

Ανωνυμία στο διαδίκτυο και δίκτυο Tor

Decentralized Web and Software Freedom meetup
Thessaloniki 8/5/2019

Vaggelis Spathas

Ανωνυμία (Anonymity)

- Τι ορίζεται ως ανωνυμία.
- Η κρυπτογράφηση δεν παρέχει ανωνυμία.

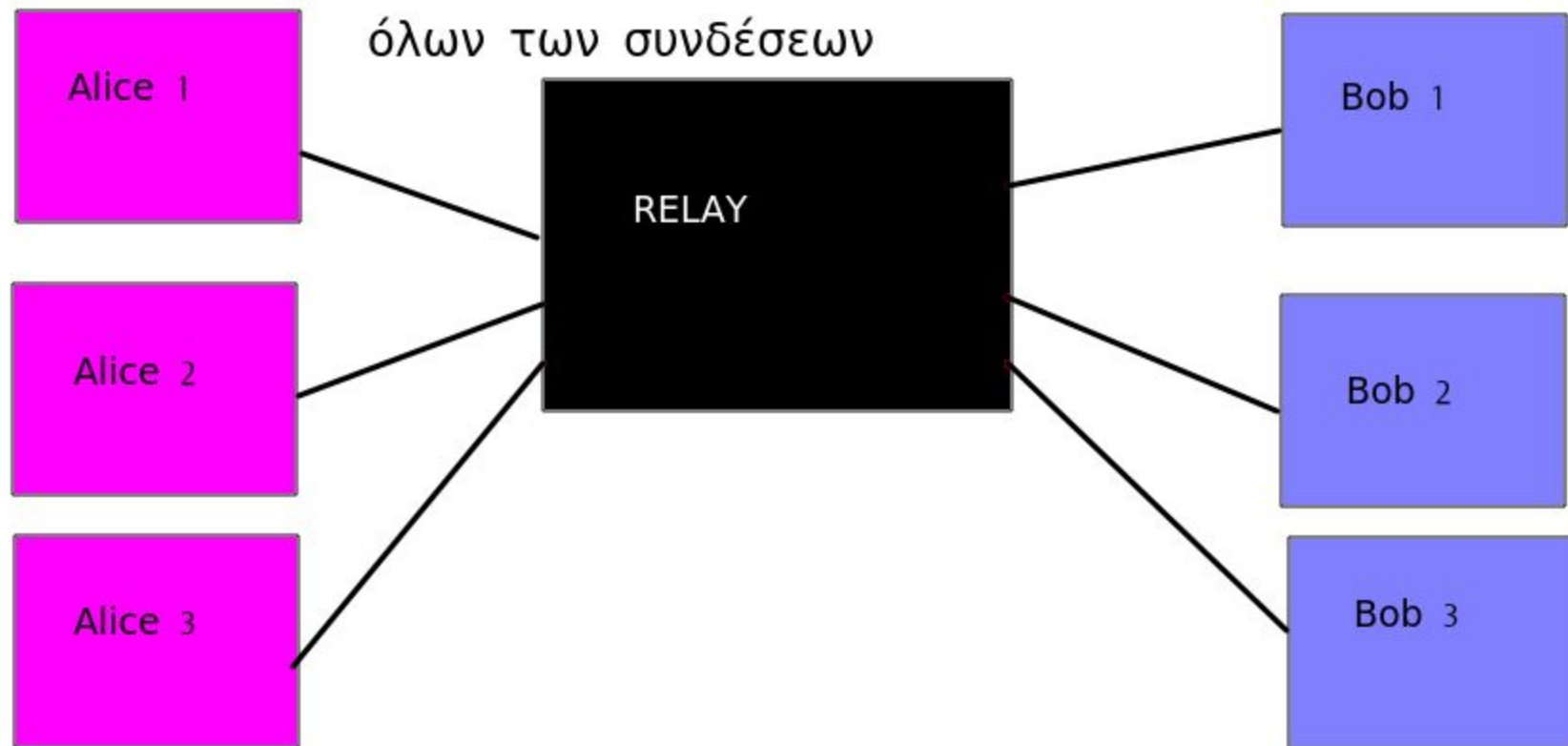
Ποιος χρειάζεται ανωνυμία?

- Ο κάθε πολίτης
- Δημοσιογράφοι / ακτιβιστές ανθρωπίνων δικαιωμάτων
- Κυβερνήσεις
- Επιχειρήσεις
- Εγκληματίες?

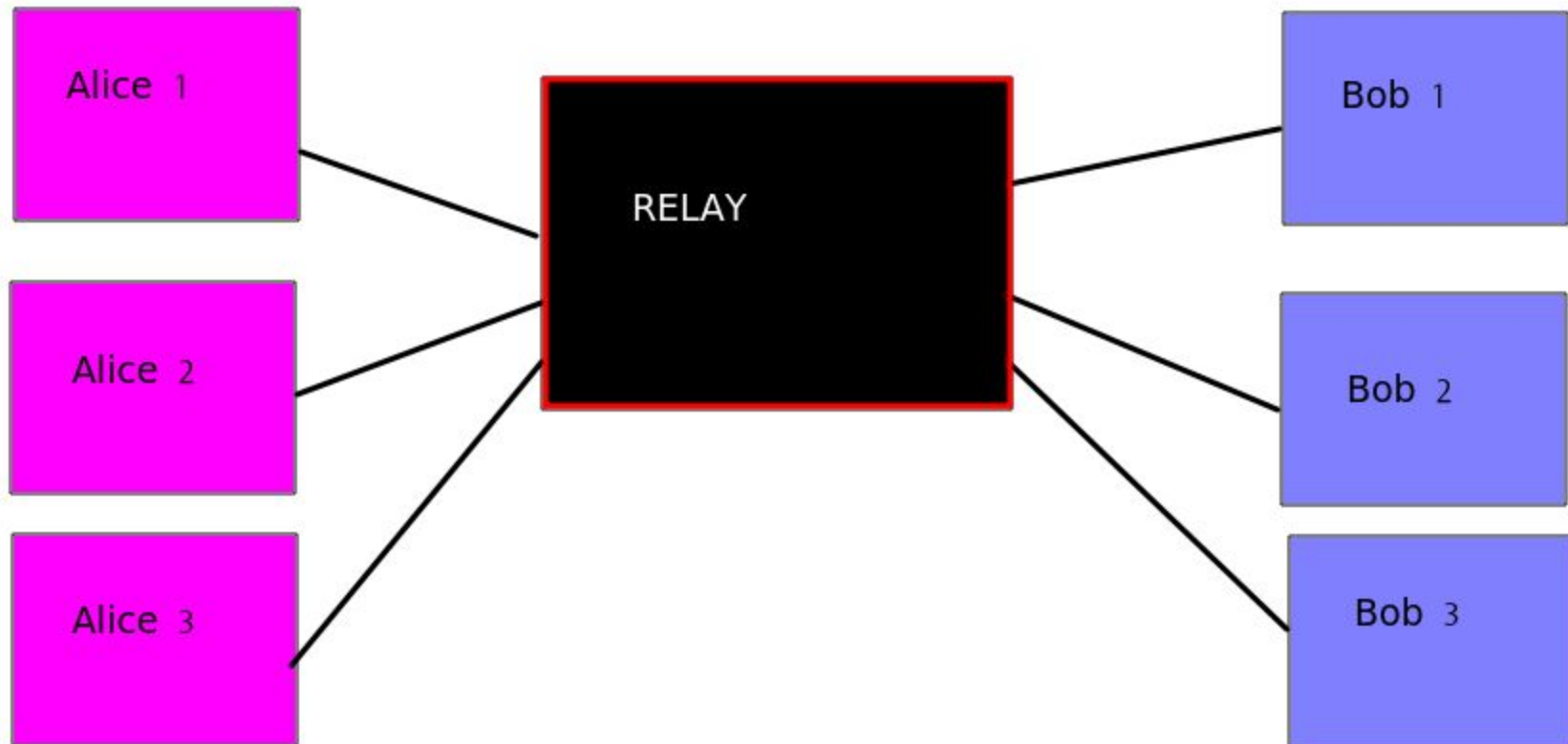
Πως μπορούμε να πετύχουμε ανωνυμία

- ασφαλή περιήγηση στους browsers?
- χρήση μηχανών αναζήτησης που δεν καταγράφουν π.χ duckduckgo
- Χρήση proxy
- Χρήση Vpn

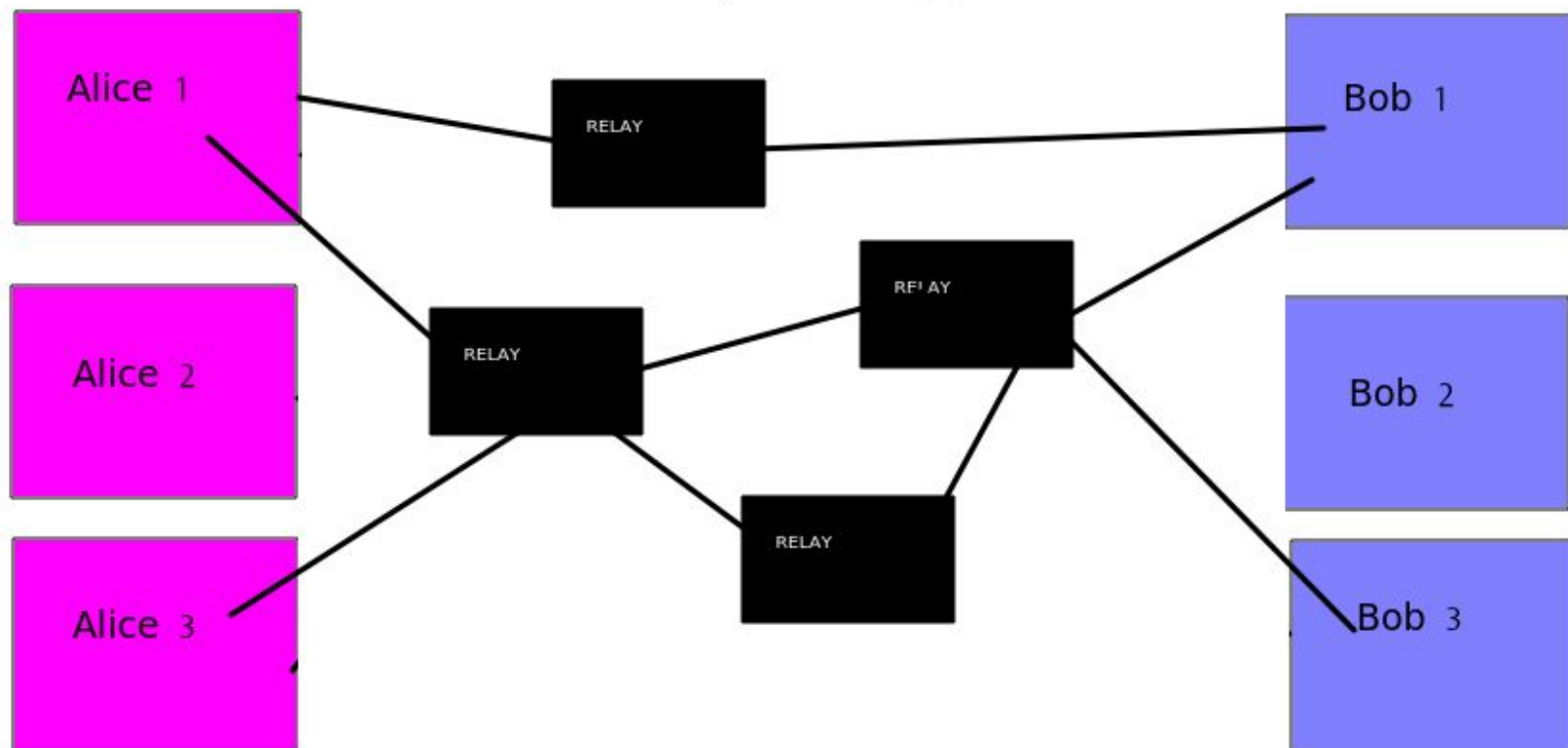
Χρήση ενός Relay για την απόκρυψη
όλων των συνδέσεων



Single Point of Failure

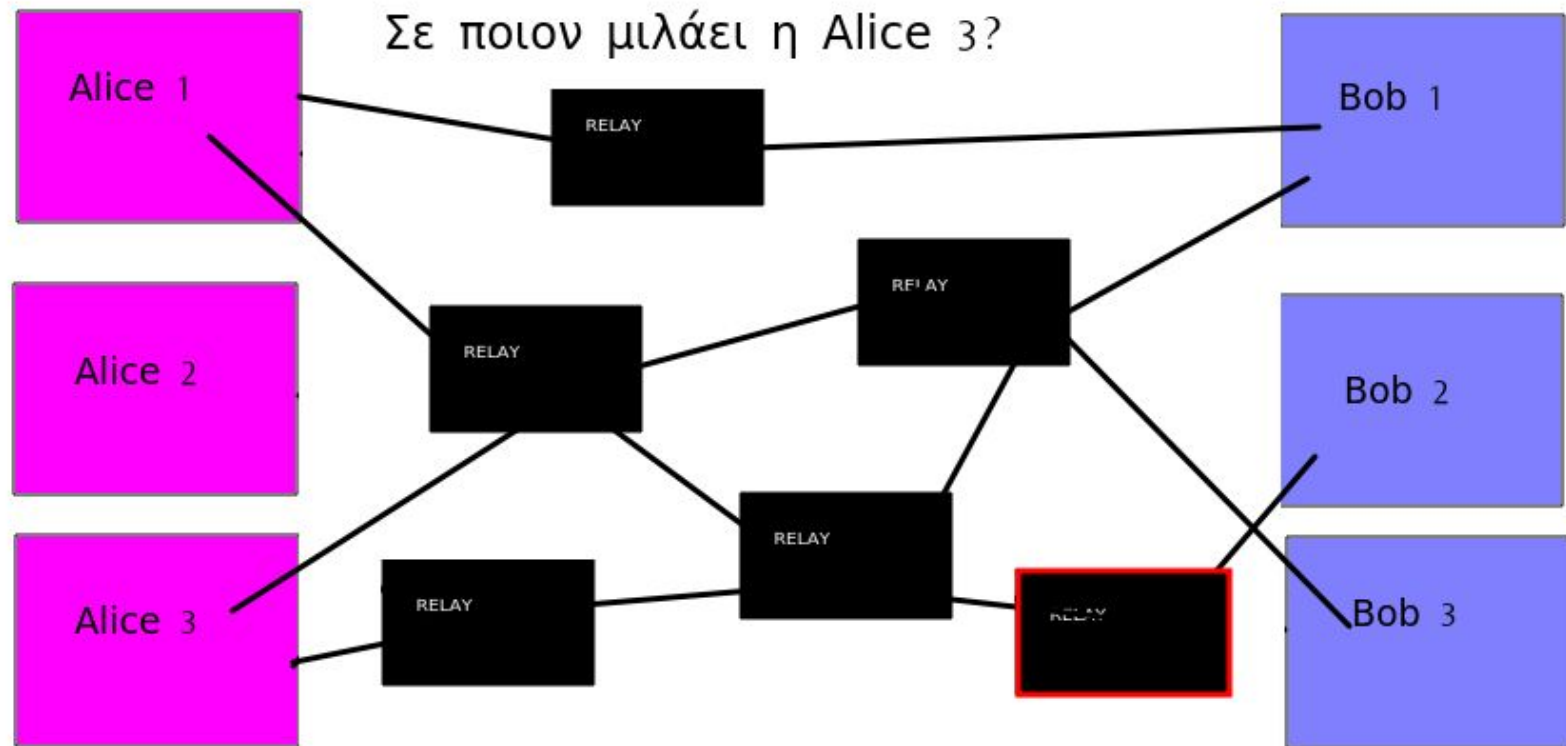


Πολλοί ενδιαμέσιοι κόμβοι



Ποιος μιλάει στο Bob 2?

Σε ποιον μιλάει η Alice 3?



Δίκτυο Tor

- Από τις πιο δημοφιλείς δυνατότητες που έχουμε να είμαστε ανώνυμοι στο διαδίκτυο.
- Ελευθερος ανοιχτός κώδικας.
- Ξεκίνησε από τους Roger Dingledine , Nick Mathewson
- Στηρίζεται στην αρχή της κατανομής της εμπιστοσύνης.
- Από 2.000.0000 έως 4.000.0000 καθημερινούς χρήστες?
- Περίπου 7000 relays 1000 bridges

Δίκτυο Tor(2)

- Ένα δίκτυο από κόμβους (relays) διαθέσιμοι για να κρύψουν την ταυτότητα μας
- Δεν μπορεί να ταυτοποιηθεί ότι η Alice αναζήτησε τον Bob
- Το Tor δεν είμαι μόνο για http.
- TCP, UDP, POP3, VoIP , FTP .e.t.c

Πως μπορώ να συνδεθώ με το Tor

- Tor browser (διατίθεται και σε android) , βασίζεται στο Mozilla Firefox.
- Με χρήση προγραμμάτων που επικοινωνούν μέσω Tor
Thunderbird plugin , Ricochet, SecureDrop , OnionShare, Tails.e.t.c..

SURFACE WEB

Wikipedia

Google

Bing

Academic Information

Medical Records

Legal Documents

Scientific Reports

Subscription Information

Multilingual Databases

Conference Proceedings

Government Resources

Competitor Websites

Organization-specific
Repositories

DEEP WEB

Illegal Information

TOR-Encrypted sites

DARK WEB

Drug Trafficking sites

Private Communications

Πως μπορώ να “κρύψω” την ιστοσελίδα μου

→ Onion services

→ Μπορώ να φτιάξω onion service για να αποκτήσουν πρόσβαση στην ιστοσελίδα/εφαρμογή μου χρήστες που είναι “κομμένοι” στην χώρα ή στο δίκτυο που χρησιμοποιώ.

facebook

Email or Phone

Password

Log In

[Forgot account?](#)

Connect with friends and the
world around you on Facebook.



See photos and updates from friends in News Feed.



Share what's new in your life on your Timeline.



Find more of what you're looking for with Facebook Search.

Sign Up

It's free and always will be.

First name

Last name

Mobile number or email

New password

Birthday

May

3

1994

[Why do I need to provide my birthday?](#)☐ Female☐ Male

By clicking Sign Up, you agree to our [Terms](#), [Data Policy](#) and [Cookies Policy](#). You may receive SMS Notifications from us and can opt out any time.

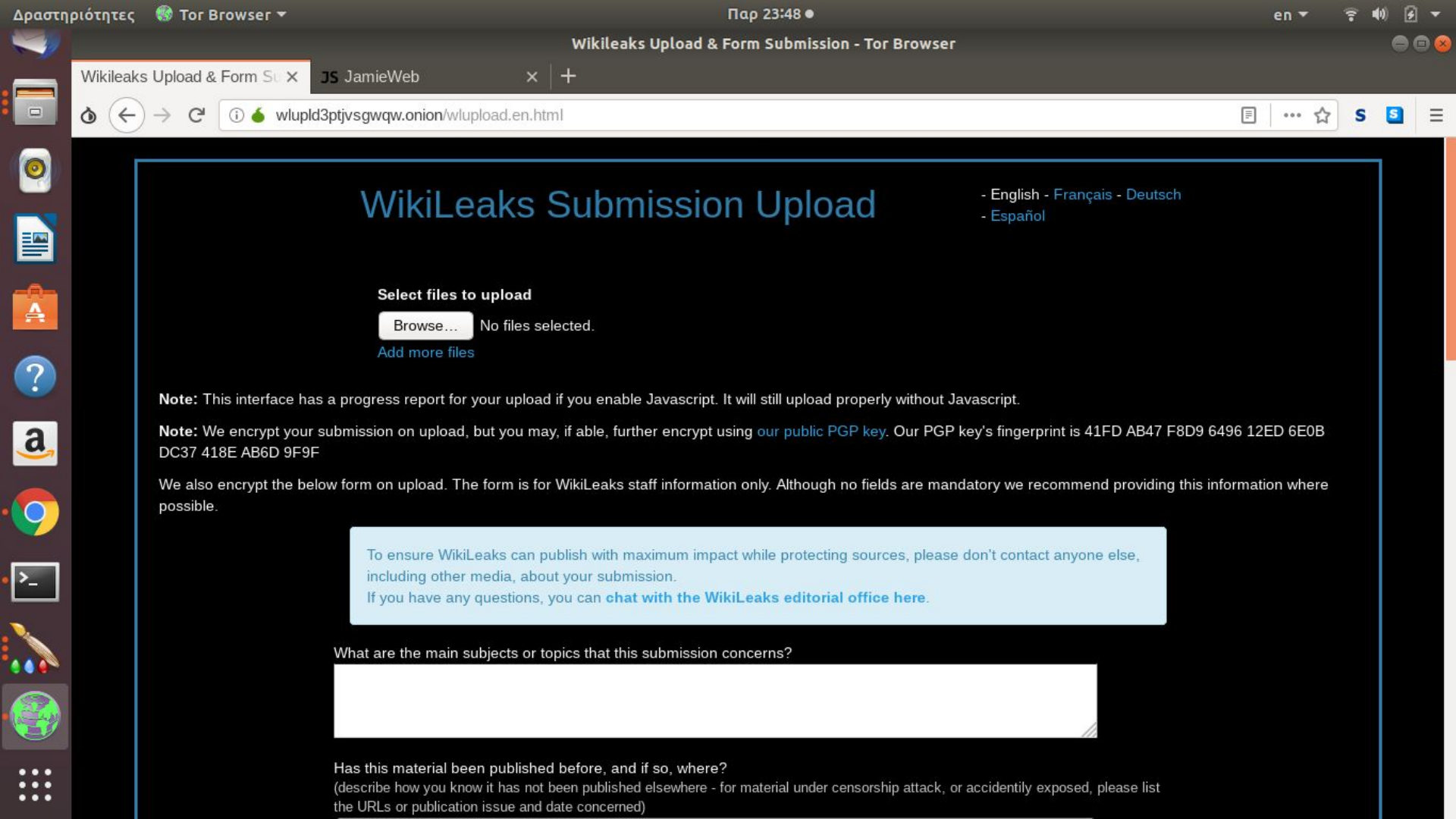
Sign Up

[Create a Page](#) for a celebrity, band or business.

Tor Browser

Onion services

- Μπορώ να στήσω ιστοσελίδα μέσα στο δίκτυο Tor.
- Πλεονεκτήματα?
- Μπορώ να ψάξω για onion ιστοσελίδες με ειδικές μηχανές αναζήτησης π.χ <https://ahmia.fi> , `hss3uro2hsxfogfq.onion`



WikiLeaks Submission Upload

- English - Français - Deutsch
- Español

Select files to upload

Browse...

No files selected.

[Add more files](#)

Note: This interface has a progress report for your upload if you enable Javascript. It will still upload properly without Javascript.

Note: We encrypt your submission on upload, but you may, if able, further encrypt using [our public PGP key](#). Our PGP key's fingerprint is 41FD AB47 F8D9 6496 12ED 6E0B DC37 418E AB6D 9F9F

We also encrypt the below form on upload. The form is for WikiLeaks staff information only. Although no fields are mandatory we recommend providing this information where possible.

To ensure WikiLeaks can publish with maximum impact while protecting sources, please don't contact anyone else, including other media, about your submission.
If you have any questions, you can [chat with the WikiLeaks editorial office here](#).

What are the main subjects or topics that this submission concerns?

Has this material been published before, and if so, where?

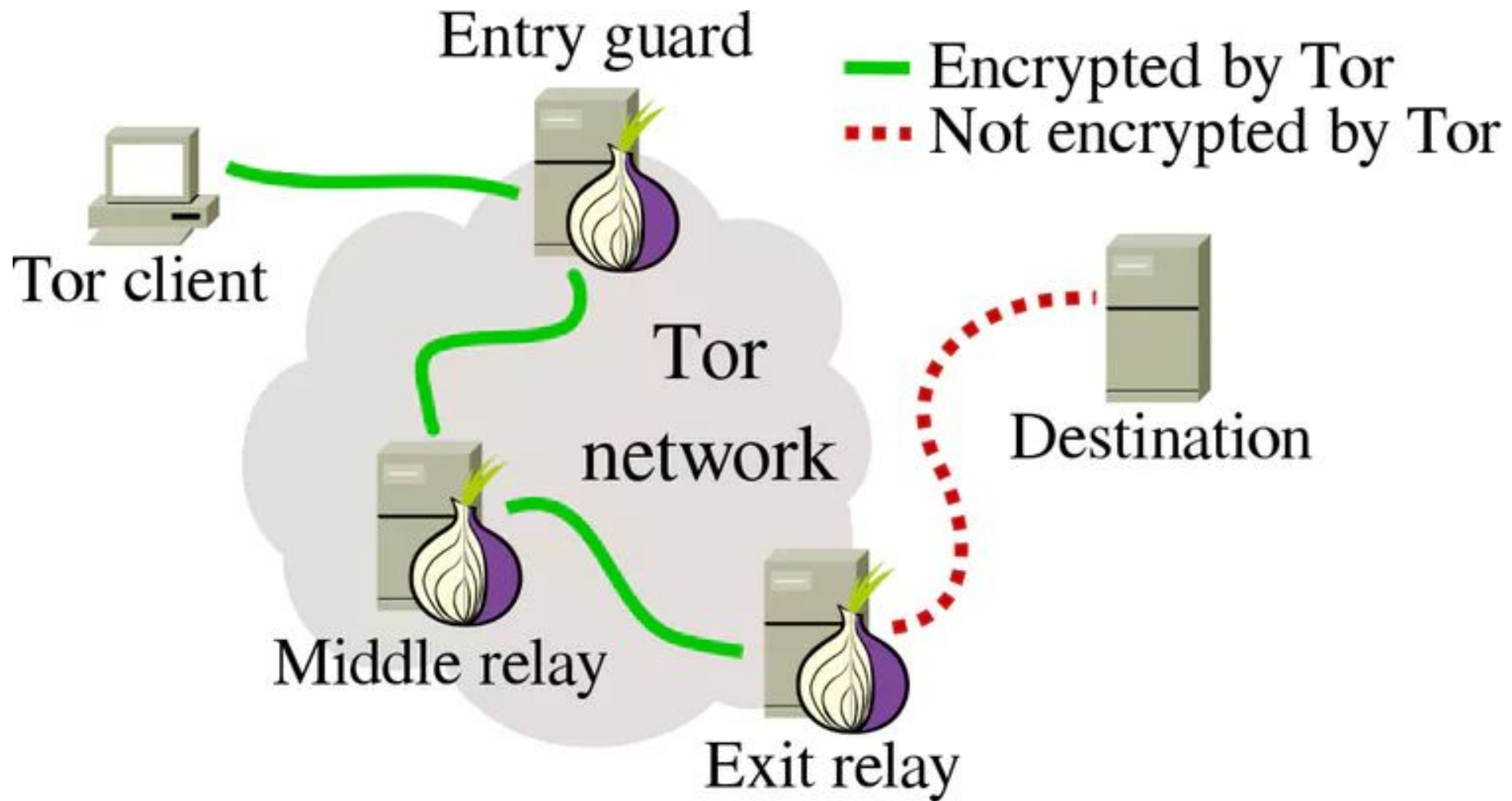
(describe how you know it has not been published elsewhere - for material under censorship attack, or accidentally exposed, please list the URLs or publication issue and date concerned)

Μέρος Β

Tor Under the hood

Πως επικοινωνούμε με το Tor?

SOCKS proxy



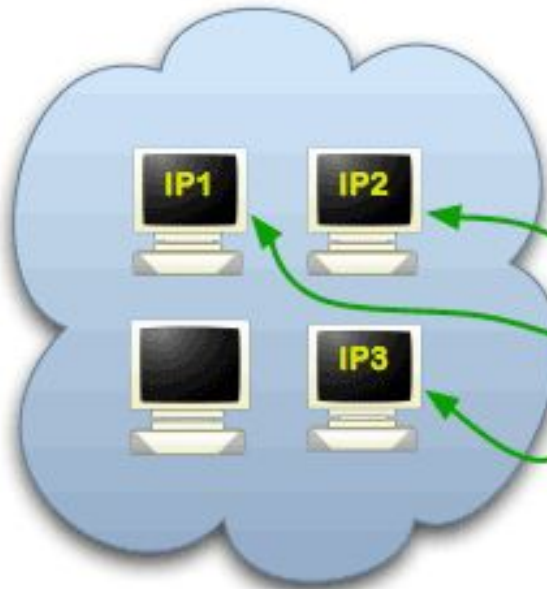


Onion Services: Step 1

Step 1: Bob picks some introduction points and builds circuits to them.



Alice



Tor cloud



Tor circuit

IP1-3

Introduction points

PK

Public key

cookie

One-time secret

RP

Rendezvous point



Bob

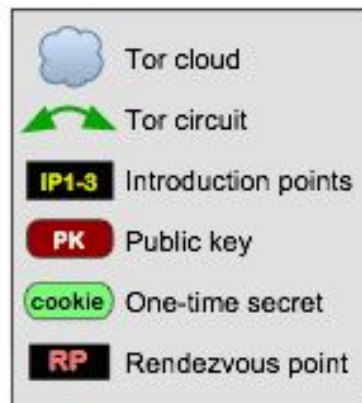
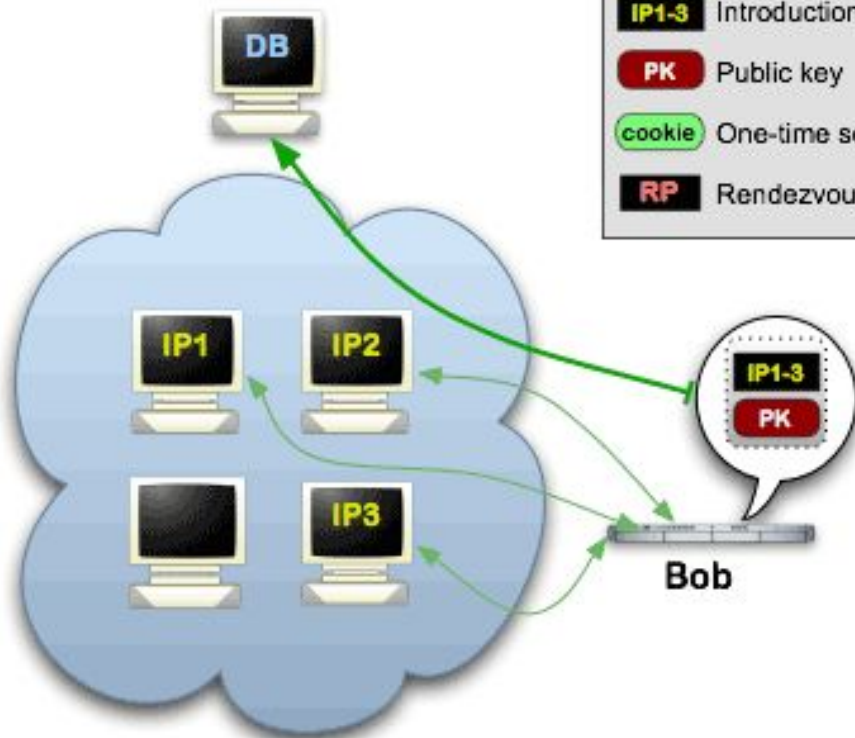


Onion Services: Step 2

Step 2: Bob advertises his service -- XYZ.onion -- at the database.



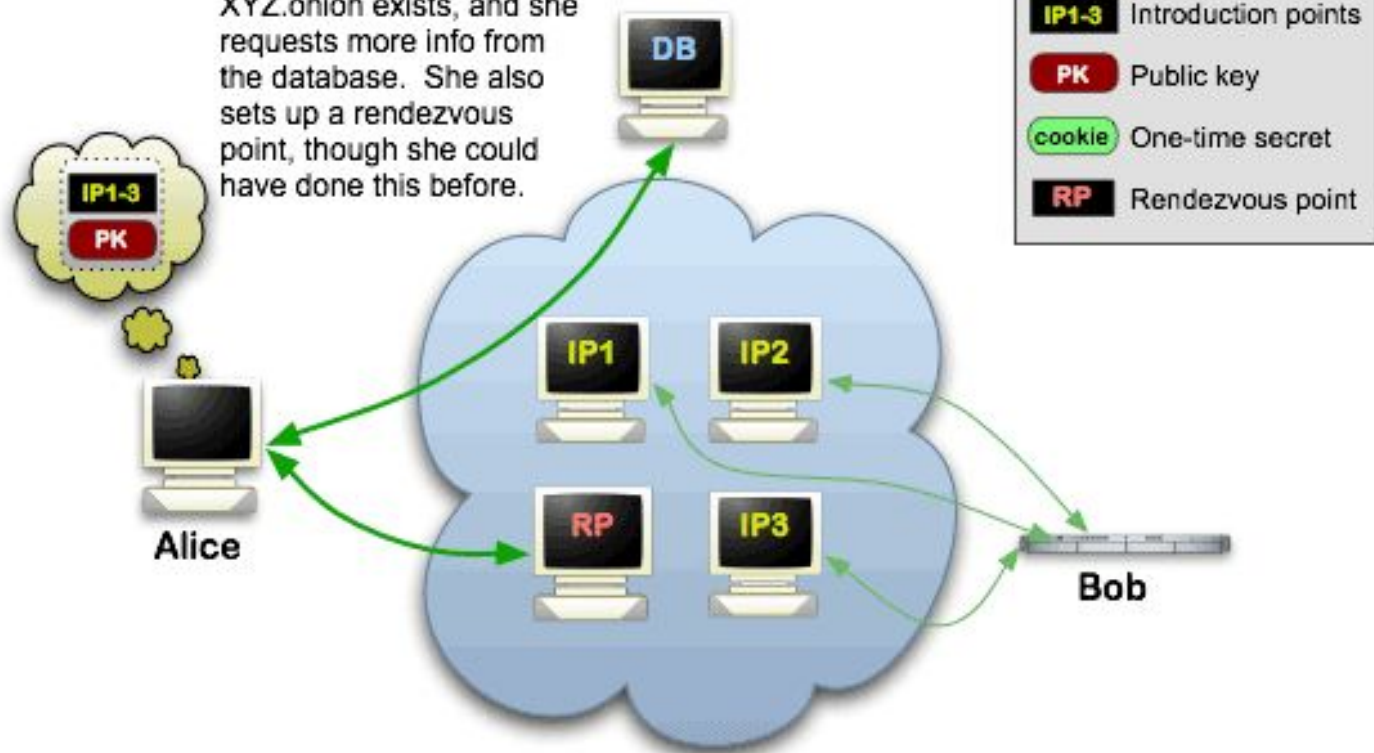
Alice





Onion Services: Step 3

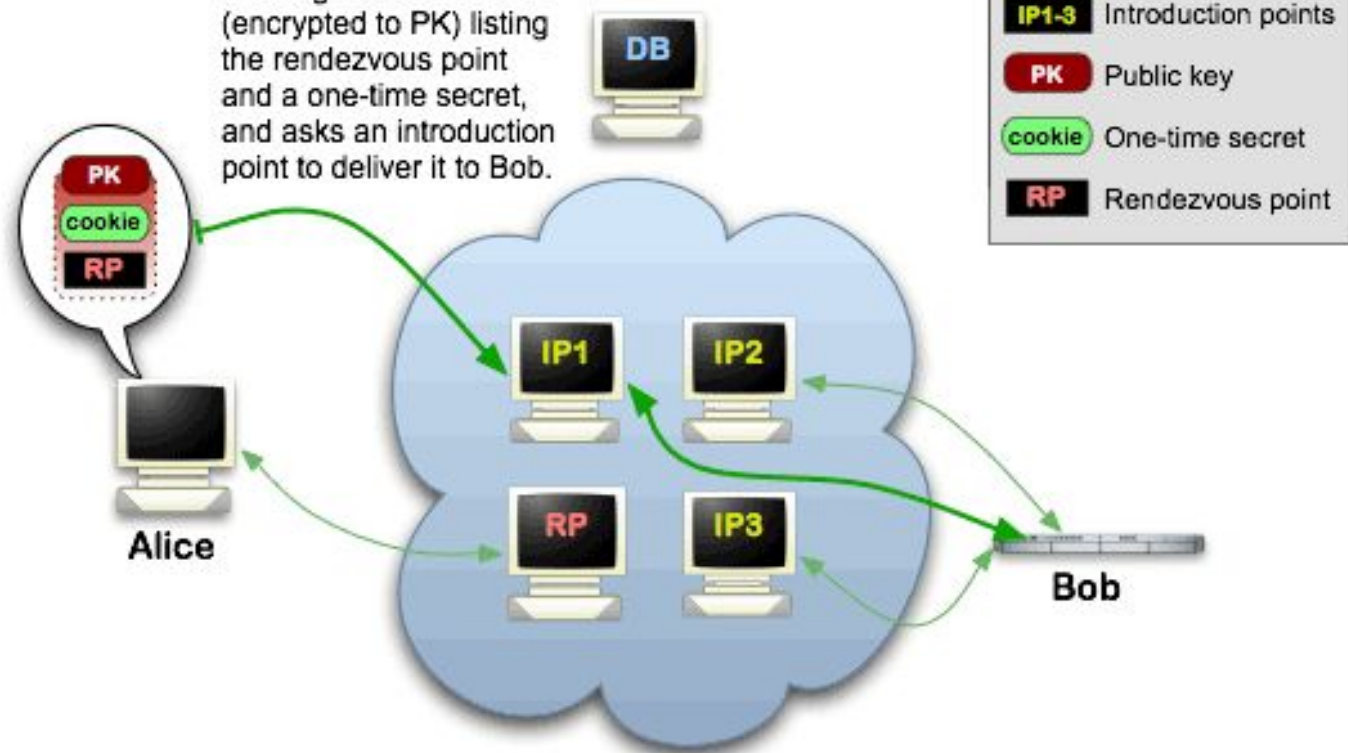
Step 3: Alice hears that XYZ.onion exists, and she requests more info from the database. She also sets up a rendezvous point, though she could have done this before.





Onion Services: Step 4

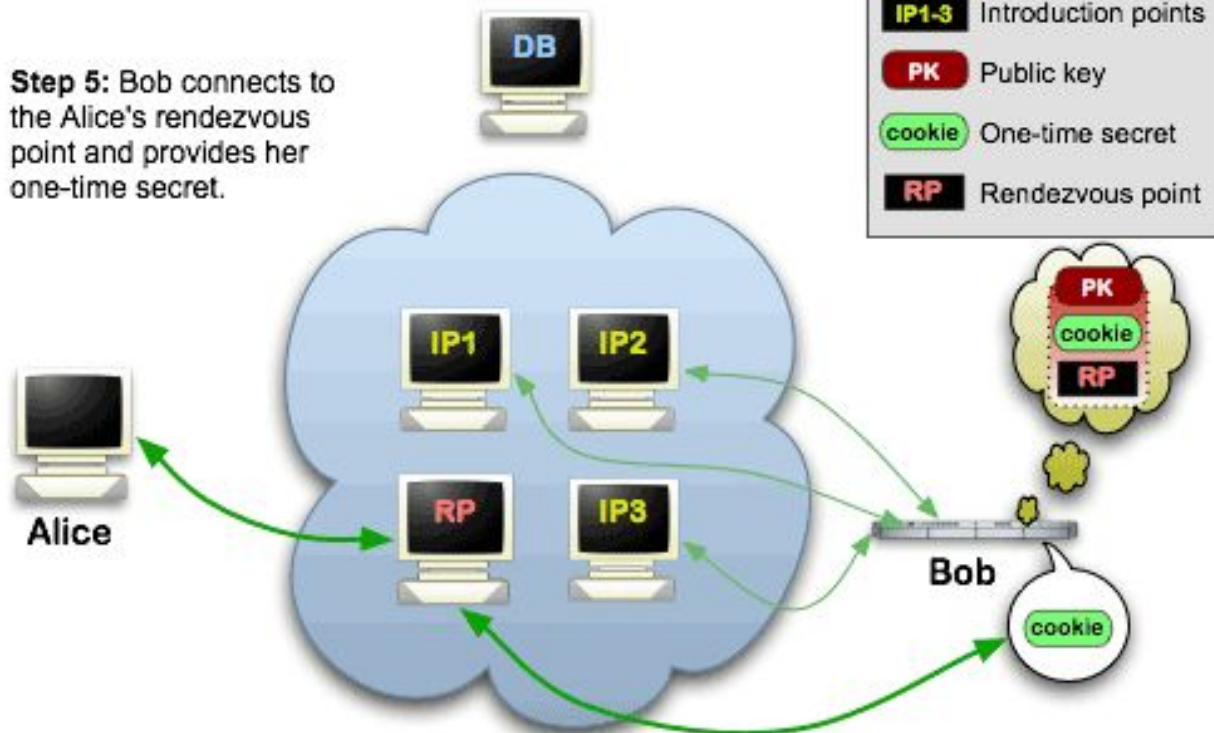
Step 4: Alice writes a message to Bob (encrypted to PK) listing the rendezvous point and a one-time secret, and asks an introduction point to deliver it to Bob.





Onion Services: Step 5

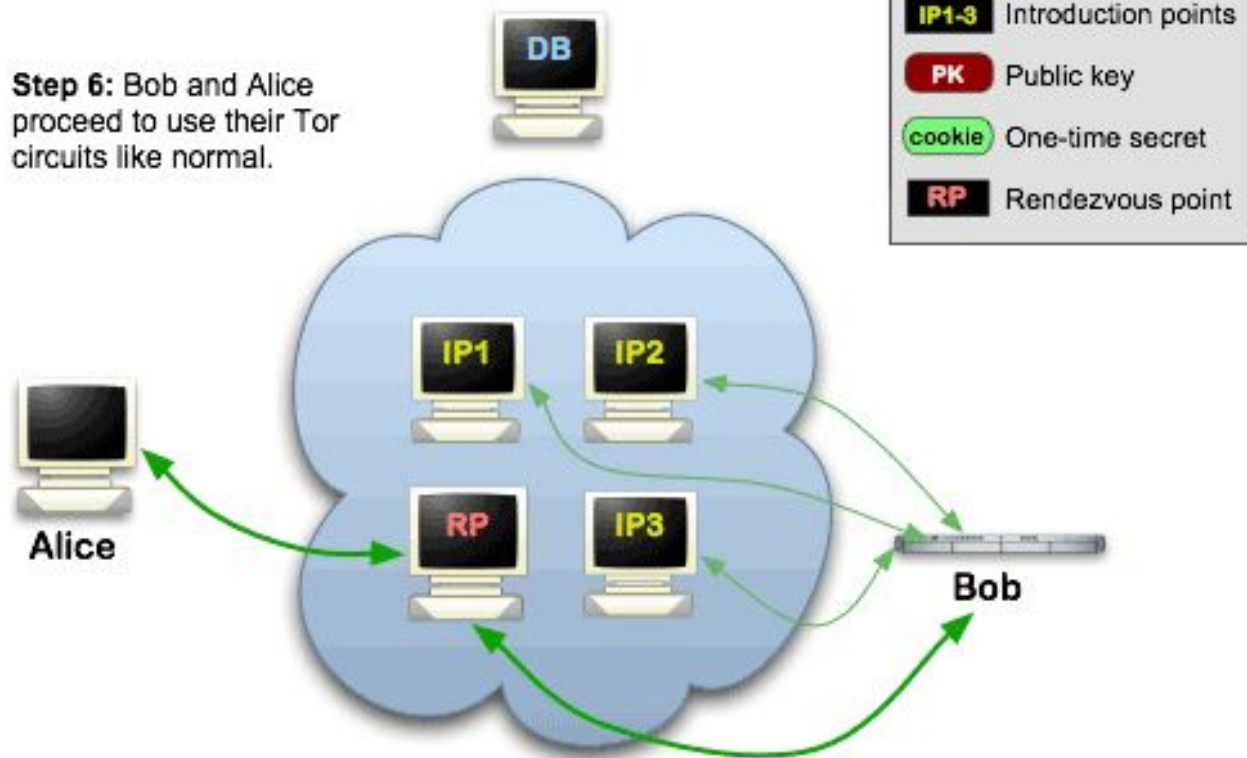
Step 5: Bob connects to the Alice's rendezvous point and provides her one-time secret.





Onion Services: Step 6

Step 6: Bob and Alice proceed to use their Tor circuits like normal.



Πως στήνω ένα onion service(1)

- Σηκώνω ένα application locally π.χ στο localhost:8080
- Εγκαθιστώ το tor client
π.χ `sudo apt install tor` (Ubuntu)

Πως στήνω ένα onion service(2)

- Προσθέτω στο `/etc/tor/torrc` τα εξής:
`HiddenServiceDir /home/myusername/hidden_service/`
`HiddenServicePort 80 127.0.0.1:8080`
- Κάνω restart to tor (service tor restart)
- Ανοίγω το `/home/myusername/hidden_service/hostname` και ανακτώ το onion url

bridges

- Κρυφά relays για χρήστες με κομμενη πρόσβαση στα public relays.
- Διατίθενται μέσα από Tor Browser (<https://bridges.torproject.org>), gmail(bridges@bridges.torproject.org).

bridges(2)

→ pluggable transports

για να αποφευχθεί το κόστος της συνδεσης σε tor
με βάση την ανάλυση της δικτυακής κίνησης.

Ευάλωτα σημεία στο Tor

- Το Exit relay μπορεί να στείλει και σε http
- Σχεδιασμένο εξάρής σαν low latency Anonymous Network

Ενίσχυση της ασφάλειας στο Tor

- Αυξηση και διασπορά των Relays
- Αύξησης και διασπορά των χρηστών

Πως μπορώ να βοηθήσω

- Αν έχω υπολογιστή που είναι διαρκώς στο διαδίκτυο. Προσφέρω bandwidth σαν Relay.
- Βοηθάω σε documentation, tor projects, ανοιχτά θέματα προς έρευνα

Πηγες

- <https://www.torproject.org/>
- Αρχικό κείμενο δημοσίευσης για Tor
- <https://www.youtube.com/watch?v=QRYzre4bf7I>
- <https://media.torproject.org/video/tor-internet-days-2010.mp4>
- <https://research.torproject.org/ideas/>
- Ανάλυση των βασικών σημείων του Tor στα Ελληνικά
(<https://www.cs.ucy.ac.cy/courses/EPL682/reports/anonymous-communication-report.pdf>)



<https://freeolabini.org/en/>