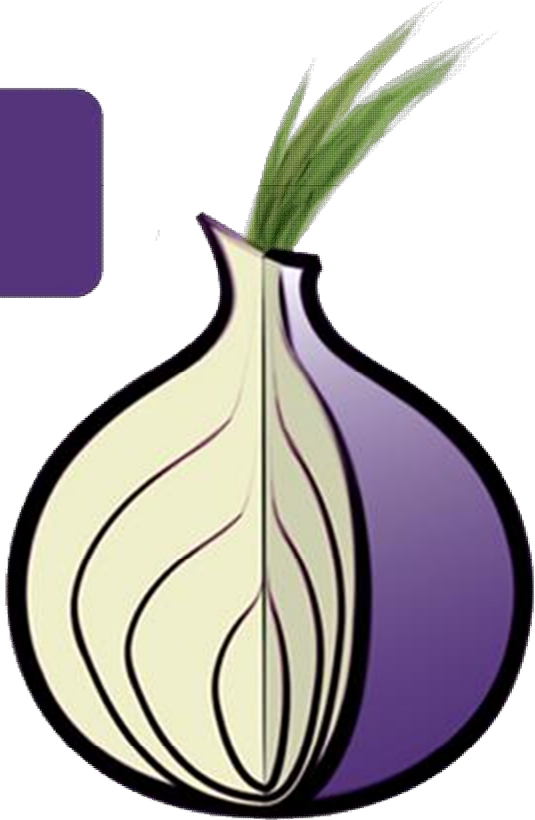


Όσο ξεκινάμε...

- Κατεβάστε το OTR για το σύστημά σας:
 - Αν έχετε Linux ή Windows, Pidgin & OTR:
 - <https://www.pidgin.im/>
 - <https://otr.cypherpunks.ca>
 - Αν έχετε Mac, Adium:
 - <https://adium.im/>
- Εγκαταστήστε τα

T  **r**

Ας κατεβάσουμε το Tor

- <https://www.torproject.org/>

Αποκάλυψη ταυτότητας

- Από το IP μπορεί να βρεθούν...
 - Η θέση μας στον πλανήτη
 - Ο παροχέας Internet που χρησιμοποιούμε
 - Το πραγματικό μας όνομα (με ένταλμα)
- Κάθε ιστοσελίδα που επισκεπτόμαστε βλέπει το IP
 - ...και ενδεχομένως το καταγράφει

Demo αποκάλυψης IP

- <http://wtfismyip.com/>

Tor

- Ένα σύστημα που μας επιτρέπει να είμαστε ανώνυμοι
- Το IP που φαίνεται είναι διαφορετικό από το πραγματικό

Tor Browser Bundle

- Ακόμα και μέσω Tor ο browser μας μπορεί να ταυτοποιηθεί
 - <https://panopticklick.eff.org/>
 - Από τα διάφορα features που έχετε ενεργοποιημένα
 - Javascript, Flash, Java, Silverlight
 - Όνομα του browser
 - Λειτουργικό σύστημα
 - Εκδόσεις
- Γι' αυτό χρησιμοποιούμε το Tor Browser Bundle
 - Ίδιος browser για όλους
 - Εγκατεστημένο HTTPS everywhere
 - Απενεργοποιήστε την Javascript!

Onion routing

- Εξασφαλίζει την ανωνυμία
- Ανάμεσα στον υπολογιστή μας και τον server υπάρχουν 3 tor nodes
- Κάθε node ξέρει μόνο για τους άμεσους γείτονές του
- Για κάθε σύνδεση, ο υπολογιστής μας διαλέγει τυχαία 3 άλλους υπολογιστές που τρέχουν το tor
- Τα δεδομένα περνούν από αυτούς

How Tor Works



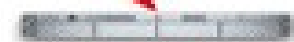
Alice



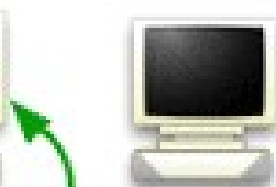
Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.



Jane



Bob



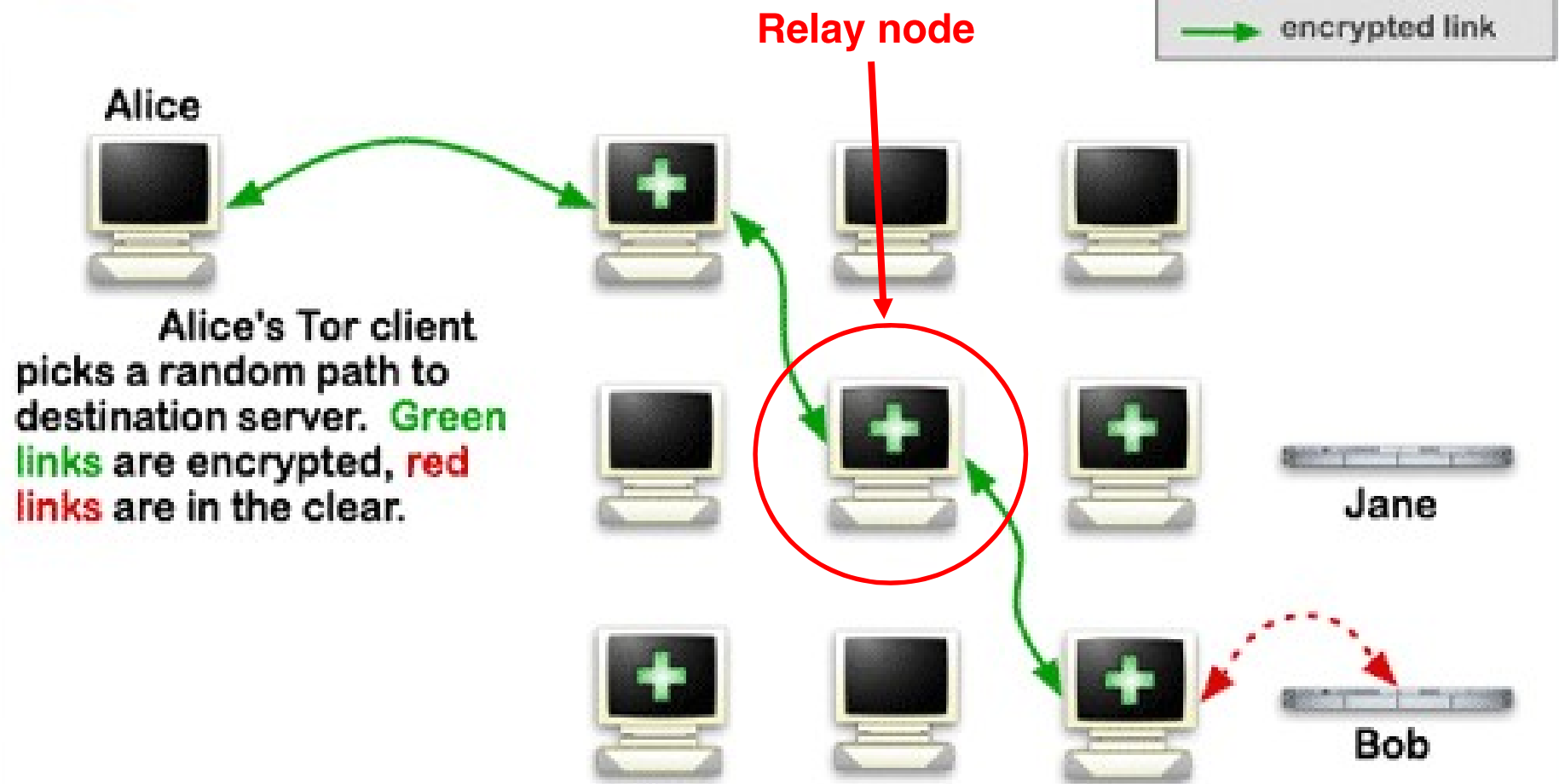
Tor nodes

- Κάθε node έχει ένα public key
- Κάνουμε encrypt τα δεδομένα μας με το public key του καθενός από τα 3 nodes αλληπάλληλα

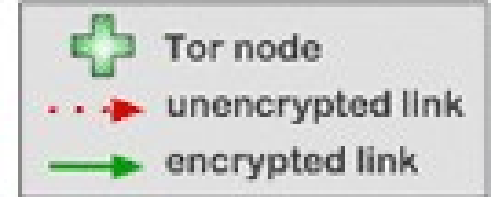
Exit & Relay nodes

- Είναι τα nodes από τα οποία βγαίνουν τελικά τα δεδομένα
 - Μπορεί να δει/αλλάξει τα δεδομένα μας αν δεν χρησιμοποιούμε HTTPS
- Ένα node μπορεί να γίνει exit node εθελοντικά αν το επιθυμεί ο χρήστης
 - Απενεργοποιημένο by default
 - Ενδεχομένως να είστε νομικά υπεύθυνοι για το traffic που βγαίνει από τη σύνδεσή σας
- Ένα node μπορεί να γίνει relay node εθελοντικά
 - Παρακαλούμε να γίνετε
 - Δεν υπάρχει νομικό πρόβλημα

How Tor Works



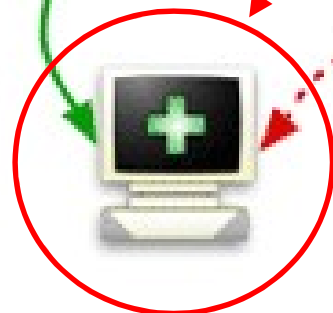
How Tor Works



Alice



Alice's Tor client picks a random path to destination server. **Green links** are encrypted, **red links** are in the clear.



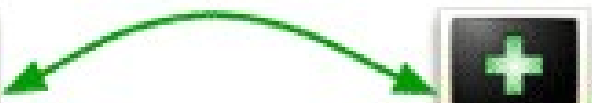
Exit node



Jane



Bob

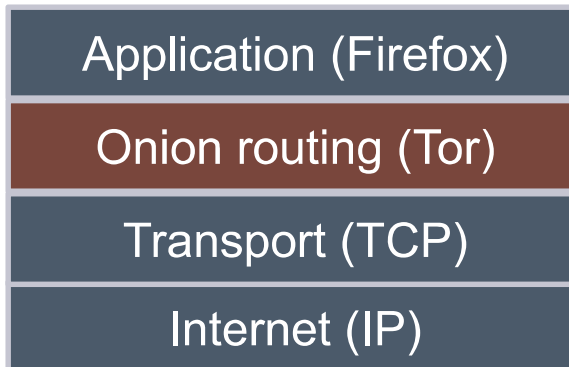


Demo ανωνυμίας

- <http://wtfismyip.com> με Tor

Tor: Όχι μόνο για browsing...

- Οποιαδήποτε υπηρεσία μπορεί να περάσει μέσω Tor
- Λειτουργεί ως SOCKS proxy



Προσοχή!

- Πολλές εφαρμογές δεν δουλεύουν σωστά μέσω Tor
 - π.χ. Torrents
- Μερικές φορές το IP μας φαίνεται με τρόπους που δεν περιμένουμε
 - DNS leaks: Η εφαρμογή προσπαθεί να κάνει resolve ένα IP και στέλνει το DNS ερώτημα εκτός Tor
- Tails: Διανομή Linux που φροντίζει όλα να περνούν από Tor



FBI agents tracked Harvard bomb threats despite Tor

By **Russell Brandom** on December 18, 2013 12:55 pm [Email](#) [@russellbrandom](#)

DON'T MISS STORIES *FOLLOW THE VERGE*



323k



386K followers



HEADLINES



iTunes Festival comes to US for the first time at SXSW



HTC's 2014 One leaks out in first press image



A North Dakota town is the most expensive place to rent an apartment in the United States



UK court says nine-hour detention of Greenwald's partner was lawful



Lose yourself to dance with this 'Happy' and 'Get Lucky' mashup



USES TOR



GETS ARRESTED

memegenerator.net

Hidden services

- Εκτός από τον client, κρύβεται και ο server
- Δεν είναι προσβάσιμα στο κανονικό Internet
 - Clearnet: Προσβάσιμα μέσω ενός κανονικού browser
 - Darknet ή Deep web: Πρόσβαση μόνο μέσω Tor
- 6 Tor relay hops
- Τα δεδομένα δεν βγαίνουν ποτέ από το Tor δίκτυο
- Αντίστοιχη διαδικασία με πριν, αλλά χωρίς exit node



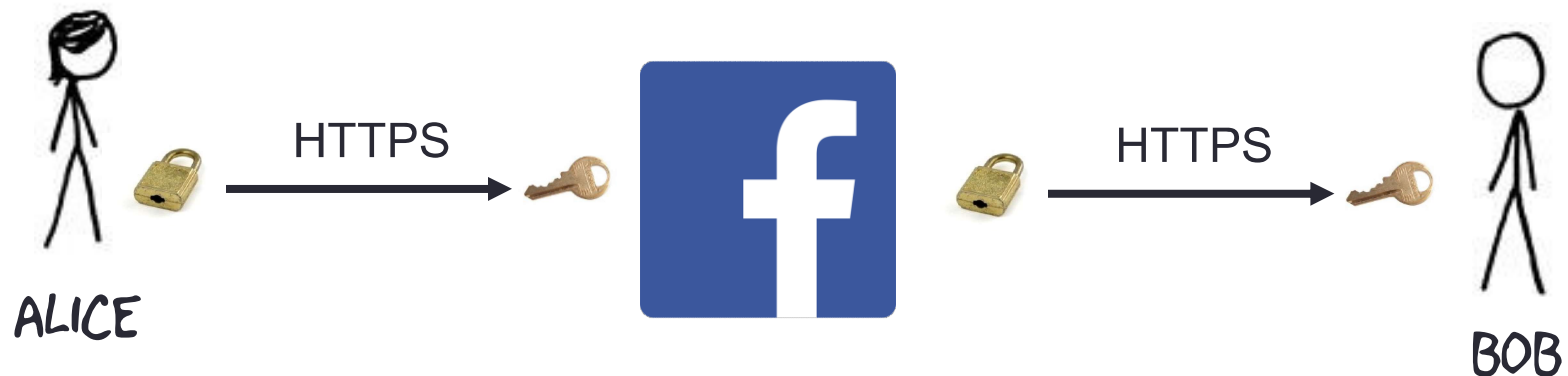
OTR: Off-the-record

Συμβατικό chat

- Παραδοσιακά συστήματα chat
 - Facebook
 - Skype
 - Google Talk
 - MSN

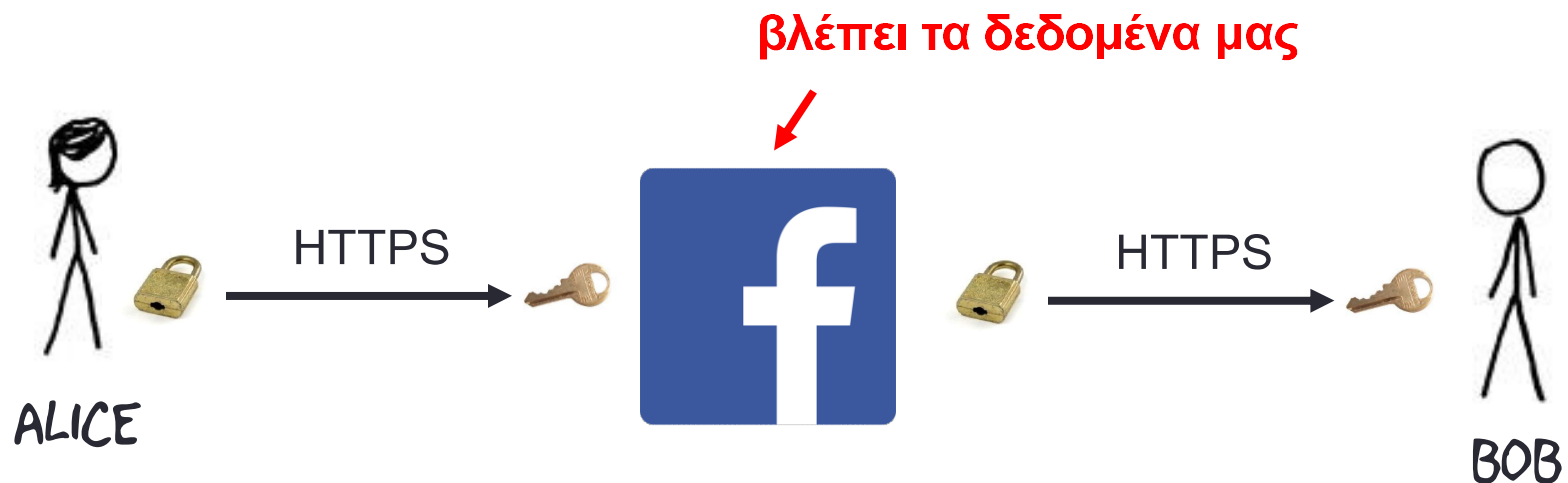
Συμβατικό chat

- Η Alice κρυπτογραφεί με το δημόσιο κλειδί του Facebook
- Το Facebook αποκρυπτογραφεί με το ιδιωτικό κλειδί του
- Το Facebook κρυπτογραφεί με το δημόσιο κλειδί του Bob
- Ο Bob αποκρυπτογραφεί με το ιδιωτικό κλειδί του
- Όμως η ίδια η υπηρεσία βλέπει καθαρό κείμενο



Συμβατικό chat

- Το Facebook διαβάζει το chat μας!
- Είναι στην πράξη «νόμιμος» man-in-the-middle
- Υπηρεσία βλέπει τα δεδομένα μας
- Τα αποθηκεύει
- Μπορεί να τα αποκαλύψει αν υπάρχει ένταλμα
- Μπορεί να μας στείλει ό,τι θέλει



Κρυπτογράφηση end-to-end

- Η Alice κρυπτογραφεί δεδομένα για τον Bob
- Το Facebook βλέπει μόνο κρυπτογραφημένα δεδομένα



Κρυπτογράφηση

- Κάθε OTR client έχει ένα ζεύγος κλειδιών
- Ασύμμετρη κρυπτογραφία
- Κλειδιά DSA
- Έχουμε ένα αποτύπωμα ανά λογαριασμό ανά client

Κρυπτογράφηση και πιστοποίηση

- Τα μηνύματα κρυπτογραφούνται
- ... αλλά υπογράφονται και ψηφιακά
- Μπορούμε να είμαστε σίγουροι ότι ο συνομιλητής μας έγραψε αυτά που έγραψε

Perfect Forward Secrecy

- Για κάθε μήνυμα χρησιμοποιείται ένα τυχαίο συμμετρικό κλειδί
- Το κλειδί αυτό δεν στέλνεται ποτέ στο δίκτυο
 - Diffie-Hellman
 - ..αλλά και οι 2 συνομιλητές καταλήγουν στο ίδιο μυστικό κλειδί
- Αν ποτέ κατασχεθεί κάποιο ή και τα 2 DSA κλειδιά, δεν μπορούν να διαβαστούν παλαιότερα μηνύματα ακόμα κι αν έχουν υποκλαπεί!

Deniability

- Ο Bob ξέρει ότι τα μηνύματα που λαμβάνει τα έχει γράψει η Alice
- Ο Bob δεν μπορεί να αποδείξει σε τρίτους μετέπειτα ότι τα έγραψε η Alice

Επιβεβαίωση αποτυπώματος OTR

- Πρέπει να επιβεβαιώσουμε ότι το κλειδί που μας παρουσιάζεται ανήκει στον άνθρωπο που πιστεύουμε
 - Παρόμοια με την GPG υπογραφή κλειδιού
- Διάφοροι τρόποι επιβεβαίωσης
- Τυπικά ζητάμε από τον ιδιοκτήτη του OTR κλειδιού να το υπογράψει με το GPG κλειδί του
 - <http://petrosagg.com/otr.txt>
 - <https://dionyziz.com/otr>

Επιβεβαίωση αποτυπώματος OTR

- Επιβεβαιώνουμε ότι το OTR αποτύπωμα που φαίνεται στο πρόγραμμα chat ταιριάζει με το GPG υπογεγραμμένο OTR αποτύπωμα
- Επιβεβαιώνουμε την ψηφιακή υπογραφή GPG
- Επιβεβαιώνουμε ότι το GPG κλειδί είναι αυτό το οποίο ήδη εμπιστευόμαστε



OTR demo