro

- **Evaluar el comportamiento con modelos formales** (i.e., Redes de Petri)
- **Sistema de evaluación para comprobar los resultados**
- **Mejora de la categorización**

Modelización del protocolo Tor y extracción de características de servicios ocultos

Jorge García de Quirós

Ricardo J. Rodríguez



Universidad
Zaragoza

Universidad de Zaragoza, Spain

28 de mayo de 2019