ΤΕΧΝΟΛΟΓΙΚΟ
ΕΚΠΑΙΔΕΥΤΙΚΟ
ΙΔΡΥΜΑ
ΔΥΤΙΚΗΣ ΕΛΛΑΔΑΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ Τ.Ε.

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΙΔΙΩΤΙΚΟΤΗΤΑ ΚΑΙ ΑΝΩΝΥΜΟΠΟΙΗΣΗ ΜΕΣΩ ΤΗΣ ΤΕΧΝΟΛΟΓΙΑΣ ONION ROUTING ΚΑΙ ΤΟΥ ΛΟΓΙΣΜΙΚΟΥ TOR.

ΚΑΪΣΗ ΑΘΗΝΑ
ΚΑΙ
ΚΟΝΤΟΓΙΑΝΝΑΤΟΣ ΝΙΚΟΛΑΟΣ

Σύνταξη: ΚΑΪΣΗ ΑΘΗΝΑ, ΑΜ:1393
Και
ΚΟΝΤΟΓΙΑΝΝΑΤΟΣ ΝΙΚΟΛΑΟΣ, ΑΜ: 1429

Επιβλέπων Καθηγητής κ. Α.Φούρναρης

Αντίρριο Φεβρουάριος 2017

Ευχαριστίες:

Θα θέλαμε να ευχαριστήσουμε τον εισηγητή μας καθηγητή κ. Α.Φούρναρη , ο οποίος μας επόπτευε στην πτυχιακή εργασία μας και τις οικογένειές μας για τη συμπαράστασή τους.

Υπεύθυνη Δήλωση:

Βεβαιώνουμε ότι είμαστε συγγραφείς αυτής της πτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην πτυχιακή εργασία.

Επίσης έχουμε αναφέρει τις όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες.

Επίσης βεβαιώνουμε ότι αυτή η πτυχιακή εργασία προετοιμάστηκε από εμάς προσωπικά ειδικά για τις απαιτήσεις του προγράμματος σπουδών του **Τμήματος Μηχανικών Πληροφορικής Αντιρρίου** ***(Πρώην Τμήμα Τηλεπικοινωνιακών Συστημάτων και Δικτύων).***

Δομή και στόχοι της διπλωματικής εργασίας:

Η διπλωματική μας εργασία αποτελείται από εννοιολογικά τμήματα. Παρουσιάζεται μια μελέτη περίπτωσης, στην οποία περιγράφονται οι αρχιτεκτονικές ανωνυμοποίησης και αναλύεται διεξοδικά το λογισμικό **"The Onion Routing" (TOR**). Αναλύουμε τη δυνατότητα ανωνυμίας στο διαδίκτυο μέσω του TOR, την εγκατάσταση, τη χρήση και την αρχιτεκτονική του και τα πλεονεκτήματα και μειονεκτήματα που παρουσιάζει.

Επίσης αναφερόμαστε στο επίπεδο ασφαλείας που προσφέρει ο συνδυασμός της εφαρμογής μέτρων ασφάλειας και ιδιωτικότητας και δρομολόγησης μέσω της εφαρμογής αυτής. Εξετάζεται η χρήση του TOR στον εντοπισμό του ηλεκτρονικού εγκλήματος και ο ρόλος της **ΕΛ.ΑΣ**.

Ακόμα κάνουμε χρήση και tutorial του Tor και του **Raspberry Pi3** και στην συνέχεια συνοψίζουμε προβλήματα που αντιμετωπίσαμε και φυσικά τον τρόπο επίλυσης τους.

Τέλος συνοψίζονται τα βασικά συμπεράσματα και τα ανοικτά προβλήματα που προκύπτουν από όλη την παρούσα διπλωματική εργασία.

Στόχο της διπλωματικής αυτής εργασίας αποτελεί η διερεύνηση των απόψεων των άμεσα εμπλεκόμενων υπηρετούντων στην ΕΛ.ΑΣ., ως προς τη χρήση του TOR στον εντοπισμό του ηλεκτρονικού εγκλήματος.

Thanks:

We would like to thank our rapporteur Professor mr. A.Fournari, who supervised us in our thesis and our families for their support.

Statutory Declaration:

We confirm that we are the writers of this thesis and that any assistance that we had to prepare, is fully recognized and refers to the thesis.

We also mention any sources from which we made use of data, ideas or words, whether relating directly or paraphrased.

Also certify that this thesis prepared by us personally especially for the requirements of the **Computer Engineering Department Antirrion curriculum** ***(former Department of Telecommunication Systems and Networks).***

Structure and objectives of the thesis:

Our dissertation consists of conceptual segments. Presented a case study, which describes the architectural anonymization and thoroughly analyzed in **"The Onion (software) Routing" (TOR).**

We analyze the possibility of anonymity on the Internet through the TOR, installation, use, and its architecture and its advantages and drawbacks.

Also refer to the level of security offered a combination of application security and privacy measures and routing through this application. Examines the use of TOR to identify cybercrime and the role of the **Police**.

Even we use tutorial and the Tor and **Raspberry Pi3** and then summarize the problems encountered and of course how they solved. Finally summarizes the main conclusions and open issues arising from throughout this dissertation.

Goal of this dissertation is to explore the views of those directly involved servicemen in Police, the use of TOR to identify cybercrime.

Περιεχόμενα

1. ΚΕΦΆΛΑΙΟ 1: Εισαγωγή

Από τους εκατομμύρια ανθρώπους που «σερφάρουν» καθημερινά από τον υπολογιστή ή την «έξυπνη» συσκευή τους, πολλοί ίσως δεν έχουν διανοηθεί πως, εκτός από το «ορατό» Ιντερνετ, υπάρχει κι ένα online «αόρατο» ιντερνετ απροσπέλαστο από τους συμβατικούς browser το οποίο έχει «βαφτισθεί» Σκοτεινό Διαδίκτυο (Darknet). Ενα όνομα που χρωστά στο γεγονός ότι παραμένει κρυμμένο από τις μηχανές αναζήτησης που «σαρώνουν» το web, όπως και από τις διωκτικές αρχές ή τις υπόλοιπες κρατικές υπηρεσίες ανά τον κόσμο. Το Darknet είναι ένα δίκτυο από σέρβερ, οι οποίοι βασίζονται σε τεχνολογίες κρυπτογράφησης για να ανταλλάσσουν δεδομένα.

Η πιο διαδεδομένη τεχνολογία γι' αυτό τον σκοπό είναι το Tor (The onion router) το οποίο έχουμε αναλάβει να αναπτύξουμε σε αυτήν τη διπλωματική εργασία.

Το Tor (συντομογραφία του The onion router) είναι ένα σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο Διαδίκτυο. Το λογισμικό πελάτη Tor δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου εθελοντικού δικτύου διακομιστών με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης από οποιονδήποτε διεξάγει διαδικτυακή παρακολούθηση ή ανάλυση της διαδικτυακής κίνησης. Η χρήση Tor κάνει δύσκολη την ανίχνευση διαδικτυακής δραστηριότητας του χρήστη όχι όμως αδύνατη, συμπεριλαμβανομένου επισκέψεων σε κάποια ιστοσελίδα, διαδικτυακές αναρτήσεις, προγράμματα άμεσων μηνυμάτων και άλλων μέσων διαδικτυακής επικοινωνίας, κι έχει σκοπό να προστατεύσει την ατομική ελευθερία, την ιδιωτικότητα και τη δυνατότητα του χρήστη να διεξάγει εμπιστευτικές εργασίες χωρίς να καταγράφονται οι διαδικτυακές δραστηριότητές του. Το "Onion routing" αναφέρεται στη στρωματοποιημένη φύση της υπηρεσίας κρυπτογράφησης: τα αρχικά δεδομένα κρυπτογραφούνται και επανακρυπτογραφούνται πολλές φορές, έπειτα στέλνονται μέσω διαδοχικών κόμβων του Tor, ο καθένας από τους οποίους αποκρυπτογραφεί ένα «στρώμα» κρυπτογράφησης προτού μεταφέρει τα δεδομένα στον επόμενο κόμβο και τελικά στον προορισμό τους. Αυτό μειώνει την πιθανότητα να αποκρυπτογραφηθούν ή να γίνουν κατανοητά κατά τη μεταφορά τους τα αρχικά δεδομένα. Το Tor είναι ελεύθερο λογισμικό πελάτη και η χρήση του είναι δωρεάν.

Αναλύοντας ιστορικά τα γεγονότα, αναπτύχθηκε από το Ερευνητικό Εργαστήριο του αμερικανικού πολεμικού ναυτικού, για την προστασία των στρατιωτικών επικοινωνιών. Χάρις στο Tor, ένα σάιτ μπορεί να αποκρύπτει τα ψηφιακά του ίχνη, «καμουφλάροντας» τον σέρβερ που το φιλοξενεί και κρυπτογραφώντας το εκάστοτε πακέτο το οποίο στέλνεται.

Μια άλφα έκδοση του λογισμικού με το δίκτυο δρομολογητών onion για να είναι «λειτουργικό

και αναπτυσσόμενο», ανακοινώθηκε στις 20 Σεπτεμβρίου του 2002. Ο Roger Dingledine, ο Nick Mathewson και ο Paul Syverson παρουσίασαν το "Tor: The Second-Generation Onion Router" στο 13ο συμπόσιο για την ασφάλεια USENIX στις 13 Αυγούστου 2004. Αν και το όνομα Tor προήρθε από το ακρωνύμιο του έργου The onion routing, το τρέχον έργο δε θεωρεί πλέον το όνομα ως ακρωνύμιο και γι' αυτό δεν γράφεται με κεφαλαία γράμματα .Χρηματοδοτούμενο αρχικά από το ερευνητικό εργαστήριο του ναυτικού των ΗΠΑ το Tor υποστηριζόταν οικονομικά από το Electronic Frontier Foundation την περίοδο μεταξύ 2004 και 2005.

Το λογισμικό Tor αναπτύσσεται πλέον από το Tor project, μία μη κυβερνητική οργάνωση που βρίσκεται στις ΗΠΑ από τον Δεκέμβριο του 2006και στηρίζεται σε διάφορες πηγές οικονομικής υποστήριξης. Τον Μάρτιο του 2011 το έργο Tor πήρε το βραβείο έργου κοινής ωφέλειας του Free Software foundation για το 2010 για τους εξής λόγους: « Χρησιμοποιώντας ελεύθερο λογισμικό, το Tor έδωσε τη δυνατότητα σε 36 εκατομμύρια ανθρώπους ανά τον κόσμο να απολαύσουν την ελευθερία πρόσβασης και έκφρασης στο Διαδίκτυο ενώ τους έδινε τον έλεγχο της ιδιωτικότητας και της ανωνυμίας τους. Το δίκτυο του αποδείχθηκε κρίσιμο σε αντικαθεστωτικά κινήματα στο Ιράν και πρόσφατα στην Αίγυπτο. Επίσης, μεγάλο ποσοστό των χρηστών προέρχεται από την Κίνα, όπου κυριαρχεί η λογοκρισία στο Διαδίκτυο.

Παράλληλα, η τεχνολογία εξασφαλίζει πως πρόσβαση στο Σκοτεινό Διαδίκτυο έχουν μόνον χρήστες που έχουν εγκαταστήσει το ανάλογο λογισμικό στο μηχάνημά τους. Λογισμικό που εγγυάται και τη δική τους ανωνυμία. Πάγια τακτική είναι οι αρχές να μην αποκαλύπτουν τι είδους ηλεκτρονικά «αντίμετρα» επιστρατεύουν, όμως οι αρχές εκμεταλλεύονται το γεγονός ότι τα εγκλήματα στον online κόσμο αφήνουν ίχνη και στον πραγματικό κόσμο. Η ΕΛ.ΑΣ στέλνει ένα ξεκάθαρο μήνυμα πως κανείς δεν μπορεί να ξεγλιστρήσει, επειδή χρησιμοποιεί το Tor.

Έπειτα, σε εργαλεία και υπηρεσίες που βασίζονται στο Tor βρίσκουν «καταφύγιο» απλοί χρήστες που θέλουν να παρακάμψουν τα «φίλτρα» ιντερνετικής λογοκρισίας στη χώρα τους και, όπως είναι φυσικό, πολιτικοί ακτιβιστές. Ετσι, σύμφωνα με την ιστοσελίδα του The Tor Project, το Darknet κατακλύσθηκε από μπλογκ κατά τη διάρκεια της «Αραβικής Ανοιξης», από ανθρώπους που συμμετείχαν στις εξεγέρσεις και ήθελαν να μεταφέρουν στο εξωτερικό τη μαρτυρία τους. Δυνατότητες που, όπως σημειώνει ο συντάκτης του PC World, δεν θα μπορούσαν να γίνουν πραγματικότητα, αν το Σκοτεινό Διαδίκτυο δεν προσέφερε ένα επίπεδο ασφάλειας το οποίο δυστυχώς το κάνει ελκυστικό και σε εγκληματίες. Έχει υπάρξει πολλή συζήτηση ως προς το κατά πόσο το Tor μπορεί να κρατήσει τις online δραστηριότητές σας ανώνυμες. Έχουμε ήδη δει πώς σελίδες του Tor που πουλούσαν ναρκωτικά έκλεισαν από τις αρχές ή πως το FBI εμπόδισε την κακοποίηση παιδιών μέσω παρόμοιων ιστοσελίδων του DARKNET. Η προσπάθεια όμως που απαιτείται από τους φορείς επιβολής του νόμου να παρακολουθήσουν χρήστες του Tor είναι πάρα πολύ δύσκολη έως και ανέφικτη. Βεβαίως, το Tor έχει και ηθική χρήση, επιτρέπει την ελευθερία του λόγου σε αυτούς που ζουν κάτω από καταπιεστικά καθεστώτα και προστατεύει τους ακτιβιστές των ανθρωπίνων δικαιωμάτων από την ποινική δίωξη.

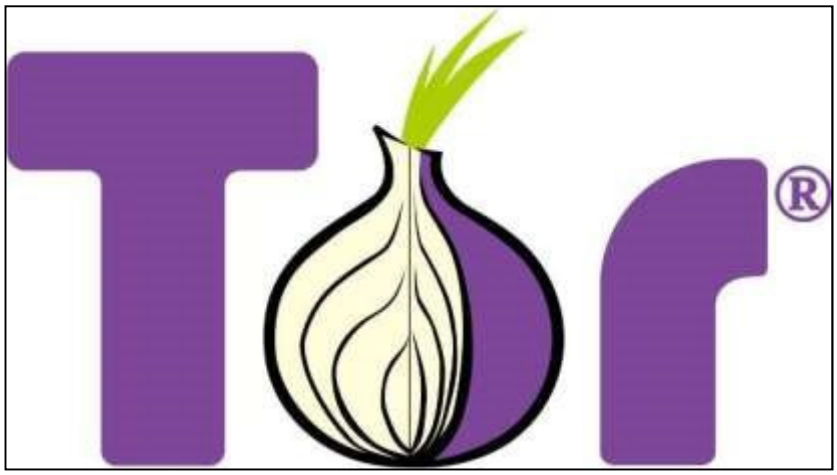
Υπάρχουν βέβαια αντίστοιχες τεχνολογίες Ανωνυμοποίησης και Ενίσχυσης της Ιδιωτικότητας σαν το TOR . Μερικές από αυτές ,ονομαστικά, είναι:

- Freenet
- l2p
- Hordes
- Crowds
- Gap
- Anonymizer
- Onion routing
- LPWA
- P3P
- TRUSTe

2. ΚΕΦΑΚΑΙΟ 2: Το λογισμικό TOR

Η δυνατότητα ανωνυμίας στο διαδίκτυο μέσω TOR

Υπάρχουν αρκετές περιπτώσεις που είναι επιθυμητή η ανώνυμη περιήγηση στο διαδίκτυο, που υποστηρίζουν ήδη οι browsers με τα Private Browsing, InPrivate Browsing και Incognito. Αυτός ο τρόπος λειτουργίας των browsers δεν καλύπτει την ανωνυμία στο δίκτυο αλλά την ανωνυμία στον Η/Υ που χρησιμοποιείται. Στο συγκεκριμένο κεφαλαίο θα ασχοληθούμε αναλυτικά με τη περίπτωση του λογισμικού The Onion Routing (TOR) (Εικόνα 4, Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

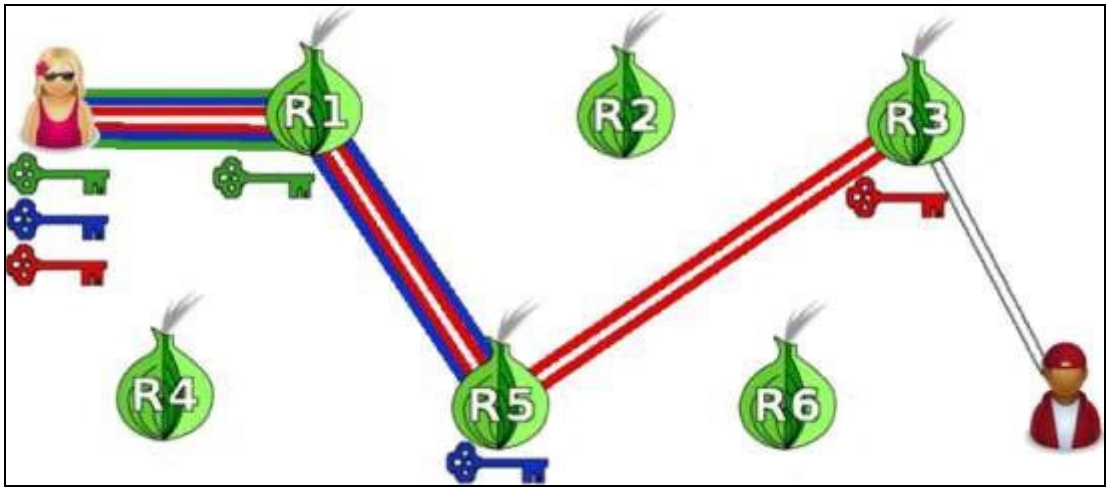


Εικόνα 1: Google Σήμα του TOR

Εικόνα 3. Το λογότυπο TOR.

Το TOR αποτελεί ένα κατανεμημένο σύστημα, που είναι ελεύθερο στον πελάτη και η χρήση του είναι δωρεάν. Έχει σχεδιαστεί ώστε να προσφέρει ανωνυμία σε εφαρμογές που βασίζονται σε συνδέσεις TCP, όπως η περιήγηση στο διαδίκτυο, η σύνδεση secure shell και το instant messaging. Εναλλακτικά, το TOR αποτελεί μια γενικού σκοπού υποδομή για ιδιωτικές συνδέσεις σε ένα δημόσιο δίκτυο μεταφοράς δεδομένων. Παρέχει ανώνυμες συνδέσεις χρησιμοποιώντας διαφορετικά επίπεδα κρυπτογράφησης που είναι ιδιαίτερα ανθεκτικά σε επιθέσεις τύπου ωτακουστών και ανάλυσης κίνησης. Οι συνδέσεις είναι κατευθυντήριες, σχεδόν στου πραγματικού χρόνου και μπορούν να χρησιμοποιηθούν είτε για κινήσεις προσανατολισμένες σε σύνδεση, είτε για κινήσεις άνευ εγκατάστασης σύνδεσης (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

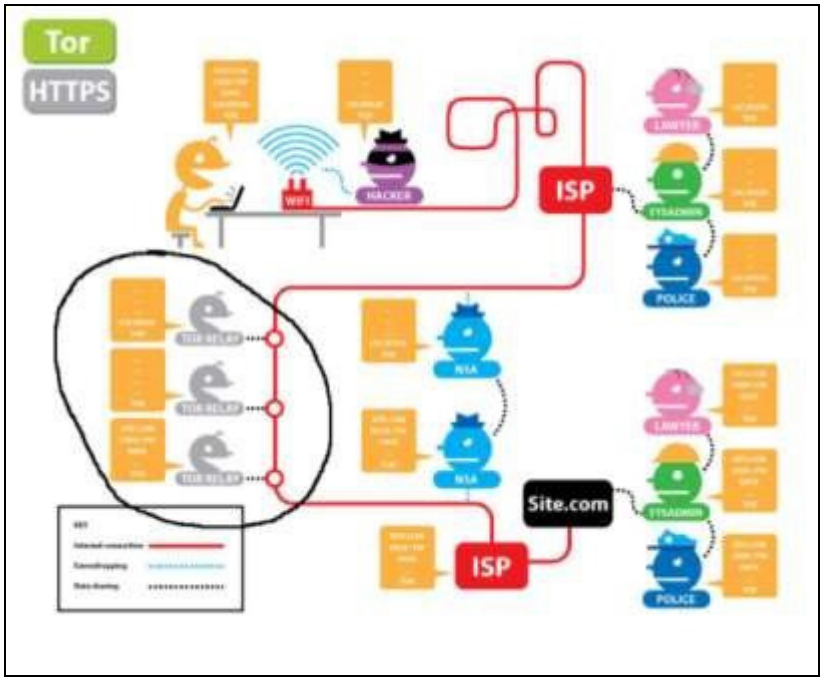
Ο μηχανισμός αυτός προστατεύει από επιθέσεις μέσω ενός δικτύου ανώνυμων server -που κρυπτογραφούν τα δεδομένα και αυξάνουν το βαθμό της ανωνυμίας στο Internet. Ξεκίνησε από το U.S. Naval Research Laboratory και υποστηρίζεται από το Electronic Frontier Foundation που μάχεται χρόνια τώρα για τα δικαιώματα των χρηστών. Λειτουργεί δε σε επίπεδο στρατολόγησης (routing), αφού ο client διαλέγει μια διαδρομή μέσα στο δίκτυο και δομεί ένα κύκλωμα, στο οποίο κάθε κόμβος γνωρίζει τον προηγούμενο και τον επόμενο, αλλά κανέναν άλλο. Πρόκειται για ένα λογισμικό σχεδιασμένο ώστε να εμποδίζει την ανάλυση κίνησης, μέσω ενός δικτύου υπολογιστών που χρησιμοποιούν κρυπτογράφηση, όπου η πρόσβαση γίνεται μέσω διακομιστών (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).



Εικόνα 2: Η αρχιτεκτονικη του TOR

Το TOR δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου εθελοντικού δικτύου διακομιστών με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης από οποιονδήποτε διεξάγει διαδικτυακή παρακολούθηση ή ανάλυση της διαδικτυακής κίνησης. Η χρήση του TOR δυσκολεύει την ανίχνευση διαδικτυακής δραστηριότητας του χρήστη, συμπεριλαμβανομένου επισκέψεων σε κάποια ιστοσελίδα, διαδικτυακές αναρτήσεις, προγράμματα άμεσων μηνυμάτων και άλλων μέσων διαδικτυακής επικοινωνίας, κι έχει σκοπό να προστατεύσει την ατομική ελευθερία, την ιδιωτικότητα και τη δυνατότητα του χρήστη να διεξάγει εμπιστευτικές εργασίες χωρίς να καταγράφονται οι διαδικτυακές δραστηριότητές του. Χρησιμοποιεί δε, στρωματοποιημένη κρυπτογράφηση, όπου τα αρχικά δεδομένα κρυπτογραφούνται και επανακρυπτογραφούνται πολλές φορές, έπειτα στέλνονται μέσω διαδοχικών κόμβων του TOR, ο καθένας από τους οποίους αποκρυπτογραφεί ένα στρώμα κρυπτογράφησης πριν μεταφέρει τα δεδομένα στον επόμενο κόμβο και τελικά στον προορισμό τους. Αυτό μειώνει την πιθανότητα, τα αρχικά δεδομένα, να αποκρυπτογραφηθούν ή να γίνουν κατανοητά κατά τη μεταφορά τους (Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008).

Η εφαρμογή δημιουργεί μια σύνδεση (socket) σε μια εφαρμογή proxy, που αποτελεί το σημείο εισόδου στο TOR. Ο proxy μετατρέπει το μήνυμα σύνδεσης σε μια μορφή, που να μπορεί να μεταφέρεται μέσω του διαδικτύου και εν συνέχεια συνδέεται με έναν TOR proxy που ορίζει τη διαδρομή που θα ακολουθηθεί δημιουργώντας ένα πολυστρωματικό δίκτυο δεδομένων μέσω μιας σειράς onion δρομολογητών. Κατά τη διάρκεια μετάδοσης διαμέσω της ανώνυμης σύνδεσης, ο κάθε δρομολογητής αποκωδικοποιεί το μήνυμα που προορίζεται γι αυτόν, ενώ ο τελευταίος δρομολογητής οδηγεί το πακέτο προς την έξοδο της διαδρομής και στον παραλήπτη. Στην περίπτωση απάντησης από τον παραλήπτη, ο τελευταίος δρομολογητής παραλαμβάνει το μήνυμα, το κρυπτογραφεί και το στέλνει πίσω από την ίδια διαδρομή. Μόλις το πακέτο φτάσει στον onion proxy αποκρυπτογραφείται (Dingledine et al., 2004; Jones, 2005).



Εικόνα 3: Η αρχιτεκτονικη του TOR

Πρόκειται για ένα πρόγραμμα ασφαλούς περιήγησης, που χρησιμοποιείται ευρέως για περιήγηση στο Darknet, που ανακατεύει τις IP του παγκόσμιου δικτύου των χρηστών του. Καθιστά την περιήγηση πιο ελεύθερη, αφού σαν IP -που είναι και το στοιχείο που προδίδει τη γεωγραφική θέση του περιηγητή- εμφανίζεται μια άλλη από ένα άλλο τυχαίο μέρος του πλανήτη. Εξαιτίας του TOR-proxy, μια ιστοσελίδα μπορεί να αποκρύπτει τα ψηφιακά της ίχνη, καμουφλάροντας τον server που το φιλοξενεί. Παράλληλα, η τεχνολογία TOR εξασφαλίζει πως πρόσβαση στο Darknet έχουν μόνον χρήστες που το έχουν εγκαταστήσει το οποίο εγγυάται και τη δική τους ανωνυμία. Το λογισμικό του χρήστη, διαπραγματεύεται ένα ξεχωριστό σετ κλειδιών κρυπτογράφησης για κάθε βήμα στο κύκλωμα που επέλεξε, για να διασφαλίζει ότι κάθε κόμβος δεν θα μπορεί να ανιχνεύσει την κίνηση την οποία δρομολογεί (Le Blond et al., 2011; Muller et al., 2012).

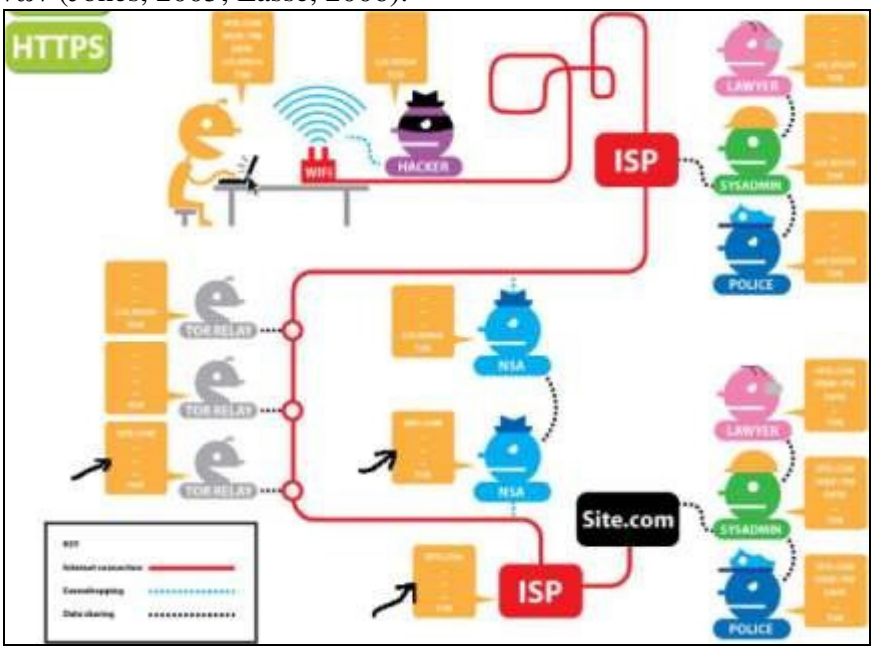
Το TOR ως εφαρμογή προστατεύει από το είδος διαδικτυακής παρακολούθησης, που είναι γνωστό ως traffic analysis. Κατά την traffic analysis τα πακέτα δεδομένων που μεταφέρονται στο διαδίκτυο αποτελούνται από δύο τμήματα. Αυτό συμβαίνει αφού το TOR προσομοιάζει με ένα δίκτυο από εικονικά τούνελ που δίνει τη δυνατότητα βελτίωσης της ασφάλειαςπροστασίας της ιδιωτικότητας στο διαδίκτυο (Εικόνες 3, 4, 5, 6, 7, 8 και 9). Παρέχει δε τη βάση για ένα ευρύ φάσμα εφαρμογών που επιτρέπουν σε οργανισμούς ή άτομα να μοιράζονται πληροφορίες μέσω δημοσίων δικτύων χωρίς να διακυβεύεται η ιδιωτικότητά τους. (Soghoian, 2007; Jacobson, 2008):

(i). Το φορτίο των δεδομένων (data payload), και

(ii). Την κεφαλίδα (header) που χρησιμοποιείται για την δρομολόγηση.

Ως συνέπεια, το βασικό πρόβλημα για την προστασία της ιδιωτικότητας εστιάζεται στο γεγονός ότι ο παραλήπτης -όπως επίσης και ο πάροχος των υπηρεσιών διαδικτύου ή και μη εξουσιοδοτημένα τρίτα πρόσωπα- μπορεί να καταλάβει το είδος των απεσταλμένων δεδομένων βάσει των επικεφαλίδων. Συμβαίνει ο οποιοδήποτε, πολύ συχνά, να έχει την ευχέρεια να εισέρθει ανάμεσα στον αποστολέα και τον παραλήπτη και να παρακολουθεί απλώς τις κεφαλίδες. Παρατηρούνται και περισσότερο εξελιγμένες μορφές ανάλυσης κίνησης, όπου ο επιτιθέμενος χρησιμοποιεί στατιστικές μεθόδους για να εντοπίσει τα πρότυπα επικοινωνίας- patterns.

Η κρυπτογράφηση, δυστυχώς, στις προαναφερόμενες περιπτώσεις δεν μπορεί να συμβάλλει στην προστασία, αφού αποκρύπτει μόνο το περιεχόμενο της επικοινωνίας αλλά όχι τις κεφαλίδες. Το TOR μειώνει τους κινδύνους -στις περιπτώσεις ανάλυσης κίνησης που προαναφέρθηκαν- αφού ανακατανέμει τις διόδους επικοινωνίας σε διάφορα ασύνδετα σημεία του διαδικτύου. Έτσι κανένα μεμονωμένο σημείο δεν μπορεί να συνδεθεί η προέλευση με τον προορισμό. Η δημιουργία ενός ιδιωτικού μονοπατιού από το TOR, γίνεται από το λογισμικό του χρήστη που δομεί σταδιακά ένα κύκλωμα κρυπτογραφημένων συνδέσεων μέσω μεταβιβαστών-relays στο δίκτυο, όπου το κύκλωμα επεκτείνεται έναν κόμβο ανά περίπτωση και ο κάθε μεταβιβαστής γνωρίζει μόνο τον προηγούμενο και τον επόμενο από αυτόν. Ως αποτέλεσμα κανένας μεταβιβαστής δεν γνωρίζει την πλήρη διαδρομή που θα ακολουθήσει το πακέτο δεδομένων (Jones, 2005; Lasse, 2006).



Εικόνα 4: Η αρχιτεκτονικη του TOR

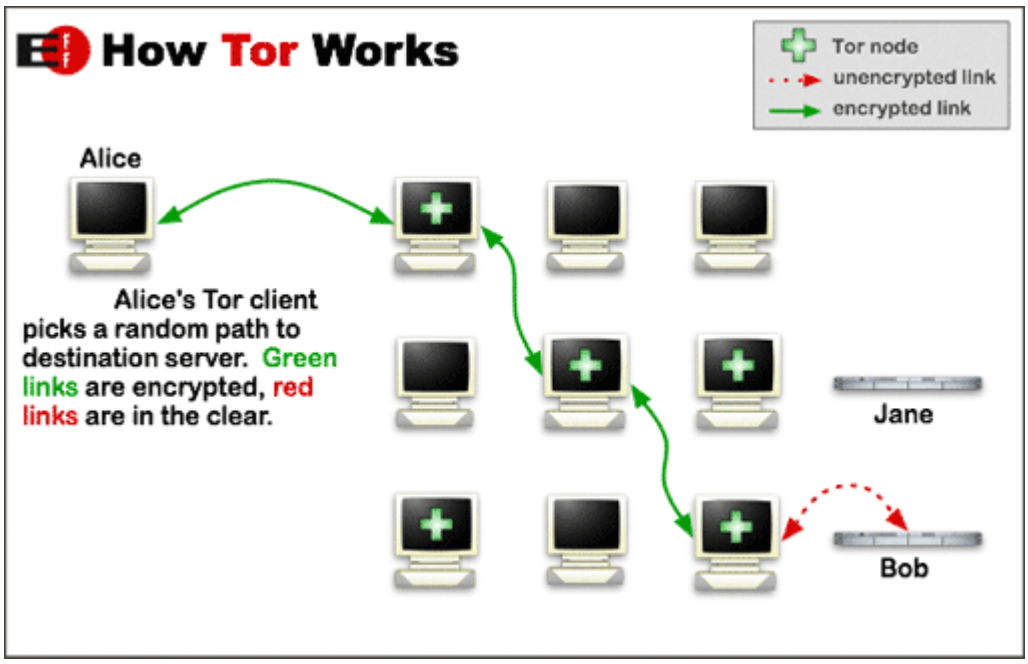
Ο χρήστης απ' τη μεριά του διαπραγματεύεται κάθε φορά με κάθε κόμβο ένα διαφορετικό σύνολο κλειδιών κρυπτογράφησης ώστε να εξασφαλίσει ότι κανένας κόμβος δεν θα μπορέσει να εντοπίσει τις κρυπτογραφημένες αυτές συνδέσεις. Μόλις ένα κύκλωμα εγκατασταθεί μπορεί να γίνει ανταλλαγή πολλών ειδών δεδομένων, καθώς και ανάπτυξη πολλών ειδών εφαρμογών λογισμικού. Επειδή κάθε μεταβιβαστής δεν μπορεί να αναγνωρίσει πάνω από έναν κόμβο στο κύκλωμα, γεγονός που διασφαλίζει ότι κανένας επιτιθέμενος αλλά ούτε και μεταβιβαστής -που έχει παραβιαστεί- μπορεί να χρησιμοποιήσει τις αναλύσεις κίνησης για να συνδέσουν την πηγή με τον προορισμό. Για μεγιστοποίηση της αποτελεσματικότητας, το TOR χρησιμοποιεί το ίδιο κύκλωμα που δημιουργήθηκε τα τελευταία δέκα λεπτά, δηλαδή αιτήσεις που θα γίνουν σε μεταγενέστερα θα δημιουργήσουν ένα καινούργιο κύκλωμα προκειμένου να αποτρέψουν τη σύνδεση των προηγούμενων ενεργειών μας με τις καινούργιες (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Η διαφορά, λοιπόν, του TOR από τα προαναφερόμενα λογισμικά είναι (π.χ., Crow, Hordes, Freedom, παράγραφοι 7.1 ως 7.3) ότι ένας κοινός proxy τοποθετεί έναν server κάπου στο διαδίκτυο και επιτρέπει να τον χρησιμοποιήσουμε για να ελέγχει κινήσεις. Αυτό δημιουργεί μια απλή και εύκολη αρχιτεκτονική, αφού όλοι οι χρήστες εισέρχονται και αποχωρούν μέσω του ίδιου server. Ο provider μπορεί να προχωρήσει σε χρεώσεις για τη χρήση του proxy ή να χρηματοδοτεί το κόστος του μέσω διαφημίσεων στο server. Ο provider γνωρίζει ποιος είσαι και πού περιηγείσαι στο διαδίκτυο. Ο TOR περνάει την κίνηση μέσα από τουλάχιστον τρεις servers πριν τη στείλει στον προορισμό της.

Επειδή υπάρχει ένα διαφορετικό επίπεδο κρυπτογράφησης για κάθε έναν από τους τρεις μεταβιβαστές, ο TOR ούτε τροποποιεί, και ίσως ούτε γνωρίζει το είδος του απεσταλμένου μηνύματος (Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Με λιγότερα λόγια, στόχος του Tor είναι να αποκρύπτει τις ταυτότητες των χρηστών του και την δραστηριότητα τους στο δίκτυο αποτρέποντας την παρακολούθηση και την ανάλυση της κίνησης και διαχωρίζοντας τον εντοπισμό από την δρομολόγηση. Αποτελεί την υλοποίηση του onion routing, το οποίο κρυπτογραφεί και δρομολογεί τυχαία την επικοινωνία μέσω ενός δικτύου από κόμβους που το λειτουργούν εθελοντές ανά την υφήλιο. Οι συγκεκριμένοι δρομολογητές onion (κρεμμύδι) εφαρμόζουν κρυπτογράφηση πολλαπλών στρωμάτων (εξ ου και η μεταφορά του κρεμμυδιού) για να εξασφαλίσουν τέλεια μυστικότητα προς τα εμπρός (perfect forward secrecy) μεταξύ των κόμβων, και γι'αυτό προσφέρει ανωνυμία της δικτυακής τοποθεσίας. Αυτή η ανωνυμία επεκτείνεται στην φιλοξενία ανθεκτικού στην λογοκρισία περιεχομένου μέσω των ανώνυμων κρυμμένων υπηρεσιών του Tor[3]. Επιπλέον , διατηρώντας κάποιους από τους κόμβους εισόδου (γεφυρωμένους κόμβους) μυστικούς, οι χρήστες αποφεύγουν την διαδικτυακή λογοκρισία η οποία στηρίζεται στο μπλοκάρισμα των δημόσιων κόμβων του Tor[8].

Η διαδικτυακή διεύθυνση του αποστολέα και του παραλήπτη δεν είναι αμφότερες σε μορφή αρχικού κειμένου (cleartext) σε κάθε πέρασμα κατά μήκος της διαδρομής προς έναν κόμβο, ο οποίος δεν είναι εξόδου (ή ενδιάμεσος) , ούτε κομμάτια της πληροφορίας είναι σε μορφή μη κρυπτογραφημένου κειμένου, έτσι ώστε οποιοσδήποτε ωτακουστής σε οποιαδήποτε σημείο κατά μήκος του καναλιού επικοινωνίας δεν μπορεί άμεσα να ταυτοποιήσει και τα δύο άκρα. Επιπλέον , στον παραλήπτη φαίνεται ότι ο τελευταίος κόμβος Tor (κόμβος εξόδου) είναι ο δημιουργός της επικοινωνίας.



Εικόνα 5: Πως λειτουργεί το TOR

Το Tor μπορεί επίσης να προσφέρει ανωνυμοποίηση στους διακομιστές στη μορφή της υπηρεσίας απόκρυψης τοποθεσίας, η οποία αποτελείται από πελάτες του Tor ή κόμβους που τρέχουν ειδικά διαμορφωμένο λογισμικό διακομιστών. Αντί να αποκαλύπτουν τη διεύθυνση IP των διακομιστών(και άρα τη διαδικτυακή τοποθεσία τους) οι κρυμμένες υπηρεσίες είναι προσβάσιμες μέσω Tor-specific .onion pseudo top-level domain (TLD), ή αλλιώς pseudomain.

Το δίκτυο Tor αντιλαμβάνεται το TLD και δρομολογεί δεδομένα από και προς τις κρυμμένες υπηρεσίες ανώνυμα. Εξαιτίας της έλλειψης εμπιστοσύνης σε μια δημόσια διευθύνση, οι κρυμμένες υπηρεσίες μπορούν να φιλοξενηθουν πίσω από αναχώματα ασφαλείας ή μεταφραστές δικτυακών διευθύνσεων (network address translators, NAT) . Ένας πελάτης Tor είναι απαραίτητος για την πρόσβαση σε μια κρυμμένη υπηρεσία.

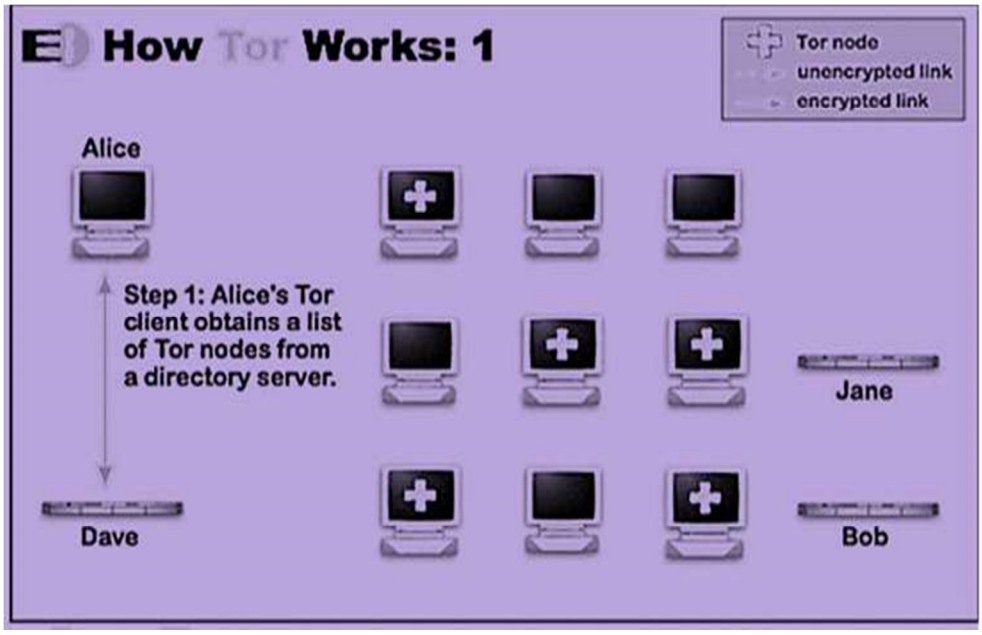
Οι κρυμμένες υπηρεσίες έχουν αναπτυχθεί στο δίκτυο Tor από τις αρχές του 2004 Εκτός από τη βάση δεδομένων που αποθηκεύει τις εγγραφές στις κρυμμένες υπηρεσίες, το Tor είναι αποκεντρωμένο με βάση τον σχεδιασμό του. Δεν υπάρχει δηλαδή άμεσα αναγνώσιμη λίστα των κρυμμένων υπηρεσιών. Υπάρχει ένας αριθμός ανεξάρτητων κρυμμένων υπηρεσιών που εξυπηρετούν αυτό το σκοπό.

Επειδή οι υπηρεσίες απόκρυψης τοποθεσίας δεν χρησιμοποιούν κόμβους εξόδου, δεν υπόκεινται σε ωτακουστές των κόμβων αυτών. Υπάρχει παρ'όλα αυτά ένας αριθμός ζητημάτων ασφαλείας που περιλαμβάνονται στις κρυμμένες υπηρεσίες. Για παράδειγμα, υπηρεσίες που είναι προσβάσιμες μέσω των κρυμμένων υπηρεσιών του Tor και του δημόσιου διαδικτύου είναι επιρρεπείς σε επιθέσεις συσχετισμού (correlation attacks) κι επομένως όχι εντελώς κρυμμένες. Άλλες παγίδες περιλαμβάνουν κακοδιαμορφωμένες υπηρεσίες (π.χ. την αναγνώριση πληροφοριών που εμπεριέχονται προεπιλεγμένα σε μηνύματα σφάλματος των δικτυακών διακομιστών), στατιστικές χρόνου λειτουργίας και χρόνου μη λειτουργίας, επιθέσεις παρεμβολής και σφάλματα του χρήστη.

2.1. Η αρχιτεκτονική του TOR

Το TOR βασίζεται σχεδιαστικά στην ιδέα της ανάμιξης των συνδέσεων των χρηστών και των εφαρμογών, ώστε να επιτευχθεί η απόκρυψη της ταυτότητας του χρήστη σε μία επικοινωνία μέσω ενός δημόσιου δικτύου. Έτσι τελικά είναι δύσκολο να διακριθεί μια συγκεκριμένη σύνδεση. Αποτρέπει εκείνους που έχουν πρόσβαση στο μέσο μετάδοσης να αναγνωρίσουν τις οντότητες που συμμετέχουν σε μια επικοινωνία, επιτρέποντάς τους μόνο να διαπιστώσουν απλώς αν διεξάγεται ή όχι. Παρέχει ανώνυμες συνδέσεις ανθεκτικές στην παρακολούθηση περιεχομένου της επικοινωνίας, αλλά και στην ανάλυση της κίνησης της πληροφορίας (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012). Το TOR αποτελείται από δύο κύρια μέρη:

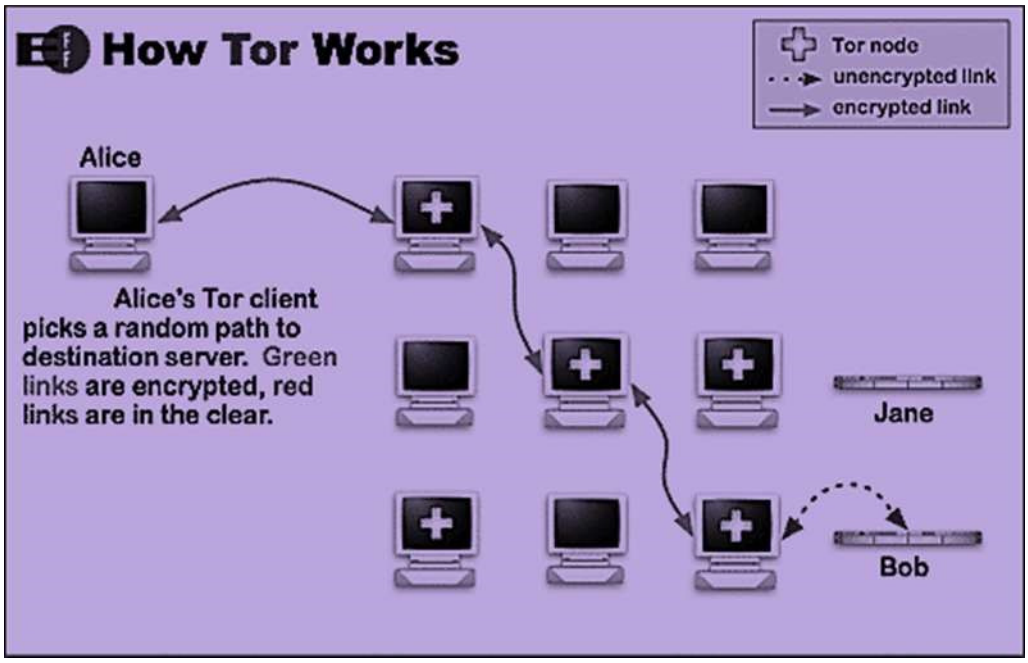
- Τη δικτυακή υποδομή που εξυπηρετεί τις ανώνυμες συνδέσεις και περιλαμβάνει τους δρομολογητές,
- Τους πληρεξούσιους που μεσολαβούν στις εφαρμογές του χρήστη και στις συνδέσεις στο διαδίκτυο.



Εικόνα 6: Η αρχιτεκτονική της εξυπηρετησης του TOR

Οι TOR δρομολογητές συνδέονται στο δημόσιο δίκτυο, αλλά έχουν αποκαταστήσει μια και μοναδική σύνδεση με καθένα από τους γειτονικούς τους δρομολογητές τους και μόνον έτσι μπορούν να επικοινωνούν. Κάθε δρομολογητής γνωρίζει την ταυτότητα και τα δημόσια κλειδιά των υπόλοιπων δρομολογητών. Ο TOR πληρεξούσιος που βρίσκεται στην πλευρά του αποστολέα, επιλέγει ένα μονοπάτι από το οποίο θα φτάσει στον παραλήπτη. Κατά μήκος του μονοπατιού υπάρχουν και άλλοι δρομολογητές. Σκοπός των πληρεξούσιων είναι να μεταφράζουν τα δεδομένα σε μορφή ανεξάρτητη της εκάστοτε εφαρμογής, η οποία θα γίνεται αποδεκτή και κατανοητή από το δίκτυο των δρομολογητών TOR. Για κάθε δρομολογητή, στο μονοπάτι που επιλέχτηκε, δημιουργείται ένα επίπεδο με ένα πακέτο που περιλαμβάνει την IP διεύθυνση του επόμενου δρομολογητή και τις πληροφορίες που απαιτούνται για τη δημιουργία του κλειδιού κρυπτογράφησης. Τα πακέτα αυτά, αντί να μεταφέρουν πληροφορίες για την πηγή και τον προορισμό τους, περιέχουν τις πληροφορίες μόνο για τον προηγούμενο και τον επόμενο σταθμό. Επομένως, στον αμέσως επόμενο από το χρήστη δρομολογητή δημιουργείται ένα το μονοπάτι της πλοήγησης και σύνδεσης στο διαδίκτυο (Εικόνες 3 ως 9) (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Οι πληρεξούσιοι λειτουργούν παράλληλα και ως μεσάζοντες δρομολογητές TOR για άλλες ανώνυμες συνδέσεις, ώστε να μην μπορούν να συναχθούν συμπεράσματα που αφορούν στην κίνηση των δεδομένων από και προς αυτούς. Οι χρήστες πρέπει να προσπελάσουν πρώτα κάποιον πληρεξούσιο, ο οποίος μπορεί να ανήκει στον ISP τους, σε κάποιον τρίτο ή ακόμη και να εκτελείται στον ίδιο τον υπολογιστή τους. Στην περίπτωση που ο πληρεξούσιος αυτός δεν εκτελείται τοπικά και η σύνδεση είναι κρυπτογραφημένη, δε χρειάζεται εγκατάσταση λογισμικού και το υπολογιστικό κόστος είναι μηδενικό για το χρήστη. Σε περίπτωση που όλες οι λειτουργίες διεξάγονται στον Η/Υ του, του παρέχεται η μεγαλύτερη προστασία για την ανωνυμία και ιδιωτικότητα, ακόμη και από αυτούς που συμμετέχουν στη σύνδεση (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).



Εικόνα 7: Η αρχιτεκτονικη της εξυπηρετησης του TOR

Ένας TOR πληρεξούσιος δημιουργεί και διαχειρίζεται τις ανώνυμες συνδέσεις και επομένως είναι το πιο έμπιστο συστατικό τμήμα του συστήματος. Αποτελεί ουσιαστικά μια διεπαφή μεταξύ των εφαρμογών και του δικτύου, όπου οι συνδέσεις μπορεί να γίνονται με sockets, αλλά αντικαθιστούν τις κλασικές TCP/IP συνδέσεις. Ένας πληρεξούσιος αποτελείται από τρία επίπεδα (Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012):

(i). Ένα μη απαραίτητο φίλτρο, εξειδικευμένο σε εφαρμογές, που ελέγχει και διαμορφώνει κατάλληλα τις ροές των δεδομένων,

(ii). Ένα φίλτρο, εξειδικευμένο για εφαρμογές πληρεξούσιου, το οποίο μεταφράζει τις ροές των δεδομένων σε μορφή ανεξάρτητη από την εκάστοτε εφαρμογή η οποία είναι αποδεκτή από το δίκτυο του TOR,

(iii). Έναν πληρεξούσιο, ο οποίος οικοδομεί και διευθύνει ανώνυμες συνδέσεις και αποτελεί το πιο αξιόπιστο τμήμα του συστήματος.

Για τον καθορισμό των διαδρομών, πρέπει ο TOR πληρεξούσιος να γνωρίζει την τοπολογία του δικτύου και την κατάσταση της διασυνδεσιμότητάς του. Ακόμη, είναι αναγκαίο να γνωρίζει τα δημόσια πιστοποιητικά, καθώς και υπό ποιες συνθήκες μπορεί και πώς θα διαχειρισθεί μια έξοδο κόμβου από το διαδίκτυο.

Αυτές οι πληροφορίες διοχετεύονται κατάλληλα και με ασφάλεια στο διαδίκτυο αυτόματα, καθώς εισέρχονται νέοι κόμβοι ή προκύπτει κάποια αλλαγή.

Προκειμένου να χρησιμοποιηθεί η υποδομή των TOR δρομολογητών, αρκεί οι δικτυακές εφαρμογές του χρήστη να υποστηρίζουν πληρεξούσιους.
Οι συνδέσεις που δημιουργούνται είναι:

- Socket σύνδεση μεταξύ αποστολέα και TOR πληρεξούσιου,
- Ανώνυμη σύνδεση μεταξύ TOR πληρεξούσιου αποστολέα και παραλήπτη,
- Socket σύνδεση μεταξύ TOR πληρεξούσιου στην πλευρά του παραλήπτη και του ίδιου του παραλήπτη.

Οι συνδέσεις είναι αμφίδρομες, τείνουν να είναι πραγματικού χρόνου και μπορούν να χρησιμοποιηθούν τόσο για τη διακίνηση πληροφορίας που είναι βασισμένη σε συνδέσεις όσο και για τη διακίνηση πληροφορίας που δε βασίζεται σε συνδέσεις. Το TOR είναι εύκολο να ενταχθεί στα υπάρχοντα συστήματα, καθώς λειτουργεί μέσω εξειδικευμένων πληρεξούσιων. Εφαρμογές που επικοινωνούν με sockets και πληρεξούσιους είναι οι φυλλομετρητές (HTTP), οι εφαρμογές ηλεκτρονικού ταχυδρομείου (SMTP), απομακρυσμένης πρόσβασης (RLOGIN), μεταφοράς αρχείων (FTP), IRC clients, Telnet, Finger, WhoIs και Raw Sockets. Επιπλέον, ολοκληρώθηκαν ή βρίσκονται στη φάση ολοκλήρωσης πληρεξούσιοι για NNTP, DNS, NFS, IRC, HTTPS, SSH αλλά και Virtual Private Networks (VPNs) (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Η λειτουργία του TOR συνίσταται στη δυναμική οικοδόμηση των ανώνυμων συνδέσεων μέσα σε ένα δίκτυο πραγματικού χρόνου (Chaum mixes). Αυτά τα mixes αποδέχονται σταθερού μεγέθους μηνύματα από ποικίλες πηγές, τα κρυπτογραφούν και στη συνέχεια τα προωθούν στον επόμενο προορισμό με τυχαία σειρά. Με τη δρομολόγηση μέσα από πολυάριθμα mixes στο διαδίκτυο είναι δύσκολο να διευκρινισθεί ποιος επικοινωνεί με ποιόν. Το δίκτυο του TOR είναι κατανεμημένο και παρουσιάζει ανοχή σε σφάλματα, ενώ βρίσκεται υπό τον έλεγχο πολλαπλών διαχειριστικών τμημάτων (domains). Με αυτό τον τρόπο, ένας μόνο δρομολογητής δεν είναι δυνατό να καταρρίψει το δίκτυο, ούτε μπορεί να παραβιάσει την ανωνυμία ενός χρήστη. Οι συνδέσεις του TOR είναι ανεξάρτητες από το πρωτόκολλο που θα χρησιμοποιηθεί, ενώ περιλαμβάνουν τρεις φάσεις: τη διαδικασία ρύθμισης της σύνδεσης, τη διακίνηση των δεδομένων και τη διαδικασία τερματισμού της σύνδεσης (Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

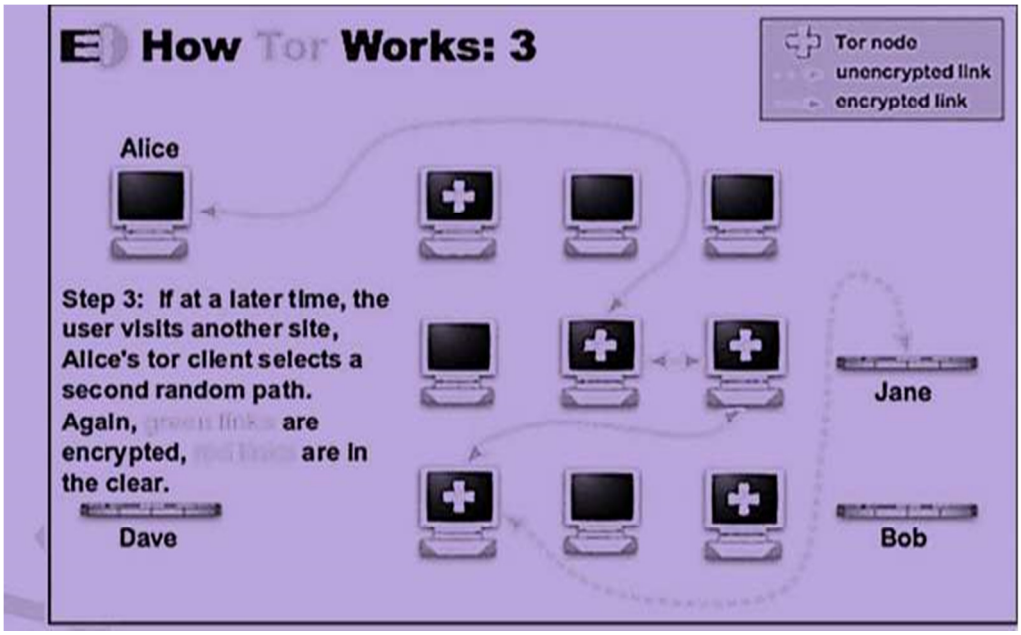
Η πρώτη φάση ξεκινά όταν ο χρήστης δημιουργήσει ένα TOR και τότε καθορίζεται το μονοπάτι του δικτύου που θα ακολουθήσει η σύνδεση. Αποτελεί μια δομή δεδομένων που αποτελείται από στρώματα και καθορίζει τις ιδιότητες της σύνδεσης, όπως τις πληροφορίες κρυπτογραφικού ελέγχου δηλαδή τους συμμετρικούς κρυπτογραφικούς αλγόριθμους και τα μυστικά κλειδιά που θα χρησιμοποιηθούν κατά τη διάρκεια διακίνησης των δεδομένων. Κάθε δρομολογητής TOR στο μονοπάτι χρησιμοποιεί το δημόσιο κλειδί του για να αποκρυπτογραφήσει ολόκληρο το TOR που παραλαμβάνει. Αυτή η διαδικασία εκθέτει τις πληροφορίες ελέγχου της κρυπτογράφησης, την ταυτότητα του επόμενου δρομολογητή TOR και το συνημμένο TOR. Εάν χρειαστεί, ο δρομολογητής TOR συμπληρώνει με στοιχεία το συνημμένο TOR και το στέλνει στον επόμενο δρομολογητή (Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Αφού πραγματοποιηθεί η σύνδεση, τα δεδομένα μπορούν να σταλούν και προς τις δύο κατευθύνσεις. Επαναλαμβανόμενα δεδομένα από τον ιδρυτή της σύνδεσης κρυπτογραφούνται με διάφορους αλγόριθμους και τα κλειδιά καθορίζονται μέσα στο Onion. Καθώς προχωρούν τα δεδομένα στην ανώνυμη σύνδεση, κάθε δρομολογητής του Onion αφαιρεί ένα επίπεδο κρυπτογράφησης και αποκαλύπτει τον επόμενο δρομολογητή, ενώ τελικά το μήνυμα φτάνει στον παραλήπτη σε αποκρυπτογραφημένη μορφή.

Εάν ακολουθηθεί η αντίστροφη πορεία, η διαστρωμάτωση αυτή ακολουθείται στην αντίστροφη σειρά με διαφορετικούς αλγόριθμους και κλειδιά.

Η διαδικασία τερματισμού της σύνδεσης μπορεί να πραγματοποιηθεί είτε από τα δύο άκρα είτε και στη μέση αν έτσι απαιτηθεί.

Μόλις τερματιστεί η σύνδεση, οι δρομολογητές TOR χάνουν όλη την πληροφορία σχετικά με τη σύνδεση. Για να μην μπορέσει κάποιος να συνάγει το μήκος του δρομολογίου, τα στρώματα πρέπει να διατηρούν σταθερό μέγεθος κατά τη διάρκεια της δρομολόγησής τους. Για να επιτευχθεί αυτό, κάθε δρομολογητής υποχρεούται να συμπληρώνει στο TOR που του αποκαλύπτεται το κενό που δημιούργησε η αφαίρεση του στρώματος από αυτό. Εάν η πληροφορία, δεν έχει το σωστό και αυστηρά καθορισμένο μέγεθος όταν σταλεί, απορρίπτεται από τον επόμενο δρομολογητή. Η συνολική πληροφορία, η οποία αποτελείται από τα δεδομένα και τις πληροφορίες ελέγχου του δικτύου, αποστέλλεται μέσα στο δίκτυο του TOR σε ομοιόμορφου μεγέθους κυψέλες. Οι κυψέλες φτάνουν σε ένα ορισμένο χρονικό διάστημα και αναμιγνύονται για να μη διαπιστωθούν τυχόν συσχετίσεις που θα διευκόλυναν την εργασία όσων θέλουν να παραβιάσουν την ανωνυμία του χρήστη. Κάτι ανάλογο είναι δυνατό να γίνει με τις συνδέσεις μεγάλης διάρκειας ή περιορισμένου εύρους ζώνης. Αυτή η τεχνική αντιστέκεται στις επιθέσεις ανάλυσης κίνησης, περισσότερο από κάθε άλλη παρόμοια τεχνική στο Internet. Το προκύπτον κόστος για τη λειτουργία του TOR είναι σχετικά μικρό (Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).



Εικόνα 8: Η αρχιτεκτονικη της εξηπηρετησης του TOR

Κάθε TOR δρομολογητής γνωρίζει τις ταυτότητες και τα δημόσια κλειδιά κάθε άλλου δρομολογητή. Ο ιδρυτής ξεκινά επιλέγοντας μια πορεία για τον ανταποκριτή. Για κάθε δρομολογητή ο ιδρυτής δημιουργεί ένα πακέτο επίπεδου εγκατάστασης σύνδεσης που αποτελείται από την IP διεύθυνση του επόμενου δρομολογητή, το κρυπτογραφημένο κλειδί με το οποίο μπορεί να διαμοιράζεται μυστικές πληροφορίες ένας δρομολογητής με τον επόμενό του. Το πιο εσωτερικό επίπεδο του TOR περιέχει την ταυτότητα του ανταποκριτή και τα δεδομένα προς αποστολή. Κάθε ζεύγος δρομολογητών χρησιμοποιεί ένα αναγνωριστικό τοπικής μοναδικής σύνδεσης (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

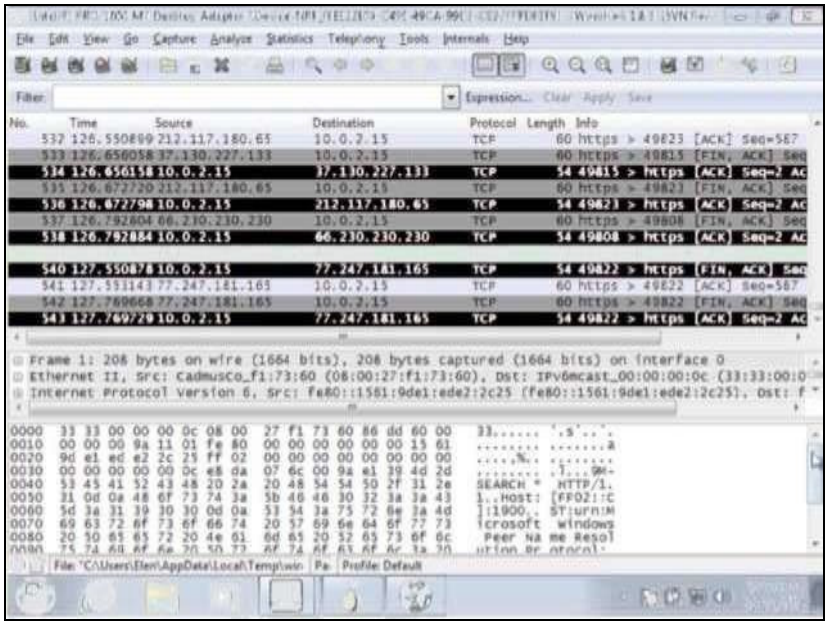
Όπως προωθείται το πακέτο στο μονοπάτι των δρομολογητών TOR, τα επίπεδα ξετυλίγονται. Όταν το πακέτο φτάσει στον τελευταίο δρομολογητή του μονοπατιού, τα δεδομένα προωθούνται άμεσα στον αποδέκτη τους. Όλες οι αιτήσεις από τον ιδρυτήαποστολέα αποστέλλονται από το ίδιο μονοπάτι των δρομολογητών TOR.

Ο ιδρυτής πρέπει να συνδεθεί σε έναν από αυτούς τους δρομολογητές για να επικοινωνήσει με τον παραλήπτη.

Οι απαντήσεις αποστέλλονται από τον τελευταίο δρομολογητή του μονοπατιού, ο οποίος επιστρέφει τα δεδομένα στον αποστολέα-ιδρυτή από το ίδιο μονοπάτι, αλλά με την αντίστροφη πορεία. Η υλοποίηση του TOR δεν αναπτύσσεται σε κάθε αιτούντα. Αντ' αυτού, είναι διαθέσιμος για χρήση ένας αριθμός δρομολογητών (Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Η πλοήγηση στο διαδίκτυο μέσω του TOR browser, μας προσφέρει ανωνυμία σε εφαρμογές που βασίζονται σε συνδέσεις Transmission Control Protocol (TCP). Η αυτονομία της εφαρμογής του TOR το διαφοροποιεί από τα περισσότερα από δίκτυα ανωνυμοποίησης, αφού λειτουργεί σε TCP επίπεδο μεταφοράς OSI. Χρησιμοποιώντας την ίδια ιστοσελίδα, παίρνουμε την ακόλουθη εικόνα (Εικόνα 10). Ως αποτέλεσμα αν προσπαθήσουμε να φιλτράρουμε -προκειμένου να βρούμε τα signin credentials-, αυτό δεν γίνεται δυνατό αφού τα δεδομένα είναι κρυπτογραφημένα και δεν μπορούμε να δούμε ποιες είναι οι εντολές του πελάτη και ποιες οι αποκρίσεις του εξυπηρετητή. Ο TOR περνάει την κίνηση από τρεις διαφορετικούς servers με διαφορετικό επίπεδο κρυπτογράφησης για κάθε έναν από αυτούς (Le Blond et al., 2011; Muller et al., 2012).

Οι χρήστες του δικτύου TOR εκτελούν στον Η/Υ έναν διακομιστή μεσολάβησης (proxy). Το λογισμικό ανά διαστήματα διαπραγματεύεται την δημιουργία ενός εικονικού κυκλώματος μέσω του δικτύου του, χρησιμοποιώντας κρυπτογράφηση πολλαπλών στρωμάτων, για να εξασφαλίσει τέλεια μυστικότητα προς τα εμπρός. Συγχρόνως, εμφανίζει στους πελάτες την διεπαφή SOCKS. Οι εφαρμογές χρησιμοποιούν τα SOCKS 4 και 5 πρωτόκολλα, τα οποία κρυπτογραφούν πολλαπλά μέσω του εικονικού κυκλώματός του TOR και του διακομιστή μεσολάβησης POLIPO. Ο POLIPO είναι ένας διαδικτυακός διακομιστής -μεσολάβησης ο οποίος ενισχύει την επικοινωνιακή λανθάνουσα του TOR, δηλαδή καθ' όλη τη διάρκεια που κάποιος βρίσκεται μέσα στο δίκτυο του TOR, η κίνηση αποστέλλεται από δρομολογητή σε δρομολογητή, και τελικά καταλήγει στο κόμβο εξόδου όπου το μη κρυπτογραφημένο πακέτο γίνεται διαθέσιμο και προωθείται στον αρχικό προορισμό (Εικόνα 10) (Le Blond et al., 2011; Muller et al., 2012).



Εικόνα 9: Καταγραφή πακέτων μέσω πλοήγησης με TOR

Σε όλες τις εκδόσεις του TOR τα άμεσα αιτήματα Domain Name System (DNS) συνήθως εκτελούνται ακόμα από πολλές εφαρμογές χωρίς την χρήση ενός διακομιστή μεσολάβησης TOR. Αυτό επιτρέπει στον οποιοδήποτε να παρακολουθεί την σύνδεση ενός χρήστη για να καθορίσει ποιες ιστοσελίδες μπορεί να επισκέπτεται, με την χρήση της εντολής torify. Επιπλέον, οποίες εφαρμογές χρησιμοποιούν το SOCKS 5 (το οποίο υποστηρίζει αιτήματα του διακομιστή μεσολάβησης βασισμένα στο όνομα) μπορούν να δρομολογήσουν τα αιτήματα DNS διαμέσω του TOR, εκτελώντας την αναζήτηση στον κόμβο εξόδου λαμβάνοντας έτσι τον μέγιστο βαθμό ανωνυμίας. Η έκδοση 0.2.0.1a περιλαμβάνει τον δικό της επιλυτή DNS που αποστέλλει τα ερωτήματα στο mix network, ώστε να κλείνει την διαρροή του DNS και να αλληλεπιδρά με την υπηρεσία χαρτογράφησης του TOR και να παρέχει πρόσβαση στις κρυμμένες υπηρεσίες του (Le Blond et al., 2011; Muller et al., 2012).

2.2. Εγκατάσταση και χρήση τουTOR

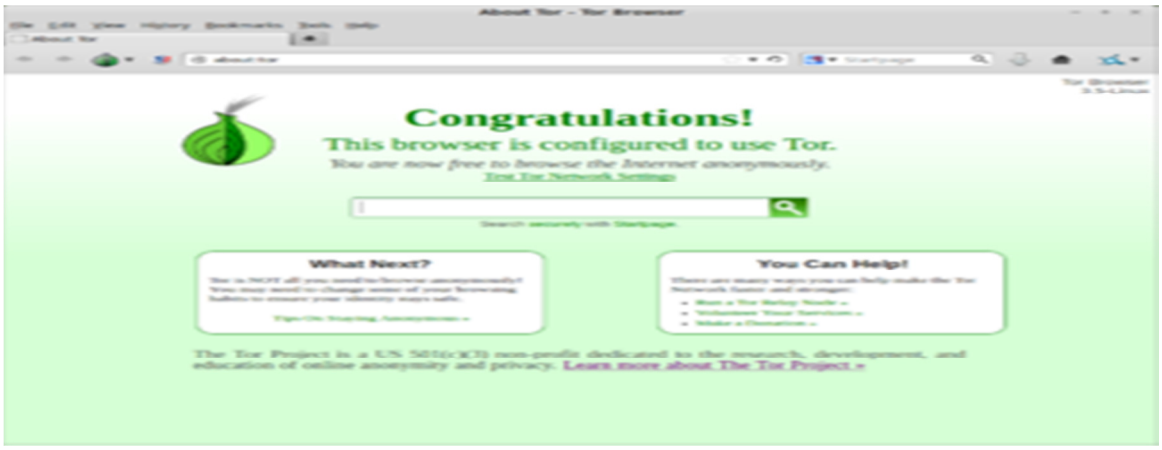
Βασικό χαρακτηριστικό του TOR αποτελεί το γεγονός ότι μπορεί να εγκατασταθεί και να χρησιμοποιηθεί από οποιοδήποτε από το οποίο ο χρήστης επιθυμεί, ακόμα και σε κινητά τηλέφωνα τα οποία χρησιμοποιούν αποκλειστικά σε λειτουργικό Android.

Όταν τρέξει το πρόγραμμα θα αποσυμπιεστούν τα κατάλληλα αρχεία στον φάκελο που αναφέρεται (TOR Browser). Μέσα σε αυτόν το φάκελο υπάρχει το πρόγραμμα Star TOR Browser.exe. Τότε θα ξεκινήσουν να τρέχουν τα κατάλληλα προγράμματα. Την πρώτη φορά μπορεί να χρειαστεί αναβάθμιση του TOR Browser Bundle. Μόλις ολοκληρωθεί η σύνδεση του Η/Υ σας με το δίκτυο TOR θα ξεκινήσει μια ειδική έκδοση του Firefox. Αυτό είναι όλο. Το παράθυρο Vidalia Control Panel (το όνομα έχει παραμείνει από προηγούμενες εκδόσεις του TOR) σας δίνει στοιχεία της σύνδεσης σας. Αν πατήσουμε το View the Network θα δούμε μια εντυπωσιακή απεικόνιση των server και των διαδρομών που ακολουθούνται, όπως επίσης και τις ρυθμίσεις και τα μετρητικά της σύνδεσης (Jacobson, 2008).

Αντικειμενικό στόχο του TOR -διαχωρίζοντας τον εντοπισμό από την δρομολόγηση- αποτελεί η απόκρυψη της ταυτότητας των χρηστών του, καθώς και της δραστηριότητά τους στο διαδίκτυο αποτρέποντας την παρακολούθηση και την ανάλυση της κίνησης. Για να υλοποιηθεί ο προαναφερόμενος σκοπός το TOR κρυπτογραφεί και δρομολογεί τυχαία την επικοινωνία μέσω ενός δικτύου από κόμβους -με κρυπτογράφηση πολλαπλών στρωμάτων για να εξασφαλίσουν μεγιστοποίηση της μυστικότητας- που το λειτουργούν εθελοντές ανά την υφήλιο.. Ως αποτέλεσμα προσφέρει ανωνυμία σε δικτυακές τοποθεσίες, που περιλαμβάνει και την λογοκρισία του περιεχομένου μέσω των ανώνυμων κρυμμένων υπηρεσιών του. Η διαδικτυακή διεύθυνση του αποστολέα και του παραλήπτη δεν βρίσκονται σε μορφή αρχικού κειμένου ώστε οποιοσδήποτε ωτακουστής σε οποιαδήποτε σημείο κατά μήκος του καναλιού επικοινωνίας δεν μην δύναται άμεσα να ταυτοποιήσει και τα δύο άκρα. Επιπλέον, στον παραλήπτη φαίνεται ότι ο τελευταίος κόμβος -κόμβος εξόδου- είναι ο δημιουργός της επικοινωνίας (Muller et al., 2012).

Η κύρια εφαρμογή του Tor είναι γραμμένο κυρίως σε C , μαζί με την Python , τη Javascript και πολλά άλλα και αποτελείται από 540.751 γραμμές κώδικα , όπως των Μάρτιο του 2016 .

Tor Browser



Εικόνα 10: Ο browser του TOR

Το Tor Browser, στο παρελθόν γνωστό ως πρόγραμμα περιήγησης Tor Bundle (TBB), είναι η ναυαρχίδα των προϊόντων του έργου του Tor. Αποτελείται από ένα τροποποιημένο Mozilla Firefox ESR web browser, το tor button, TorLauncher, NoScript και HTTPS. Παντού υπάρχουν επεκτάσεις του Firefox και ο πληρεξούσιος Tor.

Οι χρήστες μπορούν να τρέξουν το πρόγραμμα περιήγησης Tor από αφαιρούμενα μέσα . Μπορεί να λειτουργήσει σε περιβάλλον Microsoft Windows, MacOS ή Linux.

Το πρόγραμμα περιήγησης Tor ξεκινά αυτόματα τις διαδικασίες. Κατά τον τερματισμό της συνόδου το πρόγραμμα περιήγησης διαγράφει τα δεδομένα της ιδιωτικής ζωής-ευαίσθητα, όπως τα cookies HTTP και το ιστορικό περιήγησης.

Μετά από μια σειρά από αποκαλύψεις για την παγκόσμια επιτήρηση ,ο Stuart Dredge (γραπτώς στην *εφημερίδα The Guardian* , το Νοέμβριο του 2013) συνιστάται η χρήση του Tor Browser για να αποφευχθεί η υποκλοπή και να διατηρήσει την ιδιωτική ζωή στο Διαδίκτυο.

Firefox / JavaScript ανωνυμία επίθεση

Τον Αύγουστο του 2013 ανακαλύφθηκε οτι οι Firefox browsers σε πολλές παλαιότερες εκδόσεις του προγράμματος περιήγησης Tor Bundle ήταν ευάλωτοι σε μια επίθεση JavaScript, όπως NoScript όταν δεν ήταν ενεργοποιημένο από προεπιλογή. Οι επιτιθέμενοι χρησιμοποίησαν αυτό το θέμα ευπάθειας για να εξαγάγουν τις MAC και IP διευθύνσεις των χρηστών και στα Windows τα ονόματα υπολογιστών.

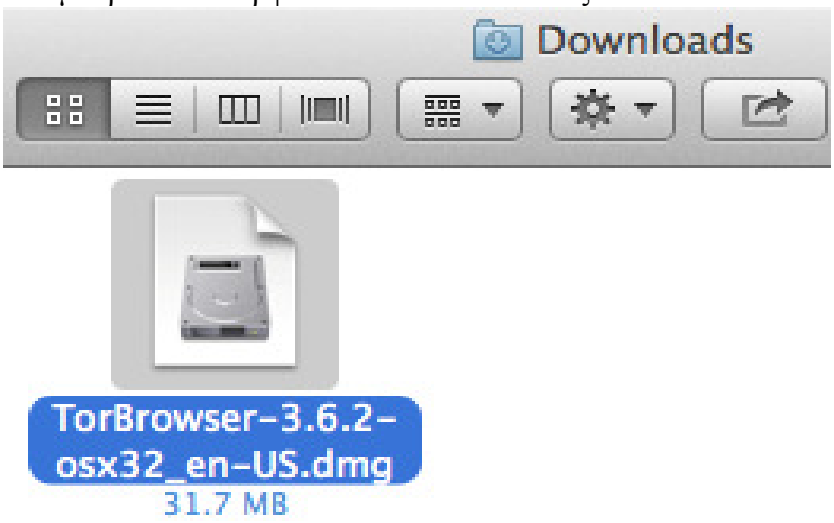
Οι εκθέσεις ειδήσεων συνδέονται με αυτό με τις Ηνωμένες Πολιτείες Ομοσπονδιακού Γραφείου Ερευνών (FBI) με ιδιοκτήτη, τον Eric Eoin Marques, ο οποίος συνελήφθη σε προσωρινο ένταλμα έκδοσης που εκδίδεται από δικαστήριο των Ηνωμένων Πολιτειών στις 29 Ιουλίου. Το FBI επιδιώκει να εκδώσει Marques από την Ιρλανδία στο Maryland σε τέσσερις κατηγορίες, συνωμοτούν για τη διανομή και τη διαφήμιση της παιδικής πορνογραφίας - καθώς και η υποβοήθηση και διαφήμιση της παιδικής πορνογραφίας. Το ένταλμα ισχυρίζεται ότι ο Marques είναι «η μεγαλύτερη διευκόλυνσης της παιδικής πορνογραφίας στον πλανήτη". Το FBI αναγνώρισε την επίθεση σε μια κατάθεση δικαστήριο 12, Σεπτεμβρίου του 2013 στο Δουβλίνο. "

Tor Browser Λήψεις

Για να αρχίσουμε να χρησιμοποιούμε το Tor Browser, κατεβάζουμε το αρχείο για την γλώσσα της προτίμησής μας. Αυτό το αρχείο μπορεί να αποθηκευτεί οπουδήποτε είναι βολικό, π.χ. στην επιφάνεια εργασίας ή μια μονάδα flash USB.

Οδηγίες Mac OS X

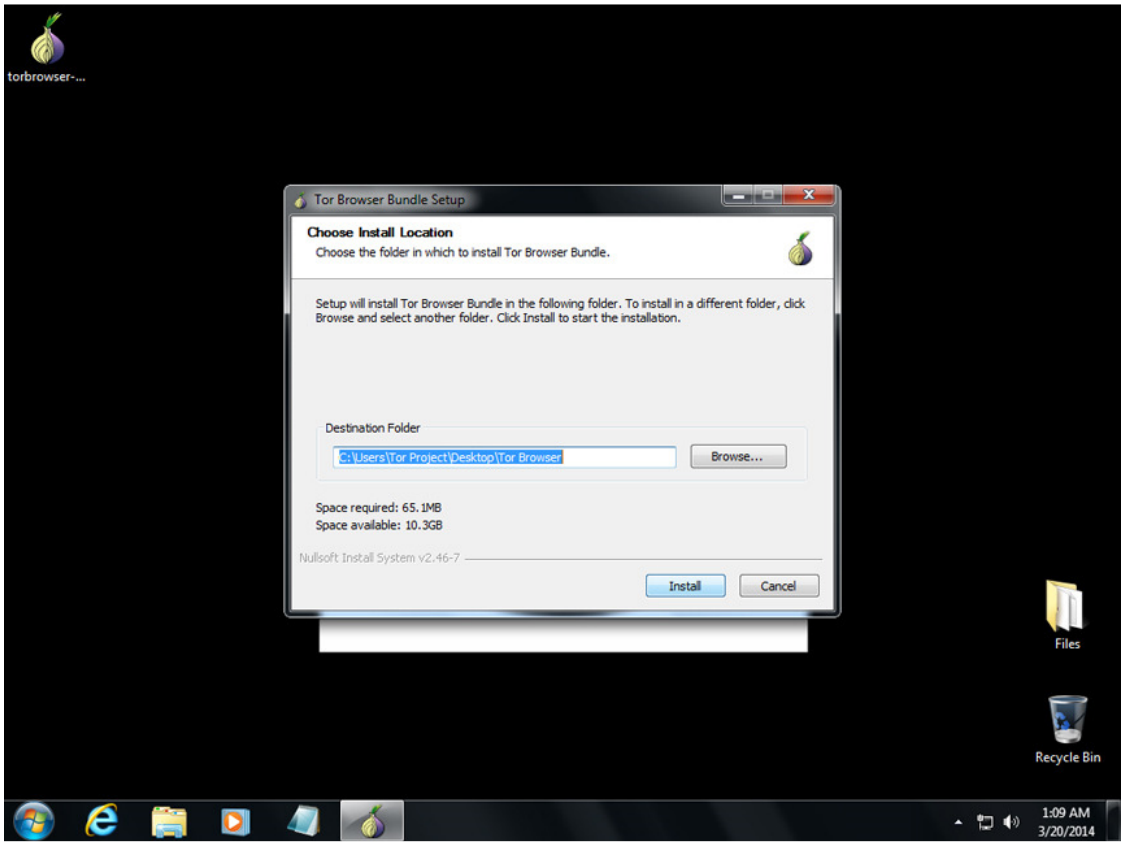
Κατεβάστε το αρχείο παραπάνω, να το αποθηκεύσετε κάπου, στη συνέχεια, κάντε κλικ σε αυτό. Αυτό ανοίγει το αρχείο .dmg. Σύρετε το συμπεριλαμβανόμενο αρχείο στο φάκελο Applications σας και θα έχετε μια εφαρμογή περιήγησης Tor στη γλώσσα της επιλογής σας, που μπορείτε να καρφιτσώσετε στο Dock σας.



Εικόνα 11: Το Mac OS x

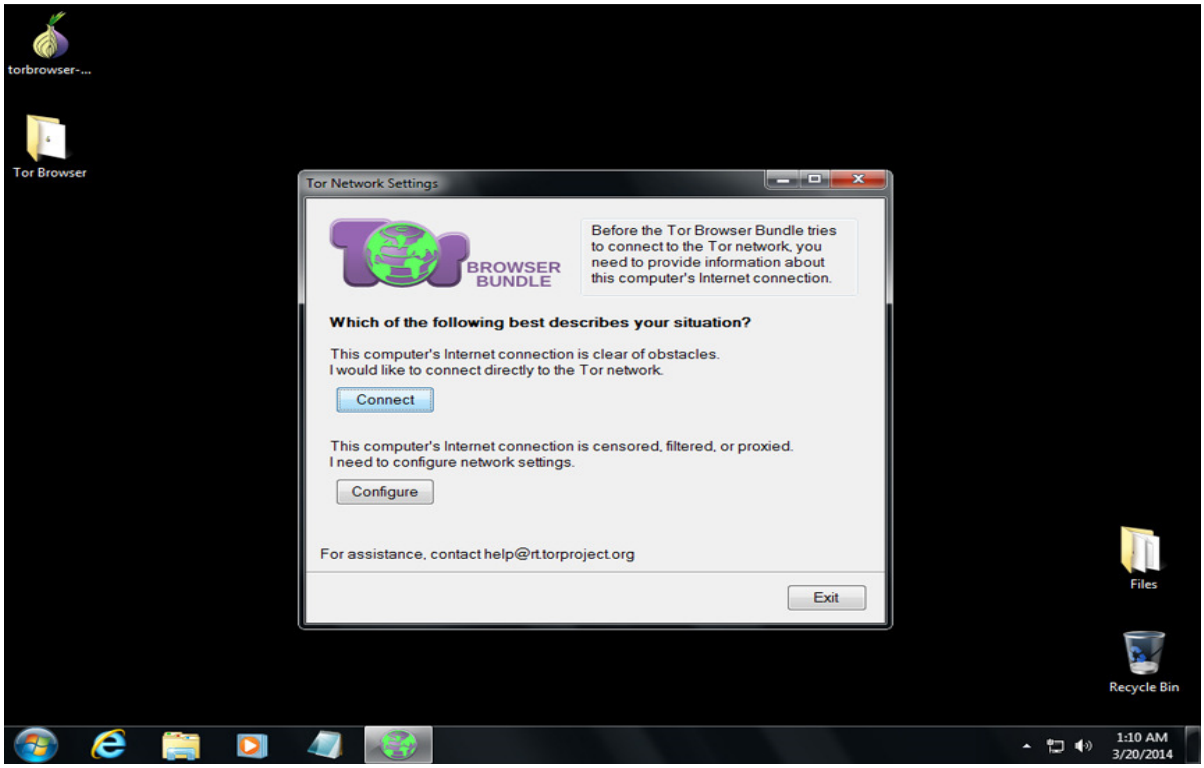
Οδηγίες παράθυρα

Κατεβάστε το αρχείο παραπάνω, και να το αποθηκεύετε κάπου, στη συνέχεια, κάντε διπλό κλικ σε αυτό. Κάντε κλικ στο "Run", στη συνέχεια, επιλέξτε τη γλώσσα της εγκατάστασης και κάντε κλικ στο OK . Βεβαιωθείτε ότι έχετε τουλάχιστον 80MB ελεύθερου χώρου στο δίσκο στη θέση που έχετε επιλέξει. Αν θέλετε να αφήσετε το πακέτο στον υπολογιστή, εξοικονομώντας το στο Desktop είναι μια καλή επιλογή. Αν θέλετε να το μετακινήσετε σε έναν διαφορετικό υπολογιστή ή να περιορίσει τα ίχνη που αφήνουν πίσω, να το αποθηκεύσετε σε ένα δίσκο USB.
Κάντε κλικ στο κουμπί Εγκατάσταση. Περιμένετε μέχρι να τελειώσει το πρόγραμμα εγκατάστασης.
Αυτό μπορεί να πάρει μερικά λεπτά για να ολοκληρωθεί.



Εικόνα 12: Εγκατάσταση του TOR

Μόλις ολοκληρωθεί η εγκατάσταση, κάντε κλικ στο κουμπί Finish για να εκκινήσετε τον οδηγό Tor Browser του.
Μόλις δείτε οδηγός Tor Browser κάντε κλικ στο Connect
Εναλλακτικά, μπορείτε να εκκινήσετε το Tor Browser πηγαίνοντας στο φάκελο Tor Browser το οποίο μπορεί να βρεθεί στη θέση που έχετε αποθηκεύσει το πακέτο σε (Προεπιλογή: Desktop) και κάντε διπλό κλικ στο Έναρξη Tor Browser .



Εικόνα 13: Εγκατασταση του TOR

Μόλις το Tor είναι έτοιμο, το Tor Browser αυτόματα θα ανοίξει. Όσες ιστοσελίδες επισκέφθηκε πλέον μέσω του Tor Browser θα αποσταλούν μέσω Tor. Άλλα προγράμματα περιήγησης στο Web, όπως ο Internet Explorer δεν επηρεάζονται.
Μόλις ολοκληρώσετε την περιήγηση, κλείστε όλα τα ανοιχτά παράθυρα στο Tor Browser
Για λόγους προστασίας της ιδιωτικής ζωής, η λίστα των ιστοσελίδων που επισκεφθήκατε και τυχόν cookies θα διαγράφονται.

Εικόνα 14: Εγκατάσταση του browser TOR

Για να χρησιμοποιήσετε το Tor Browser και πάλι, κάντε διπλό κλικ στο "Browser Εκκίνηση Tor" εφαρμογή.
Να θυμάστε ότι το Tor κρατά ανώνυμη τη προέλευση της κυκλοφορίας σας, και κρυπτογραφεί τα πάντα μέσα στο δίκτυο, αλλά δεν μπορεί να κρυπτογραφήσει την κυκλοφορία σας μεταξύ του δικτύου Tor και τον τελικό του προορισμό. Χρησιμοποιεί HTTPS ή άλλο είδος κρυπτογράφησης όπως το end-to-end. Στα οποία θα αναφερθούμε παρακάτω.

Σε ορισμένες χώρες η ιστοσελίδα Tor είναι αποκλεισμένη και δεν είναι δυνατόν να κατεβάσετε το Tor άμεσα. Το Πρόγραμμα Tor φιλοξενεί επίσης έναν καθρέφτη του Tor Browser Bundle για Github . Η GetTor υπηρεσία μπορεί επίσης να χρησιμοποιηθεί για να κατεβάσετε το Tor Browser, όταν η ιστοσελίδα του έργου και καθρέφτες έχουν αποκλειστεί.

Ουρές ή αλλιώς tails είναι ένα ζωντανό λειτουργικό σύστημα που μπορείτε να αρχίσετε για σχεδόν οποιοδήποτε υπολογιστή από ένα DVD, USB stick, ή κάρτα SD

2.3. TOR και Linux

Ο πυρήνας Linux αποτελεί έναν πυρήνας λειτουργικού συστήματος που χρησιμοποιείται από την οικογένεια Unix-ειδών λειτουργικών συστημάτων της Linux. Διανέμεται υπό την γενική άδεια δημόσιας χρήσης GNU έκδοση 2 και ορισμένων άλλων αδειών κλειστού κώδικα, για μερικά προγράμματα οδήγησης. Ο πυρήνας αυτός έχει τροποποιηθεί από πολλούς προγραμματιστές, και σε αυτόν βασίζονται οι διανομές Linux. Το Linux διατίθεται μόνο υπό την έκδοση 2 της GPL, χωρίς την επιλογή χρήσης νεότερης έκδοσης (έκδοση 3). Ο πυρήνας Linux είναι μια πρωτότυπη υλοποίηση πυρήνα λειτουργικού συστήματος. Αν και δεν χρησιμοποιεί κώδικα του UNIX, μπορεί να θεωρηθεί παρεμφερές σύστημα αφού διαθέτει τις περισσότερες εντολές του και την ίδια σχεδόν δομή αρχείων, ενώ η φιλοσοφία της σχεδίασής του πλησιάζει περισσότερο το UNIX από οποιοδήποτε άλλο λειτουργικό σύστημα (Torvalds, 2011, σ. 60-63).

Σήμερα, το Linux παρέχει όλα όσα θεωρούνται αναγκαία για ένα σύγχρονο πυρήνα λειτουργικού, όπως (Torvalds, 2011, σ. 60-63):

- Υποστήριξη πολυεπεξεργαστών (SMP),
- Πραγματική πολυδιεργασία,
- Εικονική μνήμη,
- Διαμοιραζόμενες βιβλιοθήκες,
- Διαχείριση μνήμης,
- δικτύωση μέσω TCP/IP.

Για να τρέξει το TOR σε Linux, ακολουθούνται τα επόμενα βήματα:

(i). **Πραγματοποιείται λήψη και εγκατάσταση του TOR:** Υπάρχουν πακέτα για Debian, Red Hat και Gentoo. Αν χρησιμοποιείται το Ubuntu, πρέπει αποθηκευτεί στο deb αποθετήριο, ενώ οι χρήστες CentOS/Fedora σε rpm. Γίνεται πρώτα εγκατάσταση libevent, και επιβεβαίωση ότι υπάρχει OpenSSL και zlib.Στη συνέχεια, εκτελείται το xzf Tor-0.2.6.10.tar.gz cd Tor-0.2.6.10/configure. Για να εκτελεστεί TOR ως SRC πρέπει να γίνει install (ως root αν είναι απαραίτητο). Το TOR είναι ρυθμισμένο ως πελάτης από προεπιλογή. Χρησιμοποιεί ένα ενσωματωμένο στο αρχείο ρυθμίσεων προεπιλογής, και έχει πλέον εγκατασταθεί,

(ii). **Ρύθμιση εφαρμογών διαμέσω TOR**: Η χρήση του TOR για ανώνυμη περιήγηση στο διαδίκτυο, προϋποθέτει TOR Browser, που αποτελεί διαμορφωμένο TOR και συνδυάζεται με πρόγραμμα περιήγησης patched για την καλύτερη ανωνυμία. Για να χρησιμοποιήσετε άμεσα SOCKS, για άμεσα μηνύματα, Jabber, IRC, κλπ., πρέπει να κατευθύνει η αίτηση απευθείας στο TOR. Εάν υπάρχει κάποιο τείχος προστασίας που περιορίζει την ικανότητα του υπολογιστή σας να συνδεθεί με το ίδιο πρέπει να επιτρέπει τις συνδέσεις σε TOR. Αν το SELinux config επιτρέπει το TOR για να λειτουργήσει σωστά, δημιουργείτε ένα αρχείο με το όνομα booleans.local στον κατάλογο, με επεξεργασία του συγκεκριμένου αρχείου με επεξεργαστή κειμένου.

Οδηγίες Linux

Κατεβάζουμε το κατάλληλο αρχείο όπως παραπάνω, το αποθηκεύουμε κάπου, στη συνέχεια, εκτελούμε μία από τις ακόλουθες δύο εντολές για να εξαγάγουμε το αρχείο πακέτου:

```
tar -xvJf tor-browser-linux32-6.0.8_LANG.tar.xz
```

ή (για την έκδοση 64-bit):

```
tar -xvJf tor-browser-linux64-6.0.8_LANG.tar.xz
```

(όπου LANG είναι η γλώσσα που αναφέρονται στο όνομα του αρχείου).

Μόλις γίνει αυτό, μεταβαίνουμε στον κατάλογο του προγράμματος περιήγησης Tor εκτελώντας:

```
cd tor-browser_LANG
```

(όπου LANG είναι η γλώσσα που αναφέρονται στο όνομα του αρχείου).

Για να εκτελέσουμε το Tor Browser, κάνουμε κλικ είτε στο πρόγραμμα περιήγησης Tor ή στο εικονίδιο Ρύθμιση περιήγησης Tor ή να εκτελέσει την έναρξη Tor-browser.desktop αρχείο σε ένα τερματικό:

```
./start-tor-browser.desktop
```

Αυτό θα ξεκινήσει το Tor Launcher και συνδέεται με το Tor, έτσι θα ξεκινήσει το Firefox.

Οδηγίες Android Orbot

Εικόνα 15: Το Orbot, εφαρμογη Android

Το Orbot είναι μια ελεύθερη πληρεξούσια εφαρμογή που δίνει τη δυνατότητα σε άλλες εφαρμογές να χρησιμοποιούν το Διαδίκτυο με μεγαλύτερη ασφάλεια. Επίσης χρησιμοποιεί το Tor για την κρυπτογράφηση της κυκλοφορίας μας στο Internet. Το Tor είναι ελεύθερο λογισμικό και ένα ανοικτό δίκτυο που μας υπερασπίζεται έναντια σε μια μορφη παρακολούθησης δικτύου που απειλεί την προσωπική ελευθερία και την προστασία της ιδιωτικής ζωής, εμπιστευτικές επιχειρηματικές δραστηριότητες και τις σχέσεις, και την κατάσταση της ασφάλειας γνωστή ως ανάλυση της κυκλοφορίας. Το Orbot δημιουργεί μια πραγματικά ιδιωτικη σύνδεση στο κινητό internet.

Ο πηγαίος κώδικας που χρησιμοποιεί είναι: Tor Gitweb και GitHub Mirror

Εικόνα 16: Το Orbot, εφαρμογη για Android

Tor Messenger

Εικόνα 17: Tor Messenger

Στις 29 Οκτωβρίου 2015, το Πρόγραμμα Tor κυκλοφόρησε το Tor Messenger Beta, ένα πρόγραμμα ανταλλαγής άμεσων μηνυμάτων με βάση Instantbird με Tor.
Όπως Pidgin και Adium , το Tor Messenger υποστηρίζει πολλαπλά διαφορετικά πρωτόκολλα ανταλλαγής άμεσων μηνυμάτων, ωστόσο, το επιτυγχάνει αυτό χωρίς να στηρίζονται σε *libpurple*.

2.4. Πλεονεκτήματα και μειονεκτήματα τουTOR

Το TOR μπορεί να χρησιμοποιηθεί για την απόκτηση πρόσβασης σε λογοκριμένες πληροφορίες, για την οργάνωση πολιτικών δραστηριοτήτων, είτε για την παράκαμψη νόμων που σχετιζονται με την άσκηση κριτικής κατά του κράτους. Παράλληλα, το TOR επιτρέπει ανώνυμες συκοφαντίες, αυθαίρετες διαρροές ευαίσθητων πληροφοριών, διανομή χωρίς άδεια υλικού με πνευματική ιδιοκτησία ή με παράνομο σεξουαλικό περιεχόμενο. Το δίκτυο TOR αποτελεί μια ομάδα διακομιστών που επιτρέπει στους χρήστες να βελτιώσουν την προστασία της ιδιωτικής ζωής και την ασφάλειά τους στο διαδίκτυο. Αποτελεί δε ένα αποτελεσματικό εργαλείο για τη λογοκρισία αφού επιτρέπει στους χρήστες του να δημιουργήσουν νέα εργαλεία επικοινωνίας για την προστασία της ιδιωτικής ζωής. Οι μη κυβερνητικές οργανώσεις (ΜΚΟ) και οι δημοσιογράφοι χρησιμοποιούν το TOR για να επικοινωνούν με μεγαλύτερη ασφάλεια με πληροφοριοδότες και αντιφρονούντες (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Το TOR προσφέρει ανωνυμοποίηση στους διακομιστές ως απόκρυψη της τοποθεσίας ή σε κόμβους που τρέχουν ειδικά διαμορφωμένο λογισμικό διακομιστών. Αντί να αποκαλύπτεται η διεύθυνση IP των διακομιστών, δηλαδή η διαδικτυακή τοποθεσία τους, οι κρυφές υπηρεσίες είναι προσβάσιμες μέσω του TOR-Pseudodomain (TLD). Το δίκτυο TOR αντιλαμβάνεται το TLD και δρομολογεί δεδομένα από και προς τις κρυμμένες υπηρεσίες ανώνυμα. Λόγω έλλειψης εμπιστοσύνης σε μια δημόσια διεύθυνση, οι κρυφές υπηρεσίες μπορούν να φιλοξενηθούν πίσω από “εμπόδια” ασφαλείας ή μεταφραστές δικτυακών διευθύνσεων (NAT). Επειδή οι υπηρεσίες απόκρυψης τοποθεσίας δεν χρησιμοποιούν κόμβους εξόδου, δεν υπόκεινται σε επιθέσεις (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Το μεγάλο πλεονέκτημα του TOR Browser Bundle, είναι ότι δεν χρειάζεται εγκατάσταση στο λειτουργικό σύστημα και επομένως είναι αρκετά εύκολο στη χρήση ακόμα κι από μη έμπειρους χρήστες, ενώ μπορεί να εκτελεστεί ακόμα κι από USB-stick. Στην πραγματικότητα το TOR Browser Bundle δεν απαιτεί καμιά εγκατάσταση. Το μόνο που χρειάζεται είναι να κατεβάσει ο χρήστης το συμπιεσμένο αρχείο του bundle και να το αποσυμπιέσει εξάγοντας τον φάκελο TOR Browser (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Υπάρχει παρόλα αυτά ένας αριθμός ζητημάτων ασφαλείας που περιλαμβάνονται στις κρυμμένες υπηρεσίες. Η τεχνολογία TOR δεν είναι απρόσβλητη σε επιθέσεις ανάλυσης κίνησης. Εάν υπάρχει κάποια εφαρμογή -εκφραζόμενη από αιτήσεις- δικτύου που απαιτεί σύνδεση πραγματικού χρόνου, είναι πιθανό να ανιχνευτεί η ταυτόχρονη είσοδος των πλησιέστερων συνδέσεων socket των TOR πληρεξούσιων του ιδρυτή και του ανταποκριτή.

Ωστόσο, αυτές οι μορφές επιθέσεων απαιτούν τη συλλογή και ανάλυση τεράστιων ποσοστών δεδομένων από εξωτερικούς παρατηρητές. Ένας τρόπος για βελτίωση του συστήματος και την αντιμετώπιση αυτού του είδους της επίθεσης αποτελεί η διέλευση μη ουσιαστικής κίνησης διαμέσου του δικτύου, ώστε να επιτευχθεί η σταθερότητα του επιπέδου κίνησης. Βεβαίως, με τον τρόπο αυτό, υπάρχει σχετική επιβάρυνση με όφελος τη βελτίωση της συνολικής ασφάλειας του συστήματος (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012). Για παράδειγμα, υπηρεσίες που είναι προσβάσιμες μέσω των κρυμμένων υπηρεσιών του TOR και του διαδικτύου είναι επιρρεπείς σε επιθέσεις συσχετισμού κι επομένως δεν θα χαρακτηρίζονταν ως εντελώς κρυμμένες. Άλλες παγίδες περιλαμβάνουν κακοδιαμορφωμένες υπηρεσίες, όπως η αναγνώριση πληροφοριών που εμπεριέχονται προεπιλεγμένα σε μηνύματα σφάλματος των δικτυακών διακομιστών, στατιστικές χρόνου λειτουργίας και μη, επιθέσεις παρεμβολής και σφάλματα του χρήστη (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Ως αποτέλεσμα βασικό μειονέκτημα του TOR αποτελεί η σχετικά αργή απόδοση του, εξαιτίας της οποίας πολλοί χρήστες αρνούνται να το χρησιμοποιήσουν. Αυτό, βέβαια, έχει αντίκτυπο στην προστασία της ιδιωτικότητας που παρέχεται από τον TOR, καθώς αυτή βρίσκεται σε ανάλογη εξάρτηση με τον αριθμό των χρηστών και τη διαθεσιμότητα των κοινόχρηστων πόρων. Ο ωτακουστής ως επιτιθέμενος, παραλαμβάνει αντίγραφα των πακέτων που στέλνονται ή λαμβάνονται από τις εφαρμογές και τα πρωτόκολλα που εκτελούνται στον Η/Υ. Το είδος της επίθεσης αυτής, αποτελεί την βασικότερη αιτία ενάντια στη διασφάλιση της ιδιωτικότητας και της ανωνυμίας στο διαδίκτυο. Επίσης, δεν προστατεύει στα ομότιμα δίκτυα τύπου torrent, γιατί δεν υποστηρίζει την τεχνολογία στην οποία στηρίζονται (π.χ., Crow, Hordes και Freedom) (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Επίσης, το TOR δεν μπορεί ή και δεν προσπαθεί να προστατεύσει τους χρήστες στις περιπτώσεις που η κίνηση εισέρχεται και εξέρχεται από το δίκτυο. Ενώ το λογισμικό αυτό παρέχει προστασία κατά της ανάλυσης κίνησης, δεν προλαμβάνει την επιβεβαίωση της κίνησης (από άκρη σε άκρη συσχετισμός). Το 2011, καταγράφηκε επίθεση ικανή να αποκαλύψει τη διεύθυνση IP των χρηστών του BitTorrent στο δίκτυο TOR. Η επίθεση αυτή ονομάστηκε bad apple, χρησιμοποιεί τον σχεδιασμό του TOR και εκμεταλλεύεται κάθε μη ασφαλή χρήση εφαρμογής για να συσχετίσει την ταυτόχρονη χρήση μιας ασφαλής εφαρμογής με την διεύθυνση IP του συγκεκριμένου χρήστη. Η επίθεση αυτή, που εξαρτάται από τον έλεγχο ενός κόμβο εξόδου ή την υποκλοπή της απάντησης ενός ανιχνευτή, βασίζεται εν μέρη στην στατιστική εκμετάλλευση της ανίχνευσης του κατανεμημένου πίνακα κατακερματισμού. Επίσης, την ίδια χρονιά ανακαλύφθηκε μια τεχνική που δημιουργεί ενός χάρτη των κόμβων του δικτύου TOR, που οδηγεί στον έλεγχο του ενός τρίτου από αυτούς και στην συνέχεια αποκτά τα κλειδιά κρυπτογράφησής τους. Ύστερα, χρησιμοποιώντας τα γνωστά πλέον κλειδιά και τις πηγές παρατηρείται η ικανότητα αποκρυπτογράφησης των δύο από τα τρία στρώματα κρυπτογράφησης (Dingledine et al., 2004; Jones, 2005; Lasse, 2006; Soghoian, 2007; Jacobson, 2008; Le Blond et al., 2011; Muller et al., 2012).

Όπως όλα τα τωρινά δίκτυα ανωνυμοποίησης, το Tor δεν μπορεί και δεν προσπαθεί να προστατεύσει τους χρήστες από την παρακολούθηση της κίνησης στα όρια του δικτύου, όπως για παράδειγμα, η κίνηση που εισέρχεται και εξέρχεται από το δίκτυο. Ενώ το Tor παρέχει προστασία κατά της ανάλυσης κίνησης, δεν προλαμβάνει την επιβεβαίωση της κίνησης.

Τον Μάρτιο του 2011, ερευνητές μαζί με ανθρώπους από το Rocquencourt, το εθνικό ινστιτούτο έρευνας στην επιστήμη της πληροφορικής και του ελέγχου (Institut national de recherche en informatique et en automatique, INRIA), που βρίσκεται στην Γαλλία, κατέγραψαν μια επίθεση ικανή να αποκαλύψει τη διεύθυνση IP των χρηστών του BitTorrent στο δίκτυο Tor. Η επίθεση *bad apple* χρησιμοποιεί τον σχεδιασμό του Tor και εκμεταλλεύεται κάθε μη ασφαλή χρήση εφαρμογής για να συσχετίσει την ταυτόχρονη χρήση μιας ασφαλής εφαρμογής με την διεύθυνση IP του συγκεκριμένου χρήστη Tor. Μία μέθοδος επίθεσης εξαρτάται από τον έλεγχο ενός κόμβο εξόδου ή την υποκλοπή της απάντησης ενός ανιχνευτή, ενώ μία δεύτερη μέθοδος επίθεσης βασίζεται εν μέρει στην στατιστική εκμετάλλευση της ανίχνευσης του κατανεμημένου πίνακα κατακερματισμού.

Τον Οκτώβριο του 2011 ερευνητική ομάδα από την Esiea, Γαλλική σχολή μηχανολόγων, δήλωσε ότι ανακάλυψε έναν τρόπο να υπονομεύσει το δίκτυο του Tor με το να αποκρυπτογραφήσει επικοινωνίες που το διαπερνούν. Η τεχνική που περιέγραψαν απαιτεί τη δημιουργία ενός χάρτη των κόμβων του δικτύου Tor, τον έλεγχο του ενός τρίτου από αυτούς και στην συνέχεια να αποκτήσουν τα κλειδιά κρυπτογράφησής τους και τις πηγές του αλγόριθμου. Ύστερα, χρησιμοποιώντας τα γνωστά πλέον κλειδιά και τις πηγές θεωρούν ότι έχουν την ικανότητα να αποκρυπτογραφούν δύο από τα τρία στρώματα κρυπτογράφησης. Ισχυρίζονται ότι μπορούν να σπάσουν το τρίτο κλειδί με μια επίθεση που βασίζεται στην στατιστική ανάλυση. Για να επανακατευθύνουν την κίνηση του Tor στους κόμβους που ελέγχουν, χρησιμοποίησαν μεθόδους επίθεσης άρνησης εξυπηρέτησης και επίθεσης packet spinning. Καμία τεχνική ανάλυση δεν είναι ακόμα διαθέσιμη για το κοινό ή για του κατασκευαστές του Tor για περαιτέρω μελέτη. Ο Eric Filiol και η ομάδα του σκοπεύουν να κυκλοφορήσουν τις συγκεκριμένες πληροφορίες στο επερχόμενα συνέδρια PacSec και Hackers.

Η Δρομολόγηση του Tor υλοποιείται από κρυπτογράφηση στο στρώμα εφαρμογής μιας στοίβας πρωτοκόλλου επικοινωνίας. Το Tor κρυπτογραφεί τα δεδομένα, συμπεριλαμβανομένων του προορισμού διεύθυνσης IP , πολλές φορές τα στέλνει μέσω ενός εικονικού κυκλώματος που περιλαμβάνει διαδοχικά, τυχαία επιλεγμένα ρελε. Κάθε ρελέ αποκρυπτογραφεί ένα στρώμα κρυπτογράφησης για να αποκαλύψει μόνο το επόμενο ρελέ στο κύκλωμα προκειμένου να περάσει τα υπόλοιπα κρυπτογραφημένα δεδομένα σχετικά με αυτό. Το τελικό ρελέ αποκρυπτογραφεί το εσώτατο στρώμα της κρυπτογράφησης και στέλνει τα αρχικά δεδομένα στον προορισμό του χωρίς να αποκαλύψει, ή ακόμη και γνωρίζοντας, τη διεύθυνση IP προέλευσης. Επειδή η δρομολόγηση της επικοινωνίας είναι εν μέρει κρυμμένη σε κάθε hop στο κύκλωμα Tor, η μέθοδος αυτή εξαλείφει κάθε μοναδικό σημείο στο οποίο οι επικοινωνίες συνομηλίκων μπορεί να προσδιοριστεί μέσω της επιτήρησης δικτύου που βασίζεται γνωρίζοντας την πηγή και τον προορισμό του.

Ένας αντίπαλος μπορεί να προσπαθήσει να καταργήσει την ανωνυμία του χρήστη με κάποιο τρόπο. Ένας τρόπος είναι μέσω αξιοποίησης ευάλωτου λογισμικού στον υπολογιστή του εκάστοτε χρήστη. Η NSA είχε μια τεχνική που στόχευε μια ευπάθεια - με την κωδική ονομασία "EgotisticalGiraffe» - σε μια ξεπερασμένη Firefox έκδοση του προγράμματος περιήγησης σε χρόνο που συνοδεύει το πακέτο Tor και σε, χρήστες του.

2.4.1. Βελτιωμένη ασφάλεια

Το Tor απάντησε σε αυτά τα τρωτά σημεία που αναφέρονται παραπάνω με την επιδιόρθωση τους και τη βελτίωση της ασφάλειας. Με τον ένα ή τον άλλο τρόπο, τα ανθρώπινα λάθη μπορεί να οδηγήσουν στην ανίχνευση. Η ιστοσελίδα του Tor παρέχει τις βέλτιστες οδηγίες σχετικά με το πώς να χρησιμοποιήσετε σωστά το πρόγραμμα περιήγησης Tor.

Παρακάτω δίνονται 11 οδηγίες που μπορούμε να κάνουμε ή όχι με το TOR:

1. Πρέπει να το χρησιμοποιούμε λόγο της ανωνυμίας και της κάλυψης των προσωπικών δεδομένων
2. Καλό είναι να μην χρησιμοποιούμε το Tor σε Windows διότι έχει σφάλματα ασφαλείας, και να χρησιμοποιούμε τα linux.
3. Θα πρέπει να γίνεται κάθε μέρα ubdate του λογισμικού για να εξασφαλίζονται όλες οι ενημερώσεις και οι εφαρμογές.
4. Δεν χρησιμοποιούμε ποτέ HTTP ιστοσελίδες για εντοπίζονται πολύ εύκολα.
5. Χρησιμοποιούμε κρυπτογραφικούς αλγόριθμους όπως, LUKS,TRU+Crypt κ,λ παντα σε linux για να προστατεύουμε και τα ψηφιακά δεδομένα των υπολογιστών.
6. Δεν χρησιμοποιούμε τον Tor Browser Bundle διότι το FBI μπορεί να το παρακολουθήσει.
7. Απενεργοποιούμε την javascript, την flash και την java γιατί σπάνε εύκολα.
8. Δεν χρησιμοποιούμε P2P και Bit torrent διότι καθηστερεί την περιήγηση άλλων χρηστών και μπλοκάρει την κυκλοφορία των πληροφοριών.
9. Διαγράφουμε τα Cookies και τα local data διότι παρακολουθούν τα πάντα και γίνεται πολύ ποιο εύκολο να εντοπιστεί ο εκάστοτε χρήστης.
10. Δεν χρησιμοποιούμε ποτέ το πραγματικό μας όνομα σε e-mail.
11. Και τέλος δεν χρησιμοποιούμε ποτέ το Google γιατί αποθηκεύει κάθε μας κίνηση. Καλύτερα να χρησιμοποιηθεί το DuckDuckGo που δεν έχει cookies.

2.4.2. Επίπεδα Ασφαλείας του Tor

Ανάλογα με τις ιδιαίτερες ανάγκες των χρηστών, το Tor προσφέρει τέσσερα επίπεδα ασφαλείας. Εκτός από την κρυπτογράφηση των δεδομένων, συμπεριλαμβανομένων αλλάζει συνεχώς διεύθυνση IP μέσω ενός εικονικού κυκλώματος που περιλαμβάνει διαδοχικά, τυχαία επιλεγμένα ρελέ Tor, διάφορα άλλα στρώματα της ασφάλειας είναι στη διάθεση του χρήστη:

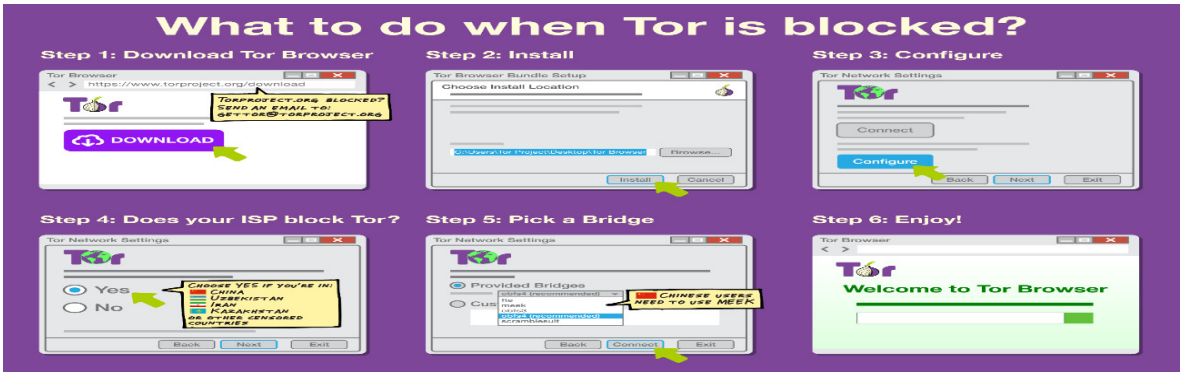
Τα επίπεδα είναι:

1. ***Χαμηλό***
   Σε αυτό το επίπεδο ασφαλείας, όλες οι λειτουργίες του προγράμματος περιήγησης είναι ενεργοποιημένες.Αυτό το επίπεδο παρέχει την πιο χρήσιμη εμπειρία, και το χαμηλότερο επίπεδο ασφάλειας.
2. ***Medium-Low***
   Σε αυτό το επίπεδο ασφαλείας, ισχύουν οι ακόλουθες αλλαγές:
   - Τα αρχεία ήχου και video HTML5, γίνονται click-to-play μέσω του NoScript.
   -Οι βελτιστοποιήσεις στην Javascript είναι απενεργοποιημένες.
   -Τα scripts σε μερικές σελίδες μπορεί να τρέχουν πιο αργά.
   -Ορισμένοι μηχανισμοί εμφάνισης μαθηματικών εξισώσεων είναι απενεργοποιημένες.
   -Και τα αρχεία Remote JAR είναι μπλοκαρισμενα.
3. ***Medium-High***
   Σε αυτό το επίπεδο ασφαλείας, ισχύουν οι ακόλουθες αλλαγές:
   - Τα αρχεία ήχου και video HTML5, γίνονται click-to-play μέσω του NoScript.
   -Οι βελτιστοποιήσεις στην Javascript είναι απενεργοποιημένες σε σελίδες που δεν λειτουργούν με πρωτόκολλο το HTTPS.
   -Τα scripts σε μερικές σελίδες μπορεί να τρέχουν πιο αργά.
   -Και τα αρχεία Remote JAR είναι μπλοκαρισμενα.
   -Ορισμένοι μηχανισμοί εμφάνισης μαθηματικών εξισώσεων είναι απενεργοποιημένες.

-Ορισμένες λειτουργίες απεικόνισης γραμματοσειρών είναι επίσης απενεργοποιημενες

Υψηλό

Σε αυτό το επίπεδο ασφαλείας, ισχύουν οι ακόλουθες αλλαγές:
- Τα αρχεία ήχου και video HTML5, γίνονται click-to-play μέσω του NoScript.
-Η Javascript είναι απενεργοποιημένη σε όλες τις ιστοσελίδες.
-Τα scripts σε μερικές σελίδες μπορεί να τρέχουν πιο αργά.
-Και τα αρχεία Remote JAR είναι μπλοκαρισμενα.
-Ορισμένοι μηχανισμοί εμφάνισης μαθηματικών εξισώσεων είναι απενεργοποιημένες.
-Ορισμένες λειτουργίες απεικόνισης γραμματοσειρών είναι επίσης απενεργοποιημενες
-Μερικοί τύποι εικόνων είναι απενεργοποιημένες.
-Ορισμένες γραμματοσειρές και εικονίδια ενδέχεται να μην εμφανίζονται σωστά.



Εικόνα 18: Τροποι επίλυσης μπλοκαρίσματος του tor

2.5. TOR και Darknet

Οι πληροφορίες στο web είναι κρυμμένες μέσα σε ιστότοπους με δυναμικά παραγόμενες ιστοσελίδες. Οι συνηθισμένες μηχανές αναζήτησης δεν μπορούν να τις εντοπίσουν και ανακτήσουν το περιεχόμενό τους γιατί οι ιστοσελίδες αυτές δεν υπάρχουν για τις μηχανές αναζήτησης μέχρι να δημιουργηθούν δυναμικά ως το αποτέλεσμα μιας συγκεκριμένης αναζήτησης. Αυτό συμβαίνει γιατί οι μηχανές αναζήτησης δεν μπορούν να καταχωρίσουν πληροφορίες που βρίσκονται σε βάσεις δεδομένων, σε δυναμικές ιστοσελίδες που δημιουργούνται από κάποιον κώδικα ή σε ιδιωτικά δίκτυα πληροφοριών. Έτσι, ο μεγαλύτερος όγκος πληροφοριών παραμένει απροσπέλαστος από τους χρήστες που χρησιμοποιούν το www. Η περιήγηση στο Darknet γίνεται ανώνυμα μέσα από την χρήση του TOR, δηλαδή διαρκώς μεταβαλλόμενων δεδομένων τα οποία καθιστούν σχεδόν αδύνατο τον εντοπισμό του χρήστη (Lemley & Reese, 2004).

Το darknet (ή σκοτεινό δίκτυο) είναι ένα δίκτυο επικάλυψης, που προσεγγίζεται μόνο με συγκεκριμένο λογισμικό, διαμορφώσεις, ή άδειες, χρησιμοποιώντας συχνά πρωτόκολλα και θύρες μη τυποποιημένων επικοινωνιών. Δύο χαρακτηριστικοί τύποι darknet είναι τα δίκτυα F2F, και δίκτυα ανωνυμίας όπως το Tor μέσω μιας σειράς ανώνυμων συνδέσεων.

Το Darknet είναι ένα δίκτυο από σέρβερ, οι οποίοι βασίζονται σε τεχνολογίες κρυπτογράφησης για να ανταλλάσσουν δεδομένα. Η πιο διαδεδομένη τεχνολογία γι' αυτό τον σκοπό είναι το TOR, που εγγυάται και τη δική τους ανωνυμία. Χάρις στο TOR, ένα site μπορεί να αποκρύπτει τα ψηφιακά του ίχνη, καμουφλάροντας τον σέρβερ που το φιλοξενεί. Παράλληλα, η τεχνολογία εξασφαλίζει πως πρόσβαση στο Darknet έχουν μόνον χρήστες που έχουν εγκαταστήσει το ανάλογο λογισμικό στο μηχάνημά τους. Οι χρήστες που επιθυμούν να συμμετάσχουν στη κατασκευή της γέφυρας αυτής πρέπει να είναι εγγεγραμμένοι στην υπηρεσία της Amazon. Το γεγονός υποδεικνύει ότι προσφέρεται για χρήση του Darknet, αφού δημιουργούνται κρυψώνες με τις υπηρεσίες cloud (Lemley & Reese, 2004).

Ένα μέρος του Darknet είναι προσβάσιμο μέσω του ανώνυμου δικτύου TOR. Η επίσκεψη σε ένα δικτυακό τόπο μέσω του TOR εκτρέπει τις συνδέσεις μέσα από μια τυχαιοποιημένη πορεία υπολογιστών άλλων χρηστών πριν από την επίτευξη του στόχου του web server, κρύβοντας ουσιαστικά την τοποθεσία σας από αυτόν το διακομιστή. Αντίθετα από τις κανονικές ιστοσελίδες, οι σελίδες του Darknet δεν έχουν φιλικές διευθύνσεις URL. Αντ' αυτού, αποτελούν μια φαινομενικά τυχαία σειρά χαρακτήρων που ακολουθείται από την κατάληξη ".onion" και παρέχει πρόσβαση σε αυτές τις κρυφές ιστοσελίδες. Στο Darknet υπάρχει το "Hidden Wiki" που παρέχει καταχωρήσεις αυτών των διευθύνσεων URL για να διευκολυνθεί η χρήση του Darknet.

Το TOR χρησιμοποιείται κυρίως από ακτιβιστές που θέλουν να αποφύγουν τη λογοκρισία, καθώς και από άτομα τα οποία επιζητούν ανωνυμία για πιο ύποπτους σκοπούς. Οι υποστηρικτές του επιθυμούν επέκταση του bandwidth της εν λόγω υπηρεσίας, και για αυτό στρέφονται στην Amazon, ή στην cloud υπηρεσία της οποίας θα κάνει δυσκολότερο για τις κυβερνήσεις να παρακολουθήσουν τα δρώμενα στο Darknet. Σε αυτό το βάθος δεν φτάνουν ποτέ οι μηχανές αναζήτησης και ο κόσμος διαμορφώνεται με άλλους κανόνες. Εμφανίζεται ο κατάλογος ταξινόμησης Hiddenwiki που ταξινομεί σελίδες με κατάληξη onion και παρέχει μια πρώτου επιπέδου διερεύνηση του πυθμένα. Με τη χρήση λογισμικού του TOR ο χρήστης εξασφαλίζοντας την ανωνυμία του, αποκτά πρόσβαση σε πληροφορίες όπως είναι η πώληση και διακίνηση όπλων, ναρκωτικών, παράνομων αγοραπωλησιών και στοιχημάτων, διακίνησης πορνογραφικού υλικού. Σε αυτή την πλευρά του διαδικτύου η ηθική απουσιάζει και εκτός από πλαστά διαβατήρια ή χαρτονομίσματα κανείς μπορεί να προσλάβει μέχρι και μισθωμένους δολοφόνους. Οι χρήστες του TOR ζητούν από τους υποστηρικτές του δικτύου να εγγραφούν στην υπηρεσία προκειμένου να τρέξουν μια γέφυρα (bridge)- ένα εξαιρετικά σημαντικό τμήμα του δικτύου, μέσω του οποίου δρομολογούνται οι επικοινωνίες. Μια τέτοιου τύπου γέφυρα δίνει την δυνατότητα για bandwidth στο δίκτυο TOR ώστε να βελτιώνεται η ασφάλεια και η ταχύτητα με την οποία οι χρήστες μπορούν να έχουν πρόσβαση στο διαδίκτυο (Lemley & Reese, 2004).

2.5.1. TOR 2 WEB

Το Tor2Web είναι ένα πρόγραμμα λογισμικού το οποίο επιτρέπει την πρόσβαση στις κρυφες υπηρεσίες του Tor και να είναι προσβάσιμες από ένα τυπικό πρόγραμμα περιήγησης χωρίς να είναι ο χρήστης συνδεδεμένος στο δίκτυο του Tor. Δημιουργήθηκε από τον Aaron Swartz και τον Virgil Griffith .

Το Tor είναι ένα δίκτυο που επιτρέπει στους ανθρώπους να χρησιμοποιούν το Διαδίκτυο ανώνυμα (αν και με γνωστές αδυναμίες) και να δημοσιεύουν περιεχόμενα που υπάρχουν μόνο μέσα σε αυτό για λόγους ασφαλείας, και έτσι είναι συνήθως προσβάσιμες μόνο στον σχετικά μικρό αριθμό ατόμων που χρησιμοποιούν το Tor2web browser. Ο Aaron Swartz και ο Virgil Griffith, που δημιούργησαν το Tor2web το 2008 ως ένα τρόπο για την υποστήριξη καταγγελίας δυσλειτουργιών και άλλες μορφές ανώνυμων εκδόσεων μέσω Tor, έβαλαν υλικά για να διατηρήσουν την ανωνυμία του, ενώ τα έκαναν προσιτά σε ένα ευρύτερο κοινό.

Σε μια συνέντευξη με τον *Wired* Swartz εξήγησε ότι το Tor είναι μεγάλο για ανώνυμη δημοσίευση, αλλά επειδή στόχος της δεν είναι η φιλικότητα προς το χρήστη, και ως εκ τούτου πολλοί άνθρωποι δεν θα το εγκαταστήσουν, ήθελε να "παράγει αυτό το υβρίδιο, όπου οι άνθρωποι θα μπορούσαν να δημοσιεύουν πράγματα χρησιμοποιώντας το Tor έτσι ώστε ο καθένας στο διαδίκτυο θα μπορούσε να το δεί "

Το λογισμικό που αναπτύχθηκε από τον Swartz και τον Griffith θεωρείται έκδοση 1.0. Από τότε, έχει διατηρηθεί και αναπτυχθεί από τον Giovanni Pellerano από την Hermes Κέντρο Διαφάνειας και Ψηφιακών Δικαιωμάτων του Ανθρώπου , ως μέρος του έργου GlobaLeaks , με την οικονομική υποστήριξη από το Open Ταμείο Τεχνολογίας . Η έκδοση 2.0 κυκλοφόρησε τον Αύγουστο του 2011.

2.5.2. Λειτουργία και Ασφάλεια

Αντί για ένα τυπικό top-level domains , όπως .com, .org, ή .net, χρησιμοποιεί κρυμμένη υπηρεσία διευθύνσεις URL που τελειώνει με .onion και είναι προσβάσιμο μόνο όταν συνδέεται με το Tor. Το Tor2web δρα ως ένα εξειδικευμένο πληρεξούσιο μεταξύ κρυμμένων υπηρεσιών και των χρηστών, καθιστώντας τα ορατά σε ανθρώπους που δεν είναι συνδεδεμένα με το Tor. Για να γίνει αυτό, ο χρήστης λαμβάνει στο URL του μια κρυφη υπηρεσίας και την αντικαθιστά το .onion με .onion.to.

Όπως το Tor, έτσι και το Tor2web λειτουργεί με εξυπηρετητές που λειτουργούν εθελοντικά από μια ανοικτή κοινότητα των ατόμων και των οργανώσεων.

Το Tor2web διατηρεί την ανωνυμία των εκδοτών περιεχομένου, αλλά δεν είναι η ίδια ανωνυμία και δεν παρέχει καμία προστασία στους χρήστες πέρα από τη μετεγκατάσταση δεδομένων χρησιμοποιώντας HTTP Secure (HTTPS). Από την έκδοση 2.0, μια προειδοποίηση της ιδιωτικής ζωής και της ασφάλειας προστίθεται στην κεφαλίδα της κάθε ιστοσελίδας που φέρνει, ενθαρρύνοντας τους αναγνώστες να χρησιμοποιήσετε το Tor Browser Bundle για την απόκτηση ανωνυμία

3. ΚΕΦΑΛΑΙΟ 3: Η Κρυπτογραφία του Tor – End-to-End.

Η βασική κρυπτογραφία που χρησιμοποιεί το TOR είναι η **End-to-End**. Είναι ένα σύστημα επικοινωνίας όπου μόνο οι χρήστες που επικοινώνουν μπορούν να διαβάσουν τα μηνύματα. Κατ 'αρχήν, αποτρέπει πιθανούς ωτακουστές από το να είναι σε θέση να έχουν πρόσβαση στα κλειδιά κρυπτογράφησης που απαιτείται για την αποκρυπτογράφηση της συνομιλίας. Τα συστήματα έχουν σχεδιαστεί για να νικήσουμε οποιαδήποτε προσπάθεια επιτήρησης ή / και αλλοίωσης επειδή τρίτοι μπορεί να αποκρυπτογραφήσουν τα δεδομένα που γνωστοποιούνται ή να αποθηκεύονται. Για παράδειγμα, οι εταιρείες που χρησιμοποιούν κρυπτογράφηση από άκρο σε άκρο δεν είναι σε θέση να παραδώσουν τα κείμενα των μηνυμάτων των πελατών τους στις αρχές.

3.1. Ανταλλαγή Κλειδίων

Σε ένα σύστημα E2EE, τα κλειδιά κρυπτογράφησης πρέπει να είναι γνωστά μόνο για τα μέρη που επικοινωνούν. Για την επίτευξη αυτού του στόχου, κρυπτογραφούνται τα δεδομένα χρησιμοποιώντας μια προκαθορισμένη σειρά από σύμβολα, που ονομάζεται PGP , ή από DUKPT . Μπορούν επίσης να διαπραγματευθουν ένα μυστικό κλειδί επί τόπου χρησιμοποιώντας Diffie-Hellman δηλαδή κλειδί ανταλλαγής (OTR).

Από το 2016, χαρακτηριστικό του server επικοινωνιών δεν περιλαμβάνουν κρυπτογράφηση end-to-end. Τα συστήματα αυτά μπορεί να εγγυηθούν μόνο την προστασία των επικοινωνιών μεταξύ των πελατών και servers , πράγμα που σημαίνει ότι οι χρήστες πρέπει να εμπιστεύονται τους τρίτους που τρέχουν στους διακομιστές με τα πρωτότυπα κείμενα.

Η End-to-end κρυπτογράφηση θεωρείται ασφαλέστερη, επειδή μειώνει τον αριθμό των μερών που μπορεί να είναι σε θέση να παρεμβαίνει ή να σπάσει την κρυπτογράφηση. Στην περίπτωση των άμεσων μηνυμάτων, οι χρήστες μπορούν να χρησιμοποιούν έναν πελάτη τρίτων (π.χ. Pidgin) να εφαρμόσει ένα σύστημα κρυπτογράφησης end-to-end (π.χ. OTR) πάνω από ένα πρωτόκολλο.

Ορισμένες εφεδρικές υπηρεσίες όπως SpiderOak και Tresorit παρέχουν client-side κρυπτογράφηση . Η κρυπτογράφηση που προσφέρουν δεν αναφέρεται ως κρυπτογράφηση end-to-end, επειδή οι υπηρεσίες αυτές δεν χρησιμοποιούνται για την επικοινωνία μεταξύ των χρηστών.

Η End-to-end κρυπτογράφηση διασφαλίζει ότι τα δεδομένα μεταφέρονται με ασφάλεια μεταξύ των τερματικών σημείων. Αλλά, αντί να προσπαθούν να σπάσουν την κρυπτογράφηση, ένας ωτακουστής μπορεί να μιμηθεί έναν παραλήπτη του μηνύματος, έτσι ώστε τα μηνύματα να είναι κρυπτογραφημένα με ένα κλειδί γνωστό για τον εισβολέα. Μετά την αποκρυπτογράφηση του μηνύματος, ο Snoop μπορεί στη συνέχεια να κρυπτογραφήσει με ένα κλειδί που αυτός / αυτή μοιράζεται με τον πραγματικό δικαιούχο, ή δημόσιο κλειδί του / της σε περίπτωση ασύμμετρων συστημάτων, και να στείλει το μήνυμα ξανά για να αποφύγουν τον εντοπισμό. Αυτό είναι γνωστό ως man-in-the-middle επίθεση .

Τα περισσότερα πρωτόκολλα κρυπτογράφησης end-to-end περιλαμβάνουν κάποια μορφή τελικού σημείου ελέγχου ταυτότητας, ειδικά για την αποτροπή επιθέσεων MITM. Για παράδειγμα, θα μπορούσε κανείς να βασιστεί σε αρχές πιστοποίησης ή ένα web εμπιστοσύνης . Μια εναλλακτική τεχνική είναι να δημιουργήσει κρυπτογραφικών hashes (δακτυλικά αποτυπώματα) με βάση δημόσια κλειδιά των χρηστών ή κοινόχρηστων μυστικών κλειδιών.

Όταν εμφανίζεται για ανθρώπινη επιθεώρηση, τα δακτυλικά αποτυπώματα είναι συνήθως κωδικοποιημένες σε διεξαδικές χορδές. Αυτές οι χορδές έχουν διαμορφωθεί σε ομάδες χαρακτήρων για αναγνωσιμότητα.

Για παράδειγμα, θα εμφανιστεί ένα 128-bit MD5 δακτυλικών αποτυπωμάτων ως εξής:

43: 51: 43: A1: B5: fc: 8β: B7: 0A: 3α: A9: β1: 0f: 66: 73: A8

Μερικά πρωτόκολλα εμφανίζουν φυσική γλώσσα αναπαραστάσεις των μπλοκ. Καθώς η προσέγγιση αποτελείται από μια χαρτογράφησης ένα-προς-ένα μεταξύ των μπλοκ δακτυλικών αποτυπωμάτων, δεν υπάρχει απώλεια σε εντροπία . Το πρωτόκολλο μπορεί να επιλέξει να εμφανίσει τις λέξεις στη μητρική γλώσσα του χρήστη. Για να βελτιωθεί η εντόπιση , κάποια πρωτόκολλα έχουν επιλέξει να εμφανίζουν τα δακτυλικά αποτυπώματα σαν βάση 10 χορδών αντί για δεκα-εξαδική ή φυσικής γλώσσας χορδές. Οι σύγχρονες εφαρμογές ανταλλαγής μηνυμάτων μπορεί επίσης να εμφανίζουν τα δακτυλικά αποτυπώματα ως κώδικες QR που οι χρήστες μπορούν να ανιχνεύσουν τη λειτουργία της συσκευής του άλλου.

3.2. Ασφάλειας καταληκτικού σημείου

Το παράδειγμα κρυπτογράφηση end-to-end δεν αντιμετωπίζει άμεσα τους κινδύνους στις επικοινωνίες τελικά.. Κάθε χρήστης ηλεκτρονικών υπολογιστών μπορεί ακόμα να χαραχτεί για να κλέψουν το κλειδί του ή της κρυπτογράφησης ή απλώς να διαβάσουν τα αποκρυπτογραφημένα μηνύματα. Ακόμη και η πιο τέλεια κρυπτογραφημένη σήραγγα επικοινωνίας είναι τόσο ασφαλές όσο το γραμματοκιβώτιο στο άλλο άκρο.

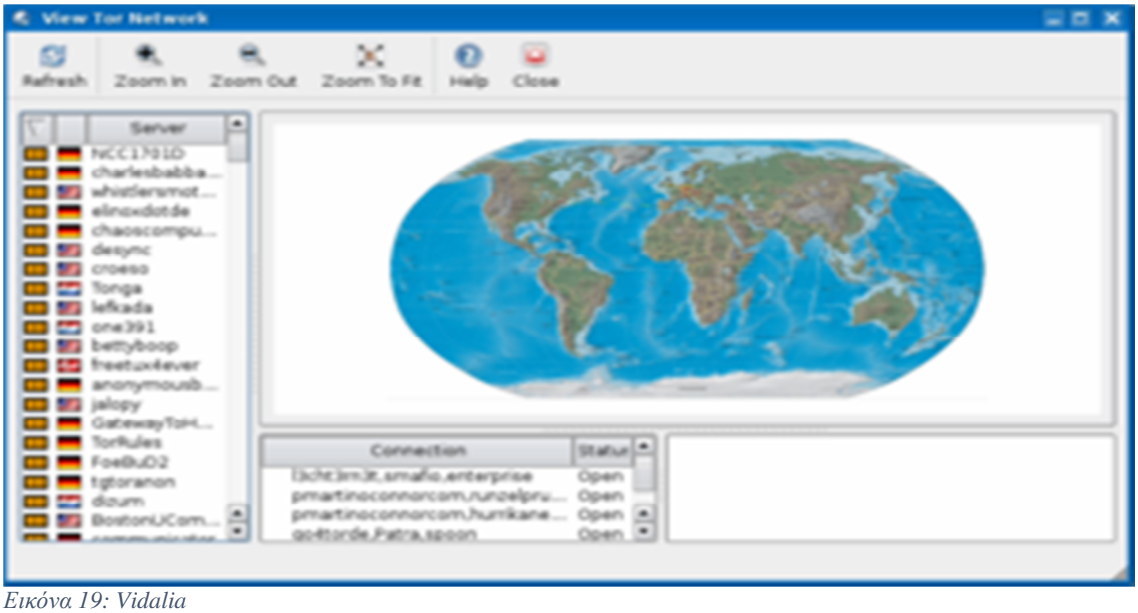
3.2.1. Κρυπτογράφηση:10 εργαλεία για να αποφύγετε την παρακολούθηση στο Internet

Στο σημείο αυτό συγκεντρώσαμε 10 υπηρεσίες και εφαρμογές ώστε να αποφύγετε να αφήσετε τα ίχνη σας κατά την περιήγησή σας στο Internet, ενώ παράλληλα θα προφυλάξετε τα δεδομένα και κλήσεις που ανταλλάσσετε. Η ιδιωτικότητα και η κρυπτογράφηση είναι μερικές έννοιες που "ακούγονται" πολύ, ενώ και μεγάλες εταιρίες αρχίζουν να δίνουν σημασία, όπως οι Apple και Google που προσφέρουν κωδικοποίηση στα iOS και Android από προεπιλογή όπως έχουμε αναφερθεί και παραπάνω, καθώς και το Facebook που είναι διαθέσιμο και μέσω του Tor.

1. Tor Project : Το Tor (The Onion Router) είναι ένα σύστημα που δίνει στους χρήστες του τη δυνατότητα ανωνυμίας στο Internet και δρομολογεί τη διαδικτυακή κίνηση μέσω ενός παγκόσμιου εθελοντικού δικτύου διακομιστών με σκοπό να αποκρύψει την τοποθεσία ενός χρήστη ή τη χρήση της κίνησης από οποιονδήποτε διεξάγει διαδικτυακή παρακολούθηση.
2. The Guardian Project : Το The Guardian Project είναι ένα σύνολο εφαρμογών (κυρίως για Android συσκευές) που αξίζει να δώσετε σημασία, αν σας ενδιαφέρει η κρυπτογράφηση και να μην "αφήνετε" τα στοιχεία σας κατά το browsing.
3. DuckDuckGo : Η DuckDuckGo είναι μία μηχανή αναζήτησης που δεν αποθηκεύει δεδομένα του χρήστη από τις αναζητήσεις του ή από το που είναι, πόσο χρόνο χρησιμοποίησε την υπηρεσία κ.λπ.
4. HTTPS Everywhere :Αν έχετε παρατηρήσει ορισμένα URLs, ξεκινούν με "http://", ενώ σταδιακά όλο και περισσότερα (ειδικά σε όσα υπάρχει η δυνατότητα login) ξεκινούν με "https://", τα οποία είναι ασφαλέστερα. Το HTTPS Everywhere plugin που λειτουργεί σε Chrome, Firefox και Opera, προσπαθεί να μετατρέψει κάθε URL από HTTP σε HTTPS.
5. Ghostery :Το Ghostery είναι ένα πρόσθετο που εμποδίζει την εκτέλεση κώδικα παρακολούθησης που υπάρχει σε κάποιες ιστοσελίδες, βελτιώνει την ταχύτητα του ανοίγματος της ιστοσελίδας και μειώνει τα "αποτυπώματα" του χρήστη στο διαδίκτυο.
6. Privacy Badger :Το Privacy Badger, είναι ένα addon για τους Firefox, Chrome και Opera που έχει δημιουργηθεί από το Electronic Frontier Foundation (EFF) και σαν στόχο έχει την προστασία των προσωπικών δεδομένων, κάνοντας αντίστοιχη δουλειά με το αμφιλεγόμενο πλέον AdBlock-Plus, μπλοκάροντας διαφημίσεις και άλλα ενοχλητικά αντικείμενα που κυκλοφορούν στο διαδίκτυο, προστατεύοντας συγχρόνως την ιδιωτικότητα.
7. GPG :Το Pretty Good Privacy (PGP) είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας για λειτουργικά συστήματα όπως τα MS DOS, Unix, VAX/VMS και για άλλες πλατφόρμες, ενώ επιτρέπει την ανταλλαγή αρχείων και μηνυμάτων διασφαλίζοντας το απόρρητο και την ταυτότητα σε συνδυασμό με την ευκολία λειτουργίας.Το GNU Privacy Guard (GnuPG ή GPG) είναι το ανοικτού κώδικα λογισμικό για κρυπτογράφηση και αποκρυπτογράφηση δεδομένων, όπως ακριβώς το PGP.
8. Cryptocat :Το Cryptocat είναι μία chat υπηρεσία στην οποία οι συνομιλίες κρυπτογραφούνται, με την διαθέσιμη εφαρμογή να μπορεί να εγκατασταθεί σε Mac, καθώς και ως πρόσθετο στον browser.
9. Wickr :Το Wickr θα μπορούσε να χαρακτηριστεί ως το "Snapchat για μεγάλους". Όπως ακριβώς συμβαίνει με τη δημοφιλής εφαρμογή, το Wickr στέλνει μηνύματα κειμένου, φωτογραφιών και βίντεο τα οποία "αυτοκαταστρέφονται", ενώ παράλληλα κρυπτογραφούνται.
10. Signal και RedPhone :Τα Signal και RedPhone είναι αντιστοίχως δύο εφαρμογές για iPhone και Android smartphones, που κρυπτογραφούν τις κλήσεις, ενώ η εταιρία πίσω από τις εφαρμογές (Open Whisper Systems), έχει δεχτεί εγκωμιαστικά σχόλια από τον Edward Snowden.

4. ΚΕΦΑΛΑΙΟ 4: Διάφορα Λογισμικά

4.1. VIDALIA(Λογισμικό)



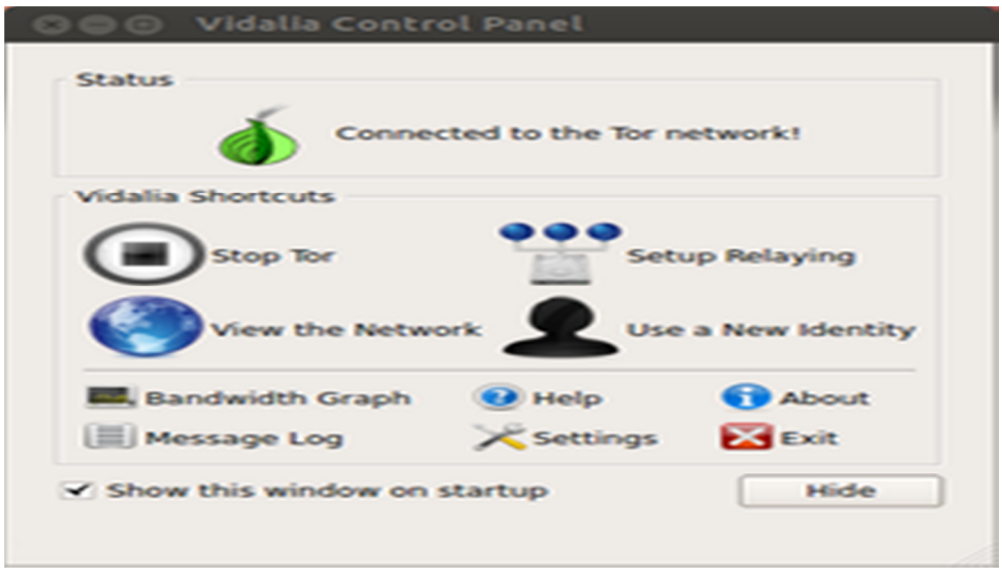
Εικόνα 19: Vidalia

Το Vidalia είναι μια διακοπή cross-platform GUI για τον έλεγχο του Tor , που χτίστηκε χρησιμοποιώντας Qt . Επιτρέπει στον χρήστη να ξεκινήσει, να σταματήσει ή να δεί την κατάσταση του Tor, και να ρυθμίσει ορισμένες πτυχές του.

Το Vidalia το καθιστά επίσης ευκολότερο να στο να συνεισφέρει στο δίκτυο βοηθώντας τον χρήστη να δημιουργήσει ένα ρελέ Tor.

Ένα άλλο σημαντικό χαρακτηριστικό του Vidalia είναι ο Tor χάρτης του δικτύου της, ο οποίος επιτρέπει στο χρήστη να δει τη γεωγραφική θέση του ρελέ στο δίκτυο Tor.

Τρέχει σε οποιαδήποτε πλατφόρμα υποστηρίζεται από Qt 4.2, συμπεριλαμβανομένων των Windows , Mac OS X και Linux ή άλλα Unix-like παραλλαγές χρησιμοποιώντας το X11 σύστημα παραθύρων.



Εικόνα 20: Vidalia control panel

4.2. Peer-to-Peer Ανταλλαγή Αρχείων

Το Peer-to-peer ανταλλαγή αρχείων είναι η διανομή και ανταλλαγή ψηφιακών μέσων χρησιμοποιώντας peer-to-peer (P2P) τεχνολογία δικτύωσης. Το P2Pε είναι επίσης η κοινή χρήση αρχείων που επιτρέπει στους χρήστες να έχουν πρόσβαση σε αρχεία πολυμέσων, όπως βιβλία, μουσική, ταινίες και παιχνίδια χρησιμοποιώντας ένα πρόγραμμα λογισμικού P2P που ψάχνει για άλλους συνδεδεμένους υπολογιστές σε ένα δίκτυο P2P για να εντοπίσετε το επιθυμητό περιεχόμενο. Οι κόμβοι τέτοιων δικτύων είναι οι υπολογιστές των τελικών χρηστών και servers διανομής.

Το Peer-to-peer έχει εξελιχθεί μέσα από διάφορα στάδια σχεδιασμού από τις αρχές της δεκαετίας , το οποίο διέδωσε την τεχνολογία, στα τελευταία μοντέλα όπως το BitTorrent πρωτόκολλο. Η Microsoft χρησιμοποιεί για τη διανομή Update (Windows 10) και σε απευθείας σύνδεση παίζοντας παιχνίδια (π.χ. το MMORPG Skyforge) χρησιμοποιούν ως δίκτυο διανομής περιεχομένου τους για τη λήψη μεγάλων ποσοτήτων δεδομένων.

Διάφοροι παράγοντες συνέβαλαν στην ευρεία υιοθέτηση και την διευκόλυνση των peer-to-peer ανταλλαγής αρχείων. Αυτές περιλάμβαναν αύξηση του εύρους ζώνης του Διαδικτύου, η ευρεία ψηφιοποίηση των φυσικών μέσων ενημέρωσης, και οι αυξανόμενες δυνατότητες των κατοικιών τους προσωπικούς υπολογιστές. Οι χρήστες ήταν σε θέση να μεταφέρουν ένα ή περισσότερα αρχεία από έναν υπολογιστή σε έναν άλλο μέσω του Internet μέσω διαφόρων μεταφορά αρχείων συστημάτων και άλλων δικτύων file-sharing.

Το Peer-to-peer ανταλλαγή αρχείων έγινε δημοφιλής το 1999 με την εισαγωγή του Napster , μια εφαρμογή ανταλλαγής αρχείων και μια σειρά κεντρικών servers που συνδέονται με τους ανθρώπους που είχαν τα αρχεία με όσους ζήτησαν αρχεία. Ο κεντρικός διακομιστής δείκτης αναπροσαρμόζονται οι χρήστες και μοιράζονται το περιεχόμενό τους. Όταν κάποιος έψαξε για ένα αρχείο, ο διακομιστής έψαξε όλα τα διαθέσιμα αντίγραφα αυτού του αρχείου και τους παρουσιάζεται στο χρήστη. Τα αρχεία θα πρέπει να μεταφέρονται απευθείας μεταξύ των δύο ιδιωτικούς υπολογιστές. Ένας περιορισμός ήταν ότι μόνο αρχεία μουσικής θα μπορούσε να μοιραστεί. [3] Επειδή η διαδικασία αυτή συνέβη σε έναν κεντρικό server, ωστόσο, το Napster είχε θεωρηθεί υπεύθυνη για παραβίαση πνευματικών δικαιωμάτων και να κλείσουν τον Ιούλιο του 2001. Αργότερα άνοιξε εκ νέου ως υπηρεσία συνδρομητικής.

Μετά Napster έκλεισε, οι πιο δημοφιλείς peer-to-peer υπηρεσιών ήταν Gnutella και Kazaa . Οι υπηρεσίες αυτές επέτρεψαν επίσης στους χρήστες να κατεβάσετε τα αρχεία, εκτός από τη μουσική, όπως ταινίες και παιχνίδια. [3]

Το Peer-to-peer ανταλλαγή αρχείων είναι επίσης αποτελεσματικό από άποψη κόστους. Τα γενικά έξοδα διαχείρισης του συστήματος είναι μικρότερη, επειδή ο χρήστης είναι ο πάροχος και συνήθως ο πάροχος είναι ο διαχειριστής, καθώς και. Επομένως, κάθε δίκτυο μπορεί να παρακολουθείται από τους ίδιους τους χρήστες. Την ίδια στιγμή, οι μεγάλες servers μερικές φορές απαιτούν περισσότερο χώρο αποθήκευσης και αυτό αυξάνει το κόστος, δεδομένου ότι η αποθήκευση θα πρέπει να ενοικιάζονται ή αγοράζονται αποκλειστικά για ένα διακομιστή. Ωστόσο, συνήθως peer-to-peer ανταλλαγή αρχείων δεν απαιτεί ένα ειδικό server .

Για να έχουν εξέχοντα ρόλο στην peer to peer τα δίκτυα και οι εφαρμογές, όπως το BitTorrent, Gnutella ή DC ++, υπάρχουν διάφορα στοιχεία που συμβάλλουν στη διαμόρφωση, την ανάπτυξη και τη σταθερότητα αυτών, τα οποία περιλαμβάνουν τα συμφέροντα, τα χαρακτηριστικά των χρηστών, τη μείωση του κόστους, τα κίνητρα των χρηστών και τη διάσταση της κοινότητας. Με ρητές αξίες, οι χρήστες δεν εκφράζουν άμεσα τις πληροφορίες για τον εαυτό τους, αν και, είναι ακόμα δυνατό να βρείτε πληροφορίες σχετικά με το συγκεκριμένο χρήστη από την αποκάλυψη του και την έρευνα που έχει διεξαχθεί σε ένα δίκτυο P2P.

Τα ιδιωτικά peer-to-peer (P2P) κάνουν χρήση ενός κεντρικού εξυπηρετητή, όπως ένα Direct Connect κόμβο για τον έλεγχο ταυτότητας των πελατών. Εναλλακτικά, οι χρήστες μπορούν να ανταλλάσσουν κωδικούς πρόσβασης ή κρυπτογραφικά κλειδιά με φίλους για να σχηματίσουν ένα αποκεντρωμένο δίκτυο. Τα ιδιωτικά peer-to-peer συστήματα μπορούν να χωριστούν σε F2F και τα συστήματα της ομάδας που βασίζεται. Τα F2F συστήματα επιτρέπουν μόνο τις συνδέσεις μεταξύ των χρηστών που γνωρίζουν ο ένας τον άλλο, αλλά μπορεί επίσης να παρέχει την αυτόματη ανώνυμία προώθησης. Συστήματα που βασίζονται σε αυτά επιτρέπουν σε κάθε χρήστη να συνδεθεί με οποιοδήποτε άλλο σύστημα, χωρίς να διακυβεύεται η προστασία της ιδιωτικής ζωής των χρηστών τους.

4.2.1. Ταξινόμηση χρήστη

Οι χρήστες που συμμετέχουν σε συστήματα P2P μπορούν να ταξινομηθούν με διάφορους τρόπους. Οι χρήστες μπορούν να ταξινομηθούν ανάλογα με τη συμμετοχή τους στο σύστημα P2P. Υπάρχουν πέντε τύποι χρηστών:

-Οι χρήστες που δημιουργούν τις υπηρεσίες,

-Οι χρήστες που χρησιμοποιούν τις υπηρεσίες,

-Οι χρήστες που διευκολύνουν την αναζήτηση,

-Οι χρήστες που επιτρέπουν την επικοινωνία,

-Και οι χρήστες οι οποίοι είναι συνεργάσιμοι.

Στην πρώτη περίπτωση, ο χρήστης δημιουργεί νέες πόρους ή υπηρεσίες, και να τους προσφέρει στην κοινότητα. Στη δεύτερη περίπτωση, ο χρήστης παρέχει στην κοινότητα με το χώρο στο δίσκο "για την αποθήκευση αρχείων για downloads" ή με "υπολογιστικών πόρων" για να διευκολυνθεί μια υπηρεσία που παρέχεται από άλλο χρήστη. Στο τρίτο, ο χρήστης παρέχει μια λίστα των σχέσεων για να βοηθήσουν άλλους χρήστες να βρουν συγκεκριμένα αρχεία ή υπηρεσίες. Στο τέταρτο, ο χρήστης συμμετέχει ενεργά στο «πρωτόκολλο του δικτύου», συμβάλλοντας στη διατήρηση του δικτύου από κοινού. Στην τελευταία περίπτωση, ο χρήστης δεν συμβάλλει στο δίκτυο, κατεβάζει ό, τι αυτός ή αυτή χρειάζεται, αλλά πηγαίνει αμέσως offline.

4.2.2. Παρακολούθηση

Καθώς η χρήση του Διαδικτύου ως εργαλείο για να αντιγράψετε και να μοιράζονται διάφορα αρχεία, ιδίως των πνευματικών δικαιωμάτων μουσικής, οι εταιρείες έχουν προσπαθήσει για την καταπολέμηση αυτού. Η ένωση βιομηχανίας καταγραφής της Αμερικής (RIAA) έχει δραστηριοποιηθεί στην προσπάθεια να οδηγήσει εκστρατείες κατά των παραβατών. Οι αγωγές έχουν κινηθεί εναντίον ιδιωτών, καθώς και προγράμματα όπως το Napster , προκειμένου να «προστατεύσουν» τους ιδιοκτήτες των πνευματικών δικαιωμάτων. Μια από τις πιο πρόσφατες προσπάθειες της RIAA ήταν να δημιουργήσουν χρήστες δόλωμα για να παρακολουθούν τη χρήση των πνευματικών δικαιωμάτων του υλικού από πρώτο χέρι.

Αυτό είναι δυνατό επειδή το δόλωμα χρήστης προσπαθεί να κατεβάσει το ίδιο αρχείο και μια λίστα με όλες τις «πηγές» που χρησιμοποιήθηκαν. Αυτές οι λίστες στέλνονται μέσω μιας διαδικασίας αναζήτησης ιδιοκτήτη, μετά από αυτό, ο κάτοχος των πνευματικών δικαιωμάτων γνωρίζει τον αρμόδιο ISP. Μετά από αυτή την κατάσταση εξαρτάται, σε ορισμένα κράτη ανεπίσημες επιστολές με τη σφραγίδα του χρόνου και IP είναι επαρκής και σε άλλους χρειάζεται ένας δικαστής.

Μετά από αυτό ο ISP φαίνεται στη βάση δεδομένων του (εάν απαιτείται από το νόμο) και επιστρέφει τη διεύθυνση του πελάτη, η οποία κατεβάσει το παράνομο περιεχόμενο. Αυτή η διαδικασία είναι ανοιχτή σε κατάχρηση, όπως ένας δικηγόρος απλά θα μπορούσε να πάρετε μια λίστα με τις διευθύνσεις IP και γραμματόσημα χρόνο από όλους τους επισκέπτες της διαφήμισης ή στην ιστοσελίδα του και να το χρησιμοποιήσετε για να προσποιηθεί τη λήψη της παράνομης μουσικής

4.2.3. Πνευματικά Δικαιώματα

Η πράξη της ανταλλαγής αρχείων δεν είναι παράνομη και τα peer-to-peer δίκτυα που χρησιμοποιούνται είναι για νομικούς σκοπούς. Τα νομικά ζητήματα ανταλλαγής αρχείων συνεπάγονται με την παραβίαση των νόμων της αντιγραφής αρχείων κ ιδιωτηκότητας. Οι περισσότερες συζητήσεις σχετικά με τη νομιμότητα της ανταλλαγής αρχείων είναι αποκλειστικά δικαιώματα πνευματικής ιδιοκτησίας.

Πολλές χώρες έχουν δίκαιη χρήση που επιτρέπουν την περιορισμένη χρήση του υλικού με πνευματικά δικαιώματα χωρίς να έχουν αποκτήσει την άδεια από τους κατόχους των δικαιωμάτων. Αυτά τα έγγραφα περιλαμβάνουν σχόλια, ειδήσεις, έρευνα και υποτροφία. Οι Νόμοι περί πνευματικής ιδιοκτησίας δεν εκτείνονται πέρα από την επικράτεια ενός συγκεκριμένου κράτους, εκτός εάν το εν λόγω κράτος είναι σε διεθνή συμφωνία. Οι περισσότερες χώρες σήμερα είναι συμβαλλόμενες σε τουλάχιστον μία τέτοια συμφωνία.

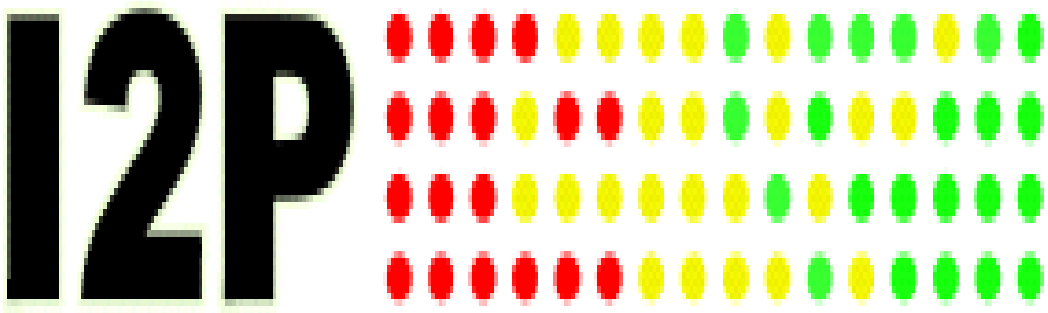
Στον τομέα της προστασίας της ιδιωτικής ζωής, οι πρόσφατες δικαστικές αποφάσεις φαίνεται να δείχνουν ότι μπορεί να υπάρχει προσδοκία της ιδιωτικής ζωής στα δεδομένα που εκτίθενται μέσω δικτύων ανταλλαγής αρχείων peer-to-peer. Σε μια απόφαση 39 σελίδων που κυκλοφόρησε 8, Νοέμ, 2013, το Περιφερειακό Δικαστήριο των ΗΠΑ αρνήθηκε την πρόταση να στείλει στοιχεία που συγκεντρώθηκαν από τις αρχές χωρίς ένταλμα έρευνας μέσω ενός αυτοματοποιημένου εργαλείου αναζήτησης peer-to-peer.

4.2.4. Ανώνυμος P2P

Ένα ανώνυμο P2P σύστημα επικοινωνίας είναι ένα peer-to-peer κατανεμημένης εφαρμογής στο οποίο οι κόμβοι ή οι συμμετέχοντες είναι ανώνυμοι ή χρησιμοποιούν ψευδώνυμα . Η ανωνυμία των συμμετεχόντων επιτυγχάνεται συνήθως με ειδική δρομολόγησης δικτύων επικάλυψης που κρύβουν τη φυσική θέση του κάθε κόμβου από άλλους συμμετέχοντες.

Το ενδιαφέρον για τα P2P συστήματα έχει αυξηθεί τα τελευταία χρόνια για πολλούς λόγους, που κυμαίνονται από την επιθυμία να μοιράζονται αρχεία χωρίς να αποκαλυφθεί η ταυτότητα του δικτύου τους και να διακινδυνεύετε η άσκηση της προσφυγής για να δυσπιστούν στις κυβερνήσεις, τις ανησυχίες σχετικά με την επιτήρηση της μάζας και τη διατήρηση των δεδομένων , καθώς και αγωγές εναντίον των bloggers .

4.3. I2P



Εικόνα 21: I2P

Το I2P (Invisible Internet Project) είναι ένα Peer To Peer δίκτυο που χρησιμοποιείται για ανωνυμία και ασφάλεια στο Διαδίκτυο, προσφέροντας ένα παραπάνω επίπεδο για ασφαλή επικοινωνία μεταξύ διαφόρων εφαρμογών. Για τη χρήση του συνοδεύεται από ειδικό λογισμικό το οποίο είναι ανοιχτού κώδικα και δωρεάν. Πρόκειται για ένα ανώνυμο, κατανεμημένο επίπεδο επικοινωνίας σχεδιασμένο να μπορεί να τρέχει σχεδόν οποιαδήποτε εφαρμογή ανώνυμα στο Διαδίκτυο. Τέτοιες εφαρμογές μπορεί να αφορούν ηλεκτρονική αλληλογραφία, ομότιμα (Peer-2-Peer) δίκτυα, συνομιλίες IRC, πλοήγηση σε ιστοσελίδες και άλλες εφαρμογές. Το λογισμικό που υλοποιεί αυτό το στρώμα ονομάζεται *I2P router* και ένας υπολογιστής που εκτελεί το I2P δίκτυο ονομάζεται *I2P κόμβος* .

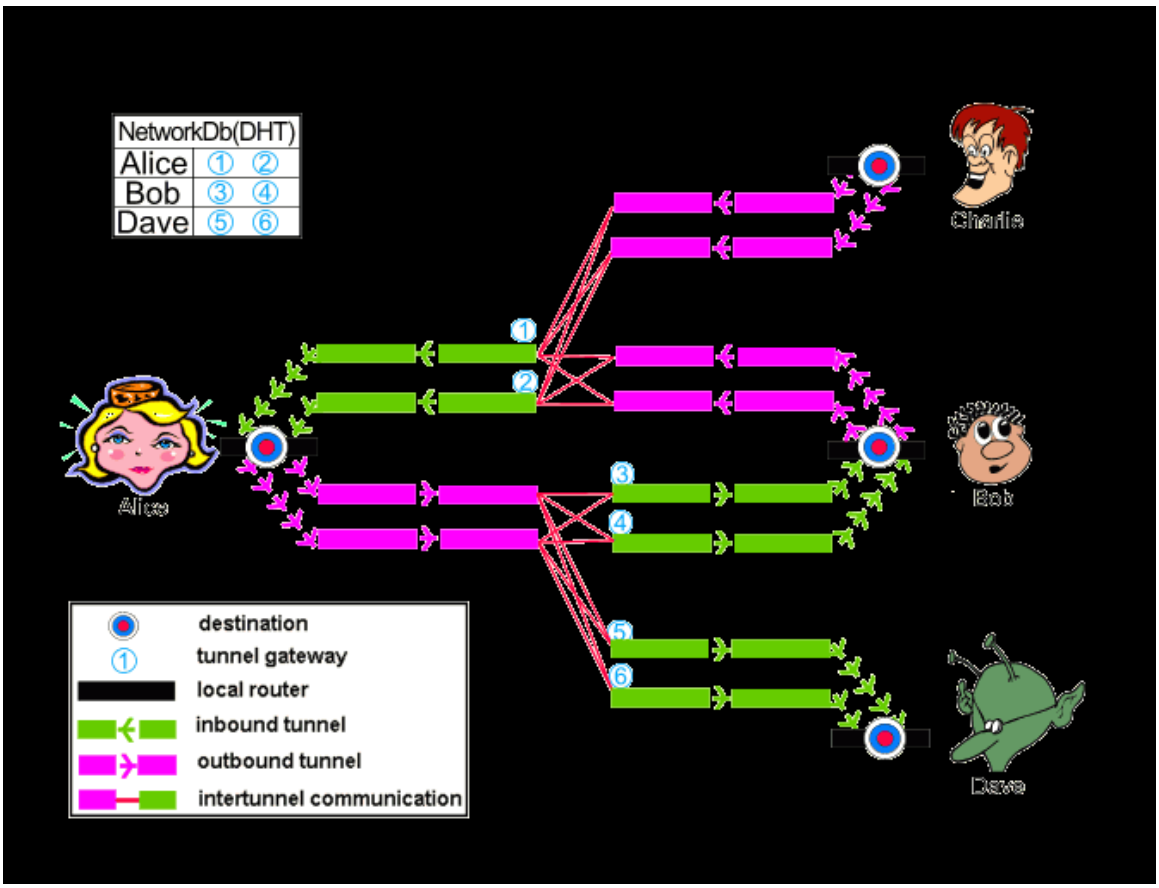
Το I2P βρίσκεται στην έκδοση beta από το 2003. Οι προγραμματιστές τονίζουν ότι είναι πιθανό να υπάρχουν σφάλματα στο λογισμικό και ότι υπήρξε ανεπαρκής ακαδημαϊκή κριτική. Ωστόσο, πιστεύουν ότι ο κώδικας είναι πλέον εύλογα σταθερός και καλά ανεπτυγμένος, και η έκθεση του μπορεί να βοηθήσει στην ανάπτυξη της I2P.

Το δίκτυο είναι "μηνυματοστραφές" - είναι ουσιαστικά ένα ασφαλές και ανώνυμο επίπεδο IP, όπου τα μηνύματα απευθύνονται σε κρυπτογραφικά κλειδιά (Προορισμοί) και μπορεί να είναι αρκετά μεγαλύτερα από τα IP πακέτα. Κάποια παραδείγματα χρήσης του δικτύου περιλαμβάνουν τα "eepsites" (εξυπηρετητές ιστού που φιλοξενούν κανονικές διαδικτυακές εφαρμογές μέσα στο I2P), μία εφαρμογή-πελάτη για το BitTorrent ("I2PSnark"), ή μία κατανεμημένη αποθήκη δεδομένων. Με τη βοήθεια της εφαρμογής I2PTunnel, είμαστε ικανοί για μία παραδοσιακή TCP/IP επικοινωνία πάνω από το I2P, όπως το SSH, IRC, ένα squid proxy ακόμα και streaming ήχου. Οι περισσότεροι άνθρωποι δεν θα χρησιμοποιήσουν το I2P ευθέως, ή ακόμα δεν χρειάζεται να ξέρουν ότι το χρησιμοποιούν. Αντιθέτως αυτό που θα βλέπουν, θα είναι μία από τις I2P εφαρμογές, ή ίσως κάποια εφαρμογή διαχείρισης που θα τους επιτρέπει να ανοίξουν και να κλείσουν κάποιους proxies που τους παρέχουν ανωνυμία.

Εν αντιθέσει με άλλα ανώνυμα δίκτυα, το I2P δεν προσπαθεί να παρέχει ανωνυμία κρύβοντας τον αποστολέα ενός μηνύματος αλλά όχι τον παραλήπτη, και αντίστροφα. Το I2P έχει σχεδιαστεί ώστε να επιτρέπει σε κόμβους που χρησιμοποιούν το I2P να επικοινωνούν μεταξύ τους ανώνυμα — και ο αποστολέας και ο παραλήπτης είναι μη αναγνωρίσιμοι μεταξύ τους αλλά και σε τρίτους. Για παράδειγμα, σήμερα υπάρχουν και ιστοσελίδες μέσα στο I2P (επιτρέποντας ανώνυμη δημοσίευση / φιλοξενία) καθώς και HTTP proxies για το κανονικό Internet (επιτρέποντας ανώνυμη περιήγηση στο διαδίκτυο). Η δυνατότητα να τρέχετε εξυπηρετητές μέσα στο I2P είναι απαραίτητη, καθώς είναι πολύ πιθανό κάποια outbound proxies για το κανονικό Internet να παρακολουθούνται, να είναι απενεργοποιημένα ή να έχουν παραβιαστεί με σκοπό κάποια επίθεση.

-Λειτουργεία I2P

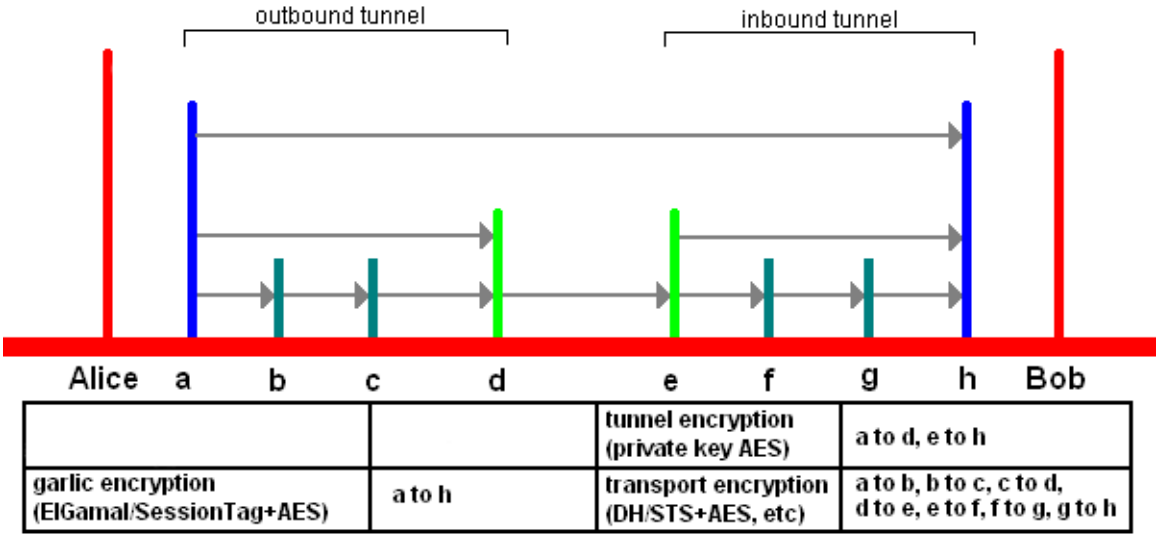
Το δίκτυο με μια ματιά αποτελείται από ένα πακέτο από κόμβους ("routers") με έναν αριθμό από μονής κατεύθυνσης inbound και outbound εικονικά μονοπάτια ("tunnels"). Κάθε router αναγνωρίζεται από μία κρυπτογραφική ταυτότητα (RouterIdentity) που συνήθως έχει μεγάλη διάρκεια ζωής. Αυτοί οι routers επικοινωνούν μεταξύ τους μέσω υπαρχόντων μηχανισμών μεταφοράς (TCP, UDP, κτλ), ανταλλάσσοντας διάφορα μηνύματα. Οι εφαρμογές πελάτη έχουν τα δικά τους κρυπτογραφικά αναγνωριστικά ("Destination") που τους επιτρέπουν να στέλνουν και να λαμβάνουν μηνύματα. Αυτές οι εφαρμογές-πελάτες μπορούν να συνδεθούν σε οποιοδήποτε router και να εξουσιοδοτηθούν για προσωρινή δέσμευση ("lease") μερικών tunnels που θα χρησιμοποιηθούν για την αποστολή και παραλαβή μηνυμάτων στο δίκτυο. Το I2P έχει τη δικιά του εσωτερική δικτυακή βάση δεδομένων (χρησιμοποιώντας μια παραλλαγή του αλγορίθμου Kademlia) για την ασφαλή κατανεμημένη δρομολόγηση και εύρεση στοιχείων επικοινωνίας.



Εικόνα 22: Λειτουργία I2P

Παραπάνω, η Alice, ο Bob, ο Charlie και ο Dave τρέχουν routers με μοναδικό Προορισμό στο τοπικό τους router. Όλοι τους έχουν ένα ζευγάρι από 2-hop inbound tunnels για κάθε προορισμό (σημειώνονται ως 1, 2, 3, 4, 5 και 6). Επίσης εμφανίζεται ένα μικρό μέρος από τα 2-hop outbound tunnels από τα router κάθε χρήστη. Χάριν απλότητας, τα inbound tunnels του Charlie και τα outbound tunnels του Dave δεν εμφανίζονται, ούτε τα διαθέσιμα outbound tunnels των υπολοίπων routers (συνήθως εφοδιασμένα με μερικά tunnels τη φορά). Όταν η Alice και ο Bob μιλάνε μεταξύ τους, η Alice στέλνει ένα μήνυμα από τα (ροζ) outbound tunnels της που επικοινωνούν με ένα από τα (πράσινα) inbound tunnels του Bob (tunnel 3 ή 4). Γνωρίζει σε ποιο από όλα τα tunnels του router να το στείλει ρωτώντας τη δικτυακή βάση δεδομένων, που είναι συνεχώς ενημερωμένη καθώς νέα leases εξουσιοδοτούνται και παλιά λήγουν.

Εάν ο Bob θέλει να απαντήσει στην Alice, ακολουθάει πάλι την ίδια διαδικασία - στέλνει ένα μήνυμα από ένα από τα outbound tunnels του που επικοινωνούν με ένα από τα inbound tunnels της Alice (tunnel 1 ή 2). Για να γίνουν πιο εύκολα τα πράγματα, τα περισσότερα μηνύματα μεταξύ της Alice και του Bob είναι garlic wrapped, έχοντας τις τωρινές lease πληροφορίες του αποστολέα έτσι ώστε ο αποδέκτης να μπορεί να απαντήσει αμέσως χωρίς να χρειάζεται να κοιτάξει στη δικτυακή βάση δεδομένων για τις τωρινές πληροφορίες.



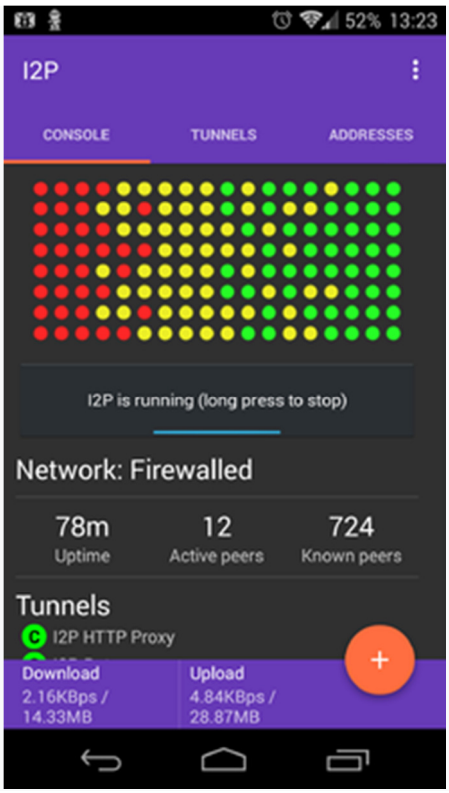
Εικόνα 23: Η κρυπτογραφία του παραδείγματος

Το περιεχόμενο που στέλνεται στο I2P κρυπτογραφείται από τρία επίπεδα garlic κρυπτογράφησης (χρησιμοποιείται για την πιστοποίηση της αποστολής του μηνύματος στον παραλήπτη), tunnel κρυπτογράφησης (όλα τα μηνύματα που περνάνε μέσα από ένα tunnel κρυπτογραφούνται από το gateway μέχρι το τέλος του tunnel) και κρυπτογράφηση μέσα στο router από το επίπεδο μεταφοράς (π.χ. το TCP επίπεδο μεταφοράς χρησιμοποιεί AES256 με εφήμερα κλειδιά). Για να αντιμετωπιστεί μία ευρεία γκάμα επιθέσεων, το I2P είναι πλήρως κατανεμημένο χωρίς κεντρικούς πόρους - συνεπώς δεν υπάρχει κάποια κεντρική υπηρεσία που να κρατάει στατιστικά για την απόδοση και την αξιοπιστία των routers στο δίκτυο. Επομένως, κάθε router θα πρέπει να διατηρεί προφίλ διάφορων routers και είναι υπεύθυνο για την επιλογή των κατάλληλων κόμβων για να επιτύχει την ανωνυμία, την απόδοση και την αξιοπιστία που χρειάζονται οι χρήστες

4.4. Δρομολογητές

I2PBerry είναι μια διανομή Linux που μπορεί να χρησιμοποιηθεί ως router για την κρυπτογράφηση και την κυκλοφορία του δικτύου διαδρομή μέσω του δικτύου I2P.

4.5. Android



Εικόνα 24: Το I2P στα Android

- Μπορεί να βρεθεί στο Play Google store στο πλαίσιο του έργου Λύσεις Απορρήτου του Google Play ή για ένα F-Droid
- *Nightweb* είναι μια εφαρμογή Android που χρησιμοποιεί I2P και Bittorrent και μοιράζονται θέσεις blog, φωτογραφίες και άλλο παρόμοιο περιεχόμενο.

Εικόνα 25: Η μασκότ του I2P, κάλυψη

4.5.1. EepProxy

Το πρόγραμμα EepProxy χειρίζεται όλη την επικοινωνία μεταξύ του browser και κάθε eepsite. Λειτουργεί ως ένας διακομιστής μεσολάβησης που μπορεί να χρησιμοποιηθεί από οποιοδήποτε πρόγραμμα περιήγησης στο web .

4.5.2. Peers, κόμβοι I2P

Άλλες μηχανές που χρησιμοποιούν I2P που είναι συνδεδεμένες με μια μηχανή του χρήστη εντός του δικτύου. Κάθε μηχάνημα μέσα στο δίκτυο συμμερίζεται την δρομολόγηση και προώθει τα κρυπτογραφημένα πακέτα.

4.5.3. Σήραγγες

Κάθε δέκα λεπτά, μια σύνδεση μεταξύ υπολογιστή χρήστη και ενός άλλου του ίδιου δικτύου, στέλνονται κρυπτογραφημένα μυνήματα μέσα από «σήραγγες». Δεδομένα από και προς τον χρήστη, μαζί με τα στοιχεία για άλλους χρήστες δρομολογούνται μέσω του υπολογιστή, περνάνε μέσα από αυτές τις σήραγγες και προωθούνται στον τελικό προορισμό τους.

5. ΚΕΦΑΛΑΙΟ 5: HTTP(Σήραγγα)-HTTPS-HTTP Cookies (Γενικά)

5.1. HTTPS(Σήραγγα)

Η HTTP διάνοιξη σηράγγων είναι μια τεχνική με την οποία η επικοινωνία εκτελείται χρησιμοποιώντας διάφορα δίκτυα και πρωτόκολλα ενθυλακώνοντας το HTTP πρωτόκολλο, τα πρωτόκολλα δικτύου συνήθως ανήκουν στον / TCP IP . Ως εκ τούτου, το πρωτόκολλο HTTP λειτουργεί ως περιτύλιγμα για ένα κανάλι. Το ρεύμα HTTP με το συγκαλυμμένο κανάλι ονομάζεται σήραγγα HTTP.

Το λογισμικό HTTP σήραγγα αποτελείται από client-server εφαρμογών HTTP tunneling που ενσωματώνονται με το υπάρχον λογισμικό εφαρμογής, που τους επιτρέπει να χρησιμοποιούνται σε συνθήκες περιορισμένης σύνδεσης με το δίκτυο, συμπεριλαμβανομένων τοίχος προστασίας δικτύων, δικτύων πίσω από proxy servers, καθώς και μετάφραση διευθύνσεων δικτύου.

Μια σήραγγα HTTP συχνά χρησιμοποιείται ως μέσο για την επικοινωνία από τοποθεσίες του δικτύου με περιορισμένη συνδεσιμότητα. Τις περισσότερες φορές πίσω από NAT , firewalls ή εξυπηρετητές proxy και τις περισσότερες φορές με εφαρμογές που δεν έχουν εγγενή υποστήριξη για την επικοινωνία σε τέτοιες συνθήκες περιορισμένης σύνδεσης. Περιορισμένη συνδεσιμότητα με τη μορφή TCP / IP, μπλοκάρουν την κυκλοφορία έξω από το δίκτυο, ή το κλειδώνουν όλα τα πρωτόκολλα δικτύου εκτός από μερικά.

5.2. HTTP cookies

Cookies HTTP είναι οι συμβολοσειρές κειμένου που αποθηκεύονται σε έναν υπολογιστή όταν ο χρήστης περιηγείται σε διαφορετικές ιστοσελίδες. Τα cookies αποθηκεύουν μικρά κομμάτια των πληροφοριών, όπως κωδικούς πρόσβασης. Οι πληροφορίες αυτές αποστέλλονται στον υπολογιστή του χρήστη και στη συνέχεια αποστέλλονται σε βάσεις δεδομένων web χωρίς την έγκριση του χρήστη. Τα cookies αποτελούν μια άλλη οδός με την οποία μπορεί να παραβιαστεί η ανωνυμία του χρήστη. Ένα HTTP cookies είναι ένα μικρό κομμάτι δεδομένων που αποστέλλονται από μια ιστοσελίδα και αποθηκεύονται στον υπολογιστή του χρήστη από τον χρήστη web browser. Τα cookies έχουν σχεδιαστεί για να καταγράφει τη δραστηριότητα περιήγησής του χρήστη. Μπορούν επίσης να χρησιμοποιηθούν για να θυμούνται κομμάτια των πληροφοριών που ο χρήστης έχει εγγραφεί προηγουμένως, όπως ονόματα, διευθύνσεις, κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.

Εξατομίκευση

Τα cookies μπορούν να χρησιμοποιηθούν για να θυμούνται πληροφορίες για τον χρήστη, προκειμένου να δείξουν το σχετικό περιεχόμενο στην πάροδο του χρόνου. Για παράδειγμα, ένας web server μπορεί να στείλει ένα cookie που περιέχει το όνομα χρήστη που χρησιμοποιείται τελευταία για να συνδεθείτε σε μια ιστοσελίδα, έτσι ώστε να μπορεί να συμπληρωθεί αυτόματα την επόμενη φορά που ο χρήστης ξανά συνδέεται.

Πολλές ιστοσελίδες χρησιμοποιούν cookies για την εξατομίκευση με βάση τις προτιμήσεις του χρήστη. Οι χρήστες επιλέγουν τις προτιμήσεις τους με την εισαγωγή τους σε μια ηλεκτρονική φόρμα και την υποβολή της φόρμας στο διακομιστή. Ο διακομιστής κωδικοποιεί τις προτιμήσεις σε ένα cookie και στέλνει το cookie πίσω στο πρόγραμμα περιήγησης. Με αυτό τον τρόπο, κάθε φορά που ο χρήστης αποκτά πρόσβαση σε μια σελίδα στον ιστότοπο, ο διακομιστής μπορεί να προσαρμόζει τη σελίδα ανάλογα με τις προτιμήσεις του χρήστη.

Για παράδειγμα, το Google χρησιμοποιεί μια φορά cookies για να επιτρέψει στους χρήστες για να αποφασίσει πόσα αποτελέσματα αναζήτησης ανά σελίδα ήθελαν να δουν. Επίσης,το DuckDuckGo χρησιμοποιεί cookies για να επιτρέπει στους χρήστες να ρυθμίζουν τις προτιμήσεις θέασης, όπως τα χρώματα της ιστοσελίδας.

Εικόνα 26: Web browser

Μια πιθανή αλληλεπίδραση μεταξύ ενός web browser και ένα web server που κατέχουν μια ιστοσελίδα στην οποία ο διακομιστής στέλνει ένα cookie στο πρόγραμμα περιήγησης και το πρόγραμμα περιήγησης στέλνει πίσω όταν ζητούν μια άλλη σελίδα.

5.3. HTTP

Το πρωτόκολλο HTTP περιλαμβάνει τον βασικό έλεγχο ταυτότητας πρόσβασης το οποίο επιτρέπει την πρόσβαση σε μια ιστοσελίδα μόνο όταν ο χρήστης έχει δώσει το σωστό όνομα χρήστη και κωδικό πρόσβασης. Εάν ο διακομιστής απαιτεί τέτοια διαπιστευτήρια για την παροχή πρόσβασης σε μια ιστοσελίδα, ο browser του ζητά και όταν αποκτηθεί τους στέλνει σε κάθε σελίδα. Αυτή η πληροφορία μπορεί να χρησιμοποιηθεί για να παρακολουθείτε το χρήστη.

5.3.1. Διεύθυνση IP

Ορισμένοι χρήστες μπορούν να παρακολουθούνται με βάση τη διεύθυνση IP του υπολογιστή που ζητούν τη σελίδα. Ο διακομιστής γνωρίζει τη IP του υπολογιστή που τρέχει το πρόγραμμα περιήγησης (ή του πληρεξουσίου , εφόσον χρησιμοποιείται) και θεωρητικά θα μπορούσε να συνδέθεί.

Ωστόσο, οι διευθύνσεις IP δεν είναι γενικά ένας αξιόπιστος τρόπος για τον εντοπισμό ενός χρήστη. Πολλοί υπολογιστές έχουν σχεδιαστεί για να χρησιμοποιηθούν από έναν μόνο χρήστη, όπως υπολογιστές γραφείο ή του σπιτιού. Αυτό σημαίνει ότι πολλοί υπολογιστές θα μοιράζονται μια δημόσια διεύθυνση IP. Επιπλέον, ορισμένα συστήματα, όπως το Tor , έχουν σχεδιαστεί για να διατηρήσουν την ανωνυμία του Διαδικτύου , καθιστώντας την παρακολούθηση από τη διεύθυνση IP ανέφικτη και αδύνατη.

5.4. HTTP-TOR

Το HTTP είναι ένα πρωτόκολλο κρυπτογράφησης και χρησιμοποιείται για την κρυπτογράφηση του περιεχομένου και το κάνουν δυσανάγνωστο εκτός από το πρόσωπο που τις λαμβάνει. Κρύβει μόνο το περιεχόμενο του μηνύματός μας. Στο δίκτυο TOR χρησιμοποιείται για να κρύψει τη διεύθυνση IP μας, και μπορούμε να χρησιμοποιήσουμε είτε HTTP ή HTTPS πάνω του, θεωρητικά. Η IP μας μπορεί να συναχθεί.

Το κύριο θέμα ευπάθειας του συστήματος TOR είναι η προσέγγιση man-in-the-middle. Δεδομένου ότι ο καθένας μπορεί να προσθέσει ένα διακομιστή στο δίκτυο TOR, είναι προς το συμφέρον της επιβολής του νόμου να θέσει τους δικούς τους servers στο δίκτυο, και να επιτεθεί την κρυπτογράφηση των δεδομένων που περνά μέσα από τους υπολογιστές τους. Πλέον παίρνουν οι IPs των υπολογιστών που συνδέονται με αυτούς. Τέλος, η ασφάλεια HTTP είναι αμφίβολη αυτή τη στιγμή.

Όταν χρησιμοποιούμε HTTPS πάνω TOR:

1. Μπορείτε να χρησιμοποιήσουμε το δημόσιο κλειδί του server για να κρυπτογραφήσουμε το μήνυμά μας.
2. Τότε θα περάσει το μήνυμα HTTPS σε έναν κόμβο TOR,
3. Αυτό μεταφέρεται από τον έναν TOR κόμβο στον άλλο, και στον άλλο και ...
4. Τέλος, ο τελευταίος κόμβος TOR θα στείλει κρυπτογραφημένο μήνυμα HTTPs στον server, η απάντηση είναι κρυπτογραφημένη με αυτό το κλειδί και θα είναι ο μόνος που είναι σε θέση να αποκρυπτογραφήσει την απάντηση από το διακομιστή.

Έτσι, η γραφική παράσταση για την δουλεία αυτή θα πρέπει να είναι ως εξής:

```
---> "Tor message"
===> "HTTPs message"
[T]  "Tor Node"
[S]  "Server"
[U]  "User"

[U]-->[T1]-->[T2]-->[T3]-->...[TN]==>[S]
[S]==>[TN]-->...[T3]-->[T2]-->[T1]-->[U]
```

ή

```
---> "Tor Connection"
===> "HTTPs Connection"
[T]  "Tor Node"
[S]  "Server"
[U]  "User"

[U]-->[T1]-->[T2]-->[T3]-->...[TN]==>[S]
[S]==>[TN]-->...[T3]-->[T2]-->[T1]-->[U]
```

Και όμως ακόμα η επικοινωνία μας θα είναι μυστική.

Θα σημειωθεί ότι το HTTP παρέχει μόνο προστασία στο τελικό στάδιο της σύνδεσης (μεταξύ του κόμβου εξόδου του κυκλώματος Tor και το διακομιστή προορισμού):

- **Οικιακό δίκτυο και ISP:** Το Tor παρέχει ισχυρή κρυπτογράφηση στο δίκτυο. Πιθανοί αντίπαλοι στο οικιακό μας δίκτυο ή τον ISP μας μπορεί να δούν ότι χρησιμοποιούμε Tor, αλλά δεν μπορούν να δουν τις ιστοσελίδες που επισκεπτήκαμε.
- **Το δίκτυο Tor:** Η κίνηση στο δίκτυο Tor έχει πολλαπλά στρώματα κρυπτογράφησης, έτσι ώστε μόνο ο τελευταίος κόμβος (ο κόμβος εξόδου) στο κύκλωμα Tor μπορεί να δει την κίνηση που στέλνουμε στον προορισμό.
- **Ο Κόμβος Έξοδος:** Σε αυτό το σημείο, η κίνηση Tor μπορεί να παρακολουθείται από τον ίδιο τον κόμβο Tor ή ISP αυτού του κόμβου.

5.5. TOR: THE SECOND-GENERATION ONION ROUTER

Σας παρουσιάζουμε το Tor, μια υπηρεσία ανώνυμης επικοινωνίας, βασισμένη σε ένα κύκλωμα χαμηλής καθυστέρησης. Αυτό το Onion routing , δεύτερης γενιάς, θέτει περιορισμούς στον αρχικό σχεδιασμό, προσθέτοντας τέλεια μυστικότητα, έλεγχο συμφόρησης ,υπηρεσίες καταλόγου, ρυθμιζόμενες πολιτικές εξόδου, και ένα πρακτικό σχέδιο για τις , κρυμμένης τοποθεσίας , υπηρεσίες.

Το tor λειτουργεί στον πραγματικό κόσμο του internet, δεν απαιτεί ιδιαίτερα προνόμια ή τροποποιήσεις του πυρήνα , απαιτεί ελάχιστο συγχρονισμό ή συντονισμό μεταξύ των κόμβων, και παρέχει έναν λογικό συμβιβασμό μεταξύ ανωνυμίας, χρηστικότητας και αποτελεσματικότητας.

Σας περιγράφουμε εν συντομία τις εμπειρίες μας μ' ένα διεθνές διαδίκτυο , με περισσότερους από 30 κόμβους. Κλείνουμε με μια λίστα ανοικτών προβλημάτων στην ανώνυμη επικοινωνία.

Επισκόπηση

Το Onion Routing όπως έχουμε προαναφέρει είναι ένα κατανεμημένο δίκτυο επικάλυψης, σχεδιασμένο να κάνει ανώνυμες τις εφαρμογές που είναι βασισμένες στο TCP, όπως το web browsing , το secure shell και το instant messaging. Οι πελάτες επιλέγουν ένα μονοπάτι και διαμορφώνουν ένα κύκλωμα , στο οποίο κάθε κόμβος (ή onion router ή OR) στη διαδρομή αυτή ,γνωρίζει τον προκάτοχο του ή το διάδοχο του , αλλα κανέναν άλλο κόμβο στο κύκλωμα. Τα δεδομένα ρέουν στο κύκλωμα σε κυψέλες σταθερού μεγέθους, οι οποίες αποκρυπτογραφούνται (ξετυλίγονται) από ένα συμμετρικό κλειδί σε κάθε κόμβο (Όπως οι στρώσεις ενός κρεμμυδιού) και συνεχίζουν παρακάτω. Η μελέτη του onion routing έχει δημοσιεύσει αρκετές εργασίες σχεδιασμού και ανάλυσης [27,41,48,49]. Ενώ σύντομα αναπτύχθηκε ένα ευρύ δίκτυο onion routing (κρυπτογραφημένο δίκτυο δρομολόγησης όπου δεν υπάρχει δυνατότητα πρόσβασης στα δεδομένα, ούτε σε περιεχόμενα, ούτε σε προορισμούς (αφορά κυρίως μηνύματα ή πακέτα)) η μοναδική μακροχρόνια δημόσια εκτέλεση (ενεργειών - διενεργειών) ήταν ένα "εύθραυστο" proof of-concept (σύνολο από "εύθραυστες", ακριβής σε αριθμό, και αυστηρές διεργασίες με διαφορετικό σκοπό η κάθε μία) που έτρεχε σε μια μηχανή (Υπολογιστική). Ακόμα και αυτή η απλή ανάπτυξη επεξεργάσθηκε συνδέσεις με ,περισσότερες από 60.000 ξεχωριστές IP διευθύνσεις σε όλο τον κόσμο με αναλογία ,περίπου 50.000 την ημέρα. Αλλά πολλά θέματα κρίσιμου σχεδιασμού και ανάπτυξης δεν επιλύθηκαν, και ο σχεδιασμός δεν αναβαθμίστηκε εδώ και χρόνια. Εδώ σας περιγράφουμε το TOR, ένα πρωτόκολλο για ασύγχρονους ,χαλαρής σύνδεσης onion routers που παρέχει τις ακόλουθες βελτιώσεις στο παλιό σχεδιασμό του Onion Router :

Τέλεια μυστικότητα προς τα εμπρός.

Διαχωρισμός του πρωτόκολλου cleaning από την ανωνυμία.

Αποκλείει τις στρατηγικές mixing, padding ή και τη διαμόρφωση δεδομένων

Πολλά TCP streams μοιράζονται ένα κύκλωμα.

Τοπολογία leaky-pipe του κυκλώματος

Έλεγχος συμφόρησης

Εξυπηρετητές Καταλόγου (directory servers)

Μεταβαλλόμενες πολιτικές εξόδου.

Συνεχόμενους ελέγχους ακεραιότητας: Ο αρχικός σχεδιασμός του onion routing δεν έκανε έλεγχους ακεραιότητας στα δεδομένα. Κάθε κόμβος μπορούσε να αλλάξει το περιεχόμενο στις κυψέλες δεδομένων καθώς περνούσαν. Για παράδειγμα, για να τροποποιήσει-αλλάξει την αίτηση σύνδεσης έτσι ώστε να συνδεθεί σε έναν διαφορετικό web server, ή να επισυνάψει κωδικοποιημένα δεδομένα και να ψάξει για αλλοιωμένα δεδομένα αντίστοιχα στις άκρες του δικτύου. Το tor εμποδίζει αυτές τις επιθέσεις επαληθεύοντας την ακεραιότητα των δεδομένων πριν φύγει από το δίκτυο.

Rendezvous points και το πρωτόκολλο κρυφών υπηρεσιών (hidden services): Το TOR παρέχει έναν ενσωματωμένο μηχανισμό ως πομπό ανωνυμίας μέσω εξυπηρετητών που προστατεύουν τη τοποθεσία.
Σε αντίθεση με το freedom, το tor δεν απαιτεί λογισμικό επιδιόρθωσης του πυρήνα OS (**OS kernel patches**) ή την υποστήριξη στοίβας πρωτόκολλων του δικτύου(network stack support). Αυτό μας εμποδίζει να ανωνυμοποιήσουμε πρωτόκολλα που δεν είναι Ελέγχου Μεταφοράς-TCP (**non-TCP protocols**), αλλά έχει βοηθήσει σε μεγάλο βαθμό τη δυνατότητα φορητότητας και ανάπτυξης μας. Έχουμε εφαρμόσει όλες τις παραπάνω λειτουργίες, συμπεριλαμβάνοντας τα rendezvous points.

Ο πηγαίος κώδικας μας είναι διαθέσιμος , με δωρεάν άδεια χρήσης, και το Tor δεν καλύπτεται από το δίπλωμα ευρεσιτεχνίας που επηρέασε τη κατανομή και τη χρήση των παλαιότερων εκδόσεων του Onion Routing.
Έχουμε αναπτύξει ένα δίκτυο alpha ευρείας περιοχής, για να ελέγξουμε τον σχεδιασμό, να αποκτήσουμε περισσότερη εμπειρία με τη χρηστικότητα και τους χρήστες, καθώς και να παρέχουμε μια ερευνητική πλατφόρμα για πειραματισμό.
Από αυτό το κείμενο , το δίκτυο ανέρχεται σε 32 κόμβους που εκτείνονται σε 2 ηπείρους.

Σχετικές εργασίες (Related Work)

Σύγχρονα συστήματα ανωνυμίας χρονολογούνται από το σχεδιασμό Mix-net του Chaum . Ο Chaum πρότεινε να κρύβει την αλληλογραφία μεταξύ του αποστολέα και του παραλήπτη, κωδικοποιώντας τα μηνύματα σε στρώματα κρυπτογράφησης δημόσιου κλειδιού, και τα αναμεταδίδει σε ένα μονοπάτι αποτελούμενο από "μείγματα''. Κάθε μείγμα αποκρυπτογραφεί , καθυστερεί και επανατοποθετεί τα μηνύματα πριν τα προωθήσει .

Μεταγενέστεροι σχεδιασμοί ανωνυμίας βασισμένοι στην αναμετάδοση έχουν χωριστεί σε δυο βασικές κατευθύνσεις. Συστήματα όπως το **Babel** , **Mixmaster** , και το **Mixminion** έχουν προσπαθήσει να μεγιστοποιήσουν την ανωνυμία με κόστος να παρουσιάζουν μεγάλες και ασταθείς καθυστερήσεις .

Εξαιτίας αυτής της απόφασης , αυτά , τα υψηλής καθυστέρησης δίκτυα αντιστέκονται σε ισχυρούς παγκόσμιους αντιπάλους αλλά παρουσιάζουν μεγάλη υστέρηση σε διαδραστικές εργασίες όπως η περιήγηση στο διαδίκτυο ,η συνομιλία στο Internet, ή οι συνδέσεις SSH.

Το Tor ανήκει στη δεύτερη κατηγορία: χαμηλής καθυστέρησης σχεδιασμοί που προσπαθούν να ανωνυμοποιήσουν δεδομένα διαδραστικού δικτύου. Αυτά τα συστήματα χειρίζονται μια πληθώρα αμφίδρομων πρωτοκόλλων . Επίσης παρέχουν πιο βολική παράδοση μηνυμάτων (αλληλογραφία) από τα υψηλής καθυστέρησης ανώνυμα δίκτυα ηλεκτρονικού ταχυδρομείου, επειδή ο δευτερεύων διακομιστής ηλεκτρονικού ταχυδρομείου παρέχει σαφή και έγκαιρη επικύρωση αποστολής.
Αλλά επειδή αυτά τα σχέδια συνήθως περιλαμβάνουν πολλά πακέτα που πρέπει να παραδοθούν γρήγορα, είναι δύσκολο να αποτρέψουν έναν εισβολέα να υποκλέπτει και τις δυο πλευρές επικοινωνίας , συσχετίζοντας τον συγχρονισμό και τον όγκο των δεδομένων , που μπαίνουν στο διαδίκτυο ανωνυμίας, με τα δεδομένα τα οποία φεύγουν απ' αυτό .

Αυτά τα πρωτόκολλα είναι εξίσου ευάλωτα σε έναν ενεργό αντίπαλο που εισάγει κάποια πρότυπα χρονισμού στα δεδομένα που εισέρχονται στο δίκτυο, και κοιτάζει για συσχετισμένα μ' αυτά πρότυπα, στα εξέρχοντα δεδομένα απ' το δίκτυο.

Αν και έχουν γίνει κάποιες εργασίες προκειμένου να εμποδίσουν αυτές τις επιθέσεις , οι περισσότεροι σχεδιασμοί τα προστατεύουν κυρίως απο την ανάλυση των δεδομένων παρά την επικύρωση τους .

Οι απλούστεροι χαμηλής καθυστέρησης σχεδιασμοί είναι μιας μεταπήδησης διαμεσολαβητές όπως ο anonymizer: ένας αξιόπιστος διακομιστής που αφαιρεί την προέλευση των δεδομένων πριν τα αναμεταδώσει. Είναι εύκολο να αναλύσει κάποιος αυτούς τους σχεδιασμούς , αλλά οι χρήστες πρέπει να εμπιστεύονται τον διαμεσολαβητή ανωνυμοποίησης (anonymizing proxy) .

Συγκεντρώνοντας τα δεδομένα σ' αυτό το συγκεκριμένο σημείο αυξάνει το βαθμό ανωνυμίας(ένας καθορισμένος χρήστης που κρύβεται ανάμεσα), αλλα είναι ευάλωτο αν ο αντίπαλος μπορεί να παρατηρήσει τα δεδομένα που εισέρχονται στο διαμεσολαβητή και μετά φεύγουν.

Το java Anon proxy-μεσολάβησης (επίσης γνωστό και ως JAP ή Web MIXes) χρησιμοποιεί σταθερά, κοινά δρομολόγια(Routes) γνωστά και ως cascades –καταρράκτες.

Ο σχεδιασμός Java Anon Proxy συνεπάγεται με την θέση ανάμεσα στους τελικούς χρήστες και την αρχή της επικάλυψης (ή καταρρακτη). Ωστόσο, δεν αποδεικνύεται ι εάν η πολιτική (θέση της πολιτικής) για την τρέχουσα εφαρμογή βελτιώνει την ανωνυμία.

Το PipeNet , ένας άλλος σχεδιασμός έδωσε ισχυρή ανωνυμία αλλά επέτρεπε σε ένα μοναδικό χρήστη να κλείσει το δίκτυο με το να μην στέλνει.

Σε P2P σχεδιασμούς όπως το **Tarzan** και το **MorphMix ,** όλοι οι συμμετέχοντες δημιουργούσαν και μετέδιδαν δεδομένα για άλλους. Τα συστήματα αυτά επιδιώκουν να κρύψουν εάν ένα δεδομένο peer (πομπός-δέκτης ή το αντίστροφο) δημιουργεί αιτήματα ή τα μεταδίδει από άλλο peer.

Το Hordes είναι βασισμένο στο Crowds ,αλλά χρησιμοποιεί επίσης multicast ανταποκρίσεις για να κρύψει εκκινητή.

Συστήματα όπως το freedom και το αρχικό onion routing δημιουργούν κυκλώματα με τη μια. Χρησιμοποιώντας ένα πολλαπλών «κρεμμύδι» με κρυπτογραφημένα μηνύματα όπου έγιναν με το σύστημα κρυπτογράφησης δημόσιου κλειδιού (public key). Κάθε στρώμα του οποίου , διαθέτει κλειδιά συνόδου (session keys) και την διεύθυνση του επόμενου server στο κύκλωμα.

Οι Σχεδιασμοί που είναι βασισμένοι στα κυκλώματα πρέπει να επιλέξουν ποιο επίπεδο πρωτοκόλλου πρέπει να ανωνυμοποιήσουν . Μπορεί να υποκλέψουν IP πακέτα άμεσα , και να τα αναμεταδώσουν ολόκληρα (Αφαιρώντας την Source address-πηγή διεύθυνσης) κατά μήκος του κυκλώματος. Όπως στο TOR, που μπορεί να δεχτει TCP streams και να αναμεταδώσει δεδομένα σ' αυτά τα streams, αγνοώντας την κατανομή των εν λόγω δεδομένων σε τμήματα TCP

Για να πάρει κανείς την απόφαση για το Protocol-layer απαιτείται μια συμβιβαστική λύση μεταξύ της ευελιξίας και της ανωνυμίας.

Τα κατανεμημένων ευθυνών συστήματα ανωνυμοποίησης χρειάζεται να εμποδίζουν τους εισβολείς από το να βάζουν πάρα πολλούς servers και να θέτουν σε κίνδυνο τα μονοπάτια των χρηστών. Το TOR βασίζεται σε μια μικρή ομάδα γνωστών server καταλόγου (directory servers), που διευθύνεται από ανεξάρτητους φορείς , για να αποφασίσει ποιοι κόμβοι μπορούν να ενταχθούν.

Η ανώνυμη επικοινωνία είναι απαραίτητη για συστήματα που είναι ανθεκτικά στη (λογοκρισία), Όπως το Eternity, το Free Haven, το Publius, και το Tangler.

Τα rendezvous points του tor επιτρέπουν τις συνδέσεις μεταξύ των αμοιβαίως ανώνυμων οντοτήτων, είναι θεμέλιο για τους ,κρυφής τοποθεσίας , servers(location-hidden servers) τα οποία απαιτούνται από το Eternity και το Free Haven.

Στόχοι σχεδιασμού και υποθέσεις

Στόχοι

Όπως και οι άλλοι σχεδιασμοί ανωνυμίας χαμηλής καθυστέρησης , το TOR επιδιώκει να εμποδίσει τους εισβολείς από το να συνδέονται με άλλους εταίρους επικοινωνίας ή τη σύνδεση πολλαπλών επικοινωνιών με έναν χρήστη ή από έναν χρήστη. Παρ' όλα αυτά ,με αυτό το συγκεκριμένο στόχο , αρκετές μελέτες έχουν κατευθύνει την εξέλιξη του TOR.

Αναπτυξιμότητα: Ο σχεδιασμός πρέπει να αναπτυχθεί και και να χρησιμοποιηθεί στο πραγματικό κόσμο . Έτσι δεν πρέπει να είναι ακριβός για να τον λειτουργήσεις και δεν πρέπει να είναι δύσκολος ή ακριβός για να τον εφαρμόσεις. Επίσης δεν πρέπει να απαιτούμε από μη ανώνυμους φορείς (όπως οι ιστότοποι) να λειτουργήσουν το λογισμικό μας.

Χρηστικότητα: Ένα σύστημα που είναι δύσκολο να το χρησιμοποιήσεις έχει λιγότερους χρήστες , και επειδή τα συστήματα ανωνυμίας κρύβουν χρήστες μεταξύ χρηστών , ένα σύστημα με λιγότερους χρήστες παρέχει λιγότερη ανωνυμία.
Το Tor πρέπει είναι εύκολο στην εφαρμογή του, σε όλες τις συνηθισμένες πλατφόρμες. Δεν μπορούμε να απαιτήσουμε από τους χρήστες να αλλάξουν το λειτουργικό τους σύστημα σε ανώνυμο.

Ευελιξία: Το πρωτόκολλο πρέπει να είναι ευέλικτο και σωστά προσδιορισμένο, έτσι το Tor να μπορεί να χρησιμεύσει ως πεδίο δοκιμών για μελλοντική έρευνα. Ας ελπίσουμε ότι τα μελλοντικά συστήματα δεν θα χρειαστεί να ανακαλύψουν ξανά τον σχεδιασμό του Tor.

Απλός σχεδιασμός: Ο σχεδιασμός πρωτοκόλλου και οι παράμετροι ασφαλείας πρέπει να είναι απολύτως κατανοητοί.
Το Tor σκοπεύει να αναπτύξει ένα απλό και σταθερό σύστημα που θα εντάξει τις καθ όλα αποδεκτές προσεγγίσεις για την προστασία της ανωνυμίας.

Non-goals

Ευνοώντας απλούς, με τη δυνατότητα ανάπτυξης σχεδιασμούς , έχουμε αναβάλλει κατηγορηματικά αρκετούς πιθανούς στόχους , είτε επειδή έχουν επιλυθεί αλλού, είτε επειδή δεν έχουν ακόμα επιλυθεί.

Όχι στο δίκτυο υπολογιστών peer to peer:
Το Tarzan και το MorphMix στοχεύουν στο να διαβαθμίσουν εντελώς αποκεντρωμένα peer-to-peer περιβάλλοντα , με μικρής διάρκειας servers ,πολλοί εκ των οποίων μπορεί να ελέγχονται από έναν αντίπαλο. Αυτή η προσέγγιση μπορεί να είναι ελκυστική , αλλά έχει ακόμα πολλά ανοιχτά προβλήματα.

Όχι ασφάλεια σε συνεχόμενες επιθέσεις :
Το Tor δεν ισχυρίζεται ότι όχι έχει λύσει εντελώς συνεχόμενες επιθέσεις χρονισμού ή διασταύρωσης .

Χωρίς πρωτόκολλο ομαλοποίησης:
Το tor δεν παρέχει πρωτόκολλο ομαλοποίησης όπως το Privoxy ή το Anonymizer
Το tor πρέπει να επικαλυφθεί με ένα μεσολαβητή φιλτραρίσματος όπως το Privoxy για να κρύψει τις διαφορές μεταξύ πελατών και να σβήσει χαρακτηριστικά πρωτοκόλλου που διαρρέουν ταυτότητας (που χάνουν τη ταυτότητα τους).

Μη στεγανογραφικό :
Το tor δεν προσπαθεί να αποκρύψει ποιος είναι συνδεδεμένος στο διαδίκτυο

Threat Model

Κατά την θεωρητική ανάλυση και το σχεδιασμό προγραμμάτων ανωνυμίας, η πιο ευρέως διαδεδομένη απειλή, είναι μια παγκόσμια παθητική εισβολή. Το Tor, όπως και όλα τα υπόλοιπα εφαρμοζόμενα χαμηλής καθυστέρησης συστήματα, δεν μας προστατεύει ενάντια σε έναν τόσο ισχυρό αντίπαλο.

Αντ' αυτού, υποψιαζόμαστε την ύπαρξη ενός αντιπάλου ο οποίος παρατηρεί κάποια τμήματα των δεδομένων του διαδικτύου, παράγει, τροποποιεί, διαγράφει ή καθυστερεί δεδομένα, δηλαδή κάποιος βάζει σε λειτουργία από μόνος του το onion-router (δρομολογητής για εισχώρηση στο Σκοτεινό Διαδίκτυο) και ίσως εκθέσει τμήματα/ λειτουργίες αυτού του δρομολογητή.

Στα χαμηλής καθυστέρησης συστήματα ανωνυμίας που έχουν πολυεπίπεδη κρυπτογράφηση, ο στόχος της τυπικής εισβολής είναι η παρατήρηση του μυητή/ πομπού και του ανταποκριτή. Παρατηρώντας και τα δύο άκρα, οι παθητικοί εισβολείς επιβεβαιώνουν την υποψία ότι κάποιος μιλάει με κάποιον άλλον αν τα μοτίβα συγχρονισμού και όγκου των δεδομένων στη σύνδεση είναι αρκετά ευδιάκριτα, ενώ ενεργοί εισβολείς προκαλούν σήματα συγχρονισμού στα δεδομένα για εξαναγκασμό δημιουργίας ευδιάκριτων μοτίβων.

Αντί να εστιάζουμε στις επιβεβαιώσεις των εισβολών στα δεδομένα, προτιμούμε να στοχεύουμε στην αποτροπή των εισβολών προς την ανάλυση των δεδομένων του δικτύου, όπου ο εισβολέας χρησιμοποιεί μοτίβα ροής για να μάθει σε ποια σημεία του διαδικτύου θα μπορούσε να εισβάλει.

Ο εισβολέας θα προσπαθούσε να συνδέσει τη μυήτρια/ πομπό με τους συνομιλητές του/η να φτιάξει ένα προφίλ της συμπεριφοράς του. Θα μπορούσε να επιτεθεί σε παθητικούς εισβολείς παρατηρώντας το περιφερειακό δίκτυο και συσχετίζοντας την είσοδο στα δεδομένα με την έξοδο από το διαδίκτυο αναπτύσσοντας σχέσεις μεταξύ του συγχρονισμού του όγκου των δεδομένων ή και με εξωτερικά επιλεγμένων από χρήστες ορατών επιλογών/ παραμέτρων.

Ο αντίπαλος αντεπιτίθεται σε ενεργούς εισβολείς εκθέτοντας τους δρομολογητές ή τα κλειδιά ασφαλείας τους αναπαράγοντας ροή πληροφοριών, αρνούμενος επιλεκτικά υπηρεσίες από αξιόπιστους δρομολογητές για να προωθήσει χρήστες σε εκτεθειμένους δρομολογητές ή στερώντας υπηρεσίες σε χρήστες για να δει αν η ροή πληροφοριών σταματά αλλού στο διαδίκτυο, ή εισάγοντας μοτίβα στα δεδομένα που αργότερα θα εκτεθούν. Ο εχθρός μπορεί να ανατρέψει/ επαναπρογραμματίσει το διακομιστή καταλόγου (directory server) να δώσει στους χρήστες διαφορετικές πλευρές της κατάστασης του διαδικτύου.

Επιπρόσθετα, μπορεί να μειώσει την αξιοπιστία του δικτύου επιτιθέμενος σε κόμβους ή εκτελώντας αντικοινωνικές δραστηριότητες από αξιόπιστους κόμβους και προσπαθώντας να τους καταρρίψει κάνοντας το διαδίκτυο αναξιόπιστο, οπότε αναγκάζει τους χρήστες να χρησιμοποιήσουν άλλα συστήματα που δεν εξασφαλίζουν την ανωνυμία τους και είναι εύκολο να δεχτούν επίθεση.

Παρακάτω, παρουσιάζουμε περιληπτικά πόσο αποτελεσματικός είναι ο σχεδιασμός του Tor ενάντια σε τέτοιες επιθέσεις.

Ο Σχεδιασμός TOR

Το δίκτυο TOR είναι ένα δίκτυο επικάλυψης. Κάθε onion router λειτουργεί σαν μια κανονική διαδικασία στο επίπεδο του χρήστη , χωρίς ειδικά προνόμια. Το κάθε onion router διατηρεί μια TLS σύνδεση με κάθε άλλο onion router. Κάθε χρήστης χρησιμοποιεί ένα τοπικό λογισμικό που ονομάζεται onion proxy, για να πάρει τους καταλόγους, να δημιουργήσει κυκλώματα σε όλο το δίκτυο, και να χειρίζεται συνδέσεις από τις εφαρμογές του χρήστη. Αυτά τα onion proxies δέχονται TCP ροές και τις πολλαπλασιάζουν σε όλο το δίκτυο. Το onion router στην άλλη άκρη του κυκλώματος συνδέεται με τους απαιτούμενους προορισμούς και αναμεταδίδει δεδομένα.

Κάθε onion router διατηρεί ένα μακράς διαρκείας identity key (κλειδί-ταυτότητα) και ένα μικρής διαρκείας onion key. Το identity key χρησιμοποιείται για να υπογράφει πιστοποιητικά TLS , το OR's router descriptor (μια σύνοψη των κλειδιών του, της διεύθυνσης, του εύρους ζώνης , της πολιτικής εξόδου και ούτω καθεξής) και(από τους διακομιστές καταλόγου – directory servers) να υπογράφει καταλόγους.

Το onion key χρησιμοποιείται για να αποκρυπτογραφήσει αιτήματα από χρήστες, να δημιουργήσει ένα κύκλωμα, και να διαπραγματευτεί εφήμερα κλειδιά. Το πρωτόκολλο TLS καθορίζει έναν βραχυπρόθεσμο σύνδεσμο-κλειδί κατά την επικοινωνία μεταξύ των Ors. Τα βραχυπρόθεσμα κλειδιά εναλλάσσονται κατά περιόδους και ανεξάρτητα , για να περιορίσουν τον αντίκτυπο του να βρίσκονται σε κίνδυνο.

Κυψέλες

Τα onion routers επικοινωνούν το ένα με το άλλο, και με τις OPs των χρηστών , μέσω των συνδέσεων TLS με κλειδιά μιας χρήσης. Η χρήση του TLS αποκρύπτει τα δεδομένα και αποτρέπει έναν εισβολέα από το να τροποποιήσει τα δεδομένα ή την μίμηση ενός OR.

Τα δεδομένα περνάνε κατά μήκος αυτών των συνδέσεων σε κυψέλες συγκεκριμένου μεγέθους. Κάθε κυψέλη είναι 512 bytes και αποτελείται από μια κεφαλίδα και ένα ωφέλιμο φορτίο. Κάθε κεφαλίδα περιλαμβάνει ένα αναγνωριστικό κύκλωμα (Κύκλωμα ID-circuitID) που προσδιορίζει σε ποιο κύκλωμα αναφέρεται η κυψέλη(πολλά κυκλώματα μπορούν να πολλαπλασιαστούν πάνω σε μια μόνο σύνδεση TLS), και μια εντολή για να περιγράψει τι κάνει με το ωφέλιμο φορτίο της κυψέλης.

Τα αναγνωριστικά κυκλώματα εξαρτώνται από τη σύνδεση: Κάθε κύκλωμα έχει διαφορετικό circID σε κάθε OP/OR ή OR/OR σύνδεση που διασχίζει.

Με βάση την εντολή τους , οι κυψέλες είναι , είτε κυψέλες ελέγχου που πάντοτε ερμηνεύονται από τον κόμβο που τις λαμβάνει ή κυψέλες μετάδοσης, οι οποίες μεταδίδουν δεδομένα σε συνεχόμενη ροή.

Οι εντολές τις κυψέλης ελέγχου είναι: Το padding (προς το παρών χρησιμοποιείται για το keepalive, επίσης είναι χρήσιμο και για link padding) , to create ή το created (που χρησιμοποιείται για να δημιουργήσει ένα νέο κύκλωμα) και το destroy (για να καταστρέψει ένα κύκλωμα).

Οι κυψέλες μετάδοσης έχουν μια πρόσθετη κεφαλίδα (κεφαλίδα μετάδοσης-header ID) στο μπροστινό μέρος του ωφέλιμου φορτίου-payload, περιλαμβάνοντας ένα stream ID (stream αναγνώρισης: πολλά streams μπορούν να πολλαπλασιαστούν πάνω σ ένα κύκλωμα) ένα συνεχές άθροισμα ελέγχων , της ακεραιότητας, του μήκους του ωφέλιμου φορτίου μετάδοσης και της εντολής μετάδοσης . . Όλο το περιεχόμενο της κεφαλίδας μετάδοσης και της κυψέλης μετάδοσης ωφέλιμου φορτίου κρυπτογραφούνται ή αποκρυπτογραφούνται μαζί καθώς η κυψέλη μετάδοσης κινείται κατά μήκος του κυκλώματος , χρησιμοποιώντας των 128-bit AES κρυπτογράφηση σε κατάσταση μετρητή για να δημιουργήσει ένα κρυπτογραφημένο stream.

Οι εντολές μετάδοσης είναι: Το *relay data* (τα δεδομένα ρέουν στο stream), *relay begin* (να ανοίξει ένα stream), *relay end* (να κλείσει σωστά ένα stream), *relay teardown* (να κλείσει ένα χαλασμένο stream), *relay connected* (Να ενημερωθεί το OP η αρχή της μετάδοσης έχει πετύχει), *relay extend* and *relay extended* (να επεκταθεί ένα κύκλωμα με μεταπήδηση ,και να αναγνωριστεί-ενημερωθεί), *relay truncate* and *relay truncated* (να καταστραφεί μέρος του κυκλώματος και να αναγνωριστεί-ενημερωθει), *relay sendme* (χρησιμοποιείται για τον έλεγχο συμφόρησης), and *relay drop* (χρησιμοποιείται για να εφαρμόσει μακροπρόθεσμα αντίγραφα). Σας δίνουμε μια εικονική επισκόπηση της δομή των κυψελών και επιπλέον τις λεπτομέρειες της μετάδοσης της δομής των κυψελών και περιγράφουμε κάθε τύπο κυψελών και εντολών με περισσότερες λεπτομέρειες παρακάτω.

Κυκλώματα και streams

Αρχικά το onion routing δημιούργησε ένα κύκλωμα για κάθε TCP stream. Διότι η δημιουργία ενός κυκλώματος μπορεί διαρκέσει αρκετά δέκατα του δευτερολέπτου (λόγω της κρυπτογράφησης δημόσιου κλειδιού-public key cryptography και της καθυστέρησης του δικτύου). Αυτός ο σχεδιασμός επέβαλλε υψηλό κόστος σε εφαρμογές όπως η περιήγηση διαδικτύου που ανοίγουν πολλά TCP streams.

Στο TOR κάθε κύκλωμα μπορεί να χρησιμοποιηθεί από πολλά TCP streams. Για να αποφύγουν τις καθυστερήσεις , οι χρήστες δημιουργούν κυκλώματα προληπτικά. Για να περιορίσουν τη δυνατότητα σύνδεσης μεταξύ των streams τους , τα Ops των χρηστών δημιουργούν ένα νέο κύκλωμα κατά περιόδους , αν τα παλαιότερα έχουν χρησιμοποιηθεί και λήγουν παλιά χρησιμοποιημένα κυκλώματα που δεν έχουν πλέον κανένα ανοιχτό stream. Τα OPs γυρνάνε σε νέο κύκλωμα ανά λεπτό: κατ'αυτόν τον τρόπο ακόμα και οι τακτικοί χρήστες (σημαντικοί) ξοδεύουν ελάχιστο χρόνο δημιουργώντας κυκλώματα, αλλά ένας περιορισμένος αριθμός αιτημάτων μπορεί να συνδεθούν το ένα με το άλλο μέσω ενός συγκεκριμένου κόμβου εξόδου.

Επίσης επειδή τα κυκλώματα δημιουργούνται στο παρασκήνιο, τα Ops μπορούν να επανέλθουν από μια αποτυχημένη δημιουργία χωρίς να βλάψουν τν εμπειρία των χρηστών.

Δείκτης περιορισμού και νομιμότητας

Οι εθελοντές είναι πιο πρόθυμοι να χρησιμοποιήσουν υπηρεσίες που περιορίζουν τη χρήση του εύρους ζώνης τους. Για να μπορέσουν να τους φιλοξενήσουν όλους, οι TOR servers χρησιμοποιούν έναν προσεγγιστικό αλγόριθμο token bucket για να εφαρμόσουν έναν μακροπρόθεσμο μέσο ρυθμό εισερχόμενων byte, ενώ ακόμα επιτρέπει τις βραχυπρόθεσμες ρήξεις πάνω από το επιτρεπόμενο εύρος ζώνης.

Επειδή το πρωτόκολλο Tor εξάγει περίπου τον ίδιο αριθμό bytes που εισάγει, είναι επαρκές, κατά την εφαρμογή, να περιορίσει μόνο τα εισερχόμενα bytes. Παρ'όλα, αυτά με τα TCP streams, η αντιστοιχία δεν είναι ένα προς ένα: η μετάδοση ενός εισερχόμενου byte μπορεί να απαιτήσει μια ολόκληρη κυψέλη 512 –bytes. (Δεν μπορούμε απλά να περιμένουμε για περισσότερα bytes, γιατί η τοπική εφαρμογή ίσως περιμένει μιαν απάντηση). Συνεπώς αντιμετωπίζουμε αυτήν την υπόθεση λες και είχε διαβαστεί ολόκληρο το μέγεθος της κυψέλης, ανεξαρτήτως της πληρότητας της κυψέλης.

Περαιτέρω, εμπνευσμένο από το σχεδιασμό του Rennhard και του al, οι άκρες ενός κυκλώματος να διακρίνουν τα διαδραστικά streams (interactive streams) από τα μαζικά streams (bulk streams) συγκρίνοντας τη συχνότητα με την οποία προμηθεύουν κυψέλες. Μπορούμε να παρέχουμε καλή καθυστέρηση (latency) για διαδραστικά streams δίνοντας τους προνομιακές υπηρεσίες, ενώ εξακολουθούμε να δίνουμε καλή συνολική απόδοση στα bulk streams . Τέτοια προνομιακή διαχείριση παρουσιάζει μια πιθανή , συνεχόμενη επίθεση , αλλά ένας αντίπαλος παρατηρώντας και τις δύο άκρες του stream να μάθει αυτές τις πληροφορίες μέσω των επιθέσεων χρονισμού.

Rendezvous Points and hidden services

Τα rendezvous pointsείναι ένα θεμέλιο για τις υπηρεσίας κρυφής τοποθεσίας (γνωστών και ως ανταποκριτές/ πάροχοι ανωνυμίας) στο διαδίκτυο του tor . Οι κρυφής τοποθεσίας υπηρεσίεςν επιτρέπουν στον Μπομπ να προσφέρει μια υπηρεσία πρωτοκόλλου ελέγχου μεταφοράς (TCP), ως διακομιστής δικτύου, χωρίς να αποκαλύπτει την διεύθυνση Πρωτοκόλλου του Διαδικτύου του. Αυτού του τύπου η ανωνυμία προστατεύει από διαμοιρασμένες επιθέσεις στο λειτουργικό σύστημα του δίσκου (DOS), δηλαδή οι εισβολείς θα αναγκαστούν να επιτεθούν στο Διαδίκτυο Onion routing διότι δεν γνωρίζουν τη διεύθυνση Πρωτοκόλλου του Διαδικτύου του Μπομπ.

Ο σχεδιασμός μας για τις τοποθεσίες απόκρυφων υπηρεσιών έχουν τους εξής στόχους. **Έλεγχος πρόσβασης**: Ο Μπομπ χρειάζεται φίλτρο για τα εισερχόμενα αιτήματα, άρα ο εισβολέας δεν θα ενοχλήσει τον Μπομπ με το να συνδέεται συχνά μαζί του. **Δύναμη**: Ο Μπομπ θα πρέπει να διατηρεί μια μακρόχρονη ταυτότητα ψευδωνύμου, ακόμα και παρουσία κατάρρευσης/ αποτυχίας της δρομολόγησης. Οι υπηρεσίες του Μπομπ δεν πρέπει να συνδέονται με ένα μόνο onion router και θα πρέπει να είναι ικανός να μεταφέρει την υπηρεσία του μέσωonion routers. **Ανθεκτικότητα στην κηλίδωση/ συκοφαντία**: Ένας εισβολέας των κοινωνικών θεμάτων δεν θα πρέπει να μπορεί να παγιδέψει έναν κόμβο δικτύου πολλαπλής διανομής προσφέροντας παράνομες υπηρεσίες κρυφής τοποθεσίας και κάνοντας τους παρατηρητές να πιστεύουν ότι είναι υπηρεσία του δικτύου. **Διαφάνεια εφαρμογών**: Αν και ζητάμε από τους χρήστες να χρησιμοποιήσουν εξειδικευμένα λογισμικά για πρόσβαση σε location-hidden servers, δεν πρέπει να ζητάμε να τροποποιούν τις εφαρμογές τους.

Παρέχουμε κρυφή τοποθεσία για τον Μπομπ επιτρέποντας του να γνωστοποιεί πολλά onion routers (τα σημεία εισόδου του) ως σημεία σύνδεσης. Μπορεί να το κάνει αυτό σε κάθε εύρωστο ή αποτελεσματικό σύστημα με κλειδιά ασφαλείας και γνήσιες αναβαθμίσεις, όπως οι διαμοιρασμένοι πίνακες κατακερματισμού (DHS) σαν τους CFS. Η Αλίκη, η πελάτισσα, διαλέγει ένα onion router σαν κόμβο συνάντησης των δικτύων. Συνδέεται με τα σημεία εισόδου του Μπομπ, τον πληροφορεί για τους κόμβους συνάντησης της και τον περιμένει να συνδεθεί και αυτός σε αυτούς τους κόμβους. Αυτό το πρόσθετο επίπεδο πλάγιου μέσου βοηθά τα σημεία εισόδου να μπορούν να αποφύγουν τα προβλήματα που σχετίζονται με παρουσίαση μη δημοφιλών αρχείων άμεσα (π.χ. αν ο Μπομπ μοιράζει υλικό που το σύνολο των σημείων εισόδου το βρίσκει απαράδεκτο ή αν η υπηρεσία του Μπομπ τείνει να δεχτεί επίθεση από εισβολείς του δικτύου). Το επιπλέον επίπεδο πλάγιων επιτρέπει στον Μπομπ να ανταποκριθεί σε κάποια αιτήματα και να αγνοήσει άλλα.

Previous rendezvous work

Τα Rendezvous points σε χαμηλής καθυστέρησης συστήματα ανωνυμίας πρώτα παρουσιάστηκαν για τη χρήση τους στο Ψηφιακό Δίκτυο Ενοποιημένων Υπηρεσιών (ISDN) τηλεφωνίας. Τα μετέπειτα προγράμματα χαμηλής καθυστέρησης χρησιμοποιούν κόμβους δικτύων πολλαπλής διανομής για απόκρυψη της τοποθεσίας των κινητών τηλεφώνων και των χαμηλής έντασης ανιχνευτών τοποθεσίας. Κόμβοι για την ανωνυμία μέσω χαμηλής καθυστέρησης συνδέσμων του Διαδικτύου προτάθηκαν στις πρώτες παρουσιάσεις του Onion Routing, αλλά ο πρώτος δημοσιευμένος σχεδιασμός ήταν του Ίαν Γκολντμπεργκ. Ο σχεδιασμός του διαφέρει από τον δικό μας σε τρία σημεία. Πρώτον, προτείνει ότι η Αλίκη χειροκίνητα καταδιώκει μια τρέχουσα τοποθεσία της υπηρεσίας μέσω της Γκνουτέλλα, δηλαδή η προσέγγιση μας κάνει τις αναζητήσεις μας διαφανείς στους χρήστες, αλλά ταχύτερες και αποτελεσματικότερες/ δυνατότερες.

Δεύτερον, στο Τορ, ο πελάτης και ο διακομιστής διαπραγματεύονται κλειδιά συνόδου με το Ντίφι-Χέλμαν πρωτόκολλο, άρα το απλό κείμενο δεν εκτίθεται ούτε στους κόμβους δικτύων πολλαπλής διανομής. Τρίτον, ο σχεδιασμός μας ελαχιστοποιεί την έκθεση και την εκτέλεση της υπηρεσίας, για να ενθαρρύνει εθελοντές να προσφέρουν σύσταση και υπηρεσίες κόμβων. Τα σημεία εισαγωγής του Τορ δεν εξάγουν ψηφιολέξεις στους πελάτες, δηλαδή οι κόμβοι δικτύων πολλαπλής διανομής δεν γνωρίζουν ούτε τον πελάτη ούτε τον διακομιστή και δεν διαβάζουν τα δεδομένα που μεταφέρονται. Η σχεδίαση του πλάγιου μέσου έγινε για να συμπεριλάβει αυθεντικότητα/ αδειοδότηση, δηλαδή αν η Αλίκη δεν περικλείσει το σωστό cookie με το αίτημα της για την υπηρεσία, ο Μπομπ δεν θα ξέρει ούτε την ύπαρξη του.

Άλλες αποφάσεις σχεδιασμού

Άρνηση υπηρεσιών

Η παροχή TOR ως μια δημόσια υπηρεσία δημιουργεί πολλές ευκαιρίες για επιθέσεις άρνησης υπηρεσιών κατά του δικτύου Καθώς ο έλεγχος της ροής και ο περιορισμός ρυθμού εμποδίζουν τους χρήστες από το να καταναλώνουν περισσότερο εύρος ζώνης απ' ότι οι δρομολογητές είναι πρόθυμοι να παρέχουν, οι ευκαιρίες παραμένουν για τους χρήστες να καταναλώσουν περισσότερες πηγές δικτύου απ' ότι το δίκαιο μερίδιο τους, ή να καταστήσουν το δίκτυο απρόσιτο για άλλους.

Πρωτ' απ' όλα, υπάρχουν αρκετές επιθέσεις άρνησης υπηρεσιών που καταναλώνουν τη CPU καθώς ο εισβολέας αναγκάζει το Σκοτεινό Δίκτυο να εκτελέσει ακριβές κρυπτογραφικές λειτουργίες. Για παράδειγμα, ένας εισβολέας μιμείται την αρχή της χειραψίας της πολυεπίπεδης ασφάλειας μεταφοράς (TLS) αναγκάζοντας το OR να διεξάγει την (συγκριτικά ακριβή) μισή από τη χειραψία σε μη πραγματικό υπολογιστικό κόστος για τον εισβολέα.

Δεν έχουμε εκτελέσει ακόμα άμυνες για αυτές τις επιθέσεις, αλλά πολλές προσεγγίσεις είναι πιθανές .Αρχικά, τα Ors μπορούν να απαιτήσουν από τους πελάτες να λύσουν έναν γρίφο καθώς ξεκινούν νέες TLS- χειραψίες(TLS handshakes)ή αποδοχή δημιουργίας κυψελών . Ως ώρας, καθώς αυτές οι λεκτικές μονάδες είναι εύκολο να ισχύσουν και είναι υπολογιστικά ακριβές να παραχθούν, αυτή η προσέγγιση περιορίζει τον πολλαπλασιαστή εισβολών.

Επιπροσθέτως, τα ORs μειώνουν το ρυθμό στον οποίο δέχονται να δημιουργήσουν κυψέλες δημιουργίας (create cells) ή TLS συνδέσεις, έτσι ώστε η υπολογιστική εργασία της διεξαγωγής τους δεν πνίγει την συμμετρική κρυπτογραφική λειτουργία που κρατά τις κυψέλες σε ροή. Αυτή η μείωση ρυθμού θα μπορούσε, όμως, να επιτρέψει σε εισβολέα να καθυστερήσει άλλους χρήστες όταν φτιάχνουν νέα κυκλώματα.

Οι εισβολείς μπορούν επίσης να επιτεθούν στους εξυπηρετητές του δικτύου TOR και τους συνδέσμους του. Διακόπτοντας ένα κύκλωμα ή σπάζοντας ένα δεσμό, όλες οι φορτώσεις δεδομένων περνούν μαζί από αυτό το κομμάτι του κυκλώματος. Οι χρήστες παρομοίως χάνουν υπηρεσίες όταν ο δρομολογητής καταρρίπτεται ή ο χειριστής τους επανεκκινεί τη λειτουργία του. Ο τρέχον σχεδιασμός του TOR συμπεριφέρεται σε αυτές τις εισβολές ως διακοπτόμενες καταρρεύσεις του δικτύου και εξαρτάται από τους χρήστες και τις εφαρμογές να ανταποκριθούν ή να επανέλθουν στην κατάλληλη κατάσταση. Ένας μελλοντικός σχεδιασμός θα μπορούσε να χρησιμοποιεί από την αρχή έως το τέλος ένα πρωτόκολλο βασισμένο στην γνώση του TCP ώστε να μην χάνονται οι ροές δεδομένων εκτός και αν τα σημεία εισόδου και εξόδου αποδιοργανώνονται. Αυτή η λύση απαιτεί περισσότερη ρύθμιση στα άκρα του δικτύου, παρ' ολ' αυτά, και οι συνέπειες της εκτέλεσης και της ανωνυμίας λόγω αυτής της πρόσθετης πολυπλοκότητας απαιτεί ακόμα έρευνα.

Exit policies and abuse

Η κατάχρηση εξόδου είναι ένα σοβαρό εμπόδιο για την ευρείας κλίμακας ανάπτυξη του Tor. Η ανωνυμία προσφέρει στους καταχραστές και τους βανδάλους μια ευκαιρία να κρύψουν την προέλευση των ενεργειών τους. Οι εισβολείς μπορούν να βλάψουν το δίκτυο Tor εμπλέκοντας διακομιστές εξόδου για δική τους κατάχρηση. Επίσης, εφαρμογές που ευρέως χρησιμοποιούν αυθεντικότητα/ προέλευση βασισμένες σε IP (π.χ., εταιρικές αλληλογραφίες ή ιστότοπους) μπορούν να εξαπατηθούν από το γεγονός ότι ανώνυμες συνδέσεις εμφανίζονται να προέρχονται από την έξοδο του Σκοτεινού Δικτύου.

Δίνουμε έμφαση στο ότι το Tor δεν καθιστά ικανές νέες μορφές κατάχρησης. Ανεπιθύμητοι αποστολείς αλληλογραφίας και άλλοι εισβολείς έχουν ήδη πρόσβαση σε χιλιάδες από τα ανεπιβεβαίωτα συστήματα παγκοσμίως, και το Tor είναι μακράν ο ευκολότερος τρόπος για να δρομολογηθεί επίθεση. Αλλά επειδή τα onion routers μπορεί να υποπέσουν σε λάθη σχετικά με τους πρωτεργάτες της επίθεσης, και οι εθελοντές που τα χρησιμοποιούν να μην θέλουν να αντιμετωπίσουν την ταλαιπωρία της εξήγησης των δικτύων ανωνυμίας σε οργισμένους διαχειριστές, πρέπει να μπλοκάρουμε ή να περιορίσουμε την κατάχρηση μέσω του δικτύου Tor.

Για να μετριάσουμε τα θέματα κατάχρησης, Η πολιτική εξόδου του κάθε onion router περιγράφει προς ποια εξωτερική διεύθυνση και σταθμούς/ κόμβους θα συνδέεται ο δρομολογητής. Στη μια πλευρά του φάσματος είναι οι κόμβοι ανοιχτής εξόδου που θα συνδεθούν οπουδήποτε. Στο άλλο άκρο υπάρχουν ενδιάμεσοι κόμβοι που μόνο θα προωθούν δεδομένα σε άλλους κόμβους του Tor, και οι κόμβοι ιδιωτικής εξόδου που συνδέονται μόνο σε ένα κεντρικό υπολογιστή ή δίκτυο πιο σίγουρα, δηλαδή ένας εξωτερικός εισβολέας δεν μπορεί να παρακολουθήσει τα δεδομένα μεταξύ ιδιωτικής εξόδου και του τελικού προορισμού, και έτσι είναι λιγότερο σίγουρος για τον προορισμό της Αλίκης και τις ενέργειές της.

Τα περισσότερα onion routers στο τρέχον δίκτυο λειτουργούν ως περιορισμένες έξοδοι που επιτρέπουν συνδέσεις στον κόσμο σε μεγάλη κλίμακα, αλλά εμποδίζουν την πρόσβαση σε συγκεκριμένες διευθύνσεις και υπηρεσίες επιρρεπείς σε κατάχρηση, όπως SMTP. Το σκοτεινό Δίκτυο μπορεί να είναι ικανό να εξουσιοδοτεί πελάτες να εμποδίζει καταχρήσεις εξόδου χωρίς να προσβάλλουν την ανωνυμία.

Πολλοί διαχειριστές χρησιμοποιούν περιορισμούς των σταθμών/ κόμβων για να υποστηρίξουν μόνο ένα περιορισμένο σύνολο υπηρεσιών, όπως HTTP, SSH, ή AIM. Αυτό δεν είναι μια ολοκληρωμένη λύση, φυσικά, αφού ευκαιρίες κατάχρησης γι' αυτά τα πρωτόκολλα είναι ακόμα πολύ γνωστά.

Δεν έχουμε ακόμα αντιμετωπίσει κάποια επίθεση στο αναπτυγμένο δίκτυο, αλλά αν το κάνουμε θα πρέπει να λάβουμε υπ' όψιν την χρήση εντολοδόχων για εκκαθάριση δεδομένων για συγκεκριμένα πρωτόκολλα καθώς αυτά εγκαταλείπουν το δίκτυο. Για παράδειγμα, έντονη καταχρηστική συμπεριφορά του HTTP(π.χ., η εκμετάλλευση ρύθμισης υπερχείλισης δεδομένων ή γνωστών αδύναμων σημείων γραφών) μπορούν να ανιχνευθούν με ένα ευθύ/ άμεσο τρόπο. Παρομοίως, κάποιος θα μπορούσε να εφαρμόσει λογισμικό αυτόματου φίλτρου ανεπιθύμητης αλληλογραφίας (π.χ., SpamAssassin στο ηλεκτρονικό ταχυδρομείο) καθώς φεύγει από το OR network.

Τα onion routers μπορούν επίσης να ξαναγράψουν δεδομένα εξόδου, να προσαρτήσουν κεφαλίδες ή άλλες πληροφορίες υπονοώντας ότι τα δεδομένα έχουν περάσει δια μέσω διακομιστή ανωνυμίας. Αυτή η προσέγγιση είναι κοινώς χρησιμοποιημένη από ηλεκτρονική αλληλογραφία με σύστημα ανωνυμίας. Τα onion routers λειτουργούν επίσης σε διακομιστές με ονόματα χρηστών όπως ανώνυμος για περεταίρω συναγερμούς κατάχρησης στοχεύοντας στη φύση των ανώνυμων δεδομένων.

Μια μίξη ανοιχτών και περιορισμένων κόμβων εξόδου επιτρέπει τη μέγιστη ευελιξία για εθελοντές που εκτελούν σε διακομιστές. Αλλά έχοντας πολλούς ενδιάμεσους κόμβους παρέχεται ένα μεγάλο και εύρωστο δίκτυο, έχοντας μόνο λίγους κόμβους εξόδου μειώνει τον αριθμό σημείων όπου ένας αντίπαλος χρειάζεται να ελέγχει για ανάλυση δεδομένων, και τοποθετεί ένα επιπλέον φορτίο στους κόμβους εξόδου. Αυτή η τάση συναντάται στο Java Anon proxy cascade model, όπου ένας μόνο κόμβος χρειάζεται για να χειριστεί καταγγελίες κατάχρησης, αλλά ένας αντίπαλος χρειάζεται να παρατηρεί την είσοδο και την έξοδο μιας αλληλουχίας (cascade) για να εκτελέσει ανάλυση δεδομένων σ' όλους τους χρήστες αυτής της αλληλουχίας. Το hydra model (πολλές είσοδοι, λίγες έξοδοι) παρουσιάζει ένα διαφορετικό συμβιβασμό: Μόνο λίγοι κόμβοι εξόδου χρειάζονται, αλλά ένας αντίπαλος πρέπει να δουλέψει περισσότερο να παρακολουθήσει όλους τους πελάτες.

Τελικά, παρατηρούμε ότι η κατάχρηση εξόδου δεν πρέπει να θεωρηθεί ως περιφερειακό θέμα: Όταν η δημόσια εικόνα ενός συστήματος κηλιδώνεται, μπορεί να μειώσει τον αριθμό και την ποικιλία των χρηστών του συστήματος, οπότε να μειωθεί και η ανωνυμία του ίδιου του συστήματος. Όπως η χρησιμότητα, έτσι και η δημόσια αντίληψη είναι παράμετρος ασφάλειας. Δυστυχώς, εμποδίζοντας την κατάχρηση εξόδου από ανοιχτό κόμβο είναι άλυτο πρόβλημα, και θα παραμείνει ένας αγώνας για το προβλεπόμενο μέλλον. Τα προβλήματα κατάχρησης αντιμετωπιζόμενα από το σχέδιο Princeton' s CoDeen μας δίνουν μια ιδέα παρόμοιων θεμάτων.

Directory servers

Οι, πρώτης γενιάς, σχεδιασμοί onion routing χρησιμοποιήθηκαν για τις ενημερώσεις κατάστασης του in-band network. Κάθε δρομολογητής έστελνε μια υπογεγραμμένη δήλωση στους γείτονες του, οι οποίοι τη προωθούσαν παρακάτω. Αλλά, τα δίκτυα ανωνυμοποίησης έχουν διαφορετικούς στόχους ασφαλείας απ'ότι το τυπικό πρωτόκολλο link-state routing. Παραδείγματος χάριν , καθυστερήσεις (τυχαίες ή εσκεμμένες) που μπορούν να προκαλέσουν διάφορα μέρη του δικτύου να έχουν διαφορετικές όψεις του link-state και της τοπολογίας(topology) δεν είναι μόνο άβολες:

Δίνουν την ευκαιρία στους εισβολείς να εκμεταλλευτούν τις διαφορές στη γνώση του πελάτη (in client knowledge). Επίσης ανησυχούμε , για επιθέσεις που θα εξαπατήσουν ένα πελάτη σχετικά με τη λίστα μελών του δρομολογητή, της τοπολογίας ή της τρέχουσας κατάστασης του δικτύου. Τέτοιες επιθέσεις partitioning στη γνώση του πελάτη ,βοηθούν έναν αντίπαλο να αναπτύξει αποτελεσματικά πόρους εναντίον του στόχου.

Το TOR χρησιμοποιεί μια μικρή ομάδα από εφεδρικά, γνωστά onion routers για να εντοπίζει τις αλλαγές στη τοπολογία του δικτύου και της κατάστασης του κόμβου, συμπεριλαμβάνοντας κλειδιά και πολιτικές εξόδου. Κάθε server καταλόγου (directory server) λειτουργεί σαν ένας HTTP server ,έτσι ώστε οι πελάτες (clients)να μπορούν να καταγράψουν την τρέχουσα κατάσταση του δικτύου και τις router lists, και έτσι τα άλλα ORs να μπορούν να ανεβάσουν της πληροφορίες της κατάστασης. Τα onion routers δημοσιεύουν, κάθε τόσο, υπογεγραμμένες δηλώσεις της κατάστασης τους , σε κάθε server καταλόγου. Οι servers καταλόγου συνδυάζουν τα στοιχεία αυτά με τις δικές τους απόψεις για τη ζωντάνια του δικτύου και δημιουργούν μια υπογεγραμμένη περιγραφή της ολόκληρης κατάστασης του δικτύου. Το λογισμικό client είναι ένα λογισμικό προ φορτωμένο με μια λίστα από τους server καταλόγου και των κλειδιών τους , για να ξεκινήσει η προβολή κάθε πελάτη του δικτύου.

Όταν ένας server καταλόγου λαμβάνει μια υπογεγραμμένη δήλωση για ένα OR, ελέγχει εάν το Identity key του OR αναγνωρίζεται. Οι servers καταλόγου δεν γνωστοποιούν μη αναγνωρισμένα ORs , αν το έκαναν αυτό , τότε ένας αντίπαλος θα μπορούσε να πάρει τον έλεγχο του δικτύου, δημιουργώντας πολλούς servers. Αντ' αυτού νέοι κόμβοι πρέπει να εγκριθούν από τον διαχειριστή του directory server πριν συμπεριληφθούν.

Μηχανισμοί για την αυτοματοποιημένη έγκριση των κόμβων, είναι τομέας ενεργούς έρευνας , και συζητούνται περισσότερο στην 9η ενότητα.

Φυσικά, ένα πλήθος επιθέσεων παραμένει. Ένας αντίπαλος που ελέγχει έναν server καταλόγου(directory server), μπορεί να παρακολουθεί-εντοπίζει πελάτες ,παρέχοντας τους διάφορες πληροφορίες. Ίσως καταχωρώντας μόνο τους κόμβους που βρίσκονται υπό τον έλεγχο του ή ενημερώνοντας ορισμένους πελάτες για έναν συγκεκριμένο κόμβο. Ακόμα και ένας εξωτερικός αντίπαλος μπορεί να εκμεταλλευτεί τις διαφορές στη γνώση του πελάτη (client knowledge): οι πελάτες χρησιμοποιούν κόμβο που είναι καταχωρημένος σε έναν server καταλόγου (directory server) χωρίς αυτό να σημαίνει ότι οι άλλοι είναι ευάλωτοι.

Έτσι, αυτοί οι server καταλόγου (directory servers) πρέπει να είναι συγχρονισμένοι και εφεδρικοί, για να μπορούν να συμφωνήσουν σε ένα κοινό κατάλογο. Οι πελάτες θα πρέπει να εμπιστεύονται μόνο αυτό το κατάλογο αν είναι υπογεγραμμένος απο ένα όριο server καταλόγου.

Οι εξυπηρετητές καταλόγου (directory servers) στο TOR , διαμορφώθηκαν μετά από αυτούς στην εφαρμογή mixminion, αλλά η δική μας κατάσταση είναι ευκολότερη. Αρχικά κάνουμε την απλουστευτική υπόθεση ότι όλοι οι συμμετέχοντες συμφωνούν με το σύνολο των directory servers. Δεύτερον, καθώς το mixminion χρειάζεται να προβλέψει τη συμπεριφορά του κόμβου, το TOR χρειάζεται μια οριακή συναίνεση για την τρέχουσα κατάσταση του δικτύου. Τρίτον , υποθέτουμε πως μπορούμε να καταφύγουμε στα άτομα που τους διαχειρίζονται , για να ανακαλύψουν και να επιλύσουν τα προβλήματα, όταν δεν μπορεί να επιτευχθεί ένας συναινετικός κατάλογος (consensus directory). Από τη στιγμή που υπάρχουν σχετικά λίγοι servers καταλόγου(directory servers) (επι του παρόντος 3, αλλά αναμένουμε 9 , όσες και οι κλίμακες του δικτύου) έχουμε τα περιθώρια για λειτουργίες όπως το broadcast για την απλοποίηση του πρωτοκόλλου συναίνεσης .

Για να αποφύγουμε επιθέσεις όπου ένας δρομολογητής συνδέεται με όλους τους servers καταλόγου , αλλά αρνείται να μεταδώσει δεδομένα από άλλους δρομολογητές (routers), οι εξυπηρετητές καταλόγου(directory servers) πρέπει να δημιουργούν κυκλώματα και να τα χρησιμοποιούν ώστε να δοκιμάσουν ανώνυμα την αξιοπιστία των routers. Δυστυχώς αυτό το είδος άμυνας δεν έχει σχεδιαστεί ή εφαρμοστεί ακόμα.

Η χρήση των server καταλόγου είναι πιο εύκολη και ευέλικτη από το flooding (μεταβίβαση πακέτων δεδομένων από έναν κόμβο σε έναν ή περισσότερους άλλους κόμβους μέσω των συνδέσεων του υποκείμενου δικτύου). Το flooding είναι ακριβό και περιπλέκει την ανάλυση , όταν ξεκινάμε να πειραματιζόμαστε με τοπολογίες δικτύου που δεν ανήκουν σε κάποια ομάδα(non-clique network topologies). Υπογεγραμμένοι κατάλογοι (Signed directories) μπορούν να αποθηκευτούν από άλλα onion routers, έτσι ώστε να μην επιβραδυνθεί η απόδοση των directory servers όταν έχουμε πολλούς χρήστες, και δεν βοηθούν την ανάλυση δεδομένων αναγκάζοντας τους πελάτες να ανακοινώσουν την ύπαρξη τους σε οποιοδήποτε κεντρικό σημείο.

Passive Attacks

Παρατηρώντας τα πρότυπα δεδομένων χρήστη. Παρατηρώντας τη σύνδεση ενός χρήστη , δεν θα αποκαλύψει το προορισμό της ή τα δεδομένα της, αλλά θα αποκαλύψει τα πρότυπα δεδομένων (και αυτά που αποστέλλονται και αυτά που λαμβάνονται). Η καταγραφή μέσω των προτύπων σύνδεσης του χρήστη, απαιτεί περεταίρω επεξεργασία γιατί πολλά streams εφαρμογών μπορεί να λειτουργούν ταυτοχρόνως ή σε σειρές πάνω από ένα κύκλωμα. *Παρατηρώντας το περιεχόμενο χρήστη*. Ενώ το περιεχόμενο στο τελικό χρήστη (user end) είναι κρυπτογραφημένο , οι συνδέσεις σε ανταποκριτές μπορεί να μην είναι (όντως, η ίδια ιστοσελίδα ανταπόκρισης μπορεί να είναι εχθρική).

Ενώ το φιλτράρισμα περιεχομένου δεν αποτελεί πρωταρχικός στόχος του Onion Routing, το tor χρησιμοποιεί απευθείας το Privoxy και σχετικές υπηρεσίες φιλτραρίσματος για ανωνυμοποιήσει τις ροές δεδομένων εφαρμογής.
*Λειτουργία ευδιακρισίας(*distinguishability*).*

Επιτρέπουμε στους πελάτες να επιλέγουν λειτουργίες ρύθμισης. Για παράδειγμα , οι πελάτες που ενδιαφέρονται για το αίτημα της συνδεσιμότητας θα πρέπει να αναστρέφουν τα κυκλώματα πιο συχνά από εκείνους που ενδιαφέρονται για την ανιχνευσιμότητα.
Η επιλογή του να έχεις τη δυνατότητα να επιτρέπεις (allowing choice) μπορεί να προσελκύσει χρήστες με διαφορετικές ανάγκες , αλλά οι πελάτες που είναι σε μειοψηφία μπορεί να χάσουν περισσότερη ανωνυμία ,γινόμενοι ευδιάκριτοι , απ'ότι να κερδίσουν , βελτιστοποιώντας τη συμπεριφορά τους.
Συνεχόμενος συσχετισμός συγχρονισμού. Το Tor δεν είναι αρκετά ικανό να κρύψει τέτοιους συσχετισμούς.
Ο εισβολέας παρακολουθεί τα πρότυπα δεδομένων στον εκκινητή και ο ανταποκριτής θα είναι σε θέση να επιβεβαιώσει την αντιστοιχία με μεγάλη πιθανότητα. Η μεγαλύτερη προστασία από τέτοια επικύρωση , η οποία είναι και προσφάτως διαθέσιμη, είναι να κρύψει την σύνδεση ανάμεσα στο μεσολαβητή Onion (onion proxy) και τον πρώτο κόμβο tor , εκτελώντας το OP στο κόμβο tor ή πίσω από ένα τείχος προστασίας .
Αυτή η προσέγγιση απαιτεί από έναν παρατηρητή να διαχωρίσει τη προέλευση δεδομένων στο onion router από τα δεδομένα που διέρχονται από αυτό : ένας παγκόσμιος παρατηρητής μπορεί να το κάνει αυτό , αλλά μπορεί να είναι πέρα από τις περιορισμένες ικανότητες ενός παρατηρητή.
Συνεχόμενος συσχετισμός μεγέθους. Η απλή καταμέτρηση του πακέτου θα είναι επίσης αποτελεσματική στην επιβεβαίωση του τελικού σημείου του stream.
Παρ'όλα αυτά, ακόμα και χωρίς το padding (σωστή τοποθέτηση), μπορεί να έχουμε κάποια περιορισμένη προστασία : Η τοπολογία leaky pipe σημαίνει ότι διάφοροι αριθμοί πακέτων μπορεί να εισέρθουν στο ένα άκρο του κυκλώματος και να εξέρθουν από το άλλο.
Ιστότοπος δακτυλικών αποτυπωμάτων. Όλες οι αποτελεσματικές παθητικές επιθέσεις ,άνωθεν, είναι επιθέσεις επιβεβαίωσης δεδομένων, κάτι το οποίο τις βγάζει έξω από τους στόχους του σχεδιασμού μας .

Υπάρχει επίσης μια παθητική επίθεση ανάλυσης δεδομένων που είναι δυνητικά αποτελεσματική. Αντί να ψάχνει συνδέσεις εξόδου για τους συσχετισμούς συγχρονισμού και όγκου , ο αντίπαλος μπορεί να κατασκευάσει-φτιάξει μια βάση δεδομένων "δακτυλικών αποτυπωμάτων" (fingerprints) εμπεριέχοντας το μέγεθος των αρχείων και μοτίβα πρόσβασης για στοχευμένες ιστοσελίδες. Αργότερα μπορεί να επιβεβαιώσει τη σύνδεση ενός χρήστη σε ένα συγκεκριμένο site συμβουλευόμενος τη βάση δεδομένων. Έχει αποδειχθεί ότι αυτή η επίθεση είναι αποτελεσματική κατά του ασφαλούς δικτύου (safe web). Μπορεί να είναι λιγότερο αποτελεσματική κατά του TOR , καθώς τα streams πολλαπλασιάζονται στο ίδιο κύκλωμα, και τα δακτυλικά αποτυπώματα -το fingerprinting θα περιορίζεται στο βαθμό ανάλυσης των κυψελών (Προς το παρόν 512 bytes). Πρόσθετες άμυνες θα μπορούσαν να περιλαμβάνουν μεγαλύτερα μεγέθη κυψελών, συστήματα padding σε websites σε μεγάλες ομάδες, σωστή τοποθέτηση συνδέσμου (link padding) και μακράς εμβέλειας ανδρείκελα.

<u>Ενεργητικές επιθέσεις</u>

Εκτεθειμένα keys (παράμετροι αλγόριθμου κρυπτογράφησης): Ένας εισβολέας που μαθαίνει τα session keys του TLS πρωτοκόλλου μπορεί να δει τις κυψελίδες ελέγχου και τις κρυπτογραφημένες κυψελίδες αναμετάδοσης σε κάθε κύκλωμα σ' αυτή τη σύνδεση, δηλαδή μαθαίνοντας το session key του επιτρέπει να ξετυλίξει ένα στρώμα της κρυπτογράφησης.

Ένας εισβολέας που μαθαίνει τα κλειδιά ασφαλείας του TLS πρωτοκόλλου των OR μπορεί να μιμηθεί αυτό το OR για όλη τη διάρκεια της ζωής του κλειδιού ασφαλείας για το TLS πρωτόκολλο, αλλά επίσης πρέπει να μάθει το onion key για αποκρυπτογράφηση των κυψελίδων δημιουργίας. Από την άλλη πλευρά, ένας εισβολέας που μαθαίνει τον κωδικό ταυτότητας ενός κόμβου μπορεί να αντικαταστήσει αυτό τον κόμβο αόριστα στέλνοντας νέες πλαστές περιγραφές στους διακομιστές καταλόγου.

Επαναλαμβανόμενοι κίνδυνοι*:* Ένας περιπλανώμενος εισβολέας που μπορεί να εκθέσει τα OR θα μπορούσε και να καταρρίψει το κύκλωμα εκθέτοντας τους κόμβους μέχρι να φτάσει στο τέλος. Αν, παρ' ολ' αυτά, ο εισβολέας δεν ολοκληρώσει την επίθεση στο χρόνο ζωής του κυκλώματος, τα OR θα έχουν απορρίψει τις απαραίτητες πληροφορίες πριν η επίθεση ολοκληρωθεί. Το πρωτόκολλο Java Anon πρόσφατα βίωσε την ανάγκη για αυτή την προσέγγιση, όταν ένα γερμανικό δικαστήριο τους ανάγκασε να προσθέσουν μια πίσω πόρτα στον κόμβο τους.

Εκτέλεση του δέκτη*:* Ένας αντίπαλος εκτελώντας σε έναν διακομιστή δικτύου επιπόλαια μαθαίνει τα μοτίβα συγχρονισμού των χρηστών συνδεόμενων σ' αυτόν, και μπορεί να εισάγει αυθόρμητα μοτίβα στις ανταποκρίσεις του. Επιθέσεις απ' άκρη σ' άκρη γίνονται ευκολότερες: Αν ο αντίπαλος μπορεί να προκαλέσει τους χρήστες να συνδεθούν στο διακομιστή ιστού του, είτε κρατά μια άκρη από τις συνδέσεις του.

Εκτέλεση του πρωτοκόλλου onion*:* Αναμένεται ότι οι τελικοί χρήστες σχεδόν πάντα θα εκτελούν το δικό τους τοπικό onion πρωτόκολλο. Παρ' ολ' αυτά, σε μερικές ρυθμίσεις, μπορεί να είναι απαραίτητο για το πρωτόκολλο να εκτελεστεί μακρόθεν, δηλαδή τυπικά σε ιδρύματα που θέλουν να ελέγχουν τις δραστηριότητες αυτών που συνδέονται στο πρωτόκολλο. Εκθέτοντας ένα onion πρωτόκολλο διακυβεύονται όλες οι μελλοντικές συνδέσεις μέσω αυτού.

Μη παρατηρήσιμοι κόμβοι λειτουργικού συστήματος δίσκου**:** Ένας παρατηρητής που μπορεί μόνο να παρατηρήσει τμήμα από το Tor δίκτυο μπορεί να αυξήσει την αξία αυτών των δεδομένων επιτίθοντας στους αόρατους κόμβους για να τους κλείσει, να μειώσει την αξιοπιστία τους, ή να πείσουν χρήστες ότι δεν είναι άξιοι εμπιστοσύνης. Η καλύτερη άμυνα εδώ είναι η ευρωστία.

Εκτέλεση σε εχθρικό OR*:* Για να είμαστε τοπικοί παρατηρητές, ένας απομονωμένος εχθρικός κόμβος μπορεί να δημιουργήσει κυκλώματα μέσω του εαυτού του , ή να παραλλάξει μοτίβα ροής δεδομένων για να επηρεάσει τα δεδομένα στους άλλους κόμβους. Ωστόσο, ένας εχθρικός κόμβος πρέπει άμεσα να γειτνιάσει και με τα δυο τελικά άκρα για να διακυνδινεύσει η ανωνυμία του κυκλώματος.

Εισαγωγή συγχρονισμού στα μηνύματα: Αυτό είναι απλά μια ισχυρότερη εκδοχή της παθητικής επίθεσης συγχρονισμού που συζητήθηκε νωρίτερα.

Σημειακές επιθέσεις*:* Ένας εχθρικός κόμβος θα μπορούσε να επισυνάψει μια κυψελίδα παραλλάσσοντας την.

***Αντικατάσταση περιεχομένων μη αυθεντικών* πρωτοκόλλων**

Αναπαραγωγή επιθέσεων: Κάποια πρωτόκολλα ανωνυμίας είναι ευάλωτα στην παραγωγή επιθέσεων.

Συκοφαντικές επιθέσεις*:* Ένας εισβολέας θα μπορούσε να χρησιμοποιήσει το Tor δίκτυο για κοινωνικά κατακριτέες πράξεις, για να φέρει το δίκτυο σε δυσφήμιση και να καταφέρει τους λειτουργούς να το κλείσουν.

Διανομή εχθρικού κωδικού: Ένας εισβολέας θα ξεγελούσε τους χρήστες για να εκτελέσουν υπομονευτικά λογισμικά του Tor, που στην πραγματικότητα, δεν ανωνυμοποιούν τις συνδέσεις τους, ή χειρότερα, θα ξεγελάσουν OR για να εκτελέσουν αποδυναμωμένα λογισμικά που παρέχουν σε χρήστες λιγότερη ανωνυμία.

Για να εμποδίσουμε έναν εισβολέα από το να υπομονεύσει την ίδια την επίσημη κυκλοφορία (μέσω απειλών, δωροδοκιών, ή εκ των έσω επιθέσεων), παρέχουμε όλες τις κυκλοφορίες σε μορφή πηγαίου κώδικα, ενθαρρύνουμε πηγαίο λογιστικό έλεγχο, και συχνά να προειδοποιούμε τους χρήστες μας ποτέ να μην εμπιστεύονται κανένα λογισμικό (ακόμα και από μας) που εμφανίζεται χωρίς προέλευση.

Επιθέσεις καταλόγου

Καταστροφή διακομιστών καταλόγου: Αν λίγοι διακομιστές καταλόγου εξαφανιστούν, οι άλλοι ακόμα συστήνουν έναν αξιόλογο κατάλογο. Αν ένας διακομιστής ελέγχου παραμείνει λειτουργικός, θα εξακολουθούν να εκπέμπουν την κατάσταση του δικτύου τους και να παράγουν έναν κοινό αποδεκτό κατάλογο.

Υπονόμευση ενός διακομιστή καταλόγου

Υπονόμευση της πλειοψηφίας διακομιστών καταλόγου

Ενθάρρυνση διαφωνίας του διακομιστή καταλόγου: Το πρωτόκολλο συμφωνίας καταλόγου βεβαιώνει ότι οι λειτουργοί του διακομιστή καταλόγου συμφωνούν στις ρυθμίσεις του διακομιστή καταλόγου.

Εξαπάτηση του διακομιστή καταλόγου κατά την καταχώρηση εχθρικών OR

Να πειστούν οι κατάλογοι ότι ένα δυσλειτουργικό OR λειτουργεί: Στην τρέχουσα εκτέλεση του Tor, οι διακομιστές καταλόγου διαβεβαιώνουν ότι ένα OR εκτελείται σωστά αν μπορούν να ξεκινήσουν μια TLS σύνδεση με αυτό.

Επιθέσεις ενάντια στα rendezvous points

-Να Γίνουν πολλά αιτήματα σύστασης
-Να φτιάξουν πολλούς εξυπηρετητές σύστασης
-Επίθεση ενός σημείου σύστασης
-Έκθεση ενός σημείου σύστασης
-Έκθεση ενός rendezvous point.

Μελλοντικές κατευθύνσεις

Το Tor συγκεντρώνει πολλές καινοτομίες σε ένα ενωμένο και αναπτυγμένο σύστημα. Τα αμέσως επόμενα βήματα συμπεριλαμβάνουν:

Επεκτασιμότητα: Η έμφαση του Tor στην ανάπτυξη του και στη σχεδιαστική του απλότητα μας έχουν οδηγήσει στην υιοθέτηση μιας κορυφής τοπολογίας, ημικεντρικών κατευθύνσεων, και ενός προτύπου διαδικτύου ορατού απ' όλες τις πλευρές για την γνώση των πελατών/ το λογισμικό client. Αυτές οι ιδιότητες δεν θα απαιτούν να ξεπεράσουν (σε αριθμό;) λίγες εκατοντάδες διακομιστών. Η ενότητα 9 περιγράφει μερικές υποσχόμενες προσεγγίσεις, αλλά περισσότερη εμπειρία ανάπτυξης θα ήταν εξυπηρετική στην μάθηση της σχετικής σημασίας αυτών των στενωπών.

Τάξεις ευρείας ζώνης: Αυτή η δημοσίευση υποθέτει ότι όλα τα ORs έχουν καλή ευρεία ζώνη και αφάνεια. Θα έπρεπε αντιθέτως να υιοθετήσουν πρότυπο του MorphMix, όπου οι κόμβοι διαφημίζουν/ αναγράφουν το επίπεδο ευρείας ζώνης τους (DSL, T1, T3), και η Αλίκη αποφεύγει τις στενωπούς διαλέγοντας κόμβους που ταιριάζουν ή ξεπερνούν το εύρος ζώνης της. Μ' αυτόν τον τρόπο χρήστες DSL συμμετέχουν στο δίκτυο Tor.

Κίνητρα*:* Εθελοντές που εκτελούν σε κόμβους ανταμείβονται με δημοσιότητα και πιθανόν καλύτερη ανωνυμία. Περισσότεροι κόμβοι σημαίνουν περισσότερη επεκτασιμότητα, και περισσότεροι χρήστες σημαίνει περισσότερη ανωνυμία. Χρειάζεται να συνεχίσουμε να εξετάζουμε τις κινητήριες δομές για να συμμετέχουμε στο Tor.

Επιπλέον, χρειάζεται να εξερευνήσουμε περισσότερες προσεγγίσεις για μείωση της κατάχρησης, και να καταλάβουμε γιατί περισσότεροι άνθρωποι δεν ενοχλούνται με τη χρήση ιδιωτικών συστημάτων.

Κάλυψη δεδομένων*:* Επί του παρόντος, το Tor παραλείπει την κάλυψη δεδομένων (τα κόστη του στην εκτέλεση στην ευρεία ζώνη είναι καθαρά αλλά τα οφέλη της ασφάλειας του δεν είναι κατανοητά). Πρέπει να επιδιώξουμε περισσότερη έρευνα στην κάλυψη δεδομένων σε επίπεδο συνδέσμων και μεγάλης εμβέλειας κάλυψης δεδομένων για να ορίσουμε αν μερικές απλές μέθοδοι κρυπτογράφησης προσφέρουν ευαπόδεικτη προστασία ενάντια στους επιλεγμένους εισβολείς μας.

Κρύψιμο στους κόμβους εξόδου *(ανάσυρση αιτημάτων):* Ίσως κάθε κόμβος εξόδου θα έπρεπε να εκτελεί ένα πρωτόκολλο για τις κρυφές ιστοσελίδες για να βελτιώσουν την ανωνυμία των κρυφών σελίδων, δηλαδή τα αιτήματα της Αλίκης δεν εγκαταλείπουν το Tor, για να βελτιώσουν την ταχύτητα και τη μείωση του κόστους ευρείας ζώνης. Από την άλλη πλευρά, η εμπρόσθια ασφάλεια αποδυναμώνεται διότι οι κρυφές σελίδες συγκροτούν ένα αρχείο από ανακτημένους φακέλους. Πρέπει να βρούμε τη σωστή ισορροπία μεταξύ χρηστικότητας και αφάνειας.

Καλύτερη διανομή καταλόγου*:* Επί του παρόντος, οι πελάτες μεταφορτώνουν μια περιγραφή του δικτύου ανά 15 λεπτά. Καθώς η κατάσταση αναπτύσσεται, και οι πελάτες πληθαίνουν, μπορεί να χρειαζόμαστε μια λύση στην οποία οι πελάτες σταδιακές ενημερώσεις για την κατάσταση του καταλόγου. Γενικότερα, πρέπει να βρούμε επεκτάσιμους αλλά και πρακτικούς τρόπους για την διανομή ενημέρωσης του στιγμιοτύπου της κατάστασης του δικτύου χωρίς την είσοδο νέων επιθέσεων.

Επιπλέον ανασκόπηση προδιαγραφών*:* Οι δημόσιες προδιαγραφές μας του byte-level χρειάζεται εξωτερική επανεξέταση. Ελπίζουμε ότι καθώς το Tor αναπτύσσεται , όλο και περισσότεροι χρήστες θα εξετάζουν τις προδιαγραφές του.

Πολυσυστημική διαλειτουργικότητα*:* Επί του παρόντος, δουλεύουμε με σχεδιαστή του MorphMix για να ενοποιήσουμε τις προδιαγραφές και τις εκτελέσεις των κοινών σημείων των συστημάτων μας. Ως ώρας, αυτό αναμένεται να είναι σχετικά ευθύ/ αποτελεσματικό (σαν λύση δηλαδή, σαν ειλικρινής προσπάθεια). Η διαλειτουργικότητα θα επιτρέψει τη σωστή και άμεση σύγκριση των δυο σχεδίων για εμπιστοσύνη και επεκτασιμότητα.

Ανάπτυξη ευρύτερης κλίμακας*:* Ο αρχικός στόχος του Tor ήταν να αποκτήσει εμπειρία στην ανάπτυξη και την ανωνυμοποίηση στην επικάλυψη του δικτύου, και να μάθει έχοντας πραγματικούς χρήστες. Είμαστε πλέον στο σημείο σχεδίασης και ανάπτυξης όπου ξεκινάμε την σύσταση ενός ευρύτερου δικτύου. Αφού αποκτήσουμε πολλούς πραγματικούς χρήστες θα είμαστε αναμφίβολα καλύτερα ικανοί να εκτιμήσουμε μερικές από τις αποφάσεις για το σχεδιασμό, συμπεριλαμβανομένων των διλημμάτων ευρωστίας/ αφάνειας, τα διλήμματα εκτέλεσης (π.χ., το μέγεθος των κυψελίδων), τους μηχανισμούς μας άμυνας ενάντια στην κατάχρηση και της συνολικής χρηστικότητας μας.

6. ΚΕΦΑΛΑΙΟ 6 :TOR vs I2P

6.1. Γενικά

Τα ανώνυμα δίκτυα ορίζουν ένα σύστημα επικοινωνίας μεταξύ ομοτίμων χρηστών ή/και κόμβων ώστε να επιτυγχάνεται η αλλοίωση της ταυτότητας των χρηστών αλλά και η προστασία των δεδομένων που διακινούνται από μη εξουσιοδοτημένη ανάγνωση.

Ανώνυμα δίκτυα (Anonymous Networks ή Darknets) ονομάζουμε δίκτυα που ως στόχο έχουν να παρέχουν στους συμμετέχοντες, ανωνυμία και ασφάλεια στην επικοινωνία. Τα ανώνυμα δίκτυα, είναι δίκτυα πάνω σε δίκτυο(network over a network), δηλαδή εδράζονται στην υπάρχουσα δικτυακή υποδομή παγκοσμιώς, το Internet. Χρησιμοποιώντας το κατάλληλο λογισμικό σε τερματικούς υπολογιστές, δημιουργούνται συνδέσεις και εικονικά κανάλια/τούνελ ανάμεσα σε διαφορετικούς υπολογιστές σε διαφορετικές τοποθεσίες του πλανήτη. Αν φανταστούμε το Internet ως ένα τεράστιο δίχτυ με πολλούς κόμβους συνδεδεμένους ποικιλλοτρόπως, τα ανώνυμα δίκτυα είναι επιπλέον ιστοί που ακουμπάνε πάνω στο Internet, και συνδέουν συγκεκριμένους κόμβους μεταξύ τους, χρησιμοποιώντας κατά κανόνα κρυπτογράφηση στην επικοινωνία.

Στο εσωτερικό του ανώνυμου δικτύου, εγκαθιδρύεται επικοινωνία ανταλλαγής δεδομένων χωρίς να είναι δυνατόν σε κάποιον εξωτερικό παρατηρητή ή ακόμα και σε κάποιον μη-εξουσιοδοτημένο εντός του ανώνυμου δικτύου, να διαβάσει τα δεδομένα αυτά. Ανάλογα με τα χαρακτηριστικά του εκάστοτε ανώνυμου δικτύου, παρέχονται διαφορές υπηρεσίες (web browsing, file sharing) στους χρήστες, ενώ κάποια ανώνυμα δίκτυα υλοποιούν καλύτερα κάποιες από αυτές.

Η συνήθης αντίληψη και χρήση των ανωνύμων δικτύων είναι να αντιμετωπίζονται ώς ένα δίκτυο ενδιάμεσων κόμβων για την κάλυψη της επικοινωνίας του χρήστη. Αντιμετωπίζεται δηλαδή ως ένα σύνολο από proxies, απομακρυσμένων υπολογιστών, οι οποίοι προωθούν τα ερωτήματα και τις απαντήσεις του χρήστη προς τον τελικό προορισμό(πχ έναν web server). Ο χρήστης του ανώνυμου δικτύου χρησιμοποιώντας κρυπτογράφηση στην επικοινωνία του με τους επόμενους ενδιάμεσους κόμβους, διασφαλίζει ότι κάποιος που παρακολουθεί την δικτυακή κίνηση αυτού ή των επόμενων κόμβων, δεν θα διαβάζει τα δεδομένα. Χρησιμοποιώντας την αλυσίδα αυτή ή tunnel ή εικονικά μονοπάτια, αποκρύπτει την ταυτότητά του(IP address) από τον τελικό αποδέκτη των ερωτημάτων, που είναι κάποιος server στο διαδίκτυο. Στην ουσία χρησιμοποεί την ταυτότητα του τελευταίου κόμβου στην αλυσίδα, του κόμβου-εξόδου(exit node) προς το Internet. Επομένως θα λέγαμε πιο σωστά ότι τα δίκτυα αυτά εξασφαλίζουν ψευδωνυμία και όχι ανωνυμία.

Πέραν από την χρήση των darknets ως μέσο για να αλλοιώσουμε την ταυτότητά μας στο Internet, μπορούμε να χρησιμοποιήσουμε τις δυνατότητες και υπηρεσίες που προσφέρουν αποκλειστικά στο εσωτερικό τους. Μπορούμε δηλαδή, πέραν από το να κρύβουμε την IP μας ενώ επισκεπτόμαστε ένα site στο Internet, να χρησιμοποιήσουμε το Darknet για να μοιραστούμε αρχεία, ανώνυμα με άλλους χρήστες του δικτύου, να στήσουμε κρυφές υπηρεσίες(hidden services) προσβάσιμες μόνο εντός του δικτύου κλπ.

Κάποια δημοφιλή darknets είναι το Tor, το i2p και το Freenet. Ανάλογα με τον σχεδιασμό του, το κάθε darknet προσανατολίζεται σε κάποιες λειτουργίες, τις οποίες και υλοποιεί καλύτερα. Για παράδειγμα το Tor χρησιμοποιείται περισσότερο για web browsing και hidden services, το Freenet περισσότερο για file sharing, το i2p για hidden services, τις ενσωματωμένες εσωτερικές υπηρεσίες.

<u>Το TOR:</u>

Το Tor (The onion router) είναι ένα σύστημα που προσφέρει ανωνυμία στο διαδίκτυο. Το λογισμικό του Tor δρομολογεί τη διαδικτυακή κίνηση των χρηστών διαμέσου ενός δικτύου από servers σε όλο τον κόσμο, με σκοπό να αποκρύψει την ταυτότητα των χρηστών από οποιονδήποτε μπορεί να παρακολουθεί την διαδικτυακή κίνηση.Το Tor αναπτύσσεται από τον μη κερδοσκοπικό οργανισμό Tor Project και χρησιμοποιείται από ένα ευρύ φάσμα ανθρώπων για πολλούς και διαφορετικούς σκοπούς, είναι ένα δίκτυο από εικονικά τούνελ (virtual tunnels) που επιτρέπει σε άτομα και ομάδες ατόμων να βελτιώσουν την ιδιωτικότητα (privacy) και την ασφάλειά (secutiry) τους στο διαδίκτυο. Αποτελεί την βάση για μια ποικιλία εφαρμογών λογισμικού που χρησιμοποιούνται για τον διαμοιρασμό πληροφοριών σε δημόσια δίκτυα χωρίς να απειλείται η ιδιωτικότητα των εμπλεκομένων.

Μέσω του Tor, άτομα αποφεύγουν την καταγραφή της ταυτότητάς τους από τα websites που επισκέπτονται, αλλά και την καταγραφή της διαδικτυακής τους κίνησης από τον τηλεπικοινωνιακό τους πάροχο(Internet Service Provider). Σε άλλες περιπτώσεις, καταφέρνουν να παρακάμπτουν τους περιορισμούς που επιβάλλουν κυβερνήσεις ή πάροχοι, οι οποίοι μπλοκάρουν συγκεκριμένους ιστότοπους. Οι κρυφές υπηρεσίες του Tor (Tor's Hidden Services) επιτρέπουν στους χρήστες του Tor να δημοσιεύουν την δικιά τους ιστοσελίδα ή άλλη υπηρεσία, χωρίς να αποκαλύπτεται η τοποθεσία ή η ταυτότητά τους. Σε άλλες περιπτώσεις το Tor χρησιμοποιείται για την καταγγελία κοινωνικά ευαίσθητων πληροφοριών όπως βιασμοί ή κακοποιήσεις, για εργοδοτικές αυθαιρεσίες, διαρροές κυβερνητικών εγγράφων προς τον Τύπο και άλλα.Η ποικιλομορφία των χρηστών του Tor, η παγκόσμια διάδοσή του και οι ετερογενείς λόγοι χρήσης του, αποτελούν ένα ακόμα προτέρημα του Tor δικτύου. Και αυτό διότι η χρήση του Tor από ένα άτομο, ακόμα κι αν γίνει αντιληπτή από κάποιον τρίτο, δεν τον κατατάσσει αυτόματα σε μια συγκεκριμένη κοινωνική ομάδα, ούτε αναγνωρίζονται αυτόματα οι λόγοι που τον ώθησαν να το χρησιμοποιήσει. Η ετερογένεια και το πλήθος των χρηστών του Tor Δικτύου είναι ένας παράγοντας αύξησης της ανωνυμίας του μεμονωμένου χρήστη.

Η χρήση του Tor μειώνει την πιθανότητα επιτυχίας κάποιου που κατασκοπεύει/επιτηρεί την διαδικτυακή κίνηση του χρήστη, με απλές ή περισσότερο πολύπλοκες μεθόδους (traffic analysis). Για να γίνει αυτό, το Tor κατανέμει την δικτυακή κίνηση μεταξύ διαφόρων σημείων στο Διαδίκτυο, ούτως ώστε κανένα από τα σημεία αυτά να μην μπορεί να συσχετίσει τον χρήστη με τον τελικό προορισμό του. Η ιδέα προσομοιάζει στο να χρησιμοποιείς μια μπερδεμένη διαδρομή, για να ξεφορτωθείς κάποιον που σε ακολουθεί - και όποτε μπορείς να σβήνεις και τα ίχνη σου. Αντί να πάρεις την πιο σύντομη και άμεση διαδρομή από την αφετηρία στον προορισμό, τα πακέτα δεδομένων στο δίκτυο του Tor παίρνουν ένα τυχαίο μονοπάτι, μέσω ενδιάμεσων κόμβων που καλύπτουν τα ίχνη του χρήστη. Έτσι, κανένας παρατηρητής σε συγκεκριμένο σημείο της διαδρομής στο Διαδίκτυο, δεν μπορεί να συμπεράνει από που πρόηλθαν τα δεδομένα και για που προορίζονται.Για να δημιουργήθεί ένα ιδιωτικό δικτυακό μονοπάτι με το Tor, το λογισμικό που ο χρήστης έχει εγκαταστήσει και τρέχει στον υπολογιστή του, κατασκευάζει αναδρομικά μια ακολουθία/κύκλωμα κρυπτογραφημένων συνδέσεων μέσω κόμβων στο δίκτυο. Το κύκλωμα αυτό εκτείνεται από κόμβο προς κόμβο, και κάθε στιγμή ο κάθε κόμβος στο μονοπάτι γνωρίζει μόνο τον προηγούμενο από τον οποίο έλαβε τα δεδομένα και τον επόμενο στον οποίο στέλνει τα δεδομένα. Κανένας κόμβος ξεχωριστά, δεν γνωρίζει ολόκληρη τη διαδρομή των δεδομένων. Το λογισμικό του χρήστη, διαπραγματεύεται ένα ξεχωριστό σετ κλειδιών κρυπτογράφησης για κάθε βήμα στο κύκλωμα που επέλεξε, για να διασφαλίζει ότι κάθε κόμβος δεν θα μπορεί να ανιχνεύσει την κίνηση την οποία δρομολογεί.

Αφού κατασκευαστεί και εγκαθιδρυθεί επικοινωνία στο κύκλωμα, ο χρήστης μπορεί να μεταφέρει δεδομένα διαφόρων ειδών, όπως επίσης να λειτουργήσει διαφορετικές εφαρμογές με βάση το Tor δίκτυο (για παράδειγμα instant messaging πάνω από το Tor, εφαρμογές email κλπ).

Ο κάθε κόμβος του κυκλώματος, είναι γνώστης μόνο ενός βήματος του μονοπατιού, επομένως ένας κακόβουλος ή ακόμα και μολυσμένος κόμβος, δεν μπορεί να προσδιορίσει την ροή των δεδομένων από άκρη σε άκρη.

Το I2P:

Το i2p είναι ένα project που αφορά στην κατασκευή, ανάπτυξη και διατήρηση ενός δικτύου που θα υποστηρίζει ασφαλή και ανώνυμη επικοινωνία. Οι άνθρωποι που χρησιμοποιούν το i2p όρίζουν οι ίδιοι τις ισορροπίες μεταξύ ανωνυμίας, αξιοπιστίας, χρήσης bandwidth και αποκρισιμότητας. Δεν υπάρχει κανένα κεντρικό σημείο στο δίκτυο, που θα μπορούσε να καταστεί ευάλωτο σε πιέσεις ή επιθέσεις, μειώνοντας ή εξαλείφοντας την ακεραιότητα, την ασφάλεια και την ανωνυμία του δικτύου. Το δίκτυο υποστηρίζει δυναμική αναδιάρθρωση ως απάντηση σε διάφορες επιθέσεις και έχει σχεδιαστεί για να χρησιμοποιεί πρόσθετους πόρους μόλις αυτοί γίνουν διαθέσιμοι. Φυσικά κάθε πτυχή του δικτύου είναι ανοιχτή και ελεύθερα διαθέσιμη.

Σε αντίθεση με άλλα ανώνυμα δίκτυα, το i2p δεν προσπαθεί να προσφέρει ανωνυμία με το να κρύβει την πηγή της επικοινωνίας και όχι τον προορισμό ή το αντίστροφο. Το i2p είναι σχεδιασμένο να επιτρέπει σε ομότιμους χρήστες να επικοινωνούν μεταξύ τους ανώνυμα - τόσο ο αποστολέας όσο και ο παραλήπτης είναι μη αναγνωρίσιμοι μεταξύ τους αλλά και απο κάποιον τρίτο. Σήμερα υπάρχουν τόσο "εσωτερικά" websites (το i2p επιτρέπει τη δημιουργία ανωνύμων website) όσο και servers που λειτουργούν σαν proxies προς το "κανονικό" Internet, επιτρέποντας την ανώνυμη πλοήγηση . Η ύπαρξη servers μέσα στο δίκτυο i2p, που προσφέρουν ενσωματωμένες εσωτερικές υπηρεσίες (web, mail, chat) είναι θεμελιώδης, θεωρώντας πως οποιοσδήποτε proxy server προς το Internet μπορεί να παρακολουθείται, να είναι ανενεργός ή ακόμα να έχει καταληφθεί με σκοπό τη διενέργεια κακόβουλων επιθέσεων.

Το δίκτυο βασίζεται στα μηνύματα - πρόκειται για ένα ασφαλές και ανώνυμο IP στρώμα, όπου τα μηνύματα απευθύνονται σε κρυπτογραφικά κλειδιά (προορισμοί) και μπορεί να είναι αρκετά μεγαλύτερα από τα συνήθη IP πακέτα. Κάποια παραδείγματα χρήσης του δικτύου περιλαμβάνουν τα "eepsites" (webservers που σερβίρουν περιεχόμενο μέσα στο i2p), διαμοιρασμό αρχείων με το BitTorrent πρωτόκολλο ή ακόμα και κατανεμημένη αποθήκευση δεδομένων. Χρησιμοποιώντας τα tunnel μεταξύ ομοτίμων που χτίζει η εφαρμογή του i2p, πολλές κλασικές εφαρμογές/προγράμματα TCP/IP (όπως ssh, IRC, cache proxies ακόμα και stream ήχου) λειτουργούν αποτελεσματικά και διοχετεύονται στο δίκτυο. Οι περισσότεροι άνθρωποι δεν χρησιμοποιούν απευθείας το i2p, αντίθετα χρησιμοποιούν τις διάφορες ειδικές εφαρμογές που πατάνε πάνω του ή απλώς ενεργοποιούν το i2p για τις υπόλοιπες εφαρμογές.

Εικόνα 27: Διαφορές του TOR και του I2P

Tor	**I2P**
Cell	Message
Client	Router or Client
Circuit	Tunnel
Directory	NetDb
Directory Server	Floodfill Router
Entry Guards	Fast Peers
Entry Node	Inproxy
Exit Node	Outproxy
Hidden Service	Hidden Service, Eepsite or Destination
Hidden Service Descriptor	LeaseSet
Introduction point	Inbound Gateway
Node	Router
Onion Proxy	I2PTunnel Client (more or less)
Onion Service	Hidden Service, Eepsite or Destination
Relay	Router
Rendezvous Point	somewhat like Inbound Gateway + Outbound Endpoint
Router Descriptor	RouterInfo
Server	Router

Οφέλη του Tor

- Έχει πολύ μεγαλύτερη βάση χρηστών. Μεγαλύτερη προβολή δηλαδή στις ακαδημαϊκές κοινότητες.
- Έχει ήδη λύσει κάποια προβλήματα που το I2P έχει ακόμη να αντιμετωπίσει
- Έχει σημαντική χρηματοδότηση.
- Έχει περισσότερους προγραμματιστές, συμπεριλαμβανομένων αρκετών που χρηματοδοτούνται.
- Είναι πιο ανθεκτικό σε μπλοκαρίσματα σε κρατικό επίπεδο, λόγω των TLS στρωμάτων μεταφοράς και γεφυρών.
- Έχει σχεδιαστεί και έχει βελτιστοποιηθεί για την κυκλοφορία εξόδου, με ένα μεγάλο αριθμό κόμβων.
- Έχει καλύτερη τεκμηρίωση, δηλαδή έχει επίσημα έγγραφα και προδιαγραφές.
- Είναι αποτελεσματικό με τη χρήση της μνήμης.
- Οι κόμβοι πελάτη του Tor έχουν πολύ χαμηλό εύρος ζώνης.
- Έχει κεντρικό έλεγχο που μειώνει την πολυπλοκότητα σε κάθε κόμβο και μπορεί να αντιμετωπίσει αποτελεσματικά τις επιθέσεις Sybil
- Ένας πυρήνας των κόμβων υψηλής χωρητικότητας παρέχει υψηλότερη απόδοση και χαμηλότερο latency.
- Και τέλος δεν χρησιμοποιεί C, Java.

Οφέλη του I2P

- Έχει σχεδιαστεί και έχει βελτιστοποιηθεί για τις κρυφές υπηρεσίες, οι οποίες είναι πολύ πιο γρήγορες από ό, τι στο Tor.
- Έχει πλήρως κατανεμημένη οργάνωση.
- Οι χρήστες επιλέγονται με βάση το προφίλ και την κατάταξη των επιδόσεών τους.
- Οι Floodfill ("servers ") είναι πολλοί και αξιόπιστοι, και όχι ενσωματωμένοι.
- Το Peer-to-Peer είναι «φιλικό».
- Έχει μεταγωγή πακέτων αντί για μεταγωγή κυκλώματος.
- Έχει σήραγγες μιας κατεύθυνσης κυκλοφορίας αντί για αμφίδρομες, οι οποίες διπλασιάζουν τον αριθμό των κόμβων.
- Προστατεύει κατά την ανίχνευση δραστηριότητας του πελάτη, ακόμη και όταν ένας εισβολέας συμμετέχει στη σήραγγα.
- Οι σήραγγες I2P μειώνουν τον αριθμό των δειγμάτων που ένας εισβολέας μπορεί να χρησιμοποιήσει για να εξαπολύσουν μια ενεργή επίθεση.
- Οι I2P APIs έχουν σχεδιαστεί ειδικά για την ανωνυμία και την ασφάλεια.
- Ουσιαστικά όλοι οι χρήστες συμμετέχουν στη δρομολόγηση για τους άλλους.
- Το εύρος ζώνης γενικά είναι χαμηλό, ενώ στο Tor, ενώ οι κόμβοι πελάτη δεν απαιτούν μεγάλο εύρος ζώνης, δεν συμμετέχουν πλήρως στην mixnet.
- Έχει ενσωματωμένο μηχανισμό αυτόματης ενημέρωσης.
- Χρησιμοποιεί τόσο TCP όσο και UDP μεταφορές.
- Και τέλος ούτε αυτό χρησιμοποιεί Java.

Με λίγα λόγια:

Βλέπουμε ότι και το Tor και το I2P παρέχουν κρυπτογραφικες μεθόδους για να έχουν πρόσβαση σε πληροφορίες ανώνυμα και επικοινωνία με απευθείας σύνδεση. Το Tor παρέχει καλύτερη ανώνυμη πρόσβαση στο ανοιχτό διαδίκτυο και το I2P παρέχει μια πιο ισχυρή και αξιόπιστη πρόσβαση στο darknet.

Από μια άλλη σκοπιά υπάρχει μια θεμελιώδης διαφορά μεταξύ του I2P και του Tor. Το Tor λειτουργεί με την παροχή ενός μεσολαβητή στον τοπικό υπολογιστή μας που θα πρέπει να ρυθμίσουμε τις εφαρμογές μας για να το χρησιμοποιήσουμε. Σε αντίθεση, με το I2P, που χρησιμοποιείται συνήθως από εφαρμογές που έχουν γραφτεί ειδικά για να τρέξουν στο δίκτυο I2P. Αυτές περιλαμβάνουν, αλλά δεν περιορίζονται σε αυτά, άμεσα μηνύματα, κοινή χρήση αρχείων, e-mail, και κατανεμημένες εφαρμογές αποθήκευσης στο διαδίκτυο.

7. ΚΕΓΑΛΑΙΟ 7: Raspberry Pi

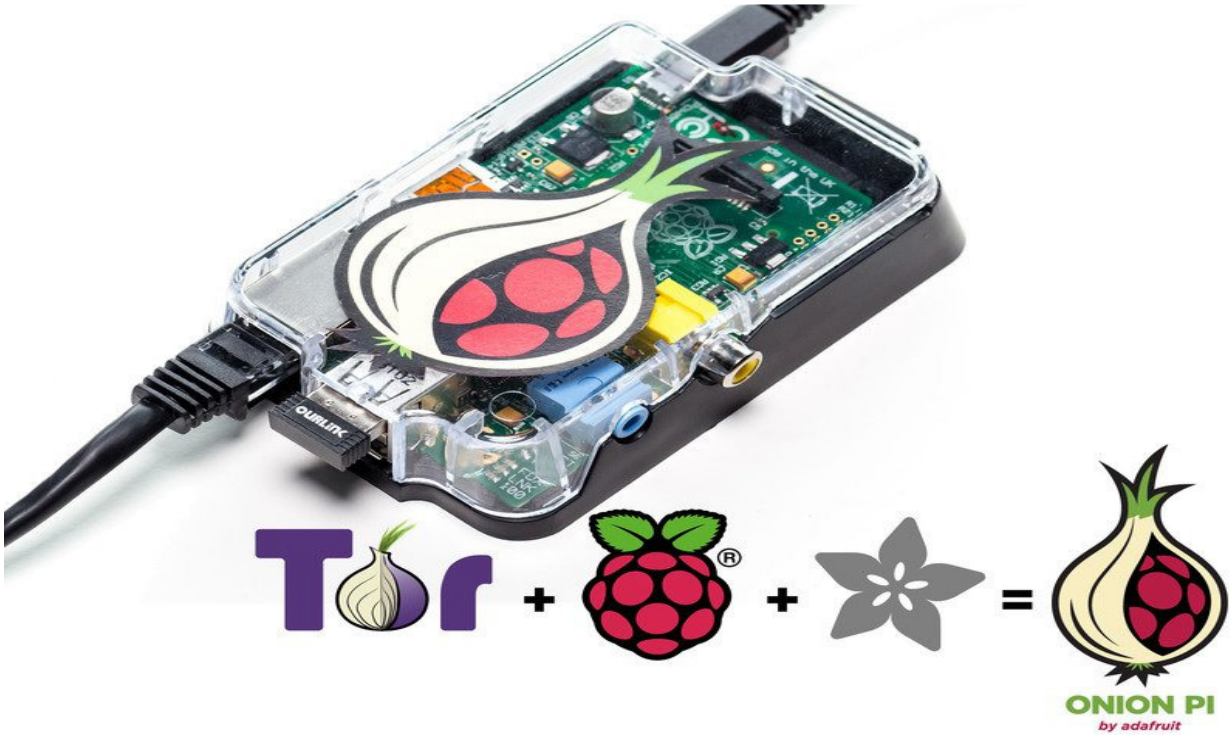
Το Raspberry Pi είναι ένας πλήρης υπολογιστής με μέγεθος πιστωτικής κάρτας.Παρά τον ελάχιστον όγκο του, το Raspberry Pi στη μεγαλύτερή έκδοσή του, διαθέτει τετραπύρηνο επεξεργαστή 1200MHz, διπύρηνη κάρτα γραφικών, 1GB RAM, μέχρι τέσσερις θύρες USB, έξοδο HDMI, τροφοδοτείται μέσω Micro USB, και διαθέτει 40 pins γενικής χρήσης για σύνδεση με άλλα ηλεκτρονικά και περιφερειακά. Η έκδοση Raspberry Pi 3 με τις παραπάνω προδιαγραφές κοστίζει γύρω στα 53 ευρώ στην Ελλάδα, ενώ μπορούμε να το αγοράσουμε και σαν μέρος ενός πλήρους Starter kit, με όσα χρειάζονται για να το αξιοποιήσουμε. Ενώ είναι εντυπωσιακό πώς αυτή η υπολογιστική ισχύς συγκεντρώνεται σε τόσο λίγο χώρο και με τόσο χαμηλό κόστος - σημαντικά χαμηλότερο από ενός smartphone - το ερώτημα είναι το τι μπορούμε να κάνουμε με το Raspberry Pi. Όπως αποδεικνύεται, με μεράκι και φαντασία οι εφαρμογές του Raspberry Pi είναι πρακτικά απεριόριστες.Κατ' αρχάς, συνδέοντάς το σε μια οθόνη και προσθέτοντας πληκτρολόγιο και ποντίκι, έχουμε έναν πλήρη υπολογιστή, ο οποίος υποστηρίζει συγκεκριμένες διανομές Linux. Με τα κατάλληλα πρόσθετα εξαρτήματα, όμως, το Raspberry Pi μπορεί να είναι η βάση για μια μικρογραφία καμπίνας ηλεκτρονικών παιχνιδιών, για μια κανονική καμπίνα, ενσωματωμένη σε τραπέζι, για να χρησιμοποιηθεί σαν "εγκέφαλος" σε συστήματα οικιακού αυτοματισμού, και μάλιστα με φωνητικές εντολές μέσω ενός iPhone, σαν χρονόμετρο για φωτογραφίες time-lapse, μέχρι και για τη δημιουργία ρομπότ. Μπορούμε ακόμα και να χρησιμοποιήσουμε το TOR πάνω σε αυτό όπως θα δούμε παρακάτω.

7.1. Raspberry Pi-TOR(tytorial)

7.2. Τι θα χρειαστείτε

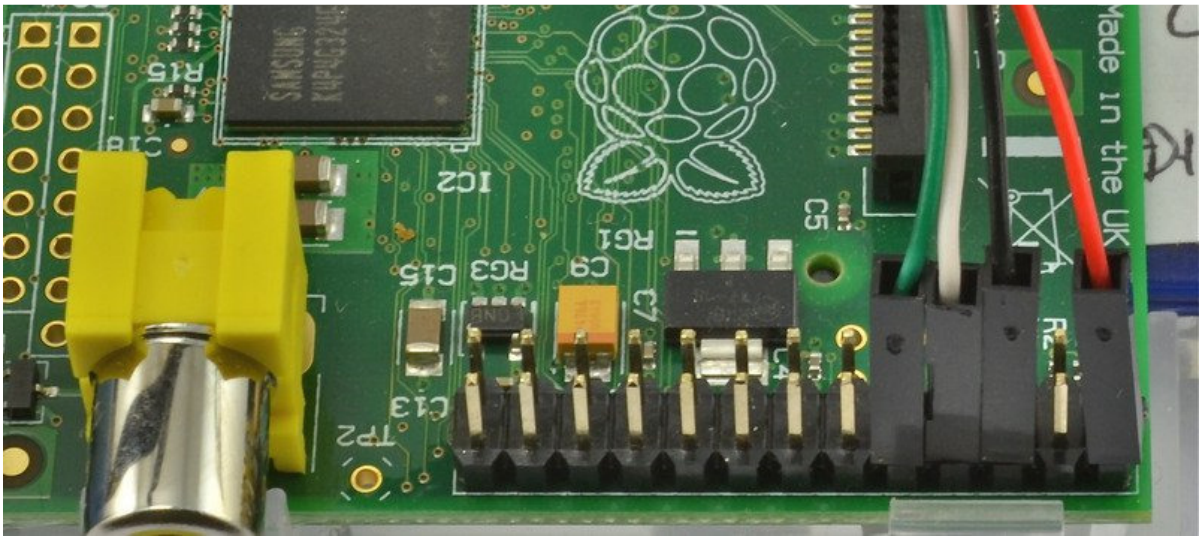
Θα χρειαστείτε μερικά πράγματα για να τρέξει αυτό το σεμινάριο:

- Raspberry Pi μοντέλο B + (ή B) - Ethernet απαιτείται
- καλώδιο Ethernet
- Προσαρμογέας WiFi HYPERLINK "http://www.adafruit.com/products/814" - Δεν λειτουργούν όλοι οι προσαρμογείς WiFi, ξέρουμε σίγουρα ότι λειτουργεί με αυτά στο κατάστημα Adafruit!
- SD Card (4GB ή μεγαλύτερη) με Raspbian σε αυτό. Μπορείτε είτε να αντιγράψετε το Raspbian εικόνα πάνω σ 'αυτό ή να αγοράσετε ένα έτοιμο Raspbian κάρτα
- Τροφοδοτικό για Pi σας
- καλώδιο Console USB (προαιρετικό) - αυτό το κάνει λίγο πιο εύκολο να εντοπίσετε το σύστημα
- Θήκη για Pi σας (προαιρετικό)
- Μια κάρτα SD ή MicroSD (προαιρετικό)



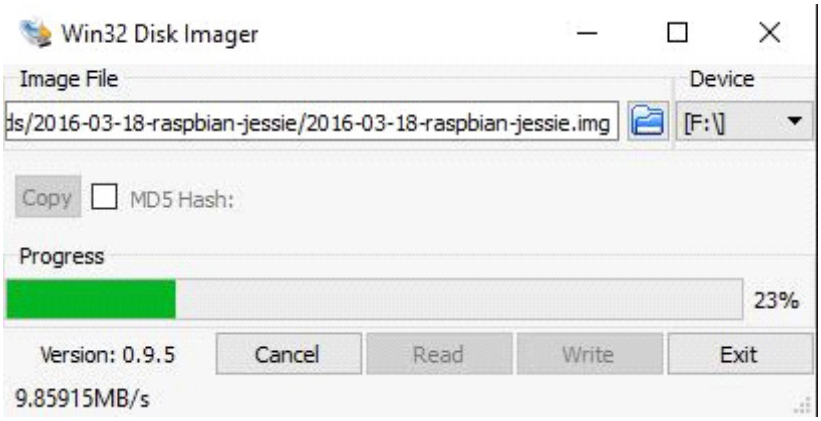
Εικόνα 28: TOR και Raspberry Pi

7.3. Παρασκευή

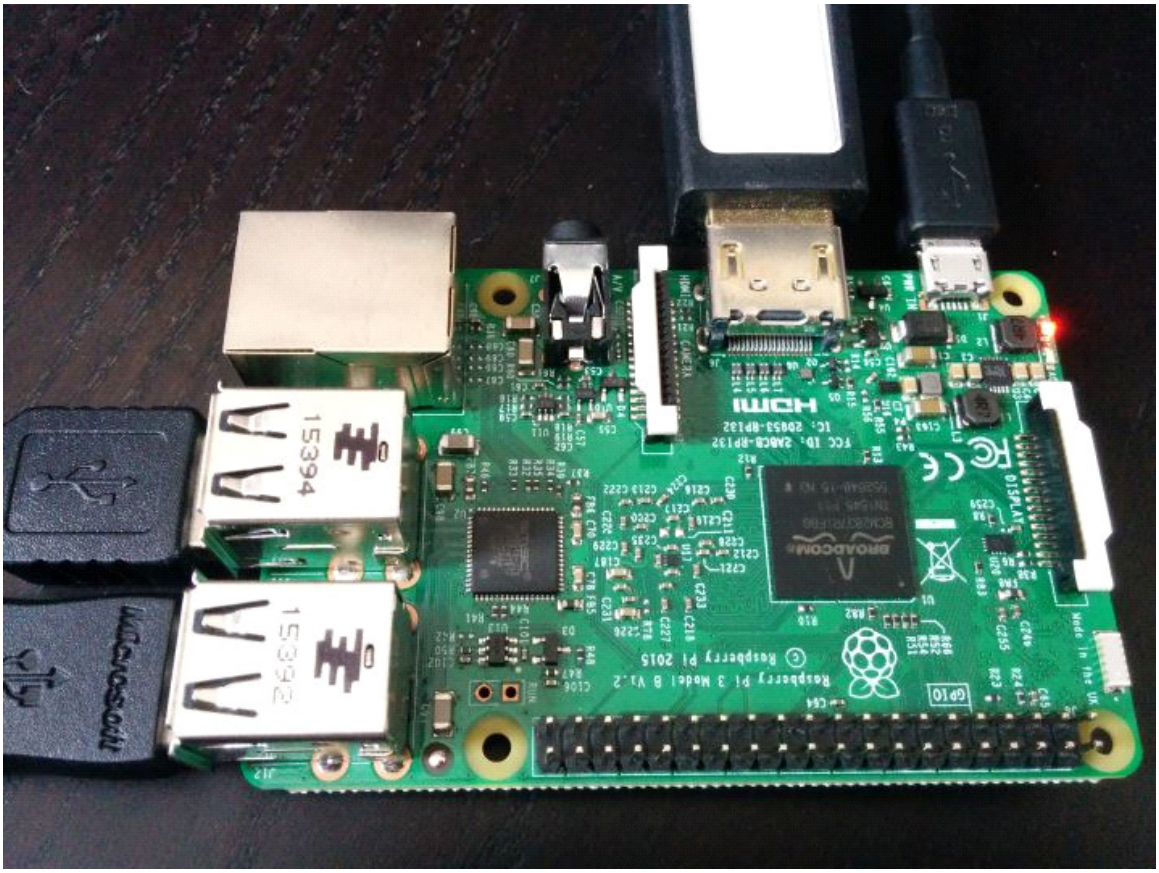


- <u>Εγκαταστήστε το λειτουργικό σύστημα στην κάρτα SD σας</u>
  Το πιο διάσημο λειτουργικό που χρησημοποιείται και αξιοποιεί πλήρως τις δυνατότητες του Rasbperry ειναι το Raspbian.

- Πάμε να εγκαταστήσουμε το "προτεινόμενο" λειτουργικό στην κάρτα μνήμης που θα βάλουμε στο Pi. Κατεβάζουμε το Raspbian .Αν κάνουμε extract σε έναν φάκελο το .zip του Raspbian, θα δούμε το .img αρχείο που πρέπει να "γράψουμε" στην κάρτα μνήμης. Τρέχουμε το Win32DiskImager και του δείχνουμε το Directory του .img, επιλέγουμε το Drive Letter του Card Reader μας και στην συνέχεια "Write".



- Συνδέουμε το HDMI, το πληκτρολόγιο, το ποντίκι, την κάρτα μνήμης και τέλος την τροφοδοσία στο Pi μας. Στην οθόνη μας θα bootάρει το Raspbian.



- Επιλέγουμε να συνδεθούμε στο WiFi μας (υπάρχει Panel πάνω δεξιά), και στην συνέχια ανοίγουμε το Terminal (Accessories, Terminal) για να αναβαθμίσουμε τα πακέτα/προγράμματα στην τελευταία έκδοση. Πληκτρολογούμε:

sudo apt-get update

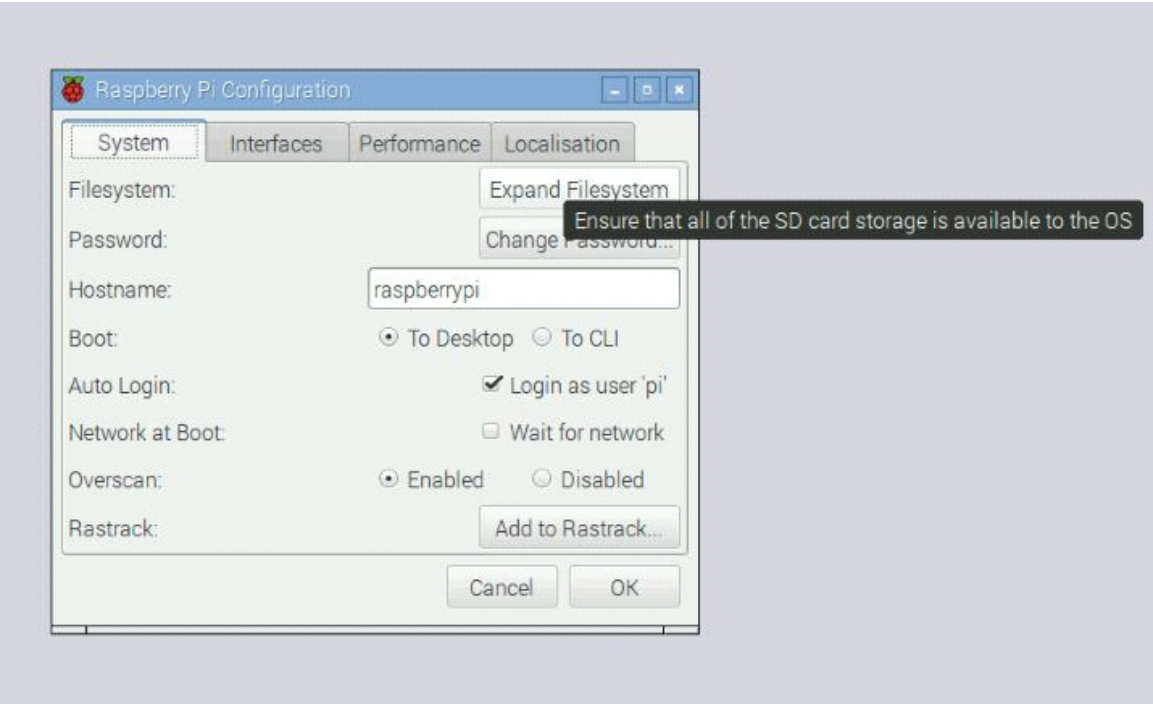
sudo apt-get upgrade

- Επιβεβαιώνουμε με **Y(Yes)** το Update.

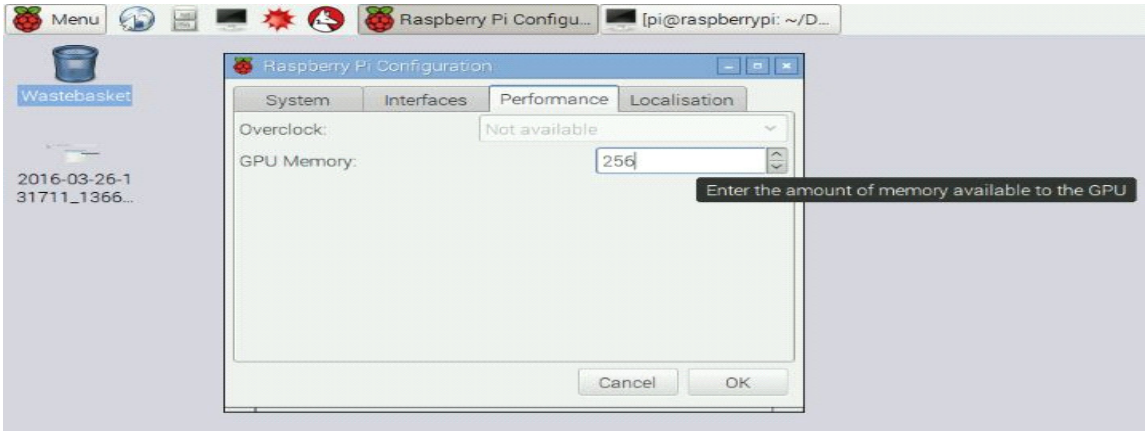
- Μόλις τελειώσει η διαδικασία αναβάθμισης, πάμε να κάνουμε κάποιες ακόμα "ρυθμίσεις" στην διανομή μας. Δίνοντας df -h στο Terminal, παρατηρούμε ότι η διανομή μας δεν "βλέπει" όλο τον διαθέσιμο χώρο της κάρτας μνήμης.

df -h

- Πηγαίνουμε Menu, Preferences, Raspberry Pi Configuration και στην συνέχεια επιλέγουμε το Expand Filesystem. Αν θέλουμε επίσης αλλάζουμε τον Default κωδικό από "Change Password".



- Μετά από την καρτέλα Performance επιλέγουμε ως GPU Memory 256MB. Θα μας ζητηθεί Reboot, το οποίο και δεχόμαστε.



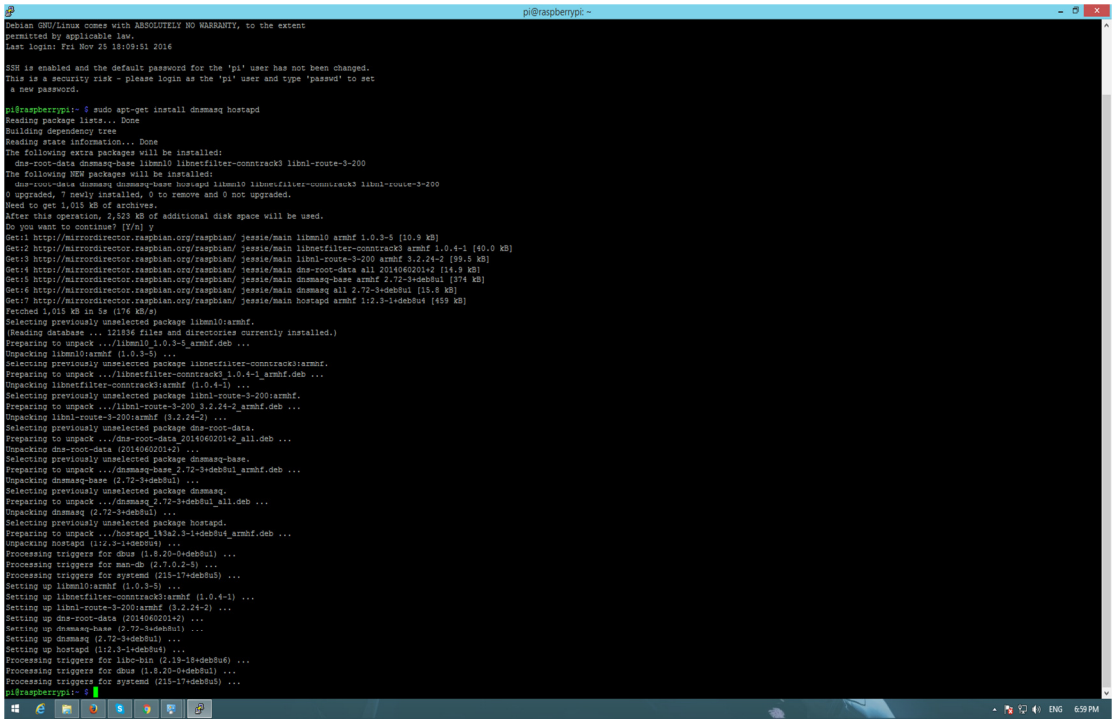
- Εναλλακτικά για τα παραπάνω θα μπορούσαμε να τρέξουμε από Terminal:

sudo raspi-config

- Το πρώτο βήμα του tutorial για να έχουμε δρομολόγηση μεσω του λογισμικού TOR είναι να μετατρέψουμε το Pi σε wifi access point.
- Αρχικά πρέπει να εγκαταστήσουμε τα απαιτούμενα πακέτα με την ακόλουθη εντολή:

sudo apt-get install dnsmasq hostapd

- **hostapd** : Αυτό το πακέτο μας επιτρέπει να χρησιμοποιήσουμε το wifi του raspberry σαν access point.
- **dnsmasq**: Πακέτο το οποίο λειτουργεί σαν DHCP και DNS server ταυτόχρονα.



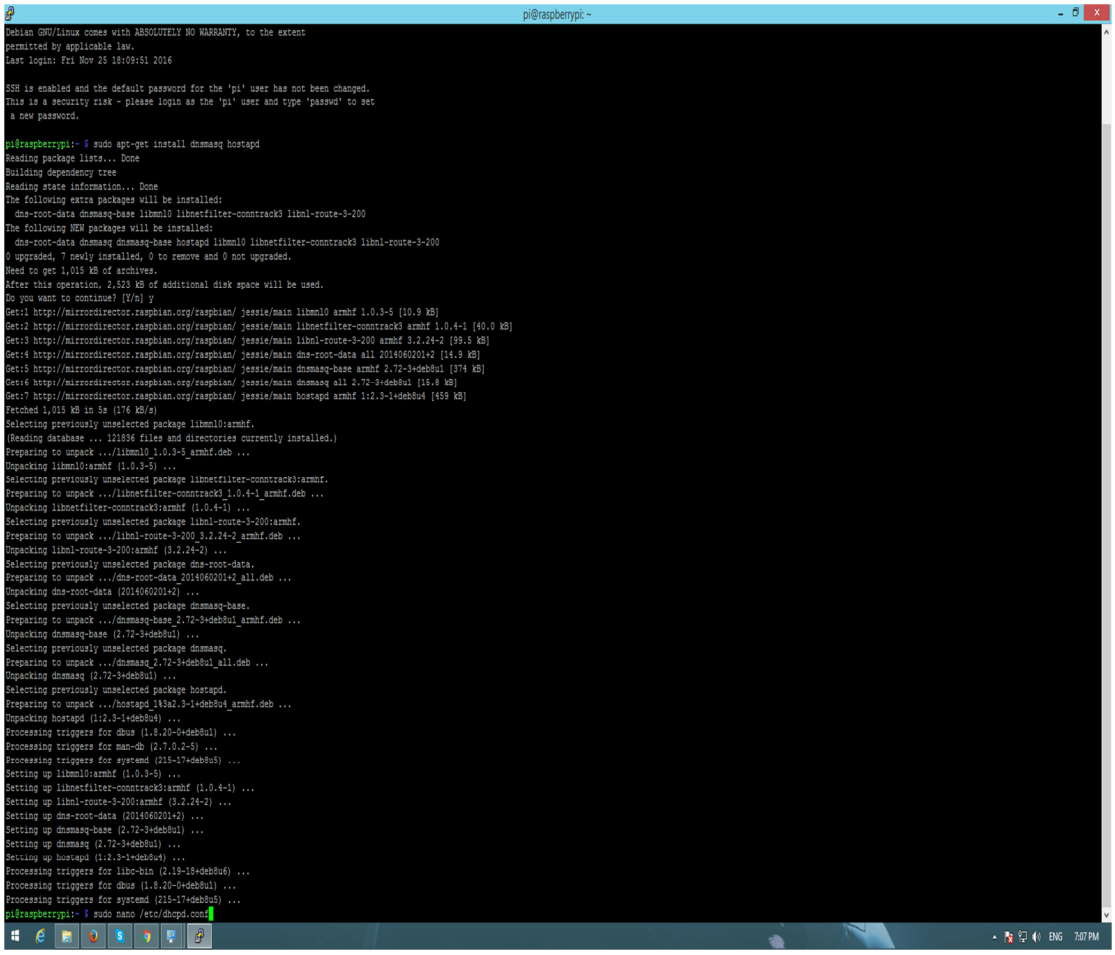
- Αφού γίνει η εγκατάσταση, κάνουμε configure τα intrefaces του wlan0 με μία στατική ip *(καλό θα ήταν να επισημανθεί ότι πρέπει να είμαστε συνδεδεμένοι μέσω καλωδίου Ethernet και όχι μέσω του wifi του raspberry.)*

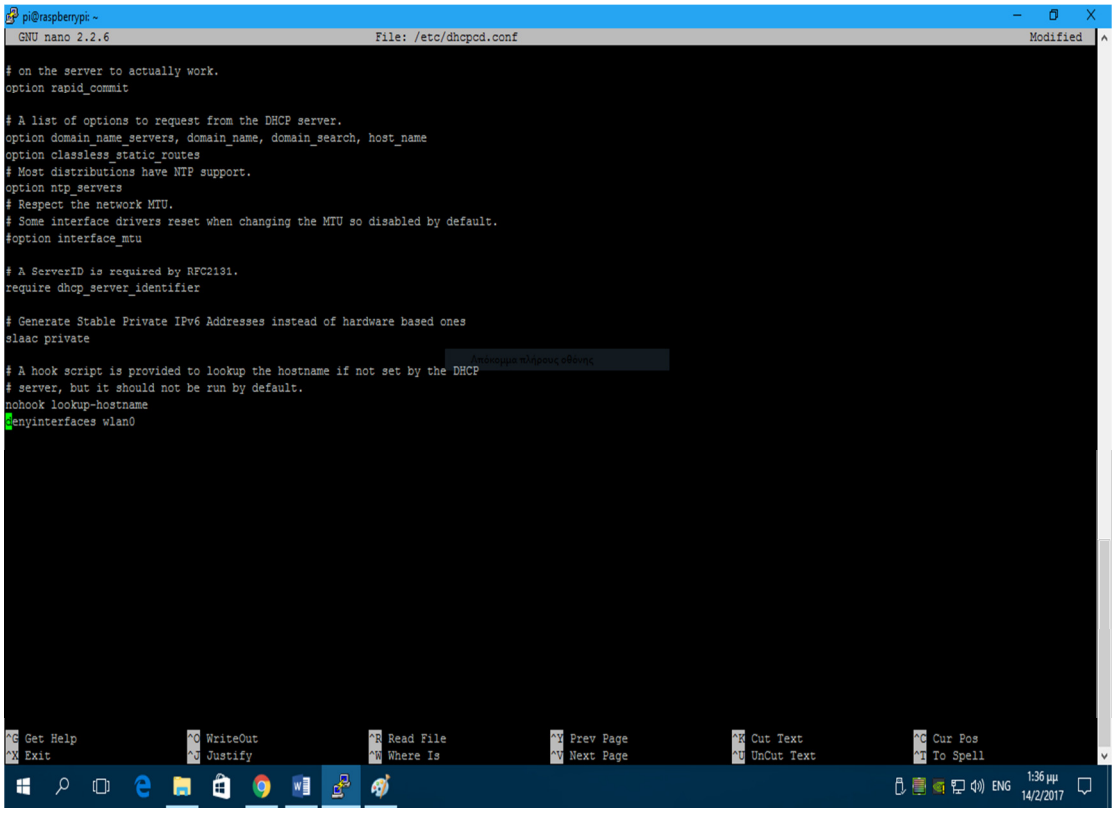
- Ανοίγουμε το αρχείο τροποποίησης του dhcpcd με την εντολή:

```
sudo nano /etc/dhcpcd.conf
```

- Και στο κάτω μέρος του αρχείου προσθέτουμε την γραμμή:

```
denyinterfaces wlan0
```


pi@raspberrypi: ~
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Nov 25 18:09:51 2016
SSH is enabled and the default password for the 'pi' user has not been changed.
This is a security risk - please login as the 'pi' user and type 'passwd' to set
a new password.
pi@raspberrypi:~ $ sudo apt-get install dnsmasq hostapd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
dns-root-data dnsmasq-base libmnl0 libnetfilter-conntrack3 libnl-route-3-200
The following NEW packages will be installed:
dns-root-data dnsmasq dnsmasq-base hostapd libmnl0 libnetfilter-conntrack3 libnl-route-3-200
0 upgraded, 7 newly installed, 0 to remove and 0 not upgraded.
Need to get 1,015 kB of archives.
After this operation, 2,523 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://mirrordirector.raspbian.org/raspbian/ jessie/main libmnl0 armhf 1.0.3-5 [10.9 kB]
Get:2 http://mirrordirector.raspbian.org/raspbian/ jessie/main libnetfilter-conntrack3 armhf 1.0.4-1 [40.0 kB]
Get:3 http://mirrordirector.raspbian.org/raspbian/ jessie/main libnl-route-3-200 armhf 3.2.24-2 [99.5 kB]
Get:4 http://mirrordirector.raspbian.org/raspbian/ jessie/main dns-root-data all 2014060201+2 [14.9 kB]
Get:5 http://mirrordirector.raspbian.org/raspbian/ jessie/main dnsmasq-base armhf 2.72-3+deb8u1 [374 kB]
Get:6 http://mirrordirector.raspbian.org/raspbian/ jessie/main dnsmasq all 2.72-3+deb8u1 [15.8 kB]
Get:7 http://mirrordirector.raspbian.org/raspbian/ jessie/main hostapd armhf 1:2.3-1+deb8u4 [459 kB]
Fetched 1,015 kB in 5s (176 kB/s)
Selecting previously unselected package libmnl0:armhf.
(Reading database ... 121836 files and directories currently installed.)
Preparing to unpack .../libmnl0_1.0.3-5_armhf.deb ...
Unpacking libmnl0:armhf (1.0.3-5) ...
Selecting previously unselected package libnetfilter-conntrack3:armhf.
Preparing to unpack .../libnetfilter-conntrack3_1.0.4-1_armhf.deb ...
Unpacking libnetfilter-conntrack3:armhf (1.0.4-1) ...
Selecting previously unselected package libnl-route-3-200:armhf.
Preparing to unpack .../libnl-route-3-200_3.2.24-2_armhf.deb ...
Unpacking libnl-route-3-200:armhf (3.2.24-2) ...
Selecting previously unselected package dns-root-data.
Preparing to unpack .../dns-root-data_2014060201+2_all.deb ...
Unpacking dns-root-data (2014060201+2) ...
Selecting previously unselected package dnsmasq-base.
Preparing to unpack .../dnsmasq-base_2.72-3+deb8u1_armhf.deb ...
Unpacking dnsmasq-base (2.72-3+deb8u1) ...
Selecting previously unselected package dnsmasq.
Preparing to unpack .../dnsmasq_2.72-3+deb8u1_all.deb ...
Unpacking dnsmasq (2.72-3+deb8u1) ...
Selecting previously unselected package hostapd.
Preparing to unpack .../hostapd_1%3a2.3-1+deb8u4_armhf.deb ...
Unpacking hostapd (1:2.3-1+deb8u4) ...
Processing triggers for dbus (1.8.20-0+deb8u1) ...
Processing triggers for man-db (2.7.0.2-5) ...
Processing triggers for systemd (215-17+deb8u5) ...
Setting up libmnl0:armhf (1.0.3-5) ...
Setting up libnetfilter-conntrack3:armhf (1.0.4-1) ...
Setting up libnl-route-3-200:armhf (3.2.24-2) ...
Setting up dns-root-data (2014060201+2) ...
Setting up dnsmasq-base (2.72-3+deb8u1) ...
Setting up dnsmasq (2.72-3+deb8u1) ...
Setting up hostapd (1:2.3-1+deb8u4) ...
Processing triggers for libc-bin (2.19-18+deb8u6) ...
Processing triggers for dbus (1.8.20-0+deb8u1) ...
Processing triggers for systemd (215-17+deb8u5) ...
pi@raspberrypi:~ $ sudo nano /etc/dhcpd.conf
ENG 7:07 PM

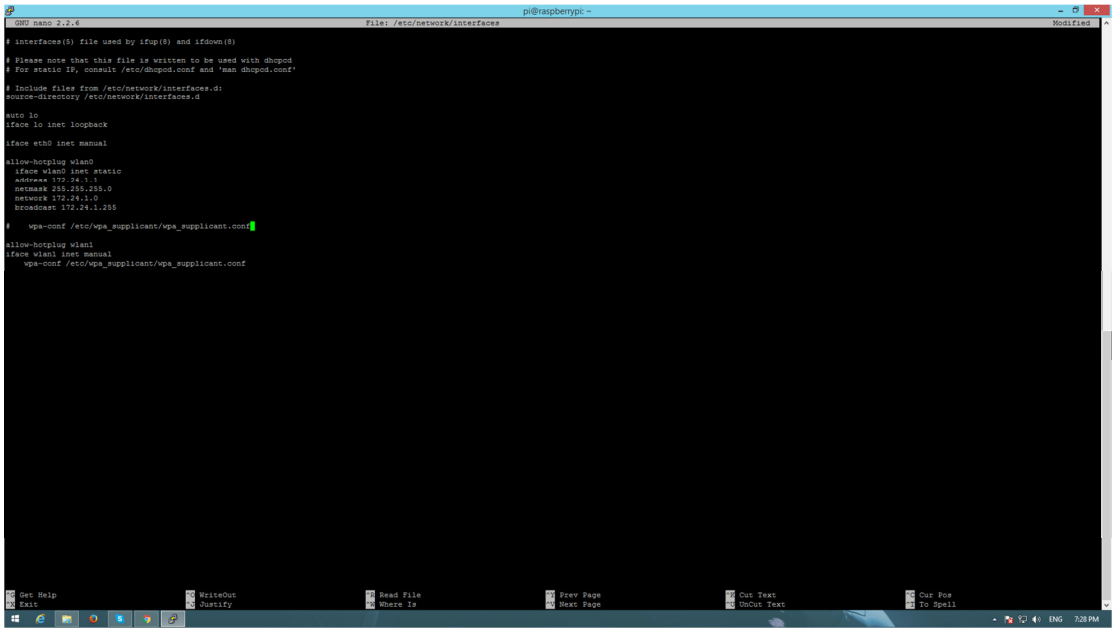

pi@raspberrypi: ~
GNU nano 2.2.6 File: /etc/dhcpd.conf Modified
on the server to actually work.
option rapid_commit
A list of options to request from the DHCP server.
option domain_name_servers, domain_name, domain_search, host_name
option classless_static_routes
Most distributions have NTP support.
option ntp_servers
Respect the network MTU.
Some interface drivers reset when changing the MTU so disabled by default.
#option interface_mtu
A ServerID is required by RFC2131.
require dhcp_server_identifier
Generate Stable Private IPv6 Addresses instead of hardware based ones
slaac private
A hook script is provided to lookup the hostname if not set by the DHCP
server, but it should not be run by default.
nohook lookup-hostname
denyinterfaces wlan0
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
ENG 1:36 μμ 14/2/2017

- Τώρα πρέπει να διαμορφώσουμε την στατική ip μας. Ανοίγουμε το αρχείο διαμόρφωσης του interface με την εντολή :

  sudo nano /etc/network/interfaces

- Και τροποποιούμε τον τομέα του wlan0 ώστε να μοιάζει όπως το παρακάτω:

```
allow-hotplug wlan0

iface wlan0 inet static

    address 172.24.1.1

    netmask 255.255.255.0

    network 172.24.1.0

    broadcast 172.24.1.255

#    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
```



- Έπειτα κάνουμε επανεκκίνηση του πακέτου dhcpd με την εντολή:

  sudo service dhcpcd restart

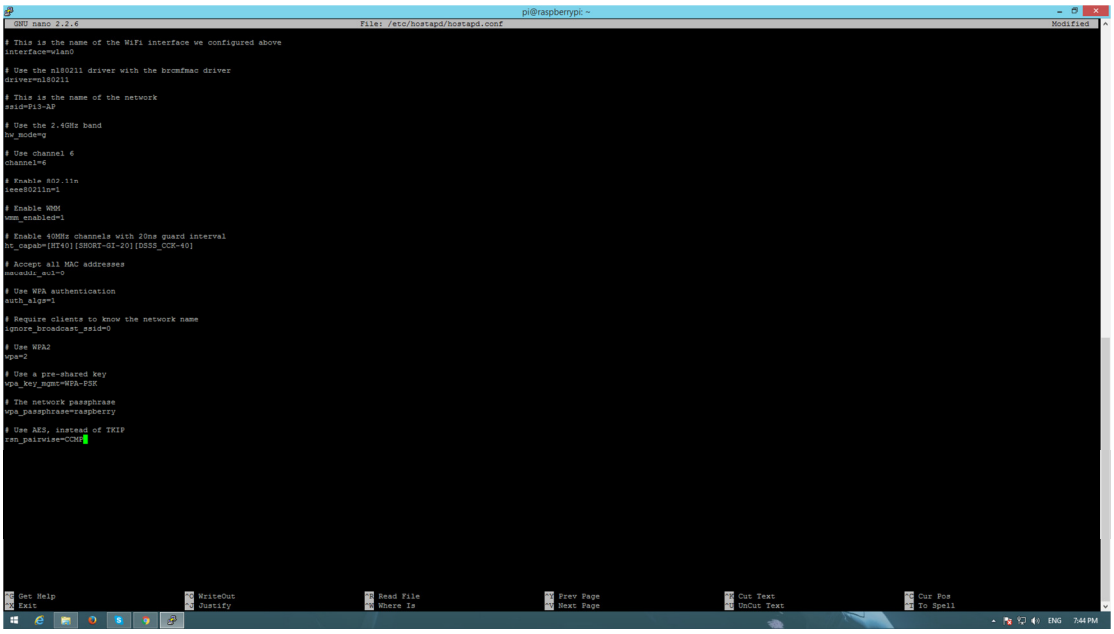
- Και ξανά φορτώνουμε το configuration για το wlan0 με την εντολη:

sudo ifdown wlan0; sudo ifup wlan0.

- Επόμενο βήμα είναι να τροποποιήσουμε το πακέτο hostapd. Δημιουργούμε ένα καινούργιο αρχείο configuration δίνοντας την εντολή :

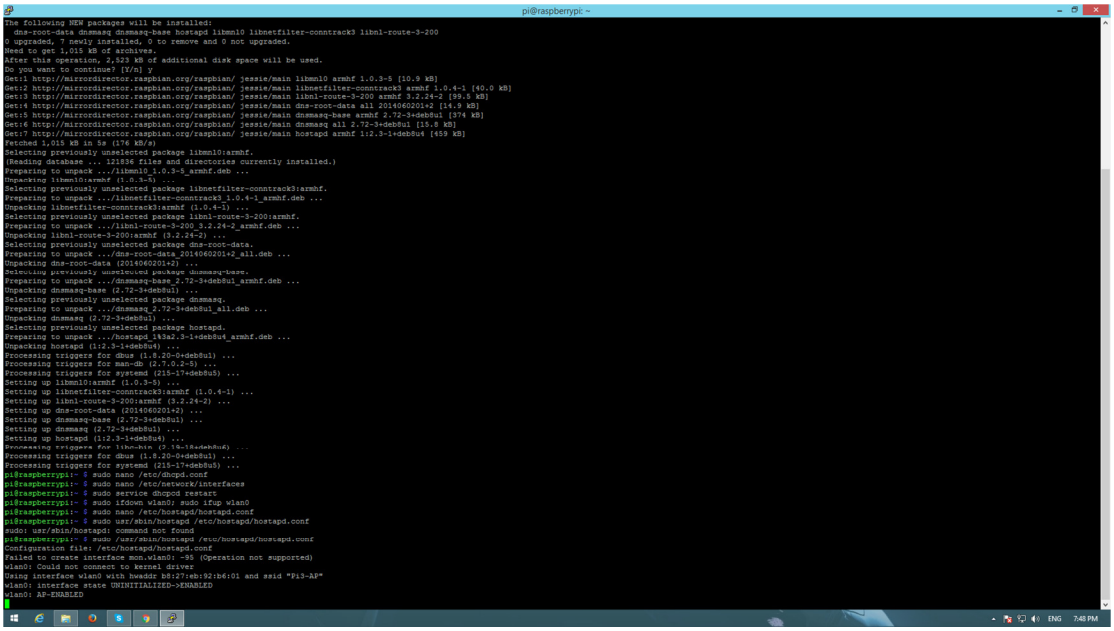
sudo nano /etc/hostapd/hostapd.conf

- Με τα ακόλουθα περιεχόμενα:



- Μπορούμε να ελέγξουμε εάν λειτουργεί μέχρι αυτό το σημείο τρέχοντας την εντολή:

sudo /usr/sbin/hostapd /etc/hostapd/hostapd.conf



- Αν όλα έχουν γίνει σωστά θα δούμε το δίκτυο Pi3-Ap να είναι ορατό στα διαθέσιμα δίκτυα.

- Ακόμα όμως δεν θα μπορούμε να πάρουμε ip μέχρι να κάνουμε setup το dnsmasq. *(πατάμε ctrl+c για να το σταματήσουμε).*
- Τώρα πρέπει να πούμε στο hostapd που να ψάξει για το αρχείο config κατά την εκκίνηση.

- Για να το καταφέρουμε αυτό δίνουμε την εντολή :

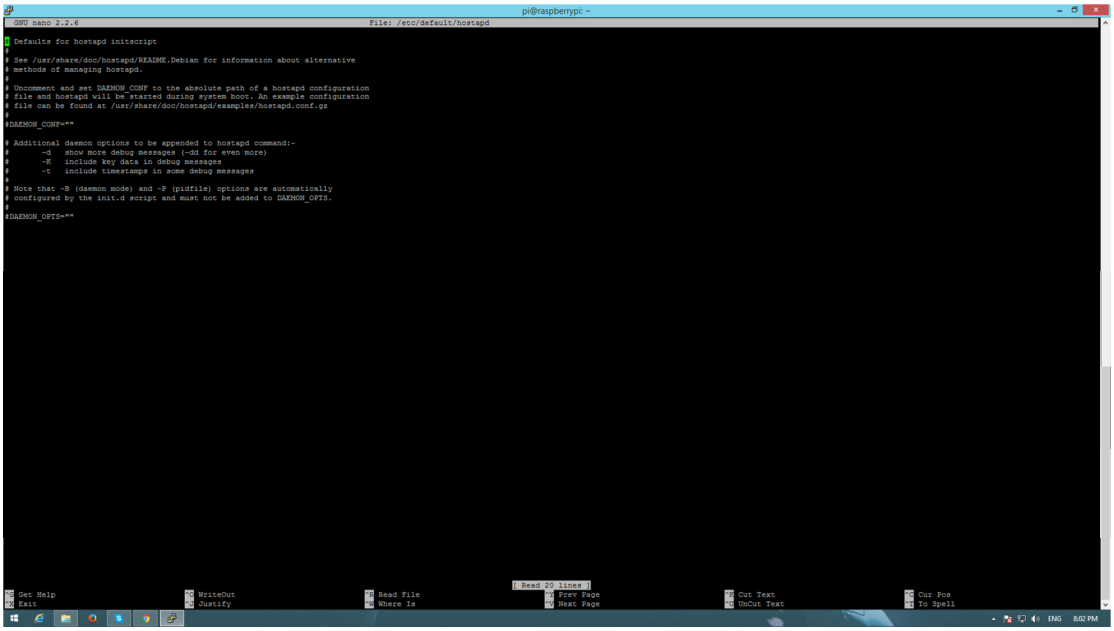
sudo nano /etc/default/hostapd

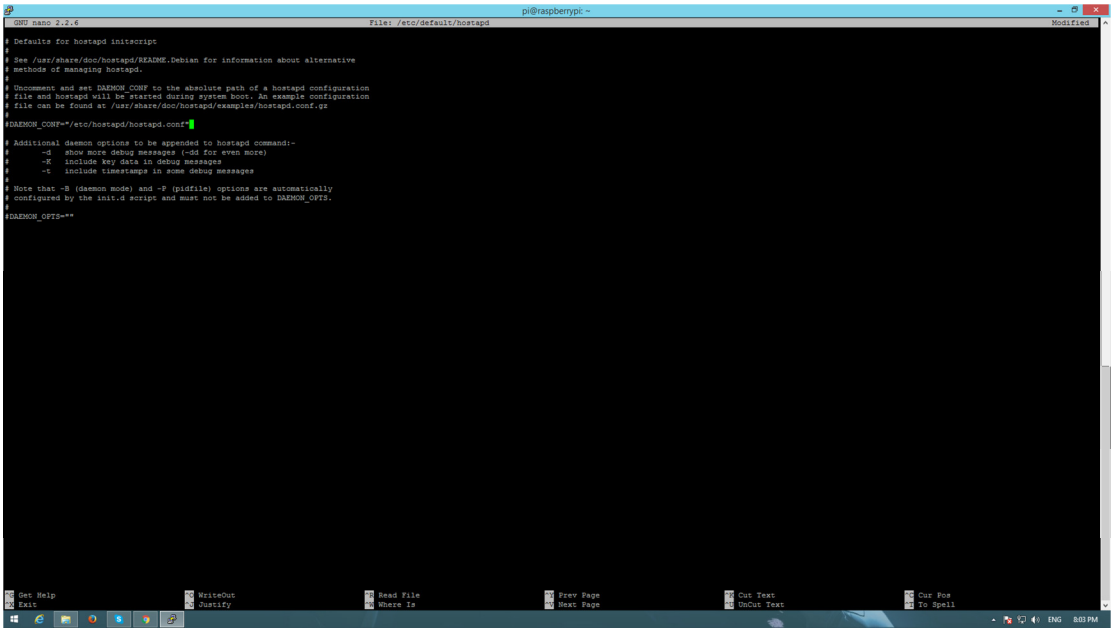
- Για να ανοίξουμε το αρχικό αρχείο διαμόρφωσης και βρίσκουμε την γραμμή:

#DAEMON_CONF=""

- Και την αντικαθηστούμε με αυτή:

DAEMON_CONF="/etc/hostapd/hostapd.conf".



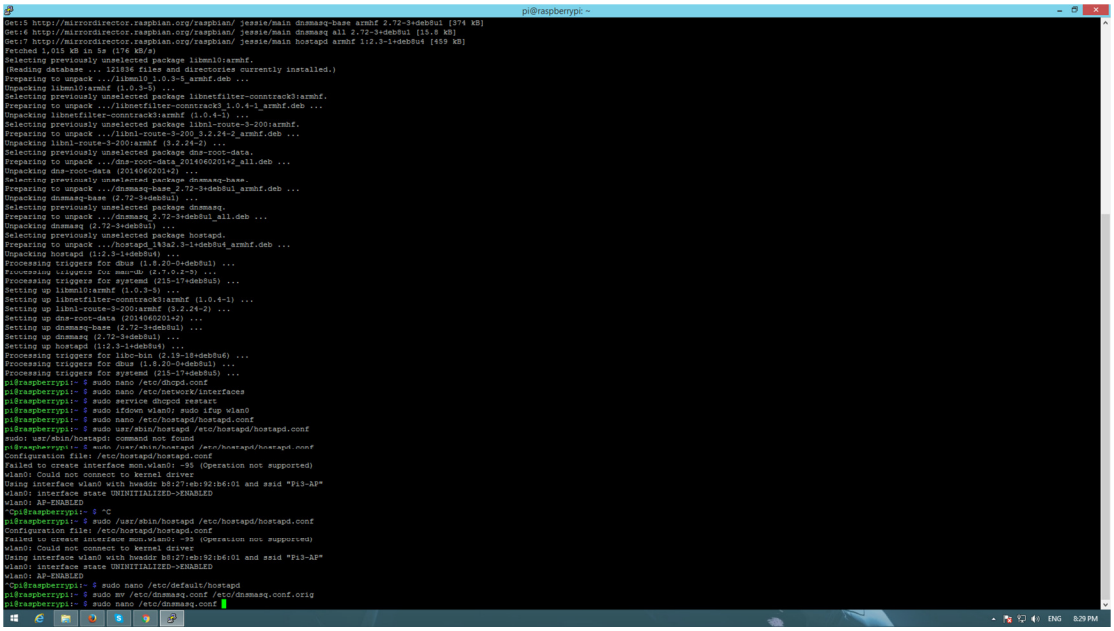


- Στην συνέχεια θα διαμορφώσουμε το πακέτο dnsmasq. Ο φάκελος διαμόρφωσης του πακέτου αυτού έχει πάρα πολλές πληροφορίες σχετικά με την χρήση του αλλά η πλειοψηφία τους είναι περιττές για τον σκοπό μας, οπότε θα τον μετακινήσουμε με την εντολή:

```
sudo mv /etc/dnsmasq.conf /etc/dnsmasq.conf.orig
```

- Και θα δημιουργήσουμε έναν καινούργιο:

```
sudo nano /etc/dnsmasq.conf
```



- Μέσα στον καινούργιο φάκελο γράφουμε τα εξής:

interface=wlan0 # Use interface wlan0

listen-address=172.24.1.1 # Explicitly specify the address to listen on

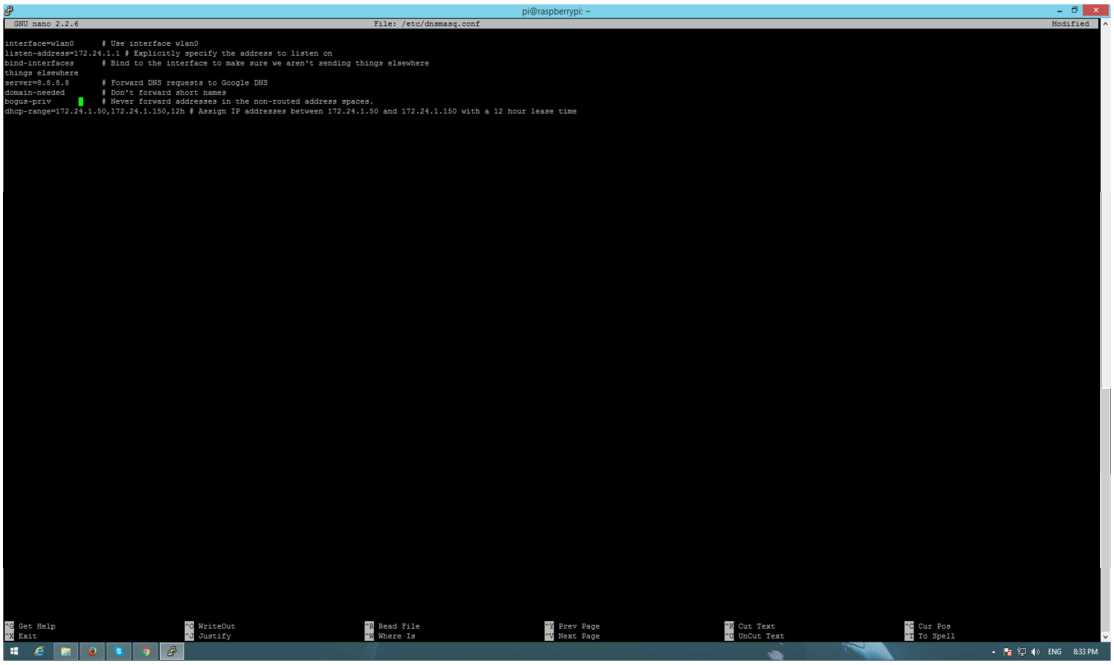
bind-interfaces # Bind to the interface to make sure we aren't sending things elsewhere

server=8.8.8.8 # Forward DNS requests to Google DNS

domain-needed # Don't forward short names

bogus-priv # Never forward addresses in the non-routed address spaces.

dhcp-range=172.24.1.50,172.24.1.150,12h # Assign IP addresses between 172.24.1.50 and 172.24.1.150 with a 12 hour lease time



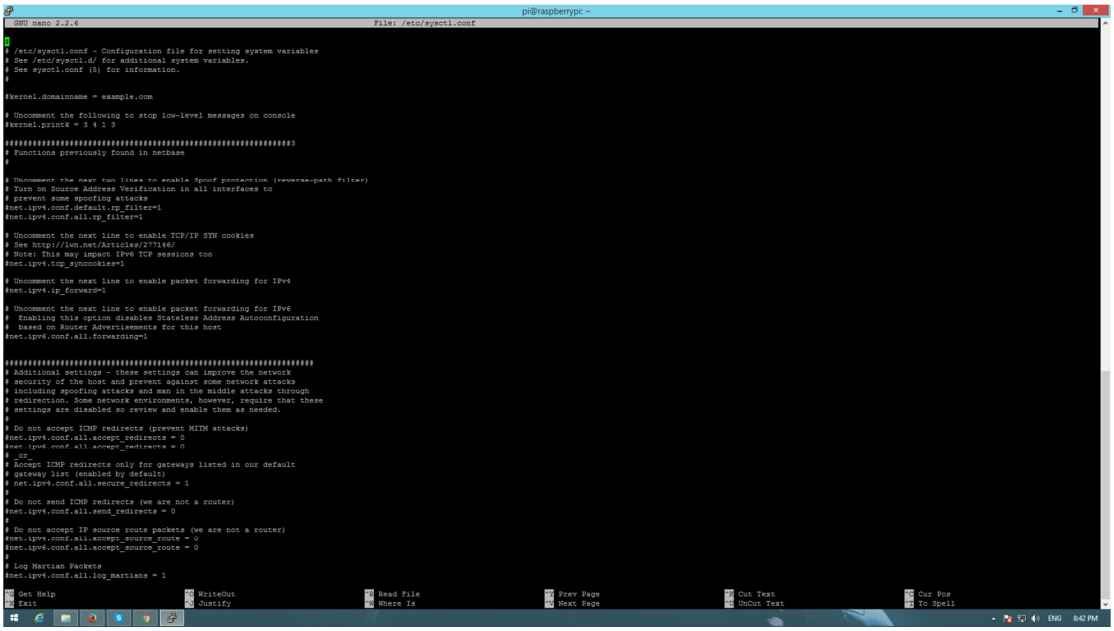
- Ένα από τα τελευταία βήματα είναι να ενεργοποιήσουμε το packet forwarding.

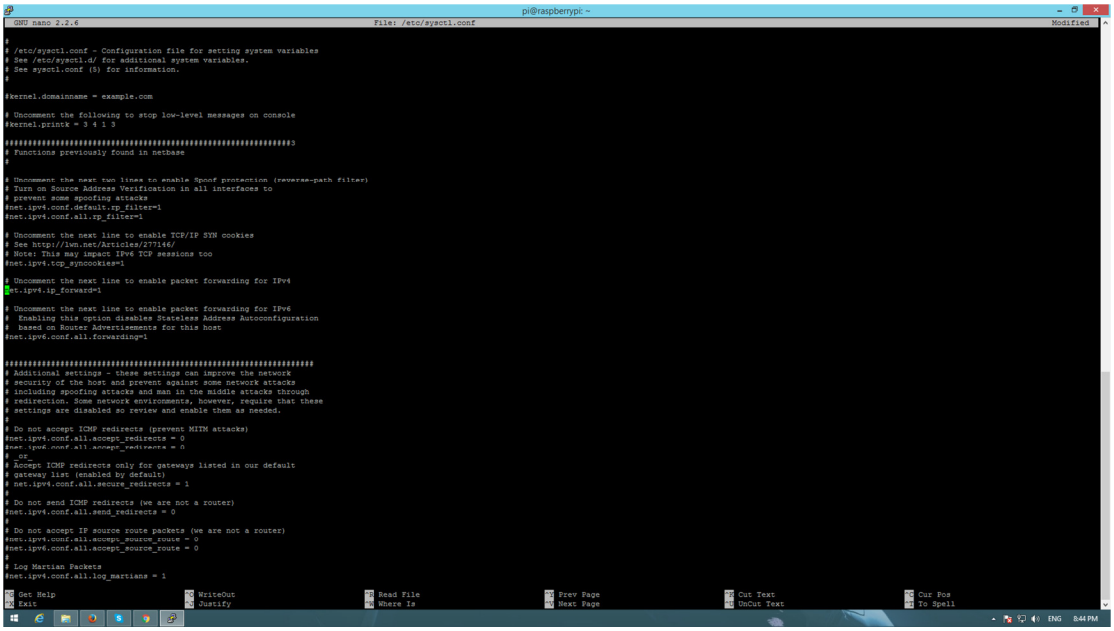
- Ανοίγουμε το αρχείο **sysctl.conf** με την εντολή:

sudo nano /etc/sysctl.conf

- Και αφαιρούμε το σύμβολο # από την γραμμή :

net.ipv4.ip_forward=1.





- Αυτή η διαδικασία θα το ενεργοποιήσει στο επόμενο reboot αλλά μπορούμε να το ενεργοποιήσουμε και αμέσως δίνοντας την εντολή :

sudo sh -c "echo 1 > /proc/sys/net/ipv4/ip_forward"

- Επιπλέον πρέπει να μοιράσουμε την σύνδεση του pi στις συσκευές που είναι συνδεδεμένες στο wifi με το να διαμορφώσουμε ένα NAT μεταξύ των interface wlan0 και eth0. Για να το καταφέρουμε αυτό γράφουμε τις ακόλουθες εντολές:

sudo iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

sudo iptables -A FORWARD -i eth0 -o wlan0 -m state --state RELATED,ESTABLISHED -j ACCEPT

sudo iptables -A FORWARD -i wlan0 -o eth0 -j ACCEPT

- Αυτές οι εντολές πρέπει να αποθηκευτούν ώστε να εφαρμόζονται κάθε φορά που θα κάνουμε reboot το pi, δίνοντας την εντολή :

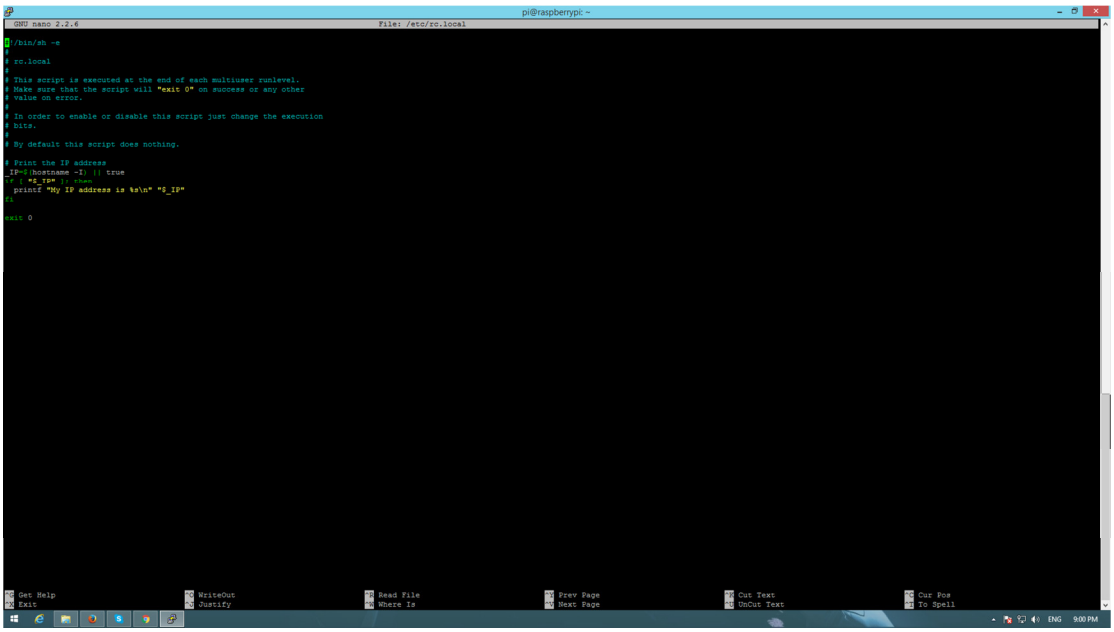
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"

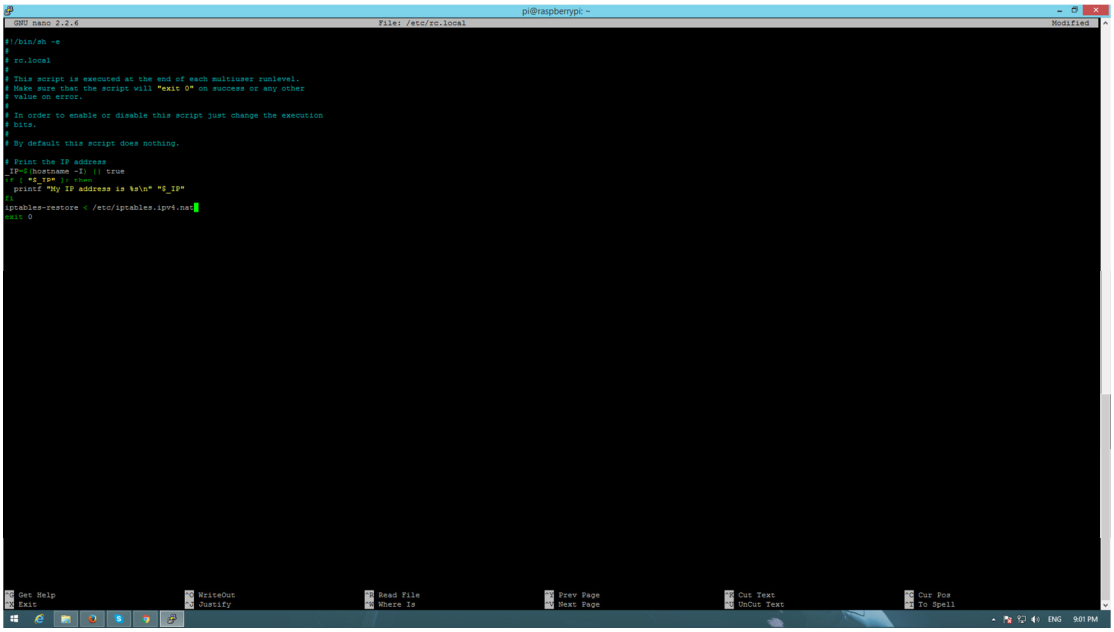
- Τώρα πρέπει να ανοίξουμε το αρχείο **rc.local** με την εντολή:

sudo nano /etc/rc.local

- Και πάνω από την γραμμή exit0 προσθέτουμε την γραμμή:

```
iptables-restore < /etc/iptables.ipv4.nat
```





- Τελευταίο βήμα είναι να ξεκινήσουμε τις υπηρεσίες μας:

```
sudo service hostapd start

sudo service dnsmasq start
```

- Πλέον μπορούμε να συνδεθούμε στο internet μέσω του wifi του pi μας.

- Για να ελέγξουμε ότι όλα έχουν διαμορφωθεί σωστά κάνουμε μια επανεκκίνηση με την εντολή:

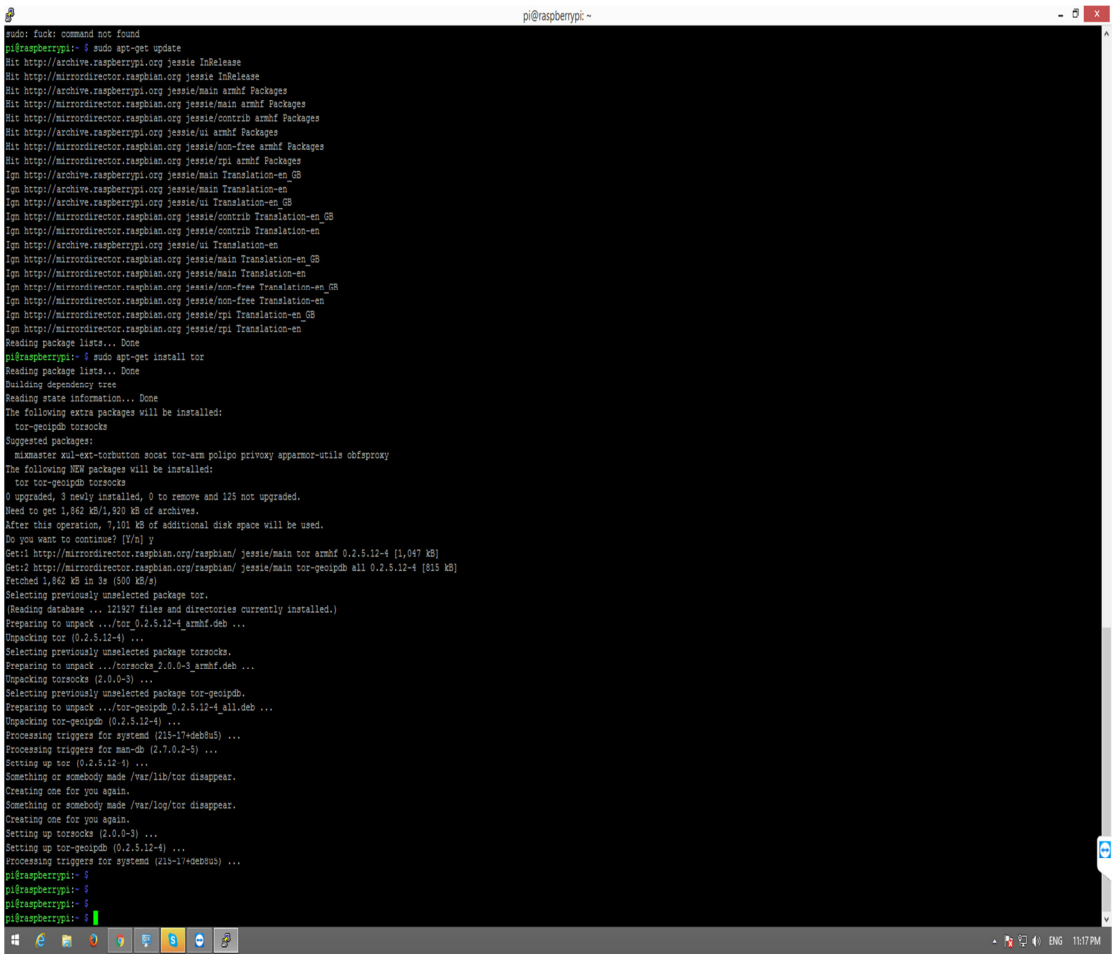
sudo reboot.

- Ήρθε η ώρα να εγκαταστήσουμε το λογισμικό TOR.

- Γράφουμε στο terminal τις ακόλουθες εντολές:

Sudo apt-get update

sudo apt-get install tor

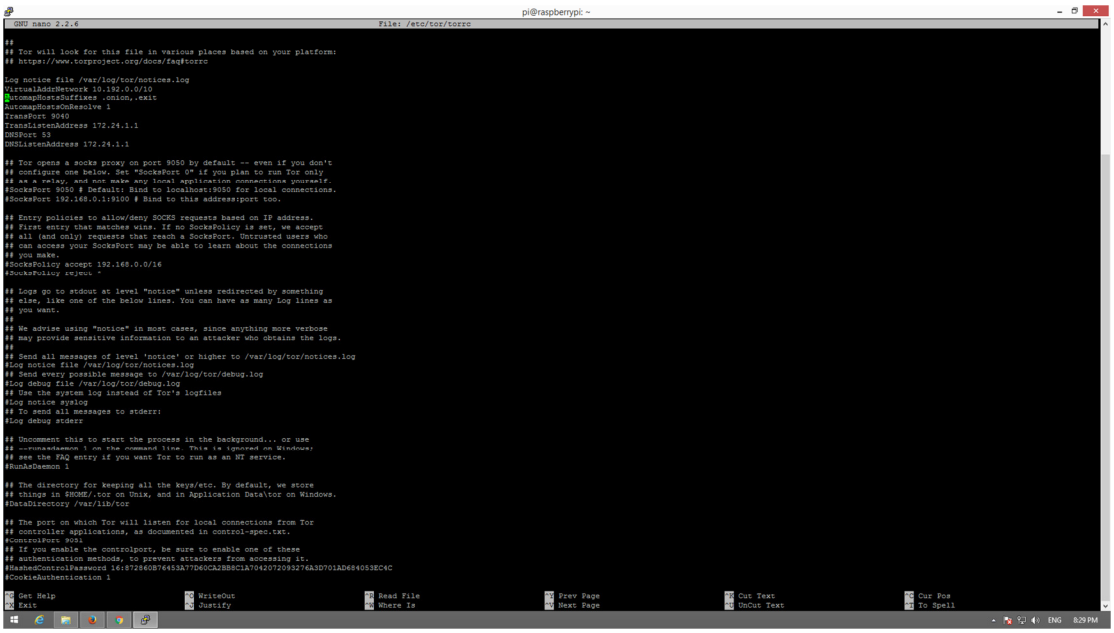


- Διαμορφώνουμε το αρχείο config του TOR δίνοτας την εντολή:

sudo nano /etc/tor/torrc

- Και γράφουμε το παρακάτω κείμενο στο πάνω μέρος του αρχείου:

1. Log notice file /var/log/tor/notices.log
2. VirtualAddrNetwork 10.192.0.0/10
3. AutomapHostsSuffixes .onion,.exit
4. AutomapHostsOnResolve 1
5. TransPort 9040
6. TransListenAddress 172.24.1.1
7. DNSPort 53
8. DNSListenAddress 172.24.1.1



- Τώρα θα αλλάξουμε τις ρυθμίσεις ώστε τα πακέτα να περνάνε μέσω του λογισμικού TOR.

- Γράγουμε τις ακόλουθες εντολές για να σβήσουμε τις παλιές ρυθμίσεις από το **ip NAT table**:

sudo iptables -F
sudo iptables -t nat -F

- Αν θέλουμε να συνεχίσουμε την εφαρμογή ssh του pi μετά από αυτή τη διαδικασία πρέπει να προσθέσουμε μια εξαίρεση για την θύρα 22:

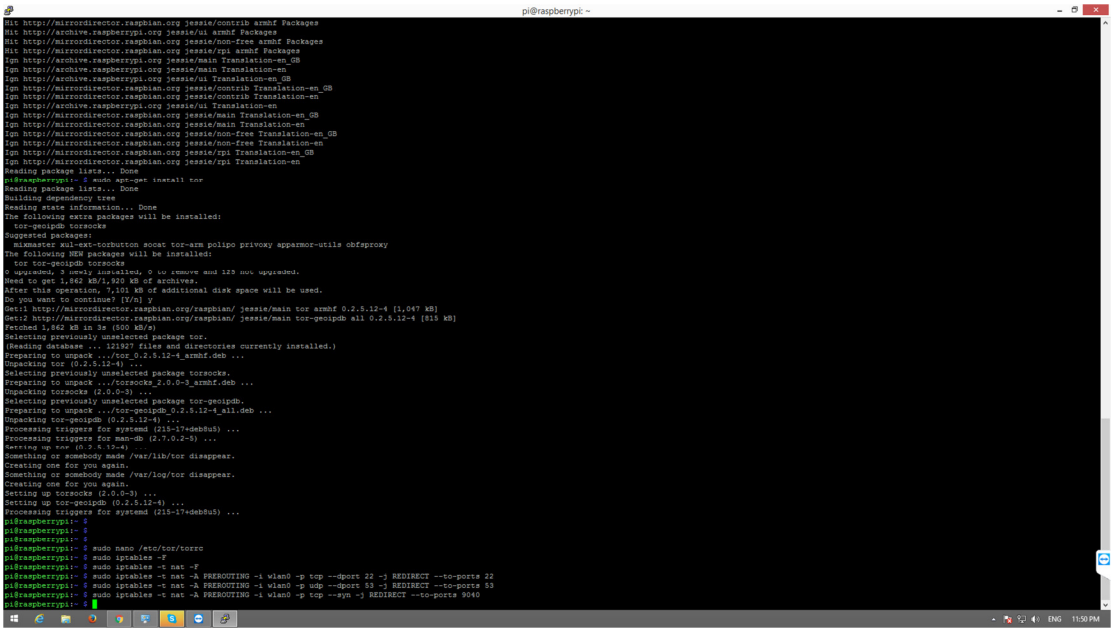
sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 22 -j REDIRECT --to-ports 22

- Έπειτα τρέχουμε την ακόλουθη εντολή για να δρομολογήσουμε όλα τα DNS πακέτα από το interface wlan0 στην θύρα 53 του wlan0*(DNSPort στο torrc):*

sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53

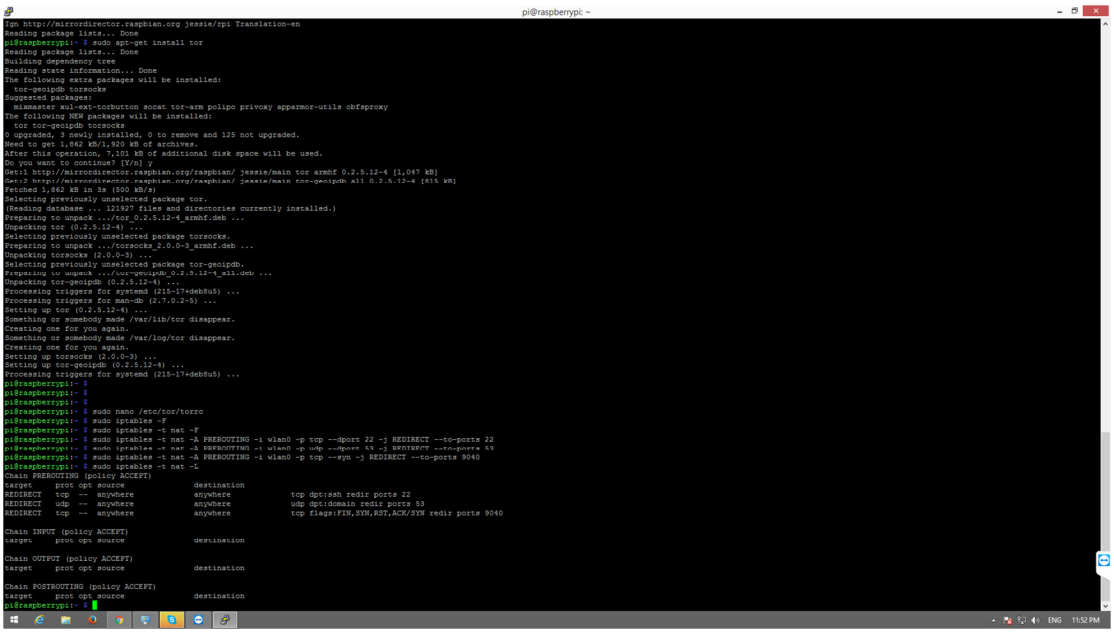
- Επιπλέον πρέπει να δρομολογήσουμε όλη την κίνηση TCP από το interface wlan0 στην θύρα 9040 *(TransPort in our torrc):*

sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --syn -j REDIRECT --to-ports 9040



- Τώρα μπορούμε να ελέγξουμε εάν η πίνακες ip είναι σωστοί με την εντολή:

sudo iptables -t nat -L



- Αν δεν υπάρχει κάποιο σφάλμα τα αποθηκεύουμε στο παλιό NAT αρχείο αποθήκευσης:

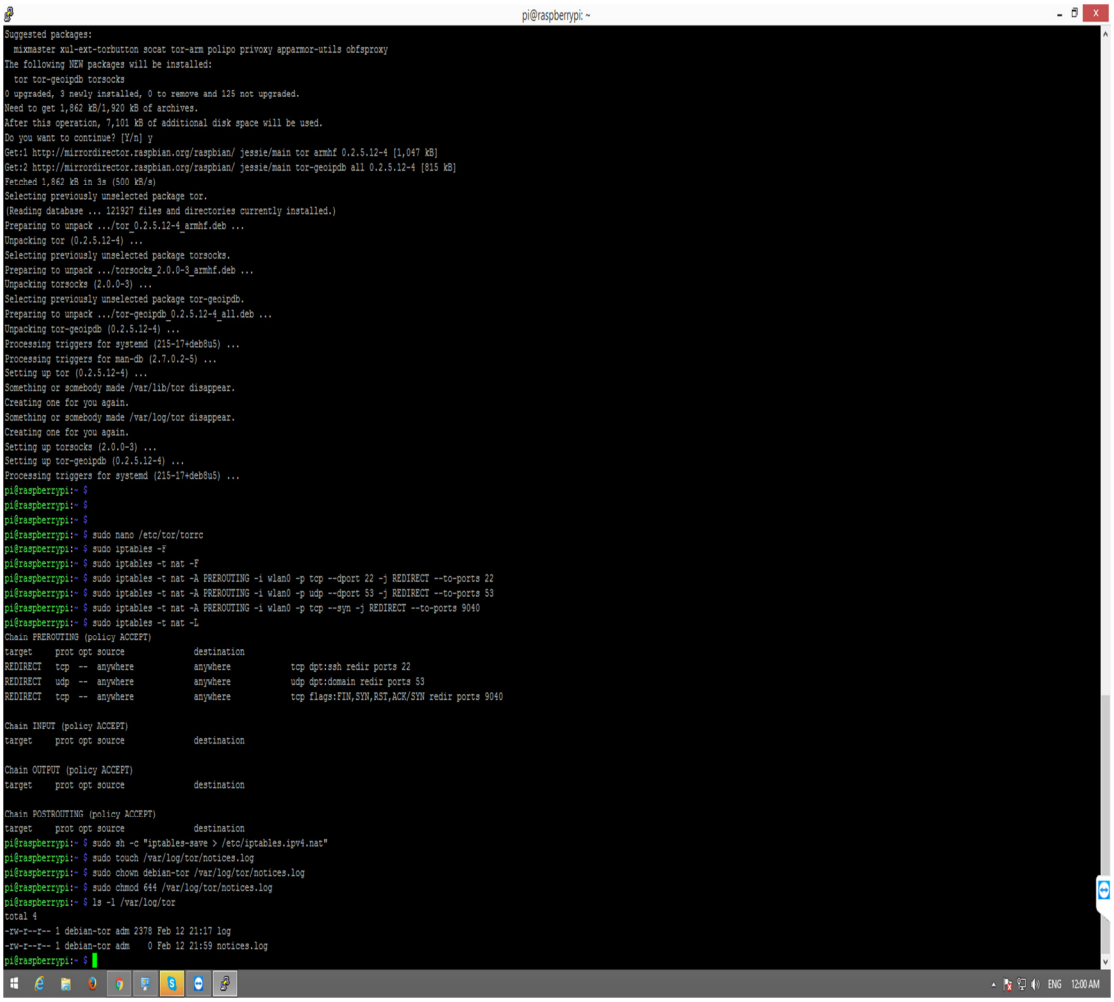
sudo sh -c "iptables-save > /etc/iptables.ipv4.nat"

- Στην συνέχεια δημιουργούμε ένα αρχείο log το οποίο είναι πολύ χρήσιμο για απασφαλμάτωση :

sudo touch /var/log/tor/notices.log
sudo chown debian-tor /var/log/tor/notices.log
sudo chmod 644 /var/log/tor/notices.log

- Και το ελέγχουμε με την εντολή:

ls -l /var/log/tor



- Πλέον είμαστε σε θέση να ξεκινήσουμε το λογισμικό TOR.

sudo service tor start

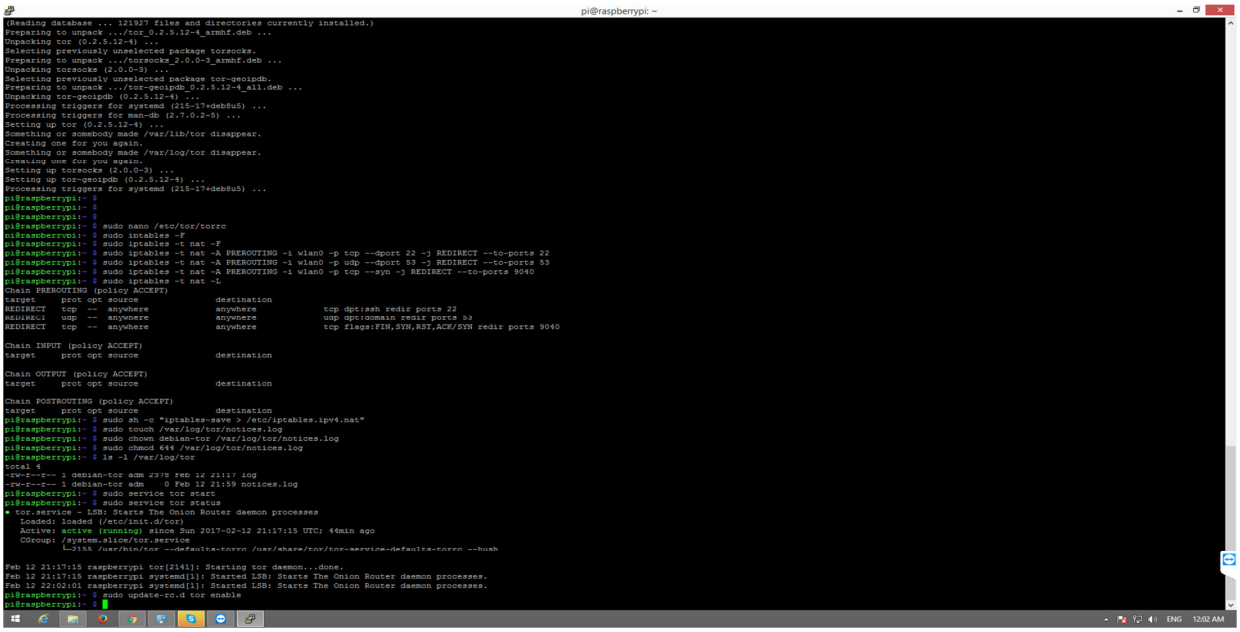
- Μπορούμε ακόμα να ελέγξουμε ότι τρέχει κανονικά με την εντολή:

sudo service tor status

*Αν κάτι δεν πάει καλά θα εμφανιστεί μια ειδοποίηση fail.

- Τέλος για να μπορέσει να ξεκινήσει το TOR κατά την εκκίνηση γράφουμε:

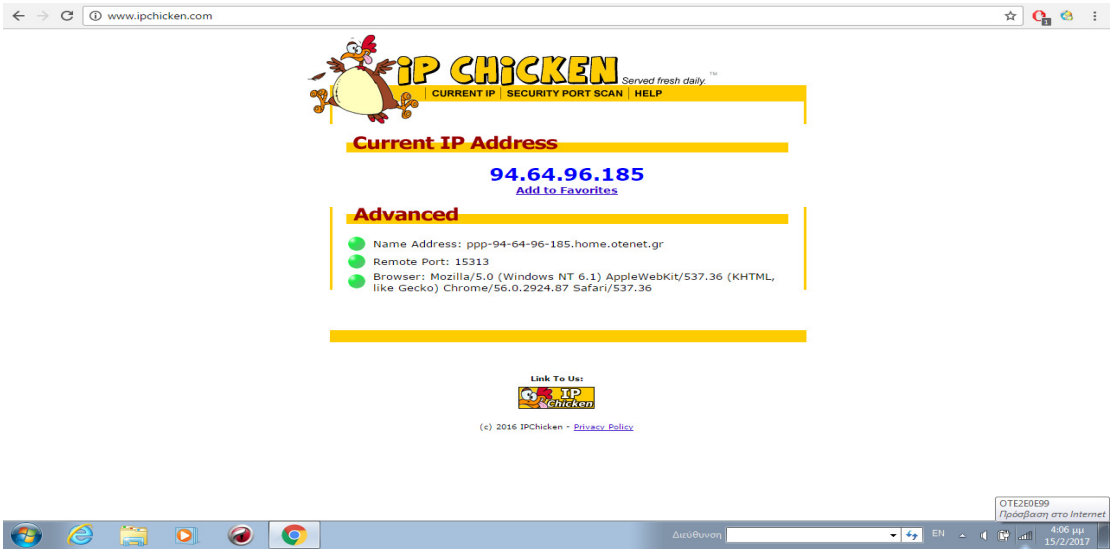
sudo update-rc.d tor enable



- Τώρα πλέον μπορούμε να περιπλανιόμαστε ανώνυμα στο διαδίκτυο μέσω του λογισμικό TOR από το Raspberry Pi3.

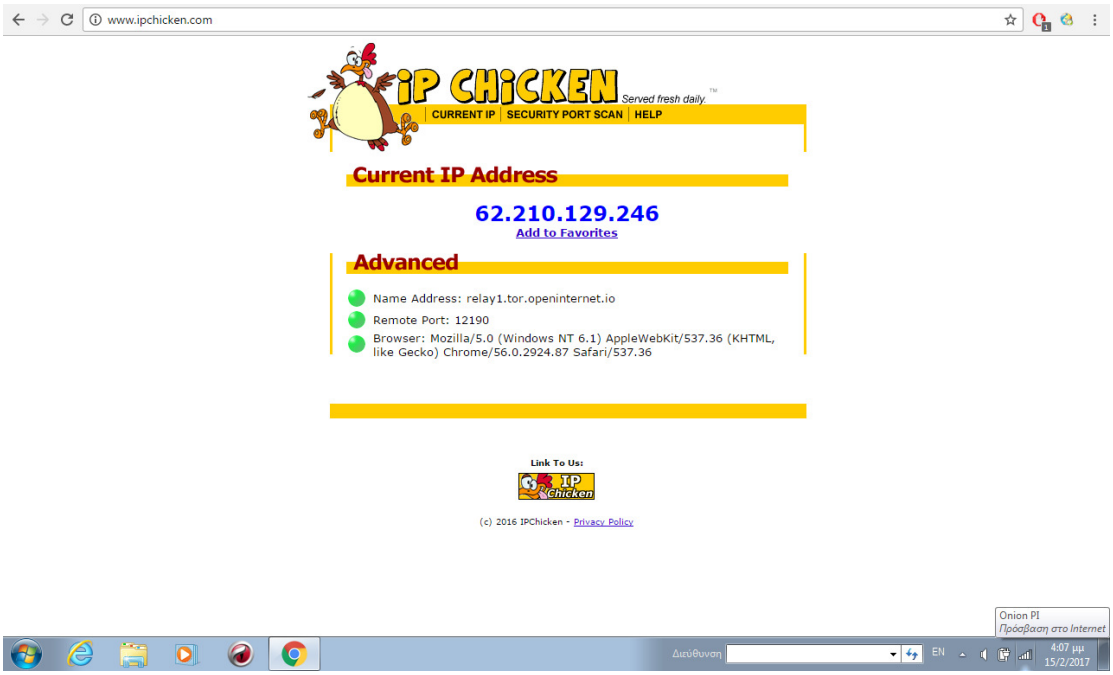
- Συνδεόμαστε από τη συσκευή μας στο δίκτυο του Pi χρησιμοποιώντας τον κωδικό που είχαμε καταχωρήσει στο hostapd configuration file.

- Αφού αποκτήσουμε πρόσβαση μπαίνουμε σε μία ιστοσελίδα η οποία μας δείχνει την Ip μας **(πχ ipchicken.com)** για να βεβαιωθούμε ότι όλα λειτουργούν κανονικά.

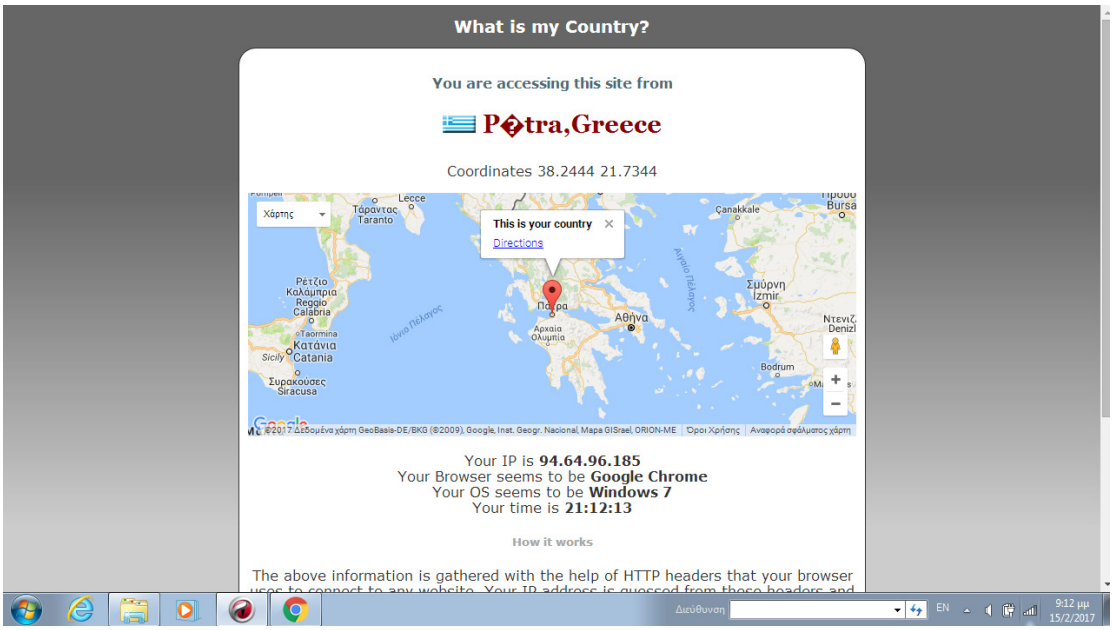


- Στην παραπάνω εικόνα βλέπουμε πως είμαστε συνδεδεμένοι στο κανονικό μας router.

- Αν όμως συνδεθούμε μέσω του Pi και του λογισμικού Tor παρατηρούμε πως η ip μας έχει αλλάξει.



- Εκτός όμως απο την Ip το λογισμικό Tor μας παρέχει την δυνατότητα να φαινόμαστε συνδεδεμένοι απο διαφορετική τοποθεσία από αυτή που είμαστε στην πραγματικότητα.



- Η παραπάνω εικόνα δίχνει την πραγματική τοποθεσία μας ενώ είμαστε συνδεδεμένοι στο αρχικό μας δίκτυο

- Και η εικόνα αυτή είναι η "εικονική" τοποθεσία μας ενώ είμαστε συνδεδεμένοι μέσω του Tor.

8. ΚΕΦΑΛΑΙΟ 8 : WIKILEAKS TOR (Επιπρόσθετες Λεπτομέρειες)

Η ακόλουθη μέθοδος απαιτεί κάποια τεχνική ικανότητα.

Το Tor, ή The Onion Router έχει αναπτυχθεί μετά από το πολεμικό ναυτικό και από το αμερικανικό πανεπιστήμιο MIT και από την Καλιφόρνια του Ιδρύματος Electronic Frontier και ενσωματώθηκε στη συνέχεια Wikileaks .

Χρησιμοποιώντας την ανώνυμη δέσμη πρόσβασης μπορείτε να αποτρέψετε κατασκόπους στο διαδίκτυο γνωρίζοντας ότι ο υπολογιστής σας έχει συνδεθεί με το Wikileaks .Οι περισσότεροι Wikileakers δεν χρειάζονται αυτή την επιπλέον ασφάλεια, και υπάρχουν απλούστερες και πιθανώς ασφαλέστερες εναλλακτικές επιλογές για διαρροές υψηλού κινδύνου. Αλλά για εκείνους που βρίσκονται σε κίνδυνο και θέλουν να αποκτήσουν πρόσβαση στο Wikileaks από την άνεση του «σπιτιού τους» είναι μια εξαιρετική λύση.Όταν έχετε εγκαταστήσει το Tor μπορείτε να συνδεθείτε με το Wikileaks μέσω ανώνυμης διεύθυνσης.

Σημείωση:

Για να αποστείλετε ένα έγγραφο ανώνυμα χρησιμοποιώντας Tor χρησιμοποιούμε τον παρακάτω σύνδεσμο:

http: //suw74isz7wqzpmgu.onion/

(αυτός ο σύνδεσμος θα λειτουργήσει μόνο όταν έχετε εγκαταστήσει και ρυθμίσει το Tor).

Χωρίς Tor, όταν έχετε πρόσβαση σε μια ιστοσελίδα Wikileaks με τον συνηθισμένο τρόπο, π.χ. μέσω https://wikileaks.org/ όλα τα δεδομένα σας είναι κρυπτογραφημένα.Το Wikileaks Tor χρησιμοποιεί πλήρως κρυπτογραφημένα end-to-end.

*Το κόστος αυτής της ανωνυμίας είναι η ταχύτητα, που ανοίγει μια σελίδα (κατά μέσο όρο 15 δευτερόλεπτα), αλλά μερικές φορές φτάνουν και τα 60.

9. <u>ΚΕΦΑΛΑΙΟ 9: ΣΤΑΤΙΣΤΙΚΑ ΧΡΗΣΕΩΝ ΤΟΥ TOR.</u>

Ο αριθμός των ανθρώπων που χρησιμοποιούν το πρόγραμμα περιήγησης Tor για τη διατήρηση της ιδιωτικότητας και της ανωνυμίας τους έχει ξεπεράσει το ένα εκατομμύριο αυτό το μήνα, σύμφωνα με το Facebook. Ακόμα και που πρόκειται απλά για μια σταγόνα στον ωκεανό, οι αριθμοί των χρηστών του Facebook, είναι μια ισχυρή απόδειξη ότι οι άνθρωποι θέλουν προστασία της ιδιωτικής τους ζωής.Το Facebook ανακοίνωσε ότι ο αριθμός των ανθρώπων που χρησιμοποιούν το πρόγραμμα περιήγησης Tor για να αποκτήσουν πρόσβαση στο μεγαλύτερο social media site στον κόσμο, το Facebook, έχει ξεπεράσει το ένα εκατομμύριο αυτό το μήνα, τον Απρίλιο, για πρώτη φορά στην ιστορία.

Το Tor, γνωστό και ως «Onion Router», είναι διάσημο για την παροχή ανωνυμίας σε όλο τον κόσμο στο διαδίκτυο, ενώ σερφάρουν σε μια ιστοσελίδα. Αυτή η τεχνολογία του δικτύου έχει σχεδιαστεί για να ενισχύσει την προστασία της ιδιωτικής ζωής του web χρήστη με την κρυπτογράφηση και τη δρομολόγηση τυχαίων συνδέσεων Internet μέσω ενός παγκόσμιου δικτύου από volunteer relays. Γίνεται δυσκολότερο για μεμονωμένες συνδέσεις web για να οδηγήσουν πίσω σε έναν συγκεκριμένο χρήστη.

Νωρίτερα, υπήρξε ένα μικρό τεχνικού είδους πρόβλημα με τη σύνδεση στο Facebook μέσω της Tor access browser. Εξαιτίας αυτού, το Facebook δημιούργησε μια αποκλειστική (dedicated) onion διεύθυνση για το Tor τον Οκτώβριο του 2014. Η δημιουργία της dedicated Onion διεύθυνσης αποσκοπούσε στο να κάνει ευκολότερο για τους χρήστες να συνδεθούν μέσω του Tor. Αυτή η διεύθυνση βοήθησε και στην επισήμανση της κυκλοφορίας των δικτυακών διαδρομών από το site με τις υποδομές ασφαλείας.

Σε ορισμένους χρήστες αρέσει να χρησιμοποιούν το Tor για διαφορετικούς λόγους ασφαλείας και προστασίας της ιδιωτικής ζωής και η ταυτοποίηση της φυσικής θέσης είναι ένας από τους σημαντικότερους λόγους για τη χρήση του Tor. Το σύστημα δρομολόγησης Tor μέσω ενός δικτύου relays καλύπτει τη φυσική τοποθεσία του χρήστη και επιπλέον κρύβει τα δεδομένα τοποθεσίας από το Facebook.

Από την άλλη πλευρά, το Tor επιβεβαίωσε τον αριθμό αυτό. Ωστόσο, για να διατηρηθεί η προστασία της ιδιωτικής ζωής, ακολουθεί μια συμβουλή από το Tor:

«Όταν χρησιμοποιείτε την ιστοσελίδα του Facebook μέσω Tor, ο Tor Browser είναι υπεύθυνος για αυτά τα δεδομένα, έτσι ώστε να είναι ανώνυμα. Βέβαια, κάποιος μπορεί να δημοσιεύσει μια ενημέρωση της κατάστασής του λέγοντας ότι είναι σε κάποιο εστιατόριο, για παράδειγμα, και αυτό θα έπαυε αυτόματα την ανωνυμία.»

Παρακάτω σας παρουσιάζουμε μια εικόνα που δείχνει τα στατιστικά χρήσεων του TOR:

Έρευνα που έγινε τον Φεβ 2016	
Κατηγορία	Τοις εκατό
Βία	0.3
Όπλα	0.8
Κανονικός	1.2
hacking	1.8
παράνομη πορνογραφία	2.3
Πλέγμα	2.3
Εξτρεμισμός	2.7
Αγνωστος	3.0
άλλων παράνομων	3.8
Χρηματοδότηση	6.3
Ναρκωτικά	8.1
Αλλα	19.6
Κανένας	47,7

Έρευνα που έγινε τον Ιανουάριο 2015.	
Κατηγορία	**Επί τις εκατό**
Χαρταπάγνιο	0.4
Guns	1.4
Κουβέντα	2.2
Νέα	2.2
Καταχρηση	2.2
Βιβλία	2.5
Τηλεφωνικός καταλογος	2.5
blog	2,75
Πορνογραφία	2,75
Φιλοξενία	3.5
hacking	4,25
Ερευνα	4,25
Ανωνυμία	4.5
Δικαστήριο	4,75
Πλαστός	5.2
πληροφοριοδότη	5.2
Wiki	5.2
Ταχυδρομείο	5.7
Bitcoin	6.2
Απάτη	9
Αγορά	9
Ναρκωτικά	15.4

10. ΚΕΦΑΛΑΙΟ 10 : Εντοπισμός του ηλεκτρονικού εγκλήματος με χρήση του TOR και ο ρόλος της ΕΛ.ΑΣ.

Η αντιμετώπιση του ηλεκτρονικού εγκλήματος αποτελεί ζήτημα ύψιστης σημασίας για τις αστυνομικές αρχές, όπως άλλωστε και τα κοινά διαπραχθέντα εγκλήματα. Συγκεκριμένα, όσο αφορά τα ηλεκτρονικά εγκλήματα, που έχουν εισέλθει στην καθημερινότητα μας τα τελευταία χρόνια, το ενδιαφέρον της αστυνομίας εστιάζεται περισσότερο στις ασταμάτητες αλλαγές που προκύπτουν στους κόλπους της τεχνολογίας. Με τον τρόπο αυτό καθίσταται το ηλεκτρονικό έγκλημα δύσκολα έγκλημα, τόσο στο εξωτερικό όσο και στην Ελλάδα. Έτσι, αυτό που φαίνεται να κάνει αποτελεσματικότερο το έργο των διωκτικών αρχών είναι η συνεχής εκπαίδευση και επιμόρφωση του προσωπικού της αστυνομικής αρχής σε θέματα κυρίως τεχνικής φύσεως σχετικά με τη διερεύνηση και τη δίωξη του ηλεκτρονικού εγκλήματος. Στην Ελλάδα, η Ελληνική Αστυνομία (ΕΛ.ΑΣ.), έχει προχωρήσει στη σύσταση Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος (ΥΔΗΕ).

Εικόνα 29: Ηλεκτρονικό έγκλημα

Οι καταγγελίες των πολιτών που διαπιστώνουν ότι έχουν παραβιαστεί προσωπικά τους δεδομένα ή ότι έπεσαν θύματα κάποια ηλεκτρονικής απάτης ή γενικότερα έχουν αντιληφθεί κάτι ύποπτο σχετικά με το διαδίκτυο ή τη χρήση Η/Υ, θα πρέπει να απευθύνονται άμεσα στην αρμόδια αρχή (Λάζος, 2001; Ζάννη, 2005; Κριθαράς, 2009; saferinternet.gr).

Επιπλέον στην Ελλάδα, σχετικός με καταγγελίες για το ηλεκτρονικό έγκλημα είναι και ο ιστότοπος www.saferinternet.gr. Στο συγκεκριμένο ιστότοπο δράσης, ενημέρωσης και επαγρύπνησης του Ελληνικού Κέντρου Ασφαλούς Διαδικτύου (υπό την αιγίδα της Ευρωπαϊκής Ένωσης) υπάρχουν πολλές, χρήσιμες πληροφορίες και συμβουλές για την ορθή χρήση του Διαδικτύου, του κινητού τηλεφώνου και άλλων διαδραστικών τεχνολογιών (Λάζος, 2001; Ζάννη, 2005; Κριθαράς, 2009; saferinternet.gr).

Η εξιχνίαση πολλών υποθέσεων μη εξουσιοδοτημένης πρόσβασης σε δίκτυα από τις διωκτικές αρχές βασίζεται στον εντοπισμό της IP διεύθυνσης. Οι ηλεκτρονικοί εγκληματίες για να πραγματοποιήσουν επίθεση σε ένα σύστημα προκειμένου να παραπλανήσουν τις διωκτικές αρχές, χρησιμοποιούν πλαστές IP διευθύνσεις. Το Σύστημα Ονομάτων Χώρου (Domain Name System D.N.S.) μετατρέπει τα ονόματα των διευθύνσεων σε αριθμούς (IP διευθύνσεις), έτσι ώστε να μπορεί να τις επεξεργαστεί το δίκτυο. Ο επιτιθέμενος λοιπόν κατά την εκδήλωση μιας επίθεσης πλαστογραφεί τη διεύθυνση του με σκοπό να φαίνεται ότι είναι ένας νόμιμος χρήστης, δεν μπορεί όμως να πλαστογραφήσει την IP διεύθυνση. Τα firewalls καθώς και άλλα εργαλεία λογισμικού και on-line δικτυακοί τόποι δίνουν τη δυνατότητα να ελέγχουν αν μια διεύθυνση είναι αληθινή ή όχι και ανάλογα να αποτρέπουν ή να απαγορεύουν την πρόσβαση ενός χρήστη (Λάζος, 2001; Ζάννη, 2005; Κριθαράς, 2009; saferinternet.gr).

Τα τείχη προστασίας αποστέλλουν μηνύματα υψηλής προτεραιότητας σε συγκεκριμένους παραλήπτες όταν διαπιστωθεί κάποια ύποπτη δραστηριότητα. Τα μηνύματα αυτά αποστέλλονται με e-mail στο διαχειριστή του συστήματος και παράλληλα η ύποπτη δραστηριότητα αποθηκεύεται στα αρχεία καταγραφής. Η συγκεκριμένη λειτουργία των firewalls είναι εξαιρετικά μεγάλης σημασίας καθώς μπορεί να αποτρέψει την επίθεση κατά τη διαδικασία γέννησης της. Επίσης, μια αναφορά δίνει αρκετές πληροφορίες για την εκδήλωση της επίθεσης όπως για παράδειγμα τη συχνότητα αποτυχημένων προσπαθειών για την απόκτηση μη εξουσιοδοτημένης πρόσβασης και τη συχνότητα σφαλμάτων (Λάζος, 2001; Ζάννη, 2005; Κριθαράς, 2009; saferinternet.gr).

Στα αρχεία καταγραφής αποθηκεύονται πληροφορίες σχετικές με τη λειτουργία του συστήματος. Η χρησιμότητα τους μεγιστοποιείται όταν έχουν ενεργοποιηθεί συγκεκριμένες πολιτικές (group policies). Εφόσον δεν έχει οριστεί συγκεκριμένη πολιτική ασφαλείας για μια ομάδα χρηστών, τα security logs παραμένουν κενά. Ο διαχειριστής του συστήματος είναι υπεύθυνος για τον καθορισμό πολιτικών ασφαλείας. Οι ερευνητές της ΥΔΗΕ μπορούν με τη βοήθεια των αρχείων καταγραφής να εξακριβώσουν αν κάποια συγκεκριμένη εφαρμογή χρησιμοποιήθηκε από χρήστη και αν ο χρήστης αυτός είχε ή όχι εξουσιοδοτημένη πρόσβαση στο σύστημα. Η εύρεση του αποστολέα των μηνυμάτων ηλεκτρονικού ταχυδρομείου αποτελεί βασική εργασία προς την αναζήτηση και τον εντοπισμό ηλεκτρονικών ιχνών του δράστη (Λάζος, 2001; Ζάννη, 2005; Κριθαράς, 2009; saferinternet.gr).

Η ΥΔΗΕ αναφέρει ότι το ηλεκτρονικό ταχυδρομείο αποτελεί ένα πολύ διαδεδομένο μέσο για τη διάπραξη πολλών αδικημάτων όπως η μετάδοση κακόβουλου λογισμικού, οι απάτες και οι απειλές κλπ. Η αναγραφή των στοιχείων του αποστολέα-δράστη στο μήνυμά του και στην περίπτωση πάντα που τα στοιχεία αυτά δεν είναι παραπλανητικά, οδηγεί εύκολα τις διωκτικές αρχές στον εντοπισμό του. Τα μηνύματα ηλεκτρονικού ταχυδρομείου καθώς μεταβαίνουν από τον αποστολέα στον παραλήπτη, διέρχονται από ενδιάμεσους υπολογιστές, καθένας από τους οποίους προσθέτει στην επικεφαλίδα του μηνύματος τις δικές του πληροφορίες. Αυτές οι πληροφορίες στην επικεφαλίδα του μηνύματος είναι καταγεγραμμένες

σε διάφορα πεδία που αφορούν τις επικεφαλίδες του παραλήπτη και του αποστολέα, τις επικεφαλίδες ημερομηνίας και άλλες. Στην αναζήτηση του αποστολέα κακόβουλων μηνυμάτων, οι κρίσιμες πληροφορίες βρίσκονται στις επικεφαλίδες του αποστολέα.

Αυτές είναι η διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα, το μονοπάτι (διεύθυνση) προς τον αποστολέα και τους διακομιστές από τους οποίους πέρασε το μήνυμα για να φτάσει στον τελικό παραλήπτη του. Ο εντοπισμός του αποστολέα ενός μηνύματος ηλεκτρονικού ταχυδρομείου είναι μια εξαιρετικά δύσκολη διαδικασία, κατά την ΥΔΗΕ. Υπάρχουν διάφοροι μέθοδοι που βοηθούν τους δράστες στην απόκρυψη των στοιχείων της ταυτότητας τους (Λάζος, 2001; Ζάννη, 2005; Κριθαράς, 2009; saferinternet.gr).

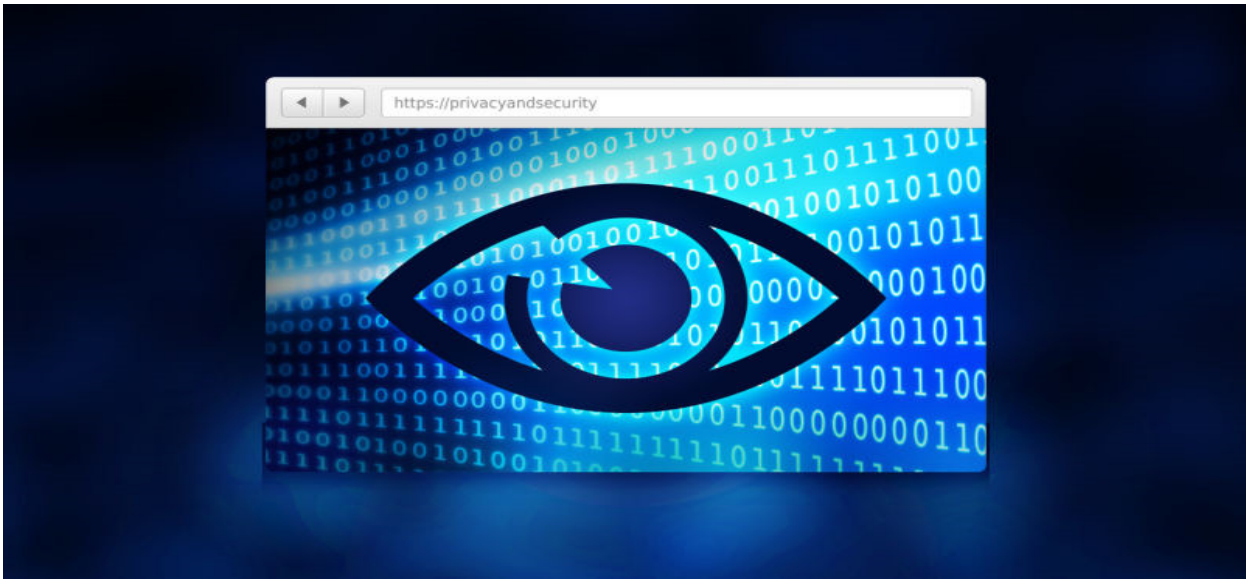
Το TOR αποτελώντας ένα δίκτυο από εικονικά τούνελ, επιτρέπει σε άτομα και ομάδες ατόμων να βελτιώσουν την ιδιωτικότητα και την ασφάλειά τους στο διαδίκτυο. Το TOR αποτελεί τη βάση για μια ποικιλία εφαρμογών λογισμικού που χρησιμοποιούνται για τον διαμοιρασμό πληροφοριών σε δημόσια δίκτυα χωρίς να απειλείται η ιδιωτικότητα των εμπλεκομένων. Μέσω του TOR, άτομα αποφεύγουν την καταγραφή της ταυτότητάς τους από τις ιστοσελίδες που επισκέπτονται, αλλά και την καταγραφή της διαδικτυακής τους κίνησης από τον τηλεπικοινωνιακό τους πάροχο. Σε άλλες περιπτώσεις, καταφέρνουν να παρακάμπτουν τους περιορισμούς που επιβάλλουν κυβερνήσεις ή πάροχοι, οι οποίοι μπλοκάρουν συγκεκριμένους ιστότοπους. Οι κρυφές υπηρεσίες του TOR επιτρέπουν στους χρήστες του να δημοσιεύουν τη δικιά τους ιστοσελίδα ή άλλη υπηρεσία, χωρίς να αποκαλύπτεται η τοποθεσία ή η ταυτότητά τους. Σε άλλες περιπτώσεις το TOR χρησιμοποιείται για την καταγγελία κοινωνικά ευαίσθητων πληροφοριών όπως βιασμοί ή κακοποιήσεις, για εργοδοτικές αυθαιρεσίες, διαρροές κυβερνητικών εγγράφων προς τον τύπο.

Εικόνα 30: Ηλεκτρονικό έγκλημα

- Η χρήση του TOR μειώνει την πιθανότητα επιτυχίας κάποιου που κατασκοπεύει ή να επιτηρεί τη διαδικτυακή κίνηση του χρήστη, με απλές ή περισσότερο πολύπλοκες μεθόδους. Για να γίνει αυτό, το TOR κατανέμει τη δικτυακή κίνηση μεταξύ διαφόρων σημείων στο διαδίκτυο, ούτως ώστε κανένα από τα σημεία αυτά να μην μπορεί να συσχετίσει τον χρήστη με τον τελικό προορισμό του. Η ιδέα προσομοιάζει με τη χρήση ενός λαβύρινθου για να ξεφορτωθείς κάποιον που σε ακολουθεί, όποτε μπορείς να σβήνεις και τα ίχνη σου. Αντί να πάρεις την πιο σύντομη και άμεση διαδρομή από την αφετηρία στον προορισμό, τα πακέτα δεδομένων στο δίκτυο του TOR παίρνουν ένα τυχαίο μονοπάτι, μέσω ενδιάμεσων κόμβων που καλύπτουν τα ίχνη του χρήστη. Έτσι, κανένας παρατηρητής σε συγκεκριμένο σημείο της διαδρομής στο διαδίκτυο, δεν μπορεί να συμπεράνει από που προέρχονται τα δεδομένα και για που προορίζονται.

Για την πληρέστερη κατανόηση του ρολού που μπορεί να παίξει το λογισμικό TOR στην εξιχνίαση του ηλεκτρονικού εγκλήματος, σύμφωνα με την εμπειρία των αστυνομικών της ΥΔΗΕ παραθέτουμε και σχολιάζουμε ορισμένα παραδείγματα από την παγκοσμία και ελληνική εμπειρία (saferinternet.gr):

- Ο χρήστης μπορεί να μεταφέρει δεδομένα διαφόρων ειδών, όπως επίσης να λειτουργήσει διαφορετικές εφαρμογές με βάση το TOR δίκτυο, ενώ ο κάθε κόμβος του κυκλώματος, είναι γνώστης μόνο ενός βήματος του μονοπατιού, επομένως ένας κακόβουλος ή ακόμα και μολυσμένος κόμβος, δεν μπορεί να προσδιορίσει τη ροή των δεδομένων από άκρη σε άκρη. Το TOR Browser Bundle, αποτελεί το λογισμικό επικοινωνία εξελιγμένων παρανόμων και τρομοκρατών. Στη δίκη της «Συνομωσίας Πυρήνων της Φωτιάς», αποκαλύφθηκε πλήρως η χρησιμοποίηση του συγκεκριμένου λογισμικού με τα ηγετικά μέλη της οργάνωση να επικοινωνούν μεταξύ τους έχοντας το λογισμικό σε USB-stick, που τοποθετούσαν σε υπολογιστές κυρίως σε διαδικτυακά καφέ. Πριν από τις συλλήψεις μελών της οργάνωσης οι έξι συλληφθέντες και η κοπέλα που διέφυγε, πριν συναντηθούν στο συγκεκριμένο σημείο είχαν κινηθεί μεμονωμένα σε τουλάχιστον τέσσερα διαδικτυακά καφέ στα Εξάρχεια, Άνω Πατήσια, Μαρούσι και Ν. Φιλαδέλφεια. Με την χρήση του TOR προέβησαν στις τελευταίες συνεννοήσεις για την ασφάλεια της συνάντησής τους. Οι αρμόδιοι αξιωματικοί της ΥΔΗΕ γνώριζαν αυτή την ηλεκτρονική δραστηριότητα. Κάποια στελέχη φαίνεται πως βρίσκονταν ως πελάτες σε ένα από τα διαδικτυακά καφέ, των Εξαρχείων, και εντόπισαν έναν από τους υπόπτους. Διαπίστωσαν ότι κατέβασε με USB-stick το συγκεκριμένο λογισμικό και τον έθεσαν υπό παρακολούθηση. Ακολούθησαν το ντόμινο των διαδοχικών συναντήσεών του με κατάληξη την σύλληψη τους.



Εικόνα 31: Ηλεκτρονικο έγκλημα

- Το TOR αναπτύσσει και διανέμει μια σειρά από λογισμικά, που προστατεύουν τον χρήστη διοχετεύοντας την επικοινωνία του σε ένα κατανεμημένο δίκτυο κόμβων ανά τον κόσμο. Αποτρέπει κάποιον που παρακολουθεί την δικτυακή κίνηση του χρήστη από το να γνωρίζει τις ιστοσελίδες που επισκέπτεται και ταυτόχρονα αποτρέπει τα site αυτά από το να γνωρίζουν την ταυτότητα του χρήστη. Το λογισμικό αυτό προσφέρει ένα καλό επίπεδο ανωνυμίας (ή καλύτερα ψευδωνυμίας) στον χρήστη. Το Facebook επιτρέπει στους χρήστες την ανώνυμη πρόσβαση μέσω της Darknet διαδικτυακής υπηρεσίας TOR, αφού δίνει τη δυνατότητα να μπαίνουν στο Facebook χωρίς να αφήνουν ίχνη. Έτσι, πλέον οι χρήστες του διαδικτύου, έχουν την δυνατότητα να συνδέονται απευθείας με το Facebook μέσω του TOR, η οποία επιτρέπει σε κάποιον να σερφάρει ανώνυμα και υπό κρυπτογραφική προστασία. Όλα τα δεδομένα του χρήστη είναι κρυπτογραφημένα, πράγμα που, σύμφωνα με το BBC, μπορεί να φανεί χρήσιμο σε χρήστες από χώρες, οι οποίες προσπαθούν να μπλοκάρουν την πρόσβαση στο Facebook, όπως το Ιράν, η Κίνα, η Βόρεια Κορέα και η Κούβα. Όμως και το TOR έχει ήδη βρεθεί στο στόχαστρο διαφόρων κυβερνήσεων που προσπαθούν επίσης να το μπλοκάρουν. Στην περίπτωση της πρόσβασης στο Facebook μέσω TOR, οι χρήστες θα πρέπει πάντα να συνδέονται με το όνομά τους. Όμως δεν θα είναι δυνατό να εντοπιστεί η τοποθεσία τους ή άλλη πληροφορία σχετική με αυτούς. Η πρόσβαση θα γίνεται μέσω του προγράμματος TOR Browser στη διεύθυνση facebookcorewwwi.onion.

- Το Facebook είναι η πρώτη μεγάλη εταιρεία η οποία επίσημα ανακοίνωσε την υποστήριξή της στο TOR, ένα δίκτυο που δημιουργήθηκε προκειμένου να επιτρέπει όχι μόνο την απολύτως μη ανιχνεύσιμη «περιήγηση» των χρηστών στο διαδίκτυο (η ταυτότητα και η γεωγραφική προέλευση του χρήστη αποκρύπτονται μέσω ειδικής τεχνολογίας παραπλάνησης), αλλά και τη δημιουργία αφανών ιστοσελίδων, οι οποίες δεν εμφανίζονται καν στις μηχανές αναζήτησης όπως της Google και των οποίων οι διευθύνσεις λήγουν σε onion. Οι υποστηρικτές του σκοτεινού διαδικτύου στρέφονται στην Amazon επιπλέον bandwidth ως TOR Project, αφού κάποιοι το αποκαλούν σκοτεινό ή μυστικό δίκτυο το οποίο επιτρέπει ανώνυμες online επικοινωνίες. Το TOR χρησιμοποιείται κυρίως από ακτιβιστές που θέλουν να αποφύγουν τη λογοκρισία, καθώς και από άτομα τα οποία επιζητούν ανωνυμία για πιο ύποπτους σκοπούς. Οι υποστηρικτές του επιθυμούν επέκταση του bandwidth της εν λόγω υπηρεσίας, και για αυτό στρέφονται στην Amazon, η cloud υπηρεσία της οποίας θα κάνει δυσκολότερο για τις κυβερνήσεις να παρακολουθήσουν τα δρώμενα στο σκοτεινό δίκτυο.

Εικόνα 32: Ηλεκτρονικο εγκλημα

- Η cloud υπηρεσία της Amazon EC2 παρέχει δυνατότητες εικονικού υπολογιστή. Οι επιτιθέμενοι μέσω του TOR ζητούν από τους υποστηρικτές του δικτύου να εγγραφούν στην υπηρεσία προκειμένου να δημιουργήσουν μια γέφυρα, μέσω του οποίου δρομολογούνται οι επικοινωνίες. Στήνοντας την γέφυρα αυτή, δωρίζετε bandwidth στο δίκτυο TOR και βοηθάτε στη βελτίωση της ασφάλειας και της ταχύτητας με την οποία οι χρήστες μπορούν να έχουν πρόσβαση στο διαδίκτυο. Οι χρήστες που επιθυμούν να συμμετάσχουν πρέπει να είναι εγγεγραμμένοι στην υπηρεσία της Amazon. Κανονικά, κοστίζει 30 δολάρια το μήνα, ωστόσο η Amazon προσφέρει δωρεάν αποθήκευση για ένα χρόνο στο πλαίσιο μίας εκστρατείας προώθησης- κάτι που η ομάδα του TOR πιστεύει ότι ενδείκνυται για τους χρήστες του σκοτεινού δικτύου.

- Το TOR χρησιμοποιείται και από άτομα τα οποία διακινούν υλικό παιδικής πορνογραφίας, κάτι που οδήγησε στην επιχείρηση σκοτεινού διαδικτύου από την ομάδα χάκερ Anonymous, με στόχο τον εντοπισμό αυτών που δραστηριοποιούνται στο διαδίκτυο με τέτοιους σκοπούς.

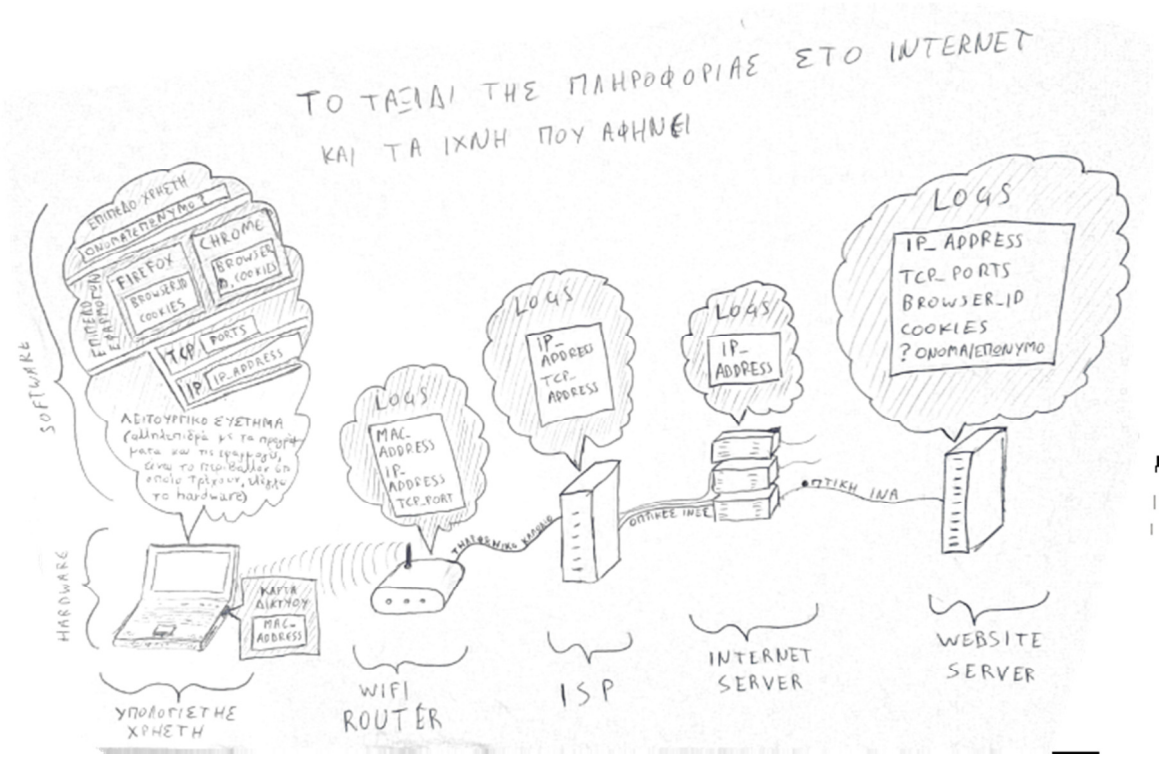
- Η πρόσβαση στο TOR δεν περιορίζεται μόνο σε σταθερές γραμμές: χρήστες Android μπορούν να έχουν πρόσβαση μέσω μίας εφαρμογής ονόματι Orbot, ενώ η Apple ενέκρινε την πώληση του Covert Browser για το iPad στο App Store. Πρόκειται για την πρώτη επίσημη εφαρμογή για το IOS που επιτρέπει στους χρήστες να δρομολογήσουν τις online επικοινωνίες του μέσω του TOR.

- Η Ελληνική Αστυνομία (ΕΛ.ΑΣ.) έχει προχωρήσει στη σύσταση Υπηρεσίας Δίωξης Ηλεκτρονικού Εγκλήματος (ΥΔΗΕ). Μόλις το 15% του διαδικτύου λειτουργεί στο φως, το υπόλοιπο 85% κινείται στο σκοτάδι», υποστηρίζουν εξειδικευμένοι αξιωματικοί της ΕΛ.ΑΣ.

11. ΚΕΦΑΛΛΑΙΟ 11: Σύνοψη εντοπισμού μας από το TOR.

Έχοντας ως κύριο στόχο την ανωνυμία, όπως είναι ευνόητο, μπορεί να το χρησιμοποιήσει ο καθένας για διαφορετικούς σκοπούς. Είναι γεγονός ότι μέσω του Tor, διακινείται πορνογραφία σε όλα τα επίπεδα, μα και πως χρησιμοποιείται για κυβερνο-επιθέσεις ή ακόμα και για πρόσβαση με χώρες όπου υπάρχει λογοκρισία στο διαδίκτυο. Το Tor είναι διαθέσιμο για όλα τα λειτουργικά συστήματα και μπορεί να χρησιμοποιηθεί τόσο σαν κανονικά εγκατεστημένη εφαρμογή όσο και σαν portable, από κάποιο usb στικάκι.

Στην ουσία, όπως αναφέρει και το ίδιο το Tor project, δεν είναι απλά μια εφαρμογή. Καθώς θα πρέπει να αλλάξετε τις μέχρι τώρα συνήθειες που είχατε κατά την πλοήγησή σας. Αυτό σημαίνει πως απευθύνεται σε ανθρώπους που λαμβάνουν σοβαρά υπόψη το ηλεκτρονικό απόρρητο και το δικαίωμα της Ανωνυμίας.



Εικόνα 33: Ιχνη και πληροφοριες που αφήνονται

Αν είσαι ύποπτος, ο πιο απλός τρόπος να γνωρίζει η αστυνομία όλη σου τη δραστηριότητα στον υπολογιστή, ανεξάρτητα απ' το αν χρησιμοποιείς ή όχι προγράμματα ανωνυμίας, είναι να εγκαταστήσουν στον υπολογιστή κατασκοπευτικό λογισμικό (spyware). Το πιο σύνηθες είναι κάποιο πρόγραμμα keylogger που στέλνει ό,τι πληκτρογραφείς και ό,τι κλικ κάνεις στους σέρβερ της αστυνομίας. Αν όμως αυτό προστατεύεσαι χρησιμοποιώντας ασφαλές λογισμικό, που δεν επιτρέπει την παρουσία τέτοιου είδους κακόβουλων προγραμμάτων, η αστυνομια είναι περιορισμένη στην υποκλοπή όλων των δεδομένων που εξέρχονται. Στην περίπτωση αυτή, έχει νόημα η χρησιμοποίηση προγραμμάτων ισχυρής κρυπτογράφησης και ανωνυμίας ώστε να μην μπορούν να διαβάσουν τα ευαίσθητα δεδομένα σου.

Υπάρχουν πολλοί τρόποι να αποκαλυφθεί η θέση και η ταυτότητα κάποιου στο ίντερνετ, αξιοποιώντας τα τεχνικά χαρακτηριστικά του δικτύου, που δε διαθέτει εγγενώς καμία υποδομή για ανωνυμία. Στον εντοπισμό συμβάλλουν χαρακτηριστικά από κάθε επίπεδο οργάνωσης της δικτύωσης:

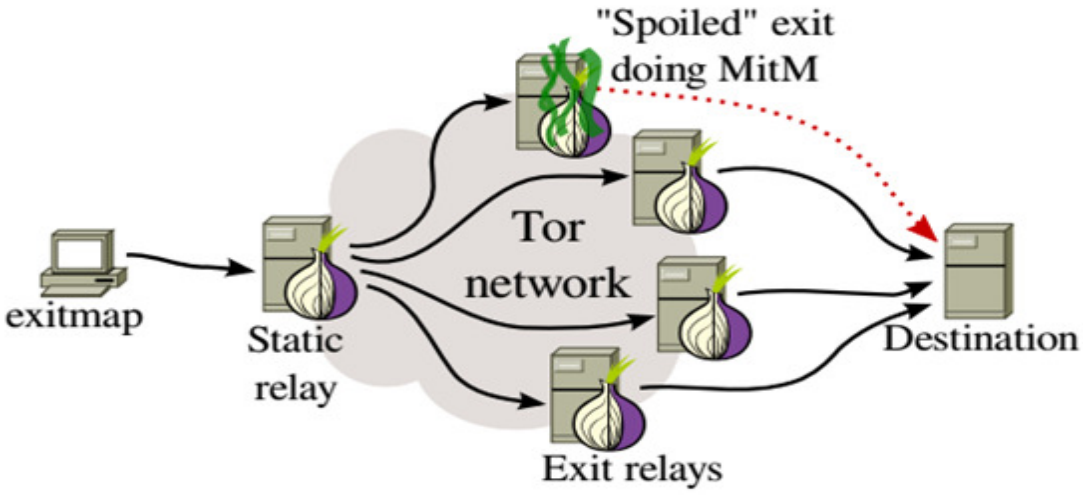
-Από προσωπικά δεδομένα στο επίπεδο χρήστη (π.χ. ονοματεπώνυμο που αποστέλλει ο χρήστης στο mail provider),

-Στο επίπεδο εφαρμογών το αναγνωριστικό του προγράμματος περιήγησης, browser_id, και τα cookies δηλαδή αρχεία που χρησιμοποιούν οι ιστοσελίδες για να σε ταυτοποιούν, ή αντίστοιχα αναγνωριστικά σε άλλες εφαρμογές.

-Τις ανοιχτές θύρες (ports) επικοινωνίας στο επίπεδο μεταφοράς δεδομένων, όπως και τη συμπεριφορά του λειτουργικού συστήματος, τη διεύθυνση IP με την οποία εκτίθεται ο υπολογιστής στο διαδίκτυο και τη διεύθυνση της κάρτας δικτύου mac address η οποία φαίνεται στο τοπικό δίκτυο.

-Κάθε χαρακτηριστικό και κάθε διεύθυνση είναι εφικτό να αλλάξει ή να μεταμφιεστεί με την εγκατάσταση κατάλληλου λογισμικού και τις αντίστοιχες ρυθμίσεις.

-Όμως το σημείο του δικτύου που συνδεθήκαμε είναι μια πληροφορία προσβάσιμη στον καθένα.



Εικόνα 34: TOR network

Σύμφωνα με το CNet, η λειτουργία ανωνυμίας του Tor "υπερθεματίζεται από το Electronic Frontier Foundation και από άλλες ομάδες πολιτικών δικαιωμάτων ως μέθοδος ανθρώπων που δουλεύουν για τα ανθρώπινα δικαιώματα για να επικοινωνούν με δημοσιογράφους".

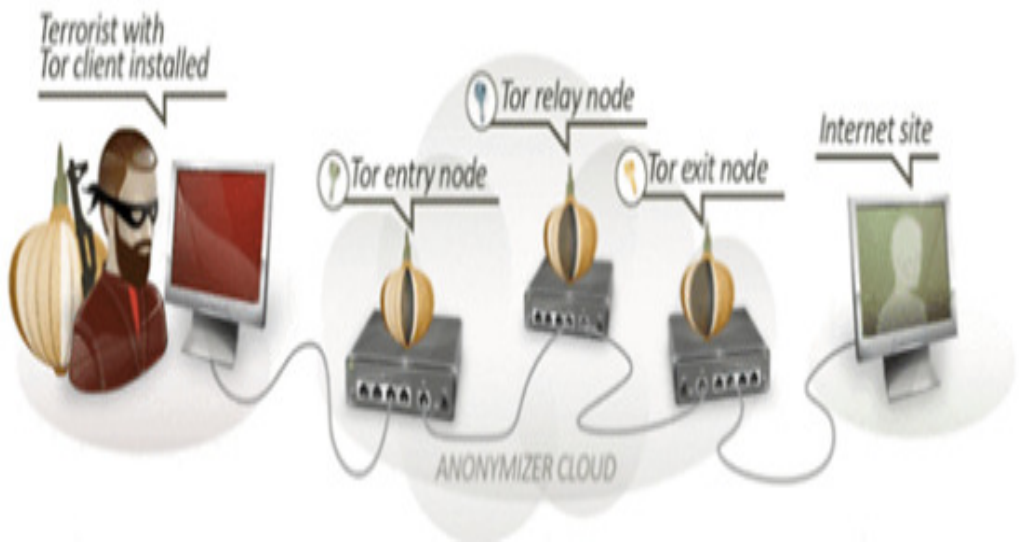
Συστήματα για ανωνυμία, όπως το Tor, χρησιμοποιούνται κατά καιρούς για ζητήματα που θεωρούνται παράνομα σε μερικές χώρες. Για παράδειγμα, το Tor μπορεί να χρησιμοποιηθεί για την απόκτηση πρόσβασης σε λογοκριμένες πληροφορίες, για την οργάνωση πολιτικών δραστηριοτήτων, είτε για την παράκαμψη νόμων ενάντια στην κριτική κατά του κράτους.

Παράλληλα, το Tor επιτρέπει ανώνυμες συκοφαντίες, αυθαίρετες διαρροές ευαίσθητων πληροφοριών, διανομή χωρίς άδεια υλικού με πνευματική ιδιοκτησία ή με παράνομο σεξουαλικό περιεχόμενο.

Το δίκτυο Tor χρησιμοποιείται ευρέως από ακτιβιστές και άτομα σε πολλές κρίσιμες περιοχές για την αποφυγή της λογοκρισίας του Διαδικτύου που λειτουργεί από τις κυβερνήσεις στην Κίνα, τη Συρία, το Μπαχρέιν και το Ιράν.Σύμφωνα με Tor Metrics, ο αριθμός των ανθρώπων σε όλο τον κόσμο που έχουν άμεση πρόσβαση στο δίκτυο ανωνυμοποίηση είναι 2,5 εκατομμύρια. Όπως όλα τα τωρινά δίκτυα ανωνυμοποίησης χαμηλής λανθάνουσας, το Tor δεν μπορεί και δεν προσπαθεί να προστατεύσει τους χρήστες από την παρακολούθηση της κίνησης στα όρια του δικτύου Tor, όπως για παράδειγμα, η κίνηση που εισέρχεται και εξέρχεται από το δίκτυο. Ενώ το Tor παρέχει προστασία κατά της ανάλυσης κίνησης, δεν προλαμβάνει την επιβεβαίωση της κίνησης.

Τον Μάρτιο του 2011, ερευνητές μαζί με ανθρώπους από το Rocquencourt, το εθνικό ινστιτούτο έρευνας στην επιστήμη της πληροφορικής και του ελέγχου που βρίσκεται στην Γαλλία, κατέγραψαν μια επίθεση ικανή να αποκαλύψει τη διεύθυνση IP των χρηστών του BitTorrent στο δίκτυο Tor. Η επίθεση ***bad apple*** χρησιμοποιεί τον σχεδιασμό του Tor και εκμεταλλεύεται κάθε μη ασφαλή χρήση εφαρμογής για να συσχετίσει την ταυτόχρονη χρήση μιας ασφαλής εφαρμογής με την διεύθυνση IP του συγκεκριμένου χρήστη Tor.

Μία μέθοδος επίθεσης εξαρτάται από τον έλεγχο ενός κόμβο εξόδου ή την υποκλοπή της απάντησης ενός ανιχνευτή, ενώ μία δεύτερη μέθοδος επίθεσης βασίζεται εν μέρει στην στατιστική εκμετάλλευση της ανίχνευσης του κατανεμημένου πίνακα κατακερματισμού.



Εικόνα 35: Anonymiser Cloud

Τον Οκτώβριο του 2011 ερευνητική ομάδα από την Esiea, Γαλλική σχολή μηχανολόγων, δήλωσε ότι ανακάλυψε έναν τρόπο να υπονομεύσει το δίκτυο του Tor με το να αποκρυπτογραφήσει επικοινωνίες που το διαπερνούν. Η τεχνική που περιέγραψαν απαιτεί

-τη δημιουργία ενός χάρτη των κόμβων του δικτύου Tor,

-τον έλεγχο του ενός τρίτου από αυτούς,

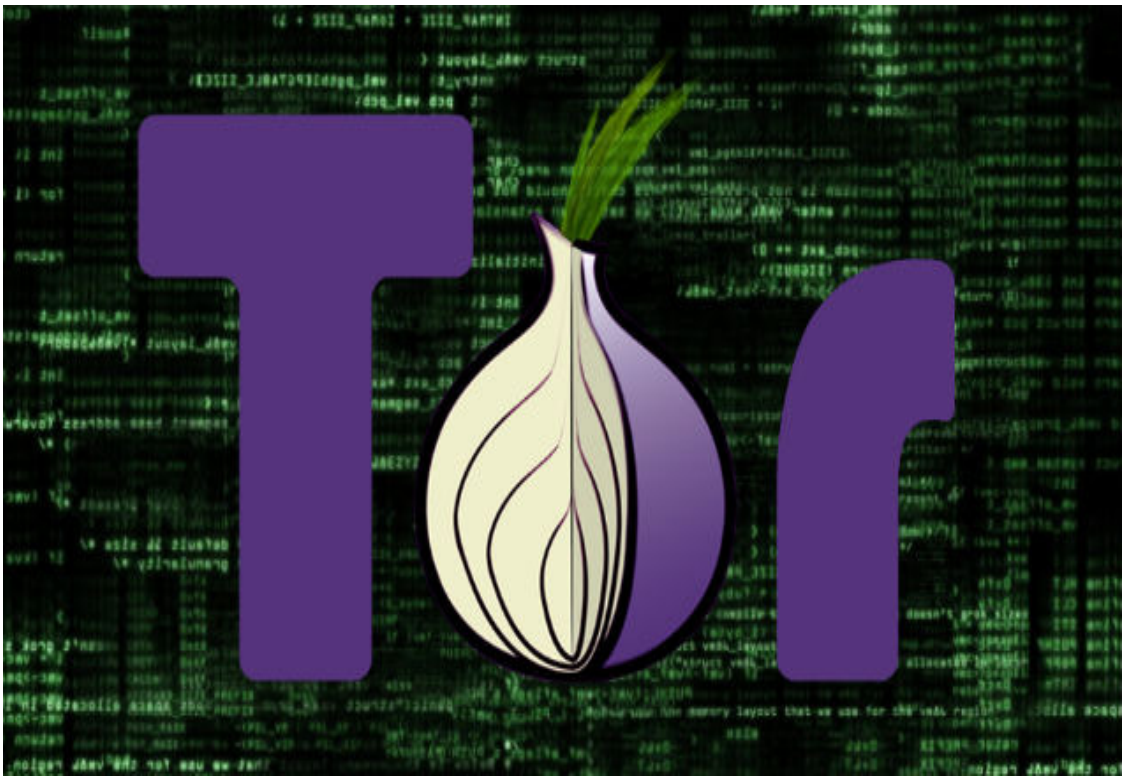
- και στην συνέχεια να αποκτήσουν τα κλειδιά κρυπτογράφησής τους και τις πηγές του αλγόριθμου.

Ύστερα, χρησιμοποιώντας τα γνωστά πλέον κλειδιά και τις πηγές θεωρούν ότι έχουν την ικανότητα να αποκρυπτογραφούν δύο από τα τρία στρώματα κρυπτογράφησης. Ισχυρίζονται ότι μπορούν να σπάσουν το τρίτο κλειδί με μια επίθεση που βασίζεται στην στατιστική ανάλυση. Για να επανακατευθύνουν την κίνηση του Tor στους κόμβους που ελέγχουν, χρησιμοποίησαν μεθόδους επίθεσης άρνησης εξυπηρέτησης και επίθεσης packet spinning.

Παρότι η αρχική ιδέα για το λογισμικό Tor χρηματοδοτήθηκε πράγματι από το πολεμικό Ναυτικό των ΗΠΑ, το εργαλείο Tor βασίζεται σε λογισμικό ανοικτού κώδικα, το οποίο έχουν επανειλημμένως ελέγξει έμπειροι κρυπτογράφοι και προγραμματιστές, επιβεβαιώνοντας την ασφάλεια και την ανωνυμία που υπόσχεται στους χρήστες. Μία ακόμη συχνή παρανόηση είναι ότι το εργαλείο Tor χρησιμοποιείται, κυρίως, από εγκληματίες.

Οι χρήστες του Tor, όμως, είναι σε μεγάλο ποσοστό ακτιβιστές, οι οποίοι προσπαθούν να διατηρήσουν την ανωνυμία τους, δημοσιογράφοι που το χρησιμοποιούν για μεγαλύτερη ασφάλεια κατά τη διεξαγωγή της έρευνάς τους, οικογένειες που επιθυμούν να προστατεύσουν τα παιδιά τους και να διατηρήσουν την ιδιωτικότητά τους, καθώς και κυβερνήσεις που το χρησιμοποιούν για ασφαλείς επικοινωνίες και σχεδιασμό. Το Tor είναι ακόμη ένα εργαλείο, όπως είναι και το internet, στη διάθεση οποιουδήποτε θέλει να το χρησιμοποιήσει για τις υπηρεσίες που παρέχει.

Επιπλέον, παρά τις φήμες που κυκλοφορούν κατά διαστήματα, δεν έχει υπάρξει καμία μήνυση, σύλληψη ή καταδίκη στις ΗΠΑ σχετιζόμενη με χρήση του εργαλείου Tor και των υπηρεσιών του, ενώ προς το παρόν δεν υπάρχει δεδικασμένο, επομένως δε θεωρείται ότι η χρήση του εργαλείου για ανώνυμη πλοήγηση αποτελεί ποινικό αδίκημα, σύμφωνα με το δίκαιο στις ΗΠΑ.



Εικόνα 36: TOR και ο εντοπισμος.

12. ΚΕΦΑΛΑΙΟ 12: Συμπεράσματα

Οι νέες τεχνολογίες αλλάζουν τους τρόπους και τα μέσα τέλεσης συμβατικών εγκλημάτων, ενώ νέες μορφές αμιγώς ηλεκτρονικών εγκλημάτων με οικονομικό αντίκτυπο τις περισσότερες φορές, κάνουν την εμφάνιση τους. Ως αποτέλεσμα το έργο των διωκτικών αρχών, η νομοθεσία και γενικά όλοι οι τομείς που επηρεάζουν την μεθοδολογία διερεύνησης των εγκλημάτων καθώς και το σύστημα απονομής δικαιοσύνης σε κάθε χώρα να μεταβάλλεται εξαιτίας ελλείψεων. Στο ηλεκτρονικό έγκλημα ο θύτης, λειτουργώντας από την μια πλευρά στην αφάνεια και αφήνοντας ελάχιστα ίχνη και από την άλλη με σύμμαχο την έλλειψη τεχνογνωσίας, καταφέρνει καθημερινά να εισβάλει ακόμα και σε εκείνο το σπίτι με το τελειότερα συστήματα ασφαλείας έχοντας σχεδόν πάντα σαν σκοπό την απολαβή οικονομικού οφέλους. Παράλληλα οι μορφές των εγκληματικών ενεργειών του καλύπτουν σχεδόν όλο το φάσμα του ποινικού κώδικα, αλλά και των αναφερθέντων νομικών κενών όσον αφορά τον ηλεκτρονικό χώρο δρα ανενόχλητος. Για την αντιμετώπιση των φαινομένων αυτών η ΥΔΗΕ πρέπει να λάβει τα μέτρα του κατά της εκδήλωσης αυτών των επιθέσεων, αλλά ταυτόχρονα να είναι σε θέση να αποκαταστήσει τη ζημιά που προκλήθηκε με όσο το δυνατότερο λιγότερες οικονομικές απώλειες, εφόσον αυτός είναι ο πρωτεύον σκοπός του εγκληματία.

Στο νέο αυτό περιβάλλον, η ΥΔΗΕ καλείται να αντιμετωπίσει το έγκλημα:

- ✓ Εκσυγχρονίζοντας τις υπηρεσίες της με τα κατάλληλα τεχνικά μέσα.

- ✓ Με τη θέσπιση νέων αντικειμενικών κριτηρίων για το ηλεκτρονικό έγκλημα, που να θέτουν όρια στην συμπεριφορά όσον χρησιμοποιούν το διαδίκτυο κατά την θέσπιση των διατάξεων αυτών πρέπει να ληφθούν υπόψη η ελεύθερη διακίνηση ιδεών και οι λοιπές συνταγματικές αρχές.

- ✓ Με την απαραίτητη η εκπαίδευση των στελεχών της ΥΔΗΕ, όπως επίσης και όλων των εμπλεκόμενων φορέων (εισαγγελικών, δικαστικών και αστυνομικών αρχών) σε θέματα διαδικτύου καθώς και η ενημέρωση των πολιτών στην χρήση του.

Τα συμπεράσματα στα οποία καταλήξαμε στην διπλωματική μας εργασία, καθώς και οι προτάσεις μας για περαιτέρω μελέτη είναι οι εξής:

- ✓ Το TOR χρησιμοποιεί ισχυρή κρυπτογραφία απέναντι σε επιθέσεις κατά της ανωνυμίας του χρήστη στο επίπεδο του Darknet. Η ανωνυμία παραβιάζεται μόνο αν γίνει παρακολούθηση όλων των κόμβων που συμμετέχουν στο κύκλωμα, αφού κάθε μεταβιβαστής δεν μπορεί να δει πάνω από έναν κόμβο στο κύκλωμα,

- ✓ Βασικό μειονέκτημα του TOR είναι η αργή απόδοσή του και οι μελλοντικές έρευνες θα πρέπει να εστιάσουν στη βελτίωση αυτής προκειμένου το TOR να γίνει ευρέως αποδεκτό.

- ✓ Πλέον η ανώνυμη περιήγηση θεωρείται απαραίτητη για κάποιους ανθρώπους όπως για παράδειγμα ερευνητές, δημοσιογράφους κλπ. ώστε να εξασφαλίσουν την ανωνυμία τους για την προσωπική τους ασφάλεια.

- ✓ Όμως απ' την στιγμή που προσφέρει ανωνυμία σε περιβάλλον με άπειρη έκταση και δυνατότητες αποτελεί ένα 'δυνατό εργαλειο το οποίο δεν θα άφηναν ανεκμετάλλευτο οι εγκληματίες για να εκτελέσουν τις παράνομες πράξεις του.

- ✓ Ενα εργαλείο με αυτές τις άπειρες δυνατότητες χρησιμοποιείται κατά κύριο λόγο για παράνομες πράξεις. Ενώ κάλλιστα θα μπορούσε να προσφέρει πολλά παραπάνω στην κοινωνία μας.

13. ΚΕΦΑΛΑΙΟ 13: Βιβλιογραφία:

Αλεξιάδης, Σ., (1996). *Εγχειρίδιο εγκληματολογίας*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Bell, S., (2008). *Encyclopedia of forensic science, revised edition*. Infobase Publishing.

Bigelow, R., (1985). *The challenges of computer law*. Western New England Law Review v. 7, p. 397.

Βελέντζας, ΕΙ., (2008). *Δίκαιο τεχνολογίας και καινοτομίας*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Βλαχόπουλος, Κ., (2007). *Ηλεκτρονικό Έγκλημα-Μορφές, Πρόληψη, Αντιμετώπιση*. Αθήνα, Νομική Βιβλιοθήκη.

Caloyannides, M., (2004). *Privacy protection and computer forensics*. 2nd Edition, Artech House.

Casey, E., (2004). *Digital evidence and computer crime: Forensic science, computers, and the internet*. 2nd Edition, Academic Press.

Γκρίτζαλης, Σ., Κάτσικας, Σ., και Γκρίτζαλης Δ., (2003). *Ασφάλεια δικτύων υπολογιστών*. Αθήνα, Παπασωτηρίου.

Dingledine, R., Mathewson, N., Syverson, P., (2004). TOR: The second-generation onion router». *Proc. 13th USENIX Security Symposium*. San Diego, California.

Δήμου, Γ., (2002). *Η διαχείριση υποθέσεων σεξουαλικής κακοποίησης ανηλίκων*, Αθήνα, Παπασωτηρίου.

Ζάννη, Α., (2005). *Το διαδικτυακό έγκλημα*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Furnell, S., (2006). *Κυβερνοέγκλημα-Καταστρέφοντας την κοινωνία της πληροφορίας*. Μετάφραση: Φ. Μηλιώνη, Αθήνα, Εκδόσεις Παπαζήση.

Glick, L, (1995). *Criminology*. Boston, Allyn and Bakon, Editors, p. 120.

Goldberg, I., and Shostack, A., (1999). Freedom network 1.0 architecture and protocols. http://www.freedom.net/info/freedompapers/index.html.

Jacobson, A., (2008). Privacy and security in internet-based information systems. Blekinge Institute of Technology, 250 p.

Jansen, W., & Ayers, R., (2007) *Guidelines on cell phone forensics. Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-101.

Jones, R., (2005). *Internet forensics*. O' Reilly Publishing. ISBN 059610006X.

Kanellis, P., (2006). *Digital crime and forensic science in cyberspace*. Idea Group Inc.

Καϊάφα-Γκμπάντι, Μ., & Συμεωνίδου-Καστανίδου, Ε., (2004). *Ποινικός κώδικας και ειδικοί ποινικοί νόμοι*. Β΄ έκδοση, Αθήνα, Νομική Βιβλιοθήκη.

Καρακώστας, Ι., (2003). Δίκαιο και internet. Νομικά ζητήματα στο διαδίκτυο. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Κάτσικας, Σ., Γκρίτζαλης, Δ., Γκρίτζαλης Σ., (2004). *Ασφάλεια πληροφοριακών συστημάτων*. Αθήνα, Εκδόσεις Νέων Τεχνολογιών.

Κιούπης, Δ., (1999). *Ποινικό δίκαιο και ιντερνέτ*. Θεσσαλονίκη: Εκδόσεις Σάκκουλα.

Κιούπης, Δ., & Ιωαννίδου, Α., (2007). *Η παιδική πορνογραφία στο διαδίκτυο*. Αθήνα, Νομική Βιβλιοθήκη.

Κριθαράς, Θ., (2009). *Ποινικό δίκαιο και διαδίκτυο*. Αθήνα, Νομική Βιβλιοθήκη.

Le Blond, S., Manils, P., Chaabane, A., Ali Kaafar, M., Castelluccia, C., Legout, A., and Dabbous, W., (2011). One bad apple spoils the bunch: exploiting p2p applications to trace and profile TOR users. National Institute for Research in Computer Science and Control, p. 550.

Lemley, M.A., & Reese, R.A., (2004). *Reducing digital copyright without restricting innovation*, 56 Stan. L. Rev. 1345, 1382.

Levine, B.N., and Shields, C., (2002). Hordes: A multicast based protocol for anonymity. The Bell System Technical Journal, 27, 623-656.

Λάζος, Γ., (2001). *Πληροφορική και έγκλημα*. Αθήνα, Νομική Βιβλιοθήκη.

Muller S., Brecht F., Fabian B., Kunz S., and Kunze D., (2012). Distributed performance and usability assesment of the TOR anonymization Network. Future Internet, 4, 488-513.

Mohay, G., (2003). *Computer and intrusion forensics*. Artech House.

Μαγκάκης, Γ.Α., (1984). *Ποινικό δίκαιο*. Έκδοση Γ΄ βελτιωμένη, εκδόσεις Παπαζήση.

Νικολαΐδης, Χ., (1999*). Η σκοτεινή πλευρά του Internet*. Αθήνα, Εκδόσεις Anubis.

Lasse, O., (2006). Locating hidden servers. *Proceedings of the 2006 IEEE Symposium on Security and Privacy*. IEEE Symposium on Security and Privacy. doi:10.1109/SP.2006.24. ISBN 0-7695-2574-1.

Reiter, M., and Rubin, A., (1998). *Crowds: Anonymity for web transactions*. ACM Transactions on Information and System Security, pp. 66-92.

Skoudis, E., (2002). *A step-by-step guide to computer attacks and effective defenses*. PrenticeHall.

Soghoian, C., (2007). TOR anonymity server admin arrested. *CNET News*.

Συκιώτου, Α., (2009). *Το διαδίκτυο ως σύγχρονο όχημα θυματοποίησης*. Θεσσαλονίκη:

Εκδόσεις Σάκκουλα.

Torvalds, L., (2011). Κυκλοφορία του Linux 3.0, Technology Review, v. 3, 56-87.

Τσουραμάνης, Χ., (2005). *Ψηφιακή εγκληματικότητα. Η (αν)ασφαλής όψη του διαδικτύου*.

https://books.google.gr/books?id=rL1sCQAAQBAJ&pg=PA64&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

https://books.google.gr/books?id=eUu7BQAAQBAJ&pg=PA171&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

https://books.google.gr/books?id=cKqeBQAAQBAJ&pg=PA121&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

https://books.google.gr/books?id=BjeLDQAAQBAJ&pg=PT155&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

https://books.google.gr/books?id=mVrNBQAAQBAJ&pg=PA116&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

https://books.google.gr/books?id=Vmthw-ziiVoC&pg=PA174&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

https://books.google.gr/books?id=mvtqCQAAQBAJ&pg=PA99&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

https://books.google.gr/books?id=mvtqCQAAQBAJ&pg=PA99&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

https://books.google.gr/books?id=Vmthw-ziiVoC&pg=PA174&dq=The+onion+router&hl=el&sa=X&redir_esc=y#v=onepage&q=The%20onion%20router&f=false

<u>Ιστοσελίδες:</u>

https://books.google.gr/books

https://www.pcsteps.gr/Raspberry_Ριεσσαλονίκη: Εκδόσεις Σάκκουλα.

www.Wikipedia.com

https://www.reddit.com/r/TOR/comments/1bxw2n/how_to_enable_sslhttps_for_onion_domains/

https://wikileaks.org/wiki/WikiLeaks:Tor

https://www.eff.org/pages/tor-and-https

https://www.youtube.com/watch?v=_dp1r4aKfe
http://www.itpro.co.uk/mobile/21862/raspberry-pi-top-22-projects-to-try-yourselfg

http://www.instructables.com/id/Raspberry-Pi-Tor-relay/

https://makezine.com/projects/browse-anonymously-with-a-diy-raspberry-pi-vpntor-router/

https://guardianproject.info/apps/orbot/

https://www.torproject.org/

https://www.torproject.org/projects/torbrowser.html.en

https://tails.boum.org/

https://www.torproject.org/docs/pluggable-transports.html.en

http://policenet.gr/article/10

Εικόνες:

Αναφορικά οι ιστοσελίδες που βρήκαμε όλες τις εικόνες:

Εικόνες λογοτύπων από:
(https://www.google.gr/search?q=tor&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjh-Yf71IrSAhVFVRQKHTmcBFYQ_AUIBigB#imgrc=7_UfSx2NGQD1MM:)

Εικόνες για το TOR γενικα:
(https://www.google.gr/search?q=TOR&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjTo4HX14rSAhWGwBQKHa_IDFEQ_AUIBigB)

Εικόνες για το ηλεκτρονικό έγκλημα:
(https://www.google.gr/search?q=TOR&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjTo4HX14rSAhWGwBQKHa_IDFEQ_AUIBigB#hl=el&tbm=isch&q=TOR+kai+%CE%B7%CE%BB%CE%B5%CE%BA%CF%84%CF%81%CE%BF%CE%BD%CE%B9%CE%BA%CE%BF+%CE%B5%CE%B3%CE%BA%CE%BB%CE%B7%CE%BC%CE%B1)

Εικόνες για TOR και Raspberry Pi3:
(https://www.google.gr/search?q=TOR&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjTo4HX14rSAhWGwBQKHa_IDFEQ_AUIBigB#hl=el&tbm=isch&q=TOR+raspberry)

Εικόνες για TOR Browser:
(https://www.google.gr/search?q=TOR&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjTo4HX14rSAhWGwBQKHa_IDFEQ_AUIBigB#hl=el&tbm=isch&q=tor+browser)

Εικόνες για TOR για Android:
(https://www.google.gr/search?q=TOR&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjTo4HX14rSAhWGwBQKHa_IDFEQ_AUIBigB#hl=el&tbm=isch&q=tor+android)

Εικόνες για TOR Messenger:
(https://www.google.gr/search?q=TOR&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjTo4HX14rSAhWGwBQKHa_IDFEQ_AUIBigB#hl=el&tbm=isch&q=tor+messenger)

Εικόνες για TOR blocked:
(https://blog.torproject.org/blog/breaking-through-censorship-barriers-even-when-tor-blocked)

Εικόνες για το Vidalia:
(https://www.google.gr/search?q=vidalia&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjmrqSo2YrSAhVF8RQKHeFYA1cQ_AUIBigB)

Εικόνες για I2P:
(https://www.google.gr/search?q=vidalia&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjmrqSo2YrSAhVF8RQKHeFYA1cQ_AUIBigB#hl=el&tbm=isch&q=i2p)

Εικόνες για το I2P Alice και Bob:
(https://www.google.gr/search?q=vidalia&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjmrqSo2YrSAhVF8RQKHeFYA1cQ_AUIBigB#hl=el&tbm=isch&q=i2p+alice+)

Εικόνες για I2P Android:
(https://www.google.gr/search?q=vidalia&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjmrqSo2YrSAhVF8RQKHeFYA1cQ_AUIBigB#hl=el&tbm=isch&q=i2p+android)

Εικόνες για Http cookies:
(https://www.google.gr/search?q=vidalia&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&ved=0ahUKEwjmrqSo2YrSAhVF8RQKHeFYA1cQ_AUIBigB#hl=el&tbm=isch&q=htttp+cookies)

Εικόνες για TOR Network:
(https://www.google.gr/search?q=tor+network&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&sqi=2&ved=0ahUKEwjZtfWL24rSAhUEM8AKHTKeA7UQ_AUIBigB)

Εικόνες για Anonymizer Cloud:
(https://www.google.gr/search?q=tor+network&hl=el&biw=1707&bih=827&site=webhp&source=lnms&tbm=isch&sa=X&sqi=2&ved=0ahUKEwjZtfWL24rSAhUEM8AKHTKeA7UQ_AUIBigB#hl=el&tbm=isch&q=anonymizer+tor&imgrc=4KilIEUFVlxX0M:)