Πανεπιστήμιο Δυτικής Αττικής
Σχολή Μηχανικών
Τμήμα Μηχανικών Πληροφορικής και Υπολογιστών
ΠΜΣ «Κυβερνοασφάλεια»

Εφαρμοσμένη Κρυπτογραφία

Διδάσκων: Δρ. Παναγιώτης Ριζομελιώτης

Υπηρεσίες Onion

Λειτουργίες, μορφή και ασφάλεια

Παραφέστας Νίκος

Ξάνθη, 30 Δεκεμβρίου, 2023

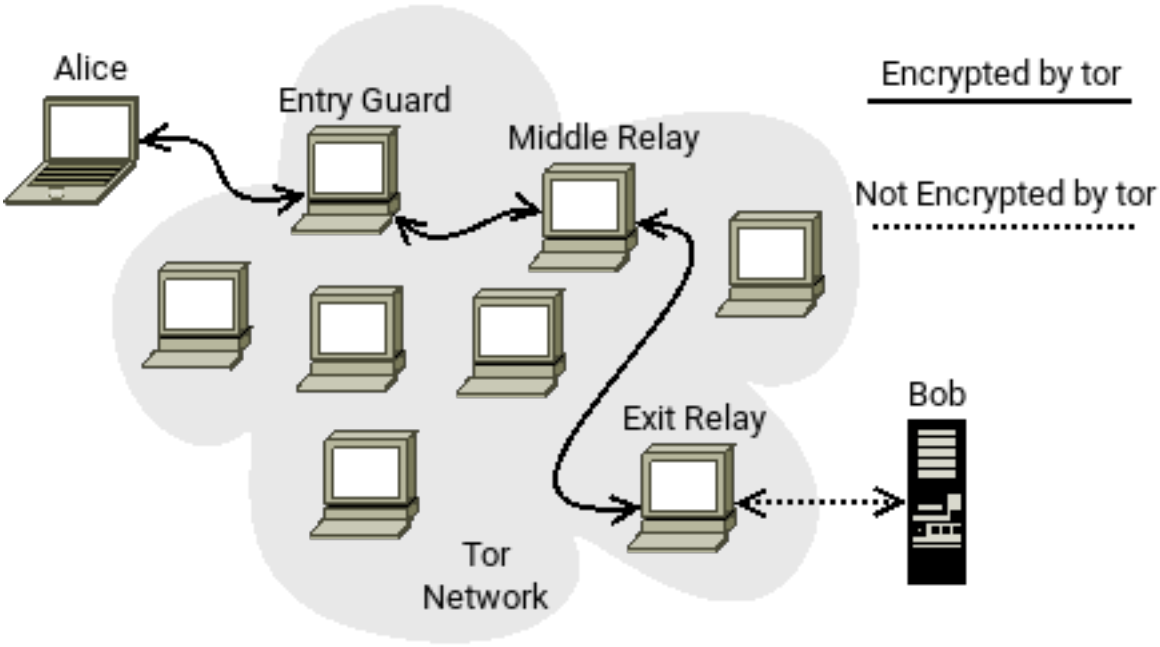
Ν. Παραφέστας, Ξάνθη 2023.

Περιεχόμενα

Κατάλογος Σχημάτων

Κεφάλαιο 1

Δίκτυο tor - Γενικά



Σχήμα 1.1: Λειτουργία του δικτύου tor

Στο Σχήμα 1.1 μπορούμε να δούμε την τυπική μέθοδο ασφαλούς μετάδοσης μιας πληροφορίας μέσω του δικτύου tor. Συγκεκριμένα χρησιμοποιούνται τρεις κόμβοι η λειτουργία των οποίων αναλύεται παρακάτω. Κάθε κόμβος και υπολογιστικό σύστημα γνωρίζει πληροφορίες μόνο για το προηγούμενο και το επόμενο στοιχείο και απολύτως τίποτα για τα υπόλοιπα.

1.1 Entry Guard

Έστω ότι η Eve[1] μπορεί να παρακολουθεί τους c από τους n διαθέσιμους κόμβους αναμετάδοσης στο δίκτυο tor, τότε η πιθανότητα της να συσχετίσει τις κινήσεις

[1]Κακόβουλος χρήστης - κακόβουλη χρήστρια.

της Alice είναι p=2(c/n).

Με τη χρήση των Entry Guards[2] γίνεται τυχαία επιλογή ενός αριθμού κόμβων από την Alice, τους οποίους χρησιμοποιεί αποκλειστικά για τα χρήση του πρώτου βήματος. Η Eve μπορεί να νικήσει μόνο αν έχει πρόσβαση σε αυτόν τον κόμβο με πιθανότητα p=1-(n-c)/n $<$ 2(c/n) [2].

1.2 Middle Relay

Κοινοί κόμβοι αναμετάδοσης. Ακόμα και αν η Eve κατέχει τον ενδιάμεσο κόμβο δεν μπορεί να αποσπάσει σημαντικές πληροφορίες.

1.3 Exit Relay

Είναι ο μοναδικός κόμβος που μπορεί να γνωρίζει ο Bob (και οποιαδήποτε οντότητα παρακολουθεί τις κινήσεις του) ότι προήλθε το αίτημα. Στις υπηρεσίες onion δεν έχει εφαρμογή ο κόμβος εξόδου, καθώς όλα συμβαίνουν μέσα στο δίκτυο.

[2]Εισαγωγικοί κόμβοι αναμετάδοσης.

Κεφάλαιο 2

Υπηρεσίες onion

2.1 Εισαγωγή στις υπηρεσίες onion

Ενώ το δίκτυο tor χρησιμοποιείται κυρίως για να διατηρούν οι χρήστ(ρι)ες την ανωνυμία τους κατά την περιήγησή τους στο διαδίκτυο, οι υπηρεσίες onion[1] προστατεύουν την ανωνυμία δημιουργίας μιας ιστοσελίδας ή άλλης δικτυακής υπηρεσίας.

2.2 Πρόσβαση στις υπηρεσίες onion

Η πρόσβαση σε υπηρεσίες onion γίνεται αποκλειστικά μέσω του δικτύου tor, συνήθως μέσω του tor browser[2], μπορεί όμως να χρησιμοποιηθεί και οποιοσδήποτε άλλος browser με χρήση κατάλληλου proxy. Αρκετές σελίδες δημοσιογραφικών οργανισμών (the guardian, new york times, bbc κ.α) και social media προσφέρουν υπηρεσίες onion [3], είναι όμως απαραίτητο οι χρήστ(ρι)ες να γνωρίζουν ότι οποιαδήποτε παροχή προσωπικών δεδομένων στις ιστοσελίδες, όπως καταχώρηση στοιχείων ταυτότητας ή χρήση τεχνολογιών όπως CSS ή/και javascript μπορεί να οδηγήσει σε κατάργηση της ανωνυμίας.

Εκτός από περιηγητές, η χρήση του δικτύου tor μπορεί να χρησιμοποιηθεί και από οποιαδήποτε εφαρμογή έχει επικοινωνία με το διαδίκτυο, όπως τερματικό, e-mail client, πρόγραμμα επικοινωνίας κτλ. Σημαντικές επίσης εφαρμογές που δημιουργήθηκαν από την ομάδα του tor και υποστηρίζουν τις υπηρεσίες onion είναι το onionshare [4] για ανώνυμη ανταλλαγή αρχείων και το securedrop [5] για αποδοχή εγγράφων από μάρτυρες δημοσίου συμφέροντος (whistleblowers) χωρίς να αποκαλύπτεται η ταυτότητά τους.

[1] Μετονομάστηκαν από «κρυφές υπηρεσίες» σε υπηρεσίες ώστε να μη θεωρούν οι χρήστες και οι χρήστριες ότι έχουν εφαρμογή μόνο σε κακόβουλες πράξεις.

[2] https://www.torproject.org

[3] Ενδεικτικός κατάλογος στο https://community.torproject.org/onion-services/

[4] https://onionshare.org/

[5] https://securedrop.org/

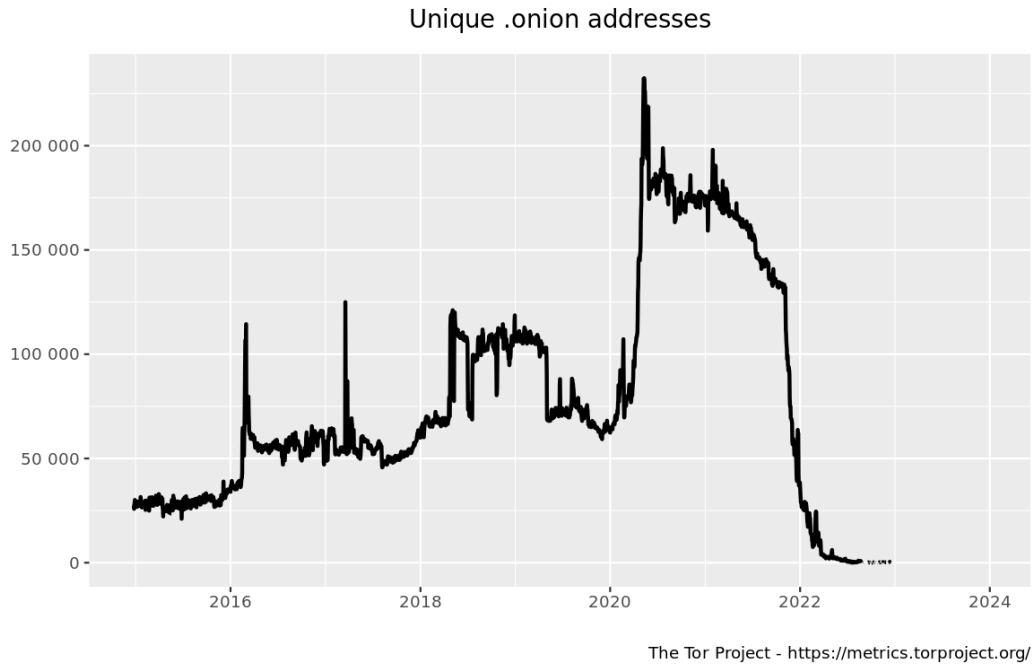
2.3 Διευθύνσεις υπηρεσιών onion

Οι διευθύνσεις των υπηρεσιών onion έχουν την κατάληξη .onion και είναι της μορφής [1]:

V2: Αποτελείται από 16 χαρακτήρες[6] που προκύπτουν από το SHA1 hash των πρώτων 80 χαρακτήρων του ιδιωτικού κλειδιού του server.

V3: Αποτελείται από 56 χαρακτήρες[7] που προκύπτουν από το πλήρες εδ25519 ιδιωτικό κλειδί του server. Αυτή είναι η τρέχουσα έκδοση που συστήνεται από την ομάδα ανάπτυξης του tor.

Η V2 έκδοση πλέον θεωρείται παρωχημένη και μη ασφαλής. Στη θέση της συστήνεται από την ομάδα ανάπτυξης του tor η έκδοση V3. Στα Σχήματα 2.1 και 2.2 παρουσιάζονται οι μοναδικές διευθύνσεις για τις εκδόσεις V2 και V3 των υπηρεσιών onion, ενώ στα Σχήματα 2.3 και 2.4 παρουσιάζεται η συνολική κίνηση στις υπηρεσίες onion[8].



Σχήμα 2.1: Συνολικός Αριθμός Υπηρεσιών Onion V2, 2015 - 2023.

2.4 Περιγραφή λειτουργίας

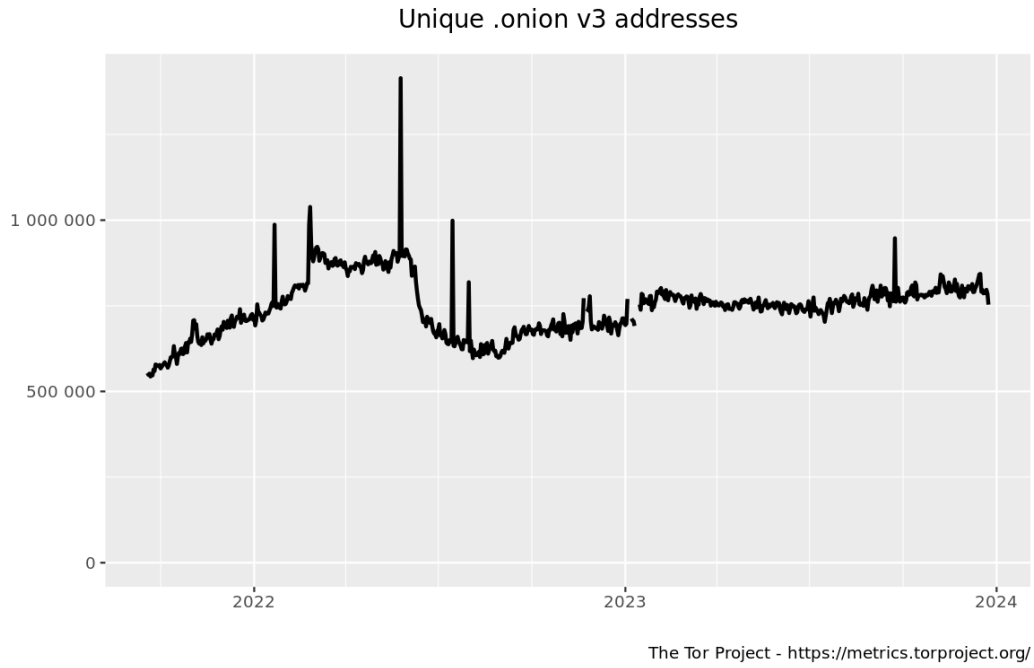
Στο Σχήμα 2.5 αναπαριστώνται τα βήματα μιας υπηρεσίας onion.

Βήμα 1: Ο Bob γνωστοποιεί ότι «τρέχει» μια υπηρεσία onion διαλέγοντας στην τύχη τρεις κόμβους με τους οποίους φτιάχνει κύκλωμα για να συνδεθεί

[6]Π.χ. e3mhbshg7kx5tfyd.onion

[7]Π.χ. x5u6sk242wvsohyivyylxzpkr2szut5aarpyomv2lg6g2qtp5dv4l3qd.onion

[8]Πηγή: https://metrics.torproject.org/hidserv-dir-onions-seen.html



Σχήμα 2.2: Συνολικός Αριθμός Υπηρεσιών Onion V3, 2021 - 2023.

και, τους ζητάει να γίνουν σημεία γνωστοποίησης [IP (Introduction Points)] στα οποία στέλνει το δημόσιο κλειδί της υπηρεσίας.

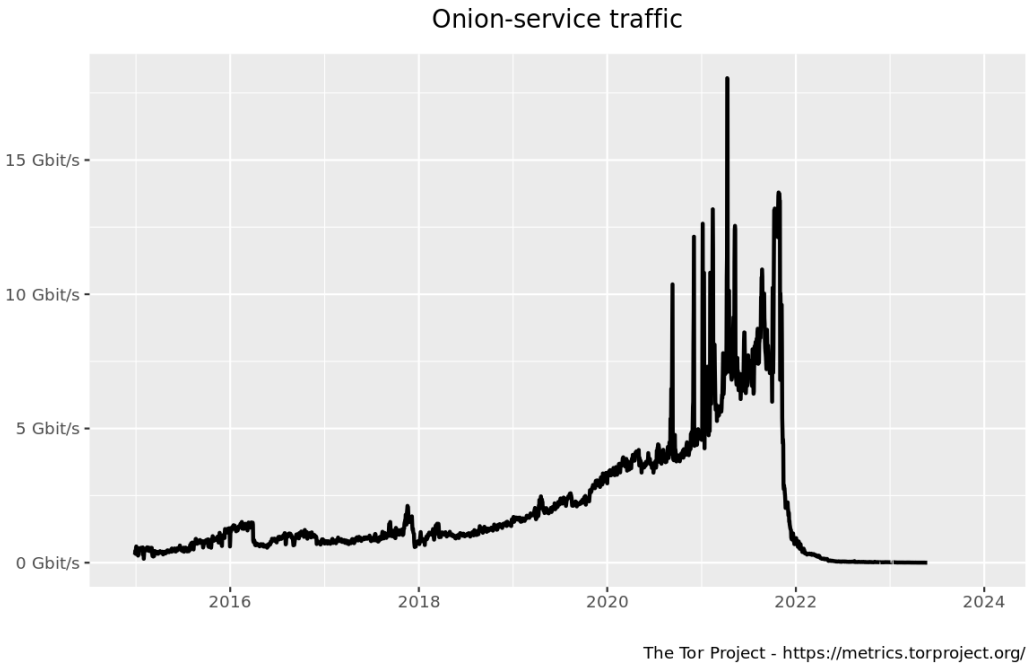
Βήμα 2: Η υπηρεσία onion κατασκευάζει μια περιγραφή, που περιλαμβάνει το δημόσιο κλειδί και μία περίληψη για κάθε IP και, την οποία υπογράφει με το ιδιωτικό της κλειδί [PK (Private key)]. Η περίληψη καταχωρείται σε μία βάση δεδομένων (DB).

Βήμα 3: a)Η Alice ζητάει την διεύθυνση XYZ.onion του Bob. b) κατεβάζει την περιγραφή (που περιέχει τα IP1-3 και PK) και c) Ταυτόχρονα φτιάχνει κύκλωμα με έναν τυχαία επιλεγμένο κόμβο, στον οποίο στέλνει ένα κωδικό μίας χρήσης [OTS (One Time Secret)]. Ο κόμβος αυτός λειτουργεί ως σημείο ραντεβού [RP (Rendezvous Point)].

Βήμα 4: Η Alice στέλνει στον Bob μέσω ενός εκ των IP, ένα κρυπτογραφημένο μήνυμά υπογεγραμμένο με το δημόσιο κλειδί της υπηρεσίας onion του Bob, που περιέχει τη διεύθυνση του RP και το OTS. Σημειώνεται ότι όλη η επικοινωνία λαμβάνει χώρα μέσα στο δίκτυο tor, έτσι η Alice παραμένει ανώνυμη.

Βήμα 5: Ο Bob αποκρυπτογραφεί το μήνυμα της Alice βρίσκοντας έτσι το RP και το OTS. Δημιουργεί κύκλωμα με το RP και του στέλνει το OTS.

Βήμα 6: Το RP ειδοποιεί την Alice ότι έχει επιτευχθεί επιτυχής σύνδεση. Πλέον η Alice μπορεί να επικοινωνήσει και να λάβει πληροφορίες κρυπτογραφημένα με την υπηρεσία onion του Bob μέσω του RP.



Σχήμα 2.3: Κίνηση Υπηρεσιών Onion V2, 2015 - 2023.

2.5 Άδεια χρήσης

Το tor είναι ελεύθερο λογισμικό[9] [10]. Μπορεί να διακινηθεί ελεύθερα και, καθώς ο κώδικάς του είναι διαθέσιμος, μπορεί να μελετηθεί ώστε να εξακριβωθεί η λειτουργία του.

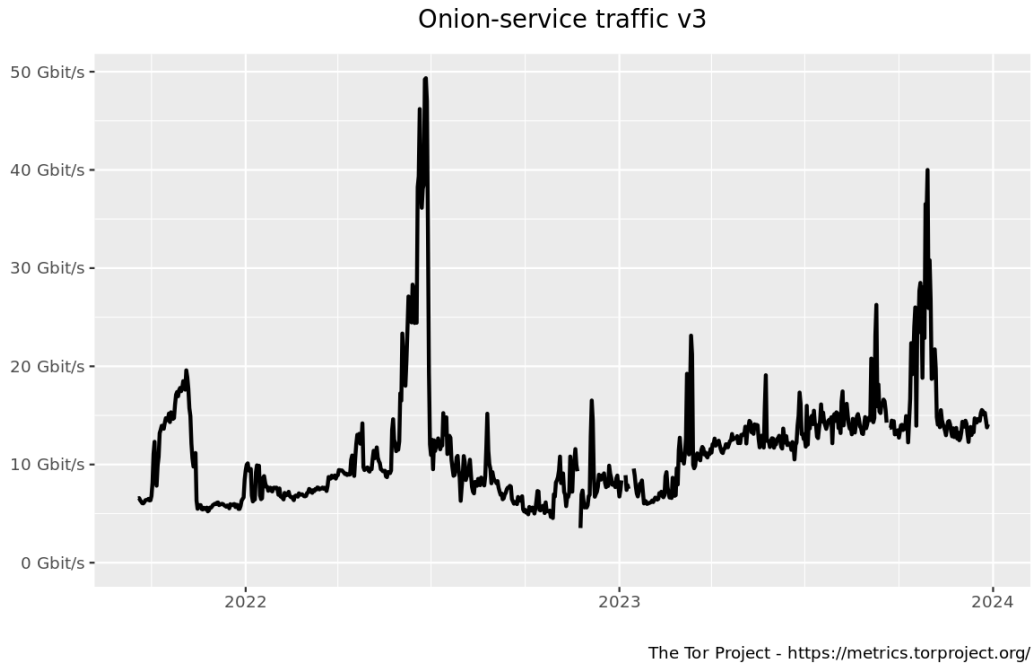
2.6 DDoS επιθέσεις στις υπηρεσίες onion

Το υψηλότερο σημείο στο Σχήμα 2.4 που εμφανίζει ασυνήθιστα υψηλή κίνηση στις υπηρεσίες onion τον Ιούνιο του 2022, οφείλεται σε DDoS επίθεση όπου ένα σημαντικά μεγάλο δίκτυο υπολογιστικών συστημάτων, προωθούσε συντονισμένα αιτήματα σε onion υπηρεσίες, υπερφορτώνοντας έτσι τους πόρους και τις δυνατότητες λειτουργίας του δικτύου tor [3].

2.7 Κενά ασφαλείας

Τα κενά ασφαλείας σχετικά με το δίκτυο tor και τις υπηρεσίες onion αναφέρονται στο TROVE (Tor Registry Of Vulnerabilities and Exposures)[11]. Κατάλογος

[9] https://www.gnu.org/philosophy/free-sw.html
[10] https://support.torproject.org/about/#about_distribute-tor
[11] https://gitlab.torproject.org/tpo/core/team/-/wikis/NetworkTeam/TROVE



Σχήμα 2.4: Κίνηση Υπηρεσιών Onion V3, 2015 - 2023.

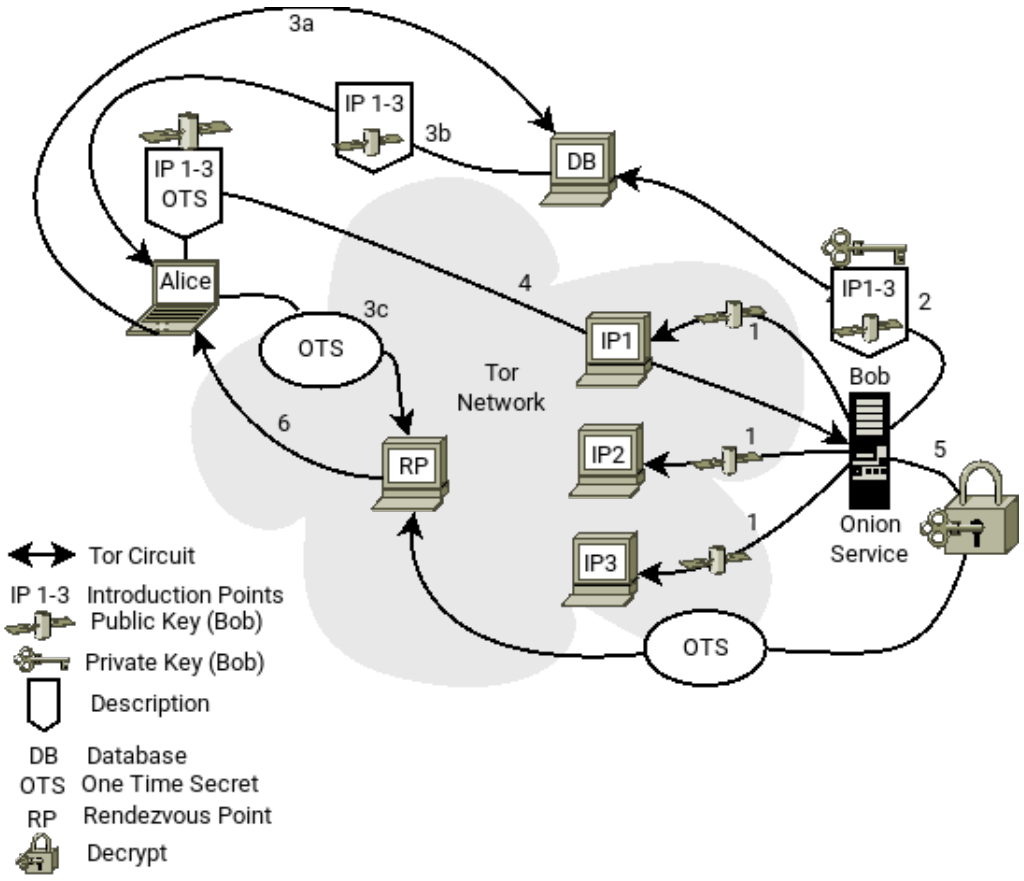
με τα CVE[12] και τη βαθμονόμηση τους κατά CVSS[13] μπορούν να βρεθούν στη σελίδα του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας των ΗΠΑ (NIST)[14].

Σε ότι αφορά τις υπηρεσίες onion, ένα κενό ασφαλείας, μπορεί να οδηγήσει σε μία επιτυχημένη κακόβουλη επίθεση που θα αποανωνυμοποιήσει τον server που παρέχει την υπηρεσία ή τους/τις χρήστ(ρι)ες που τη χρησιμοποιούν.

[12]Συνηθισμένα Ευάλωτα Σημεία και Έκθεση σε Κίνδυνο - Common Vulnerabilities and Exposures». Πρόκειται για μια λίστα καταγραφής των κενών ασφάλειας υπολογιστικών συστημάτων.

[13]Σύστημα Βαθμολόγησης Συνηθισμένης Ευαλωτότητάς - Common Vulnerability Scoring System. Αποτελεί μία μέθοδο καταγραφής των κύριων χαρακτηριστικών μιας ευπάθειας σε κλίμακα που αντικατοπτρίζει τη σοβαρότητά της.

[14]https://nvd.nist.gov/vuln/search



Σχήμα 2.5: Λειτουργία του δικτύου tor

Bibliography

[1] The Tor Project. Special Hostnames in Tor - Tor Specifications. [Online; accessed 26. Dec. 2023].

[2] The Tor Project. What are entry guards? [Online; accessed 25. Dec. 2023].

[3] The Tor Project. Network DDoS | Tor Project status, June 2022. [Online; accessed 30. Dec. 2023].