ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Βιβλιογραφική Έρευνα Ανώνυμων Δικτύων και των Αδυναμιών τους

Διπλωματική Εργασία

Μάριος Κ. Παππάς

Επιβλέπων: Ιωάννης Ψαρράς
Καθηγητής ΕΜΠ

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΤΟΜΕΑΣ ΗΛΕΚΤΡΙΚΩΝ ΒΙΟΜΗΧΑΝΙΚΩΝ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΥΣΤΗΜΑΤΩΝ ΑΠΟΦΑΣΕΩΝ

Βιβλιογραφική Έρευνα Ανώνυμων Δικτύων και των Αδυναμιών τους

Διπλωματική Εργασία

Μάριος Κ. Παππάς

Επιβλέπων: Ιωάννης Ψαρράς
Καθηγητής ΕΜΠ

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 05 Νοεμβρίου 2021

(Υπογραφή)	(Υπογραφή)	(Υπογραφή)
…….	……	……..
Ιωάννης Ψαρράς	Δημήτριος Ασκούνης	Χρυσόστομος Δούκας
Καθηγητής ΕΜΠ	Καθηγητής ΕΜΠ	Αναπληρωτής Καθηγητής ΕΜΠ

Αθήνα, 05 Νοεμβρίου 2021

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάσει επιστημονικής παράφρασης. Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στη Διπλωματική μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων. Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας.

(Υπογραφή)

. . . . . .

Μάριος Κ. Παππάς
Νοέμβριος 2021

Περίληψη

Οι τεχνολογίες ανωνύμων επικοινωνιών αποτελούν σημαντικό πεδίο έρευνας, καθώς η διασφάλιση της ανωνυμίας και της ιδιωτικότητας των χρηστών του διαδικτύου αναδεικνύεται σε μείζον ζήτημα τα τελευταία χρόνια. Ταυτόχρονα, έχουν αναπτυχθεί εξελιγμένα μοντέλα επιθέσεων που στόχο έχουν να πλήξουν την ανωνυμία των χρηστών, προκειμένου κρατικοί οργανισμοί ή και εγκληματικές οργανώσεις να μπορέσουν να αποκτήσουν πρόσβαση σε ευαίσθητα προσωπικά δεδομένα τους. Η παρούσα εργασία μελετά τις τεχνολογίες ανωνύμων επικοινωνιών που έχουν προταθεί για την ικανοποίηση των αναγκών των χρηστών για ανωνυμία, καθώς και τις επιθέσεις που έχουν σχεδιαστεί εναντίον τους.

Λέξεις Κλειδιά

Ανώνυμες Επικοινωνίες, Κυβερνοεπιθέσεις, Ανωνυμία, Κρυπτογραφία, Ανάλυση Διαδικτυακής Κίνησης

Abstract

Anonymous communication technologies have received considerable attention, since anonymity and privacy of internet users has become a major issue in recent years. At the same time, sophisticated attack models have been developed assisting government organizations or criminal groups in gaining access to sensitive information of the Internet users. This paper examines the anonymous communication technologies that have been proposed so far to meet the needs of users for anonymity, as well as the attacks that have been implemented against them.

Key Words

Anonymous Communications, Cyberattacks, Anonymity, Cryptography, Network Traffic Analysis

στην οικογένεια μου

Ευχαριστίες

Θα ήθελα καταρχάς να ευχαριστήσω τον καθηγητή κ. Ιωάννη Ψαρρά για την επίβλεψη αυτής της διπλωματικής εργασίας και για την ευκαιρία που μου έδωσε να την εκπονήσω στο εργαστήριο Συστημάτων Αποφάσεων. Επίσης ευχαριστώ ιδιαίτερα τον Μιχαήλ Κοντούλη για την συνεργασία και την καθοδήγησή του. Τέλος θα ήθελα να ευχαριστήσω την οικογένειά μου που με στήριξε σε όλη αυτή την προσπάθεια.

…….

Μάριος Κ. Παππάς

Περιεχόμενα

Κατάλογος Σχημάτων

Εισαγωγή

Το ερευνητικό πεδίο της παρούσας διπλωματικής εργασίας αφορά τις τεχνολογίες ανωνύμων επικοινωνιών καθώς και τις επιθέσεις που αυτές αντιμετωπίζουν σε Επίπεδο Δικτύου (Network Level). Στην εποχή της πληροφορίας που διανύουμε και με την ευρεία χρήση του διαδικτύου, η δικτυακή υποδομή είναι ζωτικής σημασίας τόσο για την κοινωνική όσο και για την οικονομική ευημερία των πολιτών. Παρ' όλα αυτά, οι χρήστες των υπαρχόντων δικτύων διατρέχουν διάφορους κινδύνους, όπως διαρροή ευαίσθητων προσωπικών στοιχείων και η παραβίαση της ιδιωτικότητας τους. Ήδη από το 1981 αναπτύχθηκαν και προτάθηκαν δίκτυα και τεχνολογίες ανωνύμων επικοινωνιών, έτσι ώστε να αντιμετωπιστούν οι ολοένα αυξανόμενες ανάγκες των χρηστών για ιδιωτικότητα και ανωνυμία κατά τη διάρκεια χρήσης των δικτύων υποδομής. Οι τεχνολογίες αυτές αποτελούν δίκτυα που υλοποιούνται πάνω σε δίκτυα, καθώς χρησιμοποιούν τα ήδη υπάρχοντα δίκτυα υποδομής και τα ενισχύουν με μηχανισμούς που εμποδίζουν την παρακολούθηση της δραστηριότητας των χρηστών από τρίτα μέρη, είτε αυτά είναι κακόβουλοι χρήστες, είτε κρατικοί οργανισμοί, είτε ακόμα και οι διαχειριστές του δικτύου υποδομής. Η ανωνυμία και η ιδιωτικότητα που οι τεχνολογίες αυτές προσφέρουν μπορούν να χρησιμοποιηθούν από απλούς χρήστες για εφαρμογές ανταλλαγής ανώνυμης ηλεκτρονικής αλληλογραφίας και περιήγησης στο διαδίκτυο αλλά και σε ευρεία κλίμακα, από κρατικούς οργανισμούς για τη διεξαγωγή διαδικτυακών ψηφοφοριών, την προστασία στρατιωτικών επικοινωνιών και άλλων ευαίσθητων εφαρμογών.

Η περιοχή των τεχνολογιών ανωνύμων επικοινωνιών έχει συγκεντρώσει μεγάλο ερευνητικό ενδιαφέρον, με πολλά σχήματα να σχεδιάζονται και να προτείνονται για την κάλυψη των αναγκών των χρηστών σε ανωνυμία και ιδιωτικότητα. Ταυτόχρονα όμως, το ενδιαφέρον αυτό έχει αποτελέσει και την αρχή για την ανάπτυξη τεχνικών και μεθόδων που στόχο έχουν να εκμεταλλευτούν τις αδυναμίες των τεχνολογιών αυτών, με απώτερο στόχο να πλήξουν την ανωνυμία των χρηστών τους. Οι επιθέσεις αυτές στις περισσότερες περιπτώσεις δεν προέρχονται από κακόβουλους χρήστες ή εγκληματικές οργανώσεις αλλά από κρατικούς οργανισμούς και υπηρεσίες επιβολής του νόμου που επιθυμούν να περιορίσουν τις δυνατότητες πρόσβασης των χρηστών στο διαδίκτυο (λογοκρίνοντας περιεχόμενο, σε απολυταρχικά καθεστώτα, ή απαγορεύοντας την πρόσβαση σε παράνομο περιεχόμενο στο Darknet) ή ακόμα και να παρακολουθήσουν, σε ατομικό επίπεδο ή και σε ευρεία κλίμακα τη δικτυακή δραστηριότητα των πολιτών. Για το λόγο αυτό έχουν σχεδιαστεί πολλές επιθέσεις, οι οποίες έχουν στόχο να πλήξουν τους μηχανισμούς οι οποίοι προστατεύουν την ανωνυμία των χρηστών. Ορισμένες εξ αυτών είναι πολύ αποτελεσματικές, ενώ είναι και πολύ δύσκολο να αντιμετωπιστούν από τους υπάρχοντες μηχανισμούς ασφαλείας των τεχνολογιών ανωνύμων επικοινωνιών, αποτελώντας σοβαρή απειλή για τους χρήστες τους.

Περιγραφή και Αντικείμενο της Εργασίας

Στόχος της παρούσας διπλωματικής εργασίας είναι η παρουσίαση των τεχνολογιών ανωνύμων επικοινωνιών που έχουν προταθεί, από τα αρχικά Mix Networks όπως αυτά περιγράφηκαν από τον David Chaum, μέχρι και τις σύγχρονες λύσεις που μπορούν να προσφέρουν low-latency ανώνυμες

επικοινωνίες σε ευρεία κλίμακα, όπως το Tor Network, καθώς και η αναλυτική παρουσίαση των επιθέσεων που στοχεύουν τους μηχανισμούς των τεχνολογιών αυτών για την κατάλυση της ανωνυμίας των χρηστών τους. Γίνεται αναλυτική παρουσίαση πολλών σχημάτων ανωνύμων επικοινωνιών προκειμένου ο αναγνώστης να είναι σε θέση να διακρίνει τις διαφορετικές κατηγορίες που υπάρχουν, εστιάζοντας στα πλεονεκτήματα και τις αδυναμίες της κάθε μίας, έτσι ώστε να είναι σε θέση να αναγνωρίσει τις πιθανές λύσεις αναλόγως των αναγκών του. Επιπροσθέτως, γίνεται ανάλυση των κατηγοριών των επιθέσεων που έχουν στόχο αυτές τις τεχνολογίες, προκειμένου ο αναγνώστης να είναι σε θέση να αντιληφθεί εις βάθος τους μηχανισμούς που αυτές χρησιμοποιούν και πώς αυτές μπορούν να επιφέρουν πλήγματα στην ανωνυμία των χρηστών.

Οργάνωση του τόμου

Η εργασία αυτή είναι οργανωμένη σε 4 μέρη.

Στο Μέρος Ι γίνεται μια γενική εισαγωγή στο θέμα των ανωνύμων επικοινωνιών. Γίνεται μια σύντομη ιστορική αναδρομή στις τεχνολογίες ανωνύμων επικοινωνιών, ενώ δίνεται ιδιαίτερο βάρος στα πεδία χρήσης τους, αναφέροντας χαρακτηριστικές περιπτώσεις όπου η διασφάλιση της ανωνυμία των χρηστών είναι επιβεβλημένη. Επίσης, γίνεται σαφής διαχωρισμός των όρων που σχετίζονται με τον σκοπό των τεχνολογιών αυτών, όπως η ανωνυμία, η ιδιωτικότητα, η εμπιστευτικότητα και η κρυπτογραφία.

Στο Μέρος ΙΙ γίνεται μια ενδελεχής παρουσίαση των τεχνολογιών ανωνύμων επικοινωνιών, κατηγοριοποιημένες αναλόγως του πεδίου στόχευσης τους. Έτσι, ο αναγνώστης είναι σε θέση να αντιληφθεί ποιες τεχνολογίες δίνουν έμφαση σε συγκεκριμένες ιδιότητες των χρηστών που επιδιώκουν να διασφαλίσουν, όπως η ανωνυμία ή η δυνατότητα επέκτασης του δικτύου και σε άλλους χρήστες. Η κατηγοριοποίηση αυτή επιλέχθηκε προκειμένου να δοθεί έμφαση στα πλεονεκτήματα και τα μειονεκτήματα των ομάδων αυτών που ορίστηκαν. Στο ίδιο μέρος γίνεται αναλυτική παρουσίαση των πρωτοκόλλων που χρησιμοποιεί κάθε τεχνολογία προκειμένου ο αναγνώστης να κατανοήσει εις βάθος τον τρόπο λειτουργίας τους, ενώ γίνεται ιδιαίτερη αναφορά στο βαθμό υιοθέτησης κάθε τεχνολογίας από τους χρήστες.

Στο Μέρος ΙΙΙ ο αναγνώστης έχει τη δυνατότητα να εντρυφήσει σε όλες τις κατηγορίες επιθέσεων που έχουν στόχο τις τεχνολογίες ανωνύμων επικοινωνιών. Η κατηγοριοποίηση των επιθέσεων αυτών έχει γίνει σε Passive και Active, αναλόγως του μοντέλου του επιτιθέμενου που παρουσιάζεται στην αρχή του κεφαλαίου. Δίνεται αναλυτικά ο γενικός αλγόριθμος υλοποίησης των επιθέσεων αυτών, ενώ παρουσιάζονται και οι πιο ενδιαφέρουσες παραλλαγές τους. Ειδική μνεία γίνεται στον τρόπο υλοποίησης των επιθέσεων αυτών σε ορισμένες πολύ γνωστές τεχνολογίες ανωνύμων επικοινωνιών, προκειμένου ο αναγνώστης να κατανοήσει καλύτερα το πώς εφαρμόζονται στην πράξη οι μηχανισμοί κάθε επίθεσης να δει πραγματικές επιθέσεις ή εξομοιώσεις που έχουν υλοποιηθεί και να αποκτήσει άποψη σχετικά με τους χρόνους υλοποίησης τους και τα ποσοστά επιτυχίας τους, στα συγκεκριμένα σενάρια. Κάθε κεφάλαιο που αναφέρεται σε ένα είδος επίθεσης κλείνει με μια αναφορά στην αποτελεσματικότητα των επιθέσεων αυτών καθώς και σε μέτρα αντιμετώπισης τους, με ιδιαίτερη μνεία στο trade-off μεταξύ ασφάλειας και λειτουργικότητας του δικτύου που πάντα πρέπει να επιτυγχάνεται στις περιπτώσεις αυτές. Το Μέρος ΙΙΙ κλείνει με την ανάλυση των επιθέσεων στο Tor Network, το οποίο αναμφισβήτητα είναι το πιο ευρέως διαδεδομένο δίκτυο ανωνύμων επικοινωνιών παγκοσμίως, συγκεντρώνοντας εκατομμύρια χρήστες. Η κατηγοριοποίηση των επιθέσεων έχει γίνει

πάλι στα πρότυπα του κεφαλαίου, προκειμένου να μπορέσει ο αναγνώστης να συνδέσει το θεωρητικό υπόβαθρό τους με την αντίστοιχη εφαρμογή τους στο case study του Tor Network.

Το Μέρος IV περιλαμβάνει αναφορές στο μέλον των τεχνολογιών που διασφαλίζουν την ανωνυμία των χρηστών τους, καθώς και στα εξελιγμένα μοντέλα επιθέσεων που έχουν αρχίσει να αναπτύσσονται, ιδιαίτερα με τη χρήση τεχνικών όπως το Deep Packet Inspection και Deep Learning Networks.

Μέρος I

Ανωνυμία και Ιδιωτικότητα

Η εξασφάλιση της ιδιωτικότητας των ηλεκτρονικών επικοινωνιών αποτελεί ένα από τα φλέγοντα ζητήματα της τεχνολογίας, ειδικά τα τελευταία χρόνια που ολοένα και μεγαλύτερο μέρος των δραστηριοτήτων, σε εργασιακό, οικονομικό, ακόμα και κοινωνικό επίπεδο, έχουν μεταφερθεί στο ψηφιακό περιβάλλον. Οι χρήστες του διαδικτύου ενδιαφέρονται για την εξασφάλιση του απορρήτου των προσωπικών τους επικοινωνιών και της απόκρυψης ευαίσθητων πληροφοριών τους, ενώ και τα κράτη βρίσκονται σε μια διαρκή αναζήτηση τρόπων για την εξασφάλιση των δικαιωμάτων των χρηστών του διαδικτύου μέσω τροποποίησης των υπαρχόντων νόμων και της επιτήρησης των τεχνολογικών εταιρειών, προκειμένου να βεβαιωθούν ότι οι κανόνες που έχουν επιβληθεί τηρούνται. Ταυτόχρονα, δεν είναι λίγες οι περιπτώσεις όπου εταιρείες κολοσσοί στον χώρο της τεχνολογίας και των επικοινωνιών, βρίσκονται αντιμέτωπες με κατηγορίες και βαριές ποινές λόγω παραβίασης της νομοθεσίας περί ιδιωτικότητας και προσωπικων δεδομένων των χρηστών ή συνδρομητών τους, είτε λόγω εκούσιας αξιοποίησης τους, είτε διότι δεν φρόντισαν να εξασφαλίσουν με κάθε δυνατό τρόπο ότι αυτά δε θα διαρεύσουν.

1.1 Anonymity

Ο όρος ανωνυμία (anonymity) αναφέρεται στην κατάσταση όπου η ταυτότητα και γενικότερα, τα προσωπικά στοιχεία μιας οντότητας, ατόμου ή οργανισμού, είναι άγνωστη. Σημείο κλειδί για τον ορισμό της ανωνυμίας είναι ότι η οντότητα δεν είναι αναγνωρίσιμη, δεν μπορεί να προσεγγιστεί ή δεν μπορεί να εντοπιστεί. [146] [147] Χαρακτηριστικό παράδειγμα ανωνυμίας είναι η περίπτωση ανωνύμων πληροφοριοδοτών ο οποίοι επιθυμούν να κρατήσουν μυστική την ταυτότητα τους, φοβούμενοι τις συνέπειες που μπορούν να έχουν οι αποκαλύψεις τους, σε ηθικό ή επαγγελματικό επίπεδο, ακόμα και σε ζητήματα απειλής της ζωής τους. [150] [153]

Όσον αφορά τις τεχνολογίες ανωνύμων επικοινωνιών που μελετώνται στην παρούσα εργασία, κύριος στόχος τους είναι να διασφαλίσουν ότι ένας παρατηρητής του δικτύου δε θα είναι σε θέση να συνδέσει τα μηνύματα που λαμβάνει ένας χρήστης ή μια υπηρεσία με αυτά που στέλνει ένας αποστολέας. Έτσι, ένας κακόβουλος χρήστης ακόμα και αν γνωρίζει τους συμμετέχοντες ενός

δικτύου, δε μπορεί να γνωρίζει ποιος επικοινωνεί με ποιον. Φυσικά, στόχος των παραπάνω τεχνολογιών παραμένει η αμοιβαία ανωνυμία, η δυνατότητα δηλαδή και των δύο μερών που επικοινωνούν να παραμένουν ανώνυμα. [154]

Ως anonymity set ορίζεται το σύνολο των οντοτήτων οι οποίες φέρουν παραπλήσια χαρακτηριστικά και οι οποίες επιθυμούν να παραμείνουν ανώνυμες κατά τη διάρκεια της επικοινωνίας τους. Το anonymity set μπορεί να μεταβάλλεται με την πάροδο του χρόνου. [150] [152] Τα μέλη του είναι οντότητες οι οποίες μπορούν να δημιουργήσουν ορισμένη κινητικότητα στο δίκτυο, για παράδειγμα να ξεκινήσουν μια συνομιλία ή να συμμετέχουν σε μια συναλλαγή. Επίσης, μέλη του anonymity set είναι και οι οντότητες στις οποίες είναι δυνατό να απευθυνθούν άλλοι χρήστες, όπως για παράδειγμα ορισμένα hidden services.

Βασικός στόχος των κακόβουλων χρηστών είναι να πλήξουν την ανωνυμία των χρηστών, μέσω πληροφοριών που καταφέρνουν να συλλέξουν και συσχετίσεων που υλοποιούν.

1.2 Pseudonymity

Όρος παραπλήσιος με την ανωνυμία είναι η ψευδωνυμία (pseudonymity), διαδικασία κατά την οποία χρησιμοποιούνται ψευδώνυμα προκειμένου οι οντότητες να αποκρύψουν την ταυτότητα τους. Στόχος είναι να συμμετέχουν σε ένα δίκτυο ανωνύμων επικοινωνιών με ένα όνομα που είναι εύκολο να απομνημονευτεί και να χρησιμοποιηθεί, προστατεύοντας την πραγματική τους ταυτότητα. [149]

Τα ψευδώνυμα είναι χαρακτηριστικό των οντοτήτων και χρησιμοποιούνται ως στοιχεία ταυτοποίησης από αυτές, χωρίς να μπορούν όμως να συνδεθούν με την πραγματική ταυτότητα τους. Τα ψευδώνυμα θεωρούνται μοναδικά για κάθε οντότητα, αμετάβλητα στην πάροδο του χρόνου και χωρίς τη δυνατότητα να μεταφερθούν σε άλλες οντότητες. Η έννοια του pseudonymity μπορεί να επεκταθεί και σε anonymity sets, όπου χαρακτηρίζουν ένα σύνολο οντοτήτων, παρέχοντας προστασία της δραστηριότητας που πηγάζει από αυτό. [152]

Ένα πλεονέκτημα του pseudonymity είναι ότι ενώ προστατεύεται η ταυτότητα των οντοτήτων, μπορεί να εφαρμοστεί έλεγχος για τυχόν κακόβουλη συμπεριφορά εκείνων στα πλαίσια μιας τεχνολογίας ανωνύμων επικοινωνιών. Έτσι, μια οντότητα, μέσω του ψευδωνύμου της, μπορεί να ελέγχεται για τη δραστηριότητα της και να παρακολουθείται για τυχόν κακόβουλες ενέργειες στα πλαίσια των κανόνων που ορίζουν τα πρωτόκολλα κάθε τεχνολογίας. [146] [149]

1.3 Privacy

Το απόρρητο, ή αλλιώς ιδιωτικότητα, (privacy) είναι μια ακόμα έννοια που, αν και διαφορετική με την ανωνυμία, διαφέρει από αυτή αν και πολλές φορές υπάρχει αλληλεξάρτηση και διασύνδεση μεταξύ των δύο. Και οι δύο φυσικά καθίστανται όλο και πιο αναγκαίες καθώς οι ενέργειες μας στο διαδίκτυο παρακολουθούνται και καταγράφονται, είτε με τη συναίνεση μας είτε όχι, και αναπόφευκτα σχετίζονται με τις ατομικές μας ελευθερίες ενώ αποτελούν σημαντικό παράγοντα για την ελευθερία όχι μόνο για του ατόμου αλλά και συνολικότερα της κοινωνίας και τη θεμελίωση της δημοκρατίας. Το απόρρητο είναι η ικανότητα να διατηρήσει κάποιος συγκεκριμένες πληροφορίες κρυφές. Οι πληροφορίες αυτές αφορούν πληθώρα δραστηριοτήτων στην καθημερινή μας ζωή. [146] Το απόρρητο καλύπτει για παράδειγμα τις τηλεφωνικές μας συνομιλίες ή την αλληλογραφία, έχει αναγνωριστεί μάλιστα ως θεμελιώδες ανθρώπινο δικαίωμα και σε μία δημοκρατική κοινωνία πρέπει

να προστατεύεται. [147] Η ιδιωτικότητα αφορά το δικαίωμα ενός ατόμου ή μιας ομάδας, να αποφασίζουν από μόνοι τους για το πότε, πώς και μέχρι ποιο σημείο οι πληροφορίες που τους αφορούν θα διαβιβάζονται και θα αξιοποιούνται από άλλους. [150]

1.4 Confidentiality

Ακόμα ένας όρος που σχετίζεται με την ανωνυμία και την ιδιωτικότητα, πολλώ δε μάλλον όσον αφορά το διαδίκτυο, είναι η εμπιστευτικότητα (confidentiality). [146] Η εμπιστευτικότητα αναφέρεται στον περιορισμό πρόσβασης σε συγκεκριμένες πληροφορίες και γενικότερα θέτει περιορισμούς σε συγκεκριμένους τύπους πληροφοριών. Συγκεκριμένα, αφορά την υποχρέωση ενός μέρους να διατηρήσει συγκεκριμένες πληροφορίες ενός άλλου μέρους, ανθρώπου ή οργανισμού, μυστικές. Χαρακτηριστικό παράδειγμα εμπιστευτικότητας είναι η υποχρέωση ενός εργαζόμενου σε μια εταιρεία να μην αποκαλύψει στοιχεία που σχετίζονται με το πελατολόγιο, τις εμπορικές συμφωνίες, τα προϊόντα ή τις υπηρεσίες που παρέχονται και γενικότερα, ευαίσθητες πληροφορίες που πρέπει να μείνουν μυστικές. [147]

1.5 Unobservability

Ο όρος unobservability αναφέρεται στην ιδιότητα μιας οντότητας να έχει πρόσβαση σε κάποιον πόρο του δικτύου χωρίς να έχει τη δυνατότητα ένας επιτιθέμενος να καθορίσει ποιος ακριβώς πόρος χρησιμοποιείται. Ουσιαστικά αναφέρεται στην ιδιότητα όλων των αντικειμένων ενδιαφέροντος, όπως είναι τα πακέτα που διακινούνται μέσω των συστημάτων ανωνύμων επικοινωνιών, να καθίστανται μη διακριτές μεταξύ τους. Αυτό σημαίνει ότι τα μηνύματα που διακινούνται μέσω αυτών δε μπορούν να καταστούν διακριτά από τον απλό θόρυβο που παράγεται στο δίκτυο. [150]

1.6 Unlinkability

Ο όρος unlinkability έχει έννοια παραπλήσια με αυτή του mutual anonymity, καθώς αναφέρεται στην απόκρυψη της σχέσης μεταξύ δύο οντοτήτων που επικοινωνούν, έτσι ώστε ένας κακόβουλος χρήστης να μην είναι σε θέση να τις συσχετίσει μεταξύ τους, μέσω της ανάλυσης της δικτυακής κίνησης στην οποία έχει ή απέκτησε πρόσβαση. Η παραπάνω έννοια μπορεί να χαρακτηριστεί ως absolute unlinkability, στην οποία ένας επιτιθέμενος δεν είναι σε θέση να καθορίσει αν διάφορες δραστηριότητες πηγάζουν από τον ίδιο χρήστη. [151] [152]

Στις τεχνολογίες ανωνύμων επικοινωνιών περισσότερο ενδιαφέρον είναι ο όρος του ”relative unlinkability”, όπου ο επιτιθέμενος, δεν είναι σε θέση να αποκτήσει περισσότερες πληροφορίες για την ταυτότητα και τη δραστηριότητα ενός χρήστη μετά την παρακολούθηση του συστήματος (a-posteriori knowledge), σε σχέση με τις πληροφορίες που διέθετε πριν (a-priori knowledge). Έτσι, οι πιθανότητες να αποκτήσει ο επιτιθέμενος χρήσιμες πληροφορίες δεν αυξάνονται όσο αυξάνεται και ο χρόνος παρατήρησης της κίνησης που παράγει ένα δίκτυο ή μια τεχνολογία ανωνύμων επικοινωνιών. [147]

1.7 Censorship Resistance

Βασική λειτουργία των τεχνολογιών ανωνύμων επικοινωνιών είναι η αποτροπή λογοκρισίας του περιεχομένου από τρίτα μέρη. Τα μέρη αυτά είναι συνήθως κυβερνήσεις που επιβάλλουν περιορισμούς όσονα φορά το περιεχόμενο και τους ιστότοπους στους οποίους έχουν πρόσβαση οι

χρήστες ενός δικτύου. Το περιεχόμενο αυτό μπορεί να είναι νόμιμο, όπως για παράδειγμα η λογοκρισία του Facebook και πολλών άλλων μέσων κοινωνικής δικτύωσης που επέβαλε η κυβέρνηση της Κίνας στους πολίτες της χώρας, ή παράνομο περιεχόμενο, όπως ο διαμοιρασμός περιεχομένου που τελεί υπό προστασία πνευματικής ιδιοκτησίας (πειρατικές ταινίες) ή ακόμα και διακίνησης απαγορευμένων αγαθών, όπως ναρκωτικά και όπλα. [154]

1.8 Cryptography

Η κρυπτογράφηση υπήρξε ένας από τους πρώτους τρόπους για την εξασφάλιση του απαραβίαστου των επικοινωνιών, καθώς μπορεί να αποκρύψει το περιεχόμενο της συνομιλίας δύο οντοτήτων από κακόβουλους χρήστες που προσπαθούν να τις υποκλέψουν. Δεν είναι τυχαίο άλλωστε ότι η κρυπτογραφία χρησιμοποιείται κατά κόρον στα σημερινά συστήματα επικοινωνιών, με πολύ χαρακτηριστικό παράδειγμα το HTTPS, που εξασφαλίζει την ασφάλεια και το απόρρητο των επικοινωνιών στο Internet. Αυτό σε μεγάλο βαθμό, εξασφαλίζει το απόρρητο των επικοινωνιών, δεν εγγυάται ωστόσο την ανωνυμία των χρηστών, είτε από τρίτα, κακόβουλα άτομα, είτε και μεταξύ των ίδιων των συνομιλητών. [2]

Στη σημερινή εποχή, σημαντικός όγκος των πληροφοριών που διακινούνται στο διαδίκτυο αξιοποιούνται από εταιρείες, κρατικές υπηρεσίες και οργανισμούς, ενώ αποτελούν ταυτόχρονα στόχο εγκληματιών που δραστηριοποιούνται στον κυβερνοχώρο (cyber criminals). Καθίσταται λοιπόν επιτακτική ανάγκη η διατήρηση της ανωνυμίας τόσο της ταυτότητας των χρηστών, όσο και των δεδομένων που αυτοί αποστέλλουν ή λαμβάνουν, ενώ επιδιώκεται και η διατήρηση της ανωνυμίας όσον αφορά τις κινήσεις των χρηστών, όπως για παράδειγμα το είδος των ιστοσελίδων που επισκέπτονται. [153]

Χαρακτηριστικό παράδειγμα της ευκολίας εντοπισμού ενός χρήστη και των δραστηριοτήτων του είναι η δυνατοτητα του παρόχου υπηρεσιών Internet να παρακολουθεί αναλυτικά την κίνηση του χρήστη στο διαδίκτυο, ενώ μέσω της IP Address είναι δυνατή η εύρεση της ακριβούς φυσικής τοποθεσίας του χρήστη, καθώς και της ταυτοποίησης του από οποιονδήποτε διαθέτει την πληροφορία αυτή, ακόμα και από κακόβουλους χρήστες. [150] Τη σημερινή εποχή, ο μέσος χρήστης είναι εντελώς εκτεθειμένος όσον αφορά την ανωνυμία του, όχι μόνο σε κρατικούς οργανισμούς ή μυστικές υπηρεσίες, αλλά και σε άλλους χρήστες που έχουν στοιχειώδεις τεχνολογικές γνώσεις και τα κατάλληλα εργαλεία για να αποκαλύψουν την ταυτότητα και τις δραστηριότητες του στόχου τους.

Η έννοια των ανώνυμων επικοινωνιών στο διαδίκτυο εισήχθη ήδη από τις αρχές της δεκαετίας του 1980 με την εισαγωγή των mix networks. Τα mix networks βασίζεται στη χρήση proxy relaying servers και σε χρήση τεχνικών κρυπτογράφησης προκειμένου να διασφαλιστεί η ανωνυμία των χρηστών. [30] Συγκεκριμένα, η κρυπτογράφησης με χρήση δημόσιου κλειδιού (public key) σε κάθε proxy relaying server διασφαλίζει μια συνολικά διαστρωματωμένη κρυπτογράφηση των διακινούμενων μηνυμάτων. Ταυτόχρονα, εισήχθη η έννοια της κρυπτογραφημένης ηλεκτρονικής αλληλογραφίας (anonymous email communication), η οποία υλοποιείται με την κρυπτογράφηση/αποκρυπτογράφηση των μηνυμάτων σε κάθε κόμβο του δικτύου, πριν τα προωθήσουν στον επόμενο προορισμό. Σαν επιπρόσθετο μέτρο αποτροπής παρακολούθησης της κίνησης και της ροής της πληροφορίας, εφαρμόστηκε επίσης η μέθοδος του timing alteration, η οποία

αφορά την σκόπιμη καθυστέρηση διαβίβασης των μηνυμάτων στον επόμενο κόμβο με σκοπό να καταστεί δυσκολότερο το path tracing τους. [46]

Όπως ήδη αναφέρθηκε, οι όροι ανωνυμία και ιδιωτικότητα αναφέρονται σε διαφορετικές εφαρμογές, ωστόσο οι δύο έννοιες αυτές είναι αλληλένδετες. Στην περίπτωση των κινητών ανώνυμω επικοινωνιών επί παραδείγματι, η ανωνυμία εξασφαλίζεται μόνο μέσω της ιδιωτικότητας της τοποθεσίας των δύο μερών που επικοινωνούν. [146] Αυτό πρακτικά σημαίνει ότι για την εξασφάλιση της ανωνυμίας των δύο μερών, οφείλει να ικανοποιείται το κριτήριο της ιδιωτικότητας για την ταυτότητα των δύο μερών, το είδος της συνομιλίας τους, το χρόνο έναρξης και λήξης αυτής και ασφαλώς, της φυσικής τοποθεσίας τους. Η ιδιωτικότητα αυτή θα πρέπει να διασφαλίζεται απέναντι σε κάθε τρίτο μέλος που θα επιχειρήσει να αποκτήσει πρόσβαση στις πληροφορίες αυτές, για οποιονδήποτε σκοπό, νόμιμο ή παράνομο. [31]

Έτσι, μπορούμε να συμπεράνουμε ότι, παρ’ όλο που το περιεχόμενο μιας ηλεκτρονικής επικοινωνίας μπορεί να είναι επαρκώς κρυπτογραφημένο και εξασφαλισμένο από την παραβίαση του από κακόβουλους χρήστες, η ταυτότητα των δύο συνομιλούντων μερών μπορεί να είναι εκτεθειμένη. Ένα χαρακτηριστικό παράδειγμα είναι αυτό της συνομιλίας δύο μερών μέσω ηλεκτρονικής αλληλογραφίας (email). [15] Ενώ το περιεχόμενο της συνομιλίας εξασφαλίζεται, μέσω ισχυρής κρυπτογράφησης, οι χρήστες της υπηρεσίας που συνομιλούν είναι εκτεθειμένοι όσον αφορά τα προσωπικά τους στοιχεία, μπορούν δηλαδή να ταυτοποιηθούν. Ακόμα ένα χαρακτηριστικό παράδειγμα είναι οι ηλεκτρονικές συναλλαγές, ο οποίες πλέον αποτελούν το μεγαλύτερο μέρος των συναλλαγών στην παγκόσμια οικονομία. [36] Αν και η συναλλαγή αυτή καθεαυτή εξασφαλίζεται, η ταυτότητα των συναλλασσομένων μερών δεν είναι σίγουρο ότι τυγχάνει της ίδιας, ισχυρής προστασίας. Γίνεται λοιπόν κατανοητό πώς το πλήθος και, κυρίως, το είδος των προσωπικών πληροφοριών που αποκαλύπτει ο χρήστης, μέσω της χρήσης του διαδικτύου και των ηλεκτρονικών υπηρεσιών γενικότερα, θα πρέπει να είναι αυστηρά προκαθορισμένος. [40]

Ταυτόχρονα, γίνεται αντιληπτό ότι οι εταιρείες που παρέχουν τις υπηρεσίες αυτές στους χρήστες και έχουν πλήρη έλεγχο επί των προσωπικών τους δεδομένων, μπορεί να αξιοποιήσουν τα δεδομένα αυτά, είτε οι ίδιες, είτε σε συνεργασία με άλλες εταιρείες, υπό το πρίσμα μυστικών συμφωνιών συνεργασίας, με σκοπό την εκμετάλλευση των δεδομένων αυτών για τη μεγιστοποίηση του κέρδους τους. Η αποκάλυψη της ταυτότητας ενός χρήστη υπηρεσιών κινητής τηλεφωνίας επί παραδείγματι, μπορεί να οδηγήσει στον ακριβή εντοπισμό του, καθώς εξ ορισμού, για λόγους λειτουργικότητας, τα δίκτυα κινητών επικοινωνιών πρέπει να παρακολουθούν την τοποθεσία των τερματικών κινούμενων σταθμών, για την παροχή των υπηρεσιών τους. [147] Έτσι, με απλή και εύκολα υλοποιήσιμη ανάλυση της δικτυακής κίνησης, μπορεί να αποκαλυφθεί η ταυτότητα των δύο συνομιλούντων μερών. Τέτοιες πρακτικές χρησιμοποιούνται για την εξασφάλιση της δημόσιας τάξης και την πάταξη της εγκληματικότητας από τις αστυνομικές αρχές, μετά από έγκριση της αρμόδιας εισαγγελίας. [150] Η υλοποίηση τους ωστόσο μπορεί να γίνει μόνο με πρόσβαση στη δικτυακή κίνηση, στην οποία έχουν de facto πρόσβαση οι εταιρείες κινητής τηλεφωνίας, οι οποίες μπορούν να προβούν σε αξιοποίηση τους ανά πάσα στιγμή, χωρίς να είναι δυνατό να τους ελέγξει κάποιος ή να γίνουν αντιληπτοί από τους χρήστες. [7]

Σκοπός των ανωνύμων επικοινωνιών λοιπόν είναι όχι μόνο να παρέχουν προστασία των στοιχείων που μπορούν να ταυτοποιήσουν έναν χρήστη, αλλά και να είναι ιδιαίτερα ανθεκτικές έναντι σε μεθόδους ανάλυσης δικτυακής κίνησης, έτσι ώστε να καθίσταται δυσχερής η ανάλυση πληροφοριών μέσω πρακτικών όπως η ανάλυση των επικεφαλίδων των πακέτων. [130]

Τέλος, ένας γενικός ορισμός των ανώνυμων επικοινωνιών δόθηκε από τους Gruteser and Grunwald, με τον ορισμό του K-anonymity. Σύμφωνα με το προαναφερθέν θεώρημα, προκειμένου να διασφαλίζεται η ανωνυμία ενός δικτύου επικοινωνιών, ο K-χρήστης (user) του δικτύου αυτού δε θα πρέπει να είναι διαχωρίσιμος από τουλάχιστον (K-1)-χρήστες του ίδιου δικτύου, όταν K>> (K αρκούντως μεγάλος αριθμός, προϋπόθεση η οποία καλύπτεται εκ των πραγμάτων στα σύγχρονα δίκτυα επικοινωνιών). [2] Το Θεώρημα του K-anonymity βασίζεται στην ντετερμινιστική ανωνυμία (deterministic anonymity), ενώ αργότερα εισήχθη και η έννοια της πιθανοτικής ανωνυμίας (probabilistic anonymity), χαρακτηριστικό παράδειγμα της οποίας είναι το Stop-and-Go-MIX (SG-MIX) Protocol. [16] Η βασική διαφορά των deterministic και probabilistic μοντέλως έγκειται στο ότι στο δεύτερο, δεν απαιτείται η ταυτοποίηση ενός χρήστη για τη συμμετοχή του σε ένα ανώνυμο δίκτυο επικοινωνιών, ενώ η ανωνυμία εξασφαλίζεται μέσω μιας publicly known παραμέτρου ασφαλείας που καθορίζει την ασφάλεια του πρωτοκόλλου. [20]

Μέρος ΙΙ

Τεχνολογίες Ανωνύμων Επικοινωνιών

Ο πρώτος που δημιούργησε μια αρχιτεκτονική ενός συστήματος που εξασφαλίζει την ανωνυμία των επικοινωνιών ήταν Chaum το 1981 και αφορούσε την ανώνυμη, μη ανιχνεύσιμη αποστολή mails μέσω μιας αλληλουχίας proxies. Η τεχνική που προτάθηκε από τον Chaum έγινε γνωστή ως Onion Routing και όλες οι υπόλοιπες τεχνολογίες ανωνύμων επικοινωνιών βασίστηκαν πάνω σε αυτή την αρχιτεκτονική.

Ενώ η διασφάλιση της ανωνυμίας των χρηστών είναι ο βασικός λόγος χρήσης των τεχνολογιών αυτών, υπάρχουν και άλλοι λόγοι για τους οποίους σήμερα υπάρχει ευρεία χρήση τους. Πολλοί χρήστες επιθυμούν να αποφύγουν τη λογοκρισία περιεχομένου και την απαγόρευση πρόσβασης σε συγκεκριμένους ιστότοπους, περιορισμοί που επιβάλλονται από απολυταρχικά καθεστώτα. Ολοένα και περισσότεροι χρήστες σήμερα χρησιμοποιούν αυτού του είδους τις τεχνολογίες προκειμένου να αποφύγουν την παρακολούθηση και την εξόρυξη των δεδομένων της δικτυακής τους δραστηριότητας, τα οποία πωλούνται χωρίς την έγκριση τους για διαφημιστικούς και όχι μόνο λόγους. Τέλος, υπάρχει ακόμα μια σημαντική χρήση των δικτυων ανωνύμων επικοινωνιών, αυτή για παράνομες δραστηριότητες.

Ένας διαχωρισμός όσον αφορά τις τεχνολογίες ανωνύμων επικοινωνιών είναι αυτές σε low latency και high latency. Η χρήση των πρώτων είναι ευρέως διαδεδομένη, καθώς οι σύγχρονες δικτυακές εφαρμογές απαιτούν άμεση επικοινωνία του χρήστη με το εκάστοτε web service που χρησιμοποιεί. Παραδείγματα low latency ανώνυμων τεχνολογιών είναι το Tor και το I2P. Αντιθέτως, στα high latency δίκτυα, ένα μήνυμα, όπως για παράδειγμα ένα mail μπορεί να παρουσιάσει ακόμα και καθυστέρηση ημερών έως ότου φτάσει στον τελικό προορισμό του.

Ένας ακόμα διαχωρισμός, που είναι και πολύ πιο ουσιαστικός είναι αυτός που αφορά την αρχιτεκτονικη των συστημάτων ανωνύμων επικοινωνιών. Το πιο σύνηθες μοντέλο που συναντάται είναι αυτό του Peer-to-Peer μοντέλου, στα οποία δεν υπάρχει ουσιαστικός διαχωρισμός μεταξύ των clients και servers στο δίκτυο, δυσκολεύοντας ακόμα περισσότερο τη διάκριση ενός κόμβου σε αποστολέα ή λήπτη ενός μηνύματος. Στην περίπτωση αυτή όλοι οι κόμβοι έχουν διττό ρόλο, τόσο αποστολέα όσο και παραλήπτη μηνυμάτων, αποτελώντας ομότιμες οντότητες (peers) του δικτύου. Αντίθετα, στα συστήματα ανωνύμων επικοινωνιών που βασίζονται στο client-server μοντέλο υπάρχει περιορισμένος αριθμός κόμβων των οποίων ο ρόλος είναι να παρέχουν ανωνυμία στους υπόλοιπους χρήστες.

2.1 Low-Latency Τεχνολογίες

Η κατηγορία αυτή περιλαμβάνει τεχνολογίες οι οποίες διασφαλίζουν την ανωνυμία των χρηστών του δικτύου, έχοντας ικανοποιητικές επιδόσεις όσον αφορά το παρατηρούμενο latency, με στόχο να είναι σε θέση να ικανοποιήσουν σύγχρονες, απαιτητικές δικτυακές εφαρμογές. Οι τεχνολογίες αυτές, ειδικότερα το Tor Network είναι και αυτές με τη μεγαλύτερη χρήση, καθώς οι σύγχρονες διαδραστικές εφαρμογές απαιτούν low-latency στο δίκτυο.

Παρουσιάζουν ανθεκτικότητα απέναντι σε Timing Attacks με την προϋπόθεση ότι δεν υπάρχει κάποιος global adversary που να στοχεύει στην κατάργηση της ανωνυμίας των χρηστών του δικτύου. Τα δίκτυα αυτά μπορούν να είναι τόσο client-server όσο και peer-to-peer. Η πρώτη κατηγορία παρέχει μεν καλύτερη διαθεσιμότητα, καθώς τα αιτήματα των χρηστών εξυπηρετούνται από servers και δεν εξαρτώνται από τη διαθεσιμότητα των peers του δικτύου, ωστόσο παρουσιάζουν σημαντικά προβλήματα επεκτασιμότητας, με αποτέλεσμα να μπορούν να εξυπηρετήσουν περιορισμένοα ριθμό χρηστών.

2.1.1 Onion Routing/Tor

Συνοπτική περιγραφή κάθε κατηγορίας με πληροφορίες σχετικά με τα προβλήματα και τις αδυναμίες που αυτές αντιμετωπίζουν.

***Keywords:* Client-Server, Onion Routing, Consensus**

***Maturity*: Common**

Το Onion Routing είναι ο πιο διαδεδομένος τρόπος ανώνυμων επικοινωνιών. Αναπτύχθηκε στα μέσα της δεκαετίας του 1990 από το US Naval Research Laboratory από τους Paul Syverson, Michael G. Reed και David Goldschlag. Στόχος του onion Routing) ήταν η εξασφάλιση των απόρρητων επικοινωνιών του Αμερικανικού Ναυτικού. Αναπτύχθηκε περαιτέρω από το Defense Advanced Research Projects Agency (DARPA) και κατοχυρώθηκε με δίπλωμα ευρεσιτεχνίας από το Αμερικανικό Ναυτικό το 1998. [81]

Το Tor έγινε διαθέσιμο στο ευρύτερο κοινό όταν οι ερευνητές δημοσίευσαν άρθρο στο IEEE Journal of Communications το ίδιο έτος. Στη δημοσίευση αυτή παρουσιάστηκαν αναλυτικά οι μέθοδοι για την προστασία της ανωνυμίας του χρήστη από το δίκτυο καθώς και από εξωτερικούς παρατηρητές που παρακολουθούν την κίνηση καθως και από τους διαχειριστές του δικτύου που υλοποιούν ανάλυση κυκλοφορίας σε αυτό. Κομβικό μέρος αυτής της δημοσίευσης είναι οι παραμετροποιήσεις των εφαρμογών onion routing στις υπάρχουσες ηλεκτρονικές υπηρεσίες, όπως εικονικό ιδιωτικό δίκτυο (VPN), περιήγηση στο Web, email, και απομακρυσμένη σύνδεση (remote login).

Οι Roger Dingledine and Nick Mathewson συνέχισαν την έρευνα πάνω στην τεχνολογία του onion routing και σε συνεργασία με τον Paul Syverson δημιούργησαν το 2002 την ευρέως γνωστή και χρησιμοποιούμενη έως σήμερα εφαρμογή onion routing που ονομάζεται Tor (The Onion Routing) Anonymity Network Project. Εν συνεχεία, το US Naval Research Laboratory διέθεσε τον κώδικα υλοποίησης του Tor με free license, και το 2006 ιδρύθηκε το The Tor Project, έναν μη κερδοσκοπικό οργανισμό υπό την αιγίδα του Electronic Frontier Foundation και διαφόρων άλλων οργανισμών, προκειμένου να στηριχθεί το εγχείρημα και να είναι διαθέσιμο στο ευρύ κοινό. [8]

Επί της αρχής, το onion routing παρέχει αμφίδρομη, σχεδόν πραγματικού χρόνου επικοινωνία στους χρήστες του, παρόμοια με αυτή του TCP/IP. [10] [17] Οι ανώνυμες συνδέσεις μπορούν σε μεγάλο βαθμό να αντικαταστήσουν τα sockets για μια πληθώρα διαδικτυακών εφαρμογών, με τη χρήση proxies. Οι χρησιμοποιούμενοι proxy servers μπορούν επίσης να αφαιρέσουν πληροφορίες που μπορούν να συμβάλλουν στην ταυτοποίηση των χρηστών, ώστε να διασφαλιστεί η ανωνυμία τους. Οι συνδέσεις είναι ανεξάρτητες των διαδικτυακών εφαρμογών που υποστηρίζουν, με αποτέλεσμα το onion routing να μπορεί να υποστηρίξει επιτυχώς ένα εύρος εφαρμογών, όπως mail και web browsing. [8]

Η χρήση του onion routing, ειδικότερα του Tor που ήταν και η υλοποίηση του για το ευρύ κοινό, παρ όλο που έχει συνδυαστεί στη συνείδηση αρκετών με την επίτευξη ανωνυμίας των χρηστών, προκειμένου να αποκτήσουν πρόσβαση σε παράνομο περιεχόμενο, μέσω του Darkweb, μπορεί να παρέχει ανωνυμία στους χρήστες και για την πρόσβαση σε δημόσιες, καθόλα νόμιμες ιστοσελίδες. Ένας χρήστης επί παραδείγματι, χρησιμοποιεί το onion routing προκειμένου να προστατεύσει την ταυτότητα του σε δημόσιους ιστότοπους, όπως το google.com. Για την επίτευξη της ανωτέρω ζητούμενης ανωνυμίας, θα πρέπει να αφαιρεθούν τόσο πληροφορίες που υπάρχουν στα web requests και μπορούν να οδηγήσουν στην ταυτοποίηση του χρήστη, όσο και πληροφορίες από την ίδια τη σύνδεση. [8] Η βασική διαφορά με τη μέθοδο των Anonymizers είναι ότι στο onion routing υπάρχει ανώνυμη περιήγηση στο διαδίκτυο πάνω από ανώνυμες συνδέσεις, σε αντίθεση με τον πρώτο τρόπο όπου έχουμε anonymization του datastream που διακινείται. Στην περίπτωση των anonymizers λοιπόν είναι δυνατή η ταυτοποίηση των συνομιλούντων μερών μέσω παρακολούθησης του anonymized data stream καθώς ταξιδεύει στο υπό παρακολούθηση δίκτυο επικοινωνιών, ενώ στο onion routing αυτό προστατεύεται και αποτρέπεται.

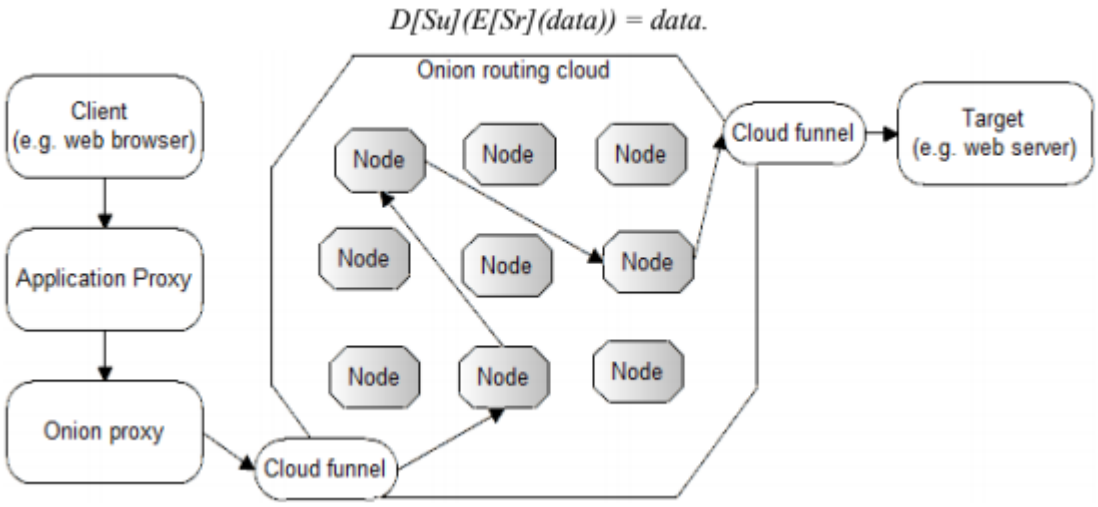
Η λειτουργία του Onion Routing εστιάζει στην παροχή ανωνύμων συνδέσεων οι οποίες παρουσιάζουν σημαντική ανθεκτικότητα έναντι προσπαθειών υποκλοπής και ανάλυσης δικτυακής κίνησης. Η διαδικασία ξεκινάει με τη σύνδεση της εφαρμογής του client με έναν application proxy (SOCKS). Σχετιζόμενες με το πρωτόκολλο συνδέσεις γίνονται αποδεκτές και μετατρέπονται σε generic πρωτόκολλο. Εν συνεχεία το πακέτο προωθείται σε onion proxy με αποτέλεσμα να δημιουργηθεί μια συγκεκριμένη δομή δεδομένων, η οποία παρουσιάζεται αναλυτικά πιο κάτω, και ονομάζεται onion. Το onion κρυπτογραφείται σε πολλαπλά επίπεδα και στη συνέχεια στέλνεται σε μια διοχέτευση εισόδου (entry funnel). [8]

Με αυτό τον τρόπο, πολλαπλώς κρυπτογραφημένα μηνύματα προωθούνται σε μια τυχαία, αδύνατο να προκαθοριστεί, διαδρομή η οποία αποτελείται από διαδοχικούς κόμβους που αποκαλούνται onion routers, οι οποίοι επικοινωνούν μεταξύ τους χρησιμοποιώντας TCP tunnels. Η κίνηση είναι αμφίδρομη, με επιδίωξη της ελάχιστης δυνατής καθυστέρησης. Το κλειδί στη συγκεκριμένη διαδικασία είναι ότι κάθε ενδιάμεσος κόμβος αφαιρεί ένα στρώμα κρυπτογράφησης πριν προωθηθεί

στον επόμενο, με αποτέλεσμα να καθίσταται αδύνατο για τους ενδιάμεσους κόμβους να γνωρίζουν την πραγματική προέλευση ή προορισμό των μηνυμάτων που διαβιβάζουν. Το Onion Routing παρέχει ανώνυμη σε πραγματικό χρόνο σύνδεση εικονικής υποδοχής (virtual socket) μέσω proxy server. Η αρχιτεκτονική αυτή μπορεί να χρησιμοποιηθεί από αρκετές εφαρμογές λόγω της δυνατότητας αυτών να λειτουργούν μέσω proxy servers. [15]

Κάθε ενδιάμεσος κόμβος μπορεί να οριστεί από τον Αριθμό Κόμβου S=1...N, ένα δημόσιο κλειδί (public key) Su, ένα ιδιωτικό κλειδί (private key) Sr, μια συνάρτηση κρυπτογράφησης (encryption function) E [key](data) και μια συνάρτηση αποκρυπτογράφησης (decryption function) D[key](data). Όπως είναι γνωστό από τις γενικές αρχές της κρυπτογραφίας, δεδομένα που κρυπτογραφούνται με το δημόσιο κλειδί μπορούν να αποκρυπτογραφηθούν με το δημόσιο κλειδί και το αντίστροφο. [44]

Η τυχαία διαδρομή καθορίζεται από τον proxy server. Ο πρώτος κόμβος αποτελεί το entry funnel και ο τελευταίος το exit funnel. Στο παρακάτω απλό παράδειγμα, αναλύεται ο τρόπος λειτουργίας του onion routing μέσω του οποίου επιτυγχάνεται η ανωνυμία. [10]



Σχήμα 2.1: Onion Routing Cloud.

Υποθέτοντας ότι η τυχαία διαδρομή που καθορίστηκε από τον onion proxy είναι η διαφαινόμενη, με router numbers {4,3,5}. Το data packet που εισέρχεται στο entry funnel μέσω του onion proxy θα έχει την ακόλουθη δομή:

E[4u](3's IP address, E[3u](5' s IP address, E[5u](data)))

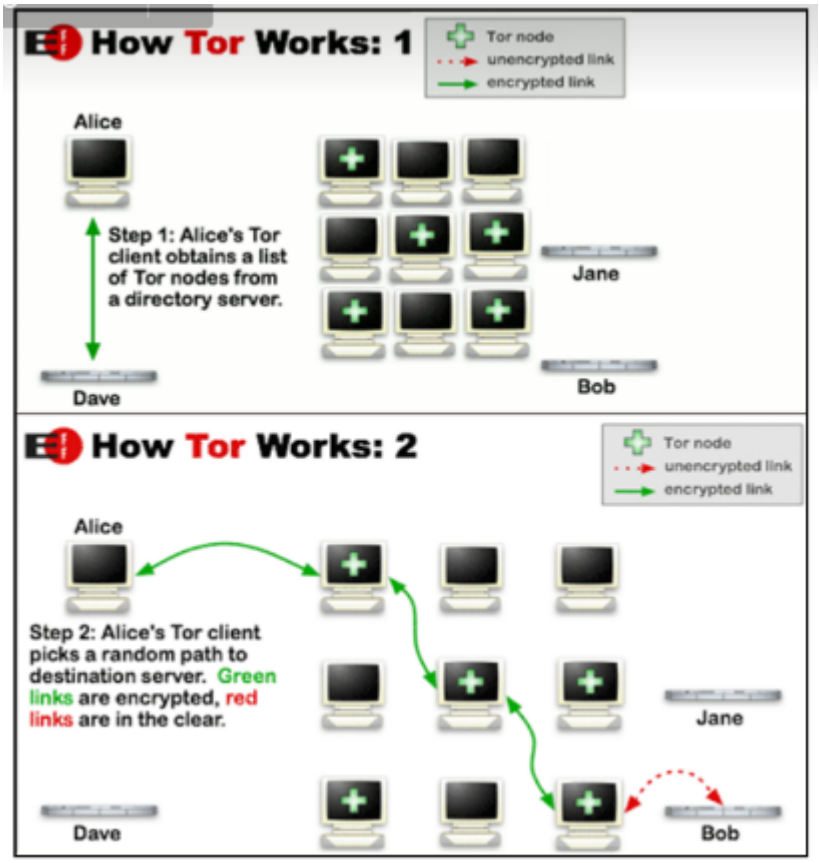
Ο Router 4 αποκρυπτογραφεί με το ιδιωτικό του κλειδί το onion packet, αφαιρώντας το πρώτο encryption layer, με αποτέλεσμα να αποκαλυφθεί η IP Address του επόμενου κατά σειρά Router, σύμφωνα πάντα με τη αλληλουχία που καθορίστηκε από τον onion proxy, ο οποίος στο παράδειγμα μας είναι ο Router 3. Η διαδικασία αυτή συνεχίζεται, καθώς εγκαθίσταται εικονικό κύκλωμα (virtual circuit) προς το exit funnel. Με αυτό τον τρόπο, το virtual circuit δε χρειάζεται να περιλαμβάνει πληροφορία δρομολόγησης, επιτυγχάνοντας την ανωνυμία της επικοινωνίας. Όταν ένα response message εισέρχεται στο exit funnel τότε τα δεδομένα κρυπτογραφούνται με το ιδιωτικό κλειδί του funnel. [8] Η διαδικασία αυτή επαναλαμβάνεται έως ότου το μήνυμα διανύσει ολόκληρη τη διαδρομή

του εικονικού κυκλώματος έως ότου τα δεδομένα φτάσουν στον onion proxy όπου γίνεται ανάκτηση του μηνύματος υπό την ακόλουθη μορφή.

D[4u](D[3u](D[5u](encrypted onion))

Χρησιμοποιώντας κρυπτογραφία ασύμμετρου κλειδιού, ο δημιουργός του μηνύματος λαμβάνει ένα δημόσιο κλειδί από τον κόμβο καταλόγου για να στείλει ένα κρυπτογραφημένο μήνυμα στον πρώτο κόμβο ("είσοδος"), δημιουργώντας μια σύνδεση και ένα κοινό μυστικό ("κλειδί περιόδου λειτουργίας"). Χρησιμοποιώντας τον δημιουργηθέντα κρυπτογραφημένο σύνδεσμο προς τον κόμβο εισόδου, ο δημιουργός μπορεί να μεταδώσει ένα μήνυμα μέσω του πρώτου κόμβου σε έναν δεύτερο κόμβο στην αλυσίδα χρησιμοποιώντας κρυπτογράφηση που μόνο ο δεύτερος κόμβος και όχι ο πρώτος μπορεί να αποκρυπτογραφήσει. Όταν ο δεύτερος κόμβος λάβει το μήνυμα, δημιουργεί μια σύνδεση με τον πρώτο κόμβο. Ενώ αυτό επεκτείνει τον κρυπτογραφημένο σύνδεσμο από τον δημιουργό, ο δεύτερος κόμβος δεν μπορεί να προσδιορίσει εάν ο πρώτος κόμβος είναι ο δημιουργός ή απλά ένας άλλος κόμβος στο κύκλωμα. Ο δημιουργός μπορεί στη συνέχεια να στείλει ένα μήνυμα μέσω του πρώτου και του δεύτερου κόμβου σε έναν τρίτο κόμβο, κρυπτογραφημένο έτσι ώστε μόνο ο τρίτος κόμβος να μπορεί να το αποκρυπτογραφήσει. Το τρίτο, όπως και με το δεύτερο, συνδέεται με τον δημιουργό αλλά συνδέεται μόνο με το δεύτερο. Αυτή η διαδικασία μπορεί να επαναληφθεί για τη δημιουργία μεγαλύτερων και μεγαλύτερων αλυσίδων, αλλά περιορίζεται συνήθως στη διατήρηση της απόδοσης. [25]

Όταν ολοκληρωθεί η δημιουργία της αλυσίδας που εξασφαλίζει την ανώνυμη επικοινωνία, ο δημιουργός μπορεί να στείλει δεδομένα μέσω του διαδικτύου χωρίς να είναι δυνατή η αποκάλυψη ταυτότητας του αποστολέα. Όταν ο τελικός παραλήπτης των δεδομένων στέλνει δεδομένα πίσω, οι ενδιάμεσοι κόμβοι διατηρούν τον ίδιο σύνδεσμο πίσω στον αρχικό δημιουργό, με τα δεδομένα να επιστρώνονται ξανά, αλλά αντίστροφα έτσι ώστε ο τελικός κόμβος να αφαιρεί το πρώτο στρώμα κρυπτογράφησης και ο πρώτος κόμβος να αφαιρεί τελευταίο επίπεδο κρυπτογράφησης πριν από την αποστολή των δεδομένων, για παράδειγμα μια ιστοσελίδα, στον δημιουργό. Με αυτό τον τρόπο εξασφαλίζεται η ανωνυμία και των δύο συμβαλλομένων στην επικοινωνία μερών. [81]

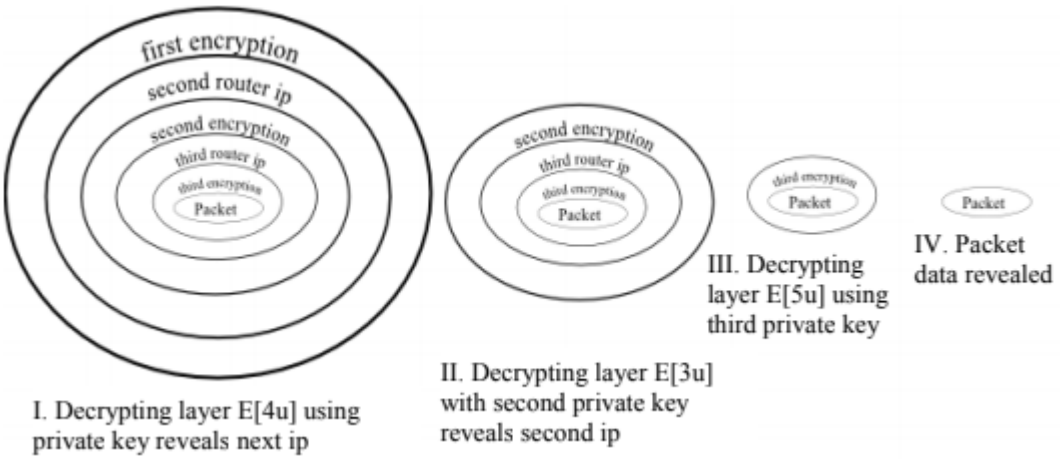


Σχήμα 2.2: The Tor Network.

Μήνυμα που στέλνεται μέσω της onion routing αρχιτεκτονικής περιέχει υποχρεωτικά το αναγνωριστικό του virtual circuit, τα δεδομένα που αποτελούν το μήνυμα καθώς και μια εντολή (create, destroy, data). Το onion προκύπτει από το πεδίο των δεδομένων. Οι εντολές χρησιμοποιούνται για τον αμέσως επόμενο κόμβο του εικονικού δικτύου, προκειμένου εκείνος να γνωρίζει τι να υλοποιήσει μόλις λάβει το μήνυμα. Αν σε κόμβο φτάσει η εντολή create μαζί με το onion, τότε δημιουργείται ακόμα μια εντολή create η οποία προωθείται στον επόμενο κόμβο μαζί με το onion και το virtual circuit identifier. [8] Αντίθετα, σε περίπτωση που λάβει κάποιος κόμβος την εντολή destroy ή data τότε στέλνει πίσω προς το virtual circuit μια εντολή destroy. Η εντολή data έχει στόχο να ειδοποιήσει τον αρχικό κόμβο να στείλει μια ροή δεδομένων προς το συγκεκριμένο virtual circuit, μαζί με άλλες πληροφορίες ελέγχου.

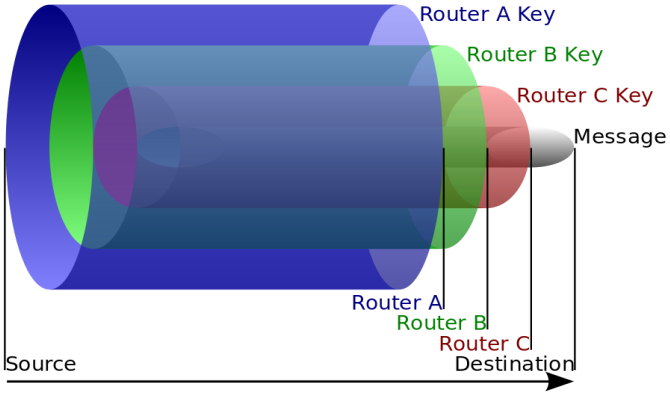
Η επιλογή του virtual circuit που αλλιώς αποκαλείται chain ή πιο απλά path, γίνεται από έναν κατάλογο κόμβων, οι οποίοι εκ των προτέρων είναι γνωστό ότι συμμετέχουν στο Tor project. Η διατήρηση της ανωνυμίας εξασφαλίζεται από το γεγονός ότι, μέσω της παραπάνω διαδικασίας, κάθε κόμβος είναι αδύνατο να καταλάβει αν ο προηγούμενος από αυτόν κόμβος στο path είναι η πηγή πληροφορίας ή ένας απλός ενδιάμεσος κόμβος, σαν τον ίδιο. Επιπλέον, κανένας κόμβος δεν είναι δυνατό να καθορίσει πόσοι επιπλέον κόμβοι βρίσκονται στη συνέχεια του path, παρά μόνο ο τελικός κόμβος. [57]

Ο τρόπος διαδοχικής κρυπτογράφησης σε κάθε κόμβο της αλυσίδας θυμίζει κρεμμύδι, λόγω των διαδοχικών στρώσεων, εξού και το όνομα του πρωτοκόλλου. Στο παρακάτω σχήμα παρουσιάζεται παραστατικά η διαδοχική αφαίρεση κρυπτογραφικών στρωμάτων, στη διαδρομή από τον αποστολέα στον παραλήπτη, προκειμένου να διασφαλιστεί η ανωνυμία.



Σχήμα 2.3: Διαστρωματωμένη Αποκρυπτογράφηση.

Επιπλέον, φαίνεται στο παρακάτω σχήμα η διαδοχική χρήση των δημοσίων και ιδιωτικών κλειδιών σε κάθε Router από την πηγή προς τον προορισμό. Μπορούμε να δούμε λοιπόν ότι υπάρχει ενθυλάκωση των δεδομένων του μηνύματος σε διαδοχικά στρώματα κρυπτογράφησης.



Σχήμα 2.4: Χρήση διαδοχικών Keys στο Onion Routing.

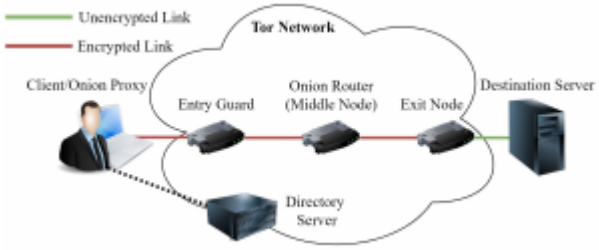
Όπως γνωρίζουμε, το Tor Network, που ονομάζεται και 2G Onion Routing, αποτελεί τη συνέχεια του Onion Routing. Εκτός από τη διασφάλιση της ανωνυμίας των χρηστών του, όπως έχουμε ήδη περιγράψει, χρησιμοποιείται πολύ συχνά για την πρόσβαση σε υπηρεσίες και περιεχόμενο που λογοκρίνεται από τις αρχές/κυβερνήσεις. Μια ακόμα πολύ συνηθισμένη λειτουργία του όμως περιλαμβάνει τη δημιουργία και υποστήριξη Hidden Services, τα οποία παρέχουν πρόσβαση σε περιεχόμενο που δεν καταχωρείται δημοσίως στο Internet (συνήθως παράνομο περιεχόμενο). Η λειτουργία του Tor Network βασίζεται στα εξής βασικά μέρη:

- Onion Proxy (Tor Client), το οποίο είναι ένα μικρό κομμάτι software που ο χρήστης πρέπει να εγκαταστήσει στο τερματικό του προκειμένου να συμμετέχει στο Tor Network. Είναι υπεύθυνο για την επικοινωνία με τα Directory Servers (Εξυπηρετητές Ευρετηρίου) μέσω των οποίων εγκαθίστανται οι συνδέσεις στο ανώνυμο δίκτυο. Μια άλλη λειτουργία του Onion Proxy είναι η διαχείριση των συνδέσεων του χρήστη με διάφορες εφαρμογές. [8]

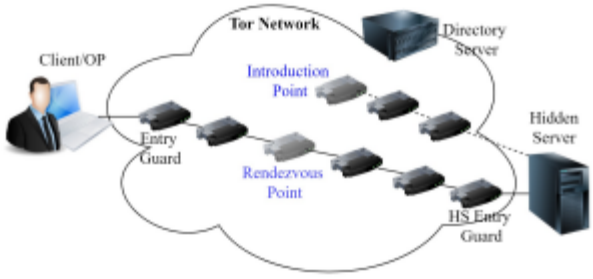
- Directory Servers, οι οποίοι είναι μερικοί λίγοι σε αριθμό, αξιόπιστοι servers οι οποίοι περιέχουν πληροφορίες και λειτουργίες για το σύνολο του ανώνυμου δικτύου. Όλοι οι Directory Servers δημιουργούν ένα consensus document το οποίο περιέχει την κατάσταση του δικτύου, των κόμβων, του bandwidth, των πολιτικών εισόδου και εξόδου κόμβων και άλλες παρόμοιες πληροφορίες. Οι Tor Clients λαμβάνουν το consensus document από κάποιον Directory Server ώστε να συμμετέχουν στο δίκτυο και να καθορίσουν το επιθυμητό μονοπάτι ανώνυμης δρομολόγησης. [8] [35]
- Entry Node/Guard, είναι ο relay που έχει άμεση σύνδεση με τον Tor Client και κατά συνέπεια γνωρίζει την πλήρη ταυτότητα του. Ο Entry Node αλλάζει συχνά, καθώς σχηματίζονται νέα μονοπάτια στο δίκτυο, με αποτέλεσμα να αποτελεί σημαντικό παράγοντα ασφαλείας στο δίκτυο. Για το λόγο αυτό, εισήχθησαν οι Guard Nodes που στην ουσία αντικατέστησαν τους Entry Nodes, ώστε να εξασφαλίζεται ότι ο Entry Node που επιλέγεται σε κάθε νέο σχηματισμό μονοπατιού θα προέρχεται από ένα μικρό γκρουπ αξιόπιστων κόμβων. Οι Guard Nodes προσδιορίζονται από την Guard flag, η οποία εκχωρείται μετά τη συμπλήρωση 8 ημερών συμμετοχής στο Tor Network και αφού πληρούνται τα επιλεχθέντα κριτήρια σχετικά με το bandwidth και το uptime του. [8] [18]
- Exit Node, ο οποίος αποτελεί και το τελευταίο hop στο Tor Network προτού τα πακέτα της δικτυακής κίνησης φτάσουν στον τελικό προορισμό. Έτσι, ο Exit Node είναι ο μοναδικός κόμβος που γνωρίζει την ταυτότητα του προορισμού (αφού είναι αυτός που υλοποιεί την αποκρυπτογράφηση του τελευταίου onion layer). [8] [22]
- Hidden Services, που αποτελούν web servers εντός ή εκτός του Tor Network. Ανήκουν στο top level domain .onion. Ο Tor Client που τρέχει στον web server που φιλοξενεί ένα Hidden Service δημοσιεύει ένα service descriptor στα Directory Servers, το οποίο περιλαμβάνει πληροφορίες σχετικά με το χρόνο λήξης του, το public key του καθώς και τα Introduction Points που μπορούν να χρησιμοποιηθούν προκειμένου να υπάρξει πρόσβαση σε αυτό. [8] [155] Η onion address μπορεί να υπάρχει διαθέσιμη στο Internet, έτσι ώστε οι χρήστες να μπορούν να το εντοπίσουν προκειμένου να αποκτήσουν πρόσβαση, ή να διακινείται μυστικά, από χρήστη σε χρήστη. Μόλις ένας χρήστης γνωρίζει την onion address ενός Hidden Service, λαμβάνει μέσω του Tor Client το service descriptor από κάποιο Directory Service προκειμένου να ξεκινήσει η διαδικασία σύνδεσης σε αυτό. Τα Hidden Services χρησιμοποιούνται κατά κόρον για παράνομες δράσεις, κυρίως ως αγορές διακίνησης ναρκωτικών ουσιών και παιδικής πορνογραφίας, αγοραπωλησιών όπλων και κυβερνοεπιθέσεων, forums εξτρεμιστικών οργανώσεων, πληρωμή λύτρων κλπ, με αποτέλεσμα να έχουν σύντομο χρόνο λειτουργίας. Συχνά, διάφορα Hidden Services δημιουργούνται για μόλις λίγες ημέρες και μετά παύουν να υπάρχουν, προκειμένου να αποτρέψουν τον εντοπισμό των δημιουργών τους από τις αρχές κι επειδή πλέον ολοκλήρωσαν τη λειτουργία τους.
- Introduction Points, τα οποία είναι τυχαίοι κόμβοι που επιλέγονται από το Hidden Services κάθε φορά που επιχειρείται να εγκατασταθεί μια σύνδεση προς αυτό. Μόλις επιλεχθεί, το Hidden Service παρέχει το public key του στο Introduction Point που έχει επιλέξει. Η συνήθης πρακτική είναι να επιλέγονται διάφορα Introduction Points προκειμένου να αποφευχθούν Denial of Service Attacks εναντίον του Hidden Service. Τα Hidden Services διαφημίζουν στα Directory Services τα διάφορα Introduction Points, προκειμένου να μπορέσουν άλλοι Tor Clients να συνδεθούν σε αυτό. Άξιο παρατήρησης είναι το γεγονός ότι τα Introduction points δε γνωρίζουν την IP Address του Hidden Service που εξυπηρετούν, καθώς συνδέονται σε αυτά πάλι μέσω διαφόρων relays στο Tor Network. [17]

- Rendezvous Points, που είναι τυχαίοι κόμβοι στο δίκτυο, οι οποίοι επιλέγονται από τους Tor Clients προκειμένου να αποτελέσουν το αμέσως προηγούμενο hop πριν το Introduction Point για κάποιο Hidden Service. Έτσι, ο Tor Client δημιουργούν ένα μονοπάτι ως το Rendezvous Point και ειδοποιεί το Hidden Service να τον “συναντήσει” εκεί, δημιουργώντας το δικό του μονοπάτι έως το Introduction Point. Έτσι, ο Tor Client μπορεί να επικοινωνήσει με το Hidden Service μέσω ενός μονοπατιού 6 hops. [18]
- Bridges, αποτελούν κανονικούς Tor relays που όμως δεν είναι καταχωρημένοι στο κύριο Tor directory. Αντικαθιστούν τους guard nodes στο Tor Network, με τον περιορισμό ότι μόνο συγκεκριμένα Bridges είναι διαθέσιμα σε κάθε Tor Client. Με τον τρόπο αυτό, κανένας δε μπορεί να έχει πλήρη εποπτεία για το σύνολο των Bridges που είναι διαθέσιμες στο Tor Network. Με το να μην είναι καταχωρημένες στο κύριο Tor directory εξασφαλίζεται ότι το Tor Network δε θα μπορεί να λογοκριθεί, καθώς υποκαθιστούν τα Directory Services σε περίπτωση που αυτά υποστούν DoS Attacks. [8]

Παρακάτω παρουσιάζεται η δομή ενός Tor Network που εξασφαλίζει την ανωνυμία των χρηστών του, προκειμένου να έχουν πρόσβαση σε περιεχόμενο και web services του Internet χωρίς να αποκαλυφθεί η ταυτότητα τους, ενώ η δεύτερη εικόνα τη δομή του ίδιου δικτύου που όμως περιλαμβάνει ένα Hidden Service.

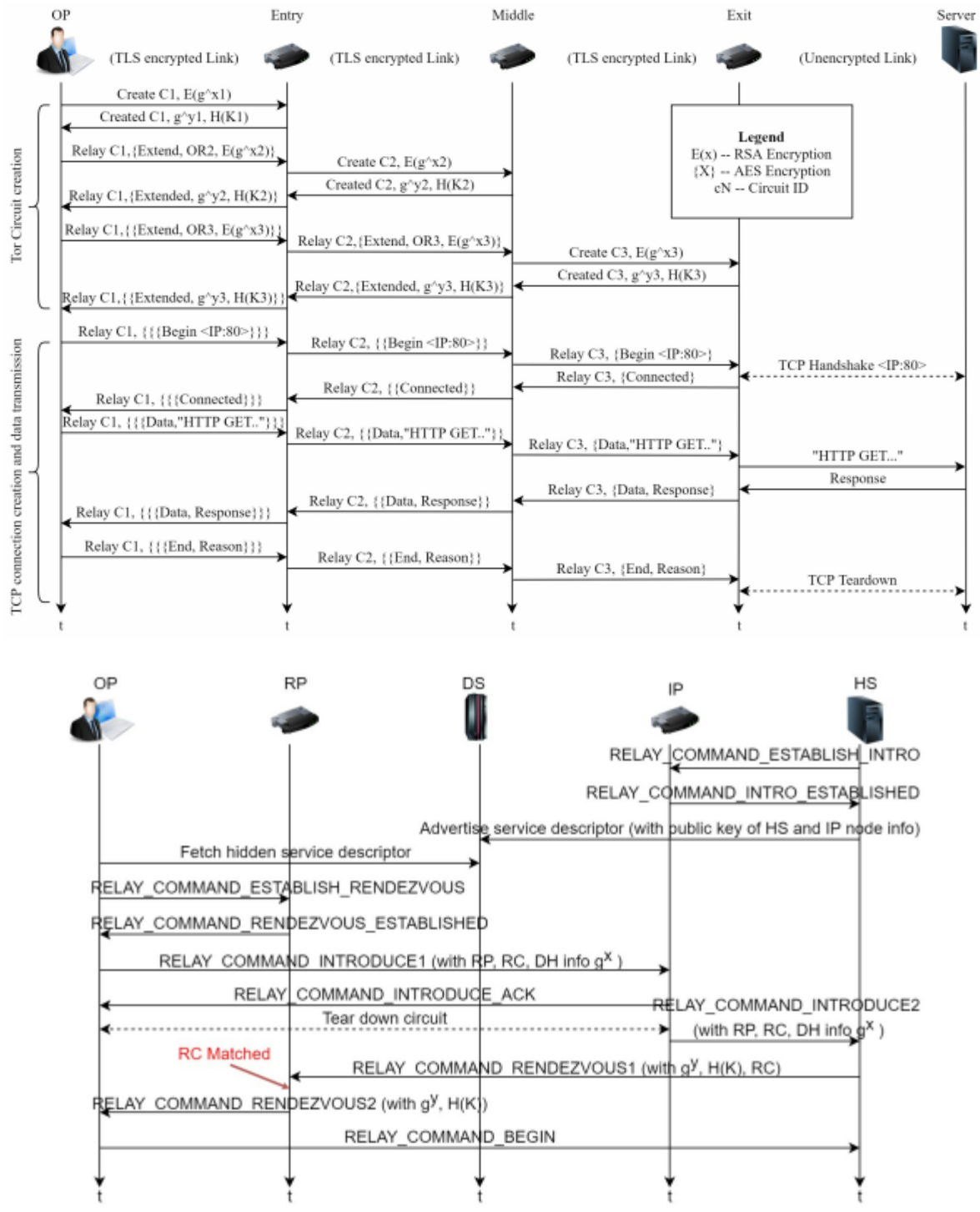


Σχήμα 2.5: Χρήση του Tor Network για πρόσβαση σε Public Server.



Σχήμα 2.6: Χρήση του Tor Network για πρόσβαση σε Hidden Server.

Αντίστοιχα, παρουσιάζεται η εγκατάσταση των παραπάνω συνδέσεων, και η λειτουργία εν γένει των παραπάνω δικτύων.



Σχήμα 2.7: Εγκατάσταση Σύνδεσης για πρόσβαση σε Public και Hidden Server.

Το Tor Network χρησιμοποιεί σταθερού μήκος cells (512 bytes) τα οποία χωρίζονται σε control cells και relay cells. Τα control cells αποτελούν, όπως είδαμε και πιο πριν, τα μηνύματα της αρχιτεκτονικής του Tor Network και περιλαμβάνουν τις εντολές create, created, destroy or padding, οι οποίες μεταφράζονται από τους κόμβους που τις λαμβάνουν. Τα relay cells περιλαμβάνουν εκτός από τα δεδομένα που διακινούνται και ένα relay header που αποτελείται από το χαρακτηριστικό της σύνδεσης, το payload length, checksum για έλεγχο της ακεραιότητας των δεδομένων και μια relay

command (relay data, relay begin, relay end, relay teardown, relay connected, relay extend, relay extended, relay truncate, relay truncated, or relay sendme). [8] [10] [17] [18]

2.1.2 PIR Tor

Keywords: ***Client-Server, Onion Routing, PIR, Consensus***
Maturity: ***Proof of Concept***

Η client-server αρχιτεκτονική εισήχθη στα δίκτυα ανωνύμων επικοινωνιών προκειμένου να αντιμετωπιστεί το πρόβλημα της επεκτασιμότητας των δικτύων. Ο Mittal πρότεινε οι clients να χρησιμοποιούν τεχνικές Private Information Retrieval (PIR) προκειμένου να ανακτούν πληροφορίες μόνο για λίγα relays, αντί ολόκληρης της database. Αυτό θα εξασφάλιζε τόσο την ομαλή επεκτασιμότητα του δικτύου, αφού κάθε client δε θα χρειαζόταν να ανακτά πληροφορίες για όλο το δίκτυο, ενώ θα διασφάλιζε και τη μείωση της πιθανότητας διαρροής πληροφοριών σε περίπτωση που οι clients επέλεγαν relays από κακόβουλους directory servers, επιτρέποντας την προστασία της ανωνυμίας των χρηστών από παθητικές επιθέσεις. Ταυτόχρονα, ο τρόπος δημιουργίας των anonymous tunnels είναι ο ίδιος ακριβώς με αυτό του συμβατικού Tor Network. [8] [155]

Για την υλοποίηση των PIR τεχνικών έχουν προταθεί δύο διαφορετικές αρχιτεκτονικές. Η πρώτη είναι η Computational PIR –CPIR, η οποία είναι μια single server αρχιτεκτονική, που χρησιμοποιεί τους υπάρχοντες directory servers για τον διαμοιρασμό της πληροφορίας του δικτύου στους συμμετέχοντες. Οι τεχνικές PIR διασφαλίζουν ότι αν ένας Tor client λάβει ένα μικρό block των descriptors από κάποιον directory server αμφιβόλου αξιοπιστίας, ο directory server δε μπορεί να γνωρίζει ποιο ακριβώς block έχει λάβει ο client. [10] [17] Για την αποφυγή δημιουργίας μεγάλου overhead προτείνεται στους clients να περιορίζουν τα queries και να επαναχρησιμοποιούν τους descriptors που ήδη έχουν λάβει σε τακτά χρονικά διαστήματα. Η δεύτερη αρχιτεκτονική είναι η Information-Theoretic PIR –ITPIR, η οποία είναι μια multi-server λύση και βασίζεται στη χρήση guard nodes για τη λήψη των descriptors του δικτύου. [155]

Και οι δύο αρχιτεκτονικές βασίζονται στο γεγονός ότι ο χρήστης λαμβάνει κάθε φορά έναν πολύ μικρό και περιορισμένο αριθμό descriptors και μάλιστα οι τεχνικές PIR διασφαλίζουν ότι ο ίδιος είναι ο μόνος που γνωρίζει ποιο ακριβώς block έχει λάβει και χρησιμοποιεί. Το PIR Tor καταφέρνει να δώσει λύση στα προβλήματα επεκτασιμότητας που έχει το αρχικό Tor Network, ωστόσο διατηρεί τα ίδια επίπεδα ασφαλείας με τη συμβατική λύση. [18] Παρέχει επαρκή ασφάλεια έναντι επιθέσεων όπως οι Route Fingerprinting Attacks, καθώς οι PIR τεχνικές αποτρέπουν τους επιτιθέμενους από τα να συνδέσουν ποιοι relays έχουν ληφθεί από τους clients και ποιοι έχουν ληφθεί από την database. Παρ όλα αυτά, οι πληροφορίες που έχουν διαρρεύσει από το δίκτυο μέσω ανάλυσης, μπορούν να χρησιμοποιηθούν προκειμένου να χτίσει ένας επιτιθέμενος συμπεριφορικά προφίλ των χρηστών. Τέλος, υποφέρει εξίσου με το συμβατικό Tor όσον αφορά σενάρια επιθέσεων όπου ο επιτιθέμενος έχει κάνει compromisation του πρώτου ή του τελευταίου κόμβου, ενώ είναι το ίδιο ευάλωτες σε Denial of Service Attacks. [155]

2.1.3 LASTor

Keywords: ***Client-Server, Onion Routing, Tor Client***
Maturity: ***Proof of Concept***

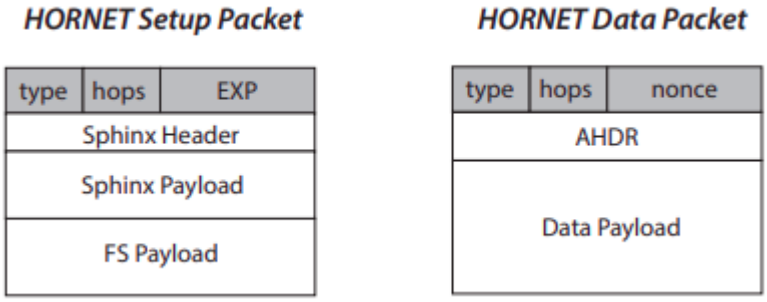
Το LASTor είναι ένας Tor client ο οποίος στοχεύει στη μείωση του latency που παρατηρείται μέσω της χρήσης του παραδοσιακής λύσης, ειδικά σε σύγχρονες και απαιτητικές διαδικτυακές εφαρμογές.

Επιπλέον, παρέχει προστασία της ανωνυμίας των χρηστών, ειδικότερα σε επίπεδα όπου το Autonomous System (AS) παρακολουθεί τη δραστηριότητα τους. Οι χρήστες έχουν έλεγχο πάνω στο πόσο ισχυρή επιθυμούν να είναι η προστασία τους, επιλέγοντας εκείνοι το κατάλληλο trade off μεταξύ της προστασίας της ανωνυμίας τους και του latency του δικτύου. [186]

2.1.4 Hornet

***Keywords:* Client-Server, High Speed**
***Maturity:* Limited Adoption**

Το HORNET (High-speed Onion Routing at the NETwork layer) αποτελεί ένα επεκτάσιμο, low-latency δίκτυο το οποίο βασίζεται στο Onion Routing και το εξελίσσει με βάση τη next-generation Internet αρχιτεκτονική. Υποστηρίζει payload protection τεχνικές ώστε να προστατεύει την ταυτότητα των χρηστών σε περιβάλλοντα στα οποία ο επιτιθέμενος διαθέτει πολλαπλά σημεία παρατήρησης του δικτύου. Είναι εξαιρετικά αποδοτικό, καθώς χρησιμοποιεί short paths μέσω των υπαρχουσών δικτυακών υποδομών, ώστε να επιτύχει υψηλότερες ταχύτητες από τη συμβατική λύση. Επιπλέον, όλα τα χαρακτηριστικά του Onion Routing ενσωματώνονται στα packet headers προκειμένου να υλοποιείται πιο γρήγορα η προώθηση των πακέτων. Προστατεύει τόσο τον Initiator οσο και τον Responder από επιθέσεις. [204] Παρακάτω παρουσιάζεται η δομή των δύο πακέτων που χρησιμοποιεί το Hornet. Χρησιμοποιούνται δύο πακέτα, τα οποία έχουν κοινό header (CHDR) που περιγράφει το είδος του πακέτου, και το μέγιστο υποστηριζόμενο μήκος μονοπατιού.

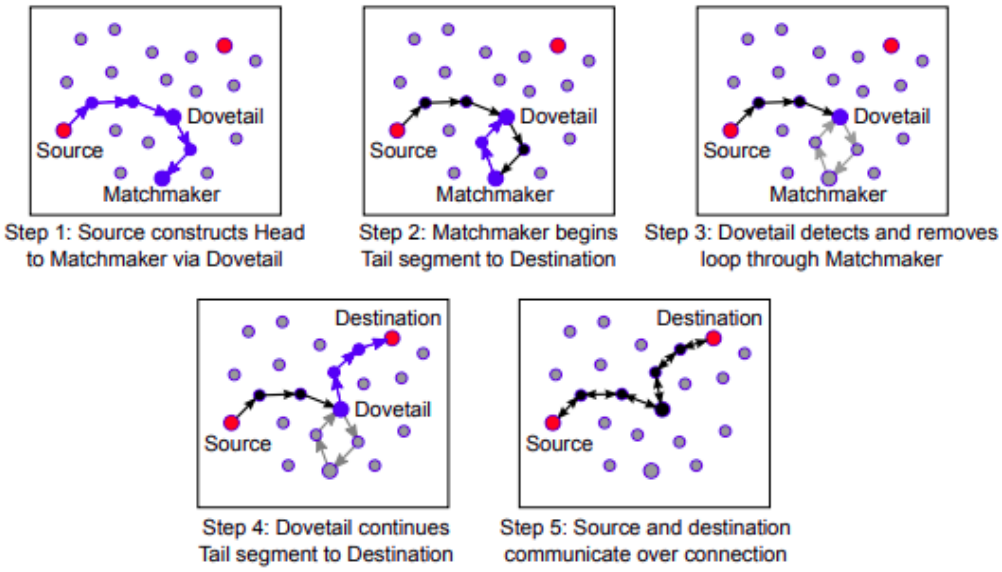


Σχήμα 2.8: Setup & Data Packets στο HORNET.

2.1.5 Dovetail

***Keywords:* Client-Server, Matchmaker, ISP, AS**
***Maturity:* Limited Adoption**

Το Dovetail είναι μια τεχνολογία η οποία αντιμετωπίζει επιθέσεις που ενδεχομένως να πηγάζουν από ISPs, παρέχοντας προστασία απέναντι σε ενεργούς επιτιθέμενους που βρίσκονται σε οποιοδήποτε σημείο του δικτύου. Χρησιμοποιεί ένα matchmaker node (δηλαδή έναν end host) οποίος υπερκαλύπτει δύο τμήματα μονοπατιών σε έναν dovetail node (δηλαδή έναν router). Στη συνέχεια ο dovetail node κόβει ένα τμήμα του μονοπατιού έτσι ώστε η διαδιδόμενη ροή δεδομένων να παρακάμψει τον matchmaker node. Μπορεί έτσι να επιτύχει καλά επίπεδα προστασίας της ανωνυμίας των χρηστών ακόμα και σε AS ή ISP επίπεδο. Παρακάτω παρουσιάζεται η διαδικασία κατασκευής μιας dovetail σύνδεσης. [206]

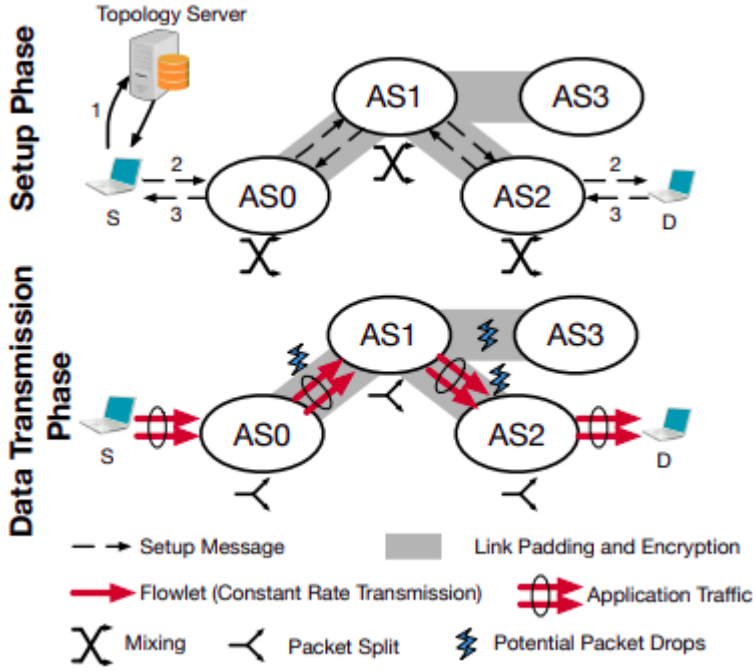


Σχήμα 2.9: Σχηματισμός Dovetail.

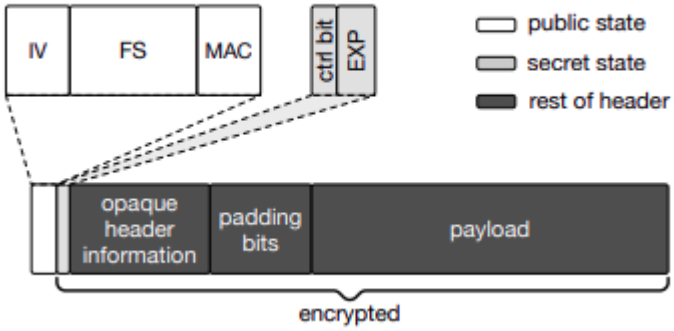
2.1.6 TARANET

Keywords: ***Client-Server, Onion Routing, Mixes, Traffic Shaping***
Maturity: ***Limited Adoption***

Αποτελεί μια σύγχρονη τεχνολογία ανωνύμων επικοινωνιών που χρησιμοποιεί συνδυαστικά την αποδοτικότητα του Onion Routing και τους μηχανισμούς ασφαλείας των Mix Networks προκειμένου να παρέχει πρόσβαση σε εφαρμογές με low-latency απαιτήσεις και να διασφαλίσει τους χρήστες απέναντι σε Traffic Analysis Attacks. Χρησιμοποιεί mixing και coordinated traffic shaping τεχνικές για την αντιμετώπιση των παραπάνω επιθέσεων κατά τις setup και data transmission φάσεις αντίστοιχα. Μπορεί να επιτύχει τόσο μεγάλη διαθεσιμότητα όσο και καλές επιθέσεις καθώς τα σύγχρονα δίκτυα υψηλών ταχυτήτων, πάνω στα οποία λειτουργεί το TARANET, μπορεί να επεξεργαστεί μεγάλο όγκο mixed traffic με αποτέλεσμα να μη δημιουργείται σημαντικό overhead. [205] Παρακάτω παρουσιάζεται η δομή του δικτύου, καθώς και η δομή του πακέτου που χρησιμοποιείται.



Σχήμα 2.10: Αρχιτεκτονική του TARANET



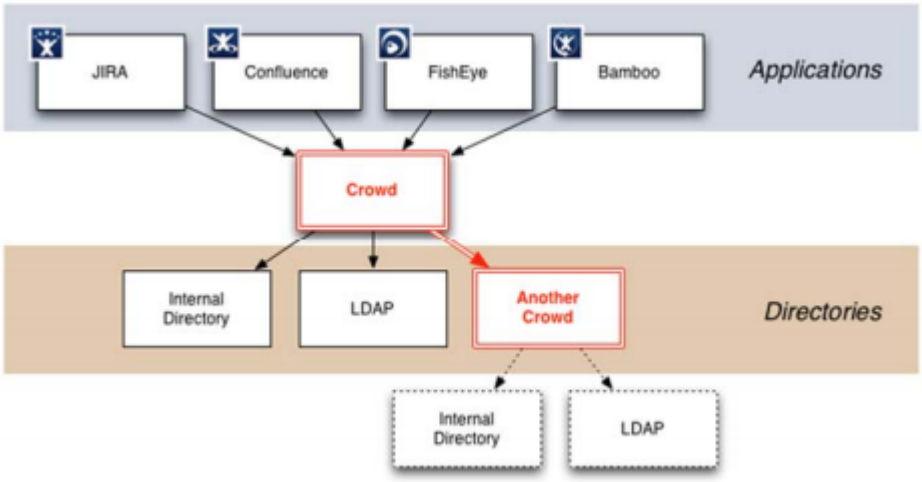
Σχήμα 2.11: Δομή ενός πακέτου στο TARANET.

2.1.7 Crowds

***Keywords:* Client-Server, Proxies, Jondos, Blender**
***Maturity:* Limited Adoption**

Το Crowds (Reiter & Rubin, 1998) είναι μια ακόμη υπηρεσία που προσφέρεται στους χρήστες για την επίτευξη ανωνυμίας τους. Εμποδίζει τον web server που προσφέρει το περιεχόμενο στον χρήστη να συλλέξει πληροφορίες σχετικά με τον web browser που εκτελεί τα requests, καθώς και οποιοδήποτε στοιχείο αφορά την τοποθεσία του ή το domain name του. Ουσιαστικά, ένα γκρουπ κόμβων λειτουργούν ως proxies για έναν κόμβο που επιθυμεί να ξεκινήσει να επικοινωνεί ανώνυμα. Κατά την έναρξη της επικοινωνίας, σχηματίζεται ένα μονοπάτι, μέσω του οποίου διέρχονται όλα τα μελλοντικά μηνύματα της συγκεκριμένης πηγής. [16] Κάθε ενδιάμεσος κόμβος που λαμβάνει ένα μήνυμα, αποφασίζει αν θα προωθήσει το μήνυμα σε ακόμη έναν κόμβο, ή αν θα γίνει εκείνος ο τελευταίος κόμβος του μονοπατιού και θα επικοινωνήσει με τον τελικό προορισμό. Το εκάστοτε μονοπάτι έχει περιορισμένη χρονική διάρκεια, με το πέρας της οποίας όλα τα σχηματισθέντα μονοπάτια πρέπει να

ξαναχτιστούν. Έτσι, νεοεισερχόμενοι στο Crowd κόμβοι έχουν τη δυνατότητα να φτιάξουν νέα μονοπάτια ταυτόχρονα με όλους τους υπόλοιπους, χωρίς να υπάρχει εύκολη συσχέτιση των νέων μονοπατιών με τους νέους κόμβους. [81] Η ίδια διαδικασία ακολουθείται μάλιστα και στην περίπτωση που ένας κόμβος αποχωρήσει από το Crowd.



Σχήμα 2.12: Αρχιτεκτονική του Crowds.

2.1.8 PIPENET

***Keywords:* Client-Server, Proxies**
***Maturity:* Proof of Concept**

Το Pipenet βασίζεται στο mix network του Chaum, εισάγοντας ωστόσο πολύ πιο αυστηρά κριτήρια reactive ασφαλείας, βασιζόμενο σε ένα κατανεμημένο σύνολο packet forwarders. Εάν παρατηρείτο η παραμικρή ανωμαλία στη λειτουργία του PIPENET, αυτομάτως αυτό εκλαμβανόταν ως επίθεση, με αποτέλεσμα να διακόπτεται ολόκληρη η λειτουργία του δικτύου με σκοπό να διασφαλιστεί η προστασία της ανωνυμίας των χρηστών του. Η λειτουργία του βασίζεται στη δημιουργία ανώνυμων channels μέσω των οποίων υλοποιείται αμφίδρομη επικοινωνία κρυπτογραφημένων μηνυμάτων, μεταξύ των συνομιλούντων μερών. Ο χρήστης επιλέγει το μονοπάτι, το οποίο είναι ουσιαστικά μια αλυσίδα κόμβων, στο οποίο στη συνέχεια κρυπτογραφείται διαδοχικα η δικτυακή του κίνηση. Αναμένεται να διακινείται ένα πακέτο σε κάθε σύνδεσμο, στη μονάδα του χρόνου. Αν κάποιος κόμβος δε λάβει κάποιο μήνυμα σε καμία υποδοχή του, τότε παύει η λειτουργία ολόκληρου του δικτύου. Αυτό διασφαλίζει την αδυναμία υλοποίησης επιτυχών παθητικών επιθέσεων, καθώς υπάρχει μονίμως δικτυακή κίνηση με αποτέλεσμα να μην είναι εύκολο να διαχωριστεί. Ωστόσο είναι μη εφαρμόσιμο στη χρήση, ιδιαίτερα σε σύγχρονα δίκτυα όπως το Internet. [158]

2.1.9 Oceanstore

***Keywords:* Client-Server, File Storage**
***Maturity:* Proof of Concept**

Το Oceanstore αποτελεί ένα παγκόσμιας κλίμακας και υψηλής διαθεσιμότητας σύστημα αποθήκευσης δεδομένων. Οι χρήστες που θέλουν να έχουν πρόσβαση στο περιεχόμενο καταβάλουν το απαραίτητο αντίτιμο στους παρόχους του, και όταν αποδεσμεύσουν το περιεχόμενο, το Oceanstore εντοπίζει τον εγγύτερο server που έχει ένα αντίγραφο του περιεχομένου, προκειμένου να το παρέχει στον χρήστη. Οι Servers χρησιμοποιούν το Tapestry για την αποθήκευση και τον εντοπισμό των αντικειμένων, με

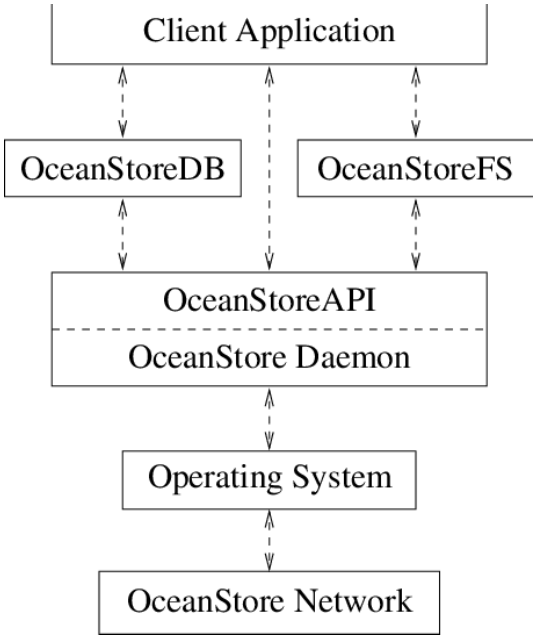
αποτέλεσμα η ανάκτηση περιεχομένου από τους χρήστες να είναι γρήγορη και διαρκής, ακόμα και σε περιπτώσεις που υπάρχουν servers failures ή προβλήματα στο δίκτυο. [20]

Το περιεχόμενο διαφοροποιείται μέσω ενός Global Unique ID (GUID) το οποίο είναι το secure hash του κλειδιού του ιδιοκτήτη του περιεχομένου και ένα όνομα, με αποτέλεσμα να καθίσταται εύκολος και γρήγορος ο εντοπισμός και η επαλήθευση του ιδιοκτήτη του περιεχομένου. Κάθε μήνυμα στο Tapestry αναγνωρίζεται από το GUID και όχι από την IP Address. Επιπλέον, χρησιμοποιεί ACL για τους περιορισμούς εγγραφής στα δεδομένα, ενώ η ανάγνωση τους είναι διαθέσιμη μέσω των προαναφερθέντων κλειδιών. Τα updates του περιεχομένου γίνονται μέσω του Byzantine Agreement πρωτοκόλλου. Το Oceanstore χρησιμοποιεί αρκετούς αυτοματισμούς για την καλύτερη διαχείριση των δεδομένων καθώς και για την ευκολότερη ανάκτηση τους. [45]

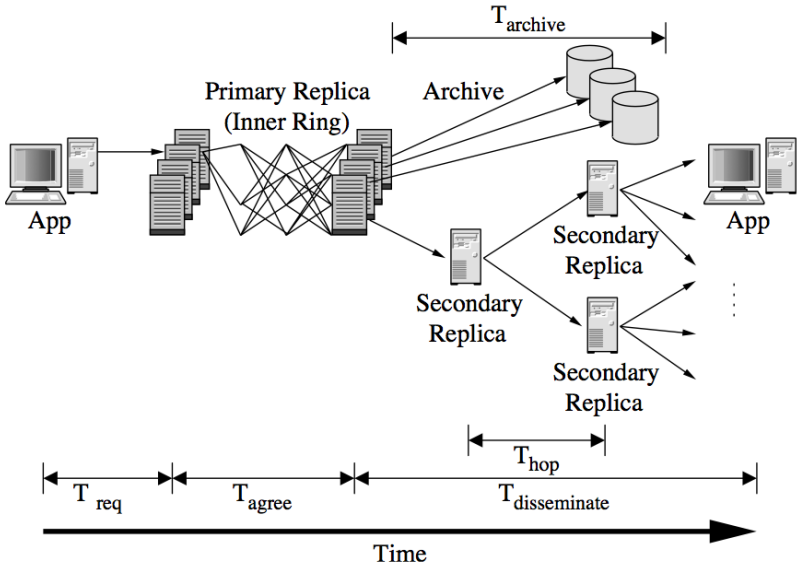
Έχει τη δυνατότητα να υλοποιηθεί από μη δομημένη υποδομή, ενώ υλοποιεί μηχανισμούς aggressive promiscuous catching, οι οποίοι παρέχουν ταχύτερη πρόσβαση στα δεδομένα, αποφυγής δικτυακής συμφόρησης και μεγαλύτερη συμπάγεια στα network partitions. Έτσι, αποφεύγεται το ενδεχόμενο διαρροής δεδομένων σε περίπτωση που ένας server τεθεί εκτός λειτουργίας. [36] Οι μηχανισμοί αυτοί απαιτούν redundancy και ισχυρά κρυπτογραφικά σχήματα προκειμένου να εγγυηθούν την ακεραιότητα και τη διαθεσιμότητα των δεδομένων.

Τέλος, το API του Oceanstore χρησιμοποιεί byzantine-fault tolerant commit πρωτόκολλο προκειμένου να εγγυηθεί τη συνοχή των δεδομένων, ανάμεσα στα διαφορετικά αντίγραφα που υπάρχουν στο δίκτυο. Κάθε έκδοση του εκάστοτε περιεχομένου αποθηκεύεται σε μια μόνιμη read-only μορφή η οποία κωδικοποιείται σε ένα erasure code και διανέμεται σε εκατοντάδες ή χιλιάδες servers. Ένα μικρό υποσύνολο των fragments αυτών είναι επαρκές για την ανάκτηση των δεδομένων.

Όπως προαναφέραμε το Oceanstore υλοποιεί μηχανισμούς ενδοσκόπησης και καταγραφής συμβάντων προκειμένου να βελτιώνει τις επιδόσεις του δικτύου και να κρατάει σε χαμηλό ρυθμό τα σφάλματα. Με τον τρόπο αυτό, μπορεί όχι μόνο να βελτιώνει τη λειτουργία του αναλόγως των αιτημάτων των χρηστών για περιεχόμενο, αλλά και να προλαμβάνει Denial of Service Attacks, ακόμα και σε τοπικό επίπεδο.



Σχήμα 2.13: Αρχιτεκτονική του OceanStore.



Σχήμα 2.14: Ενδεικτική αναζήτηση πόρων στο OceanStore.

2.1.10 Tarzan

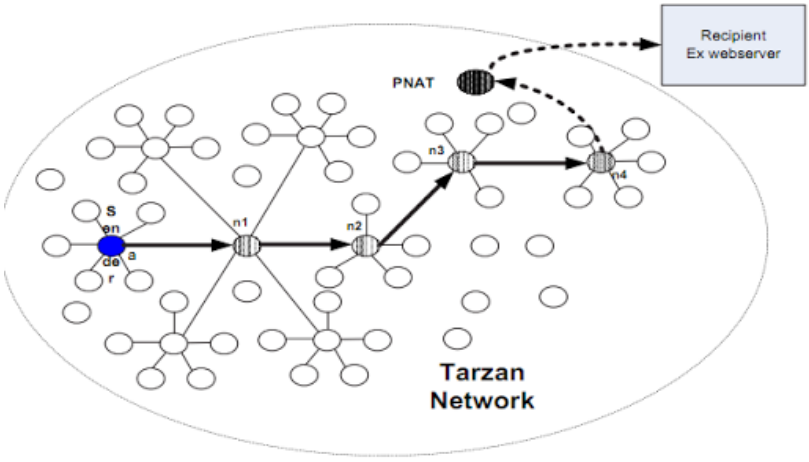
Keywords: ***Peer-To-Peer, Dummy Traffic, Mimics, Neighbours***
Maturity: ***Proof of Concept***

Το Tarzan είναι ένα low latency δίκτυο ανωνύμων επικοινωνιών, με στόχο να προσφέρει ανωνυμία σε μια ευρεία γκάμα διαδικτυακών εφαρμογών και υπηρεσιών, όπως instant messaging. Πρόκειται για ένα πλήρως αποκεντρωμένο P2P δίκτυο, βασισμένο στο IP, καθιστώντας το δίκτυο ανωνύμων γενικής χρήσης, αφού έχει τη δυνατότητα να εξυπηρετήσει δικτυακή κίνηση από και προς τις περισσότερες διαδικτυακές εφαρμογές. Κάθε κόμβος μπορεί να έχει ρόλο τόσο του client όσο και του relay.

Παρέχει διαστρωματωμένη κρυπτογράφηση και δρομολόγηση πολλαπλών επιπέδων, στο οποίο ο client επιλέγει ένα μονοπάτι, με αυστηρά καθορισμένες προδιαγραφές. Οι peers επιλέγονται μέσω αλγορίθμου ο οποίος εξασφαλίζει τυχαιότητα και ισότητα μεταξύ τους. [2]

Οι συμμετέχοντες κόμβοι χρησιμοποιούν ειδικό λογισμικό το οποίο τους επιτρέπει να ανακαλύπτουν άλλους κόμβους που διαφημίζονται στο δίκτυο, να κρυπτογραφούν μηνύματα σύμφωνα με τις προδιαγραφές των πρωτοκόλλων του Tarzan, να δρομολογούν τα πακέτα μέσω μονοπατιών αλλά και να συμμετέχουν οι ίδιοι, ως μέρος μονοπατιών για τη διακίνηση μηνυμάτων άλλων χρηστών. Ο παραλήπτης των μηνυμάτων δεν απαιτείται να είναι μέρος του Tarzan. [9]

Οι γείτονες κάθε κόμβου αποκαλούνται mimies και είναι υπεύθυνοι για την παραγωγή dummy traffic προκειμένου να καταστούν δυσκολότερες διάφορες Traffic Analysis Attacks. Επίσης, χρησιμοποιεί το peer-to-peer gossip protocol μέσω του οποίου οι clients μπορούν να συλλέξουν πληροφορίες για άλλους servers στο δίκτυο μοιράζοντας πληροφορίες σχετικά με αυτούς. Ουσιαστικά κάθε κόμβος ρωτάει τους γείτονες του σχετικά με την ύπαρξη servers στο δίκτυο, ώστε να ανακαλύψει εκείνους που δεν γνωρίζει ακόμα. Η δυνατότητα ενός επιτιθέμενου να συμμετέχει στο gossip protocol αποτελεί πρόσφορο έδαφος για την έναρξη επιθέσεων εναντίων του πρωτοκόλλου, ωστόσο το δίκτυο είναι ανθεκτικό απέναντι σε global eavesdroppers και κακόβουλους κόμβους. Τέλος, το Tarzan, λόγω της χρήσης των mimies περιορίζεται αισθητά όσον αφορά το μέγιστο πλήθος clients που μπορεί να εξυπηρετήσει, καθώς μπορεί να υποστηρίξει έως 10,000 κόμβους ταυτόχρονα. [9]



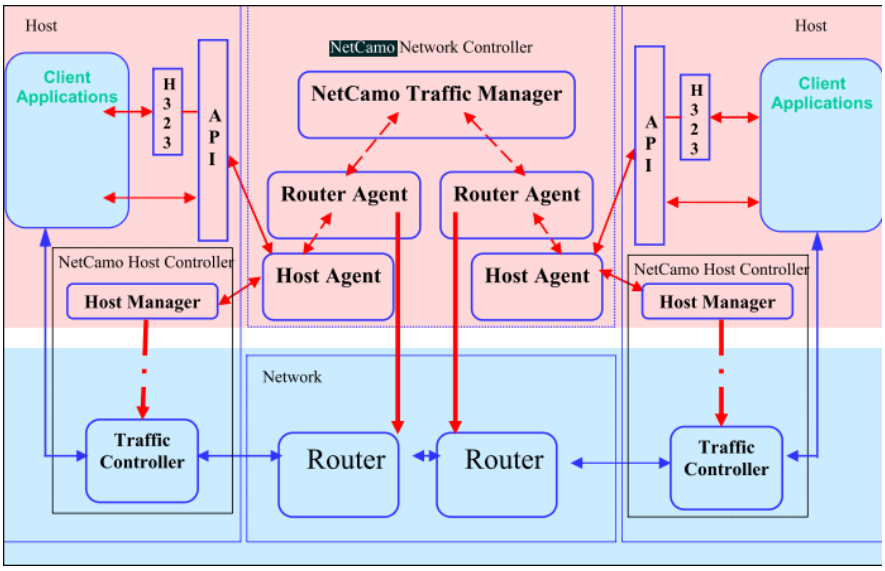
Σχήμα 2.15: Αρχιτεκτονική του Tarzan.

2.1.11 NetCamo

***Keywords:* Client-Server, Dummy Traffic**
***Maturity:* Limited Adoption**

Συντομογραφία του Network Camouflage, το οποίο αποτελεί ένα σύστημα ανωνύμων επικοινωνιών μέσω του οποίου εξασφαλίζεται τόσο η ανωνυμία των χρηστών όσο και η αποδοτικότητα του δικτύου. Η λειτουργία του βασίζεται σε δύο πυλώνες. Ο πρώτος είναι το traffic padding, στο οποίο κρυπτογραφημένα προς διακίνηση δεδομένα ενώνονται με dummy πακέτα, προκειμένου να καταστεί δυσκολότερη η ανάλυση της δικτυακής κίνησης. Ο δεύτερος πυλώνας λειτουργίας είναι το traffic rerouting, το οποίο διασφαλίζει ότι τα δεδομένα θα φτάσουν στον προορισμό μέσω πολλών και διαφορετικών μονοπατιών. [2]

Βασικός στόχος του NetCamo, είναι η εύρεση του βέλτιστου trade-off μεταξύ της διασφάλισης της ανωνυμίας και του low latency. Έτσι, αποτελεί έναν πολύ αποδοτικό τρόπο ανωνύμων επικοινωνιών που καταφέρνει να ανταποκριθεί στις απαιτήσεις των σύγχρονων διαδικτυακών εφαρμογών. Οι επιδόσεις του δικτύου φθίνουν όσο μεγαλώνει το ποσοστό των dummy πακέτων που εισάγονται στο σύστημα.

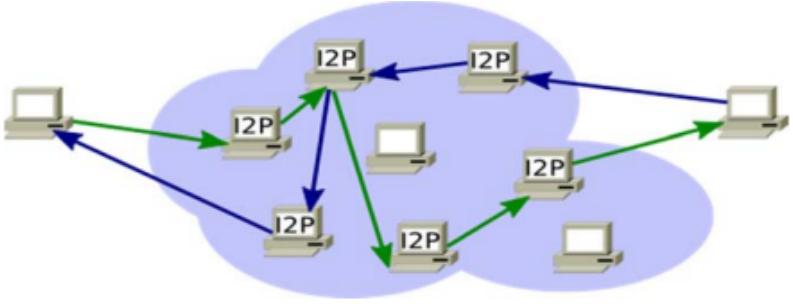


Σχήμα 2.16: Αρχιτεκτονική του NetCamo.

2.1.12 I2P

Keywords: ***Peer-To-Peer, File Sharing, Web Hosting, Dummy Traffic***
Maturity: ***Common***

Το Invisible Internet Project είναι ένα low latency mix δίκτυο ανωνύμων επικοινωνιών, με σκοπό να καλύψει τις ανάγκες των χρηστών του για ανώνυμο file sharing και web hosting. Σε αντίθεση με το Tor, το I2P έχει ως κύριο στόχο να αποκρύψει την ταυτότητα τόσο των αποστολέων, όσο και των παραληπτών της δικτυακής κίνησης και όχι μόνο του αποστολέα. Το I2P λειτουργεί στο Στρώμα Δικτύου, διαχωρίζοντας την ταυτότητα του εκάστοτε χρήστη από τη γεωγραφική του θέση (δηλαδή την IP Address του). Βασίζεται στη μεταγωγή πακέτου και όχι κυκλώματος. Αποτελεί ένα πλήρως κατανεμημένο και αυτόνομο P2P σύστημα που δε βασίζεται σε καταλόγους και ευρετήρια που παρέχουν Directory Servers. Όπως και το Onion Routing, χρησιμοποιεί διαστρωματωμένη κρυπτογράφηση στα προς διακίνηση onion cells, τα οποία ομαδοποιεί, ενισχύει με padding (dummy messages), δημιουργώντας τα garlic cloves. Χρησιμοποιούνται διάφορα σχήματα κρυπτογράφησης, ενώ οι κόμβοι έχουν τη δυνατότητα να δεχθούν delay/no delay εντολές, αναλόγως των δικτυακών εφαρμογών προς τις οποίες απευθύνεται η δικτυακή κίνηση και τις απαιτήσεις σε low latency. [156]



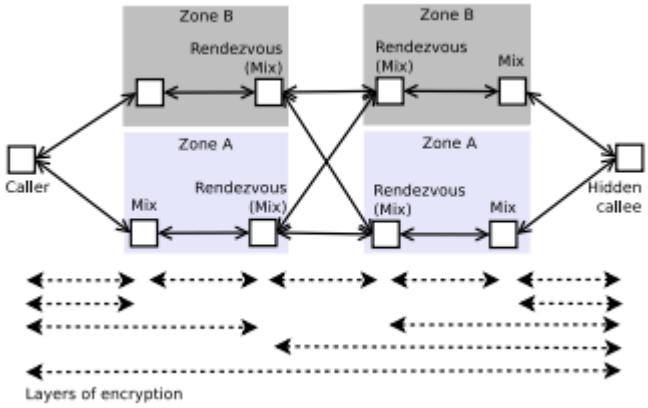
Σχήμα 2.17: Αρχιτεκτονική του I2P.

2.1.13 Herd

Keywords: ***Client-Server, VoIP, Network Coding, Cloud-based, Proxies***
Maturity: ***Proof of Concept***

Στο Herd ένα σύνολο από cloud-based proxies συνεργάζονται προκειμένου να παρέχουν ανωνυμία στους χρήστες του δικτύου, μέσω κυκλωμάτων χαμηλής καθυστέρησης. Στόχος του είναι η εξυπηρέτηση των αναγκών των χρηστών για ανωνυμία σε VoIP υπηρεσίες. Πρόκειται για μια σύγχρονη λύση η οποία έχει τη δυνατότητα εξυπηρέτησης εκατομμυρίων χρηστών με καλή ποιότητα κλήσης και σχετικά χαμηλό κόστος. Η ανωνυμία επιτυγχάνεται σε ζώνες, μέσω αξιόπιστης υποδομής την οποία απαρτίζουν οι proxies του δικτύου.

Μη αξιόπιστα μέρη μπορούν να συμμετέχουν στο δίκτυο, παρέχοντας πόρους, καθώς χρησιμοποιούνται network coding τεχνικές που επιτρέπουν στους αξιόπιστους proxies να ενσωματώνουν περαιτέρω πόρους για την καλύτερη επεκτασιμότητα του δικτύου καθώς και για τη μείωση του κόστους. Αποτελεί μια ανθεκτική λύση απέναντι σε global adversaries καθώς χρησιμοποιεί διαστρωματωμένη κρυπτογράφηση, ενώ έχει και σημαντικά μειωμένες απαιτήσεις σε bandwidth. Στο παρακάτω σχήμα παρουσιάζεται συνοπτικά η δομή του δικτύου. [176]



Σχήμα 2.18: Αρχιτεκτονική του Herd.

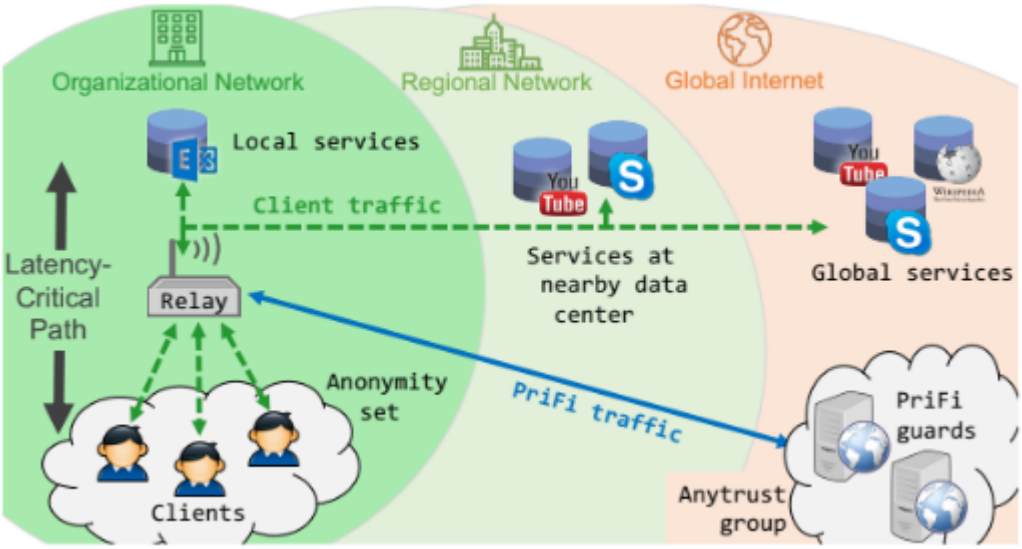
2.1.14 PriFi

Keywords: ***Client-Relay-Server, LAN, WLAN, Anytrust***
Maturity: ***Proof of Concept***

Το PriFi είναι χτισμένο πάνω στο DC-Net και χρησιμοποιείται για να παρέχει ανώνυμες επικοινωνίες σε LANs και WLANs τα οποία χρησιμοποιούνται από οργανισμούς και είναι ευάλωτα απέναντι σε Eavesdropping Attacks, κυρίως μέσω της ανάλυσης των μεταδεδομένων και των patterns της δικτυακής κίνησης. [2] Το δίκτυο προσφέρει ανωνυμία, accountability των χρηστών για τυχόν κακόβουλες ενέργειες, χαμηλό latency καθώς και καλή επεκτασιμότητα του. Λειτουργεί παρόμοια με μια VPN λύση, χωρίς ωστόσο να χρειάζεται να το εμπιστεύονται οι χρήστες προκειμένου να το χρησιμοποιήσουν, όπως θα έκαναν με έναν πάροχο υπηρεσίας.

Χρησιμοποιεί μια client/relay/server αρχιτεκτονική αφαιρώντας από το δίκτυο τις κοστοβόρες server-to-server επικοινωνίες, επιτρέποντας την κρυπτογράφηση της δικτυακής κίνησης των χρηστών σε τοπικό επίπεδο, αποτρέποντας έτσι τα latency bottlenecks. Αυτή η ιδιότητα εγγυάται και την προστασία του δικτύου από Eavesdropping Attacks, αφού τα πακέτα διέρχονται από τη συνηθισμένη

οδό και όχι δια μέσω κάποιου anonymous tunnel που μπορεί να έχει γίνει compromised. Κομβικής σημασίας είναι η έννοια του Anytrust, που υπαγορεύει ότι εφόσον έστω και ένας server είναι ασφαλής, τότε το PriFi μπορεί να εγγυηθεί για την ασφάλεια του δικτύου. Τόσο οι Tracking Attacks όσο και οι Disruptive Attacks αποτρέπονται αποτελεσματικά χωρίς πρόσθετο latency στο δίκτυο. Έτσι, είναι σε θέση να υποστηρίξει μεγάλο αριθμό χρηστών που συμμετέχουν ταυτόχρονα σε απαιτητικές, low-latency εφαρμογές όπως VoIP και videoconferencing. Στην παρακάτω εικόνα παρουσιάζεται συνοπτικά η αρχιτεκτονική του. [172]



Σχήμα 2.19: Αρχιτεκτονική του PriFi.

2.1.15 LAP: Lightweight Anonymity and Privacy

***Keywords:* Client-Relay-Server, LAN, WLAN, Anytrust**
***Maturity:* Proof of Concept**

Το Lightweight Anonymity and Privacy (LAP) αποτελεί μια network-based λύση η οποία χρησιμοποιεί lightweight path establishment και stateless communication τεχνικές, προκειμένου να προστατεύσει την ανωνυμία των χρηστών του δικτύου, παρέχοντας ικανοποιητική προστασία από μέσου επιπέδου και ικανοτήτων επιτιθέμενους. Στόχος του LAP είναι να πετύχει το βέλτιστο trade-off μεταξύ της διατήρησης της ανωνυμίας των χρηστών και του επιθυμητού latency, παρέχοντας, όπως υποδηλώνει και το όνομα, lightweight anonymity στους χρήστες. Η διασφάλιση της ανωνυμίας των χρηστών γίνεται με τεχνικές Encrypted, Asymmetric Paths Establishment, ενώ υποστηρίζεται και το Mobility των χρηστών. Αποτελεί μια αξιόπιστη λύση όταν ο κίνδυνος επιθέσεων είναι χαμηλός και όταν οι χρήστες επιθυμούν να αποφύγουν κυρίως την παρακολούθηση της δραστηριότητας τους από ISPs και όχι από κρατικούς οργανισμούς ή υπηρεσίες επιβολής του νόμου. [187]

2.2 Anonymity-focused Τεχνολογίες

Πρόκειται για τεχνολογίες που δίνουν βαρύτητα στην προστασία της ανωνυμίας των χρηστών του δικτύου. Μερικές εξ αυτών χρησιμοποιούνται για ανταλλαγή μηνυμάτων ή ηλεκτρονικής αλληλογραφίας, αυξάνοντας σημαντικά την καθυστέρηση των διακινούμενων πακέτων, προκειμένου να διασφαλιστεί η ανωνυμία των χρηστών. Άλλες εξ αυτών χρησιμοποιούν random paths και random

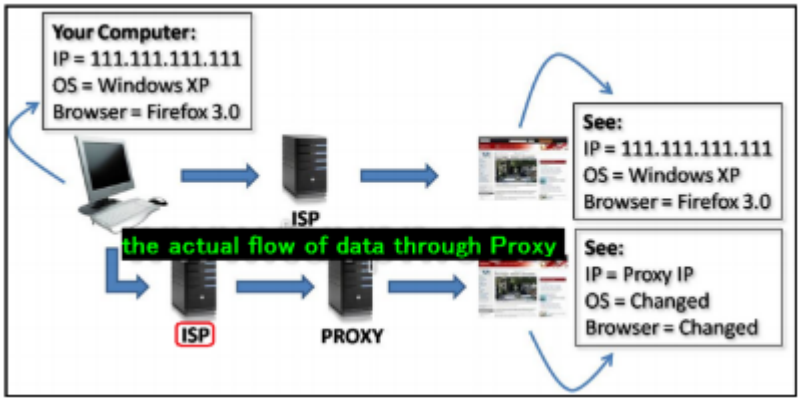
lookups τεχνικές προκειμένου να αυξήσουν την ανθεκτικότητα τους απέναντι σε επιθέσεις ανάλυσης της δικτυακής κίνησης.

2.2.1 Anonymizer/Anonymity via Proxy

***Keywords:* Client-Server, Proxies**

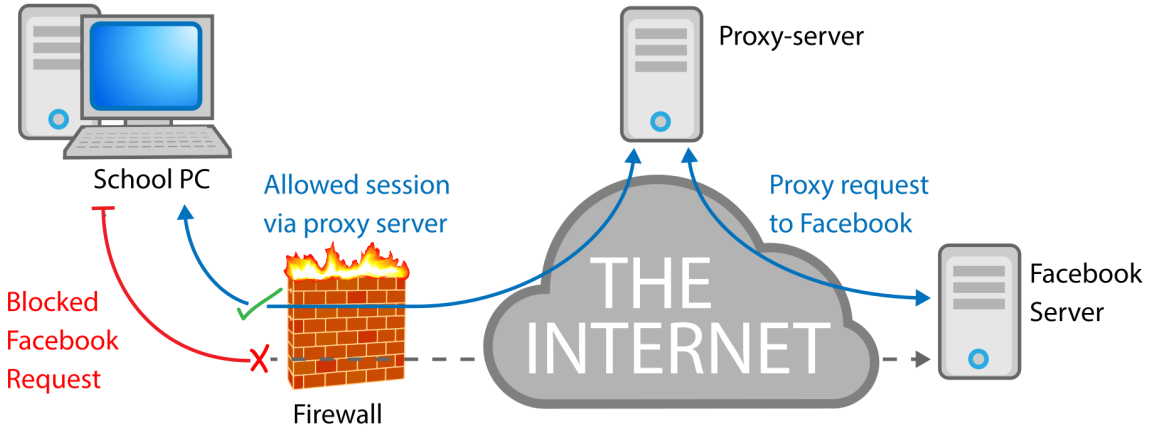
***Maturity:* Common**

Ο διακομιστής μεσολάβησης (proxy server) είναι ένα θεμελιώδες εργαλείο στα δίκτυα υπολογιστών που χρησιμοποιείται για πάρα πολλούς λόγους, μεταξύ των οποίων η ασφάλεια ενός server ή ενός ολόκληρου δικτύου, αλλά και από κακόβουλους χρήστες οι οποίοι θέλουν να καταστήσουν δυσκολότερο τον εντοπισμό τους. Έτσι, το proxying αποτελεί σημαντικό εργαλείο για τη διατήρηση της ανωνυμίας και της ιδιωτικότητας των χρηστών. Η γενική λειτουργία ενός proxy server έγκειται στην τοποθέτηση του ανάμεσα στον χρήστη και σε οποιαδήποτε εξωτερική αλληλεπίδραση που αυτός μπορεί να έχει με το διαδίκτυο. Έτσι, σε εφαρμογές ανώνυμων επικοινωνιών, ένας Web Server που εξυπηρετεί τα αιτήματα του χρήστη, μπορεί να δει μόνο την IP Address του Proxy Server και όχι αυτή του πραγματικού χρήστη, με αποτέλεσμα να μη μπορεί να συγκεντρώσει πληροφορίες για την πραγματική ταυτότητα και τοποθεσία του χρήστη. Η γενική λειτουργία ενός anonymous proxy server φαίνεται στην παρακάτω εικόνα. [2]



Σχήμα 2.20: Λειτουργία του Anonymizer.

Ο proxy server είναι μια πολύ δημοφιλής μέθοδος για την παράκαμψη περιορισμών στην πρόσβαση περιεχομένου από παρόχους (για παράδειγμα πρόσβαση σε περιεχόμενο πλατφόρμας streaming το οποίο δεν προορίζεται για τη χώρα διαμονής του χρήστη) ή λόγω λογοκρισίας από τις κρατικές αρχές (για παράδειγμα απαγόρευση χρήσης του Facebook από τους πολίτες της Κίνας, λόγω σχετικού νόμου στη χώρα). Φυσικά, ακόμα και με τη χρήση ενός proxy server, τα δεδομένα θα συνεχίσουν να περνάνε από τον Πάροχο Υπηρεσιών Internet (ISP-Internet Service Provider), ο οποίος φυσικά θα έχει πλήρη εικόνα για την IP Address του χρήστη. [154] Με άλλα λόγια, ο ίδιος ο ISP ή ένας κακόβουλος χρήστης που συλλαμβάνει πακέτα στη διαδρομή από και προς τον ISP , μπορεί να προβεί σε ανάλυση της διαδικτυακής κυκλοφορίας μιας συγκεκριμένης IP Address και κατά συνέπεια να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες. Η παράκαμψη περιορισμών πρόσβασης σε ιστότοπους λόγω τοποθέτησης γεωγραφικών ή κυβερνητικών περιορισμών μέσω proxy server βασίζεται φυσικά στην ανωνυμία του χρήστη και φαίνεται στο παρακάτω απλό παράδειγμα. [146]



Σχήμα 2.21: Λειτουργία ενός Proxy Server.

Οι φοιτητές της σχολής, η οποία απαγορεύει την πρόσβαση των χρηστών του δικτύου της στον ιστότοπο του Facebook, μπορούν να χρησιμοποιούν διακομιστές μεσολάβησης για να παρακάμψουν τον περιορισμό αυτό. Ο proxy server τους βοηθά να αποκρύψουν ουσιαστικά την κίνηση τους, καθώς στην κίνηση του δικτύου που φτάνει στο Firewall, εμφανίζονται requests προς αυτόν και όχι προς τους web servers του Facebook. [148] Ωστόσο, με τη σύνδεση σε διακομιστές μεσολάβησης, ενδέχεται να υπάρξει κίνδυνος έκθεσης ευαίσθητων πληροφοριών των χρηστών, όπως προσωπικές φωτογραφίες και κωδικοί πρόσβασης στον διαχειριστή του διακομιστή μεσολάβησης, ειδικά όταν αυτός είναι αμφιβόλου αξιοπιστίας. Για την αντιμετώπιση του παραπάνω φαινομένου, υπάρχουν firewall rules που αποκλείουν διακομιστές μεσολάβησης, προκειμένου να αποτρέψουν τους χρήστες από τη χρήση τους για να παρακάμψουν το φίλτρο. [151]

Το Anonymizer αποτελεί μια εμπορική λύση VPN η οποία στόχο έχει να καταστήσει ανώνυμη τη δραστηριότητα ενός χρήστη στο Internet. [147] Η ανωνυμία επιτυγχάνεται πάλι με τη χρήση ενός proxy server, ο οποίος ονομάζεται anonymous proxy, μέσω του οποίου διέρχεται ολόκληρη η κίνηση του χρήστη. Ο anonymous proxy αναλαμβάνει ως ενδιάμεσος server ολόκληρη την επικοινωνία του χρήστη με το υπόλοιπο Διαδίκτυο, προσφέροντας ένα ασφαλές, κρυπτογραφημένο κανάλι επικοινωνίας, με στόχο να υπάρξει προστασία των προσωπικών δεδομένων του χρήστη καθώς και οποιονδήποτε στοιχείων και πληροφοριών μπορούν να οδηγήσουν σε ταυτοποίηση και τον εντοπισμό του τερματικού του. [81] Πρόκειται επί της ουσίας για ένα single-point system, καθώς σε αντίθεση με το onion routing, η κίνηση διέρχεται μόνο μέσω του anonymous server, αντί των πολλαπλών επιπέδων που παρέχουν οι onion routers. Όπως γίνεται εύκολα αντιληπτό, το Anonymizer προσφέρει μικρότερο επίπεδο ασφάλειας και ανωνυμίας από το onion routing, ωστόσο προσφέρει λιγότερο latency, καθώς η κίνηση διέρχεται μόνο μέσω ενός σημείου και όχι μέσω διαδοχικών onion routers οι οποίοι χωρίζονται από μεγάλη φυσική απόσταση και επιβαρύνονται από κίνηση πολλών χρηστών.

Τα τρια βασικά δομικά στοιχεία του Anonymizer είναι τα εξής:

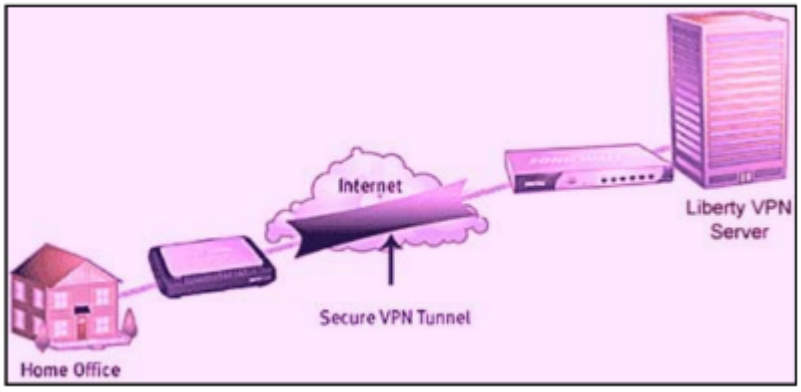
- Anonymizer Client: εμπορικό software το οποίο εγκαθίσταται στο τερματικό του χρήστη προκειμένου να επιτευχθεί η ανώνυμη διακίνηση των δεδομένων του.
- Anonymizer Server: αποτελείται από έναν Reverse Proxy/NAT Server, διαδοχικούς SSH Servers και Web Proxies. Οι SSH Servers και Web Proxies χρησιμοποιούνται για τον διαμοιρασμό του φορτίου της κίνησης (load balancing). Ολόκληρη η κρυπτογραφημένη TCP κίνηση του client σε πρωτόκολλα POP3, SMTP, FTP και HTTP διακομίζεται σε έναν SSH

server μέσω ενός SSH tunnel. Στη συνέχεια η κίνηση αποκρυπτογραφείται και προωθείται σε έναν Web Proxy.

- Destination Server: όλες οι TCP εφαρμογές υλοποιούνται σε αυτόν τον server. [81]

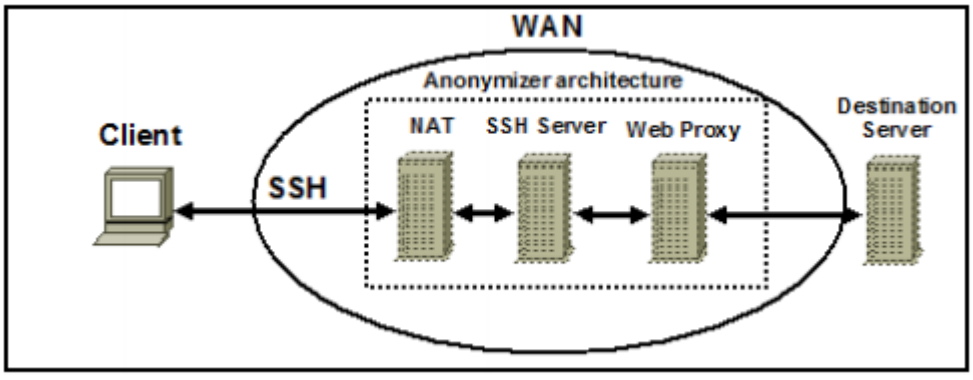
Το μέγεθος των HTTP πακέτων είναι δυναμικό και υπάρχει μεγάλη τυχαιότητα, εξαρτώμενη από τον client. Έχει αποδειχθεί ότι η αρχιτεκτονική του Anonymizer είναι ευάλωτη σε κρυφές επιθέσεις που βασίζονται στην ανάλυση του μεγέθους πακέτου, γεγονός που υπονομεύει την ανωνυμία των επικοινωνιών.

Η πιο ευρέως γνωστή εφαρμογή Anonymizer είναι μέσω της Protocol-independent εκδοχής τους. Εδώ, υλοποιείται σύνδεση του client στον Anonymizer μέσω ενός tunnel, με χρήση διαφόρων τεχνολογιών, μεταξύ των οποίων είναι τα SOCKS, PPTP, και OpenVPN. Σε αυτή την περίπτωση, το εξειδικευμένο λογισμικό είναι αναγκαίο να υπάρχει στη μεριά του client, προκειμένου να υλοποιηθεί η προώθηση όλης της κίνησης προς το tunnel. Η παρακάτω εικόνα περιγράφει παραστατικά τον τρόπο με τον οποίο επιτυγχάνεται η ανώνυμη, κρυπτογραφημένη σύνδεση μέσω μιας VPN εφαρμογής. [19]



Σχήμα 2.22: Λειτουργία ενός VPN.

Ο Anonymizer μπορεί επίσης να είναι Protocol-specific, που σημαίνει ότι έχουν τη δυνατότητα να λειτουργούν μόνο για κίνηση μέσω ενός συγκεκριμένου πρωτοκόλλου. Σε αυτή την περίπτωση, υπάρχει το πλεονέκτημα ότι δε χρειάζεται να εγκατασταθεί συγκεκριμένο λογισμικό στη μεριά του χρήστη. Ο client επικοινωνεί απευθείας με τον Anonymizer, με τις αναγκαίες εντολές να περιλαμβάνονται μέσα στο μήνυμα που διακινείται. Εν συνεχεία, ο Anonymizer αφαιρεί τον εντολή που απευθύνεται σε αυτόν και προωθεί το μήνυμα για την ανάκτηση του ζητηθέντος πόρου.



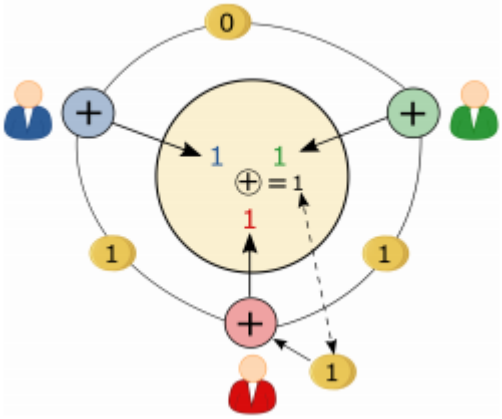
Σχήμα 2.23: Αρχιτεκτονική του Anonymizer.

2.2.2 DC-Net

Keywords: ***Peer-To-Peer, Mixes***
Maturity: ***Common***

Το Dining Philosophers Network (DC-Net) είναι ένα πρωτόκολλο ανώνυμης ανταλλαγής μηνυμάτων που προτάθηκε από τον Chaum το 1988. [13] Μεταγενέστερα πρωτόκολλα όπως το Herbivore βασίστηκαν στο DC-Net, προσφέροντας μεγαλύτερες δυνατότητες κλιμάκωσης. Το 2010 προτάθηκε το Dissent, ένα group messaging protocol το οποίο παρέχει αποδεδειγμένη ανωνυμία, υποστηρίζοντας ομάδες άνω των 40 χρηστών. Η υλοποίηση του Dissent βασίζεται στην Python και στο OpenSSL με χρήση κρυπτογραφίας δημόσιου κλειδιού.

Στο DC-Net κάθε συμμετέχοντας μοιράζεται με τους υπόλοιπους, ανά ζεύγη, μυστικά coin flips. Η ισοτιμία των coin flips που έχει δει ο κάθε συμμετέχοντας ανακοινώνεται σε όλους τους υπόλοιπους, και καθώς το κάθε coin flip έχει ανακοινωθεί δύο φορές, μια από κάθε έναν από το εκάστοτε ζεύγος συμμετεχόντων, η συνολική ισοτιμία για κάθε ένα θα πρέπει να είναι ζυγός αριθμός. Κάθε συμμετέχοντας, προκειμένου να στείλει ένα μήνυμα, δηλώνει εσφαλμένη τιμή για την εκάστοτε ισοτιμία του coin flip, καθιστώντας την μονό αριθμό, πράγμα που σημαίνει το μετάδοση ενός bit. Με αυτό τον τρόπο, κανένας συμμετέχοντας δε γνωρίζει τον αποστολέα του μηνύματος, εκτός αν όλοι όσοι συμμετείχαν σε coin flips με τον αποστολέα αποκαλύψουν μεταξύ τους τις ισοτιμίες τους.

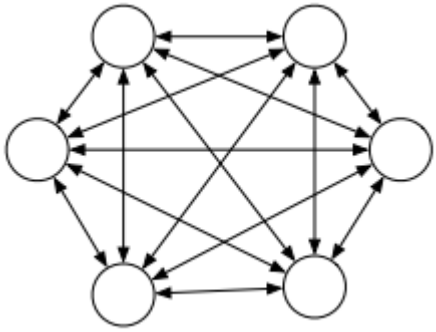


Σχήμα 2.24: DC Net.

Η πιο δημοφιλής τοπολογία του DC-Net είναι το DC-Ring, επειδή προσφέρει μια καλή σχέση επιδόσεων-προστασίας της ανωνυμίας των χρηστών του. [26] Ο βασικός λόγος είναι ότι χρειάζεται μειωμένο overhead για τις επικοινωνίες των συμμετεχόντων, καθώς δεν είναι όλοι οι κόμβοι γειτονικοί μεταξύ τους και δε χρειάζεται να ανταλλάξουν όλοι με όλους τις αντίστοιχες ισοτιμίες των coin flips τους. Η αρχή λειτουργίας του προκειμένου να διασφαλίζεται η ανωνυμία, που είναι άλλωστε και το βασικό ζήτημα, είναι να μην υπάρχουν αποχωρήσεις των χρηστών από το δίκτυο. Αυτό ωστόσο, στα σύγχρονα δίκτυα επικοινωνιών δεν είναι εύκολα εφαρμόσιμο, αφού η συμμετοχή ενός κόμβου σε μια ομάδα μπορεί να σταματήσει λόγω επανεκκινήσεων των συστημάτων, να υπάρξουν διαχωρισμοί του δικτύου (network partitions) αλλά και να προστεθούν νέα μέλη. Έτσι, δε μπορεί να εξασφαλιστεί ούτε η συμμετοχή ενός συγκεκριμένου κόμβου, ούτε φυσικά και να καθοριστεί ο ακριβής αριθμός των συμμετεχόντων peers σε κάθε ομάδα.

Η αμέσως επόμενη πιο δημοφιλής εκδοχή του DC-Net είναι το DC-Clique, όπου έχουμε πλήρη γειτνίαση όλων των peers με όλους τους υπόλοιπους. Αυτή η τοπολογία, όπως θα δούμε και παρακάτω, προσφέρει ισχυρά πλεονεκτήματα έναντι συγκεκριμένων τύπων επιθέσεων,

παρουσιάζοντας ωστόσο σοβαρές και αναπότρεπτες αδυναμίες σε άλλες. [20] Σε θέματα επιδόσεων, το βέβαιο είναι ότι το DC-Clique εισάγει πολύ μεγάλο overhead το οποίο αυξάνει κατακόρυφα τον φόρτο εργασίας των peers, καθιστώντας δυνατή τη χρήση της συγκεκριμένης τοπολογίας μόνο σε δίκτυα που απαρτίζονται από περιορισμένο αριθμό χρηστών, έτσι ώστε η καθυστέρηση και ο απαιτούμενος όγκων διαχειριστικού φόρτου να βρίσκεται σε λελογισμένα επίπεδα. Παρακάτω φαίνεται η λογική τοπολογία του DC-Clique.

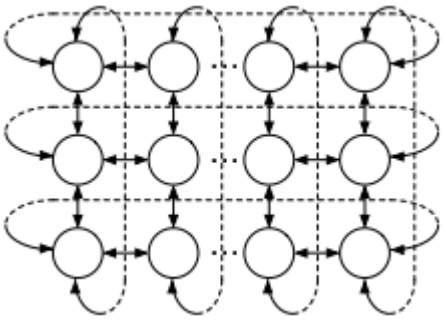


Σχήμα 2.25: DC Clique.

Μεταξύ των δύο αυτών τοπολογιών, έχουν προταθεί και διάφορες ενδιάμεσες λύσεις, προκειμένου να επιτευχθεί το βέλτιστο trade-off μεταξύ λειτουργικότητας του δικτύου και εξασφάλισης της ανωνυμίας των χρηστών. Η λογική πίσω από τις λύσεις αυτές είναι να εκκινεί το δίκτυο με τοπολογία DC-Ring και σταδιακά να προστίθενται σχέσεις γειτνίασης, παρατηρώντας τον φόρτο το δικτύου και την καθυστέρηση ώστε αυτή να μην υπερβεί κάποια συγκεκριμένα όρια. Η αναλογία του φόρτου εργασίας που επωμίζεται κάθε κόμβος είναι ανάλογη των γειτόνων του, ενώ σχετικά με την ασφάλεια του δικτύου, αυτή αυξάνεται με πολύ μεγαλύτερο ρυθμό.

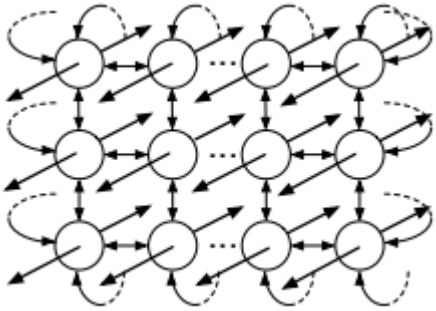
Το βασικό ζήτημα που ανακύπτει είναι η δράση που θα πρέπει να ακολουθηθεί όταν κάποιος κόμβος εισέρχεται ή αποχωρεί στο δίκτυο, καθώς στη μεν πρώτη περίπτωση πρέπει να σχηματιστούν νέες σχέσεις γειτνίασης, στη δε δεύτερη υπάρχει απώλεια του κόμβου που αποχωρεί από τις σχέσεις γειτνίασης που έχει συνάψει με τους υπόλοιπους. Έχουν προταθεί διάφορες λύσεις για το συγκεκριμένο ζήτημα, όπως η δημιουργία νέων σχέσεων γειτνίασης όταν εισέρχεται ένας νέος κόμβος και η σύναψη αιχμών (edges) μεταξύ των εκάστοτε γειτόνων ενός αποχωρούντος κόμβου. Η πιο ενδεδειγμένη ωστόσο λύση, για την εξασφάλιση του δικτύου από επιθέσεις, είναι η περιοδική επαναφορά του πρωτοκόλλου έτσι ώστε ο κάθε κόμβος να αποκτά ανά τακτά διαστήματα ένα νέο, τυχαίο σετ γειτόνων, με μικρό μάλιστα επιπλέον διαχειριστικό κόστος. [31]

Μια παραλλαγή του DC-Net είναι το DC-Torus, στην οποία κάθε κόμβος μοιράζεται coin flips με 4 μόνο γείτονες του σε ένα x-επι-z πλέγμα. Στα edges που σχηματίζονται, το πλέγμα αναδιπλώνεται σχηματίζοντας στην ουσία έναν δακτύλιο (Torus) στην οποία κανένας κόμβος δεν έχει λιγότερους από 4 γείτονες, όπως φαίνεται παρακάτω. [26]



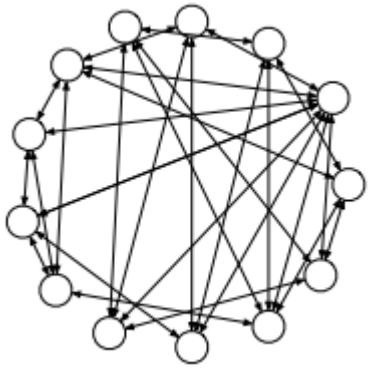
Σχήμα 2.26: DC Torus.

Το DC-Cube αποτελεί επέκταση του DC-Torus σε μια τρίτη διάσταση, έτσι ώστε κάθε κόμβος να έχει πλέον όχι 4 αλλά 6 γείτονες. Σε αυτή την περίπτωση έχουμε έναν κύβο, ο οποίος σχηματίζεται με αναδίπλωση των edges που σχηματίζονται, όπως φαίνεται στην εικόνα. [26]



Σχήμα 2.27: DC Cube.

Τέλος, το DC-Random είναι μια τοπολογία στην οποία ο κάθε κόμβος επιλέγει τυχαία άλλους κόμβους, κατ ελάχιστους i στο πλήθος και με μέγιστο όριο j κόμβους, με τους οποίους θα ανταλλάξει coin flips. Κάθε κόμβος έχει τη δυνατότητα να απορρίψει άλλους κόμβους, σε περίπτωση που ο ίδιος έχει ήδη συνάψει σχέσεις γειτνίασης με j άλλους κόμβους. Η διαδικασία συνεχίζεται έως ότου συναφθούν τουλάχιστον i γειτνιάσεις για κάθε κόμβο. Εδώ, κάθε κόμβος πρακτικά εξετάζει πρώτα πόσες σχέσεις μπορεί να συνάψει από τα δικά του αιτήματα γειτνίασης πρώτα και στη συνέχεια εξετάζει τα εναπομείναντα αιτήματα γειτνίασης από άλλους κόμβους. Κόμβοι που σε διαδοχικούς γύρους του απευθύνουν αιτήματα γειτνίασης θεωρούνται ύποπτοι ως κακόβουλοι. Η λογική τοπολογία του DC-Random παρατίθεται στην παρακάτω εικόνα. [26]



Σχήμα 2.28: DC Random.

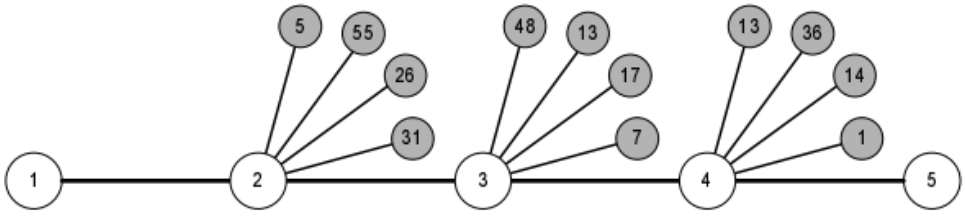
Η DC-Random είναι η πιο ευέλικτη εναλλακτική τοπολογία του DC-Net, από αυτές που παρουσιάστηκαν, καθώς είναι ευκολότερο να υλοποιηθεί σε σχέση με τις Torus και Cube, καθώς δεν είναι βέβαιο ότι θα μπορέσει να υπάρχει πάντα συμμετρία των κόμβων του δικτύου για να χτιστεί ένα Torus ή ένα Cube, ενώ είναι και αποδοτικό σε θέματα φόρτου εργασίας. [20]

2.2.3 MorphMix

Keywords: ***Peer-To-Peer, Mixes, Morphing***
Maturity: ***Proof of Concept***

Το MorphMix είναι μια τεχνολογία μεταγωγής κυκλώματος που αποτελείται από πολλούς κόμβους, οι οποίοι ονομάζονται MorphMix Clients. Οι κόμβοι αυτοί λειτουργούν τόσο ως Initiators όσο και ως Routers που δρομολογούν πακέτα στο δίκτυο. Κάθε κόμβος διατηρεί ένας περιορισμένο αριθμό εικονικών συνδέσμων (virtual links) προς γειτονικούς κόμβους μέσω TCP συνδέσεων. Κάτι που διαφοροποιεί το MorphMix από τις υπόλοιπες τεχνολογίες ανωνύμων επικοινωνιών είναι ότι το μονοπάτι που χρησιμοποιεί ένας κόμβος για μια σύνδεση του κατασκευάζεται επαναληπτικά από τους υπόλοιπους κόμβους στο δίκτυο. [157] Το μονοπάτι αυτό είναι ένα anonymous tunnel, και αποτελείται από τον κόμβο που εγκαθιστά τη σύνδεση, τον initiator και προαιρετικά, από έναν ή περισσότερους ενδιάμεσους κόμβους, καθώς και τον τελευταίο κόμβο του anonymous tunnel.

Για την προστασία της ανωνυμίας των χρηστών του δικτύου, το MorphMix χρησιμοποιεί, όπως και το Onion Routing, πακέτα σταθερού μήκους και διαδοχικά στρώματα κρυπτογράφησης σε κάθε κόμβο του anonymous tunnel, προκειμένου να είναι ανθεκτικό ενάντια σε Traffic Analysis Attacks και να προστατεύσει το περιεχόμενο των πακέτων. Όταν ένας κόμβος a επιθυμεί να εγκαταστήσει μια σύνδεση, μοιράζεται πρώτα ένα κοινό κλειδί με τους γειτονικούς του κόμβους, οι οποίοι θα αναλάβουν την κρυπτογράφηση των διακινούμενων κατά μήκος της διαδρομής πακέτων. Υποθέτοντας ότι ο πρώτος κατά σειρά κόμβος είναι ο b, ο a ζητάει από τον b να προτείνει μια σειρά από γειτονικούς προς τον b κόμβους οι οποίοι μπορούν να χρησιμοποιηθούν ως next hop. Από τους κόμβους που προτείνει ο b, ο a επιλέγει έναν κόμβο, υποθετικά τον c. Ο a εγκαθιστά ένα συμμετρικό κλειδί κρυπτογράφησης με τον c δια μέσω του b, το οποίο θα χρησιμοποιηθεί για την κρυπτογράφηση των μηνυμάτων. [2]



Σχήμα 2.29: Αναζήτηση κόμβων για τον σχηματισμό του anonymous tunnel στο MorphMix.

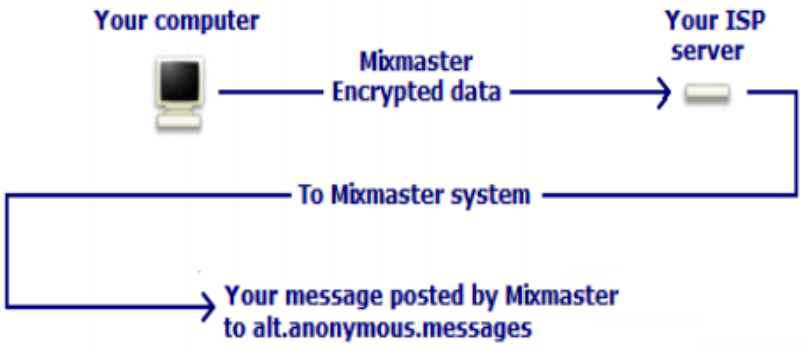
Προκειμένου να διασφαλιστεί ο a από έναν corrupt b node ο οποίος ενδέχεται να υλοποιήσει κάποια man-in-the-middle attack, ο a επιλέγει έναν ήδη γνωστό και επιβεβαιωμένο κόμβο προκειμένου να εγκαταστήσει το συμμετρικό κλειδί με τον κόμβο c. Μόλις εγκατασταθεί η σύνδεση προς τον κόμβο c, ο a ζητάει από αυτόν ορισμένες προτάσεις από αυτόν, σχετικά με τον επόμενο κόμβο που θα αποτελέσει το next hop. [125] [157] Η διαδικασία αυτή συνεχίζεται μέχρι να ολοκληρωθεί το χτίσιμο του μονοπατιού. Ουσιαστικά, η δημιουργία του μονοπατιού βασίζεται στο reputation system του δικτύου, το οποίο διατηρείται αποκεντρωμένα από κάθε κόμβο, σχετικά με τους γείτονες του. Αυτό

επιτρέπει την επέκταση του δικτύου χωρίς να επιβαρύνεται από το πλήθος τον κόμβων που συμμετέχουν σε αυτό.

2.2.4 Mixmaster

***Keywords:* Client-Server, Email, Mixes**
***Maturity:* Limited Adoption**

Το Mixmaster αποτελεί ένα remailer σύστημα ανωνύμων επικοινωνιών. Είναι ευρέως χρησιμοποιούμενο, και αποτελείται από διαδοχικούς servers που έχουν στόχο τη διακίνηση ηλεκτρονικής αλληλογραφίας χωρίς να είναι δυνατή η αποκάλυψη της πηγής ή του προορισμού της σε τρίτους. Όλα τα μηνύματα έχουν ακριβώς το ίδιο μέγεθος, προκειμένου να καθίσταται δυσκολότερος ο διαχωρισμός τους μέσω ανάλυσης, ενώ κρυπτογραφούνται. Ο επιπλέον θόρυβος που χρησιμοποιείται για να φτάσει το μέγεθος που απαιτείται στο εκάστοτε mail δεν είναι τυχαίος, αλλά παράγεται βάσει ενός μυστικού που μοιράζονται ο αποστολέας με τον παραλήπτη. Έτσι, ο θόρυβος αυτός, ενισχύει εκτός από την ασφάλεια του μηνύματος, την ακεραιότητα των δεδομένων. Τέλος, έχει τη δυνατότητα αποστολής μεγάλων emails χωρίς τη χρήση ειδικού λογισμικού. [2] [3] [4]



Σχήμα 2.30: Λειτουργία του Mixmaster.

2.2.5 Rumor Riding

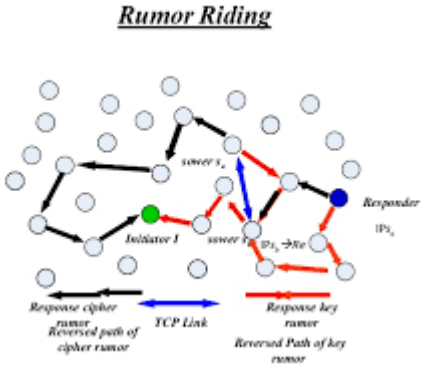
***Keywords:* Peer-To-Peer, CRC, AES**
***Maturity:* Proof of Concept**

Το Rumor Riding χρησιμοποιεί έναν AES αλγόριθμο για να κρυπτογραφήσει τα μηνύματα με ένα κλειδί μήκους 128 bits. Όταν ένας Initiator θέλει να ξεκινήσει μια ανώνυμη αναζήτηση, δημιουργεί το query content και ένα public key K. Στη συνέχεια κρυπτογραφεί το μήνυμα της αναζήτησης με το συμμετρικό κλειδί σε ένα κρυπτογραφημένο κείμενο και τα στέλνει σε διαφορετικούς γείτονες. Αυτά ακολουθούν διαφορετικά μονοπάτια, τα οποία αποκαλούνται rumors. Όταν τόσο το κλειδί όσο και το κρυπτογραφημένο κείμενο συναντηθούν σε κάποιον κόμβο τότε εκείνος είναι σε θέση να αποκρυπτογραφήσει το query. Η επιβεβαίωση γίνεται μέσω ενός Cyclid Redundancy Check (CRC) μηχανισμού, έτσι όταν ένας κόμβος αποκρυπτογραφήσει και τα δύο μηνύματα, μπορεί να ελέγξει την ορθότητα των αποτελεσμάτων. [2] [28]

Ο κόμβος που θα αποκρυπτογραφήσει με επιτυχία το μήνυμα μπορεί να απαντήσει στο query, κρυπτογραφώντας την απάντηση με το public key K του Initiator. Στη συνέχεια το κρυπτογραφεί χρησιμοποιώντας τον AES αλγόριθμο, στέλνοντας το κρυπτογραφημένο κείμενο και το κλειδί σε διαφορετικά rumors, αναθέτοντας δύο χαρακτηριστικά identifiers, το IDrK για το κλειδί και το IDrC

για το κείμενο. Τέλος, ο Initiator θα στείλει στον Responder ένα επιβεβαιωτικό μήνυμα λήψης απάντησης, χρησιμοποιώντας την ίδια διαδικασία. [35]

Το κύριο πρόβλημα που αντιμετωπίζει το δίκτυο είναι η ανάγκη αποθήκευσης κλειδιών και κειμένων, έως ότου μπορέσουν αυτά να ταιριάξουν και α αποκρυπτογραφηθεί το περιεχόμενο ενός query. Επίσης, είναι επιρρεπές σε Timing Attacks καθώς ο επιτιθέμενος εύκολα μπορεί να υλοποιήσει συσχετίσεις των χρόνων μεταξύ των πακέτων. Αντίθετα, είναι ιδιαίτερα ανθεκτικό απέναντι στις Predecessor Attacks.



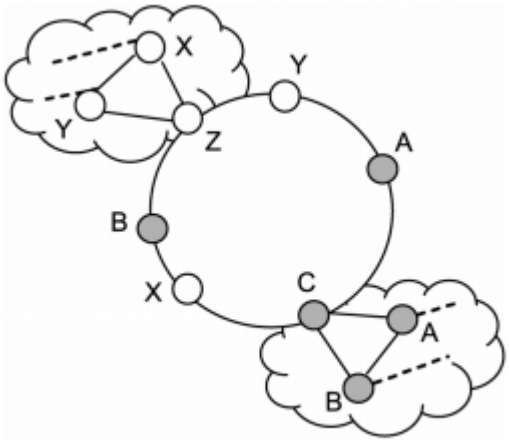
Σχήμα 2.31: Λειτουργία του Rumor Riding.

2.2.6 Agyaat

Keywords: ***Peer-To-Peer, Clouds, Services***
Maturity: ***Proof of Concept***

Πρόκειται για ένα αποκεντρωμένο σύστημα που διασφαλίζει την ανωνυμία των χρηστών χωρίς τη χρήση κάποιου κρυπτογραφικού σχήματος. Όταν ένας κόμβος θέλει να εισέλθει στο δίκτυο πρέπει να εισέλθει σε ένα ή περισσότερα μη δομημένα clouds, καθώς τα μηνύματα απευθύνονται σε clouds και όχι σε μεμονωμένους κόμβους. Η διαδικασία ξεκινά όταν το cloud του Initiator ξεκινάει μια τυχαία διαδρομή προκειμένου να αποκρύψει την ταυτότητα του. Το μήνυμα στη συνέχεια προωθείται στο rendezvous κόμβο του cloud του παραλήπτη, ο οποίος υλοποιεί broadcast του μηνύματος μέσα σε αυτό, αποκρύπτοντας την ταυτότητα του παραλήπτη. Για την αντιμετώπιση του φόρτου στο δίκτυο χρησιμοποιούνται πολλαπλά δομημένα overlays με ανεξάρτητα key spaces, τέτοια ώστε ένα cloud να έχει διαφορετικούς rendezvous κόμβους για κάθε overlay. [42]

Ο εντοπισμός των πόρων του δικτύου γίνεται με τρεις διαφορετικούς τρόπους. Ο πρώτος είναι ο semantic groups, όπου πόροι με παρόμοιο περιεχόμενο εντάσσονται στο ίδιο γκρουπ σε ένα cloud. Ο δεύτερος είναι το centralized directory service, το οποίο διευκολύνει τον εντοπισμό των πόρων ενώ ο τρίτος είναι τα dynamic services τα οποία εξυπηρετούν τον ίδιο σκοπό. Οι πόροι αντιστοιχούνται σε συγκεκριμένο cloud, ενώ υπάρχει ένας κεντρικός server ο οποίος αναλαμβάνει τη δεικτοδότηση τους.



Σχήμα 2.32: Agyaat Clouds.

2.2.7 AP3: Anonymous Peer-to-Peer Protocol

Keywords: ***Peer-To-Peer, Pseudonyms***
Maturity: ***Proof of Concept***

Το AP3 δομείται πάνω στο Pastry, με σχεδιασμό παρόμοιο με το Crowds, καθώς τα μονοπάτια δημιουργούνται με έναν στοχαστικό τρόπο, δημιουργώντας μονοπάτια συγκεκριμένου μεγέθους. Ο στοχαστικός τρόπος αυτός δυσκολεύει τον επιτιθέμενο στο να καθορίσει αν το προηγούμενο hop, δηλαδή ο κόμβος από τον οποίο έκανε intercept το πακέτο, είναι ο Initiator ή απλώς ένας ακόμη κόμβος. Παρά ταύτα, ο συνδυασμός των Predecessor Attacks με τις Timing Attacks μπορεί να δώσει πολύ καλά αποτελέσματα και να υπονομεύσει την ανωνυμία των χρηστών του δικτύου. [50]

Το πρωτόκολλο παροσφέρει Anonymous Message Delivery, Anonymous Channels και Secure Anonymous Pseudonyms μηχανισμούς για να εγγυηθεί την ανωνυμία των συμμετεχόντων. Για την αποστολή ενός ανώνυμου μηνύματος, δημιουργείται το περιεχόμενο του ενώ ταυτόχρονα γίνεται απόκρυψη των πληροφοριών που μπορούν να ταυτοποιήσουν τον Initiator. Στη συνέχεια το μήνυμα προωθείται σε έναν κόμβο που επιλέγεται τυχαία. Όταν φτάσει εκεί, υπάρχει μια coin-toss διαδικασία σχετικά με το αν το μήνυμα θα παραδοθεί στον τελικό αποδέκτη ή σε κάποιον άλλον ενδιάμεσο κόμβο. [69] Για το λόγο αυτό χρησιμοποιείται ένας forward probability μηχανισμός που επιτρέπει τη δημιουργία τυχαίων μονοπατιών που δημιουργούνται από έναν μεταβαλλόμενο αριθμό τυχαίων hops.

Το AP3 επιτρέπει τη χρήση ψευδώνυμων, καθώς κάθε χρήστης μπορεί να δημιουργήσει όσα ζεύγη κλειδιών επιθυμει, χωρίς κάποια Public Key Infrastructure (PKI). Έτσι, έχει τη δυνατότητα να δημιουργεί ψευδώνυμα τα οποία δεν μπορούν να συσχετιστούν μεταξύ τους. Ο χρήστης ενός ψευδώνυμου δημιουργεί ένα anonymous channel το οποίο πρέπει να ανανεώνει περιοδικά. [6] Κάθε μήνυμα που απευθύνεται σε συγκεκριμένο ψευδώνυμο κρυπτογραφείται με το αντίστοιχο public key, με αποτέλεσμα μόνο ο χρήστης του να μπορεί να το αποκρυπτογραφήσει. Το δίκτυο είναι ευάλωτο απέναντι σε Passive Attacks, οι οποίες έχουν αποδειχθεί εξαιρετικά επικίνδυνες για την ταυτοποίηση των χρηστών του.

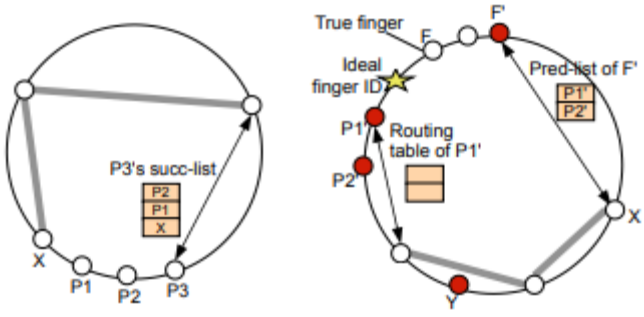
2.2.8 Octopus

Keywords: ***Peer-To-Peer, Dummy Traffic, Lookups***
Maturity: ***Proof of Concept***

Ο εν λόγω DHT lookup μηχανισμός εγγυάται τόσο την ανωνυμία όσο και την ασφάλεια των χρηστών, δίνοντας έμφαση στους μηχανισμούς έγκαιρου εντοπισμού και αφαίρεσης από το δίκτυο των κακόβουλων κόμβων. Χρησιμοποιεί Anonymous path construction μηχανισμούς για να κρύψει την ταυτότητα του Initiator, κάνει χρήση όλου του finger table προκειμένου να διαχωρίσει τα queries και να δημιουργήσει dummy κίνηση προκειμένου να προστατεύσει τον προορισμό του lookup και τέλος, χρησιμοποιεί secret security checks προκειμένου να αντιμετωπίσει την ύπαρξη κακόβουλων κόμβων στο δίκτυο.

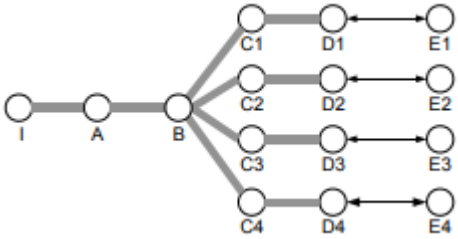
Για τη δημιουργία του random walk υπάρχει bound checking μηχανισμός και ταυτόχρονα οι παραπάνω μηχανισμοί εντοπίζουν κόμβους που επιχειρούν να τροποποιήσουν τα finger tables και τους αφαιρεί από το δίκτυο. Έτσι, διασφαλίζεται τόσο η ασφάλεια των χρηστών, όσο και η επεκτασιμότητα του δικτύου. Επιπλέον, υπάρχουν πολλαπλά ανώνυμα μονοπάτια στα lookups καθώς και προσθήκη dummy traffic προκειμένου να διασφαλίζεται η ανωνυμία τους από range estimation Attacks. [28]

Για την προστασία των finger tables υπάρχουν neighbour surveillance μηχανισμοί που επιτηρούν τους διάδοχους κόμβους έτσι ώστε να εντοπίζονται απόπειρες αλλαγής τους από κακόβουλους χρήστες. Κάθε κόμβος διατηρεί μια λίστα με τους προκάτοχους και τους διάδοχους κομβους. Περιοδικά ένας κόμβος n στέλνει ένα query προς έναν προκάτοχο κόμβο p προκειμένου να δει αν βρίσκεται στη λίστα του. [42] Ο p δε μπορεί να γνωρίζει την πηγή του query αυτού, με αποτέλεσμα αν αυτός προσπαθήσει να επηρεάσει το lookup να εντοπίζεται από τον κόμβο n, με αποτέλεσμα να αναφέρεται το συμβάν στη CA. Επίσης, κάθε routing table υπογράφεται από τον κάτοχο του για να διασφαλιστεί η ακεραιότητα τους.



Σχήμα 2.33: Λειτουργία του Octopus.

Το Octopus έχει πολύ καλά αποτελέσματα σε πειράματα που έχουν γίνει σχετικά με την ασφάλεια που προσφέρει. Ακόμα και με ποσοστά κακόβουλων κόμβων στο 20% επί του συνόλου καταφέρνει να έχει πολύ μικρή διαρροή πληροφοριών προς τον επιτιθέμενο. Τέλος, είναι πλήρως θωρακισμένο απέναντι σε Relay Exhaustion Attacks.



Σχήμα 2.34: Querying στο Octopus.

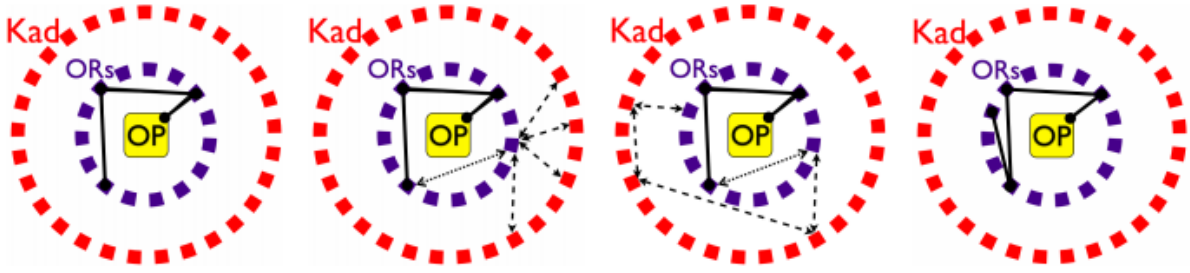
2.2.9 Torsk

Keywords: ***Peer-To-Peer, Lookups, Fingers, Buddies***
Maturity: ***Limited Adoption***

Το Torsk επιχειρεί να προσφέρει υψηλά επίπεδα ακεραιότητας και εμπιστευτικότητας στα lookups που υλοποιούνται μέσω του πρωτοκόλλου. Για τη δημιουργία των μονοπατιών χρησιμοποιούνται οι secret buddies, κόμβοι δηλαδή που λειτουργούν ως proxies κατά τη διάρκεια των lookups. [115] Κάθε κόμβος επιλέγει αρχικά τους buddies του από το δίκτυο και στη συνέχεια ο εκάστοτε Initiator επιλέγει κάποιον από αυτούς για να υλοποιήσει ένα lookup, έτσι ώστε να μην είναι δυνατή η συσχέτιση του με τον Responder. Κάθε φορά που ένας κακόβουλος κόμβος επιστρέφει ένα μη έγκυρο πιστοποιητικό η διαδικασία επιλογής buddies πρέπει να ξεκινήσει από την αρχή.

Το Torsk χρησιμοποιεί τον μηχανισμό lookups που υπάρχει στο Kademlia. Κάποιος Initiator που επιθυμεί να εντοπίσει έναν Responder x ξεκινάει την αναζήτηση επιλέγοντας τα κοντινότερα t fingers στον x από το Finger Table και τα χρησιμοποιεί σα σημεία εκκίνησης για t ανεξάρτητα lookups. Για κάθε ένα από αυτά ο Initiator διατηρεί μια λίστα με τα κοντινότερα fingers στον x. Σε κάθε επανάληψη τα t fingers που δεν είχαν επιλεχθεί πριν, αναλαμβάνουν να κάνουν queries στον x παράλληλα. Η διαδικασία συνεχίζεται έως ότου μια λίστα παραμείνει αμετάβλητη στο τέλος μιας επανάληψης. [120] [159]

Σημαντικό είναι ότι κάθε κόμβος διατηρεί ένα πιστοποιητικό που εκδίδεται από μια CA, το οποίο περιλαμβάνει όλα τα fingers, με αποτέλεσμα να είναι σε θέση να γνωρίζει αν οι απαντήσεις σε ένα query προέρχονται από honest ή malicious κόμβο. Ενάντια στο Torsk σχεδιάστηκαν οι Buddy Exhaustion Attacks, ένα είδος DoS Attack που αποκλείει έναν κόμβο από όλους τους honest buddies, έως ότου επιλέξει στη θέση τους malicious κόμβους. Οι επιθέσεις αυτές έχουν αρκετά καλές πιθανότητες να πετύχουν το στόχο τους, επειδή όπως προαναφέρθηκε, η διαδικασία εύρεσης νέων buddies ξεκινάει από την αρχή κάθε φορά που επιστρέφεται μη έγκυρο πιστοποιητικό, δίνοντας την ευκαιρία στον επιτιθέμενο να παρεμβάλει τους δικούς του κόμβους στη διαδικασία. Τέλος, το Torsk είναι ευάλωτο τόσο σε Passive όσο και σε Active Attacks για τον ίδιο ακριβώς λόγο.



Σχήμα 2.35: Torsk Operations.

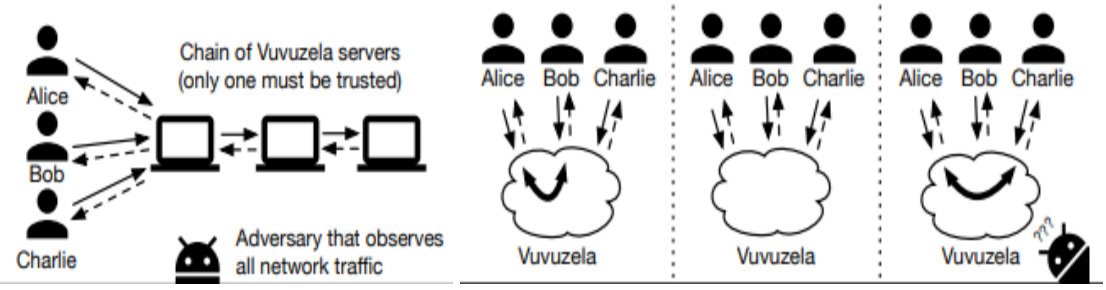
2.2.10 Bitfrost

***Keywords:* Peer-To-Peer, PSK**
***Maturity:* Proof of Concept**
Το Bitfrost διαχωρίζει τα Node Management (NML) και Anonymous Routing Layers (ARL). Έτσι, η διαχείριση των κόμβων παραμένει ανεξάρτητη από την ανωνυμία που προσφέρεται στο δίκτυο. Η αρχιτεκτονική του αποτελείται από πολλούς κόμβους και έναν Public Key Server (PKS) ο οποίος διαχειρίζεται τα δημόσια κλειδιά των κόμβων. Όταν ένας κόμβος επιθυμεί να εισέλθει στο δίκτυο τότε καταχωρεί το δημόσιο κλειδί του στον PKS. [2]

Χρησιμοποιεί το Chord για τη διαχείριση των κόμβων, οι οποίοι διατηρούν την IP Address μόνο του προκάτοχου και του διαδόχου κόμβου. Το ARL χρησιμοποιεί πολλαπλώς κρυπτογραφημένα μηνύματα. Για την αποφυγή Traffic Analysis Attacks ο παραλήπτης βρίσκεται περίπου στο μέσο της διαδρομής, ενώ ο Initiator επιλέγει τους ενδιάμεσους κόμβους. Χρησιμοποιούνται μηνύματα τύπου construction, data και control. Για κάθε κόμβο που κάνει seeding υπάρχει ένας Backup Node, ο οποίος είναι ο διάδοχος κόμβος του seeder. [150]

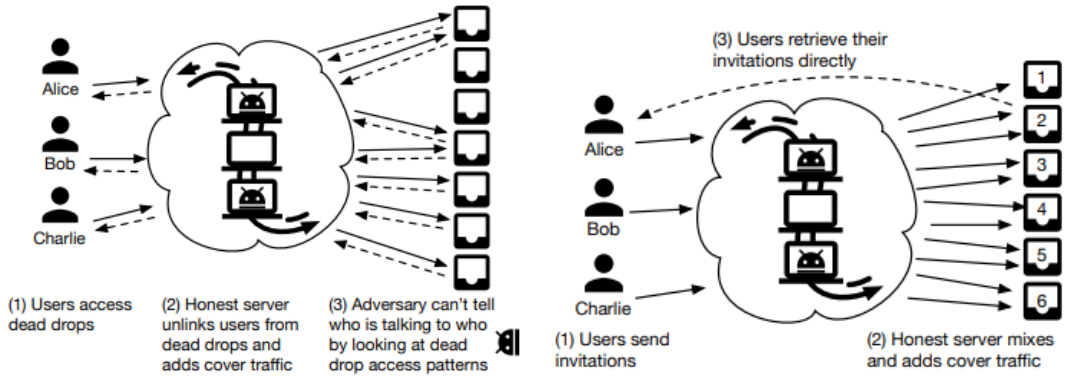
2.2.11 Vuvuzela

***Keywords:* Client-Server, Metadata, Proxies, Message Exchange**
***Maturity:* Proof of Concept**
Πρόκειται για ένα επεκτάσιμο messaging σύστημα το οποίο παρέχει ισχυρές δικλείδες ασφαλείας που διασφαλίζουν τόσο την ανωνυμία των δεδομένων όσο και των μεταδεδομένων, τα οποία μπορούν να αξιοποιηθούν από τους επιτιθέμενους για να αποκαλύψουν την ταυτότητα των συνομιλούντων. Αρκεί ένας server να είναι ασφαλής για να διαφυλάξει την ανωνυμία των χρηστών του δικτύου από έναν επιτιθέμενο που ελέγχει όλους τους υπόλοιπους exit nodes.



Σχήμα 2.36: Traffic Masking στο Vuvuzela.

Το δίκτυο ελαχιστοποιεί το πλήθος των μεταβλητών στοιχείων της δικτυακής κίνησης και των μεταδεδομένων, προσθέτοντας θόρυβο σε όσα υπάρχουν στο δίκτυο, αποτρέποντας έτσι τους επιτιθέμενους από την αξιοποίηση τους. Μπορεί να υποστηρίξει εκατομμύρια χρήστες και δεκάδες χιλιάδες μηνύματα ανά δευτερόλεπτο. Στις παρακάτω εικόνες παρουσιάζονται τα conversation και dialing πρωτόκολλα του δικτύου.



Σχήμα 2.37: Λειτουργία του Vuvuzela.

2.2.12 DP5

***Keywords:* Client-Server, Diffie-Hellman, Epochs, Ephemeral Secrets**
***Maturity:* Proof of Concept**

Πρόκειται για μια εξειδικευμένη τεχνολογία η οποία εστιάζει στην παροχή πληροφοριών σχετικά με την online παρουσία των χρηστών ενός κοινωνικού δικτύου με τρόπο τέτοιο ώστε να διασφαλίζεται η ανωνυμία τους. Η συμβατική αρχιτεκτονική υλοποίησης μιας τέτοιας λύσης απαιτεί έναν κεντρικό server ο οποίος περιέχει την πληροφορία αυτή αποθηκευμένη σε μια λίστα. Το DP5 χρησιμοποιεί κρυπτογραφικά σχήματα για να διατηρήσει το περιεχόμενο της προαναφερθείσας λίστας κρυφό.

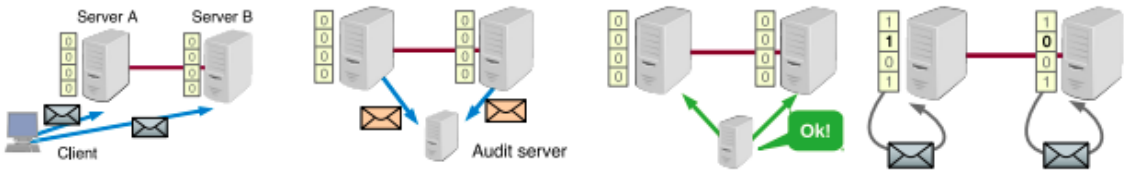
Στόχος του είναι να διασφαλίσει τόσο την ιδιωτικότητα όσο και την ακεραιότητα της παρουσίας των χρηστών στο δίκτυο, προστατεύοντας τόσο ολόκληρο τον γράφο ο οποίος περιέχει τους χρήστες όσο και τα μεταδεδομένα που διακινούνται σε αυτό και μπορούν να αποτελέσουν πηγή διαρροής πληροφοριών. Η κρυπτογράφηση υλοποιείται πάνω στο Diffie-Hellman πρωτόκολλο και βασίζεται στην ανταλλαγή ephemeral secrets δια μέσω κατανεμημένων servers υποδομής στο δίκτυο. Για την ανταλλαγή των secrets υλοποιούνται epochs, τα οποία υποδηλώνουν και την παρουσία των χρηστών στο δίκτυο. Χωρίζονται σε short term και long term. Το DP5 υποστηρίζει διάφορες παραμετροποιήσεις προκειμένου να επιτυγχάνεται το κατάλληλο trade-off που είναι επιθυμητό κάθε στιγμή. Η λύση είναι ιδανική για δίκτυα με περιορισμένο αριθμό χρηστών, όπου η προστασία της online κατάστασης των χρηστών είναι σημαντική. [177]

2.2.13 Riposte

***Keywords:* Client-Server, Online Messaging, Multi-Party Protocol, Distributed Point Function**
***Maturity:* Proof of Concept**

Το συγκεκριμένο δίκτυο αποτελεί μια λύση για anonymous online messaging το οποίο παρέχει προστασία τόσο ενάντια σε Traffic Analysis Attacks όσο και σε DoS Attacks, διατηρώντας τη δυνατότητα υποστήριξης εκατομμυρίων χρηστών. Η προστασία της ανωνυμίας των χρηστών επιτυγχάνεται μέσω της ανταλλαγής μυστικών μεταξύ τους, με παρόμοιο τρόπο όπως στο DC-Net. Επιπλέον, χρησιμοποιεί ένα multi-party protocol για τον γρήγορο εντοπισμό κακόβουλων client requests έτσι ώστε να προλαμβάνονται οι DoS Attacks. Τέλος, μέσω της distributed point function,

επιτυγχάνει την καλή επεκτασιμότητα του δικτύου. [178] Η αρχιτεκτονική του παρουσιάζεται στην παρακάτω εικόνα.



Σχήμα 2.38: Ανταλλαγή ηλεκτρονικής αλληλογραφίας στο Riposte.

2.2.14 Shadow Walker

Keywords: ***Peer-To-Per, Shadow Nodes, Lookups***
Maturity: ***Proof of Concept***

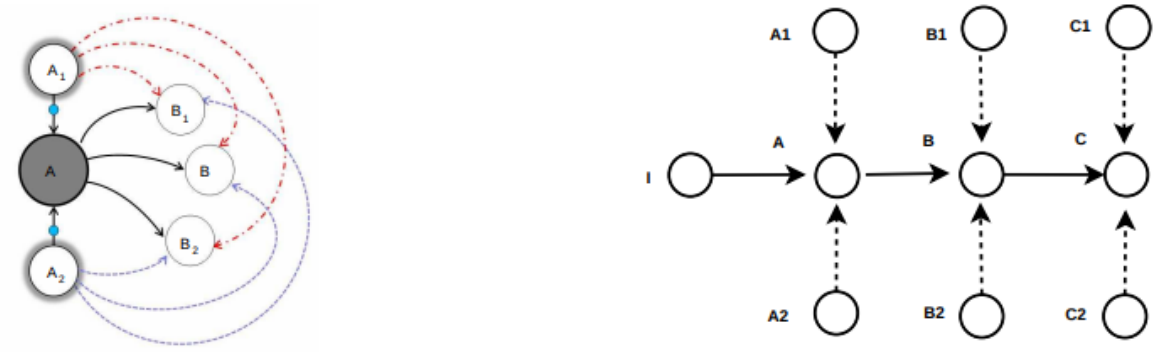
Πρόκειται για ένα σύστημα ανωνύμων επικοινωνιών που βασίζεται σε ένα random walk πάνω από πλεονάζουσες δομημένες τοπολογίες. Χρησιμοποιούνται shadow nodes οι οποίοι επιβεβαιώνουν αν το routing table ενός κόμβου είναι σωστό και το πιστοποιούν. Χρησιμοποιεί πιστοποιητικά προκειμένου να ελέγχει τα διαφορετικά στάδια ενός random walk ώστε να αποφευχθεί η διαρροή πληροφοριών στο δίκτυο. Τα Shadows είναι οι γειτονικοί κόμβοι που εγγυώνται για τις απαντήσεις των lookups, προσπαθώντας να παρεμποδίσουν κακόβουλους χρήστες να αποκτήσουν πρόσβαση σε αυτά. Παρέχουν ψηφιακές υπογραφες στα routing tables τα οποία χρησιμοποιούνται για τη δημιουργία των random walks και διατηρούν το DHT routing. [160]

Τα shadows κάθε κόμβου επιλέγονται τυχαία, καθιστώντας δύσκολο να είναι σε θέση ένας επιτιθέμενος να έχει πρόσβαση τόσο σε έναν κόμβο όσο και σε όλα τα shadows του. Με τον τρόπο αυτό αποτρέπονται οι Sybil Attacks. Περιοδικά κάθε κόμβος τρέχει ένα stabilization πρωτόκολλο έτσι ώστε να εντοπίζει τους σωστούς γείτονες του, κάτι που, λόγω της ύπαρξης των shadow κόμβων αυξάνει το κόστος του δικτύου σε πόρους.

Χρησιμοποιείται ένα ασφαλές lookup πρωτόκολλο το οποίο ξεκινάει όταν ένας κόμβος n επιθυμεί να εντοπίσει ένα identifier ID. Αν ο m είναι ο κοντινότερος κόμβος στο ID, ως προς το finger table, ο n θα υλοποιήσει ένα query (ερώτημα) προς τον m για το finger του p, το οποίο είναι ο εγγύτερος προκάτοχος κόμβος στο ID. Ο n γνωρίζει όλους τους shadows του m με αποτέλεσμα να μπορεί να επαληθεύσει αν οι απαντήσεις στο ερώτημα είναι ορθές. Η διαδικασία επαναλαμβάνεται έως ότου εντοπιστεί το ID. [160] Όσο έστω και ένα από τα shadows του m κόμβου είναι honest, τα αποτελέσματα του ερωτήματος θα είναι σωστά, έτσι για την επιτυχή υλοποίηση ενός ερωτήματος πρέπει να υπάρχει ένας τουλάχιστον honest κόμβος σε κάθε στάδιο του lookup. Η ασφάλεια του δικτύου βασίζεται στο γεγονός ότι είναι εξαιρετικά απίθανο ένας κακόβουλος χρήστης να αποκτήσει τον έλεγχο του συνόλου των κόμβων που αποτελούν ένα neighbourhood.

Το πρωτόκολλο έχει αποδειχθεί ευάλωτο απέναντι σε Collusion Attacks, αφού κάθε βήμα του lookup βασίζεται στο αμέσως προηγούμενο για να παρέχει honest shadows στον κόμβο που έχει σε εκείνο το στάδιο το ερώτημα. Έτσι, τυχόν κακόβουλοι κόμβοι μπορούν να τροποποιήσουν το δημόσιο κλειδί των υπόλοιπων κόμβων στο μονοπάτι αναζήτησης, επιστρέφοντας κακόβουλους κόμβους για να υλοποιηθούν τα εναπομείναντα στάδια. Αυτό πολύ εύκολα μπορεί να οδηγήσει στην αποκάλυψη της ταυτότητας του Initiator. Επίσης, οι επιθέσεις είναι ευάλωτες απέναντι σε end-to-end Timing Attacks.

Οι παραπάνω επιθέσεις μπορούν να συνδυαστούν με Denial of Service Attacks, επιφέροντας σημαντικά πλήγματα στην αξιοπιστία του δικτύου και στην προστασία της ανωνυμίας των χρηστών. Οι επιτιθέμενοι μπορούν να κάνουν compromise ολόκληρα neighbourhoods, πλήττοντας έτσι τον shadow μηχανισμό του δικτύου. Όταν ένας κακόβουλος κόμβος ερωτάται για έναν άλλον κόμβο στο δίκτυο, μπορεί να επιστρέψει ψευδή IDs τα οποία ανήκουν σε άλλους malicious κόμβους. Με μόλις 10% των κόμβων να είναι κακόβουλοι, ο επιτιθέμενος μπορεί να κάνει compromise πάνω από το 90% του αντίστοιχου κυκλώματος. Οι DoS Attacks επηρεάζουν τον αριθμό των υπογραφών που χρειάζεται ένας κόμβος για να συμμετέχει στην κατασκευή του κυκλώματος. Ένα lookup θεωρείται ασφαλές όταν ένας κόμβος παρέχει τουλάχιστον μια υπογραφή. Έτσι, αν ο επιτιθέμενος αποτρέπει τη συλλογή των υπογραφών αυτών, μέσω DoS Attacks μπορεί να αποτρέψει μια συγκεκριμένη υπογραφή από το να χρησιμοποιηθεί για την κατασκευή του κυκλώματος. [160]



Σχήμα 2.39: Σχηματισμός γειτνίασης στο Shadow Walker.

2.2.15 NISAN: Network Information Service for Anonymization Networks

Keywords: ***Peer-To-Peer, Diffie-Hellman, Aggregated Greedy Search, Hiding the Search Value, Bounds Checking in Finger Tables***
Maturity: ***Proof of Concept***

Το NISAN βασίζεται στο DHT, χρησιμοποιώντας τους Aggregated Greedy Search, Hiding the Search Value και Bounds Checking in Finger Tables μηχανισμούς για την αποτροπή κακόβουλων ενεργειών στο δίκτυο. Στον πρώτο μηχανισμό μια αναζήτηση ξεκινάει όταν ο Initiator v δημιουργεί ένα τυχαίο ID x και σε κάθε round επιλέγει τους εγγύτερους προς τον x κόμβους που εκείνος γνωρίζει, προκειμένου να στείλει το ερώτημα. Η αναζήτηση ολοκληρώνεται όταν η λίστα με τους εγγύτερους peers παραμείνει αμετάβλητη σε δύο διαδοχικές επαναλήψεις. Η γνώση αυτή είναι διαθέσιμη σε όλα τα διαφορετικά branches του δικτύου. Έχει αποδειχθεί ότι λειτουργεί καλά σε δίκτυα έως και 50,000 κόμβων.

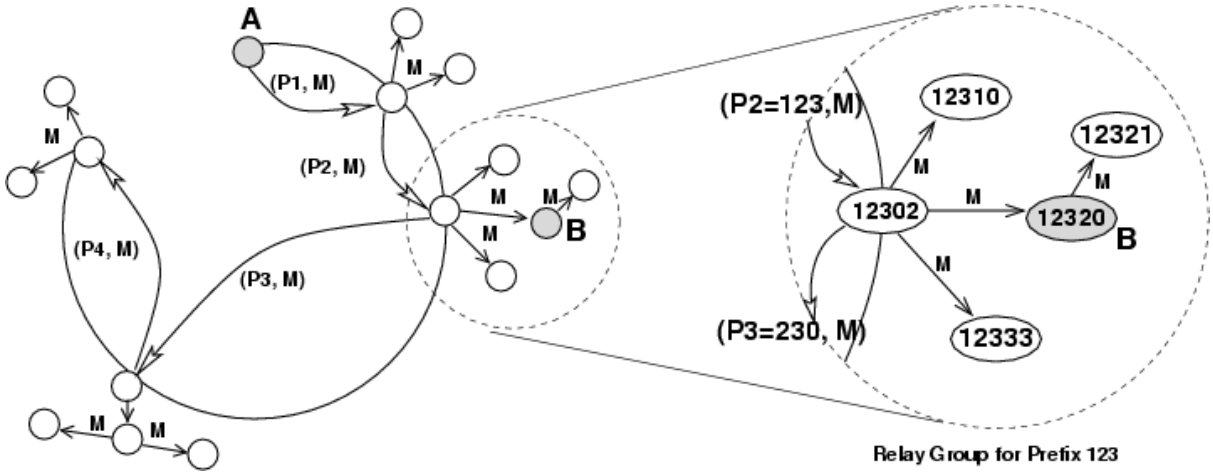
Ο Hiding the Search Value μηχανισμός επιτρέπει στον Initiator να ζητάει ολόκληρο το finger table αντί μόνο του ID x. Το finger table περιέχει $\log_2 N$ συνολικά καταγραφές, από τις οποίες η καλύτερη θα επιλεχθεί ως το επόμενο iteration. Η διαδικασία επαναλαμβάνεται έως ότου εντοπιστεί η κορυφή της λίστας ή ο εγγύτερος peer. Στη συνέχεια επιστρέφεται το αποτέλεσμα της αναζήτησης. Τέλος, ο Bounds Checking in Finger Tables μηχανισμός βοηθάει στον εντοπισμό colluding nodes στο δίκτυο. Υπολογίζεται η μέση απόσταση μεταξύ ενός ID στο finger table και του βέλτιστου ID, πολλαπλασιαζόμενη με έναν FT tolerance factor. Το παραπάνω τεστ επαναλαμβάνεται σε κάθε βήμα του lookup και μόνο οι κόμβοι που επιτυγχάνουν γίνονται δεκτοί. Το δίκτυο έχει καλές επιδόσεις όσον αφορά την ασφάλεια, ωστόσο αυτές φθίνουν όσο μεγαλώνει το μέγεθος του. [161]

2.2.16 Cashmere

Keywords: ***Peer-To-Peer, Relay Groups, Root***
Maturity: ***Limited Adoption***

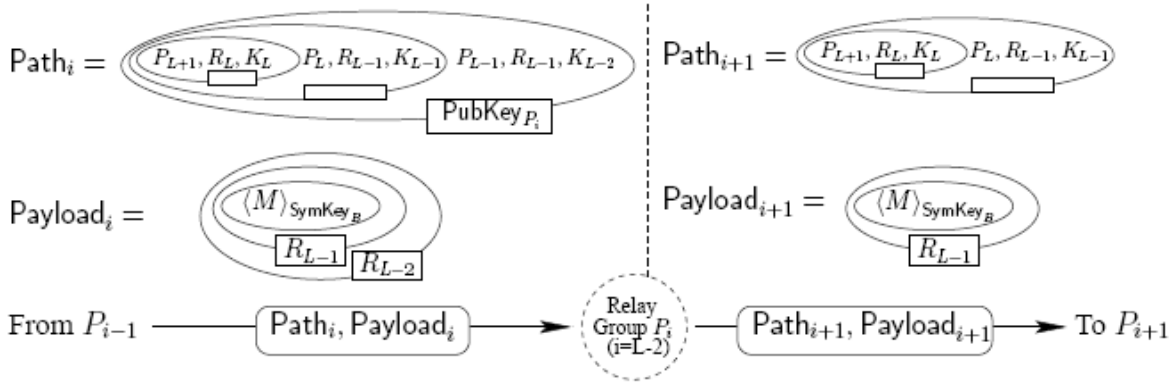
Το Cashmere είναι ένα anonymous routing layer που χρησιμοποιεί γκρουπ αναμεταδοτών (relay groups) αντί για mixes που αποτελούνται από έναν μόνο κόμβο προκειμένου να παρέχουν υψηλή διαθεσιμότητα υπηρεσίας. Κάθε relay group αποτελείται από ένα σετ κόμβων που μοιράζονται μεταξύ τους ένα κοινό public/private ζεύγος κλειδιών. Αυτό δίνει τη δυνατότητα σε κάθε μέλος του εκάστοτε relay group να υλοποιεί αποκρυπτογράφηση του μηνύματος που λαμβάνει ώστε στη συνέχεια να το προωθήσει στο επόμενο relay group.

Κάθε κόμβος στο Cashmere χαρακτηρίζεται από ένα μοναδικό nodeID, ενώ κάθε relay group έχει ένα επίσης μοναδικό groupID. Το groupID αποτελεί πρόθεμα όλων των nodeIDs που συμμετέχουν στο ίδιο relay group. Το Cashmere είναι δομημένο πάνω από το Pastry και κάνει χρήση του μηχανισμού anycast για τη δρομολόγηση ενός μηνύματος προς οποιοδήποτε κόμβο με το κατάλληλο groupID πρόθεμα. Ο κόμβος που παραλαμβανει το μήνυμα αποτελείται relay group root. Οι μηχανισμοί των πρωτοκόλλων του Pastry εγγυώνται ότι σε κάθε περίπτωση θα υπάρχει ένας relay group root, αρκεί σε κάθε relay group να υπάρχει τουλάχιστον ένας ενεργός κόμβος. [113]



Σχήμα 2.40: Relay Groups στο Cashmere.

Ο root αποκρυπτογραφεί το μήνυμα, το στέλνει μέσω broadcast σε όλους τους ενεργούς κόμβους που ανήκουν στο ίδιο relay group και στη συνέχεια στέλνει το μήνυμα στο επόμενο relay group, σύμφωνα με το μονοπάτι προώθησης. Ο τελικός παραλήπτης του μηνύματος μπορεί να βρίσκεται σε οποιοδήποτε relay group, όχι κατ ανάγκη στο τελευταίο. Ένας κόμβος αναγνωρίζει τον εαυτό του ως παραλήπτη όταν μπορεί να αποκρυπτογραφήσει το μήνυμα που λαμβάνει.



Σχήμα 2.41: Μετάδοση πακέτων στο Cashmere.

2.3 Unobservability-focused Τεχνολογίες

Πρόκειται για τεχνολογίες που στοχεύουν στην επιτυχή απόκρυψη της ταυτότητας και των χαρακτηριστικών όλων των εμπλεκομένων στην επικοινωνία μερών. Συγκεκριμένα, τόσο ο Initiator όσο και ο Receiver αλλά και τα διακινούμενα μηνύματα καθίστανται δυσδιάκριτα στην ανάλυση δικτυακής κίνησης που ενδεχομένως θα επιχειρήσει κάποιος κακόβουλος χρήστης.

2.3.1 Herbivore

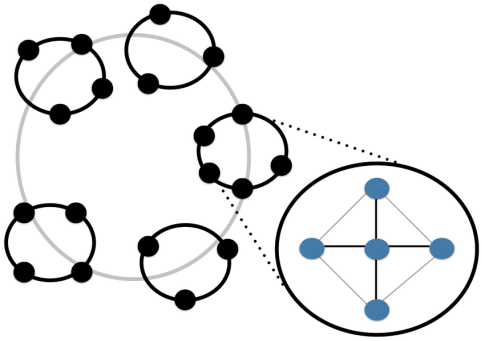
Keywords: ***Peer-To-Peer, Cliques, Puzzles***
Maturity: ***Limited Adoption***

Το Herbivore αποτελείται από ένα round πρωτόκολλο, σε συνδυασμό με έναν global topology control αλγόριθμο. Το πρωτόκολλο καθορίζει τη σειρά με την οποία τα bits αποστέλλονται στους συμμετέχοντες κόμβους, ενώ ο αλγόριθμος διαμοιράζει το δίκτυο σε μικρότερα κομμάτια που διασφαλίζουν την ανωνυμία, γνωστά ως anonymizing cliques. Οι κόμβοι εντός ενός clique διαρθρώνονται σε τοπολογία αστέρα και επικοινωνούν μεταξύ τους μέσω ενός κεντρικού κόμβου. Κάθε χρήστης διαθέτει ένα shared key με κάθε άλλο μέλος που συμμετέχει στο ίδιο clique. Τα cliques συνδέονται μεταξύ τους σε τοπολογία δακτυλίου, η οποία επιτρέπει τη μεταξύ τους επικοινωνία.

Κάθε νέος κόμβος που εισέρχεται στο Herbivore εντάσσεται σε ένα clique, κάθε ένα εκ των οποίων έχει τουλάχιστον k κόμβους. Ο όρος k είναι και αυτός που καθορίζει το επίπεδο ανωνυμίας που προσφέρει το Herbivore. Η διαχείριση των cliques γίνεται από τον αλγόριθμο, ο οποίος εγγυάται ότι ο αριθμός k παραμένει πάντα εντός ορισμένων ανεκτών ορίων. Έτσι, αν το k μεγαλώσει σημαντικά, οι cliques χωρίζονται σε μικρότερες έτσι ώστε να αποφευχθούν καθυστερήσεις στο δίκτυο, ενώ αν το k μειωθεί, γιατί αποχώρησαν κόμβοι από τα cliques, τότε υλοποιείται συνένωση αυτών προκειμένου να εξασφαλιστεί επαρκής προστασία της ανωνυμίας των συμμετεχόντων στο Herbivore. Επιπροσθέτως, προκειμένου να αποφευχθεί η εισαγωγή νεοεισελθέντων κόμβων σε τυχαίες cliques, το Herbivore επιστρατεύει ορισμένα υπολογιστικά puzzles. [15]

Το Herbivore εξασφαλίζει σημαντική κλιμάκωση στο δίκτυο, καθώς κάθε clique μπορεί να φιλοξενήσει ως και 128 κόμβους. Αυτό βέβαια καθιστά επιρρεπές το δίκτυο σε Denial of Service Attacks, καθώς είναι πολύ πιθανό ένας επιτιθέμενος να καταφέρει να ελέγξει έναν από τους συμμετέχοντες κόμβους σε κάθε clique. Στην περίπτωση μιας επιτυχημένης DoS Attack, όπου οι

κόμβοι ενός clique δε θα μπορούν να επικοινωνήσουν, ο αλγόριθμος προβλέπει τη μεταφορά τους σε κάποια άλλη clique, αυτό ωστόσο καθιστά το δίκτυο επιρρεπές σε Intersection Attacks.



Σχήμα 2.42: Herbivore.

2.3.2 P5 - Peer-to-Peer Personal Privacy Protocol

Keywords: ***Peer-To-Peer, Root, Leaf***
Maturity: ***Proof of Concept***

Το P5 διαστρωματώνεται σε διαφορετικά επίπεδα ιεραρχίας, τα οποία παρέχουν διαφορετικά επίπεδα ανωνυμίας. Διαθέτει επαυξημένες δυνατότητες κλιμάκωσης ως δίκτυο, ωστόσο παρουσιάζει περιορισμούς στην αποδοτικότητα, το bandwidth και την αξιοπιστία. Οι κόμβοι επικοινωνούν μεταξύ τους στέλνοντας μηνύματα πάνω από το πρωτόκολλο, κάτι που εγγυάται την ανωνυμία τόσο των clients όσο και των servers. [2]

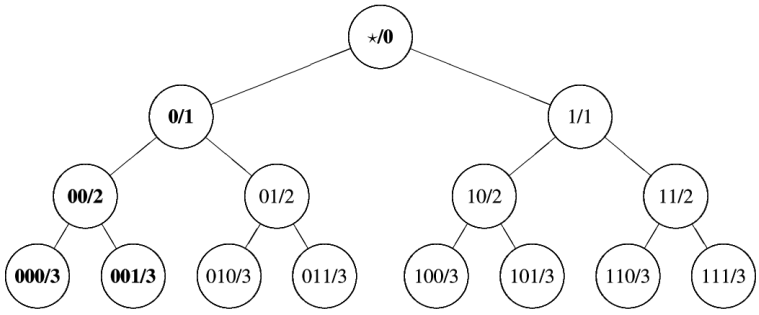
Το πρωτόκολλο παρέχει τη δυνατότητα στους χρήστες να επιλέξουν την καταλληλότερη για εκείνους σχέσεις ανωνυμίας-επιδόσεων του δικτύου, υλοποιώντας μεγάλα δίκτυα στα οποία οι χρήστες επιλέγουν το επίπεδο ιεραρχίας στο οποίο θέλουν να ανήκουν. Κάθε κόμβος στο δέντρο αναπαρίσταται από ένα μια καθορισμένου μήκους σειρά bits που απεικονίζουν το επίπεδο και το γκρουπ στο οποίο ανήκουν. Οι χρήστες αντιστοιχίζονται σε έναν κόμβο και σε ένα γκρουπ. Το κανάλι της ρίζας του δυαδικού δέντρου σχηματίζεται από όλο το overlay του P5. Το κανάλι του αριστερού διαδόχου της ρίζας (root) είναι το αριστερό υποδεντρο του overlay και ούτω καθεξής. Όταν ένας νέος χρήστης θέλει να εισέλθει στο P5, πρέπει να εντοπίσει τη ρίζα του καναλιού και να κατέλθει το δέντρο, σχηματίζοντας ένα φύλλο (leaf) στην τυχαία θέση στην οποία θα καταλήξει. [49]

Ο χρήστης που θέλει να στείλει ένα μήνυμα το κρυπτογραφεί με το δημόσιο κλειδί του παραλήπτη και στη συνέχεια κάνει broadcast το ciphertext σε ένα από τα broadcast groups στα οποία ανήκει. Το μήνυμα θα καταλήξει διαδοχικά στη ρίζα του δέντρου στο οποίο ανήκει ο χρήστης και στη συνέχεια στη ρίζα του overlay. Αντίστοιχα, το μήνυμα θα κατέλθει, μέσω του κατάλληλου δέντρου στο κανάλι που ανήκει ο παραλήπτης. Ακόμα και αν αποστολέας και παραλήπτης δεν ανήκουν στο ίδιο broadcast group, το μήνυμα μπορεί να εκπεμφθεί ανώνυμα σε όλα τα σχηματισθέντα δέντρα του P5. [35]

Το P5 βασίζεται στο σχήμα της κρυπτογράφησης δημοσίου κλειδιού, πράγμα που είναι κοστοβόρο και αργό. Η ανάκτηση των public keys γίνεται μέσω μιας τρίτης, ανεξάρτητης αρχής, ενός directory server ή ακόμα και μέσω ενός ανώνυμου public key P5 server. Με τον τρόπο αυτό ένας συμμετέχοντας στο δίκτυο μπορεί να ανακτήσει το δημόσιο κλειδί μιας οντότητας χωρίς να

αποκαλύψει τη δική του ταυτότητα. Επιπλέον, χρησιμοποιείται dummy traffic προκειμένου να καταστήσει τις Network Traffic Analysis Attacks μη βιώσιμες. [147]

Τα πακέτα αποστέλλονται με συγκεκριμένο ρυθμό, προκειμένου να ενισχυθεί η ασφάλεια του δικτύου έναντι Network Traffic Analysis Attacks. Αυτό επιτυγχάνεται με την εισαγωγή noise traffic το οποίο αποστέλλεται, με τυχαίο τρόπο, σε κάποιο group. Αυτό φυσικά δημιουργεί πλεόνασμα δικτυακής κίνησης, καθιστώντας το δίκτυο μη αποδοτικό, ενώ οι χρήστες, ελλείψει πόρων, ίσως χρειαστεί να απορρίψουν δικτυακή κίνηση, εισάγοντας αξιοσημείωτα packet loss rates στο δίκτυο.



Σχήμα 2.43: P5 Tree.

2.3.3 Encrypted DNS

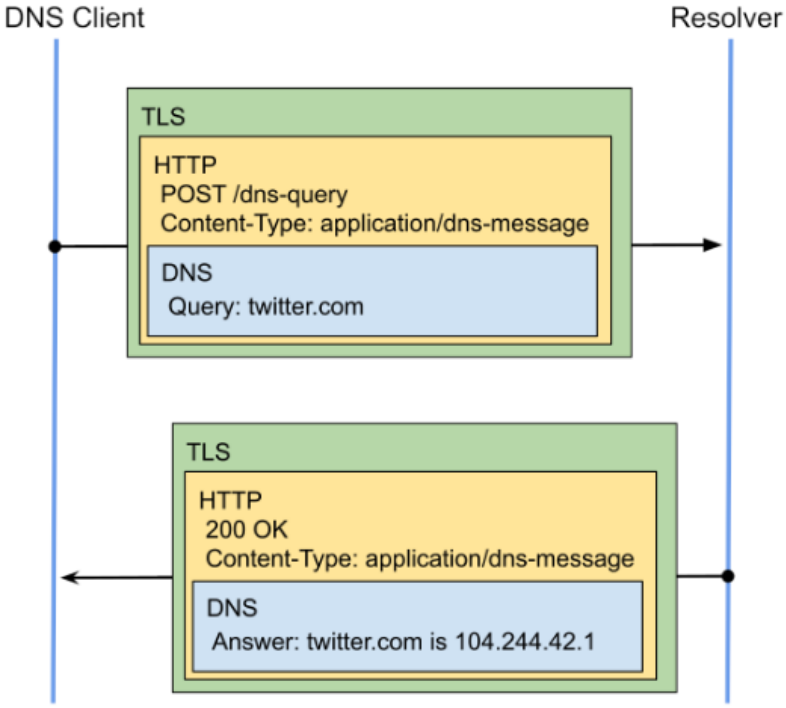
Keywords: ***DNS, TSL, HTTPS***
Maturity: ***Common***

Το DNS πρωτόκολλο είναι ένα από τα δομικά στοιχεία του TCP/IP, καθώς κάθε σύνδεση σε ιστότοπο ή χρήση διαδικτυακής υπηρεσίας προϋποθέτει ένα DNS lookup. Τα lookups αυτά πραγματοποιούνται έως τώρα με ανταλλαγή μη κρυπτογραφημένων queries και replies, με αποτέλεσμα να μη διαθέτουν κάποια προστασία έναντι της ανάλυσης της δικτυακής κίνησης που παράγεται. Έτσι, καθίσταται πολύ εύκολο οι Internet Service Providers (ISPs), οι διαχειριστές των Autonomous Systems (ASs) αλλά και οι κρατικοί φορείς να είναι σε θέση να παρακολουθούν την ψηφιακή δραστηριότητα των χρηστών σε ευρεία κλίμακα, να είναι σε θέση να γνωρίζουν τους ιστότοπους που επισκέπτεται κάθε χρήστης ξεχωριστά αλλά και να λογοκρίνουν, σε τοπικό επίπεδο, περιεχόμενο που φιλοξενείται στον παγκόσμιο ιστό.

Δύο τεχνολογίες που κρυπτογραφούν τα queries και τα replies μεταξύ των χρηστών και των Recursive Resolvers αντιμετωπίζουν το συγκεκριμένο πρόβλημα, χωρίς να καθίσταται αναγκαία η χρήση κάποιας άλλης, εξειδικευμένης τεχνολογίας ανωνύμων επικοινωνιών, όπως για παράδειγμα η πρόσβαση στο διαδίκτυο μέσω του Tor Network. Η πρώτη τεχνολογία ονομάζεται DNS-over-TLS (DoT) και η δεύτερη DNS-over-HTTPS (DoH). Αμφότερες στηρίζονται στο Transport Layer Security (TLS).

Στο DoT τα DNS μηνύματα ενσωματώνονται σε ένα ασφαλές TLS tunnel, με αποτέλεσμα οι εξωτερικοί παρατηρητές να μην είναι σε θέση να γνωρίζουν το περιεχόμενο τους ή να το αλλάξουν. Η λύση αυτή είναι επιρρεπής σε Fallback Attacks, στις οποίες το port στο οποίο κατευθύνονται τα μηνύματα (εν προκειμένει περιπτώσει εισάγεται η χρήση ενός νέου port, του 853) μπλοκάρεται από κάποιο Firewall με αποτέλεσμα οι χρήστες να εξαναγκάζονται στη χρήση του παλιού, μη κρυπτογραφημένου DNS πρωτοκόλλου.

Το DoH αντιμετωπίζει επιτυχώς το παραπάνω πρόβλημα, ενώ ταυτόχρονα επιτρέπει στα web applications να έχουν πρόσβαση σε DNS μέσω browser APIs. Η διασφάλιση της εμπιστευτικότητας και της ακεραιότητας των μηνυμάτων γίνεται με τον ίδιο ακριβώς τρόπο με τον οποίο υλοποιείται και το HTTPS πρωτόκολλο, όπως παρουσιάζεται παρακάτω.



Σχήμα 2.44: DoT & DoH.

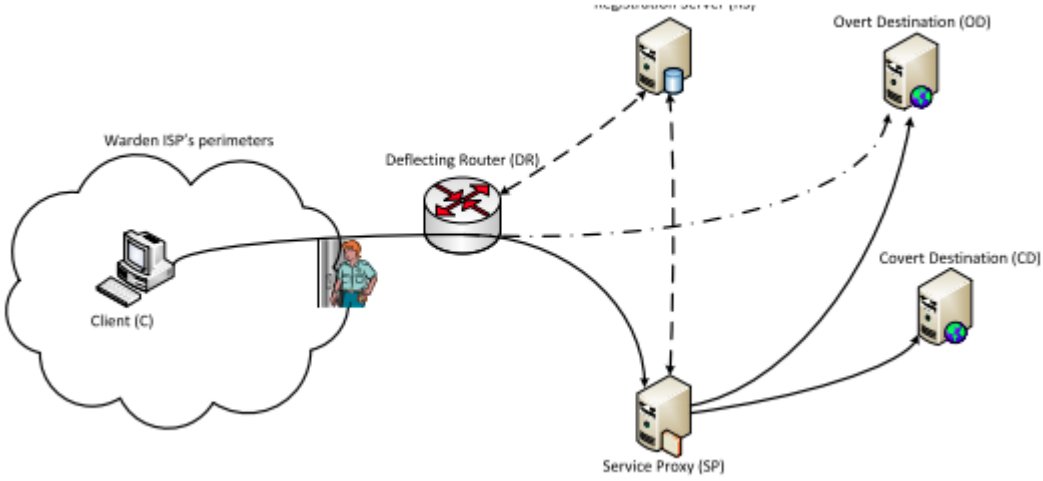
Οι λύσεις αυτές, αν και αποτελούν σημαντικό βήμα για την ενίσχυση της ιδιωτικότητας των χρηστών του Διαδικτύου, δεν αποτελούν πανάκεια, καθώς αντιμετωπίζουν προβλήματα ασφαλείας, ιδιαίτερα απέναντι σε κακόβουλους χρήστες με επάρκεια πόρων. Οι επιθέσεις αυτές είναι πολύ ευκολότερες μάλιστα από τις επιθέσεις που πραγματοποιούνται σε wep applications που χρησιμοποιούν το HTTPS πρωτόκολλο, παρόλο που ουσιαστικά χρησιμοποιούν την ίδια ακριβώς τεχνολογία. Οι επιθέσεις αυτές μπορούν να οδηγήσουν με σχετική ευκολία στην αποκάλυψη των ιστοτόπων τους οποίους επισκέπτεται ένας χρήστης, αλλά και στην επιτυχή λογοκρισία περιεχομένου στο Διαδίκτυο. Η πλήρης εξάλειψη πληροφοριών που σχετίζονται με το μέγεθος των διακινούμενων DNS μηνυμάτων, με παρόμοιο τρόπο που υλοποιούνται τα one-size Tor cells, είναι ένας αποτελεσματικός τρόπος αντιμετώπισης των κινδύνων που αναφέρθηκαν παραπάνω. [183]

2.3.4 Cirripede

***Keywords:* Client-Server, ISP, AS, Proxies**
***Maturity:* Proof of Concept**

Το Cirripede είναι σύστημα ανωνύμων επικοινωνιών που εστιάζει στο unobservability των χρηστών του και είναι σχεδιασμένο να γίνεται deployed από τους ISPs. Σκοπός του είναι να παρουσιάζεται σε τρίτους παρατηρητές ότι η δικτυακή κίνηση ενός χρήστη έχει προορισμό κάποιον dummy προορισμό, με τον ISP να ανακατευθύνει την κίνηση προς τον πραγματικό προορισμό που επιθυμεί ο χρήστης. Έχει σχεδιαστεί να λειτουργεί σε routers οι οποίοι διαχειρίζονται μεγάλο όγκο δικτυακής κίνησης, χωρίς να επιβαρύνει τη συνολική εικόνα του δικτύου με επιπλέον overhead.

Οι Cirripede proxies τοποθετούνται σε κεντρικά, στρατηγικά σημεία, με αποτέλεσμα να καθίσταται ιδιαίτερα δύσκολος ο εντοπισμός και το μπλοκάρισμα τους. Επιπλέον, παρουσιάζει και πολύ καλή ανθεκτικότητα απέναντι σε Censorship Attacks. Το πρωτόκολλο αρκεί να υιοθετηθεί από έναν περιορισμένο αριθμό ASs στο Internet προκειμένου να παρέχει ανωνυμία σε μεγάλο μέρος των χρηστών. [188] Παρακάτω παρουσιάζεται συνοπτικά η αρχιτεκτονική του.



Σχήμα 2.45: Αρχιτεκτονική του Cirripede.

2.3.5 Drac

Keywords: ***Client-Server, Peer-to-Peer, Instant Messaging, VoIP***
Maturity: ***Proof of Concept***

Πρόκειται για μια τεχνολογία η οποία εστιάζει στη διατήρηση της ανωνυμίας και του unobservability των χρηστών της, ιδιαίτερα σε instant messaging και VoIP εφαρμογές. Είναι ιδιαίτερα αποτελεσματικό απέναντι σε επιθέσεις, ακόμα και εναντίον global passive adversaries. Εξυπηρετεί πολύ καλά τις low volume επικοινωνίες τέτοιου είδους, καθώς η μεγάλη συχνότητα τους τις καθιστά δυσκολότερο να εντοπιστούν από άλλες δραστηριότητες. Μάλιστα, ο μικρός όγκος διακινούμενης πληροφορίας στις τεχνολογίες αυτές επιτρέπει την εισαγωγή padding για τη μεγαλύτερη ενίσχυση της προστασίας τους σε επιθέσεις. Στα μειονεκτήματα του Drac προσμετράται το γεγονός ότι εισάγει σημαντικό overhead το δίκτυο, γι αυτό ακριβώς απευθύνεται σε low volume επικοινωνίες.

Το Drac συνδυάζει στοιχεία τόσο από Client-Server όσο και από Peer-to-Peer συστήματα προκειμένου να καταστεί ανθεκτικό απέναντι σε διάφορες επιθέσεις, ειδικά τις Sybil Attacks. Το social graph αποκαλύπτεται σε οποιονδήποτε χρήστη, ωστόσο το unobservability του δικτύου το θωρακίζει απέναντι σε τυχόν κακόβουλους χρήστες. Μπορεί να χρησιμοποιηθεί τόσο σε P2P αρχιτεκτονικές, για χρήση από ευρύ κοινό, όσο και σε Client-Server αρχιτεκτονική για την κάλυψη ανώνυμων VoIP επικοινωνιών ακόμα και σε κρατικούς οργανισμούς. [192]

2.4 Censorship Resistant Τεχνολογίες

Πρόκειται για τεχνολογίες που παρέχουν συνδυαστικά τα privacy, unlinkability, και robustness του δικτύου. Ένας επιτιθέμενος δεν είναι σε θέση να αναγνωρίσει το περιεχόμενο ενός διακινούμενου μηνύματος, ενώ δε μπορεί να αναγνωρίσει τα μέλη που συμμετέχουν σε μια μεταξύ τους επικοινωνία. Το

robustness τέλος αναφέρεται στη διαθεσιμότητα του δικτύου, με αποτέλεσμα δύο μέρη που επιθυμούν να επικοινωνήσουν να μη μπορεί να παρεμποδιστούν από έναν κακόβουλο χρήστη.

2.4.1 Freenet

Keywords: ***Peer-To-Peer, Chat, File Sharing***
Maturity: ***Common***

Το Freenet είναι μια μορφής κοινωνικό δίκτυο το οποίο παρέχει στους χρήστες του τη δυνατότητα να μοιράζονται αρχεία ανώνυμα, να συμμετέχουν σε ανώνυμες εφαρμογές συνομιλίας (chat) καθώς και να έχουν ανώνυμη πρόσβαση ή δυνατότητα δημοσίευσης ιστοσελίδων οι οποίες είναι αποκλειστικά προσβάσιμες μέσω του Freenet. [7] Για την επίτευξη της ανωνυμίας και της ιδιωτικότητας των χρηστών του, το Freenet υλοποιείται ως ένα αποκεντρωμένο peer-to-peer network. Το Freenet χρησιμοποιείται ευρέως ως ένας τρόπος για την αντιμετώπισης της λογοκρισίας στο διαδίκτυο, καθώς, όπως προαναφέρθηκε, παρέχει τη δυνατότητα σε χρήστες να δημιουργούν και να ανεβάζουν ιστοσελίδες χωρίς να εκτίθεται η ταυτότητα τους και να ελέγχεται το περιεχόμενο τους.

Το Freenet προέκυψε από την έρευνα του Ian Clarke στο Πανεπιστήμιο του Εδιμβούργου, το οποίο στην απαρχή του αναφερόταν ως “κατανεμημένο αποκεντρωμένο σύστημα αποθήκευσης και ανάκτησης πληροφοριών”. Οι ερευνητές που ανέπτυξαν το Freenet υποστήριξαν ότι το Freenet μπορεί να παρέχει ανωνυμία στο Διαδίκτυο με τον εξής τρόπο: μικρά κρυπτογραφημένα αποσπάσματα (snippets) του περιεχομένου που διακινείται μεταξύ των υπολογιστών των χρηστών αποθηκεύονται, ενώ η σύνδεση γίνεται αποκλειστικά μέσω ενδιάμεσων υπολογιστών που μεταβιβάζουν αιτήματα για περιεχόμενο και τα στέλνουν πίσω, χωρίς όμως να γνωρίζουν πλήρως τα περιεχόμενα του αρχείου. Η αρχή λειτουργίας του Freenet βασίστηκε σε αυτή του routing, όπου η δρομολογητές στην ουσία απλά δρομολογούν τα πακέτα στο κατάλληλο interface χωρίς να γνωρίζουν λεπτομέρειες για τα αρχεία που διακινούν. Το Freenet παρέχει προσωρινή αποθήκευση (caching) των snippets, ένα επίπεδο ισχυρής κρυπτογράφησης χωρίς να εξαρτάται από κεντρικές δομές (decentralized). Αυτό επιτρέπει στους χρήστες να δημοσιεύουν ή να ανακτούν ανώνυμα διάφορα είδη πληροφοριών. Στις 11 Φεβρουαρίου 2015, η Freenet έλαβε το βραβείο SUMA για την «πλήρη προστασία ενάντια στην παρακολούθηση». [81]

Το δίκτυο διαμοιρασμού αρχείων του Freenet παρέχει τη δυνατότητα αποθήκευσης εγγράφων, τα οποία είναι προσβάσιμα μέσω ενός συσχετιζόμενου κλειδιού, όπως γίνεται πλέον και στο HTTP. Το Freenet εξαρχής σχεδιάστηκε ώστε να είναι εξαιρετικά βιώσιμο μέσω του decentralization, με αποτέλεσμα να μην υπάρχουν κεντρικοί διακομιστές που να λειτουργούν ως υποδομή και να μην υπάρχει καμία απολύτως εξάρτηση από συγκεκριμένα άτομα ή οργανισμούς, συμπεριλαμβανομένων και των σχεδιαστών του Freenet. Ο κώδικας υλοποίησης του Freenet αποτελείται από πλέον 192,000 γραμμές, ενώ πληροφορίες που αποθηκεύονται στο Freenet κατανέμονται σε όλο το δίκτυο και αποθηκεύονται σε διάφορους κόμβους. [7] Παράλληλα, η κρυπτογράφηση των snippets και η μετάδοση των αιτημάτων μέσω διαφόρων κόμβων καθιστά εξαιρετικά δύσκολο τον εντοπισμό των δημιουργών και των ληπτών του εκάστοτε περιεχομένου, καθώς και τον εντοπισμό του ακριβούς σημείου αποθήκευσης του. Με αυτό τον τρόπο εξασφαλίζεται τόσο η ανωνυμία των χρηστών, όσο και η ελευθερία λόγου και περιεχομένου. Από τη στιγμή που όλο το περιεχόμενο που βρίσκεται αποθηκευμένο σε έναν τυχαίο κόμβο έχει κρυπτογραφηθεί με ισχυρές μεθόδους, είναι εξαιρετικά δύσκολο να υπάρξει πρόσβαση σε αυτό από μη εξουσιοδοτημένα άτομα, ακόμα και από τους ίδιους τους διαχειριστές του συγκεκριμένου κόμβου.

Κάθε κόμβος εκχωρεί συγκεκριμένο χώρο στον σκληρό του δίσκο, προκειμένου να αποθηκεύει περιεχόμενο που διακινείται μέσω του Freenet. Τα αρχεία που συνθέτουν το περιεχόμενο του Freenet χωρίζονται συνήθως σε πολλά μικρά μπλοκ, κάθε ένα εκ των οποίων υπόκειται ανεξάρτητη επεξεργασία, πράγμα που σημαίνει ότι ένα αρχείο μπορεί να έχει τμήματα του αποθηκευμένα σε πολλούς διαφορετικούς κόμβους. Η διαδικασία διαμοιρασμού περιεχομένου και αρχείων στο Freenet είναι αυτή που ακολουθεί:

1. Ένας χρήστης που επιθυμεί να μοιραστεί ένα αρχείο ή να ενημερώσει έναν ελεύθερο ιστότοπο εισάγει το αρχείο στο δίκτυο.
2. Αφού ολοκληρωθεί η εισαγωγή, ο κόμβος δημοσίευσης είναι ελεύθερος να τερματιστεί, επειδή το αρχείο είναι αποθηκευμένο στο δίκτυο. Θα παραμείνει διαθέσιμο για άλλους χρήστες, ανεξάρτητα από το εάν ο αρχικός κόμβος δημοσίευσης είναι συνδεδεμένος ή όχι. Κανένας κόμβος δεν είναι υπεύθυνος για το περιεχόμενο. Αντίθετα, αναπαράγεται σε πολλούς διαφορετικούς κόμβους.

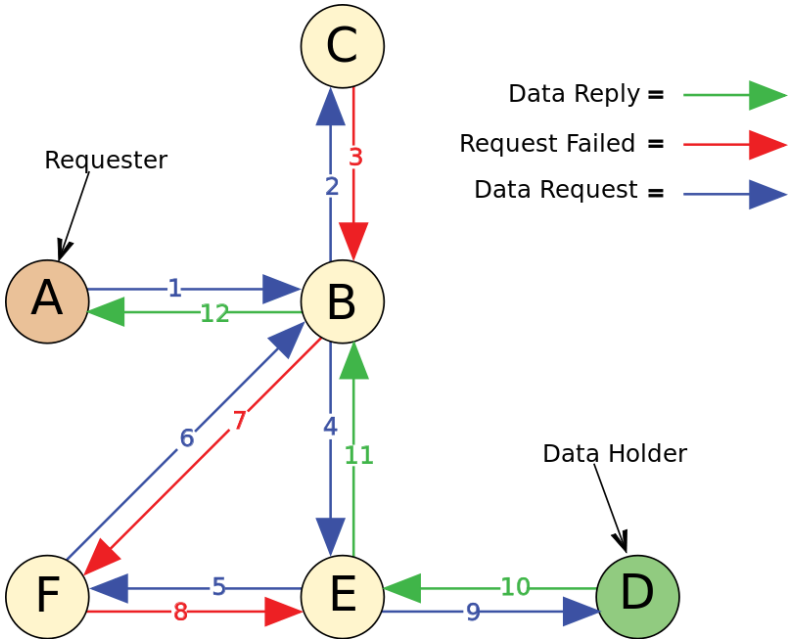
Δύο πλεονεκτήματα αυτού του σχεδιασμού είναι η υψηλή αξιοπιστία και η ανωνυμία. Οι πληροφορίες παραμένουν διαθέσιμες ακόμη και αν ο αρχικός κόμβος δημοσίευσης βρίσκεται εκτός σύνδεσης, ενώ διανέμεται ανώνυμα σε πολλούς κόμβους ως κρυπτογραφημένα μπλοκ, όχι ολόκληρα αρχεία. Το βασικό μειονέκτημα της παραπάνω μεθόδου είναι ότι κανένας κόμβος δεν είναι υπεύθυνος για οποιοδήποτε κομμάτι δεδομένων. Εάν ένα κομμάτι δεδομένων δεν ανακτηθεί για κάποιο χρονικό διάστημα και ένας κόμβος συνεχίζει να λαμβάνει νέα δεδομένα, θα διαγράψει τα παλιά δεδομένα όταν ο εκχωρημένος για περιεχόμενο χώρος στο δίσκο του χρησιμοποιηθεί πλήρως. Με αυτόν τον τρόπο το Freenet τείνει να «ξεχνάει» δεδομένα που δεν ανακτώνται τακτικά. [81] Επίσης, άλλη μία ουσιώδης διαφορά του Freenet σε σχέση με τον περιεχόμενο που φιλοξενεί είναι ότι ενώ οι χρήστες μπορούν να εισάγουν ελεύθερα δεδομένα στο δίκτυο, δεν υπάρχει τρόπος διαγραφής τους. Λόγω της ανώνυμης φύσης της Freenet, ο αρχικός κόμβος δημοσίευσης ή ο κάτοχος οποιουδήποτε τμήματος δεδομένων είναι άγνωστος. Ο μόνος τρόπος με τον οποίο μπορούν να καταργηθούν τα δεδομένα είναι εάν οι χρήστες δεν το ζητήσουν για αρκετό χρονικό διάστημα, όπως αναφέρθηκε παραπάνω.

Σχετικά με τον τρόπο με τον οποίο οργανώνεται το δικτυακό μέρος του Freenet, συνήθως ένας κεντρικός υπολογιστής στο δίκτυο χρησιμοποιεί λογισμικό που λειτουργεί ως κόμβος και συνδέεται με άλλους κεντρικούς υπολογιστές που εκτελούν το ίδιο λογισμικό για να σχηματίσει ένα μεγάλο κατανεμημένο δίκτυο μεταβλητού μεγέθους από ομότιμους κόμβους. Ορισμένοι κόμβοι είναι κόμβοι τελικού χρήστη, από τους οποίους γίνεται εισαγωγή ή ανάκτηση περιεχομένου. Άλλοι κόμβοι εξυπηρετούν μόνο τη δρομολόγηση των δεδομένων. Όλοι οι κόμβοι επικοινωνούν μεταξύ τους ταυτόσημα - δεν υπάρχουν αποκλειστικοί "πελάτες" ή "διακομιστές". Δεν είναι δυνατόν για έναν κόμβο να αξιολογήσει έναν άλλο κόμβο εκτός από την ικανότητά του να εισάγει και να ανακτά δεδομένα που σχετίζονται με ένα κλειδί. Αυτό δεν συμβαίνει στα περισσότερα άλλα δίκτυα P2P όπου οι διαχειριστές μπορούν να χρησιμοποιούν ένα σύστημα αναλογίας, όπου οι χρήστες πρέπει να μοιραστούν μια συγκεκριμένη ποσότητα περιεχομένου προτού κάνουν λήψη περιεχομένου που έχουν διαθέσει άλλοι χρήστες. Το Freenet μπορεί επίσης να θεωρηθεί ένα μικρό παγκόσμιο δίκτυο. [7]

Το πρωτόκολλο Freenet προορίζεται να χρησιμοποιηθεί σε ένα δίκτυο πολύπλοκης τοπολογίας, όπως ακριβώς είναι το Διαδίκτυο (Internet Protocol). Κάθε κόμβος γνωρίζει μόνο έναν συγκεκριμένο αριθμό άλλων κόμβων που μπορεί να προσεγγίσει άμεσα (οι "γείτονες" του), αλλά οποιοσδήποτε κόμβος μπορεί να είναι γειτονικός με οποιονδήποτε άλλο, υπό την έννοια ότι οποιοσδήποτε κόμβος μπορεί να διαμοιραστεί δεδομένα, δηλαδή να στείλει ή να ανακτήσει περιεχόμενο από οποιονδήποτε κόμβο συμμετέχει στο Freenet. Δεν υπάρχει ιεραρχία ή οποιαδήποτε άλλη οργανωτική δομή του

δικτύου. Κάθε μήνυμα δρομολογείται μέσω του δικτύου περνώντας από γείτονα σε γείτονα μέχρι να φτάσει στον προορισμό του. Κάθε κόμβος που μεταδίδει ένα μήνυμα σε έναν γείτονα του, δεν γνωρίζει εάν αυτός θα προωθήσει το μήνυμα σε έναν άλλο κόμβο ή είναι ο τελικός προορισμός, ούτε αν πρόκειται για την αρχική πηγή του μηνύματος. Αυτό διασφαλίζει την προστασία της ανωνυμίας των χρηστών και των δημιουργών του περιεχομένου και διακινείται μέσω του Freenet. Κάθε κόμβος διατηρεί ένα χώρο αποθήκευσης δεδομένων που περιέχει έγγραφα που σχετίζονται με κλειδιά, καθώς και έναν πίνακα δρομολόγησης που συνδέει τους κόμβους με εγγραφές σχετικά με την απόδοσής τους στην ανάκτηση διαφορετικών κλειδιών.

Το Freenet χρησιμοποιεί ένα πρωτόκολλο δρομολόγησης βασισμένο σε κλειδιά, παρόμοιο με αυτό των κατανεμημένων πινάκων κατακερματισμού (distributed hash table-DHT). Στην έκδοση 0.7, το Freenet υποστηρίζει τόσο το Opennet όσο και το Darknet όλες οι συνδέσεις κόμβων έχουν ρυθμιστεί χειροκίνητα, επομένως μόνο οι “φίλοι” κάθε χρήστη γνωρίζουν την διεύθυνση IP του κόμβου τους). Το Darknet είναι λιγότερο βολικό, αλλά πολύ πιο ασφαλές ενάντια σε έναν εισβολέα. Κάθε κόμβος έχει μια θέση, η οποία είναι ένας αριθμός μεταξύ 0 και 1. Όταν ζητείται ένα κλειδί, πρώτα ο κόμβος ελέγχει την τοπική αποθήκευση δεδομένων. Εάν δεν βρεθεί, το hash του κλειδιού μετατρέπεται σε άλλο αριθμό στο ίδιο εύρος και το αίτημα δρομολογείται σε κόμβο του οποίου η τοποθεσία είναι πλησιέστερη στο κλειδί. [7] Αυτό συνεχίζεται μέχρι να ξεπεραστεί κάποιος αριθμός βημάτων ή όταν δεν υπάρχουν πλέον άλλοι κόμβοι για αναζήτηση ή αν δε βρεθούν τα δεδομένα. Εάν τα δεδομένα βρεθούν, αποθηκεύονται προσωρινά σε κάθε κόμβο κατά μήκος της διαδρομής. Επομένως, δεν υπάρχει κανένας κόμβος προέλευσης για ένα κλειδί και η προσπάθεια εύρεσης της τοποθεσίας αποθήκευσης μιας πληροφορίας θα έχει ως αποτέλεσμα την ευρύτερη αποθήκευση στην κρυφή μνήμη στο σύνολο του δικτύου. Ουσιαστικά η ίδια διαδικασία χρησιμοποιείται για την εισαγωγή ενός εγγράφου στο δίκτυο: τα δεδομένα δρομολογούνται σύμφωνα με το κλειδί έως ότου ολοκληρωθεί ένας συγκεκριμένος αριθμός βημάτων (hops). Αν δε βρεθεί έγγραφο με το ίδιο κλειδί, τότε αποθηκεύεται σε κάθε κόμβο. Εάν βρεθούν παλαιότερα δεδομένα, τα παλαιότερα δεδομένα διαβιβάζονται στο δίκτυο και επιστρέφονται στον εντολέα. Εν τέλει, είτε θα βρεθεί το έγγραφο που αναζητά ένας χρήστης είτε θα ξεπεραστεί το όριο των βημάτων (hops) που έχει καθοριστεί. Ο τελικός κόμβος στέλνει μια απάντηση που επιστρέφει στον αρχικό κόμβο κατά μήκος της διαδρομής, η οποία καθορίζεται από τις εγγραφές εκκρεμών αιτημάτων των ενδιάμεσων κόμβων. Οι ενδιάμεσοι κόμβοι ενδέχεται να προβούν σε προσωρινή αποθήκευση του εγγράφου, με αποτέλεσμα να εξοικονομείται εύρος ζώνης και να θωρακίζονται τα έγγραφα απέναντι στη λογοκρισία, καθώς δεν υπάρχει κανένας κόμβος πηγής της πληροφορίας.



Σχήμα 2.46: Ανταλλαγή μηνυμάτων για εγκατάσταση σύνδεσης στο Freenet.

Λόγω της τυχαιότητας των φυσικών τοποθεσιών στο Darknet, η δρομολόγηση των αιτημάτων για περιεχόμενο ακολουθεί τυχαία διαδρομή. Καθώς η εναλλαγή θέσης (location swapping) στο Darknet και η αναδίπλωση διαδρομής (path folding) στο Opennet συνεχίζεται, οι κόμβοι που είναι κοντά ο ένας στον άλλο θα έχουν ολοένα και πιο κοντινές θέσεις, ενώ οι κόμβοι που βρίσκονται πολύ μακριά θα συνεχίσουν να απομακρύνονται. Τα δεδομένα με παρόμοια κλειδιά θα αποθηκευτούν στον ίδιο κόμβο. Έτσι, το δίκτυο τείνει να αυτο-οργανωθεί σε μια κατανεμημένη, ομαδοποιημένη δομή, όπου οι κόμβοι τείνουν να συγκρατούν στοιχεία δεδομένων που βρίσκονται κοντά, όσον αφορά τη συσχέτιση των κλειδιών τους. Πιθανότατα θα υπάρχουν πολλά τέτοια συμπλέγματα σε ολόκληρο το δίκτυο, όπου κάθε δεδομένο έγγραφο θα αναπαραχθεί πολλές φορές, ανάλογα με το πόσο χρησιμοποιείται. [81] Αυτό είναι ένα είδος αυθόρμητης διακοπής της συμμετρίας, στην οποία μια αρχικά συμμετρική κατάσταση (όλοι οι κόμβοι είναι ίδιοι, με τυχαία αρχικά πλήκτρα ο ένας για τον άλλο) οδηγεί σε μια εξαιρετικά ασύμμετρη κατάσταση, με κόμβους να εξειδικεύονται σε δεδομένα που έχουν στενά συσχετιζόμενα κλειδιά.

Υπάρχουν τάσεις που προκαλούν ομαδοποίηση (κοινά δεδομένα, σε όρους εγγύτητας, απλώνονται σε όλο το δίκτυο), και τάσεις οι οποίες διαλύουν την ομαδοποίηση (τοπική προσωρινή αποθήκευση δεδομένων που χρησιμοποιούνται συνήθως). Αυτές οι τάσεις είναι διαφορετικές ανάλογα με τη συχνότητα χρήσης των δεδομένων, έτσι ώστε τα δεδομένα που σπάνια χρησιμοποιούνται να τείνουν να βρίσκονται σε λίγους κόμβους που ειδικεύονται στην παροχή αυτών των δεδομένων, και τα στοιχεία που χρησιμοποιούνται συχνά θα εξαπλωθούν ευρέως σε όλο το δίκτυο. Αυτό το είδος καθρεπτισμού (mirroring) των δεδομένων που γίνεται αυτόματα, αντισταθμίζει τις στιγμές κατά τις οποίες η κυκλοφορία ιστού υπερφορτώνεται και λόγω της έξυπνης δρομολόγησης ενός σύγχρονου δικτύου για το οποίο έχει παρέλθει επαρκής χρόνος ώστε να έχει ενημερωθεί, ένα δίκτυο μεγέθους n θα πρέπει να απαιτεί κατά μέσο όρο μόνο log(n) χρόνο καταγραφής για την ανάκτηση ενός εγγράφου.

Τα κλειδιά είναι hashes, ενώ η εγγύτητα κλειδιού δεν αναφέρεται στη σημασιολογική εγγύτητα, δηλαδή το κλειδί δεν καθορίζει ή υποδεικνύει με κάποιον τρόπο τη δημοφιλία ενός εγγράφου. Επομένως, δεν υπάρχει συσχέτιση μεταξύ της εγγύτητας των κλειδιών και της δημοφιλίας των

δεδομένων, όπως θα μπορούσε να υπάρχει εάν τα κλειδιά εμφανίζουν κάποια σημασιολογική σημασία, αποφεύγοντας έτσι σημεία συμφόρησης που προκαλούνται από δημοφιλή θέματα. Τα δύο βασικά είδη κλειδιών που χρησιμοποιούνται στο Freenet, είναι το Content Hash Key (CHK) και το Signed Subspace Key (SSK). Μια υποκατηγορία του SSK που χρησιμοποιείται είναι το Updatable Subspace Key (USK) που προσθέτει τη δυνατότητα διαφορετικών εκδόσεων του εγγράφου (versioning), ώστε να επιτρέπει την ασφαλή ενημέρωση του περιεχομένου. [25]

Το CHK είναι ένα SHA-256 hash ενός εγγράφου (μετά την κρυπτογράφηση, το οποίο εξαρτάται από το hash του απλού κειμένου) και έτσι ένας κόμβος μπορεί να ελέγξει ότι το έγγραφο που του επιστρέφεται είναι το σωστό, ελέγχοντας το digest έναντι του κλειδιού. Αυτό το κλειδί μεταφέρει όλα τα δυαδικά δομικά στοιχεία για το περιεχόμενο που θα παραδοθεί στον πελάτη για επανασυναρμολόγηση και αποκρυπτογράφηση. Το CHK είναι μοναδικό από τη φύση του και παρέχει περιεχόμενο που δε μπορεί να παραποιηθεί. [81] Ένας κακόβουλος κόμβος που θα επιχειρήσει να αλλάξει τα δεδομένα θα εντοπιστεί αμέσως από τον επόμενο κόμβο ή στον client. Τα CHK μειώνουν επίσης τον πλεονασμό δεδομένων δεδομένου ότι τα ίδια δεδομένα θα έχουν το ίδιο CHK και όταν πολλαπλοί ιστότοποι παραπέμπουν στα ίδια αρχεία, μπορούν να αναφέρονται στο ίδιο CHK.

Τα SSK βασίζονται σε μεθόδους κρυπτογράφησης δημόσιου κλειδιού. Προς το παρόν η Freenet χρησιμοποιεί τον αλγόριθμο DSA. Τα έγγραφα που εισάγονται στο δίκτυο με SSK υπογράφονται από τον χρήστη που τα εισάγει και αυτή η υπογραφή μπορεί να χρησιμοποιηθεί για επαλήθευση από κάθε κόμβο ώστε να διασφαλιστεί ότι τα δεδομένα δεν έχουν παραποιηθεί από κακόβουλους χρήστες. Τα SSK μπορούν να χρησιμοποιηθούν και για τη δημιουργία μιας εικονικής, ψεύτικης ταυτότητας στο Freenet, η οποία ωστόσο μπορεί να επαληθευτεί από τους υπόλοιπους χρήστες, και επιτρέπουν την ασφαλή εισαγωγή πολλών εγγράφων από ένα άτομο. Έτσι, μπορεί κάποιος να εισάγει αρχεία στο Freenet χωρίς να αποκαλύψει την κανονική του ταυτότητα, διατηρώντας ωστόσο την αξιοπιστία του ως χρήστης. Τα αρχεία που εισάγονται με SSK είναι ουσιαστικά αμετάβλητα, καθώς η εισαγωγή ενός δεύτερου αρχείου με το ίδιο όνομα μπορεί θα προκαλέσει συγκρούσεις. Το USK επιλύει το πρόβλημα αυτό προσθέτοντας έναν αριθμό έκδοσης στα κλειδιά. Μια ακόμα χρησιμοποιούμενη στο Freenet υποκατηγορία του SSK είναι το Keyword Signed Key ή KSK, στο οποίο το ζεύγος κλειδιών δημιουργείται από μια απλή συμβολοσειρά σε αναγνώσιμη από τον άνθρωπο μορφή. Η εισαγωγή εγγράφου με χρήση KSK επιτρέπει την ανάκτηση και την αποκρυπτογράφηση του εγγράφου εάν και μόνο εάν ο αιτών γνωρίζει τη συμβολοσειρά αυτή. Αυτό επιτρέπει την πιο εύκολη (αλλά λιγότερο ασφαλή) πρόσβαση στα URIs στα οποία αναφέρονται οι χρήστες. [7]

2.4.2 Free Haven

Keywords: ***Peer-To-Peer, Onion Routing, Servnets, Pseudonyms***
Maturity: ***Limited Adoption***

Το Free Haven είναι ένα ανώνυμο δίκτυο δημοσίευσης που αποτελείται από έναν αριθμό servnets που φιλοξενούν και παρέχουν έγγραφα προς οποιονδήποτε τα ζητήσει. Οι ταυτότητες των servnets είναι ανοιχτές και προσβάσιμες από όλους. Όλες οι επικοινωνίες για τη δημοσίευση και την ανάκτηση αρχείων λαμβάνουν χώρα σε ένα εξωτερικό Mix-based στρώμα επικοινωνιών. Όταν κάποιος χρήστης επιθυμεί να δημοσιεύσει ένα αρχείο, υλοποιεί κατακερματισμό του χρησιμοποιώντας τον information dispersal αλγόριθμο του Rabin και στέλνει κάθε κομμάτι σε διαφορετικό servnet. Όταν ένας χρήστης επιθυμεί να ανακτήσει ένα από αυτα τα αρχεία τότε πρέπει αρχικά να βρει το hash του συγκεκριμένου αρχείου και εν συνεχεία να το στείλει σε ένα servnet, το οποίο μέσω broadcast κοινοποιεί το αίτημα

στους υπόλοιπους servnets. Από αυτούς, όσοι έχουν αποθηκευμένα κομμάτια του αρχείου που έχει ζητήσει ο χρήστης αναλαμβάνουν να του το παρέχουν. [162]

Κάθε κόμβος είναι ισότιμος με τους υπόλοιπους και το σύνολο των επικοινωνιών γίνεται με έναν συμμετρικό και ισορροπημένο τρόπο. Οι ανώνυμες επικοινωνίες γίνονται με τη χρήση του Onion Routing ώστε να αποτραπούν τυχόν επιτιθέμενοι από το να συμπεράνουν ποιοι χρήστες αιτούνται συγκεκριμένα αρχεία. Οι users και οι servers χρησιμοποιούν ψευδώνυμα για να προστατεύσουν την ταυτότητα τους στο δίκτυο, τα οποία αξιολογούνται μέσω ενός reputation συστήματος για τη διασφάλιση της αξιοπιστιας τους. Οι κόμβοι επικοινωνούν τυχαία μεταξύ τους, αλλάζοντας ψευδώνυμα σε κάθε hop, ώστε να καταστήσουν ακόμα δυσκολότερη την ανάλυση της δικτυακής κίνησης που θα μπορούσε να αποκαλύψει σε κακόβουλους χρήστες την ταυτότητα του Initiator ή του Destination των αιτημάτων. [149]

Το Free Haven είναι ένα δίκτυο που δίνει βάρος στην ασφάλεια των επικοινωνιών έχοντας σαφή μειονεκτήματα όσον αφορά την απόδοση του, σε σύγκριση με άλλες λύσεις ανωνύμων επικοινωνιών. Το persistence των δεδομένων που δημοσιεύονται σε αυτό βασίζεται στη διάρκεια και όχι στο πόσο δημοφιλές είναι ένα αρχείο. Έτσι, δημοφιλή αρχεία δε μπορούν να πάρουν τη θέση άλλων αρχείων, κάτι που αποτρέπει τη λογοκρισία του δικτύου από επιτιθέμενους. Η ανθεκτικότητα στη λογοκρισία περιεχομένου είναι το βασικό χαρακτηριστικό του Free Haven, το οποίο αποτελεί μια εξαιρετική λύση για τέτοιου είδους εφαρμογές. [2]

2.4.3 Endsuleit and Mie’s censorship-resistant system

Keywords: ***Peer-To-Peer, Keywords, Lookups***
Maturity: ***Proof of Concept***

Στη συγκεκριμένη λύση, τα αρχεία αναπαριστώνται ως ένα σετ από keywords. Ένα αρχείο δημοσιεύεται με την κρυπτογράφηση του από ένα κλειδί που προκύπτει από τα keywords και κατακερματίζεται σε δύο fragments, τα οποία είναι απαραίτητα για την ανακατασκευή του. Τα fragments γίνονται signed με το private key του publisher, κάτι που του επιτρέπει να ενημερώνει ή να διαγράψει το αρχείο του. Τα fragments αποθηκεύονται σε ένα distributed hash table σε διαφορετικές τοποθεσίες που προκύπτουν από τα keywords. Οι χρήστες που επιθυμούν να ανακτήσουν το εκάστοτε αρχείο χρειάζεται μόνο να γνωρίζουν τα keywords, ενώ για να γνωρίζει ότι το αρχείο δεν έχει τροποποιηθεί κακόβουλα από κάποιο τρίτο μέρος, χρειάζεται να γνωρίζει και το public key του publisher. [146]

Το συγκεκριμένο δίκτυο ανώνυμης αποθήκευσης και ανάκτησης αρχείων διασφαλίζει την ανωνυμία των δημιουργών, ειδικά σε περιπτώσεις διαρροής ευαίσθητων εγγράφων που επιφέρουν νομικές κυρώσεις. Επιπλέον, μειώνει τις πιθανότητες εκδήλωσης επιτυχημένης Denial of Service Attack καθώς αποτρέπεται η δημιουργία πολλαπλών ταυτοτήτων από έναν host. Τα signatures των publishers και των κόμβων γίνονται blinded προκειμένου να αποτραπεί η certification authority να συνδέει τους χρήστες με τα αρχεία και τους κόμβους.

2.4.4 Achord

Keywords: ***Peer-To-Peer, Lookups***
Maturity: ***Proof of Concept***

Το Achord αποτελεί μια ανώνυμη, βελτιωμένη έκδοση του Chord lookup, προκειμένου να ενισχυθεί η ανθεκτικότητα του σε περιβάλλον λογοκρισίας. Για να επιτευχθεί αυτό, κάθε κόμβος έχει περιορισμένη εικόνα του συστήματος. Για να γίνει αυτό το σύστημα θα πρέπει να είναι σε θέση να εντοπίζει τα δεδομένα με έναν επεκτάσιμο τρόπο, χωρίς να αποκαλύπτει την ταυτότητα του εκδότη και του παραλήπτη, έτσι ώστε να μην είναι σε θέση κάποιος κακόβουλος χρήστης να λογοκρίνει την πληροφορία που υπάρχει στο δίκτυο. [2]

Μια επιπλέον αρχή που πρέπει να τηρείται στο δίκτυο είναι να καθίσταται δύσκολη η εισαγωγή ενός νέου κόμβου στο δίκτυο. Οι κόμβοι περιέχουν αρχεία και δεν είναι δυνατή η διαγραφή τους, ώστε να αποτρέπεται η λογοκρισία του περιεχομένου. Τέλος, θα πρέπει να είναι εξίσου δύσκολο να ταυτοποιήσεις έναν κόμβο που φιλοξενεί ένα συγκεκριμένο αρχείο. Έτσι, όπως και η διαγραφή αρχείων, η διαγραφή κόμβων δεν είναι δυνατή στο δίκτυο.

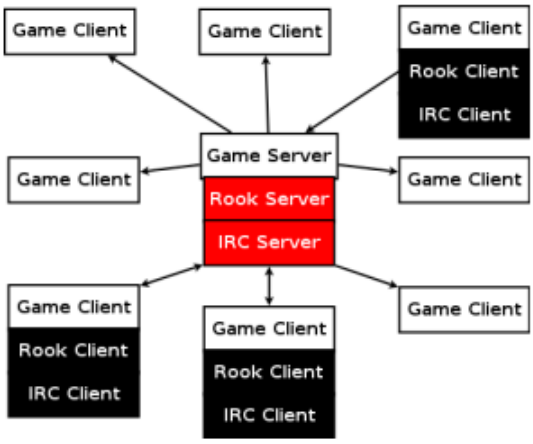
Ο lookup μηχανισμός του δικτύου είναι ίδιος με αυτόν του Chord, τόσο σε επιδόσεις όσο και σε ορθότητα αποτελεσμάτων, ωστόσο έχει τροποποιηθεί ώστε να μην αποκαλύπτονται πληροφορίες που μπορούν να ταυτοποιήσουν τους χρήστες του. Επιπροσθέτως, ένας κόμβος δε μπορεί να στείλουν finger requests σε κάθε κόμβο. [69] [70] Το key lookup του Achord χρησιμοποιεί το connect_to_successor. Όταν ο successor ενός κόμβου κατά τη διάρκεια του request λαμβάνει μήνυμα για σύνδεση, τη τιμή του στέλνεται πίσω μαζί με το recursive search path προς την πηγή του μηνύματος. Για την εισαγωγή μαις τιμής στο σύστημα ένας κόμβος υλοποιεί ένα connect_to_successor ώστε να εγκαταστήσει ένα tunnel προς τον κόμβο που είναι υπεύθυνος για το key κσι στέλνει την τιμή αυτή μέσω του path.

Το tunneling αυτό προσφέρει μια μορφή ανωνυμίας στους requesters και τους inserters, διότι ένας κόμβος που λαμβάνει ένα request δε μπορεί να καθορίσει αν ο requester είναι η πραγματική πηγή του ή αν αυτό προέρχεται από κάποιον άλλο κόμβο του δικτύου. Με παρόμοιο τρόπο, η ταυτότητα ενός κόμβου που φιλοξενεί ένα key προστατεύεται. Υπάρχει επίσης μηχανισμός απόκρυψης των ταυτοτήτων των inserters και των requesters, ωστόσο δεν είναι τόσο ισχυρός όσο σε άλλα δίκτυα όπως το Freenet, καθώς στο Achord, ένας κόμβος που λαμβάνει ένα request μπορεί να υπολογίσει κατά προσέγγιση την απόσταση μεταξύ του key και της ταυτότητας του κόμβου του requester. Αυτό είναι ένα σαφές μειονέκτημα καθώς επιτρέπει την εκτίμηση της πιθανότητας ο requester να είναι και ο πραγματικός Initiator του αιτήματος. Τέλος, το Achord είναι ευάλωτο απέναντι σε Correlation Attacks καθώς και σε οποιαδήποτε μορφή Passive Attack που γίνεται από έναν global adversary.

2.4.5 Rook

Keywords: ***Client-Server, Online Gaming***
Maturity: ***Proof of Concept***

Το Rook διασφαλίζει την πρόσβαση των χρηστών σε λογοκριμένο περιεχόμενο μέσω της απόκρυψης του σε δικτυακή κίνηση που δημιουργείται από online gaming δραστηριότητα. Τα πακέτα δεν μεταβάλλονται ούτε ως προς το μέγεθος ούτε ως προς το πλήθος, καθιστώντας το πιο ανθεκτικό σε Deep Traffic and Packet Inspection μεθοδους επιθέσεων. Οι υπηρεσίες που υποστηρίζονται μπορεί να είναι ακόμα και αυτές σε απαιτήσεις με χαμηλό latency. Παρακάτω παρουσιάζεται η βασική δομή του. [174]

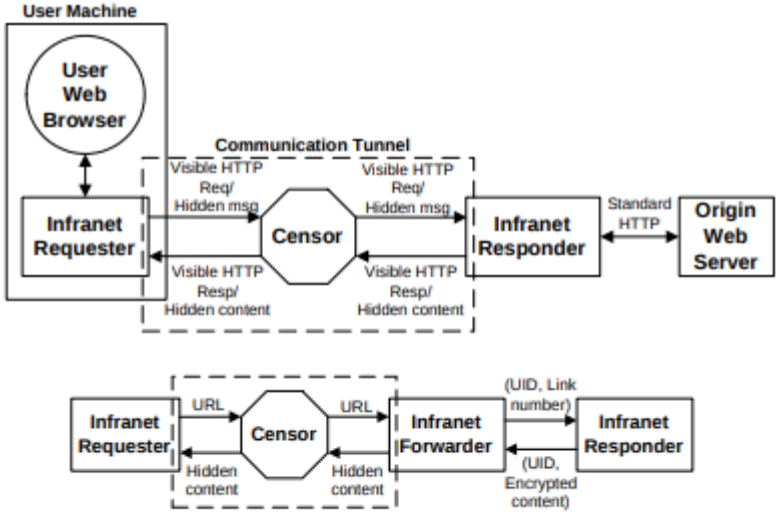


Σχήμα 2.47: Αρχιτεκτονική του Rook.

2.4.6 Infranet

***Keywords:* Client-Server, Covert Channels**
***Maturity:* Proof of Concept**

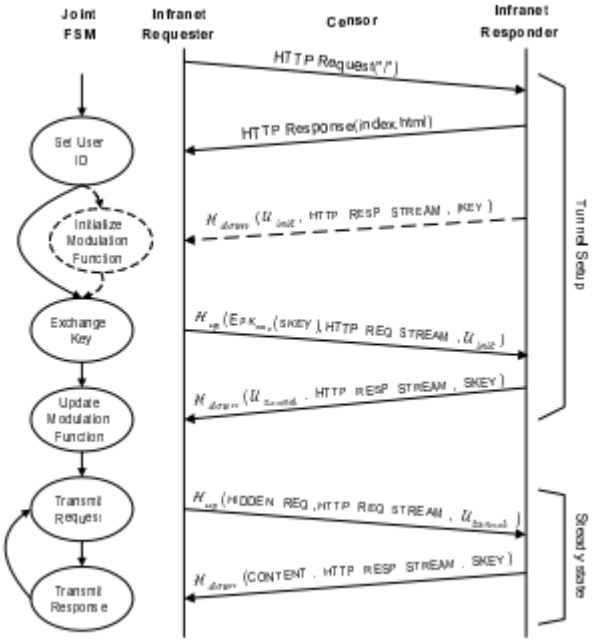
Το Infranet αποτελεί μια τεχνολογία ανωνύμων επικοινωνιών η οποία επιτρέπει στους χρήστες της να παρακάμπτουν τη λογοκρισία περιεχομένου στο Internet. Αυτό υλοποιείται με τη δημιουργία covert channels που παρέχουν πρόσβαση σε Web servers οι οποίοι μπορούν να παρέχουν τόσο νόμιμο όσο και λογοκριμένο περιεχόμενο. Οι χρήστες δημιουργούν μυστικά μηνύματα μέσω αλληλουχιών από requests τα οποία είναι δύσκολο να γίνουν intercepted από censorship συστήματα, ενώ το λογοκριμένο περιεχόμενο επιστρέφεται στους χρήστες υπό κεκαλυμμένη μορφή με τρόπο τέτοιο που είναι δύσκολο να γίνει διακριτό από τη συνήθη δικτυακή κίνηση. Παρακάτω φαίνεται η δομή του Infranet, καθώς και το εξελιγμένο μοντέλο του.



Σχήμα 2.48: Δομή του Infanet και του εξελιγμένου μοντέλου του.

Η λειτουργία του βασίζεται στο HTTP μεταξύ των requesters και των responders. Η επιστροφή περιεχομένου από τους δεύτερους στους πρωτους γίνεται μέσω της χρήσης τεχνικών steganography σε εικόνες που περιέχουν νόμιμο μη λογοκριμένο περιεχόμενο. Η downstream εμπιστευτικότητα διασφαλίζεται με τη χρήση ενός session key και η upstream μέσω της εμπιστευτικής ανταλλαγής μιας

modulus function. Η ανταλλαγή μηνυμάτων για την εγκατάσταση ενός covert channel απεικονίζεται παρακάτω.



Σχήμα 2.49: Εγκατάσταση cover channel στο Infanet.

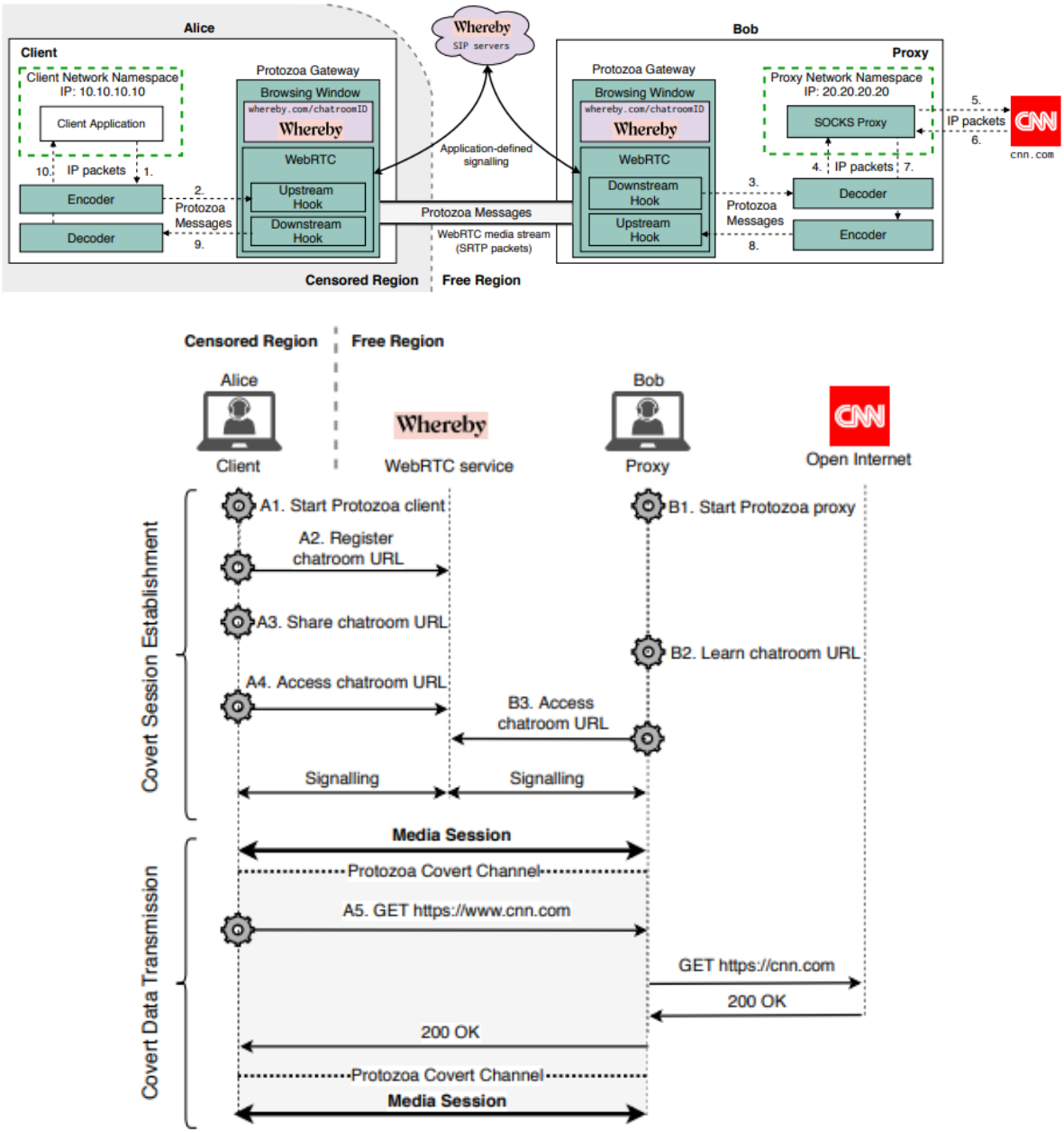
Το δίκτυο μπορούσε να παρακάμψει αρκετά συστήματα λογοκρισίας, αν και πλέον θεωρείται απαρχαιωμένο, καθώς οι steganography τεχνικές μπορούν εύκολα να εντοπιστούν ακόμα και με απλά εργαλεία, ενώ οι Communication Pattern Attacks μπορούν να δώσουν στον επιτιθέμενο χρήσιμα στοιχεία για τη δικτυακή κίνηση που παράγεται μέσω της διακίνησης εικόνων. [168]

2.4.7 Protozoa

***Keywords*: Client-Server, Multimedia, WebRTC**
***Maturity:* Proof of Concept**

Το Protozoa αποτελεί μια multimedia-based τεχνολογία πρόσβασης σε λογοκριμένο περιεχόμενο το οποίο επιστρατεύει τους δομικούς μηχανισμούς του WebRTC multimedia framework. Επιτυγχάνεται η διακίνηση περιεχομένου που έχει λογοκριθεί μέσω της δικτυακής κίνησης που παράγεται από την ανταλλαγή νόμιμου περιεχομένου στο WebRTC χωρίς να μπορεί να γίνει αντιληπτό ακόμα και από τις πλέον εξελιγμένες τεχνικές ανάλυσης δικτυακής κίνησης.

Οι χρήστες μπορούν να δημιουργήσουν covert channels δημιουργώντας ένα video call με κάποιον που εμπιστεύεται, εκτός της γεωγραφικής περιοχής όπου υπάρχει λογοκρισία περιεχομένου, χρησιμοποιώντας μια εφαρμογή του WebRTC, όπως το Whereby. Στη συνέχεια, μέσω του Protozoa η δικτυακή κίνηση που αφορά το λογοκριμένο περιεχόμενο διακινείται μέσω αυτής που αντιστοιχεί στη βιντεοκλήση. Παρακάτω παρουσιάζεται η δομή του πρωτοκόλλου καθώς και η διαδικασία εγκατάστασης ενός covert channel και η πρόσβαση σε λογοκριμένο περιεχόμενο. [169]



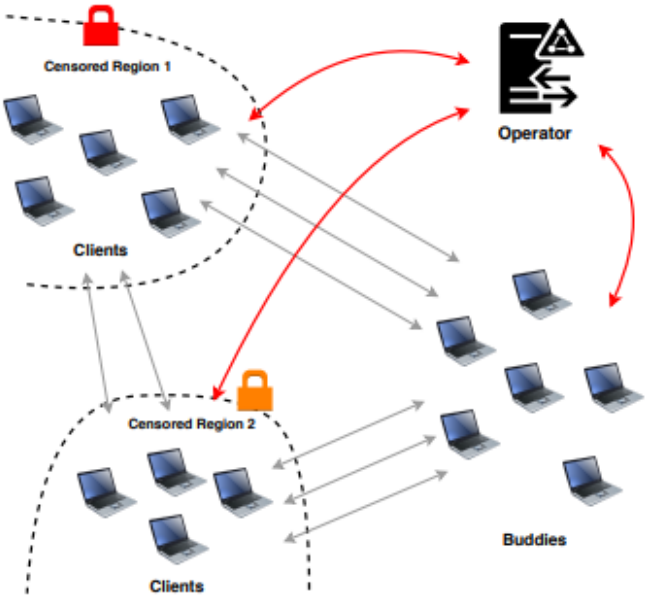
Σχήμα 2.50: Λειτουργία του Protozoa.

2.4.8 MassBrowser

***Keywords:* Client-Server, Peer-To-Peer, Internet Browsing**
***Maturity:* Limited Adoption**

Αποτελεί μια open-source λύση η οποία στοχεύει στο να παρέχει λογοκριμένο περιεχόμενο σε χρήστες του διαδικτύου μέσω άλλων χρηστών οι οποίοι έχουν πρόσβαση σε αυτό. Ένα τμήμα των χρηστών οι οποίοι αναλαμβάνουν να παρέχουν πρόσβαση σε περιεχόμενο σε άλλους χρήστες ονομάζεται Buddies, ενώ οι χρήστες που επιθυμούν να έχουν πρόσβαση σε περιεχόμενο ονομάζονται Clients. Οι χρήστες μπορούν ακόμα και να λειτουργούν ως ενδιάμεσοι proxies χωρίς να παρέχουν άμεσα λογοκριμένο περιεχόμενο.

Η αντιστοίχιση των Clients και Buddies γίνεται μέσω του MassBrowser Operator το οποίο λαμβάνει υπόψη του το bandwidth, τη διαθεσιμότητα τους, τη γεωγραφική τους θέση και άλλα παρόμοια στοιχεία. Υπάρχει η δυνατότητα υποστήριξης μεγάλου αριθμού χρηστών με πολύ καλές επιδόσεις. [170]



Σχήμα 2.51: Λειτουργία του Massbrowser.

2.4.9 Salmon

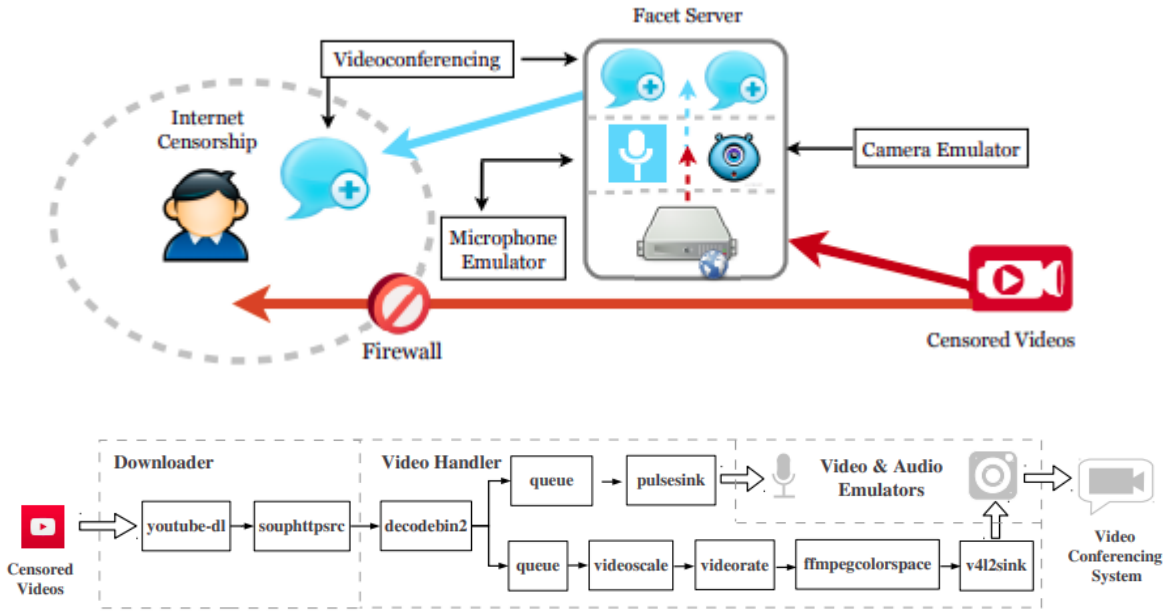
***Keywords:* Peer-To-Peer, Internet Browsing, Proxies**
***Maturity:* Proof of Concept**

Αποτελεί παρόμοια με το Massbrowser λύση, καθώς πρόκειται για ένα δίκτυο χρηστών που έχει στόχο να παρακάμπτει censorship-resist συστήματα, όπως το “Great Firewall” of China, μέσω συνεργασίας των χρηστών του. Χρήστες που έχουν πρόσβαση σε λογοκριμένο περιεχόμενο λειτουργούν ως proxies παρέχοντας περιεχόμενο σε άλλους χρήστες. Δομικό στοιχείο του δικτύου είναι ο αλγόριθμος γρήγορου εντοπισμού κακόβουλων χρηστών, έτσι ώστε να προστατευθεί η πλειοψηφία των servers από επιθέσεις. Κάθε χρήστης μπορεί να γίνει μέλος του δικτύου, ωστόσο απαιτείται επαλήθευση της ταυτότητας του είτε μέσω refferal από ένα άλλο μέλος, είτε με τον έλεγχο του χρήστη από κάποιον λογαριασμό σε ένα social network. [173]

2.4.10 Facet

***Keywords:* Client-Server, Online Streaming**
***Maturity:* Proof of Concept**

Το Facet αποτελεί μια ακόμα λύση για πρόσβαση σε περιεχόμενο το οποίο έχει λογοκριθεί. Χρησιμοποιεί Skype calls προκειμένου οι χρήστες να αποκτήσουν πρόσβαση σε streaming social videos με παρόμοιο τρόπο όπως τα SkypeMorph, CensorSpoofer, StegoTorus και FreeWave, επιτυγχάνοντας ωστόσο πολύ καλύτερη συμβατότητα μεταξύ των proxy και cover πρωτοκόλλων. Επιπλέον χρησιμοποιεί morphing τεχνικές για την προστασία του περιεχομένου από εξελιγμένες Traffic Analysis τεχνικές. [179] Η δομή του δικτύου παρουσιάζεται στις παρακάτω εικόνες.



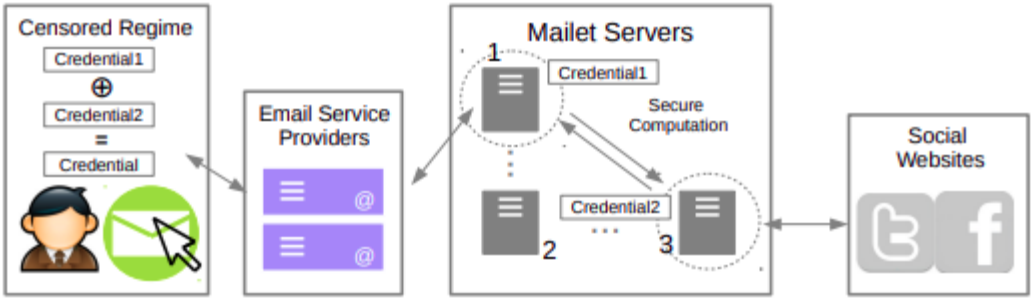
Σχήμα 2.52: Αρχιτεκτονική και λειτουργία του Facet.

2.4.11 Mailet

***Keywords:* Client-Server, Social Media**

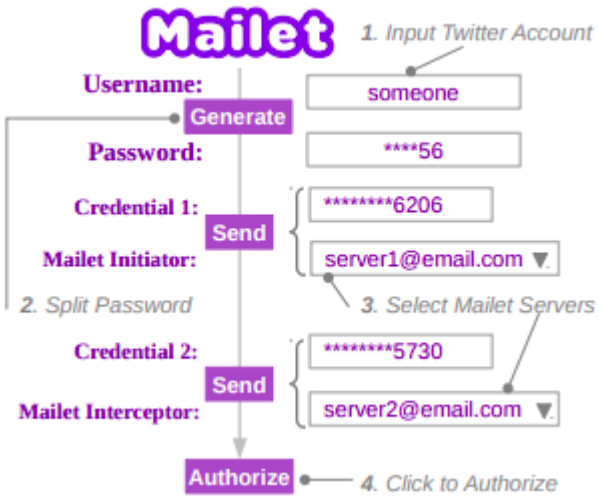
***Maturity:* Proof of Concept**

Πρόκειται για ένα πρωτόκολλο παράκαμψης της λογοκρισίας σε ιστοσελίδες social media. Οι χρήστες μπορούν να έχουν πρόσβαση σε αυτά κάνοντας χρήση mail εφαρμογών. Τα credentials του χρήστη διοχετεύονται στον τελικό προορισμό μέσω δύο διαφορετικών servers, κανένας εκ των οποίων δεν είναι σε θέση να υλοποιήσει εξ ολοκλήρου την ανάκτηση τους. Η ανάκτηση τους στον τελικό προορισμό γίνεται μέσω Galois/Counter Mode(GCM) υπολογιστικών προβλημάτων. Η αρχιτεκτονική του παρουσιάζεται στην εικόνα που ακολουθεί.



Σχήμα 2.53: Αρχιτεκτονική και λειτουργία του Mailet.

Ο χρήστης μέσω ενός GUI μπορεί να επιλέξει τους Mailet servers που επιθυμεί να χρησιμοποιήσει και να στείλει κρυφά τα credentials του για το μέσο κοινωνικής δικτύωσης που επιθυμεί, χωρίς να καθίσταται δυνατό το tracking των δραστηριοτήτων του ή η επαλήθευση της ταυτότητας του από την αρχή που επιβάλλει τη λογοκρισία. Ο χρήστης επίσης μπορεί να χρησιμοποιήσει άλλους Mailet servers και να μην παρέχει καθόλου credentials για δραστηριότητα που δεν τα απαιτεί, όπως για παράδειγμα για την ανάγνωση posts. [180]

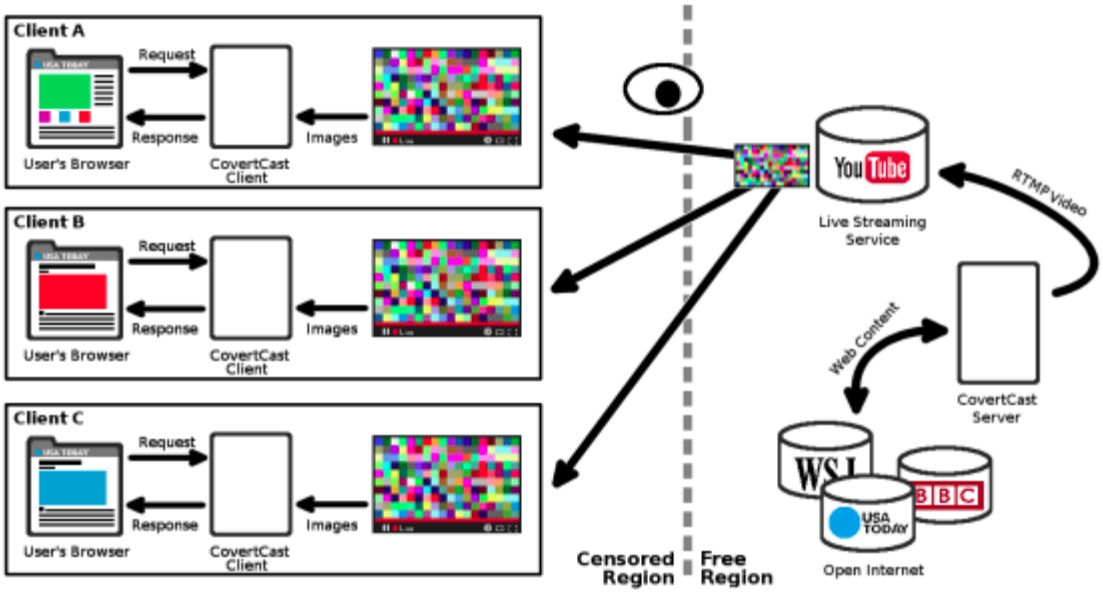


Σχήμα 2.54: Mailet GUI.

2.4.12 CoverCast

***Keywords:* Client-Server, Live Streaming**
***Maturity:* Proof of Concept**

Censorship-resistant εφαρμογή η οποία επιτρέπει την broadcast μετάδοση video streams τα οποία υπόκεινται σε λογοκρισία. Καθώς χρησιμοποιεί τα ίδια ακριβώς πρωτόκολλα, servers και λογισμικό με κάθε άλλο χρήστη της υπηρεσίας, δεν είναι δυνατός ο εντοπισμός της IP Address ή του πρωτοκόλλου από τα συστήματα λογοκρισίας. Έχει καλή επεκτασιμότητα και είναι ανθεκτικό ακόμα και σε προηγμένες Deep Packet Inspection τεχνικές. [181] Στις παρακάτω εικόνες παρουσιάζονται συνοπτικά τόσο η αρχιτεκτονική όσο και η λειτουργία του.

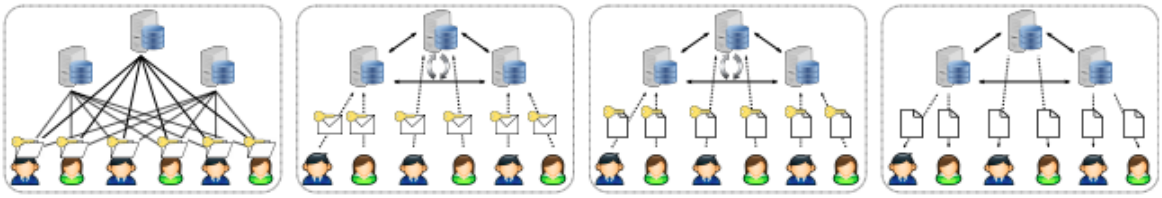


Σχήμα 2.55: Αρχιτεκτονική του CoverCast.

2.4.13 Riffle

***Keywords:* Client-Server, File Sharing, PIR**
***Maturity:* Proof of Concept**

Αποτελείται από έναν περιορισμένο αριθμό anonymity servers και έναν μεγάλο αριθμό χρηστών οι οποίοι έχουν προστασία της ταυτότητας τους εφόσον έστω ένας από τους servers είναι honest. Πρόκειται για μια τεχνολογία που δίνει βάρος στην αποδοτικότητα του bandwidth και των απαιτήσεων σε υπολογιστική ισχύ. [182] Παρακάτω παρουσιάζεται συνοπτικά η διαδικασία του anonymous file transfer, όπως επιτυγχάνεται μέσω του δικτύου.



(a) Setup: Clients share the torrent files anonymously.

(b) Request: Each client requests a file by uploading the hash of the file using Riffle.

(c) Upload: Each client uploads an encrypted file based on the requests using Riffle.

(d) Download: Each client downloads the file he or she requested using PIR.

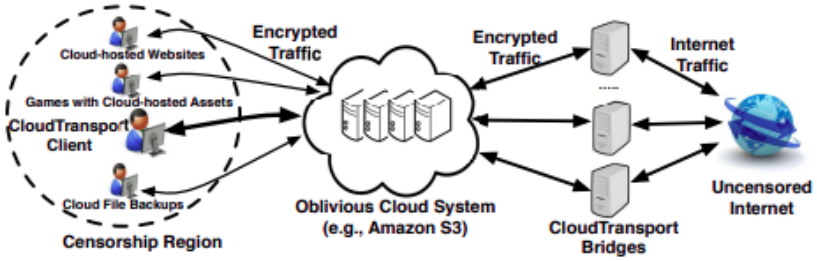
Σχήμα 2.56: Anonymous File Transfer στο Riffle.

2.4.14 CloudTransport

***Keywords:* Client-Server, Cloud, Onion Routing, Proxies**
***Maturity:* Proof of Concept**

Το CloudTransport αποτελεί μια σύγχρονη λύση που στοχεύει στον περιορισμό των σύγχρονων μεθόδων λογοκρισίας, ειδικά στο επίπεδο δικτύου (Network level), στο οποίο οι περισσότερες παραδοσιακές λύσεις, όπως το Tor Network, αντιμετωπίζουν δυσκολίες. Στο CloudTransport η παράκαμψη του φιλτραρίσματος της δικτυακής κίνησης γίνεται μέσω της χρήσης Cloud Storage Service, οπως το Amazon S3, μέσω του οποίου κρύβεται η δικτυακή κίνηση των χρηστών, με αποτέλεσμα να μη μπορεί να καταστεί διακριτή από την υπόλοιπη κίνηση.

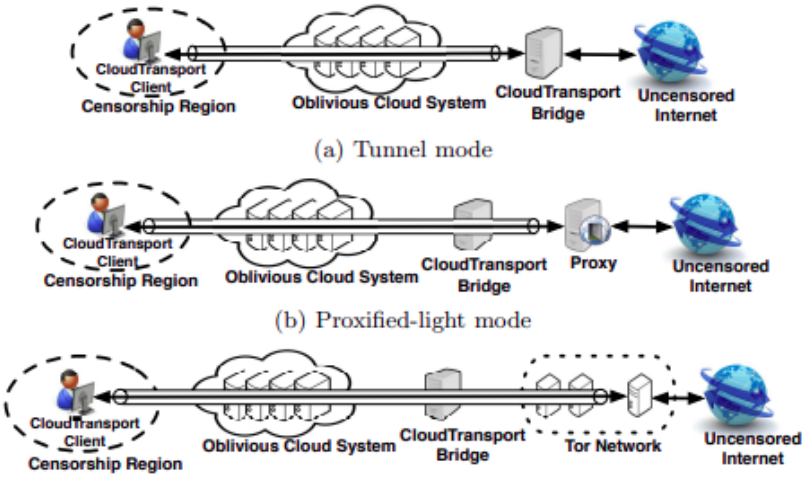
Ο στόχος της νέας αυτής τεχνολογίας είναι να εξαναγκάσει τους κρατικούς οργανισμούς που επιβάλλουν τη λογοκρισία περιεχομένου να χρησιμοποιήσουν πολύ πιο εξελιγμένες τεχνικές λογοκρισίας, οι οποίες ωστόσο σε πολλές περιπτώσεις καθίστανται εξαιρετικά κοστοβόρες και μη βιώσιμες, είτε να ρισκάρουν να προβούν σε διακοπή παροχής υπηρεσίας σε διάφορα τέτοια Cloud Storage Services, διακόπτοντας την παροχή υπηρεσιών ακόμα και σε χρήστες οι οποίοι δεν κάνουν χρήση ανωνύμων επικοινωνιών. Η αρχιτεκτονική του πρωτοκόλλου παρουσιάζεται στην παρακάτω εικόνα.



Σχήμα 2.57: Αρχιτεκτονική του CloudTransport.

Χρησιμοποιεί ένα νέο rendezvous πρωτόκολλο, το οποίο εγγυάται ότι δεν υπάρχουν απευθείας συνδέσεις μεταξύ ενός a CloudTransport client και ενός CloudTransport bridge, με αποτέλεσμα ακόμα και αν εντοπιστεί το πρώτο, οι επιτιθέμενοι να μην είναι σε θεση να εντοπίσουν το δεύτερο, το οποίο εξυπηρετεί πολλαπλές ανώνυμες συνδέσεις.

Το μεγάλο πλεονέκτημα της τεχνολογίας αυτής είναι ότι μπορεί να χρησιμοποιηθεί είτε ως αυτόνομος τρόπος προστασίας ανωνύμων επικοινωνιών, είτε να προσαρτηθεί σε κάποια άλλη τεχνολογία, όπως το Tor, προκειμένου να το θωρακίσει από τυχόν επιθέσεις που αφορούν την πρόσβαση σε λογοκριμένο περιεχόμενο, όπως φαίνεται στην παρακάτω εικόνα. Θα πρέπει να σημειωθεί ότι προοδευτικά, παρέχεται πολύ μεγαλύτερη προστασία απέναντι σε Censorship Attacks.



Σχήμα 2.58: Διαφορετικά μοντέλα λειτουργίας του CloudTransport.

Ο χρήστης μπορεί να κάνει χρήση του CloudTransport εγκαθιστώντας το αντίστοιχο λογισμικό στο τερματικό του και επιλέγοντας ένα rendezvous account και ένα CloudTransport bridge, στο οποίο στέλνει τα credentials του πρώτου, προκειμένου να υλοποιηθεί η ανώνυμη σύνδεση. Υπάρχουν δύο παραλλαγές του πρωτοκόλλου, οι οποίες διαφέρουν στο πόσο συχνά γίνονται εγγραφές στο cloud-based rendezvous account και ζητάνε ενημερώσεις. Η πρώτη παραλλαγή, η οποία ονομάζεται Cirriform, χρησιμοποιεί ένα αρχείο για κάθε σύνδεση στο rendezvous account ανά κατεύθυνση καθώς και ένα αρχείο ανά κατεύθυνση για την εγκατάσταση της σύνδεσης. Η δεύτερη παραλλαγή ονομάζεται Cumuliform και χρησιμοποιεί ένα αρχείο ανά κατεύθυνση, με όλα τα requests να μπαίνουν σε σειρά αναμονής.

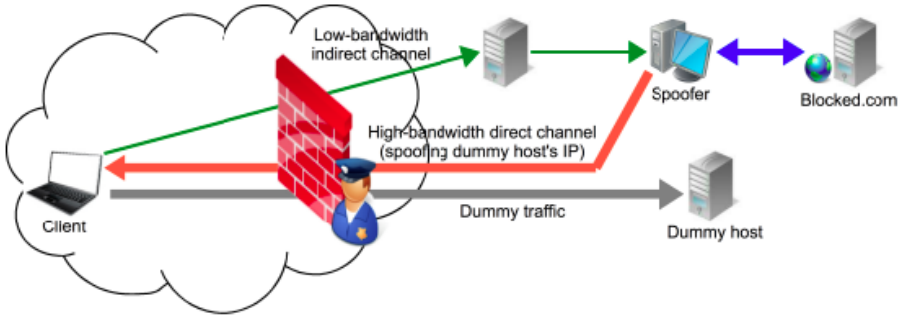
Η συγκεκριμένη λύση αποτελεί μια καλή επιλογή για την αντιμετώπιση της λογοκρισίας περιεχομένου, η οποία στοχεύει στην αύξηση του κόστους, οικονομικού αλλά και κοινωνικού, εκτέλεσης επιθέσεων λογοκρισίας περιεχομένου, εξαναγκάζοντας τις κυβερνήσεις που χρησιμοποιούν τέτοιες τεχνικές να ανέχονται ένα αρκετά μεγάλο ποσοστό, ανώνυμων επικοινωνιών στην επικράτεια τους. [184]

2.4.15 CensorSpoofer

Keywords: ***Client-Server, Framework***
Maturity: ***Proof of Concept***

Πρόκειται για ένα framework το οποίο έχει στόχο την αποτροπή της λογοκρισίας περιεχομένου κατά τη διάρκεια της περιήγησης ιστού. Για το λόγο αυτό, χρησιμοποιεί την ασυμμετρία που παρατηρείται στη δικτυακή κίνηση, χρησιμοποιώντας IP spoofing τεχνικές. Τα upstream και downstream καθίστανται πλέον ανεξάρτητα μεταξύ τους, καθώς γίνεται χρήση ενός low-bandwidth καναλιού για την πρόσβαση σε URLs και ενός high-bandwidth καναλιού για τη λήψη του αντίστοιχου περιεχομένου.

Το upstream κανάλι αποκρύπτει το περιεχόμενο των requests κάνοντας χρήση τεχνικών στεγανογραφίας μέσω mails ή instant messages, ενώ το downstream κανάλι χρησιμοποιεί IP spoofing τεχνικές για την απόκρυψη της ταυτότητας του proxy σε όλους τους χρήστες του δικτύου. Ο χρήστης προσποιείται ότι επικοινωνεί με έναν εξωτερικό dummy host και στέλνει στον spoofer το URL που οδηγεί στο λογοκριμένο περιεχόμενο στο οποίο θέλει να αποκτήσει πρόσβαση. Αντίστοιχα, ο spoofer εισάγει το λογοκριμένο περιεχόμενο στο downstream data και το στέλνει στον χρήστη, υλοποιόντας spoofing της IP Address του dummy host. [185] Η λειτουργία του CensorSpoofer framework παρουσιάζεται συνοπτικά στην παρακάτω εικόνα.

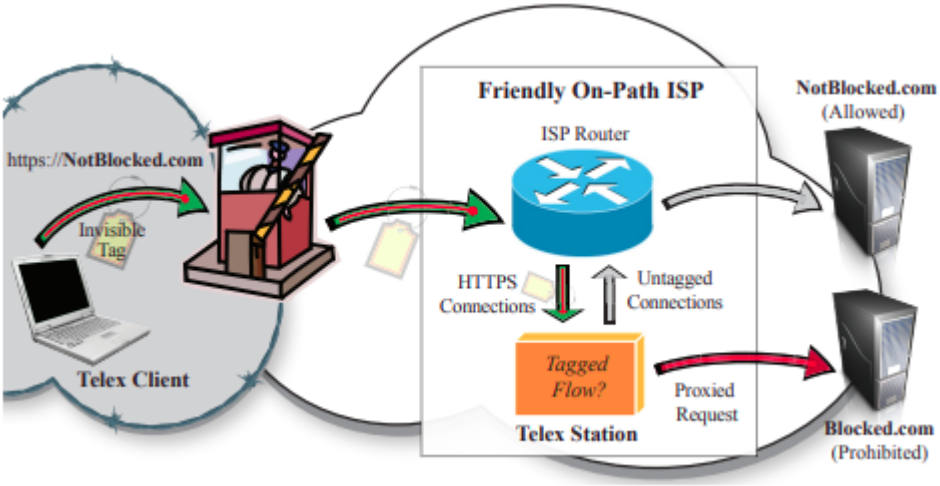


Σχήμα 2.59: Αρχιτεκτονική του CensorSpoofer.

2.4.16 Telex

***Keywords:* Client-Server, ISP, Proxies**
***Maturity:* Proof of Concept**

Το Telex εντάσσεται στην κατηγορία των τεχνολογιών αντιμετώπισης της λογοκρισίας περιεχομένου, οι οποίες επιστρατεύουν κανονικούς κόμβους και υπηρεσίες στο διαδίκτυο προκειμένου να χρησιμοποιηθούν εκείνοι ως proxies, για την πρόσβαση στο περιεχόμενο αυτό. Προϋποθέτει το deployment του σε κάποιο φίλα προσκείμενο ISP το οποίο θα αναλάβει να προωθήσει τα αιτήματα προς τον λογοκριμένο προορισμό, και αντίστοιχα ν επιστρέψει το περιεχόμενο αυτό στον τελικό χρήστη. [189] Η φιλοσοφία του προρομοιάζει πολύ αυτή των τεχνολογιών CloudTransport [184] και CensorSpoofer [185]. Η αρχιτεκτονική του Telex παρουσιάζεται συνοπτικά παρακάτω.



Σχήμα 2.60: Αρχιτεκτονική του Telex.

2.4.17 Dust

Keywords: ***Client-Server, Proxies***
Maturity: ***Proof of Concept***

Αποτελεί μια λύση για την αντιμετώπιση Censorship Attacks, προκειμένου να επιτρέψει στους χρήστες την πρόσβαση σε λογοκριμένο περιεχόμενο. Μπορεί να χρησιμοποιηθεί είτε μόνο του, είτε σε συνδυασμό με άλλες τεχνολογίες ανωνύμων επικοινωνιών για παροχή μέγιστης πρόσβασης στο λογοκριμένο περιεχόμενο. Αν συνδυαστεί με ένα anonymous proxy και με ένα anonymous publishing system, προκειμένου να προσφέρει end-to-end unobservability και censorship resistance στους χρήστες του. [190]

2.4.18 Proximax

Keywords: ***Client-Server, Proxies***
Maturity: ***Proof of Concept***

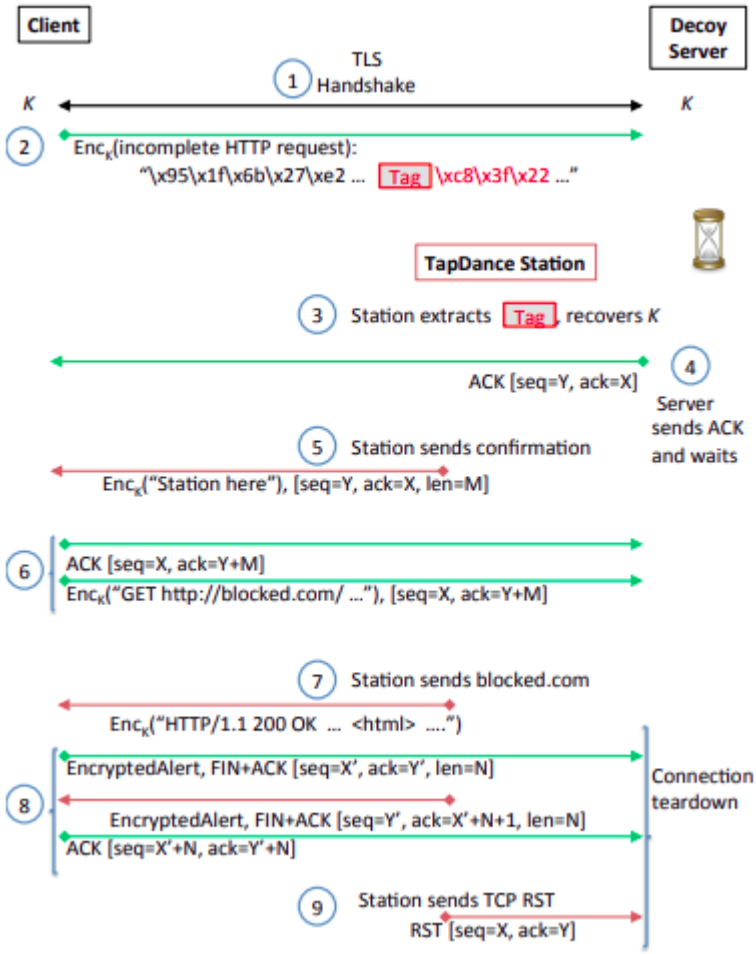
Πρόκειται για ένα σύστημα το οποίο διανέμει συνεχώς δεξαμενές με proxies σε ένα μεγάλο αριθμό channels με τρόπο τέτοιο ώστε να μεγιστοποιείται τόσο η αξιοποίηση τους από τους χρήστες αλλά και να καθίσταται δύσκολο να εντοπιστούν και να τα μπλοκάρουν οι αρχές που επιβάλλουν τη λογοκρισία περιεχομένου. Στόχος του είναι η διανομή των πόρων του δικτύου με έξυπνο τρόπο ώστε να εξυπηρετούνται οι ανάγκες των χρηστών, ενώ ταυτόχρονα να διασφαλίσει την ομαλή λειτουργία του προκειμένου να παραμένουν όσο δυνατό περισσότεροι proxies ενεργοί. [191]

2.4.19 TapDance

Keywords: ***Client-Server, TCP, TLS***
Maturity: ***Proof of Concept***

Η εν λόγω τεχνολογία αποτελεί μια εξελιγμένη μορφή των Telex και Cirripede που αναφέρθηκαν παραπάνω, και σκοπό έχει να αντιμετωπίσει τα προβλήματα ασφαλείας που προκύπτουν από τα end-to-middle σχήματα που υλοποιούν οι προαναφερθείσες τεχνολογίες. Χρησιμοποιεί μια νέα TCP-level τεχνική η οποία επιτρέπει το anti censorship σύστημα που υπάρχει στον ISP να λειτουργεί ως ένα passive network tap χωρίς ένα inline blocking component. Επίσης, χρησιμοποιεί τεχνικές

στεγανογραφίας για την ενσωματωση των control messages σε TLS ciphertext, με αποτέλεσμα να καθίσταται εφικτή η λειτουργία HTTPS συνδέσεων ακόμα και σε συνθήκες μη συμμετρικού routing. [193] Παρακάτω παρουσιάζεται συνοπτικά η λειτουργία του TapDance.



Σχήμα 2.61: Λειτουργία του TapDance.

2.5 Scalability-focused Τεχνολογίες

Στην κατηγορία αυτή εντάσσονται οι τεχνολογίες ανωνύμων επικοινωνιών που δομούνται με τρόπο τέτοιο ώστε να επιτρέπουν την εύκολη επεκτασιμότητα τους, έτσι ώστε να μπορούν μελλοντικά να αυξήσουν τον αριθμό των χρηστών τους, χωρίς να υπονομεύεται το UX τους. Οι τεχνολογίες αυτές είναι κατά κύριο λόγο peer-to-peer, κάτι που μειώνει σημαντικά την επιβάρυνση του δικτύου τόσο με διαχειριστική πληροφορία, όσο και με τον καταμερισμό της κίνησης, ωστόσο, λόγω της φύσης τους, αποτελούν πρόσφορο έδαφος για την παρείσφρηση κακόβουλων χρηστών.

2.5.1 Skipnet

***Keywords:* Peer-To-Peer, Ring Membership, Lookups**

***Maturity:* Proof of Concept**

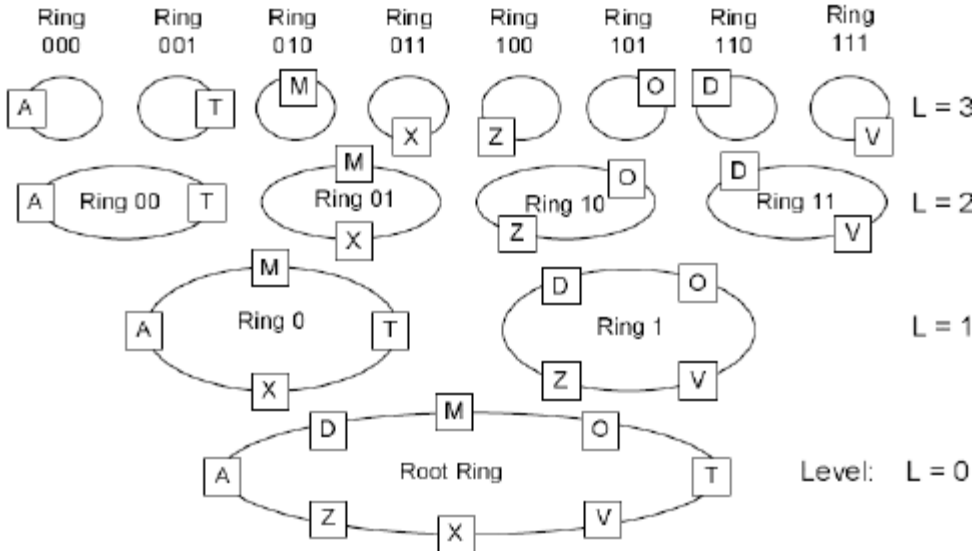
Το Skipnet βασίζει τη λειτουργία του στο SkipList, το οποίο είναι μια λίστα σύντομων σε μήκος συνδέσεων, στην οποία ορισμένοι κόμβοι έχουν δείκτες που κάνουν skip σε ορισμένα στοιχεία της λίστας, με αποτέλεσμα να μειώνουν τους χρόνους αναζήτησης σε αυτή. Το Skipnet επεκτείνει την

ιδέα αυτή σε μια τοπολογία δακτυλίου, όπου τα δεδομένα και οι κόμβοι διατηρούν συμπληρωματικούς δείκτες. Το σχημα του nameID σπιτρέπει στα κλειδιά να αποθηκεύονται σοπικά ή σε ένα σαφώς καθορισμένο διαχειριστικό domain, επιτυγχάνοντας έτσι την ιδιότητα του path locality. [67] Έτσι, η λίστα συνδέσεων μετατρέπεται σε έναν δακτύλιο διπλής σύνδεσης και περιορίζει τα lookups στο DHT μόνο στα domains που έχουν το απαιτούμενο κλειδί. Όλοι οι κόμβοι αποθηκεύουν 2logN δείκτες όπου το N υποδηλώνει τον αριθμό των P2P κόμβων. Οι δείκτες αυτοί, σε κάθε κόμβο, απαρτίζουν και το routing table.

Το δίκτυο υποστηρίζει περιορισμένης μορφής load balancing, καθώς δίνει τη δυνατότητα να χωριστούν τα αρχεία σε δύο μέρη, ένα prefix και ένα suffix. Το prefix καθορίζει το domain στο οποίο θα πρέπει να υλοποιηθεί ο διαμοιρασμός φορτίου ενώ το suffix γίνεται hashed με ομοιόμορφο τρόπο στους peers που ανήκουν στο συγκεκριμένο domain. Η αποδοτικότητα της δρομολόγησης είναι της τάξης του O(logN). Το Skipnet δημιουργεί έναν τυχαία binary bit vector για κάθε peer. Όλοι αυτοί καθορίζουν το τυχαίο ring membership των peers. Ένας δακτύλιος στο στάδιο i απαρτίζεται από όλους τους peers των οποίων οι vectors έχουν το ίδιο i-bit prefix. Κάθε επίπεδο στο δίκτυο κάνει skip σε 2^h κόμβους. [90]

Τα αρχεία αποθηκεύονται στον κόμβο ο οποίος έχει παραπλήσιο nameID στο όνομα του αρχείου, έτσι το όνομα κάθε κόμβου χρησιμοποιείται ως prefix του ονόματος αρχείου. Η αναζήτηση αρχείων γίνεται είτε με το nameID είτε με το numericID. Η αναζήτηση με βάση το πρώτο κριτήριο γίνεται με τη διάσχιση κόμβων των οποίων τα nameIDs μοιράζονται ένα prefix το οποίο δε μειώνεται, με το όνομα αρχείου που αναζητείται. Η αναζήτηση με βάση το numericID γίνεται ξεκινώντας από το πρώτο επίπεδο, έως ότου βρεθεί το numericID που ταιριάζει στο πρώτο bit της αναζήτησης. Στη συνέχεια η αναζήτηση γίνεται στο αμέσως επόμενο επίπεδο, με βάση το ταίριασμα στα δύο επόμενα bits, ενώ η διαδικασία συνεχίζεται έως ότου βρεθεί το numericID που ταιριάζει. [113]

Όταν ένας κόμβος αναχωρεί από το δίκτυο, το Skipnet συνεχίζει να λειτουργεί. Προϋπόθεση είναι το πρώτο στάδιο να διατηρείται, έτσι ώστε τα επόμενα να διορθώνονται καταλλήλως. Κάθε κόμβος διατηρεί ένα leaf-set το οποίο διατηρεί συνδέσεις προς κόμβους του πρώτου επιπέδου, έτσι ώστε να διατηρείται η δυνατότητα διατήρησης των συνδέσεων σε περίπτωση αποχώρησης κόμβων.



Σχήμα 2.62: Αρχιτεκτονική του Skipnet.

2.5.2 Bamboo

Keywords: ***Peer-To-Peer, Leafset, Recovery Mechanisms, Lookups***
Maturity: ***Proof of Concept***
Πρόκειται για έναν κατανεμημένο αλγόριθμο ο οποίος βασίζεται στο Pastry, αν και είναι πολύ πιο επεκτάσιμο σε δυναμικά περιβάλλοντα. Η δομή του βασίζεται σε δύο σετ πληροφοριών που αφορούν τους γείτονες κάθε κόμβου. Αυτά είναι το leafset, το οποίο περιλαμβάνει τους προκάτοχους και τους διάδοχους κόμβους καθώς και το routing table. Κατά τη διαρκεια μιας αναζήτησης ο προκάτοχος προωθείται έως ότου ένας κόμβος ο οποίος διαθέτει το κλειδί στο leafset του επιβεβαιώσει ότι το lookup εκτελέστηκε επιτυχώς. Για την πιο αποδοτική υλοποίηση τους, χρησιμοποιείται το routing table το οποίο περιέχει κόμβους οι οποίοι μοιράζονται ένα συγκεκριμένο prefix. [136]

Το Bamboo πραγματοποιεί lookups σε OlogN hops. Το leafset επιτρέπει τη συνέχιση της διαδικασίας στην περίπτωση που το routing table είναι ακόμα ημιτελές. Επίσης, επιτρέπει τη διατήρηση της ανθεκτικότητας του δικτύου, ακόμα και στην περίπτωση που καταρρεύσει μεγάλο ποσοστό συνδέσεων, της τάξης του 30%. Διαθέτει επίσης δύο μηχανισμούς ανάκτησης σε περίπτωση που ένας κόμβος τεθεί εκτός λειτουργίας. Αυτές είναι οι reactive και periodic recovery. Στον πρώτο μηχανισμό, σε περίπτωση που οι γείτονες ενός κόμβου τεθούν εκτός λειτουργίας γίνεται broadcast τόσο το routing table όσο και το leafset στους k-l γείτονες του. [145] Ο μηχανισμός αυτός ενδέχεται να προκαλέσει υπερφόρτωση του δικτύου όταν πολλοί κόμβοι έχουν αντιληφθεί την ίδια αποτυχία και επιχειρούν ταυτόχρονα να ενημερώσουν τους υπόλοιπους, ή όταν δεν υπάρχει αποτυχία και απλά ένας κόμβος καθυστερεί να στείλει τα keep-alive μηνύματα του. Στην περίπτωση του periodic recovery ένας κόμβος μοιράζεται περιορικά το leafset του με τα υπόλοιπα μέλη του σετ, ασχέτως αν παρατηρήθηκαν αλλαγές σε αυτό. Κάθε μηχανισμός έχει πλεονεκτήματα και μειονεκτήματα. Με μικρό churn rate, ο reactive recovery μηχανισμός είναι πολύ πιο αποδοτικός, ενώ όσο αυτός αυξάνεται, συμβαίνει το αντίθετο. Επειδή συνήθως το churn rate είναι υψηλό στο Bamboo επιλέγεται να δίνεται βάρος στον periodic recovery μηχανισμό.

Υποστηρίζονται δύο timeout μηχανισμοί. Ο πρώτος είναι ο TCP-style όπου οι κόμβοι έχουν μια γενική ιδέα για τα timeouts ώστε να υλοποιούν αναζητήσεις σε διαφορετικά μέρη του δικτύου. Ο δεύτερος είναι ο virtual coordinates μηχανισμός, στον οποίο coordinates αναθέτονται σε κάθε κόμβο, σε ένα εικονικό μετρικό περιβάλλον, όπου η καθυστέρηση μεταξύ δύο κόμβων αναπαρίσταται από μια γραμμή που τους ενώνει. [153]

2.5.3 Westermann et al’ lookup

Keywords: ***Peer-To-Peer, Lookups***
Maturity: ***Proof of Concept***
Πρόκειται για ένα πρωτόκολλο υλοποίησης κλιμακωτών lookups προς κόμβους βασισμένο στο Kademlia, το οποίο προσφέρει ανωνυμία στους χρήστες του. Όλοι οι servers διαθέτουν ένα μοναδικό nodeID και μόνο αυτοί που παρέχουν ανωνυμία στους χρήστες τους αποτελούν μέρη του DHT. Οι χρήστες χρησιμοποιούν έναν μικρό αριθμό servers που εμπιστεύονται για να υλοποιήσουν lookups. Επιπροσθέτως, τα αποτελέσματα δεν χρησιμοποιούνται αμέσως, προκειμένου να αποτραπούν τυχόν Correlation Attacks στο δίκτυο από κακόβουλους χρήστες. [25]

Οι clients δεν είναι καταχωρημένοι ως μέλη του δικτύου και προκειμένου να υλοποιήσουν ερωτήματα χρησιμοποιούν κρυπτογραφημένες συνδέσεις σε ορισμένους servers τους οποίους εμπιστεύονται

μερικώς, στους οποίους αποστέλλουν τα αποτελέσματα. Στη συνέχεια εκτελούν τα ερωτήματα και στέλνουν τα αποτελέσματα πίσω στους χρήστες. Η διαδικασία αυτή καθιστά το πρωτόκολλο ανθεκτικό απέναντι σε Fingerprinting Attacks. [40]

Το nodeID είναι το SHA-1 hash του δημοσίου κλειδιού του κόμβου στο DHT. Η χρήση κρυπτογράφησης περιορίζει την ικανότητα ενός επιτιθέμενου να επιλέγει ελεύθερα τη θέση του στο DHT, αποτρέποντας τον από το να τοποθετεί τους ίδιους descriptors πολλές φορές υπό διαφορετικές ταυτότητες ή από τα να τοποθετεί ψεύτικους descriptors για honest κόμβους.Το ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή των descriptors και των πιστοποιητικών των servers που χρησιμοποιούνται για την κατασκευή των anonymous tunnels. [63] Αυτό διασφαλίζει μια αμφιμονοσήμαντη σύνδεση μεταξύ ενός descriptor και του αντίστοιχου πιστοποιητικού ενός server. Μέσω της επιβεβαίωσης ενός πιστοποιητικού με το δημόσιο κλειδί του descriptor ο client μπορεί να ελέγξει αν ο server είναι πράγματι αυτός που αντιστοιχεί στον συγκεκριμένο descriptor.

Οι Collusion Attacks αποτελούν μια πηγή κινδύνου για το συγκεκριμένο πρωτόκολλο, όπως και οι Fingerprinting Attacks. Επίσης, δεν παρέχεται κανένα επίπεδο προστασίας απέναντι σε Sybil και Denial of Service Attacks. Έτσι, το πρωτόκολλο δεν προστατεύει επαρκώς την ανωνυμία των χρηστών όταν χρησιμοποιηθεί σε δίκτυα μεγαλύτερης έκτασης.

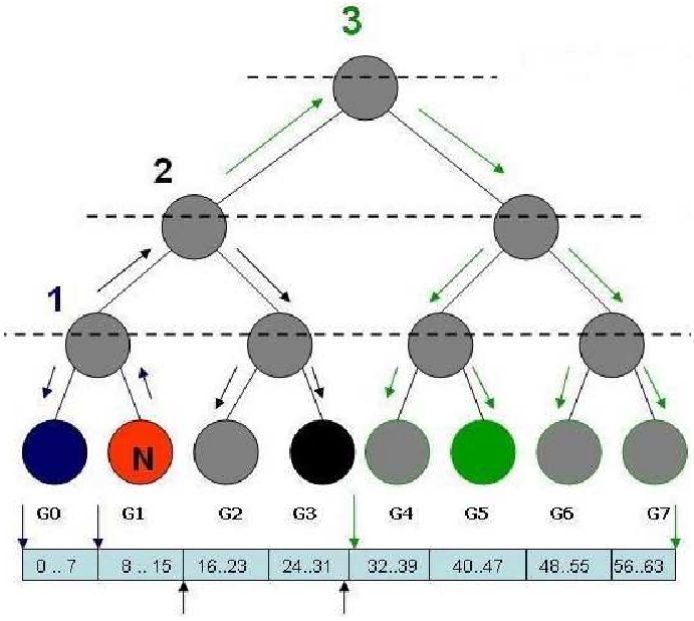
2.5.4 Salsa

Keywords: ***Peer-To-Peer, Contacts***
Maturity: ***Limited Adoption***

Το Salsa αποτελεί ένα δίκτυο ανωνύμων επικοινωνιών με κύρια επιδίωξη να ξεπεράσει τα προβλήματα που προκύπτουν από την υλοποίηση των Mix Networks σε μεγάλη κλίμακα. Η αρχή λειτουργίας του βασίζεται στη δημιουργία ενός tunnel μεταξύ του Initiator και του Recipient προκειμένου να διασφαλιστεί η ανωνυμία των επικοινωνιών. Υπάρχει διαστρωματωμένη κρυπτογράφηση, έτσι κάθε κόμβος γνωρίζει μόνο τον προηγούμενο. Κάθε κόμβος έχει περιορισμένη γνώση του δικτύου ώστε να αποφεύγεται η υπερφόρτωση του με το διαχειριστικό overhead, ενώ όλοι συμμετέχουν σε ένα global pool, από όπου επιλέγονται τυχαία για τον σχηματισμό των tunnels. [2]

Βασίζεται σε ένα distributed hash table (DHT) το οποίο αντιστοιχεί κόμβους σε ένα space ID που αντιστοιχεί στην IP Address τους. Τα δύο βασικά στοιχεία πάνω στα οποία δομείται το εν λόγω πρωτόκολλο ανωνύμων επικοινωνιών είναι ο lookup μηχανισμός και ο μηχανισμός που δημιουργεί τα tunnels. Ο lookup μηχανισμός επιστρέφει την IP Address και το Public Key ενός κόμβου του εγγύτερου στο space ID το οποίο βρίσκεται στο DHT, ενώ ο tunnel building μηχανισμός δημιουργεί τα tunnels με τρόπο παρόμοιο με αυτόν του Tor Network.

Για τη δημιουργία ενός tunnel ο Initiator επιλέγει r τυχαία IDs και αναζητεί τους αντίστοιχους κόμβους μέσω του lookup μηχανισμού. Αυτοί απαρτίζουν το πρώτο σετ κόμβων. Για κάθε έναν από αυτούς του κβους δημιουργούνται keys. Κάθε ένας από τους κόμβους που σχηματίζουν το πρώτο σετ κόμβων αναζητά με τη σειρά του r επιπλέον κόμβους, οι οποίοι απαρτίζουν το δεύτερο σετ κόμβων. Η διαδικασία αυτή συνεχίζεται καθώς το tunnel σχηματίζεται, εγκαθιστώντας κυκλώματα μεταξύ των κόμβων. Ένα από τα σχηματισθέντα μονοπάτια μεταξύ του πρώτου και του δεύτερου σετ επιλέγεται ως το anonymous tunnel. Η προεπιλογή των σετ που δημιουργούνται καθώς και του αριθμού των κόμβων που έχει κάθε σετ είναι 3 και στις δύο περιπτώσεις. [3]



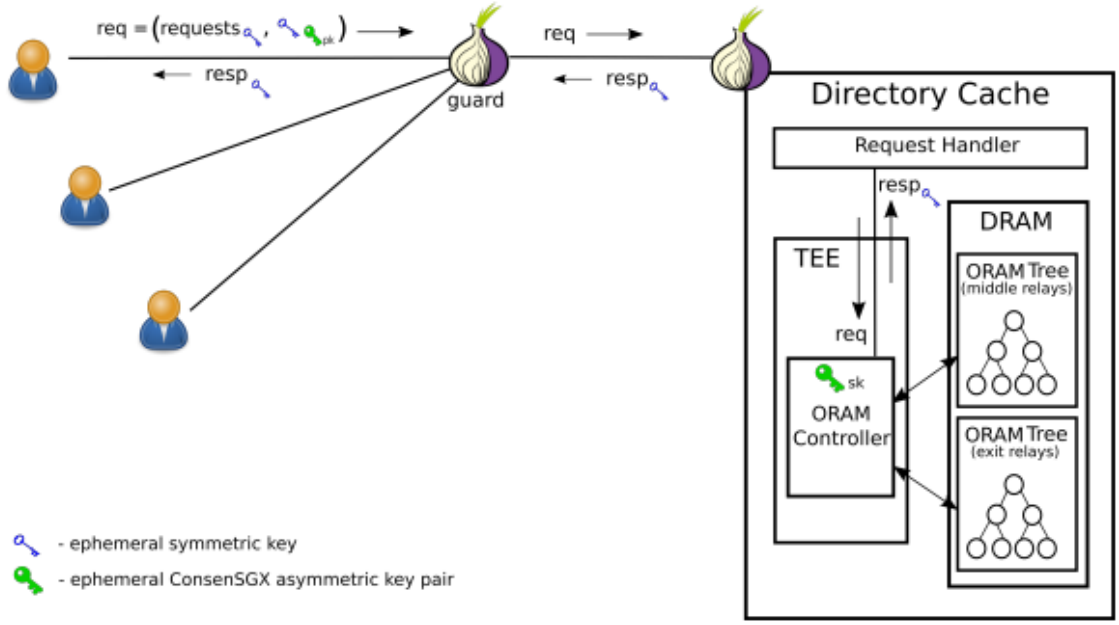
Σχήμα 2.63: Αρχιτεκτονική του Salsa.

2.5.5 ConsenSGX

***Keywords:* Client-Server, Onion Routing**

***Maturity:* Proof of Concept**

Πρόκειται για μια λύση που στοχεύει στην επεκτασιμότητα σε μεγάλη κλίμακα των ανωνύμων επικοινωνιών. Σκοπός του είναι η ανάκτηση από τους χρήστες μόνο των μερών του δικτύου τα οποία εκείνοι χρειάζονται, χωρίς να γνωρίζουν οι Directory Servers ποια κομμάτια λαμβάνουν εκείνοι. Οι clients κάνουν directory requests μέσω ενός one-hop κυκλώματος μέσω των guard relays τους. Το ConsenSGX υλοποιείται πάνω από το Tor Network. Παρακάτω παρουσιάζεται συνοπτικά η αρχιτεκτονική του. [171]



Σχήμα 2.64: Αρχιτεκτονική του ConsenSGX.

2.6 Secure Lookups-focused Τεχνολογίες

Αποτελεί μια βελτιωμένη εκδοχή των Scalability-focused τεχνολογιών, καθώς εκτός από σημαντικές δυνατότητες επέκτασης του δικτύου παρέχουν αυξημένα μέτρα ασφαλείας έναντι κακόβουλων χρηστών που εισέρχονται στο δίκτυο για την αποκάλυψη πληροφοριών οι οποίες περιέχονται στα lookups.

2.6.1 Castro et al's secure lookup

Keywords: ***Peer-To-Peer, Lookups, CRT***
Maturity: ***Proof of Concept***

Πρόκειται για ένα ισχυρό DHT σύστημα που στηρίζεται στην υπερεπάρκεια των lookups, υλοποιώντας flooding των μηνυμάτων μέσω πολλών paths. Κάθε κλειδί έχει αντίγραφα σε πολλούς κόμβους, με τον Initiator να πραγματοποιεί lookups προς όλους αυτούς τους κόμβους. Το εκάστοτε lookup παραμένει ασφαλές εφόσον σε ένα τουλάχιστον μονοπάτι δεν υπάρχουν κακόβουλοι κόμβοι.

Οι Eclipse Attacks παραμένουν ο κυριότερος κίνδυνος που αντιμετωπίζουν οι χρήστες του δικτύου. Για την αντιμετώπιση τους έχουν προταθεί τα Constrained Routing Tables (CRT), τα οποία εισάγουν ισχυρούς δομικούς περιορισμούς στα σετ γειτόνων και είναι πολύ καλός τρόπος αντιμετώπισης των προαναφερθέντων επιθέσεων, ωστόσο εισάγουν στο δίκτυο τεράστιο κόστος. [154]

Ως επιπρόσθετο μέτρο για την εξασφάλιση της ακεραιότητας των lookups έχει προταθεί και ο μηχανισμός Secure node identifier assignment, μέσω του οποίου μια κεντρική αρχή πιστοποίησης των κόμβων διασφαλίζει την ακεραιότητα τους. Επιπλέον, έχει προταθεί η τεχνική Secure routing table Maintenance η οποία εισάγει ένα παράλληλο routing table ενώ ενδιαφέρον έχει και η Secure lookups. Στην τελευταία κάθε μήνυμα υπόκειται σε ένα failure test. Αν το μήνυμα αποτύχει να παραδοθεί τότε επιστρατεύονται όλοι οι μηχανισμοί του CRT. Οι παραπάνω τεχνικές ενώ διασφαλίζουν την παράδοση των μηνυμάτων, αποτελούν πηγή παραγωγής πολλών πλεοναζόντων μηνυμάτων που επιβαρύνουν το δίκτυο. Επιπλέον, η περίσσεια μηνυμάτων μπορεί να αποτελέσει ένδειξη για τους επιτιθέμενους, οδηγώντας σε απώλεια τόσο της ιδιωτικότητας όσο και της ανωνυμίας των χρηστών. [2]

Σε δοκιμές που έχουν πραγματοποιηθεί έχει βρεθεί ότι με παρουσία κακόβουλων κόμβων στο 5% του συνόλου, μπορούν να ταυτοποιηθούν επιτυχώς έως και το 60% των lookups, ενώ με 10% ποσοστό οι επιτυχείς επιθέσεις αγγίζουν το 90%. Έτσι, ενώ το δίκτυο είναι ιδιαίτερα ανθεκτικό απέναντι σε Active Attacks, υστερεί σημαντικά απέναντι στις Passive, καθώς η διαδικασία lookup είναι ιδιαίτερα ευαίσθητη σε αυτές, ενώ αποτελεί και τη βάση της ανωνυμίας των χρηστών του δικτύου.

2.6.2 S/Kademlia

Keywords: ***Peer-To-Peer, Crypto-Puzzles, Lookups***
Maturity: ***Proof of Concept***

Αποτελεί ένα secure key-based πρωτόκολλο δρομολόγησης που βασίζεται στο Kademlia, με στόχο να γίνει πιο ανθεκτικό απέναντι στις επιθέσεις. Επιστρατεύει τη χρήση crypto-puzzles για να αποτρέψει διάφορα collusions κακόβουλων κόμβων, περιορίζοντας τη δημιουργία νέων nodeIDs με το να κάνει τη διαδικασία ιδιαίτερα δαπανηρή σε πόρους. Παρ όλα αυτά, ο επιτιθέμενος μπορεί να δημιουργήσει offline τέτοια nodeIDs πριν επιχειρήσει να εισέλθει στο δίκτυο, παρακάμπτοντας τα αυστηρά χρονικά όρια που απαιτούνται από το πρωτόκολλο. [147]

Επιπλέον, το S/Kademlia αναβάθμισε τους μηχανισμούς του πρωτοκόλλου επεκτείνοντας το routing table με μια sibling broadcast list ώστε να προστατευθεί από Storage Attacks, ενώ χρησιμοποιεί πολλά μονοπάτια που δεν επικαλύπτονται προκειμένου να προστατεύσει τα lookups από Routing Attacks. Η επέκταση αυτή του πρωτοκόλλου οδηγεί στην ανεξαρτησία των lookups, έτσι ώστε κάθε κόμβος να χρησιμοποιείται μόνο μια φορά κατά τη διαδικασία αυτή, παρέχοντας ασφάλεια στο δίκτυο.

2.6.3 Halo

Keywords: ***Peer-To-Peer, Lookups***
Maturity: ***Proof of Concept***
Το Halo βασίζεται στο Chord και προσφέρει επιπλέον ασφάλεια όσον αφορά τη διαδικασία των lookups που πραγματοποιούνται για την εύρεση κόμβων και πόρων του δικτύου. Λόγω της δομής του δικτύου, γίνεται αναζήτηση μέσω των knuckles, δηλαδή των κόμβων που έχουν άμεσα σύνδεση με τον προορισμό του lookup. Έτσι, αντί να χρησιμοποιούνται παράλληλα lookups, γίνεται αναζήτηση των κοντινών στον προορισμό κόμβων, ώστε να αποφευχθεί η χρήση των ίδιων corrupt κόμβων πολλές φορές, αν αυτοί βρίσκονται στο μονοπάτι του lookup. Το Halo είναι ανθεκτικό απέναντι σε Path Construction Attacks, ή αλλιώς Collusion Attacks, ωστόσο είναι ευπαθές σε Message Coding Attacks. [2]

2.7 Anonymous Use of Internet Applications

Στην παρούσα ενότητα αναφέρονται συνοπτικά και για λόγους πληρότητας, ορισμένες ακόμα ενδεικτικές λύσεις VPN ή Web Proxies.

- Το SmartHide αποτελεί μία εμπορική λύση Anonymizer, η οποία παρέχει τη δυνατότητα απόκρυψης της Source IP Address, καθώς ισχυρής κρυπτογράφησης της επικοινωνίας. [82]

- Το Java Anon Proxy (JAP) αποτελεί ένα anonymous proxy service διαθέσιμο για την προστασία και την ανωνυμία του χρήστη κατά τη διάρκεια του Web Surfing. Η αρχή λειτουργίας του βασίζεται στη μέθοδο του proxying, καθώς ο χρήστης συνδέεται στην τελική ιστοσελίδα μέσω μιας αλυσίδας ενδιάμεσων servers. Η αλυσίδα αυτή προσφέρεται έτοιμη στο χρήστη, ωστόσο υπάρχει η δυνατότητα παραμετροποίησης της, αλλάζοντας την αλληλουχία τους, ανάλογα με τις ανάγκες του χρήστη. [81]

- Το Hordes αποτελεί ένα πρωτόκολλο που παρέχει ανωνυμία στον εκκινητή της επικοινωνίας, χρησιμοποιώντας δρομολόγηση πολλαπλής διανομής (multicasting routing), επιτυγχάνοντας λήψη των δεδομένων χωρίς να εκτίθεται οποιοδήποτε στοιχείο ταυτοποίησης του χρήστη ή του τερματικού που χρησιμοποιεί. [81] Έχει αποδειχθεί ότι παρέχει παρόμοιο επίπεδο προστασίας της ανωνυμίας και της ιδιωτικότητας του χρήστη, με αυτό των Crowds και Onion Routing, με καλύτερες ωστόσο επιδόσεις σε αρκετούς τομείς, με χαρακτηριστικότερο το latency. [83]

- Το GTunnel είναι μια freeware υπηρεσία για το λειτουργικό σύστημα Windows και χρησιμοποιείται ως local proxy ενός Web Browser ή κάποιας άλλης εφαρμογής. Παρέχει

απόκρυψη της ταυτότητας της πηγής καθώς και ισχυρή κρυπτογράφηση του περιεχομένου που διακινείται κατά τη διάρκεια της επικοινωνίας.

- Το Your Freedom είναι ακόμα μια εμπορική λύση που εξασφαλίζει την ανωνυμία του χρήστη στις περισσότερες διαδικτυακές εφαρμογές. Απαιτείται η εγκατάσταση του client στο λειτουργικό σύστημα του χρήστη (το Your Freedom) είναι διαθέσιμο για όλα τα υπάρχοντα λειτουργικά συστήματα), η οποία, με κατάλληλη προσαρμογή των δικτυακών ρυθμίσεων, επιτρέπει όλη η κίνηση να δρομολογείται μέσω του anonymous web proxy ή του anonymous SOCKS proxy που δημιουργήθηκε από την εγκατάσταση του client.

Ακόμα μια λύση, είναι το SubRosa, που αποτελεί έναν εξομοιωτή του Tor δικτύου και υποστηρίζεται από το παγκόσμιο ερευνητικό δίκτυο PlanetLab (PLANETLAB, 2007). Στόχος του είναι η συλλογή δεδομένων δικτυακής κίνησης με σκοπό να αξιοποιηθούν, ώστε να αναπτυχθούν αλγόριθμοι που θα αντιμετωπίζουν timing attacks [19] σε συστήματα ανώνυμων επικοινωνιών.

2.8 Non-Anonymous Peer-To-Peer Τοπολογίες

Παρακάτω παρουσιάζονται για λόγους πληρότητας τα δίκτυα Chord, Pastry, Tapestry, CAN, Viceroy, Koorde και Kademlia, καθώς πολλές τεχνολογίες ανωνύμων επικοινωνιών αποτελούν προεκτάσεις τους, εξελίσσοντας τους μηχανισμούς που χρησιμοποιούν προκειμένου να επιτύχουν την προστασία της ανωνυμίας των χρηστών τους.

2.8.1 Chord

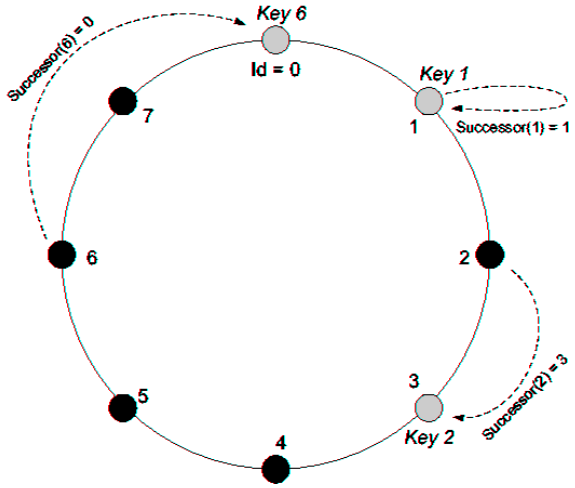
Το Chord είναι ένα επεκτάσιμο lookup πρωτόκολλο για peer-to-peer κατανεμημένα συστήματα το οποίο είναι υπεύθυνο για την ανάθεση keys στους ενεργούς κόμβους ενός δικτύου. Το σύστημα αποτελείται από 2^n κόμβους οι οποίοι μπορούν να είναι ενεργοί ή ανενεργοί. Το Chord ακολουθεί μια κυκλική διαδικασία με ένα ID space μεγέθους N που δείχνει που ακριβώς βρίσκονται οι κόμβοι. Τόσο οι identifiers όσο και τα keys βρίσκονται στο ίδιο ring. Τα μηνύματα διακινούνται κατά την ωρολογιακή φορά στο ID space. [57]

Το Chord χρησιμοποιεί έναν κατανεμημένο αλγόριθμο που βασίζεται στην hashing function SHA-1, η οποία αποτελείται consistent hashing, και αναθέτει keys στους peers. Ο αλγόριθμος έχει σχεδιαστεί με τέτοιο τρόπο ώστε να επιτρέπει στους κόμβους να εισέρχονται και να εξέρχονται από το δίκτυο προκαλώντας την ελάχιστη δυνατή αποδιοργάνωση σε αυτό, ενώ η hashing function παράγει έναν identifier αποτελούμενο από m bits τόσο για τους κόμβους όσο και για τα keys. Κάθε κόμβος n αποθηκεύει ένα routing table το οποίο περιέχει έως m καταχωρήσεις, το οποίο ονομάζεται Finger Table. Σε αυτό αποθηκεύονται οι identifiers του Chord, των peers και το port number τους. Οι διάδοχοι κόμβοι διαθέτουν επίσης Finger Tables, στα οποία οι ith καταχώρηση του κόμβου n περιέχει τη διεύθυνση του αντίστοιχου διαδόχου κόμβου $((n + 2^{i-1}) \bmod 2^m)$ κατά την ωρολογιακή φορά. [163]

Ο node identifier, γνωστός και ως nodeID δημιουργείται μέσω του hashing της IP Address, ενώ το keyID μέσω του hashing του data key. Το keyID k ανατίθεται στον πρώτο κόμβο του οποίου το nodeID είναι το ίδιο ή ακολουθεί το spaceID. Αυτός είναι και ο κόμβος που ορίζεται ως διάδοχος. Όταν ο k συνδέεται στο δίκτυο ο διάδοχος κόμβος μεταφέρει τα keys, ενώ όταν αποχωρεί από αυτό, μεταφέρει τα κλειδιά για τα οποία ήταν υπεύθυνος ο διάδοχος του. Η διαδικασία αυτή παρέχει προστασία ενάντια σε κακόβουλους χρήστες.

Το lookup γίνεται μέσω του κατακερματισμού του spaceID. Τόσο η εισαγωγή όσο και η αναζήτηση στο δίκτυο εξαρτώνται από την εύρεση του διαδόχου του εκάστοτε ID. Οποιοσδήποτε κόμβος αναζητά ένα key δε θα χρειαστεί περισσότερα από M hops. Υπό φυσιολογικές συνθήκες ένα lookup χρειάζεται $O\log_2(N))$ hops. Σε περίπτωση που ένας κόμβος τεθεί εκτός λειτουργίας, η αλυσίδα σπάει με αποτέλεσμα αφ ενός να χαθούν ορισμένα αντικείμενα, τα οποία αυτός φιλοξενούσε, αφετέρου να μη μπορούν να εντοπιστούν ορισμένα IDs. Επιπλέον, αν κάποιος κόμβος δεν αποκρίνεται στα αιτήματα για επαρκές χρονικό διάστημα, τότε οι κόμβοι ενημερώνουν τους δείκτες τους με τους αντίστοιχους του προκατόχου και του διαδόχου του κόμβου αυτού και μεταφέρουν την ευθύνη του keyID του κόμβου αυτού στους υπόλοιπους. Για την αντιμετώπιση τέτοιων προβλημάτων, αν ένας κόμβος αντιληφθεί ότι ο γείτονας του έχει τεθεί εκτός λειτουργίας τότε θα τον αντικαταστήσει με τον επόμενο κατά σειρά κόμβο στη λίστα, αντιγράφοντας όλα τα στοιχεία του failed κόμβου στον διάδοχο του. Έτσι, ο μόνος τρόπος να υπάρξει οριστική απώλεια αντικειμένων είναι να τεθούν ταυτόχρονα εκτός λειτουργίας τόσο ένας κόμβος όσο και ο διάδοχος του. [150]

Η αποκεντροποιημένη δομή του Chord έχει σαφή πλεονεκτήματα όσον αφορά το διαμοιρασμό του φορτίου, καθώς κάθε κόμβος φιλοξενεί περίπου το ίδιο πλήθος αντικειμένων, ενώ οι προσθήκες ή αποχωρήσεις κόμβων είναι μη σύνηθες φαινόμενο. Το πλήθος των αναμενόμενων hops εντός του Chord υπολογίζεται σε $0.5*\log_2 N$. Το Chord εστιάζει περισσότερο στην ανθεκτικότητα του δικτύου, ωστόσο είναι ιδιαίτερα ανθεκτικό απέναντι σε Passive Attacks όταν υλοποιείται η recursive εκδοχή του.



Σχήμα 2.65: Αρχιτεκτονική του Chord.

2.8.2 Pastry

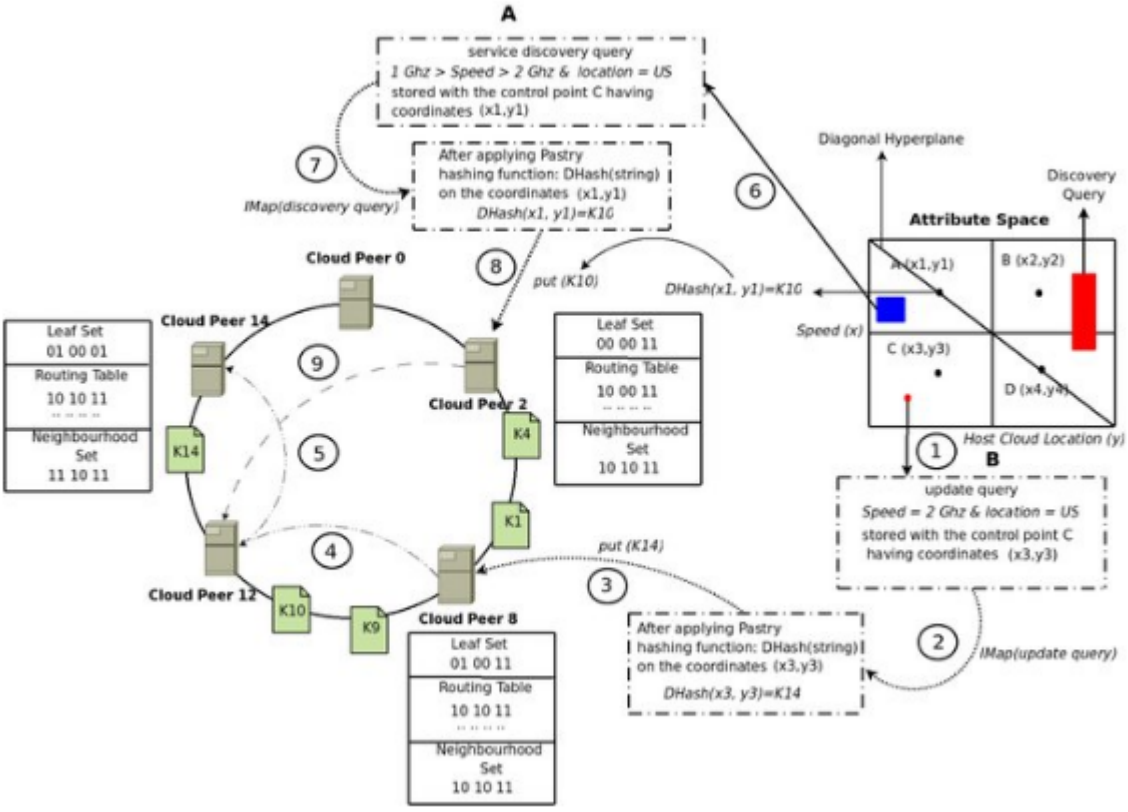
Το Pastry είναι ένα self-organized, αποκεντροποιημένο overlay network το οποίο χρησιμοποιεί prefix routing τέτοιο ώστε κάθε peer υλοποιεί δρομολόγηση των clients και των interfaces με local instances

μιας ή περισσοτέρων εφαρμογών. Ο κύριος στόχος του είναι η αποδοτική δρομολόγηση των αντικειμένων στο δίκτυο. Οι κόμβοι και τα data έχουν μια μοναδική 128-bit ID. Αυτές διανέμονται κυκλικά στο δίκτυο, παρόμοια με το Chord. Τα nodeIDs απορρέουν από το hashing της IP Address και των Public Keys. Τα IDs οργανώνονται με βάση την αριθμητική εγγύτητα τους, με αποτέλεσμα κόμβοι που έχουν παρόμοια IDs ενδεχομένως να βρίσκονται μακριά γεωγραφικά.

Κάθε κόμβος διατηρεί τρεις πίνακες, τα Routing Table, Leaf Set και Neighbourhood Set. Το Routing Table περιέχει $log_{2}^{b}N$ γραμμές και 2^{b} στήλες, με το N να είναι ο συνολικός αριθμός κόμβων στο δίκτυο. Σε μια γραμμή i υπάρχει πληροφορία σχετικά με τους κόμβους που μοιράζονται το ίδιο prefix στα πρώτα i ψηφία. Το Leaf Set είναι μια λίστα που περιέχει τους L/2 προκάτοχους κόμβους και L/2 διάδοχους κόμβους. Ο κόμβος καταγράφει τους m εγγύτερους κόμβους μέσω ενός διαφορετικού metric, όπως το delay που παρατηρείται στο δίκτυο. Το Neighbourhood Set περιέχει πληροφορίες σχετικά με τους κόμβους που παρουσιάζουν γεωγραφική εγγύτητα. [164]

Το routing στο Pastry γίνεται με έναν πολύ καθορισμένο τρόπο. Μόλις λαμβάνεται ένα μήνυμα με το key του, αρχικά γίνεται αναζήτηση στο Leaf Set. Έτσι, αν υπάρχει κάποιο ID που να παρουσιάζει εγγύτητα με το key το μήνυμα δρομολογείται εκεί. Αν αυτό δεν υλοποιηθεί, ελέγχεται το Routing Table, ώστε να διαπιστωθεί η εγγύτητα ως προς το prefix, ενώ ως τελευταία επιλογή έρχεται η δρομολόγηση του μηνύματος βάσει του Neighbourhood Set, όπου υλοποιείται δρομολόγηση του μηνύματος στον τελικό προορισμό βάσει γεωγραφικής εγγύτητας. Η τάξη μεγέθους για τα απαιτούμενα hops στο Pastry είναι $O(logN)$. [125]

Η είσοδος ενός κόμβου στο δίκτυο προϋποθέτει να γνωρίζει ήδη αυτός κάποιον άλλο κόμβο που βρίσκεται ήδη στο Pastry. Δημιουργεί μια ID την οποία στέλνει στον κόμβο που γνωρίζει. Όλοι οι nodes που βρίσκονται στο route της αρχικής αυτής επικοινωνίας αποστέλλουν τα Routing Tables τους στον νέο κόμβο, ο οποίος στη συνέχεια θα σχηματίσει τα δικά του, ενημερώνοντας αντίστοιχα τους γειτονικούς κόμβους του. Γίνεται χρήση keep-alive μηνυμάτων προκειμένου να διαπιστώνεται αν οι κόμβοι είναι λειτουργικοί ή όχι. Αν ένας κόμβος βγει εκτός λειτουργίας, οι γειτονικοί του κόμβοι ενημερώνουν το Leaf Set τους.



Σχήμα 2.66: Αρχιτεκτονική του Pastry.

2.8.3 Tapestry

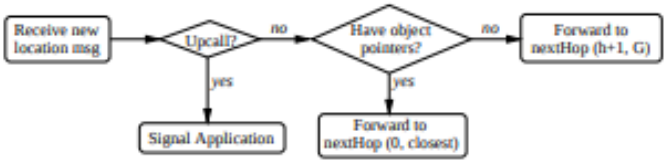
Το Tapestry είναι μια peer-to-peer overlay routing υποδομή στην οποία ανατίθενται nodeIDs στους κόμβους και τα μηνύματα δρομολογούνται ανάλογα με τα IDs αυτά. Χρησιμοποιούνται δύο δείκτες σε κάθε neighbourhood map entry έτσι ώστε να μη διαταραχθεί η δρομολόγηση σε περίπτωση που κόμβοι τεθούν εκτός λειτουργίας. Τα αντικείμενα που αποθηκεύονται στο Tapestry αντιστοιχίζονται σε έναν κόμβο. Για την ανάκτηση τους δρομολογούνται αιτήματα προς αυτό τον κόμβο δια μέσω του δικτύου.

Τόσο ο μηχανισμός lookup όσο και ο μηχανισμός routing βασίζονται στην ομοιότητα του suffix στο nodeID. Οι routing maps οργανώνονται σε επίπεδα, κάθε ένα εκ των οποίων περιέχει εγγραφές που δείχνουν προς τους εγγύτερους με βάση την απόσταση peers, οι οποίοι ικανοποιούν το suffix matching του επιπέδου αυτού. Κάθε κόμβος διαθέτει pointers προς peers που είναι οι γείτονες τους. Οι γειτνιάζοντες κόμβοι στο namespace δε γνωρίζουν την ύπαρξη των άλλων γειτόνων τους. Το Tapestry αποθηκεύει την τοποθεσία όλων των αντιγράφων των αντικειμένων που αποθηκεύονται σε αυτό, επιτρέποντας την αναζήτηση αντικειμένων με βάση κάποιο συγκεκριμένο χαρακτηριστικό, όπως η ημερομηνία δημιουργίας. [165]

Όταν το routing table ενός κόμβου δε διαθέτει εγγραφή για έναν κόμβο του οποίου το κλειδί ταιριάζει σε ένα n_{th} κλειδί τότε το μήνυμα προωθείται στον επόμενο κόμβο με την αμέσως επόμενη τιμή στο n_{th} digit modulo 2^b που βρίσκεται σε αυτό. Η διαδικασία αυτή που ονομάζεται surrogate routing αντιστοιχεί τα keys σε έναν μοναδικό, ενεργό κόμβο.

Στόχος του συγκεκριμένου δικτύου ανωνύμων επικοινωνιών είναι η γρήγορη επαναφορά του σε περίπτωση αποτυχιών όπως link failures και neighbour map corruptions. Με τη χρήση TCP timeouts το δίκτυο μπορεί να εντοπίζει και να επιδιορθώνει τις όποιες βλάβες προκύψουν γρήγορα. Για να διασφαλιστεί η επικοινωνία με τον Initiator οι κόμβοι στέλνουν περιοδικά UDP heartbeat packets. Δια μέσω του ελέγχου του ID κάθε μηνύματος που παραδίδεται καθίσταται δυνατός ο τάχιστος εντοπισμός και διαγραφή των neighbour tables που έχουν γίνει corrupted. Κάθε κόμβος διαθέτει δύο εφεδρικούς neighbours προκειμένου να διασφαλιστεί η διαθεσιμότητα του δικτύου. Κατά τη δημιουργία αντιγράφων των αντικειμένων που αποθηκεύονται στο Tapestry δημιουργείται ένα τυχαίο σετ από keys. Ο εκτιμώμενος αριθμός hops στο δίκτυο είναι $log_2^b N$. [165]

Σε περίπτωση που ένας κόμβος ανιχνευθεί ως ανενεργός από κάποιον άλλο, δεν αφαιρείται ο αντίστοιχος pointer αλλά χαρακτηρίζεται ο κόμβος αυτός ως unreachable. Σε περίπτωση που το μήνυμα δεν καταφέρει να παραδοθεί στον συγκεκριμένο κόμβο μετά την παρέλευση εύλογου χρονικού διαστήματος, ο κόμβος αυτός αφαιρείται από τον neighbour map.



Σχήμα 2.67: Αρχιτεκτονική του Tapestry.

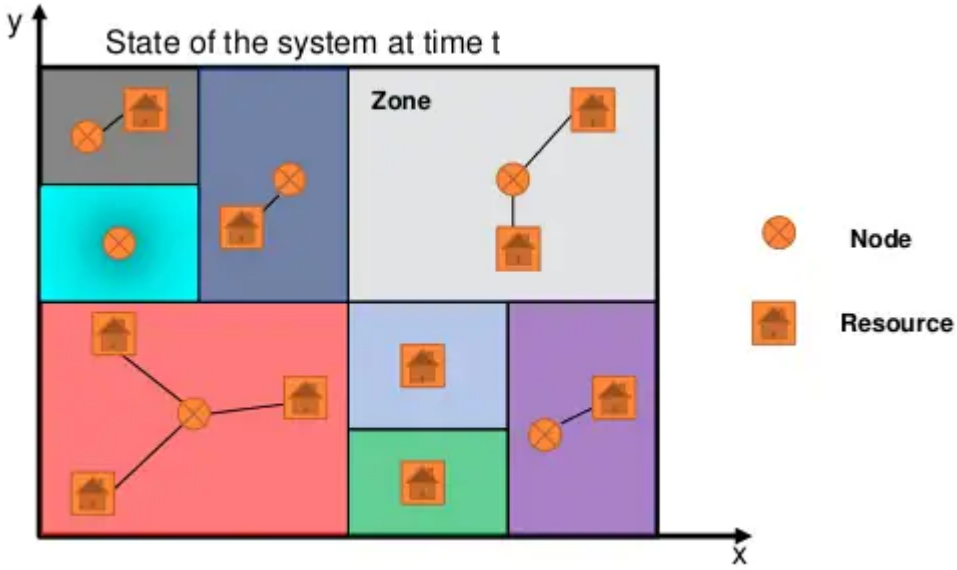
2.8.4 CAN: Content Addressable Network

Το CAN αποτελεί ένα αυτόνομο κατανεμημένο σύστημα το οποίο παρέχει hash table-like λειτουργικότητα σε πολύ μεγάλη κλίμακα. Το key space είναι ένας d-διαστάσεων χώρος καρτεσιανών συντεταγμένων στο οποίο κάθε κόμβος έχει έναν identifier που αντιστοιχείται σε ένα point P στο key space και είναι υπεύθυνο για τη ζώνη του.

Το δίκτυο δρομολογεί τα μηνύματα στον d-διαστάσεων χώρο στον οποίο κάθε κόμβος διαθέτει ένα routing table με O(d) εγγραφές και κάθε κόμβος μπορεί να είναι προσβάσιμος σε κατά μέσο όρο $(d/4)N^{\frac{1}{d}}$ hops. Οι εγγραφές αναφέρονται στους γείτονες του κόμβου στον χώρο αυτό, η δε δρομολόγηση γίνεται χρησιμοποιώντας μόνο πληροφορίες σχετικά με τους γείτονες κόμβους και τις ζώνες τους. Τα βασικά requests για τα κλειδιά είναι τα insert, lookup και delete και δρομολογούνται στους κόμβους χρησιμοποιώντας έναν greedy routing algorithm. Κάθε κόμβος χρειάζεται να διατηρεί την κατάσταση λίγων μόνο κόμβων στο δίκτυο, επιτρέποντας την επεκτασιμότητα του δικτύου. Δημιουργούνται κλειδιά με βάση τα αντίγραφα του περιεχομένου τα οποία μπορούν να αποθηκευτούν σε διαφορετικές τοποθεσίες. Σημαντικό είναι ότι τα routing tables του CAN δεν αλλάζουν μέγεθος ανεξαρτήτως από το πώς κλιμακώνεται το δίκτυο και το μέγεθος έχει. [2]

Σε περίπτωση αποτυχίας ενός κόμβου υπάρχει πρόβλεψη για άμεση αποκατάσταση του route ενώ το lookup γίνεται με την υλοποίηση ενός μονοπατιού ευθείας γραμμής μέσα στον d-διαστάσεων χώρο. Αν ένας κόμβος επιθυμεί να αποχωρήσει από το δίκτυο, τότε αυτός παραδίδει τη ζώνη του και τη σχετική key-value pair database σε έναν από τους γείτονες του. Αναλόγως του αν οι δύο αυτές ζώνες μπορούν να ενωθούνε, δημιουργείται μια καινούρια ζώνη ή η ζώνη του κόμβου που αποχώρησε παραχωρείται στον κόμβο με τη μικρότερη εκείνη τη στιγμή ζώνη. Αν ένας κόμβος αποτύχει αναλαμβάνει ο take over αλγόριθμος.

Οι γειτνιάζοντες κόμβοι μπορούν να είναι σε μεγάλη απόσταση μεταξύ τους, ενώ μπορούν να εισέρχονται ή να αποχωρούν από το δίκτυο χωρίς περιορισμούς αλλάζοντας τις ζώνες κατά περίσταση. Αυτό κάνει το δίκτυο ασταθές και ευάλωτο απέναντι σε DoS Attacks καθώς οι παραπάνω μηχανισμοί επιτρέπουν σε έναν επιτιθέμενο να έχει τον ταυτόχρονο έλεγχο πολλών ζωνών και να καταφέρει να απομονώσει ή να εξαντλήσει τους πόρους του στόχου του.



Σχήμα 2.65: Αρχιτεκτονική του CAN.

2.8.5 Viceroy

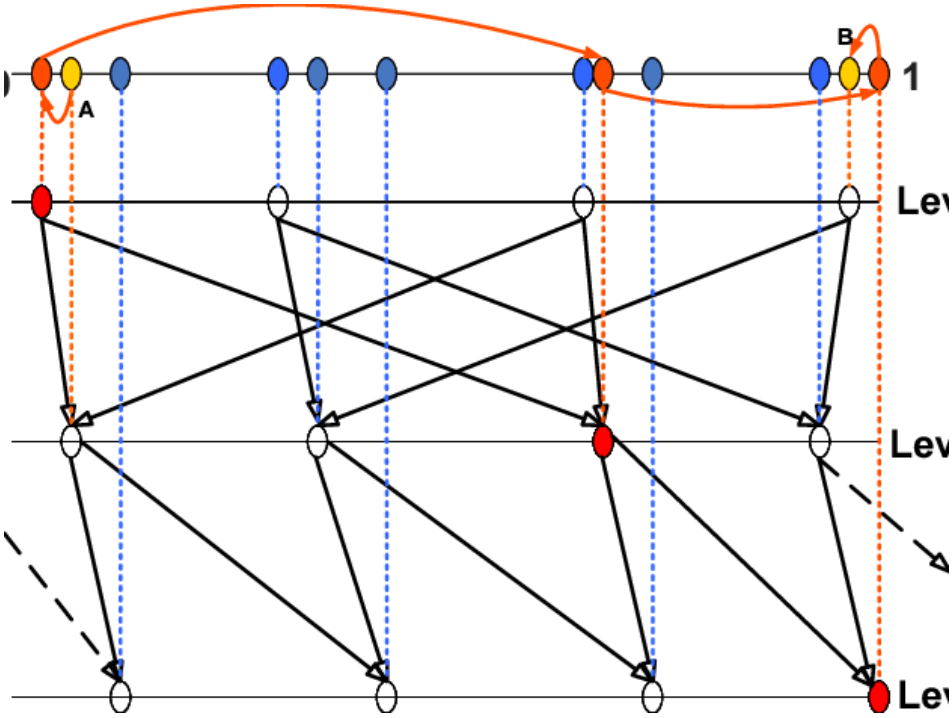
Το Viceroy αποτελεί ένα ακόμα βασισμένο στο DHT overlay peer-to-peer δίκτυο το οποίο προορίζεται για την εύρεση δεδομένων και πόρων σε ένα δίκτυο με μια butterfly τεχνική. Κάθε κόμβος στο δίκτυο μπορεί να αναζητήσει, βάσει ονόματος, πόρους που βρίσκονται διαθέσιμοι στο δίκτυο. Το hashing διασφαλίζει ομοιόμορφη και ισορροπημένη κατανομή των δεδομένων στο δίκτυο. Το ID space οργανώνεται σε έναν δακτύλιο μήκους 1, δημιουργώντας ένα overlay σε σχήμα πεταλούδας στο οποίο οργανώνονται οι γείτονες σε $\log_2 N$ επίπεδα, όπου N ο αριθμός των κόμβων του δικτύου. Οι κόμβοι του 1ου επιπέδου συνδέονται μέσω ακμών με τους peers του l+1 επιπέδου. Ένας κάτω-δεξιά κόμβος προστίθεται στην επαφή με τη μεγαλύτερη απόσταση, στο επίπεδο l+1, σε απόσταση $1/(2)^l$, ενώ ένας κάτω-αριστερά κόμβος προστίθεται στην επαφή του δακτυλίου με τη μικρότερη απόσταση. [166]

Κάθε κόμβος, εκτός από αυτούς που ανήκουν στο 1ο επίπεδο, έχουν έναν άνω δείκτη και κάθε κόμβος, εκτός από εκείνους που ανήκουν στο τελευταίο επίπεδο, διαθέτουν δύο κάτω δείκτες, ενν μεγάλο και έναν μικρό. Οι τρεις αυτοί δείκτες αποκαλούνται butterfly pointers. Κάθε κόμβος διαθέτει pointers προς άλλους pointers που βρίσκονται εντός κοντινής απόστασης, ανεβάζοντας τον συνολικό αριθμό outgoing pointers κάθε κόμβου στους 7.

Για την αναζήτηση ενός πόρου στο δίκτυο ένας κόμβος ακολουθεί τον άνω δείκτη έως ότου φτάσει στο επίπεδο 1. Από εκεί, χρησιμοποιεί τους κάτω δείκτες για να μετακινηθεί στο δέντρο. Σε κάθε hop ο κόμβος θα πρέπει να διασχίσει μια απόσταση βάσει του δείκτη τέτοια ώστε να μην είναι μεγαλύτερη από τον προορισμό x. Στη χειρότερη περίπτωση, όλοι οι κόμβοι μπορούν να προσεγγιστούν τόσο προς τα πάνω όσο και προς τα κάτω. Με ενδεικτικό αριθμό hops (OlogN), ένας

κόμβος μπορεί να προσεγγιστεί για την εύρεση ενός πόρου έως ότου δεν υπάρχουν επιπλέον κάτω δείκτες. [2] [146]

Ένας κόμβος μπορεί να εισέλει στο δίκτυο αφού βρει τους διάδοχους κόμβους του, διαμορφώσει τους δείκτες του δακτυλίου και λάβει τα απαιτούμενα αντικείμενα από τον s. Ύστερα, επιλέγει κάποιο επίπεδο βάσει του συνολικού αριθμού των κόμβων. Βρίσκει, βάσει lookups και διάσχισης του δακτυλίου, τους υπολειπόμενους pointers. Η αναχώρηση από το δίκτυο προϋποθέτει την παράδοση των ζευγαριών κλειδιών στον διάδοχο στο δακτύλιο κόμβο, όπως και των αντικειμένων που φιλοξενεί, ώστε να εξασφαλιστεί η ακεραιότητα του δικτύου.



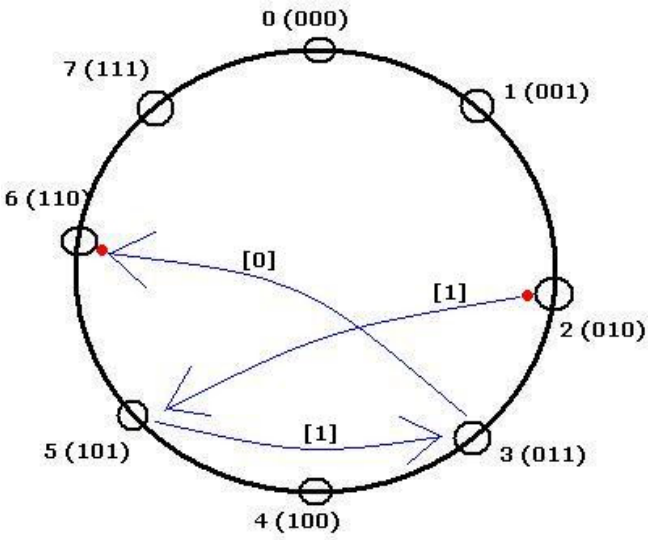
Σχήμα 2.68: Λειτουργία του Viceroy.

2.8.6 Koorde

Η εν λόγω τεχνολογία βασίζεται στο Chord και τους Γράφους De Bruijn, μέσω των οποίων διατηρείται ένας μόνιμος αριθμός αιχμών για τη συγκράτηση του overhead σε χαμηλά επίπεδα. Ένας κόμβος και ένα κλειδί διαθέτουν identifiers οι οποίοι κατανέμονται σε έναν 2^d χώρο. Ένα οποιοδήποτε κλειδί αποθηκεύεται στον διάδοχο κόμβο, ο οποίος ορίζεται ως ο κόμβος που έχει το αμέσως επόμενο ID στον χώρο. Για την εισαγωγή ενός De Bruijn γράφου απαιτείται κάθε κόμβος να γνωρίζει τον διάδοχο του στο δίκτυο καθώς και τον πρώτο De Bruijn κόμβο. Ένας De Bruijn γράφος διαθέτει δύο δείκτες σε κάθε κόμβο στον γράφο. Κάθε nodeID αποτελεί μια σειρά δυαδικών ψηφίων, έτσι κάθε κόμβος συνδέεται με κόμβους που έχουν identifiers 2m και 2m+1, με το m να είναι μια δεκαδική τιμή του nodeID.

Για την αναζήτηση ενός κλειδιού k, γίνεται η αναζήτηση του διαδόχου κόμβου διασχίζοντας τον De Bruijn γράφο. Κάθε κόμβος έχει ως identifier έναν n-m bits συνδυασμό, όπου n είναι οι base values του γράφου και m τα resolution bits. Μέσω αυτής της ταξινομημένης διασυνδεσιμότητας των κόμβων, το Koorde επιτυγχάνει να έχει μειωμένο μέγεθος routing tables, ακολουθώντας κατά τα άλλα τον αλγόριθμο του Chord.

Έχει τη δυνατότητα να επιτύχει υψηλά ποσοστά επιδόσεων με πολύ μικρό αριθμό links, ενώ μπορεί να υλοποιεί lookups με (logN)/(log(logN)) hops, όταν κάθε κόμβος έχει logN γείτονες. Για να είναι επεκτάσιμο το δίκτυο το key space πρέπει να τροποποιηθεί κατάλληλα. Το μεγαλύτερο μειονέκτημα του αφορά την ανάγκη αυτή ακριβώς να διατηρείται μια αυστηρά καθορισμένη ταξινόμηση των κόμβων στο δίκτυο καθώς και τη συχνή ανάγκη αναδιοργάνωσης του όταν αυτό επεκτείνεται, με αποτέλεσμα να οδηγείται σε υψηλά διαχειριστικά κόστη. Επιπλέον, ορισμένοι κόμβοι θα έχουν αισθητά αυξημένη κίνηση, της τάξης του θlogN από τον μέσο όρο.



Σχήμα 2.69: Αρχιτεκτονική του Koorde.

2.8.7 Kademlia

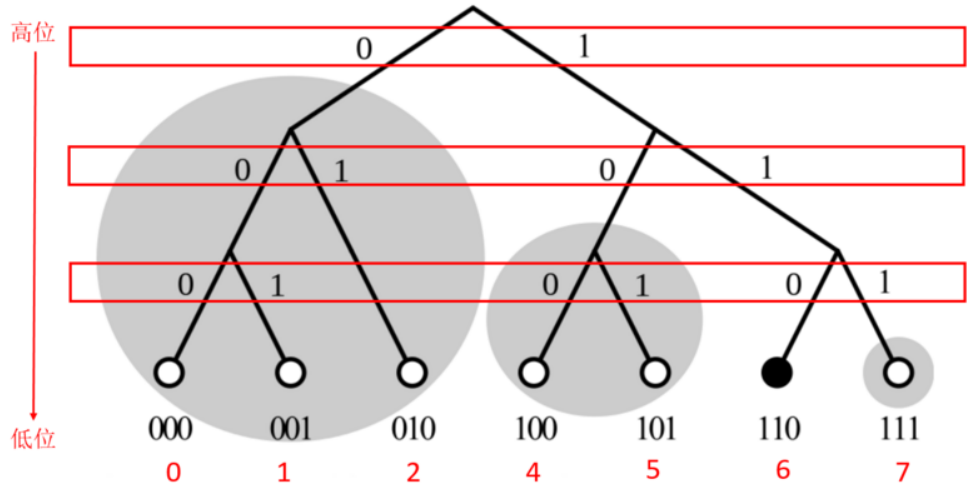
Το Kademlia αποτελεί πρωτόκολλο το οποίο εστιάζει στο συνδυασμό των τρόπων λειτουργίας των Pastry και Chord, χρησιμοποιώντας bitwise XOR operations για να υπολογίσει την απόσταση από τον εκάστοτε κόμβο. Δημιουργεί partitions στο ID space, όπου τα NodeIDs είναι φύλλα ενός δυαδικού δέντρου. Το κύριο δέντρο χωρίζεται σταδιακά σε επιμέρους, διατηρώντας σύνδεση με όλα τα υποδέντρα του. Για κάθε υποδέντρο διατηρούνται k επαφές αντί για μια, που αποκαλείται k-bucket. Σε αυτά τα buckets διατηρούνται εγγραφές σχετικά με τις επαφές ταξινομημένες σε μια last seen-least-recently-seen σειρά. Κάθε bucket μπορεί να διατηρείσαι έως k εγγραφές. [151]

Κάθε κόμβος έχει ένα nodeID, ενώ μέσω ενός SHA-1 αλγορίθμου δημιουργείται ένα κλειδί μήκους 160 bits για κάθε έναν από αυτούς. Μέσω της πολιτικής που ακολουθείται, κάθε κόμβος γνωρίζει περισσότερες λεπτομέρειες σχετικά με τους κοντινούς του παρά σε σχέση με τους μακρινούς του. Το lookup γίνεται με τρόπο συνεχή και ταυτόχρονο. Σε κάθε αναζήτηση πρώτα γίνεται εύρεση του υποδέντρου στο οποίο ανήκει ο κόμβος, και στη συνέχεια στέλνονται ερωτήματα σε α κόμβους από αυτούς που βρίσκονται στο bucket. Κάθε κόμβος επιστρέφει ένα μικρότερο υποδέντρο. Η ίδια διαδικασία συνεχίζεται έως ότου εντοπιστεί το nodeID. Το lookup ολοκληρώνεται σε O(logN) hops. [2]

Το Kademlia χρησιμοποιεί parallel, asynchronous queries έτσι ώστε να αποφύγει καθυστερήσεις που οφείλονται σε κόμβους που δεν είναι πια ενεργοί. Κάθε λίστα ανήκει σε μια συγκεκριμένη απόσταση

από τον κόμβο ο οποίος έχει αναλάβει να υλοποιεί τα ερωτήματα. Επίσης, χρησιμοποιείται ένα routing table μήκους 128 bits το οποίο επιτρέπει την υλοποίηση ταχύτερων queries.

Όταν ένας κόμβος θέλει να εισέλθει στο πρωτόκολλο τότε τοποθετείται στον κατάλληλο k-bucket και ξεκινάει μια αναζήτηση προς αυτόν, επιτρέποντας τη συλλογή πληροφοριών για τους άλλους κόμβους. Τέλος, ο κόμβος n ανανεώνει όλους τους k-buckets του. Αν κάποιος κόμβος εντοπίσει ότι κάποια από τα κλειδιά του νέου κόμβου είναι πιο κοντά σε άλλο κόμβο, τότε αντιγράφει τα κλειδιά αυτά σε εκείνον. Όσο πιο δημοφιλές είναι ένα κλειδί, τόσο πιο συχνά αναζητάται και τόσο πιο συχνά εμφανίζεται σε διαφορετικούς κόμβους, με αποτέλεσμα να εντοπίζεται συντομότερα.



Σχήμα 2.70: Αρχιτεκτονική του Kademlia.

Μέρος III

Αδυναμίες Ανωνύμων Επικοινωνιών

3.1 Επιθέσεις Εναντίων των Τεχνολογιών Ανώνυμων Επικοινωνιών

Οι ανώνυμες επικοινωνίες είναι συχνός στόχος κυβερνοεπιθέσεων, οι οποίες είναι δυνατόν να διεξαχθούν είτε από εγκληματίες του κυβερνοχώρου (hackers) είτε και από κυβερνήσεις ή επίσημες αρχές, που επιθυμούν να παρακολουθήσουν τις ηλεκτρονικές κινήσεις και συνομιλίες συγκεκριμένων ατόμων ή οργανισμών. Καθίσταται φυσικά προφανές ότι ο κύριος στόχος των επιθέσεων αυτών είναι η αποκάλυψη της ταυτότητας των χρηστών που επιθυμούν να αποκρύψουν τα στοιχεία τους. Οι επιθέσεις αυτές μπορούν να κατηγοριοποιηθούν σε παθητικές και ενεργητικές. [81]

Οι παθητικές επιθέσεις (passive attacks) είναι οι δυσκολότερες να ανιχνευτούν, καθώς ο κακόβουλος χρήστης δεν επεμβαίνει στην ανώνυμη σύνδεση ενεργά. Ουσιαστικά, ο εισβολέας επιχειρεί να

“κρυφακούσει” την ανώνυμη σύνδεση (eavesdropping) χωρίς να μεταβάλλει την κατάσταση του δικτύου. Στόχος τέτοιου είδους επιθέσεων είναι κυρίως η αναγνώριση (reconnaissance) τεχνολογιών και δικτυακών πρωτοκόλλων, προκειμένου να σχεδιαστεί καλύτερα η επίθεση εναντίον του στόχου. Έτσι, τα δεδομένα που ανταλλάσσονται κατά τις ανώνυμες επικοινωνίες, δεν μεταβάλλονται, γεγονός που καθιστά τον εντοπισμό τους ιδιαίτερα δύσκολο. [28]

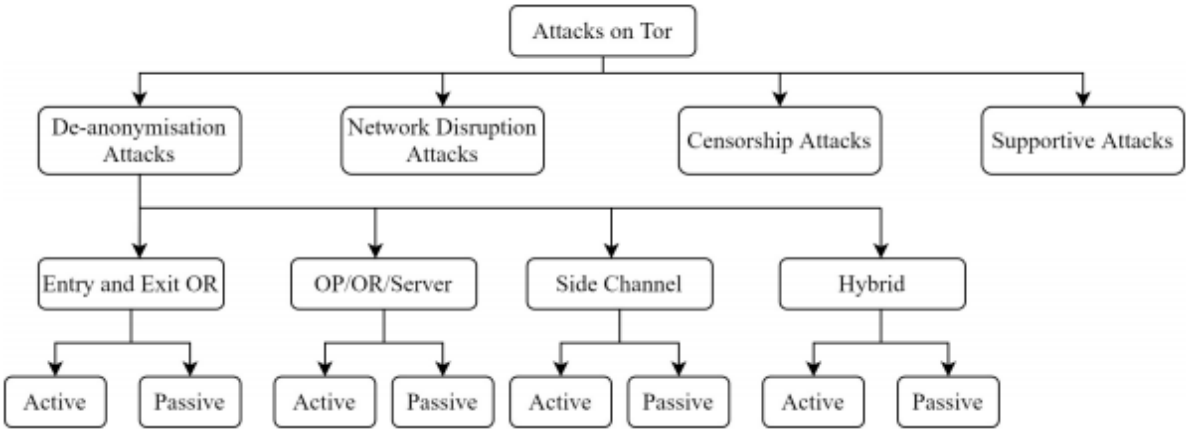
Αντίθετα, οι ενεργητικού τύπου επιθέσεις (active attacks) έχουν σκοπό την αντιγραφή, την αλλοίωση, τη διαγραφή ή ακόμα και την πλήρη διακοπή της ροής δεδομένων μεταξύ των επικοινωνούντων κόμβων. Σε αυτού τους είδους τις επιθέσεις είναι δυνατή η υποκλοπή δεδομένων, ακόμα και η καταστροφή συστημάτων που αποτελούν την υποδομή των ανώνυμων επικοινωνιών (anonymous servers, onion routers κλπ). Οι ενεργητικές επιθέσεις μπορεί να έχουν πολύ πιο σοβαρές συνέπειες, ωστόσο, λόγω των εμφανών αποτελεσμάτων τους, είναι πιο εύκολο να εντοπιστούν και να ληφθούν τα απαραίτητα αντίμετρα. Οι ενεργητικού τύπου επιθέσεις μπορεί να είναι ήπιες, όπως man-in-the-middle attacks(MitM), να περιλαμβάνουν τακτικές όπως πλαστοπροσωπία (impersonation) και η υποκλοπή συνεδρίας (session highjacking), μέχρι και πλήρως καταστροφικές, όπως οι Denial of Service attacks. [2]

Στις περισσότερες περιπτώσεις, οι παθητικές και ενεργητικές επιθέσεις χρησιμοποιούνται ταυτόχρονα, με στόχο να καταστεί πιο αποτελεσματική η επίθεση. Ένα χαρακτηριστικό παράδειγμα, είναι να εκτελεστεί μια παθητική επίθεση αναγνώρισης του ανώνυμου δικτυακού πρωτοκόλλου/εφαρμογής που χρησιμοποιεί ο στόχος, και στη συνέχεια να ακολουθήσει μια MitM επίθεση, με σκοπό να υποκλαπούν οι πληροφορίες που ανταλλάσουν τα συνομιλούντα μέρη.

Οι επιθέσεις, εκτός από την κατηγοριοποίηση τους σε παθητικού και ενεργητικού τύπου, μπορούν να διακριθούν επίσης και σε εσωτερικές και εξωτερικές. Στις εσωτερικές επιθέσεις, το επιτιθέμενο μέρος αποτελεί χρήστη του δικτύου (πχ είναι χρήστης του Freenet/Darknet ή του Tor) και μέσω αυτού εκτελεί τις επιθέσεις του προκειμένου να αποκαλύψει την ταυτότητα του στόχου του. Αντίθετα, στις εξωτερικές επιθέσεις, το επιτιθέμενο μέρος δεν αποτελεί μέρος του δικτύου και εκτελεί την επίθεση του από κάποιο άλλο περιβάλλον. [26]

Τέλος, ακόμα μια διαφοροποίηση έγκειται στις δυνατότητες του επιτιθέμενου να προσαρμόζουν τους πόρους που θέλουν να υποκλέψουν ή να καταστρέψουν κατά τη διάρκεια της επίθεσης. Έτσι, έχουμε τις στατικές (Static) επιθέσεις στις οποίες ο κακόβουλος χρήστης επιλέγει εξ αρχής τους πόρους που θέλει να υποκλέψει και δε μπορεί να τους αλλάξει μόλις η επίθεση ξεκινήσει. Αντίθετα, οι προσαρμοστικές (adaptive) επιθέσεις, αν και πιο πολύπλοκες στην υλοποίηση τους, επιτρέπουν στον επιτιθέμενο να μεταβάλλουν τους επιθυμητούς πόρους, έχοντας τη δυνατότητα να ακολουθήσουν μια ροή μηνυμάτων, και έτσι να αποσπάσουν μεγαλύτερο εύρος πληροφοριών. [81]

Οι επιθέσεις εναντίων των δικτύων ανωνύμων επικοινωνιών ταξινομούνται επίσης και με βάση τον κύριο στόχο στα δικτυακά πρωτόκολλα που χρησιμοποιούνται. Στην παρακάτω εικόνα, φαίνεται η κατηγοριοποίηση των επιθέσεων εναντίον του Tor, η οποία ισχύει για όλες τις τεχνολογίες ανωνύμων επικοινωνιών.



Σχήμα 3.1: Επιθέσεις στο Tor σε Επίπεδο Δικτύου.

Στην πρώτη κατηγορία, συναντούμε τις De-anonymization Attacks. Αυτές αποτελούν την πλειοψηφία των επιθέσεων που γίνονται στα δίκτυα ανωνύμων επικοινωνιών και έχουν στόχο να αποκαλύψουν την ταυτότητα και τη δραστηριότητα των χρηστών οι οποίοι συμμετέχουν στο δίκτυο. Οι De-anonymization Attacks συνήθως έχουν στόχο να ταυτοποιήσουν τους χρήστες (δηλαδή να βρουν την πραγματική IP Address ενός χρήστη), καθώς και να συλλέξουν πληροφορίες σχετικά με τους ιστότοπους και τα web services που αυτοί επισκέπτονται. Οι επιθέσεις αυτές είναι αρκετά συνήθεις όχι μόνο από hackers αλλά και από διάφορες υπηρεσίες επιβολής του νόμου οι οποίες θέλουν να αποκαλύψουν παράνομες συναλλαγές στο διαδίκτυο, των οποίων η πλειοψηφία λαμβάνει χώρα μέσω δικτύων ανωνύμων επικοινωνιών, για ευνόητους λόγους. Ένας άλλος στόχος των επιθέσεων αυτών είναι η ανακάλυψη της πραγματικής IP Address κάποιου Hidden Service, στο οποίο λαμβάνουν χώρα παράνομες δραστηριότητες (αγοραπωλησίες ναρκωτικών ουσιών και όπλων, διακίνηση παιδικής πορνογραφίας, κυβερνοεπιθέσεις κλπ). [2] [203]

Οι De-anonymization Attacks, ως η πολυπληθέστερη κατηγορία επιθέσεων αποτελείται από διαφόρων ειδών επιθέσεις, οι περισσότερες εκ των οποίων εντάσσονται στις Traffic Analysis Attacks. Αυτού του είδους οι επιθέσεις βασίζονται στην παρατήρηση της δικτυακής κίνησης προκειμένου ο επιτιθέμενος να εξάγει χρήσιμα συμπεράσματα σχετικά με αυτή και εν τέλει να αποκαλύψει την ταυτότητα του χρήστη ή του web service με το οποίο επικοινωνεί. Οι Traffic Confirmation Attacks αποτελούν χαρακτηριστικό παράδειγμα, στις οποίες ο επιτιθέμενος παρατηρεί τη δικτυακή κίνηση από και προς το δίκτυο προσπαθώντας να συνδέσει την πηγή με τον προορισμό, επιβεβαιώνοντας την κίνηση του χρήστη προς έναν άλλο χρήστη ή προς κάποιο service. Οι Correlation Attacks λειτουργούν με παρόμοιο τρόπο, έχοντας στόχο να διασυνδέσουν τη δικτυακή κίνηση που παρατηρείται σε διάφορα σημεία του δικτύου ανωνύμων επικοινωνιών με την ταυτότητα του χρήστη. Χαρακτηριστικό παράδειγμα των Correlation Attacks είναι οι Timing Attacks και οι Watermarking Attacks, με τις τελευταίες να είναι επιθέσεις ενεργητικού τύπου, καθώς ο επιτιθέμενος εισάγει στοιχεία στη δικτυακή κίνηση προκειμένου να δημιουργήσει ένα διακριτό μοτίβο το οποίο θα του επιτρέψει να εξάγει συμπεράσματα σχετικά με την ταυτότητα και τη δραστηριότητα του στόχου. [26] [28]

Η δεύτερη κατηγορία περιλαμβάνει τις Network Disruption Attacks. Στόχος των επιθέσεων αυτών είναι να καταστήσουν το δίκτυο και τις υπηρεσίες που φιλοξενεί ανίκανο να δεχθεί άλλες συνδέσεις και έτσι να μην μπορεί να εξυπηρετήσει άλλους πιθανούς πελάτες. Οι πιο συνήθεις επιθέσεις είναι οι Denial of Service Attacks που σκοπό έχουν να καταναλώσουν τους πόρους του δικτύου.

Παραδείγματα τέτοιων επιθέσεων στο Tor Network είναι οι Sniper Attacks, οι Packet Spinning Attacks και οι CellFlood Attacks. [203]

Μια ακόμα κατηγορία, είναι οι Censorship Attacks. Ένα μεγάλο μέρος των χρηστών των δικτύων ανωνύμων επικοινωνιών δεν κάνει χρήση των συγκεκριμένων τεχνολογιών επειδή θέλει να προβεί σε έκνομες ενέργειες, αλλά επειδή οι τεχνολογίες αυτές δίνουν τη δυνατότητα παράκαμψης των περιορισμών πρόσβασης σε υπηρεσίες και περιεχόμενο (censorship) που επιβάλλονται από τις εκάστοτε αρχές (πχ απαγόρευση χρήσης του Facebook στην Κίνα). Έτσι, μέσω των Censorship Attacks οι αρχές και οι υπηρεσίες επιβολής του νόμου έχουν στόχο να περιορίσουν την πρόσβαση των χρηστών των ανωνύμων δικτύων στο απαγορευμένο, σύμφωνα με τους νόμους, περιεχόμενο, χωρίς ωστόσο να διαταράσουν τη λειτουργία του δικτύου ή να στοχοποιούν συγκεκριμένους χρήστες. [2]

Το τελευταίο είδος επιθέσεων είναι οι Supportive Attacks. Αυτές οι επιθέσεις δεν έχουν κάποιο στόχο στο δίκτυο από μόνες τους, παρά λειτουργούν υποστηρικτικά προς άλλες επιθέσεις. Χαρακτηριστικό παράδειγμα είναι οι Sybil Attacks, μέσω των οποίων ο επιτιθέμενος προσπαθεί να αποκτήσει μεγάλη επιρροή στο δίκτυο, διευκολύνοντας σε πολύ μεγάλο βαθμό μετέπειτα De-anonymization, Network Disruption και Censorship Attacks. [2]

3.1.1 Κατηγοριοποίηση Επιτιθέμενων

Για την καλύτερη κατανόηση του τρόπου υλοποίησης των επιθέσεων, αξίζει να αναλυθούν οι συνηθέστερες κατηγορίες επιτιθέμενων γενικότερα σε δίκτυα υπολογιστών, προκειμένου να γίνει καλύτερα κατανοητό το μοντέλο κινδύνου που εισάγει κάθε κατηγορία καθώς και οι δυνατότητες τους αλλά και οι αδυναμίες τους. Η κατηγοριοποίηση αυτή είναι πολύ σημαντική, καθώς δίνει μια πληρέστερη εικόνα για τον κίνδυνο που εισάγει στο δίκτυο κάθε κατηγορία, ενώ καταδεικνύει ότι σε κάθε περίπτωση ο σχεδιασμός των μέτρων αντιμετώπισης επιθέσεων θα πρέπει να γίνεται πάντα με γνώμονα το trade-off που επιθυμεί ο σχεδιαστής να επιτύχει. Ως εκ τούτου, δε θα πρέπει να αποτελεί στόχο ο αντιμετώπισης επιθέσεων ακόμα και από τον ισχυρότερο επιτιθέμενο, καθώς αυτό είναι ένα σενάριο σπάνια υλοποιήσιμο, ενώ οποιοδήποτε μέτρο προστασίας, ειδικά στα δίκτυα ανωνύμων επικοινωνιών, μειώνει τη χρηστικότητα του. [26]

Θα πρέπει να θεωρείται δεδομένο ότι στις περιπτώσεις επιθέσεων εναντίον των τεχνολογιών και των δικτύων που μελετά η παρούσα εργασία, ο επιτιθέμενος υλοποιεί White Box Attacks. Αυτό συμβαίνει διότι όλες οι τεχνολογίες αυτές είναι open source λύσεις και έτσι ο επιτιθέμενος μπορεί να γνωρίζει επακριβώς τα πρωτόκολλα που χρησιμοποιούν, ώστε να βρει τρόπους να σχεδιάσει επιθέσεις εναντίον τους.

Σε γενικές γραμμές, η σφοδρότητα των επιθέσεων που μπορεί να εξαπολύσει ένας κακόβουλος χρήστης εναντίον των τεχνολογιών ανωνύμων επικοινωνιών εξαρτάται από δύο παράγοντες. Ο πρώτος είναι η υπολογιστική ισχύς που εκείνος διαθέτει και ο δεύτερος είναι η επιρροή του επιτιθέμενου στο δίκτυο, δηλαδή πόσους κόμβους και συνδέσμους εκείνος ελέγχει στο συγκεκριμένο δίκτυο. Ο δεύτερος παράγοντας είναι βαρύνουσας σημασίας και είναι εκείνος που επηρεάζει ουσιαστικά το ποσοστό επιτυχίας των επιθέσεων. [81]

Οι επιτιθέμενοι μπορούν να ενταχθούν σε μια από τις παρακάτω κατηγορίες.

- External Party

Πρόκειται για επιτιθέμενους οι οποίοι δεν διαθέτουν κάποιον compromised κόμβο στο δίκτυο. Είναι η λιγότερο επικίνδυνη κατηγορία, καθώς δεν έχουν τρόπο να υλοποιήσουν ανάλυση ή παραμόρφωση της δικτυακής κίνησης. Οι διαχειριστές του δικτύου θα πρέπει να λαμβάνουν μέτρα ώστε να αποτρέπουν τέτοιους κακόβουλους χρήστες από τα να γίνονται μέλη του δικτύου με διάφορα αντίμετρα.

- Service Provider
  Πρόκειται για τον πάροχο περιεχομένου ή υπηρεσίας σε χρήστες του δικτύου. Συνήθως ο επιτιθέμενος έχει κάνει compromisation του ίδιου του server ή κάποιου γειτονικού κόμβου, μέσω του οποίου διέρχεται κίνηση προς εκείνον, με αποτέλεσμα να έχει δυνατότητες υλοποίησης ανάλυσης της δικτυακής κίνησης.
- Local administration
  Στην περίπτωση αυτή ο επιτιθέμενος συνήθως ελέγχει κάποιον κόμβο κοντά στον Initiator της επικοινωνίας, με αποτέλεσμα να έχει τη δυνατότητα να παρατηρεί και να αλλάζει όλη τη δικτυακή κίνηση στην περιοχή αυτή. Αποτελεί σοβαρό κίνδυνο για την ανωνυμία του Initiator, ιδιαίτερα αν εκείνος εμπιστεύεται τους γείτονες τους. Μπορεί να αντιμετωπιστεί αν ο Initiator επιλέξει έναν εξωτερικό relay τον οποίον εμπιστεύεται για τις επικοινωνίες του, όπως συμβαίνει με τα guard nodes στο Tor Network.
- ISP
  Οι Internet Service Providers αποτελούν μια ακόμα επικίνδυνη κατηγορία επιτιθέμενων. Όπως έχει ήδη αναφερθεί, τα δίκτυα ανωνύμων επικοινωνιών αποτελούν δίκτυα πάνω σε δίκτυα. Έτσι, τα δίκτυα των ISPs αποτελούν δίκτυα υποδομής, πάνω στα οποία λειτουργούν οι τεχνολογίες αυτές, ενώ έχουν έλεγχο και πρόσβαση στη δικτυακή κίνηση όλων των χρηστών που εξυπηρετούν. Έτσι, όλοι οι routers και οι σύνδεσμοι που ανήκουν στην υποδομή του δικτύου αποτελούν αν δυνάμει σημεία εξαπόλυσης επιθέσεων κατά της ανωνυμίας των χρηστών.
- Governments
  Οι κυβερνήσεις αποτελούν έναν εξαιρετικά επικίνδυνο αντίπαλο εναντίον των τεχνολογιών αυτών, καθώς έχουν πρόσβαση σε μεγάλο μέρος της δικτυακής υποδομής αλλά και επαρκείς πόρους ώστε να υλοποιήσουν fake services αλλά και να σπάσουν πιο αδύναμα κρυπτογραφικά σχήματα. Ακόμα ένα σημαντικό πλεονέκτημα των επιθέσεων που πηγάζουν από κυβερνήσεις είναι ότι έχουν τη δυνατότητα να παραβιάζουν νόμους προστασίας ατομικών δικαιωμάτων, ειδικότερα σε απολυταρχικά καθεστώτα, αποκτώντας μεγαλύτερη ελευθερία κινήσεων όσον αφορά τα μέσα που θα χρησιμοποιήσουν στις επιθέσεις.
- Secret Services
  Αποτελεί τη σημαντικότερη πηγή κινδύνου για τις τεχνολογίες ανωνύμων επικοινωνιών. Μπορούν να αποκτήσουν πρόσβαση στο μεγαλύτερο μέρος της παγκόσμιας δικτυακής υποδομής, με αποτέλεσμα να έχουν τη δυνατότητα παρακολούθησης της κίνησης του στόχου που έχουν επιλέξει. Επιπροσθέτως, όλες αυτές οι επιχειρήσεις εντάσσονται στην κατηγορία των Black Ops, επομένως μπορούν να παραβιάσουν οποιονδήποτε νόμο προκειμένου να πετύχουν το στόχο τους. Έτσι, μπορούν να προβούν ακόμα και σε φυσική κατάληψη των κόμβων που τους ενδιαφέρουν προκειμένου να υλοποιήσουν ευκολότερα τις επιθέσεις τους, μέσω wiretapping.

Οι κατηγορίες αυτές των επιτιθέμενων, όπως γίνεται φανερό, έχουν διαφορετικές δυνατότητες καθώς έχουν πρόσβαση σε συγκεκριμένους πόρους και μπορούν να εκτελέσουν συγκεκριμένες επιθέσεις. Οι δύο τελευταίες κατηγορίες αποτελούν και τους κυριότερες πηγές κινδύνων απέναντι σε αυτές τις τεχνολογίες, καθώς είναι αυτοί που έχουν κατεξοχήν συμφέρον να καταπολεμήσουν την ανωνυμία

των χρηστών, για λόγους καταστολής παράνομων δραστηριοτήτων, λογοκρισίας περιεχομένου ή ακόμα και κατασκοπίας, αλλά και διαθέτουν τα μέσα για να υλοποιήσουν πολύπλοκες και κοστοβόρες επιθέσεις. [203]

3.1.2 Passive Attacks

3.1.2.1 Predecessor Attacks

Εισαγωγικά Στοιχεία

Οι Predecessor Attacks αποτελεί μια από τις πιο επικίνδυνες επιθέσεις στις ανώνυμες επικοινωνίες. Πρόκειται για παθητικού τύπου επιθέσεις, στις οποίες ο επιτιθέμενος συλλέγει στατιστικά στοιχεία σχετικά με τη δικτυακή κίνηση του στόχου του, προκειμένου να ανακαλύψει peers που έχουν τη μεγαλύτερη εγγύτητα στον τελικό προορισμό. Αυτό γίνεται με συμμετοχή στα tunnels τους (επομένως πρόκειται για παθητική και εσωτερική επίθεση, αφού ο επιτιθέμενος συμμετέχει στο δίκτυο), παρακολουθώντας το προηγούμενο ή το επόμενο βήμα (hop). Για την επίτευξη τους, απαιτείται ο στόχος να συνομιλεί με την ίδια οντότητα (για παράδειγμα με το ίδιο άτομο). Ο επιτιθέμενος συλλέγει πληροφορίες από κάθε κόμβο που δρομολογεί τα μηνύματα και με την πάροδο του χρόνου, χρησιμοποιώντας ένα τυχαίο δείγμα peers και μια τυχαία σειρά, μπορεί να καταλάβει ποιος peer εμφανίζεται στατιστικά ως εγγύτερος από τους υπόλοιπους, και να τον ταυτοποιήσει ως τον εκκινητή της συνομιλίας.

Οι Predecessor Attacks έχουν δύο βασικές προϋποθέσεις ώστε να είναι επιτυχείς:

- Υπάρχει μια σύνδεση η οποία επαναλαμβάνεται, μεταξύ κάποιου μέρους που ξεκινά την αποστολή των μηνυμάτων και του παραλήπτη αυτών των μηνυμάτων.
- Υπάρχουν διαθέσιμες πληροφορίες στα μεταφερόμενα πακέτα που είναι ικανά να χαρακτηρίσουν μοναδικά την εκάστοτε εγκαθιδρυμένη σύνδεση, μεταξύ του αποστολέα και του παραλήπτη. [20]

Η πρώτη απαίτηση, μπορεί να φαντάζει αρκετά δύσκολο να πραγματοποιηθεί, ωστόσο η επαναλαμβανόμενη επικοινωνία δύο μερών είναι πολύ συχνό φαινόμενο στη δικτυακή κίνηση. Για παράδειγμα ένας χρήστης επισκέπτεται πολύ συχνά κάποιον συγκεκριμένο ιστότοπο ή χρησιμοποιεί τις ίδιες εφαρμογές συνομιλιών (chat) ή συνδέεται μέσω ssh σε συγκεκριμένα τερματικά. Σε πολλές από αυτές τις περιπτώσεις ο χρήστης χρησιμοποιεί ορισμένες πληροφορίες ταυτοποίησης, όπως ονόματα χρήστη (usernames), συνθηματικά (passwords) και φυσικά, cookies, τα οποία μπορούν να χρησιμοποιηθούν για την ταυτοποίηση μιας σύνδεσης σε στρώμα εφαρμογής (application layer). Τα πρωτόκολλα ανωνύμων επικοινωνιών δεν είναι σίγουρο ότι μπορούν να προστατεύσουν τον χρήστη από την απόκρυψη των πληροφοριών αυτών που χαρακτηρίζουν την εκάστοτε σύνδεση. Σε πάρα πολλές περιπτώσεις μάλιστα, η χρήση τέτοιων στοιχείων, όπως cookies και credentials είναι απολύτως αναγκαία και δε μπορεί να αποφευχθεί. Έτσι, αν κάποιος χρησιμοποιεί μια τεχνολογία ανώνυμων επικοινωνιών (πχ Tor), στοιχεία που αφορούν τη σύνδεση του σε ορισμένους ιστότοπους και υπηρεσίες μπορούν να χρησιμοποιηθούν και τον χαρακτηρισμό της συγκεκριμένης σύνδεσης. Ακόμη και χωρίς αυτά τα στοιχεία όμως, ένας χρήστης μπορεί να εξακολουθεί να παρακολουθείται εάν οι συνδέσεις που υλοποιεί χρησιμοποιούν μοναδικούς ανταποκριτές (unique responders). Οι επιτιθέμενοι μπορούν ακόμα και να εντοπίσουν ένα συγκεκριμένο μοτίβο στις επικοινωνίες του χρήστη το οποίο θα μπορούσε να κάνει τις connection sessions ανιχνεύσιμες.

Μοντέλο Επιθέσεων

Το εκάστοτε πρωτόκολλο ανώνυμων επικοινωνιών που χρησιμοποιείται είναι κατ' ουσίαν ένα σύνολο κανόνων που ακολουθούν όλοι οι συμμετέχοντες στο δίκτυο κόμβοι, προκειμένου να διασφαλιστεί η ανωνυμία του χρήστη. Ως συμμετέχοντας ορίζεται ένας κόμβος που ακολουθεί τους κανόνες που επιβάλλει το εν χρήση πρωτόκολλο, προκειμένου να διοχετεύσει τα μηνύματα του ανώνυμα στο δίκτυο. Ο επιτιθέμενος είναι ένας συμμετέχοντας στο δίκτυο (όπως είπαμε,) ο οποίος συλλέγει πληροφορίες που αφορούν την αλληλεπίδραση άλλων χρηστών με τους κόμβους του δικτύου. Εδώ θα πρέπει να σημειωθεί ότι, ενώ οι Predecessor Attacks αποτελούν εσωτερική επίθεση, ο επιτιθέμενος δε χρειάζεται να συμμετέχει ως πλήρως ομότιμος peer στο δίκτυο, καθώς αυτού του τύπου επιθέσεις μπορούν να λειτουργήσουν αρκεί ο κακόβουλος χρήστης είναι σε θέση να αποστέλλει και να λαμβάνει μηνύματα μέσω του πρωτοκόλλου ανώνυμων επικοινωνιών που χρησιμοποιεί και ο στόχος του. [26]

Ο χρήστης που εκκινεί τη διαδικασία της επικοινωνίας ορίζεται ως ο εκκινητής (initiaTor) αυτής. Ο παραλήπτης του μηνύματος ορίζεται ως ανταποκριτής (responder) και δεν αποτελεί συμμετέχοντα στο δίκτυο. Ως συνεδρία (session) ορίζεται η συνεχής επικοινωνία μεταξύ του initiaTor και του responder. Ως αποστολέας (sender) ορίζεται οποιοσδήποτε κόμβος που συμμετέχει στο πρωτόκολλο και στέλνει πακέτα προς άλλον κόμβο ή προς τον responder, ενώ ο όρος αποδέκτης (receiver) είναι οποιοσδήποτε κόμβος δέχεται πακέτα από κόμβο που αποτελεί μέρος του πρωτοκόλλου. Ο receiver μπορεί να καθορίσει την ταυτότητα του sender, ενώ, όπως είναι αναμενόμενο, ο sender γνωρίζει εκ των προτέρων την ταυτότητά του receiver (όπου ως ταυτότητα ενός κόμβου στα δίκτυα υπολογιστών εννοείται η IP Address του). [27]

Η επίθεση βασίζεται στο γεγονός ότι με σε βάθος χρόνου, ο επιτιθέμενος, ή μια ομάδα επιτιθέμενων, μπορεί να αυξάνει επ αόριστον τις πιθανότητες να αποκαλύψει την ταυτότητα ενός initiaTor, για μια συγκεκριμένη συνομιλία (πχ σύνδεση ενός χρήστη στο email του μέσω του Tor). Από τη στιγμή που ο initiaTor ξεκινήσει μια σύνδεση, τότε οι συμμετέχοντες (participants) ανταλλάσουν μεταξύ τους μηνύματα. Όλοι αυτοί οι participants συμμετέχουν στο active set, με πρώτο και κύριο μέλος αυτού τον initiaTor. Το Active Set ορίζεται ως Α. Ταυτόχρονα, ως Total Order Π ορίζεται η σειρά των peers που χρησιμοποιήθηκαν, μέσω των οποίων πέρασαν τα μηνύματα έως ότου φτάσουν από τον initiaTor στον responder. Το Total Order καθορίζεται αυστηρά από τον χρόνο ο οποίος μεσολάβησε μέχρι να λάβει ο κάθε peer το μήνυμα και επηρεάζεται τόσο από το πρωτόκολλο ανώνυμων επικοινωνιών που χρησιμοποιείται, όσο και από την κατάσταση του δικτύου.

Θεωρώντας ως Π_i την i-οστη θέση στο δίκτυο στην οποία φτάνουν τα, υπό παρακολούθηση από το επιτιθέμενο μέρος, πακέτα, υπάρχει πάντα η θέση Π_I η οποία είναι η αρχική θέση στην οποία ο initiaTor στέλνει τα πακέτα. Οι participants στη συνέχεια επιλέγονται ομοιόμορφα τυχαία,με ή χωρίς αντικατάσταση τους. Ως A_{min} ορίζεται ο ελάχιστος αριθμός participants που είναι αναγκαίος για να καθοριστεί το I και το R, δηλαδή ο initiaTor και ο responder. Έτσι, στην ουσία το A_{min} είναι ο ελάχιστος αριθμός επιτιθέμενων προκειμένου να αποκαλυφθεί επιτυχώς η ταυτότητα των I και R. Χαρακτηριστικό παράδειγμα είναι η περίπτωση του Onion Routing όπου $A_{min}=2$ καθώς δύο επιτιθέμενοι μπορούν να εκτελέσουν επιτυχώς μια επίθεση, εφόσον ο ένας από αυτούς είναι ο πρώτος participant και ο άλλος ο τελευταίος participant της επιλεχθείσας διαδρομής (path). [16]

Εδώ θα πρέπει να σημειωθεί ότι καθώς οι κόμβοι δεν έχουν κατ ανάγκη σταθερές συνδέσεις στο δίκτυο ανώνυμων επικοινωνιών στο οποίο λαμβάνει χώρα η επίθεση, όταν κάποιος από αυτούς καταστεί ανενεργός, τότε το ίδιο συμβαίνει και στο Active Set στο οποίο εκείνος συμμετέχει. Η

διαδικασία αυτή ονομάζεται reset και συμβαίνει διαρκώς σε όλα τα δικτυακά πρωτόκολλα, είτε αφορούν ανώνυμες επικοινωνίες, είτε όχι. Οι περίοδοι μεταξύ των resets αποκαλούνται γύροι (rounds). [26] Θα πρέπει επίσης να σημειωθεί ότι ενώ είναι δυνατόν να συμβούν partial resets όταν έχουμε αποσύνδεση κόμβων, στην περίπτωση που ένας νέος κόμβος εισαγεται στο δίκτυο έχουμε full reset, καθώς ακολουθεί η δημιουργία νέων, μοναδικά ορισμένων paths. Φυσικά, καθίσταται αναγκαίο το reset να γίνεται ταυτόχρονα και για όλα τα Active Sets που υπάρχουν στο δίκτυο, καθώς σε διαφορετική περίπτωση θα είναι δυνατή η άμεση ταυτοποίηση του Initiator.

Άξιο παρατήρησης είναι επίσης το γεγονός ότι οι nodes δεν μπορούν να υλοποιούν αμέσως resets μόλις υπάρχει εισαγωγή ή απόσυρση ενός node στο δίκτυο, καθώς αυτό θα διευκόλυνε πολύ τον εντοπισμό των I και R, με την εισαγωγή πολλών, επαναλαμβανόμενων resets από τον επιτιθέμενο. Έτσι, θα πρέπει το round, η περίοδος δηλαδή μεταξύ των resets να είναι αρκούντως μεγάλη. Παρ όλα αυτά, γίνεται επίσης κατανοητό ότι το round δε γίνεται να λάβει απεριόριστα μεγάλες τιμές, καθώς αυτό σημαίνει ότι οι χρήστες μένουν χωρίς υπηρεσίες δικτύου έως το επόμενο reset. Έχοντας λοιπόν αυτό το trade-off υπόψη, συμπεραίνουμε πως τα rounds συμβαίνουν ανά σύντομα, τακτικά διαστήματα. Ένα πρωτόκολλο ανώνυμων επικοινωνιών που ικανοποιεί όλες τις παραπάνω παρατηρήσεις ονομάζεται Uniform Active Set Protocol. [20]

Ο επιτιθέμενος στην περίπτωση των Uniform Active Set Protocols έχει τη δυνατότητα να ταυτοποιήσει όλους τους Initiators οι οποίοι έχουν ενεργή σύνδεση με τον Responder. Σε αυτή την περίπτωση, για τη σύνδεση του εκάστοτε Initiator με την αντίστοιχη ροή δεδομένων, χρειάζεται να υπάρχουν χαρακτηριστικές πληροφορίες στα πακέτα έτσι ώστε να καθίσταται εφικτή η διαφοροποίηση μεταξύ των sessions. Μόνο έτσι μπορεί να είναι εφικτή η ταυτοποίηση του κάθε Initiator.

Στην περίπτωση που έχουμε μόνο έναν Initiator που επικοινωνεί με τον Responder, τότε θεωρούμε ότι ο I επικοινωνεί με τον R σε κάθε round ή λαμβάνουμε υπόψη μας αποκλειστικά τα rounds στα οποία υπάρχει επικοινωνία μεταξύ των I και R. Γενικά, ο I είναι υπεύθυνος για τη διατήρηση του session που έχει εγκατασταθεί με τον R, πάνω από το πρωτόκολλο ανωνύμων επικοινωνιών. Ακόμα και αν σταματήσει προσωρινά την επικοινωνία με τον R, το session πρέπει υποχρεωτικά να διατηρείται προκειμένου να καταστεί επιτυχής η επίθεση. Επιπλέον, ο επιτιθέμενος θα πρέπει να είναι σε θέση να διακρίνει τα μηνύματα που αποτελούν μέρος ενός συγκεκριμένου session, μέσω των μοναδικών χαρακτηριστικών που έχουμε ήδη αναφέρει (credentials, cookies κλπ). [24] Τέλος, ο κάθε κόμβος θα πρέπει να επιλέγεται τυχαία, όπως έχουμε ήδη δει.

Σε περίπτωση που ο Initiator παραμείνει σε σύνδεση με τον Responder για ένα παρατεταμένο χρονικό διάστημα, το session μεταξύ τους θα επηρεαστεί από πολλά, διαδοχικά resets. Σε κάθε ένα από αυτά, ένα νέο Active Set δημιουργείται μεταξύ των I και R, για κάθε ένα εκ των οποίων πρέπει να υπάρχει ένας participant που προωθεί τα μηνύματα από το ανώνυμο δίκτυο στον R. Ο συγκεκριμένος participant έχει τη δυνατότητα να συσχετίσει τα μηνύματα αυτά με το συγκεκριμένο session. Έτσι, κάθε φορά που ο επιτιθέμενος εντοπίζει τη συγκεκριμένη σύνδεση μέσω του session της, υπάρχει κάποιος πρώτος attacker που βλέπει τα μηνύματα που σχετίζονται με αυτή. [27] Ο I είναι πολύ πιθανότερο να στείλει τα μηνύματα αυτά πρώτα στο επιτιθέμενο participant παρά στους άλλους, με συνέπεια να καθίσταται επιτυχής η επίθεση.

Στην περίπτωση που οι κόμβοι επιλέγονται με αντικατάσταση τους, ο επιτιθέμενος, έχοντας τη δυνατότητα να ταυτοποιήσει τον R, καταγράφει τον participant που έστειλε πρώτος το μήνυμα που

συνδέεται με το συγκεκριμένο session σε αυτόν. Επειδή στο συγκεκριμένο μοντέλο που μελετάμε (Uniform Active Set Protocol) όλοι οι participants έχουν την ίδια πιθανότητα να επιλεχθούν, μετά από ικανό χρονικό διάστημα και πολλά resets, ο participant που θα έχει καταγραφεί ως αποστολέας τις περισσότερες φορές θα είναι ο I. [26] Είναι προφανές ότι όσο μεγαλώνει το διάστημα παρατήρησης του δικτύου και ο αριθμός των resets, τόσο μεγαλύτερη και η πιθανότητα σωστής ταυτοποίησης του I από τον επιτιθέμενο.

Στην περίπτωση που δεν έχουμε αντικατάσταση των ενεργών nodes σε κάθε δημιουργία ενός νέου Active Set, η ανάλυση της δικτυακής κίνησης γίνεται ακόμα πιο εύκολη. Σε αυτή την περίπτωση, καθίσταται προφανές ότι ο I δε μπορεί να εμφανιστεί σε άλλη θέση εντός του Active Set, επομένως θα είναι ο λιγότερο πιθανός υποψήφιος participant για να λάβει μηνύματα από άλλους participants. Ο επιτιθέμενος εδώ καταγράφει τους κόμβους στους οποίους προωθεί τα μηνύματα, υπολογίζοντας τις πιθανότητες να μην είναι ο Initiator. Μετά από επαρκή χρόνο παρατήρησης και αρκετά resets, ο I θα είναι ο participant στον οποίο ο attacker θα έχει προωθήσει μηνύματα τις λιγότερες φορές, καθιστώντας δυνατή την ταυτοποίηση του ως Initiator.

Θα πρέπει τέλος να τονιστεί ότι οι επιτιθέμενοι σπάνια γνωρίζουν αν υπάρχει αντικατάσταση των κόμβων ή όχι, σε κάθε δημιουργία ενός νέου Active Set. Έτσι, η συνήθης τακτική σε μια Predecessor Attack είναι η καταγραφή τόσο των Predecessor όσο και των Receivers participants, έως ότου αναγνωριστεί ο Initiator είτε μέσω της περίπτωσης των περισσότερων καταγραφών, είτε με τη μέθοδο των ελαχίστων εμφανίσεων. Φυσικά, οι predecessor attacks απαιτούν τη συμμετοχή του επιτιθέμενου ως participant στο δίκτυο ανωνύμων επικοινωνιών, τη δυνατότητα να υλοποιεί resets σε πολλαπλά rounds, με την πάροδο ικανού χρονικού διαστήματος, προκειμένου να ταυτοποιηθεί ο Initiator με μεγάλη πιθανότητα σωστής πρόβλεψης. [36]

Predecessor Attacks Case Studies

1. *Predecessor Attacks στο Crowds*

Το Crowds ήταν το πρώτο δίκτυο ανώνυμων επικοινωνών στο οποίο εφαρμόστηκαν οι Predecessor Attacks και ως εκ τούτου αποτελεί το χαρακτηριστικότερο case study για τέτοιου είδους κυβερνοεπιθέσεις. [20] Παρεμφερείς επιθέσεις στους υπόλοιπα δίκτυα ανώνυμων επικοινωνιών βασίστηκαν εν πολλοίς στη μεθοδολογία των επιθέσεων που περιγράφηκαν παραπάνω και εφαρμόστηκαν για πρώτη φορά με μεγάλη επιτυχία στο Crowds, το οποίο μάλιστα αναγκάστηκε να προβεί σε σημαντικές αλλαγές όσον αφορά το χρησιμοποιούμενο πρωτόκολλο προκειμένου να τις αντιμετωπίσει, χωρίς ωστόσο να τις αποτρέψει απόλυτα.

Μια Predecessor Attack στο Crowds βασίζεται στη συμμετοχή του επιτιθέμενου σε ένα crowd και στην παρατήρηση του reformation των paths. Στο Crowds αυτό συνήθως συμβαίνει κάθε μία ώρα. Κάθε επιτιθέμενος κόμβος παρατηρεί και καταγράφει τους predecessors μετά από κάθε path reformation. Καθώς ο Initiator, όπως είναι λογικό, εμφανίζεται πολύ πιο συχνά στο path, οι επιτιθέμενοι κόμβοι θα καταγράφουν πολύ πιο συχνά τον Initiator. Αποτέλεσμα αυτού είναι, μετά από αρκούντως μεγάλο αριθμό path reformations να μπορεί να καθοριστεί με πολύ μεγάλη ακρίβεια ο Initiator. Αν και η επίθεση μπορεί να είναι επιτυχής ακόμα και από μόνο έναν επιτιθέμενο, ο συνδυασμός επιθέσεων παράλληλα και συντονισμένα από έναν master attacker, μπορεί να οδηγήσει στην ταχύτερη ταυτοποίηση του Initiator. Στην περίπτωση των πολλών επιτιθέμενων, η ανάλυση μπορεί να απλοποιηθεί σημαντικά αν οι μεταγενέστεροι στο μονοπάτι επιτιθέμενοι να γνωρίζουν την

ύπαρξη ενός προγενέστερου επιτιθέμενου, καθώς έτσι θα μπορέσουν εύκολα να απορρίψουν τον predecessor τους ως μη πιθανό Initiator. [41] Μια ακόμα προσφιλής στους επιτιθέμενους τακτική είναι να προωθούν το μήνυμα απευθείας στον Responder, με αποτέλεσμα να τελειώνει αυτομάτως το εκάστοτε μονοπάτι και να δημιουργείται νέο, επιταχύνοντας τη διαδικασία δημιουργίας νέων rounds.

Η μελέτη των Predecessor Attacks στο Crowd αφορούν κατά κύριο λόγο τον αριθμό των rounds που απαιτούνται για την ταυτοποίηση του Initiator, και όχι για τον καθορισμό του ποσοστού επιτυχίας τους, καθώς είναι δεδομένο ότι για αρκούντως μεγάλο αριθμό rounds θα υπάρξει βέβαιη επιτυχία αυτού του είδους των επιθέσεων.

Με μαθηματική ανάλυση, προκύπτει ότι ένας κόμβος του δικτύου που δεν είναι Initiator, καταγράφεται από έναν επιτιθέμενο λιγότερο από $\frac{1}{2} \frac{c}{n} T$, όπου T ο αριθμός των rounds ο οποίος είναι αρκούντως μεγάλος και στον οποίο έχει τις περισσότερες εμφανίσεις ο Initiator στον επιτιθέμενο, c ο αριθμός των επιτιθέμενων και n ο αριθμός των participants. Έτσι, ένας κόμβος που δεν είναι Initiator, έχει λιγότερες από $\frac{1}{n}$ πιθανότητες να εμφανιστεί περισσότερες από $\frac{1}{2} \frac{c}{n} T f$ φορές στον επιτιθέμενο ($f \rightarrow significant\ fraction$). [20]

Θέτοντας τον αριθμό των rounds σε $\frac{8n}{c}$, ο επιτιθέμενος μπορεί να ακολουθήσει τον παρακάτω αλγόριθμο. Σε περίπτωση που ένας κόμβος καταγραφεί περισσότερες από $\frac{1}{2} \frac{c}{n} T$ φορές τότε εξάγεται το συμπέρασμα ότι πρόκειται για τον Initiator. Αν παραπάνω από ένας κόμβοι εμφανίζονται με συχνότητα άνω του προαναφερθέντος ορίου, τότε ο επιτιθέμενος δε μπορεί να εξάγει κάποιο σαφές συμπέρασμα. Η πιθανότητα αποτυχίας είναι το πολύ $\frac{2}{n}$ και συνίσταται είτε στην πιθανότητα να εμφανιστεί ο Initiator λιγότερες φορές από το προκαθορισμένο κατώφλι, είτε κάποιος άλλος κόμβος να εμφανιστεί περισσότερες φορές από αυτό. [20]

2. *Predecessor Attacks στο Onion Routing*

Η κρυπτογράφηση του μηνύματος σε στρώματα στο συγκεκριμένο τρόπο ανώνυμων επικοινωνιών είναι πολύ σημαντική για την αποτροπή τέτοιου είδους επιθέσεων, καθώς μόνο ο τελευταίος εν σειρά κόμβος είναι σε θέση να αποκαλύψει τη ροή δεδομένων, η οποία παραμένει κρυπτογραφημένη έως ότου φτάσει εκεί. Έτσι, ο επιτιθέμενος θα χρειαστεί να έχει αποκτήσει πρόσβαση τόσο στον πρώτο όσο και στον τελευταίο κόμβο του δικτύου, συνδυάζοντας την predecessor attack με μια timing analysis attack. [36]

Ένα πιθανό σενάριο επιτυχημένης επίθεσης στο Onion Routing μπορεί να συμβεί στην περίπτωση που το latency του δικτύου είναι ομοιόμορφο (αυτό μπορεί να συμβεί όταν ο κύριος παράγοντας που διαμορφώνει το latency είναι η πολυπλοκότητα της κρυπτογράφησης των μηνυμάτων και όταν οι κόμβοι έχουν ισάξια υπολογιστική δύναμη). Μέσω timing analysis στο δίκτυο, ο επιτιθέμενος μπορεί να αποκαλύψει στους δύο κόμβους που ελέγχει ο επιτιθέμενος τον αριθμό των βημάτων που πραγματοποίησαν τα onion packets. Έτσι, και γνωρίζοντας το μήκος μονοπατιού, ο επιτιθέμενος μπορεί να ελέγξει αν ο πρώτος κόμβος που ελέγχει συνδέεται άμεσα με τον Initiator. [44] Έτσι, ελέγχοντας τον πρώτο και τον τελευταίο κόμβο του δικτύου, μπορεί πολύ εύκολα και γρήγορα να ταυτοποιήσει τον Initiator.

Ένα άλλο σενάριο περιλαμβάνει το μεταβλητό latency μέσα στο δίκτυο, που είναι και η πιο πιθανή περίπτωση όταν το Onion Routing υλοποιείται πάνω στο Internet. Σε αυτή την περίπτωση, δύο επιτιθέμενοι μπορούν να καθορίσουν αν βρίσκονται στο ίδιο μονοπάτι υλοποιώντας time analysis στον Initiator. Αναλόγως του μήκους του μονοπατιού, οι επιτιθέμενοι κόμβοι μπορούν να καθορίσουν αν συνδέονται απευθείας στον Initiator (όταν το μήκος μονοπατιού είναι μικρότερο ή ίσο του 3), είτε να υλοποιήσουν καταγραφή των στιγμών που εμφανίζεται ο κάθε κόμβος, και τον εντοπισμό του Initiator καθώς αυτός θα εμφανιστεί τις περισσότερες φορές.

Ορίζοντας κάποιον κόμβο N έναν κόμβο του δικτύου που δεν είναι ο Initiator, τότε αν θέσουμε ως $T \geq 2\frac{2n^2}{c^2}$, τότε ο N εμφανίζεται περισσότερες από $\frac{1}{2}\frac{c^2}{n^2}$ T φορές με πιθανότητα $\frac{1}{n^2}$. Εξασφαλίζεται έτσι ότι κανένας κόμβος εκτός του Initiator δε θα εμφανιστεί $\frac{1}{2}\frac{c^2}{n^2}$ T φορές, με πιθανότητα $\frac{n-1}{n}$. Έτσι, ο Initiator θα εμφανιστεί περισσότερο από κάθε άλλο κόμβο στις καταγραφές του επιτιθέμενου με πιθανότητα $\frac{n-2}{n}$, εφόσον

$T \geq 8\frac{n^2}{c^2} ln(n)$ rounds. Φυσικά, το Onion Routing είναι το πιο ανθεκτικό από τα δίκτυα ανώνυμων επικοινωνιών όσον αφορά τις Predecessor Attacks.Έτσι, συχνά οι πολύ επικίνδυνες και δύσκολο να εντοπιστούν επιθέσεις αυτές αποτυγχάνουν. [20]

3. *Predecessor Attacks στο Mix-Net*

Το Mix-Net δεν αποτελεί κάποιο ξεχωριστό δίκτυο ανώνυμων επικοινωνιών, αλλά αναφέρεται σε ένα δίκτυο που συνδυάζει τα υπάρχοντα πρωτόκολλα που υφίστανται, προκειμένου να ενισχύσει την προστασία της ανωνυμίας των χρηστών του, αποτρέποντας κυρίως τις Timing Attacks εναντίον τους. Ως βάση του πρωτοκόλλου του χρησιμοποιεί το Onion Routing και τη διαστρωματωμένη κρυπτογράφηση των μηνυμάτων που διακινούνται στο δίκτυο, σε συνδυασμό με mixing τεχνικές, όπως η διακίνηση μηνυμάτων στα οποία έχει αλλαχθεί η σειρά τους, αποστολή εικονικών μηνυμάτων, εισαγωγή τυχαίων καθυστερήσεων στη δικτυακή κίνηση, προκειμένου να καταστεί δυσκολότερη η διαδικασία της παρατήρησης (reconnaissance) του δικτύου από κακόβουλους χρήστες. Ο κύριος λόγος που αυτό γίνεται είναι, όπως προαναφέρθηκε, προκειμένου να αποτραπούν Timing αναλύσεις της δικτυακής κίνησης, έναντι των οποίων το Onion Routing από μόνο του δεν προσφέρει κάποια προστασία. [19]

Όταν οι Timing Attacks, οι οποίες αναλύονται στη συνέχεια, δεν είναι εφικτό να υλοποιηθούν, τότε οι Initiators αποκτούν σημαντικά πλεονεκτήματα όσον αφορά την απόκρυψη της ταυτότητας τους και τη θωράκιση τους έναντι των Predecessor Attacks. [23] Συγκεκριμένα, σε αυτή την περίπτωση, καθώς ο επιτιθέμενος δεν έχει τη δυνατότητα να υλοποιήσει χρονικές αναλύσεις όσον αφορά τη διαδικασία κρυπτογράφησης/αποκρυπτογράφησης των διακινουμενων στο δίκτυο μηνυμάτων, πρέπει να έχει αποκτήσει πρόσβαση σε κάθε κόμβο που παρεμβάλλεται μεταξύ των I και R. Αυτό πρακτικά σημαίνει ότι θα πρέπει να έχει πρόσβαση σε ολόκληρο το Active Set, ώστε να έχει πρόσβαση καθ όλο το μήκος μονοπατιού που έχει καθοριστεί για την ανώνυμη επικοινωνία των δύο μερών.

Θεωρώντας l ως μήκος μονοπατιού, και ότι αυτό είναι αμετάβλητο, η πιθανότητα ένας επιτιθέμενος να αναγνωρίσει τον Initiator είναι $\frac{c(c-1)^{l-1}}{n^2}$. Προϋπόθεση για μια επιτυχή επίθεση είναι να έχω αρκούντως μεγάλο αριθμό rounds, τέτοιον ώστε $T = 2\frac{n^l}{c(c-1)^{l-1}} ln(n)$. Ο επιτιθέμενος, εφόσον

πληρούνται οι παραπάνω προϋποθέσεις, είναι σε θέση να γνωρίζει ακριβώς πότε έχει ταυτοποιήσει επιτυχώς τον Initiator μιας ανώνυμης επικοινωνίας. Φυσικά, όπως τονίστηκε, είναι αναγκαίο να ελέγχει πλήρως κάθε κόμβο του δικτύου καθώς και να υπάρχει καθορισμένο, αμετάβλητο μήκος μονοπατιού από τον I στον R. [26]

Στην περίπτωση που έχουμε μεταβλητό μήκος μονοπατιού, τα πλεονεκτήματα όσον αφορά την προστασία από Predecessor Attacks είναι περιορισμένα, σε σχέση με το κόστος που καλούμαστε να καταβάλουμε σε πόρους και πολυπλοκότητα. Έτσι, η εμπειρία των χρηστών (UX) στο ανώνυμο δίκτυο μπορεί να επηρεαστεί αρνητικά εφόσον επιλέγονται μονοπάτια με μεγάλο μήκος, χωρίς να προσφέρεται ουσιαστικό πλεονέκτημα στην ασφάλεια του δικτύου. [26]

Υποθέτοντας ότι η επιλογή του μήκους μονοπατιού γίνεται από τον Initiator και επιλέγεται τυχαία από ένα διαθέσιμο εύρος μηκών μονοπατιών, ορίζουμε l_s το μικρότερο δυνατό μήκος μονοπατιού, το οποίο επιλέγεται με πιθανότητα τουλάχιστον $p > \frac{1}{n}$. Σε περίπτωση που δεν μπορούν να οριστούν τέτοια μονοπάτια, τότε η Predecessor Attack θα χρειαστεί πολύ περισσότερο έως ότου καταφέρει να αναγνωρίσει τον Initiator, με το κόστος, από τη μεριά του δικτύου, να έχουν τα περισσότερα μονοπάτια που θα οριστούν μήκος τουλάχιστον $\frac{n}{2}$. Σε αντίθετη περίπτωση, αν όντως μπορεί να οριστεί μονοπάτι με μήκος l_s τότε οι επιτιθέμενοι θα καταγράψουν εμφανίσεις του Initiator σε $\frac{1}{2}\ Tp\ \frac{c(c-1)^{ls-1}}{n^{ls}}$ rounds, με μεγάλη πιθανότητα, εφόσον $T \geq \frac{16}{p}\ \frac{n^{ls}}{c(c-1)^{ls-1}}\ ln(n)$. [20]

Σε περίπτωση που ο επιτιθέμενος δεις l_s κόμβους στη σειρά, ενώ το πραγματικό μήκος μονοπατιού είναι μεγαλύτερο, τότε υπάρχει πιθανότητα να αντιληφθούν ως Initiator λάθος κόμβο, με πιθανότητα $\frac{(1-p)}{(n-c)}\ \frac{c(c-1)^{ls-1}}{n^{ls}}$. Προκύπτει μέσω πιθανοτικής ανάλυσης ότι σε $T \geq \frac{4}{p}\ \frac{n^{ls}}{c(c-1)^{ls-1}} \log_2(n)$ rounds, ο λάθος κόμβος θα καταγραφεί στο επιτιθέμενο $\frac{1}{2}\ Tp\frac{c}{n}$ ή περισσότερες φορές με πιθανότητα μόλις $\frac{1}{n^2}$. Επομένως η ολική πιθανότητα να συμβεί αυτό είναι μικρότερη από $\frac{1}{n}$. Εν τέλει, εφόσον το T οριστεί μεγαλύτερο τόσο από $\frac{16}{1-p}\ \frac{n^{ls}}{c(c-1)^{ls-1}}\ ln(n)$ όσο και από $\frac{4}{p}\ \frac{n^{ls}}{c(c-1)^{ls-1}} \log_2(n)$ rounds, τότε ο Initiator θα εμφανιστεί στις καταγραφές του επιτιθέμενου τουλάχιστον $\frac{1}{2}\ Tp\frac{c}{n}$ φορές και θα είναι ο μόνος κόμβος με τόσες πολλές εμφανίσεις με πιθανότητα μεγαλύτερη από $\frac{n-2}{n}$. [26]

Παρατηρώντας τις παραπάνω σχέσεις, προκύπτει ότι ο απαιτούμενος αριθμός rounds για την ταυτοποίηση του Initiator από τον επιτιθέμενο έχει την ίδια τάξη πολυπλοκότητας με την περίπτωση του σταθερού μήκους μονοπατιού με μήκος $l=l_s$. Το δίκτυο λοιπόν είναι τόσο ευαίσθητο όσο επιβάλλει το ελάχιστο μήκος μονοπατιού που είναι δυνατό να οριστεί. Κατά συνέπεια, ενώ το μεταβλητό μήκος αυξάνει το κόστος και την πολυπλοκότητα ενός Mix-Net, με σημαντικό αντίκτυπο στη μέση και μέγιστη καθυστέρηση (delay), δεν συνεισφέρει σημαντικά στην προστασία του δικτύου από Predecessor Attacks. Σημαντικό πλεονέκτημα προσφέρει ωστόσο η μέθοδος του μεταβλητού μήκους μονοπατιού όσον αφορά την εισαγωγή αβεβαιότητας στον επιτιθέμενο για το αν κατάφερε να ταυτοποιήσει τον πραγματικό Initiator ή κάποιον άλλο κόμβο. [16] Έτσι, ενώ σε μονοπάτια προκαθορισμένου μήκους ο επιτιθέμενος έχει τη δυνατότητα, ακόμα και από τον πρώτο round να ταυτοποιήσουν τον Initiator με καθορισμένη πιθανότητα επιτυχίας, σε περιπτώσεις μεταβλητού

μήκους μονοπατιού, για μια ομάδα επιτιθέμενων κόμβων l, δεν είναι απολύτως βέβαιο ότι έχουν προβεί σε ορθή ταυτοποίηση του στόχου της επίθεσης αν υπάρχει πιθανότητα το μήκος μονοπατιού να είναι l+1.

Το μεταβλητό μήκος μονοπατιού όπως είδαμε, εισάγει σημαντικούς περιορισμούς στο δίκτυο ανώνυμων επικοινωνιών και μπορεί να έχει σημαντικό αντίκτυπο στην εμπειρία του χρήστη. Έτσι, κρίνεται σκόπιμο να χρησιμοποιείται ως άνω όριο του εύρους τιμών που μπορεί να πάρει το μήκος μονοπατιού, το μέγιστο δυνατό μήκος το οποίο δεν εισάγει σημαντικές επιπτώσεις στις επιδόσεις του δικτύου. Συμπεραίνουμε λοιπόν την ανάγκη εύρεσης της βέλτιστης τιμής σχέσης-κόστους (trade-off) σχετικά με τη ασφάλεια και τις επιδόσεις του δικτύου ανωνύμων επικοινωνιών. Σε περιβάλλοντα μεγαλύτερης αβεβαιότητας, που χαρακτηρίζονται από υψηλό ρίσκο κυβερνοεπιθέσεων, μπορεί να δοθεί μεγαλύτερο βάρος στην ασφάλεια του δικτύου, καθώς δεν πρέπει να ξεχνάμε ότι ο κύριος λόγος χρήσης των δικτύων ανώνυμων επικοινωνιών είναι η προστασία της ταυτότητας των χρηστών του. Τέλος, αξίζει να τονιστεί ότι στην περίπτωση του Onion Routing οι Timing Attacks μπορούν να χρησιμοποιηθούν ανεξάρτητα από το μήκος μονοπατιού. [17] Γενικά, η ασφάλεια που βασίζεται στο μεγαλύτερο μήκος μονοπατιού εξαρτάται από το γενικότερο επίπεδο ασφαλείας που έχει επιλεχθεί για το δίκτυο, περιορίζοντας δραστικά τις πιθανότητες των επιτιθέμενων για αποκάλυψη της ταυτότητας των χρηστών του.

Η τελευταία προς εξέταση περίπτωση είναι αυτή όπου το μήκος μονοπατιού είναι άγνωστο στον επιτιθέμενο, μέσω της απόκρυψης του από τις ρυθμίσεις του δικτύου. Αποδεικνύεται πως η απόκρυψη του μήκους μονοπατιού προσφέρει μικρή επιπλέον προστασία έναντι των Predecessor Attacks, καθώς το εύρος του μήκους μονοπατιού μπορεί εύκολα να προσδιοριστεί από τους περιορισμούς που θέτουν οι απαιτήσεις επιδόσεων του δικτύου ανωνύμων επικοινωνιών. Στην πράξη, μόνο δίκτυα που περιλαμβάνουν ένα εύρος 10-20 κόμβων μπορούν να εξασφαλίσουν ικανοποιητικές επιδόσεις όσον αφορά το latency. Έτσι, σπάνια θα επιλεχθεί μήκος μονοπατιού άνω των 20 κόμβων και μόνο για εξαιρετικά επιρρεπή σε επιθέσεις δίκτυα και επικοινωνίες. [18] Ακόμα και σε αυτή την περίπτωση όμως, ο επιτιθέμενος μπορεί να προσδιορίσει σχετικά γρήγορα και με μεγάλη ακρίβεια το μήκος μονοπατιού του δικτύου.

Αναλυτικότερα, υποθέτοντας άγνωστο μήκος μονοπατιού l, το οποίο είναι αμετάβλητο, ο επιτιθέμενος γνωρίζει πως όταν καταφέρει να εντοπίσει όλους τους κόμβους του δικτύου, τότε οι περισσότερες καταγραφές κόμβου κατά τη διάρκεια της παρατήρησης του δικτύου θα αφορούν τον Initiator. Αυτό σημαίνει ότι κάθε $\frac{n^{l-1}}{c(c-1)^{l-2}}$ φορές θα παρατηρείται μήκος μονοπατιού *l-1*. [26] Μόλις το παραπάνω επαναληφθεί δύο φορές (δεν χρειάζονται περισσότερες), τότε ο επιτιθέμενος θα παρατηρήσει δύο κόμβους στην αρχή του μονοπατιού, εξάγωντας το συμπέρασμα ότι πράγματι, το μήκος μονοπατιού είναι *l-1*. Με αρκετές επιπλέον επαναλήψεις, θα εμφανίζεται πλέον με μεγαλύτερη συχνότητα ένας συγκεκριμένος κόμβος ως ο αρχικός του δικτύου, ο οποίος μπορεί να ταυτοποιηθεί ως ο Initiator με μεγάλη πιθανότητα. Φυσικά, για την επιτυχή ταυτοποίηση του, είναι αναγκαίο να προηγηθεί ο σωστός προσδιορισμός του μήκους μονοπατιού, με τη διαδικασία που αναλύσαμε. Προκειμένου να αποκλειστεί κάθε πιθανότητα λάθους εκτίμησης, ο επιτιθέμενος μπορεί να περιμένει περισσότερες από $\frac{n^{l-1}}{c(c-1)^{l-2}}$ φορές ώστε να βεβαιωθεί ότι δε θα προκύψει κάποιο μεγαλύτερο μήκος μονοπατιού. Η διαδικασία αυτή έχει κόστος σε χρόνο, το οποίο είναι ίδιο με το κόστος που θα είχε η επίθεση σε ένα δίκτυο ανωνύμων επικοινωνιών με *l+1* κόμβους. [20] Εν τέλει, ενώ είναι θεμιτή η απόκρυψη του μήκους μονοπατιού, ως ένα μέσο που αυξάνει, έστω και περιορισμένα, την απαίτηση

σε χρόνο για να καταστεί επιτυχής μια Predecessor Attack, δε θα πρέπει να είναι η μοναδική γραμμή άμυνας, καθώς είναι ένα εμπόδιο που μπορεί να ξεπεραστεί σχετικά εύκολα.

4. Predecessor Attacks στο DC-Net

Στο DC-Net ο γράφος του δικτύου μπορεί να κατασκευαστεί μέσω των shared secrets. Συγκεκριμένα, κάθε shared secret αντικατοπτρίζει μια αιχμή (edge) στον γράφο του δικτύου. Η επίθεση στο DC-Net έχει στόχο την ανάκτηση των μηνυμάτων ενός κόμβου N, περικυκλώνοντας τον με τους γειτονικούς κόμβους του, με τους οποίους μοιράζεται ένα edge, και μοιράζοντας τα coin flips τους μεταξύ τους. Έτσι, είναι σε θέση να γνωρίζουν όλα τα coin flips που έχει μοιραστεί ο κόμβος N, την ισοτιμία του και συνεπώς μπορούν να ανιχνεύσουν όλα τα μηνύματα του.

Στην περίπτωση της ταυτοποίησης του Initiator, η παραπάνω διαδικασία επαναλαμβάνεται μέχρις ότου βρεθεί ο κόμβος στον οποίο αυτός βρίσκεται. Έτσι, ο επιτιθέμενος, μπορεί να αναγνωρίσει τον Initiator μέσω της επικοινωνίας που έχει με όλους τους άλλους κόμβους του δικτύου. Φυσικά, στην περίπτωση πυκνών DC-Nets, όπως είναι το DC-Clique, οι Predecessor Attacks είναι αδύνατο να επιτύχουν τέτοιες επιθέσεις, καθώς κάθε στιγμή το Active Set είναι ολόκληρο το γκρουπ των κόμβων. Ωστόσο σε τοπολογίες όπως το Ring-based DC-Net, τέτοιου είδους επιθέσεις είναι εφικτές και μάλιστα με πολύ χαμηλό αριθμό επιτιθέμενων. [13]

Εν προκειμένω, η προστασία της ανωνυμίας του Initiator σε ένα Ring-based DC-Net μπορεί πολύ γρήγορα να διαταραχθεί και μαλιστα με μόλις δύο επιτιθέμενους, ύστερα από Θ(n) rounds. [20] Σε κάθε round ο επιτιθέμενος χρειάζεται να αποχωρήσει και στη συνέχεια να προσχωρήσει ξανά στο Chaum ring, αποκτώντας, στη δεύτερη περίπτωση, κάποια τυχαία θέση στον δακτύλιο. Σε περίπτωση που η τοποθέτηση γίνεται με ντετερμινιστικό τρόπο, λαμβάνοντας για παράδειγμα υπόψη τις IP Addresses των κόμβων, τότε ο επιτιθέμενος μπορεί να πλαστογραφήσει τις πληροφορίες αυτές, ή να προκαλέσει κακόβουλες αλλαγές σε άλλους κόμβους σε ήδη γνωστές, στατικές θέσεις. Με αυτό τον τρόπο, ο επιτιθέμενος έχει τη δυνατότητα να επιλέξει την καταλληλότερη θέση στον δακτύλιο προκειμένου να υλοποιήσει την επίθεση του.

Δύο μη γειτονικοί επιτιθέμενοι κόμβοι, κατά τη διάρκεια ενός round, μπορεί να μοιραστούν μεταξύ τους τα coin flips τους, δημιουργώντας ένα νέο edge στο δίκτυο, το οποίο ωστόσο είναι ορατή μόνο από τους επιτιθέμενους και όχι από τους υπόλοιπους κόμβους. Το νέο αυτό edge δημιουργεί δύο νέα sub-rings ως εξής: το ένα περιλαμβάνει όλα τα edges μεταξύ των A και B μαζί με το νεοδημιουργηθέν edge, και το άλλο όλα τα edges μεταξύ των B και A, πάλι μαζί με το νεοδημιουργηθέν edge. Σύμφωνα με το πρωτόκολλο του Chaum, οι ισοτιμίες στο sub-ring χωρίς τον Initiator λαμβάνουν την τιμή 0, με συνέπεια όλοι οι κόμβοι στον συγκεκριμένο δακτύλιο να είναι βέβαιο ότι δεν είναι Initiators. [31] Σε περίπτωση που υπάρχει κάποιος κόμβος εντός του sub-ring, τότε αυτός μπορεί να ταυτοποιηθεί με βεβαιότητα ως ο Initiator.

Με την υπόθεση ότι και οι δύο επιτιθέμενοι αποχωρούν και επανέρχονται στο δακτύλιο σε κάθε round, μπορούν σε κάθε round να καθορίζουν ένα υποσύνολο κόμβων ως πιθανούς Initiators. Μετά από *T* rounds, μέσω της σύγκρισης των πιθανών κόμβων που έχουν συλλεχθεί σε κάθε round, προκύπτει ένα σύνολο κόμβων οι οποίοι είναι πιθανοί Initiators. Σε περίπτωση που ο ένας εκ των δύο επιτιθέμενων είναι αμέσως δεξιά ή αριστερά στον δακτύλιο, σε σχέση με τον Initiator και ο άλλος επιτιθέμενος είναι το πολύ [n/2] θέσεις μακριά του από την αντίθετη πλευρά, τότε το σύνολο που προκύπτει από την ανάλυση περιλαμβάνε έναν μόνο κόμβο, ο οποίος ταυτοποιείται με βεβαιότητα ως

Initiator. [20] Η αποκάλυψη της ταυτοτητας του Initiator μπορεί μάλιστα να συμβεί ακόμα και από τον πρώτο γύρο, ενώ αξίζει να αναφέρουμε ότι η προστασία της ανωνυμίας του φθίνει σημαντικά ήδη από τους πρώτους κιόλας rounds.

Τέλος, ο επιτιθέμενος μπορεί να καθορίσει και το είδος της επικοινωνίας που έχει ένας κόμβος με τους υπόλοιπους, περικυκλώνοντας τον σε Θ(n) rounds. Χρειάζονται δύο rounds στους οποίους οι επιτιθέμενοι θα καταλάβουν θέση αμέσως στα αριστερά ή στα δεξιά του στόχου, με οποιαδήποτε σειρά γίνει αυτό. Οι επικοινωνίες του στόχου, μόλις γίνει το παραπάνω, έχουν εκτεθεί στον επιτιθέμενο ο οποίος πλέον αποκτά πρόσβαση σε αυτές. [31]

Όσον αφορά τις παραλλαγές του DC-Net (Torus, Cube, Random), οι επιτιθέμενοι μπορούν να επιχειρήσουν να διαχωρίσουν το δίκτυο σε δύο τμήματα (Partitioning), το ένα εκ των οποίο θα περιλαμβάνει τον Initiator, με σκοπό, μέσα από διαδοχικούς rounds να αποκλείσουν τους κόμβους που δεν είναι Initiators και εμφανίζονται στο γκρουπ που δεν τον περιέχει. Ο δεύτερος τρόπος επίθεσης είναι, μέσα από διαδοχικούς rounds να επιχειρήσουν να καταλάβουν κάθε πιθανή θέση γειτνίασης με τον Initiator, απομονώνοντας τον (Isolation). Οι δύο αυτές επιθέσεις μπορούν να λειτουργήσουν παράλληλα, επιταχύνοντας τον χρόνο διεκπαιρέωσης της. Οι τοπολογίες Torus και Cube δυσχαιρένουν σημαντικά το partitioning του δικτύου, καθώς απαιτούν σημαντικό αριθμό επιτιθέμενων. Όσον αφορά τη μέθοδο του isolation, στην τοπολογία DC-Torus χρειάζονται 4 επιτιθέμενοι για να απομονώσουν έναν κόμβο και έξι επιτιθέμενοι για να απομονώσουν δύο κόμβους, σε κάθε round. Αντίθετα, στην περίπτωση του DC-Cube χρειάζονται 6 επιτιθέμενοι για να απομονώσουν έναν κόμβο, αυξάνοντας τους απαιτούμενους rounds για να καταστεί επιτυχής η επίθεση Η πιο συχνά χρησιμοποιούμενη επίθεση εκ των δύο, στις εναλλακτικές αυτές τοπολογίες του DC-Net είναι αυτή που ακολουθεί τη μέθοδο του Isolation, καθώς το Partitioning καθίσταται ιδιαίτερα δύσκολο για μεγάλο αριθμό κόμβων. [26]

5. Predecessor Attacks σε Σύγχρονα Πρωτόκολλα Ανώνυμων Επικοινωνιών

Στην περίπτωση του P5 πρωτοκόλλου, η αρχή που το διέπει ότι “οι χρήστες αφότου εισέλθουν στο δίκτυο δεν μπορούν να αποχωρήσουν από αυτό” εξασφαλίζει ότι το κάθε peers group δε θα συρρικνωθεί αρκετά ώστε να καταστεί εύκολη η ταυτοποίηση των peers. Παρ ολ αυτά, στα σημερινά δίκτυα, όπου συχνά οι κόμβοι καθίστανται ανενεργοί, κάθε φορά που υπάρχουν αρκετές αποχωρήσεις χρηστών ώστε να φτάσουν κάτω από έναν ορισμένο αριθμό, εξαναγκάζονται σε ανασχηματισμό του δέντρου ευρυεκπομπής, μαζί με τη δημιουργία ενός νέου κλειδιού. [49] Η διαδικασία αυτή, αν και αρκετά κοστοβόρα, εξασφαλίζει την προστασία της ανωνυμίας των χρηστών απέναντι σε Predecessor Attacks, όταν ο αριθμός των επιτιθέμενων είναι μικρότερος από το γκρουπ ανωνύμων χρηστών στο οποίο συμμετέχει ο στόχος της επίθεσης.

Στο Tarzan μπορεί να επιτευχθεί ένα επιπλέον επίπεδο προστασίας έναντι των Predecessor Attacks, καθώς οι κόμβοι μπορούν να επιλέξουν relays με τυχαία επιλογή δικτυακού τομέα (domain). Έτσι, οι επιτιθέμενοι δε μπορούν να αποκτήσουν τον έλεγχο πολλών κόμβων εντός του ίδιου domain, καθώς θα επιλέγονται proxies και έξω από αυτό, με την ίδια μάλιστα συχνότητα με την οποία επιλέγονται κόμβοι εντός του χρησιμοποιούμενου domain. Παρ ολ αυτά, αν ο αριθμός των domains που είναι αξιόπιστα είναι μικρός, οι επιτιθέμενοι μπορούν να υλοποιήσουν τις επιθέσεις τους από ελεγχόμενους κόμβους από λιγα σε αριθμό εξωτερικών domains και να βρεθούν στο επιλεχθέν από τον Initiator μονοπάτι, με αποτέλεσμα να είναι σε θέση να τον ταυτοποιήσουν.

Το MorphMix είναι ένα peer-2-peer path-based πρωτόκολλο το οποίο επιτρέπει σε αξιόπιστους κόμβους να ταυτοποιήσουν επιτιθέμενους, έχοντας ωστόσο το μειονέκτημα ότι οι επιτιθέμενοι μπορούν να διαμορφώσουν ειδικά, ελεγχόμενα από εκείνους μονοπάτια. [9] Παρ ολ αυτά, το γεγονός ότι για την επιτυχή δημιουργία του path ο κάθε peer δε χρειάζεται να γνωρίζει όλους τους υπόλοιπους, καθιστά δύσκολη την ανάκτηση όλων των πιθανών peers από τους επιτιθέμενους, αυξάνοντας το βαθμό δυσκολίας της επίθεσης.

Τέλος, σε περίπτωση πρωτοκόλλων που αφορούν το file sharing, τα μονοπάτια συνήθως δε διατηρούνται. Αυτό μπορεί να αποβεί προς όφελος των επιτιθέμενων, καθώς η συχνή δημιουργία νέων μονοπατιών δίνει περισσότερες πιθανότητες σε αυτούς να βρεθούν στο μονοπάτι που έχει δημιουργηθεί (εξάλλου πάνω σε αυτό βασίζεται και το μοντέλο των Predecessor Attacks), ωστόσο στην περίπτωση αυτή, οι χρήστες δεν επισκέπτονται τόσο συχνά στους συγκεκριμένους Responders όσο σε μια διαδραστική διαδικτυακή εφαρμογή, με αποτέλεσμα να μη δημιουργούνται τόσο συχνά νέα μονοπάτια ώστε να διευκολύνουν το έργο των επιτιθέμενων. [24] [26]

Set-up Attacks

Σε όλες τις παραπάνω περιπτώσεις, εξετάσαμε το πιο σύνηθες σενάριο, σύμφωνα με το οποίο ο επιτιθέμενος έχει στόχο να αποκαλύψει την ταυτότητα του Initiator μιας επικοινωνίας. Στην περίπτωση αυτή, ο Initiator ακολουθεί επακριβώς τους κανόνες του εκάστοτε πρωτοκόλλου, επιλέγοντας τυχαία, με ίδιο τρόπο τους κόμβους μέσα από τους οποίους θα περάσουν τα μηνύματα του και ο επιτιθέμενος προσπαθεί να αποκαλύψει την ταυτότητα του, με τις μεθόδους που εξηγήσαμε πιο πάνω. Υπάρχει όμως και ένα άλλο είδος επίθεσης, στις οποίες ο κακόβουλος χρήστης λαμβάνει το ρόλο του Initiator και επιλέγει ο ίδιος τους κόμβους δρομολόγησης των μηνυμάτων, με σκοπό η κίνηση του να φαίνεται ότι ξεκίνησε από κάποιον άλλο κόμβο του δικτύου, που ονομάζεται θύμα (victim). Το σενάριο αυτό είναι πιθανό σε όλα τα πρωτόκολλα που επιτρέπουν την επιλογή του μονοπατιού από τον Initiator και δεν επιβάλλουν την τυχαιοποίηση του από το δίκτυο. Αποτελεί μια συνήθη τακτική για την εκτέλεση κυβερνοεπιθέσεων μέσω δικτύων ανωνύμων επικοινωνιών, προκειμένου ως Initiator της κακόβουλης κίνησης να ταυτοποιηθεί κάποιος άλλος κόμβος (victim) και όχι ο πραγματικός δημιουργός της, εξ ου και το όνομα Set-up Attacks. Ακόμα, αποτελεί συνήθη τρόπο για την στοχοποίηση του V, όταν ο I θέλει να αποκτήσει πρόσβαση σε Responders που παρέχουν παράνομο περιεχόμενο (πχ Darknet), σε περίπτωση που υπάρχει υποψία παρακολούθησης της κίνησης ενός δικτύου ανωνύμων επικοινωνιών από τις αρχές. Σε κάθε περίπτωση, αν η επίθεση καταστεί επιτυχής, ο V θα φέρει όλες τις πιθανές συνέπειες από την κίνηση του I. [26]

Η υλοποίηση της επίθεσης αυτής είναι σχετικά απλή και ακολουθεί τις παραπάνω μεθόδους που έχουμε αναλύσει. Ο Initiator, επιλέγει ως διάδοχο κόμβο (direct successor) V τον κόμβο-θύμα στο επιλεχθέν μονοπάτι. Έτσι, αν κάποιος πραγματοποιήσει ανάλυση της δικτυακής κίνησης, ο πρώτος κόμβος που θα εμφανιστεί με μεγάλη συχνότητα είναι ο V, αφού είναι ο αμέσως επόμενος κόμβος μετά τον I και δρομολογεί όλη την κίνηση του. Όπως έχουμε ήδη πει, η ταυτοποίηση του Initiator γίνεται μέσω ανάλυσης της κίνησης, προκειμένου να εμφανιστεί ο πιθανός Initiator για συγκεκριμένο αριθμό καταγραφών, επομένως ο I δε θα προλάβει να ταυτοποιηθεί ως η πραγματική πηγή της κίνησης. Μόλις ταυτοποιηθεί, εσφαλμένα, ο V ως Initiator, ο I διακόπτει την κίνηση προκειμένου να καταστεί μη ανιχνεύσιμος. Η επίθεση γίνεται ακόμα πιο αποτελεσματική όταν περισσότεροι από έναν επιτιθέμενοι στοχοποιήσουν τον ίδιο κόμβο-θύμα. [26] Στην περίπτωση του Mix-Net, υπάρχει η δυνατότητα της επιλογής από τον Initiator ακόμα και του πλήρους μονοπατιού. Αν ο κακόβουλος Initiator γνωρίζει τους κόμβους που χρησιμοποιούνται για την παρακολούθηση της δικτυακής

κίνησης, δηλαδή τους επιτιθέμενους, τότε μπορεί ως μονοπάτι να ορίσει το σύνολο των επιτιθέμενων κόμβων, οδηγώντας στη σίγουρη ταυτοποίηση του V.

Ο κακόβουλος Initiator μπορεί να διακινδυνεύσει να αποκαλύψει τη δική του ταυτότητα, αν επιλέξει κάποιον επιτιθέμενο κόμβο ως τον κόμβο-θύμα, ή αν ο V ενσωματωθεί στους επιτιθέμενους κόμβους με αποτέλεσμα να είναι σε θέση να αποκαλύψει τον πραγματικό Initiator. [26] [27] [28] Επιπλέον, υπάρχει η πιθανότητα ο κόμβος που έχει στοχοποιηθεί ώστε να γίνει θύμα να απορρίψει τυχόν ύποπτη κίνηση προς αυτόν από κάποιον πιθανώς κακόβουλο Initiator, πράγμα που μπορεί ο κακόβουλος I να αποτρέψει επιλέγοντας να τοποθετήσει ανάμεσα σε αυτόν και τον V έναν τυχαίο άλλο κόμβο διαδοχικά, για κάθε reset.

Άξιο αναφοράς είναι ότι οι Set-up Attacks αποτελούν ένα πολύ ισχυρό αντίμετρο κατά των Predecessor Attacks. Ο Initiator, επιλέγοντας να τοποθετήσει έναν έμπιστο κόμβο δικής του επιλογής στο εκάστοτε μονοπάτι βεβαιώνεται ότι τουλάχιστον ένας κόμβος του Active Set δεν είναι επιτιθέμενος, ενώ σε περίπτωση που επιλεχθεί ως τελευταίος κόμβος, τότε μπορεί να επιτευχθεί η απόκρυψη της ταυτότητας του Responder καθώς και άλλων στοιχείων που μπορούν να ταυτοποιήσουν τη σύνδεση. Η εύρεση έμπιστων κόμβων σε ένα δίκτυο ανώνυμων επικοινωνιών φυσικά είναι εξαιρετικά δύσκολη, ωστόσο κόμβοι μπορούν να δράσουν συνεργατικά και να σχηματίσουν ένα σύνολο έμπιστων μεταξύ τους κόμβων σε ένα δίκτυο. [20] [26]

Τέλος, θα πρέπει να τονιστεί ότι η αντιμετώπιση Set-up Attacks είναι εξαιρετικά πολύπλοκη και αποτελεί θεμελιώδες πρόβλημα ασφαλείας τόσο στο Onion Routing όσο και στο Crowds, αποτελώντας σημαντικό πεδίο έρευνας στον τομέα των δικτύων ανώνυμων επικοινωνιών.

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Predecessor Attacks

Καθίσταται σαφές από την παραπάνω ανάλυση, ότι η διατήρηση της ανωνυμίας των συμμετεχόντων σε ένα δίκτυο ανώνυμων επικοινωνιών είναι ένα σύνθετο ζήτημα και συχνά το κόστος ανεβαίνει πολύ για τη διατήρηση του επιπέδου προστασίας τους. Ο παρακάτω πίνακας δείχνει συνοπτικά τα αποτελέσματα διαφόρων μετρήσεων όσον αφορά την επιτυχία των Predecessor Attacks.

Protocol	Rounds to attack, with high probability	Rounds to attack, Expectation	Work required of participants	Latency from I and R
Crowds (from [13])	$O\left(\frac{n}{c}\log n + \frac{n}{c-n\sigma}\log n\right)$	$O\left(\frac{n}{c} + \frac{n}{c-n\sigma}\right)$	$O\left(\frac{1}{(1-p)^2}\left(1+\frac{1}{n}\right)\right)$	$\left(\frac{p}{1-p}+2\right)$
Onion Routing	$O\left(\left(\frac{n}{c}\right)^2 \ln n\right)$	$O\left(\left(\frac{n}{c}\right)^2\right)$	$O(l)$	$O(l)$
Mix-Net				
fixed path length l	$O\left(\frac{n^l}{c(c-1)^{l-1}}\ln n\right)$	$O\left(\frac{n^l}{c(c-1)^{l-1}}\right)$	$O(l)$	$O(l)$
variable path length	$O\left(\frac{n^{l_{min}}}{c(c-1)^{l_{min}-1}}\ln n\right)$	$O\left(\frac{n^{l_{min}}}{c(c-1)^{l_{min}-1}}\right)$	$O(l_{ave})$	$O(l_{ave})$
DC-Net				
fully connected, $c < (n-1)$	n/a	n/a	$O(n)$	$O(\lg n)$
fully connected, $c = (n-1)$	1	1	$O(n)$	$O(\lg n)$
ring connection	$O(n)$	$O(n)$	$O(n)$	$O(\lg n)$

Σχήμα 3.2: Απαιτούμενοι Rounds για διάφορες τεχνολογίες ανωνύμων επικοινωνιών.

Το Crowds παρουσιάζει τη φτωχότερη επίδοση στην αντιμετώπιση των συγκεκριμένων επιθέσεων. Η αύξηση του μήκους μονοπατιού, παρ όλο που αυξάνει την καθυστέρηση και τον φόρτο εργασίας των

κόμβων του δικτύου, έχει μικρή επίπτωση στον αριθμό των rounds που απαιτούνται για την αποκάλυψη της ταυτότητας του Initiator. Παρ ολ αυτά, μπορεί να συμβάλει στην αντιμετώπιση επιθέσεων με τη μέθοδο του traceback. [16] [26] Το Onion Routing εμφανίζει πολλές ομοιότητες με το Crowds όσον αφορά τη συσχέτιση της καθυστέρησης με το μήκος μονοπατιού, απαιτώντας περισσότερο χρόνο λόγω της διαστρωματωμένης κρυπτογράφησης/αποκρυπτογράφησης των μηνυμάτων, έχοντας ωστόσο καλύτερες επιδόσεις σε βάθος χρόνου. Η εισαγωγή μεταβλητότητας στο μήκος μονοπατιού μπορεί να εισάγει σοβαρά προβλήματα στην απόκριση του δικτύου δυσχεραίνοντας σημαντικά την εμπειρία των χρηστών του, ειδικά σε διαδραστικές διαδικτυακές εφαρμογές και όταν υπάρχει μεγάλος αριθμός χρηστών. Στην περίπτωση των Mix-Nets, υπάρχει αυξημένο κόστος και φόρτος εργασίας στους κόμβους, τα οποία προέρχονται κυρίως από τις mixing τεχνικές που χρησιμοποιούνται. Συμπερασματικά, το μήκος μονοπατιού, σε όλες τις προαναφερθέντες περιπτώσεις, επηρεάζει γραμμικά την εισαγόμενη καθυστέρηση στο εκάστοτε δίκτυο.

Στην περίπτωση του DC-Net έχουμε σημαντικό φόρτο εργασίας για όλους τους συμμετέχοντες στο δίκτυο συνεχώς, καθώς για κάθε coin flip και για όλους τους πιθανούς συνδυασμούς, προκύπτει ένας σημαντικός όγκος δεδομένων ο οποίος πρέπει να διαβιβαστεί σε όλο το δίκτυο. Χαρακτηριστικό παράδειγμα είναι το γεγονός ότι ένας νέος κόμβος που εισέρχεται στο δίκτυο θα πρέπει να ανταλλάξει μηνύματα με όλους τους υπόλοιπους. Μετά την είσοδο του θα πρέπει να ενημερώσει όλους τους υπόλοιπους κόμβους για την ισοτιμία των coin flips του, το οποίο εισάγει καθυστέρηση $O(lg\ n)$ στο δίκτυο. Όταν ο όρος αυτός είναι ίδιος με το μήκος μονοπατιού, τότε η εισαγόμενη καθυστέρηση είναι της τάξης του Crowds και του Onion Routing, καθώς όμως οι κόμβοι αυξάνονται, η καθυστέρηση που εισάγεται αυξάνεται εκθετικά. Στην περίπτωση που δεν είναι κάθε κόμβος γειτονικός με οποιονδήποτε άλλο κόμβο στο δίκτυο, δηλαδή δεν έχουμε άμεση σύνδεση όλων με όλους, οι Predecessor Attacks θα είναι επιτυχείς. Ακόμα ένα σημαντικό πρόβλημα στις επιδόσεις του DC-Net είναι το επιπλέον διαχειριστικό κόστος για την αντιμετώπιση τυχόν συγκρούσεων (collision resolution). Επιπροσθέτως, σημαντικό πρόβλημα ασφαλείας είναι και η ευκολία με την οποία κάποιος μπορεί να υλοποιήσει μια Denial-of-Service επίθεση, στέλνοντας μια συνεχή ροή δεδομένων σε κάθε coin flips round, με μηδενική πρακτικά πιθανότητα να εντοπιστεί. Παρ όλο που υπάρχει μηχανισμός αντιμετώπισης των DoS Attacks, αυτός, όπως είναι φυσικό, εισάγει περεταίρω πολυπλοκότητα και κόστος στο δίκτυο. Παρ όλο λοιπόν που το DC-Net είναι πολύ ανθεκτικό έναντι των Predecessor Attacks, η πολυπλοκότητα του το καθιστά καλή λύση μόνο για ένα μικρό αριθμό έμπιστων μεταξύ τους συμμετεχόντων. Αντίθετα, το Crowds και το Onion Routing είναι ανθεκτικά απέναντι σε DoS Attacks, καθώς ποτέ δε χρησιμοποιούν σε ένα Active Set όλους τους συμμετέχοντες στο δίκτυο. Τέλος, το DC-Net δεν επιτρέπει την επιλογή γειτόνων, με αποτέλεσμα να είναι αδιαπέραστο απέναντι σε Set-up Attacks, στις οποίες το Crowds και το Onion Routing είναι ευάλωτα. [20]

Γενικότερα, εφόσον οι επιτιθέμενοι κόμβοι μπορούν να επιλεχθούν ως μέρος του Active Set και εφόσον οι sessions μπορούν να ταυτοποιηθούν μέσω πληροφοριών σε κάθε αναδιάταξη μονοπατιού, η προστασία της ανωνυμίας του Initiator φθίνει με την πάροδο των rounds. Το Onion Routing, λόγω της διαστρωματωμένης κρυπτογράφησης των μηνυμάτων που διακινούνται, επιτυγχάνει να καθίσταται δυνατή μόνο στον τελευταίο κόμβο η ταυτοποίηση της ροής δεδομένων και η σύνδεση της με την εκάστοτε session, επιμηκύνοντας το χρόνο ο οποίος απαιτείται για να καταστεί επιτυχής μια Predecessor Attack, ενώ οι mixing τεχνικές στο Mix-Net προσφέρουν επιπλέον προστασία έναντι των ίδιων επιθέσεων. Στην περίπτωση του DC-Net, μόνο η DC-Clique παραλλαγή του, στην οποία υπάρχει πλήρης γειτνίαση όλων των κόμβων με όλους τους υπόλοιπους καθιστά τις Predecessor Attacks πρακτικά αδύνατες να επιτύχουν, λόγω των εξαιρετικά υψηλών απαιτήσεων σε πόρους και

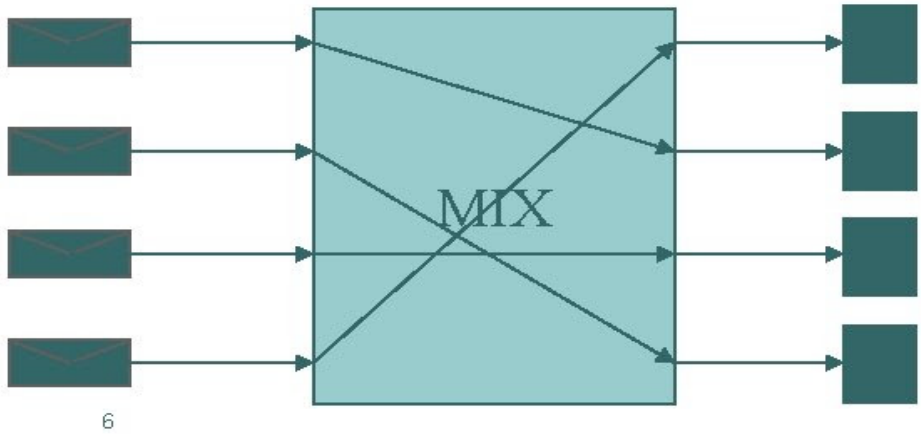
χρόνο από την πλευρά του επιτιθέμενου, κάτι που όμως δεν ισχύει και για τις υπόλοιπες παραλλαγές, όπως το DC-Ring. Τέλος, άξιο παρατήρησης είναι ότι οι Predecessor Attacks εφαρμόζονται και για την αποκάλυψη της ταυτότητας των Responders σε δίκτυα ανωνύμων επικοινωνιών, κυρίως servers που είναι η υποστηρίζουν ανώνυμους ιστότοπους.

3.1.2.2 Disclosure Attacks

Εισαγωγικά Στοιχεία

Οι Disclosure Attacks αξιοποιούν τις επαναλαμβανόμενες συνδέσεις μεταξύ δύο συμμετεχόντων ενός δικτύου ανωνύμων επικοινωνιών, προκειμένου να αποκαλύψουν την ταυτότητα τους. Οι επιπτώσεις τους στην ασφάλεια ενός δικτύου ανωνύμων επικοινωνιών μπορεί να είναι εξαιρετικά σοβαρές, αν και υπάρχουν αντίμετρα που μπορούν να εφαρμοστούν για την αντιμετώπιση τους. Η γενική μέθοδος μιας Disclosure Attack βασίζεται στην παρατήρηση ενός κόμβου που στέλνει μηνύματα και την καταγραφή όλων των πιθανών προορισμών τους, με σκοπό να αποκαλυφθεί επιτυχώς η ταυτότητα των μερών που επικοινωνούν μεταξύ τους.

Το μοντέλο που αρχικά χρησιμοποιήθηκε για την περιγραφή του τρόπου πλήττουν οι επιθέσεις αυτές τα δίκτυα ανωνύμων επικοινωνιών είναι αυτό των threshold mix, σύμφωνα με το οποίο οι χρήστες στέλνουν τυχαία μηνύματα μεταξύ τους σε κάθε round και ο εκάστοτε κόμβος αλλάζει τη σειρά των μηνυμάτων με τέτοιο τρόπο ώστε να διασφαλίζεται πως η ταυτότητα των συνομιλούντων μερών παραμένει κρυφή. Πάνω σε αυτό το μοντέλο, το οποίο εισήχθη από τον Chaum, βασίστηκαν όλες οι μετέπειτα τεχνικές ενίσχυσης της προστασίας των δικτύων ανωνύμων επικοινωνιών, όπως το Onion Routing, το οποίο προσφέρει διαστρωματωμένη κρυπτογράφηση των μηνυμάτων αυτών ως ένα επιπλέον μέτρο προστασίας. [5] Αν και αρχικά το mixing ήταν άρρηκτα συνδεδεμένο με την ύπαρξη κάποιου πραγματικού κόμβου στο δίκτυο, σύντομα επικράτησε η έννοια να αναφέρεται σε ολόκληρο το δίκτυο ανωνύμων επικοινωνιών, λαμβάνοντας την ονομασία threshold mix.

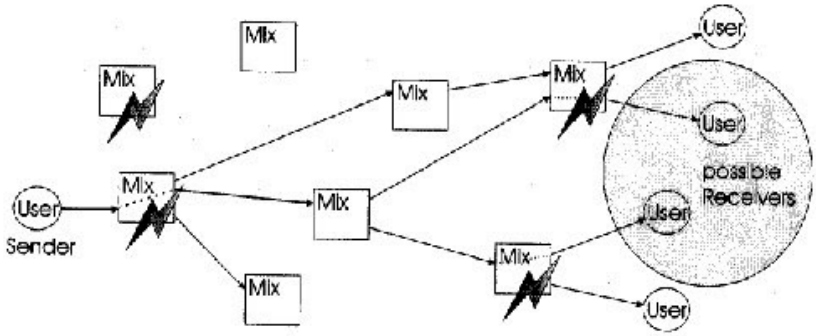


Σχήμα 3.3: Δομή ενός Mix Network.

Πάνω σε αυτή ακριβώς την έννοια του threshold mix, που όπως είπαμε χαρακτηρίζει πλέον ολόκληρο το δίκτυο και το πρωτόκολλο ανωνύμων επικοινωνιών, μελετήθηκαν οι Disclosure Attacks, οι οποίες έχουν ως στόχο τον εντοπισμό και την ταυτοποίηση των αποδεκτών των μηνυμάτων ενός αποστολέα.

[21] Οι επιθέσεις αυτές αναφέρονται και ως Disclosure Attacks όταν αφορούν σε single mixes ή αλλιώς Partitioning Attacks όταν αφορούν επιθέσεις στο σύνολο του δικτύου ανωνύμων επικοινωνιών. Η αντιμετώπιση των πρώτων είναι ευκολότερη, θέτοντας περιορισμούς στα πιθανά μονοπάτια που μπορεί να ακολουθήσει κάθε μήνυμα, ενώ στην περίπτωση που η επίθεση αφορά ολόκληρο το δίκτυο, τότε οι επιθέσεις είναι πολύ ευκολότερο να αποφέρουν αποτελέσματα. Το Onion Routing ήταν ο πρώτος τρόπος ανώνυμων επικοινωνιών στην οποία παρατηρήθηκαν αυτού του είδους οι επιθέσεις, γνωστές ως Traffic Confirmation Attacks. [22]

Οι Disclosure Attacks αποτελούν παθητικές, εσωτερικού τύπου επιθέσεις, καθώς όπως ακριβώς και στην περίπτωση των Predecessor Attacks, ο χρήστης παρακολουθεί τη δικτυακή κίνηση, προσπαθόντας να τη συσχετίσει με συγκεκριμένους αποδέκτες αυτή τη φορά. Οι συγκεκριμένες επιθέσεις είναι εξαιρετικά επικίνδυνες και δύσκολο να ανιχνευθούν, έχοντας τη δυνατότητα να επιφέρουν σημαντικά πλήγματα στην προστασία της ανωνυμίας των χρηστών ενός δικτύου. Παρ ολ' αυτά, έχουν σημαντικά υψηλό κόστος όσον αφορά τους απαιτούμενους υπολογιστικούς πόρους, καθώς η παρατήρηση του όγκου αυτού της δικτυακής κίνησης και οι απαιτούμενες συσχετίσεις σε βάθος μεγάλου αριθμού rounds για την ταυτοποίηση των παραληπτών των μηνυμάτων απαιτεί σημαντική υπολογιστική δύναμη.



Σχήμα 3.4: Επιθέσεις σε Mix Networks.

Ένα άλλο μοντέλο δικτύου ανωνύμων επικοινωνιών πάνω στο οποίο έχουν μελετηθεί οι Disclosure Attacks είναι αυτό του pool mix, στο οποίο αριθμός των απεσταλμένων μηνυμάτων διατηρείται και στέλνεται σε επόμενα rounds, εισάγοντας έτσι μια mixing τεχνική που προφυλάσσει την ανωνυμία των χρηστών. [21] [23] Με βάση αυτό το πιο ρεαλιστικό αυτό μοντέλο περιγράφεται μια στατιστική επίθεση που μοντελοποιεί καλύτερα τους πραγματικούς κινδύνους για την ανωνυμία των χρηστών σε ένα δίκτυο. Η στατιστική αυτή επίθεση προτάθηκε από τον Danezis, η οποία μπορεί εύκολα να επεκταθεί και σε άλλα μοντέλα δικτύων ανωνύμων επικοινωνιών.

Disclosure Attacks Case Studies

1. *Disclosure Attacks σε Threshold Mix Anonymity Networks*

Στα συγκεκριμένα δίκτυα, ο όρος Threshold αναφέρεται στο σύνολο των μηνυμάτων τα οποία υπόκεινται επεξεργασία σε κάθε round. Έτσι, B+1 Threshold σημαίνει ότι σε κάθε γύρο, B+1 μηνύματα θα υποστούν mixing. Υποθέτουμε ότι το θύμα της επίθεσης, ο Initiator της συνομιλίας, στέλνει σε κάθε γύρο ένα ακριβώς μήνυμα, σε κάποιον τυχαίο παραλήπτη από ένα σετ παραληπτών M. [8] Σε περίπτωση που σε κάποιο round ο I δεν στείλει κάποιο μήνυμα, το round αυτό εξαιρείται της ανάλυσης της δικτυακής κίνησης. Οι υπόλοιποι B αποστολείς μηνυμάτων στέλνουν με παρόμοιο

τρόπο μηνύματα προς τυχαίους παραλήπτες οι οποίοι ανήκουν σε ένα σύνολο N, όπου ισχύει ότι $M \subseteq N$. Ο επιτιθέμενος, γνωρίζοντας τα |M| και |N| έχει στόχο να καθορίσει το M. [88]

Επίσης, ορίζουμε ως p_r την πιθανότητα οποιοσδήποτε άλλος από τους B αποστολείς να στείλει ένα μήνυμα σε κάποιον συγκεκριμένο παραλήπτη r, όπου $p_r = \frac{1}{|N|}$, εφόσον όλοι οι πιθανοί παραλήπτες έχουν την ίδια πιθανότητα να παραλάβουν κάποιο μήνυμα, και $q_r = 1 - p_r$ δηλαδή η πιθανότητα οποιοσδήποτε άλλος από τους B αποστολείς να μη στείλει ένα μήνυμα σε κάποιον συγκεκριμένο παραλήπτη r. Θεωρούμε επίσης ότι M={r} και ότι ο επιτιθέμενος παρατηρεί για ένα round το δίκτυο επικοινωνιών. [84] [86] Η πιθανότητα κάποιος συγκεκριμένος παραλήπτης r να λάβει μήνυμα είναι q_r^B. Ο στόχος της επίθεσης έχει σίγουρα στείλει ένα μήνυμα και οι υπόλοιποι B αποστολείς στέλνουν μηνύματα σε διαφορετικούς αποστολείς. Η πιθανότητα λοιπόν να λάβει ακριβώς ένα μήνυμα οποιοσδήποτε από τους εναπομείναντες παραλήπτες r' είναι $Bp_{r'} q_{r'}^{B-1}$. [21]

Για τη διερεύνηση της επίθεσης, ορίζουμε δύο γεγονότα. Έστω το συμβάν X όπου ένας συγκεκριμένος χρήστης k λαμβάνει ένα μήνυμα και συμβάν Y όπου ισχύει M={k}, δηλαδή ο χρήστης k είναι ο παραλήπτης ο οποίος έλαβε μήνυμα από τον στόχο της επίθεσης. Το γεγονός Y|X συμβολίζει το εξαρτημένο γεγονός ο χρήστης k να είναι αυτός που έλαβε μήνυμα από τον στόχο, δεδομένου ότι ο k έλαβε ένα μήνυμα. [89] Με τον τρόπο αυτό, ορίζουμε δύο πιθανότητες που εξυπηρετούν την ανάλυση της κίνησης από μέρους του επιτιθέμενου, δηλαδή την πιθανότητα ο k να λάβει ένα μήνυμα αν είναι ο προορισμός που επέλεξε ο στόχος, και την πιθανότητα ο k να λάβει ένα μήνυμα αν δεν είναι ο προορισμός που επέλεξε ο στόχος. Επομένως $P_r[X|Y] = qB_r$. [90]

Στα εισαγωγικά στοιχεία της ενότητας αυτής, θεωρήσαμε ότι ο επιτιθέμενος γνωρίζει το M, δηλαδή το μέγεθος του συνόλου των πιθανών παραληπτών των μηνυμάτων του στόχου. Δεδομένου ότι ο επιτιθέμενος δε γνωρίζει κάτι άλλο, θεωρεί όλα τα μέρη που απαρτίζουν το M ισοπίθανα να επιλεγούν από το στόχο, επομένως ισχύει ότι $P_r[Y] = \frac{1}{|N|}$. Ισχύει ότι:

$Pr[X] = Pr[X|Y]Pr[Y] + Pr[X|\neg Y]Pr[\neg Y] = qB_k \frac{1}{|N|} + B p_k \; qB - 1_k \frac{|N|-1}{|N|}$ [89]

Σύμφωνα με το Θεώρημα του Bayes για τις δεσμευμένες πιθανότητες, ισχύει ότι:

$Pr[Y|X] = \frac{Pr[X|Y]Pr[Y]}{Pr[X]}$ το οποίο προκύπτει $\frac{1}{1+B}$. Αυτό είναι πρακτικά το αναμενόμενο αποτέλεσμα, αφού γνωρίζουμε ότι στο συγκεκριμένο round που παρατηρεί ο επιτιθέμενος ο στόχος συμμετέχει, στέλνοντας ένα μήνυμα (αλλιώς ο συγκεκριμένος round δε θα λαμβανόταν υπόψη), και κάποιος συγκεκριμένος παραλήπτης r έχει λάβει ένα μήνυμα. Έτσι, η πιθανότητα ο r να είναι ο παραλήπτης του μηνύματος του στόχου προκύπτει $\frac{1}{1+B}$. [84] [85] [86] Χωρίς μάλιστα να γνωρίζουμε που ακριβώς πήγαν τα υπόλοιπα μηνύματα και θεωρώντας ότι τα μηνύματα στο συγκεκριμένο round πήγαν σε διαφορετικούς παραλήπτες (μια απλοποιημένη και ενδεχομένως μη ρεαλιστική εκδοχή, που βοηθάει ωστόσο στην κατάστρωση του αρχικού προβλήματος και θα επεκταθεί στη συνέχεια), προκύπτει ότι η πιθανότητα οποιοσδήποτε παραλήπτης στο δίκτυο έχει πιθανότητα να επιλεχθεί από τον στόχο με πιθανότητα $\frac{1}{1+B}$.

Η πιθανότητα ο r παραλήπτης να λάβει ακριβώς c μηνύματα είναι $\binom{B}{c-1} p_r^{C-1} \; q_r^{B-c+1}$. Εδώ το c έχει ως ανώτατο όριο το B+1, το οποίο φυσικά σημαίνει ότι όλα τα μηνύματα θα πάνε στον ίδιο παραλήπτη r. *[89]*

Αντίστοιχα, η πιθανότητα οποιουδήποτε άλλου παραλήπτη r' να λάβει μηνύματα είναι

$\binom{B}{c} p_{r'}^{c} \quad q_{r'}^{B-c}$. Φυσικά, στην περίπτωση που c=B+1 η πιθανότητα αυτή μηδενίζεται, καθώς παραλήπτης εκτός του r δε μπορεί να λάβει όλα τα μηνύματα που διακινούνται, καθώς ο στόχος στέλνει το δικό του μήνυμα στον r παραλήπτη.

Έτσι, η πιθανότητα ο χρήστης k, ο οποίος λαμβάνει c μηνύματα, να είναι ο παραλήπτης του μηνύματος του στόχου της επίθεσης είναι:
$\Pr[X|Y]=\binom{B}{c-1} p_r^{c-1} \quad q_r^{B-c+1}$ και $\Pr[X]=\binom{B}{c-1} p_r \quad q_r^{B-c+1} \quad \frac{1}{|N|} + \binom{B}{c} p_r^{c} \quad q_r^{B-c} \quad \frac{|N|-1}{|N|}$. [89]

Επομένως προκύπτει ότι $\Pr[Y|X]=\frac{Pr[X|Y]Pr[Y]}{Pr[X]} = \frac{\binom{B}{c-1}}{\binom{B}{c-1}+\binom{B}{c}}$. Έτσι, αν έχουμε ένα δίκτυο με B=10 και 10 πιθανούς παραλήπτες, το δίκτυο θα επεξεργαστεί B+1=11 μηνύματα σε κάθε round. Αν ο παραλήπτης δει δύο μηνύματα να στέλνονται σε ένα χρήστη κατά τη διάρκεια ενός round, τότε μπορεί να εξάγει το συμπέρασμα ότι ο στόχος που παρατηρεί έστειλε μήνυμα στον συγκεκριμένο αυτό παραλήπτη με πιθανότητα $\frac{10}{55}$ =0.1818. [87] [88]

Η μέθοδος που έχει περιγραφεί, θα επεκταθεί σε έναν αριθμό rounds l, προκειμένου να καταστεί επιτυχής η επίθεση και να ταυτοποιηθεί ο παραλήπτης με μεγαλύτερη πιθανότητα επιτυχίας. Θεωρούμε, αντίστοιχα με τις προηγούμενες παραδοχές, X_l το συμβάν στο οποίο ο χρήστης k λαμβάνει ακριβώς ένα μήνυμα, σε κάθε έναν από τους l rounds που παρατηρούμε. Οι αντίστοιχες πιθανότητες που εξετάσαμε πριν επεκτείνονται τώρα σε ένα σύνολο l rounds, με $\Pr[X_l|Y]= q_r^{Bl}$ και $\Pr[X_l|\neg Y]= B^l \quad p_r^l \quad q_r^{(B-1)l}$. Προκύπτει λοιπόν η εξής δεσμευμένη πιθανότητα: $\Pr[Y|X_l]= \frac{(|N|-1)^{l-1}}{(|N|-1)^{l-1}+B^l}$ η οποία φυσικά περιλαμβάνει και την περίπτωση που εξετάσαμε πριν, δηλαδή αυτή στην οποία l=1 (εξετάζουμε μόνο ένα round). [92]

Έτσι, αν όλοι οι πιθανοί αποστολείς επιλέγουν τυχαία έναν από τους 10 πιθανούς παραλήπτες ενώ ο στόχος στέλνει σε συγκεκριμένο παραλήπτη, αν ο στόχος συμμετείχε σε 2 rounds με κάθε round να έχει threshold 5 (B=5), τότε ο επιτιθέμενος μπορεί να συμπεράνει ότι ο στόχος συνομιλεί με τον συγκεκριμένο παραλήπτη με πιθανότητα 0.36. Οι rounds είναι φυσικά μεταξύ τους ανεξάρτητοι, επομένως οι πιθανές ανταλλαγές μηνυμάτων σε έναν round επ ουδενί δεν επηρεάζουν τους επόμενους. [93]

Το μοντέλο επεκτείνεται και στο ελαφρώς πιο σύνθετο και ρεαλιστικό σενάριο, στο οποίο ο στόχος στέλνει μηνύματα σε παραπάνω από έναν παραλήπτες, σε έναν αριθμό l rounds. Εδώ, ορίζουμε ως X το συμβάν στο οποίο υπάρχει ένα σετ K παραληπτών, από το οποίο ένα μέλος του είναι παραλήπτης μηνύματος σε κάθε round και Y το συμβάν στο οποίο ισχύει ότι M=K, δηλαδή το σετ πιθανών παραληπτών των μηνυμάτων του υπό παρακολούθηση στόχου είναι ίδιο με το K. Εφόσον ο επιτιθέμενος γνωρίζει το μέγεθος του M, τότε οι πιθανοί συνδυασμοί που συνθέτουν το σύνολο K δίνονται από την έκφραση $\binom{|N|}{|M|}$. Προκύπτει ότι $\Pr[Y]= \frac{1}{\binom{|N|}{|M|}}$. Στην περίπτωση αυτή, το σύνολο πιθανών αποδεκτών του στόχου μπορεί να είναι οποιοσδήποτε συνδυασμός παραληπτών αυτού του συγκεκριμένου μεγέθους. Με την παραπάνω μέθοδο καθίσταται δυνατή η μελέτη της ανωνυμίας του M ως συνόλου, υπολογίζοντας την εντροπία της συνάρτησης κατανομής distribution probability πιθανότητας. Αν για παράδειγμα ο στόχος στέλνει σε κάθε round ένα μήνυμα σε έναν από δύο πιθανούς παραλήπτες, τότε ορίζουμε ως r τον παραλήπτη του πρώτου round και ως r’ τον παραλήπτη

του δεύτερου round. Η πιθανότητα λοιπόν να ταυτοποιηθεί επακριβώς το σύνολο παραληπτών του στόχου ως {r, r'} είναι μόλις 0.009. [85] [87] [89] [90]

2. *Disclosure Attacks σε Threshold Pool Mix Anonymity Networks*

Στην περίπτωση των Pool Mix δικτύων, όπως αναφέραμε και στα εισαγωγικά στοιχεία των Disclosure Attacks, έχουμε σε κάθε round την αποστολή μηνυμάτων από προηγούμενους rounds. Φυσικά, ό,τι έχουμε αναφέρει για το Threshold ισχύει στο ακέραιο, δηλαδή κάθε round μπορούν να σταλούν τόσα μηνύματα συνολικά όσα υπαγορεύει το Threshold (B στην περίπτωση μας), είτε προέρχονται από το ίδιο είτε από προηγούμενο round. Θεωρούμε ότι σε κάθε round προστίθεται b αριθμός μηνυμάτων από το ακριβώς προηγούμενο round και ορίζουμε το b ως δεξαμενή (pool). Επιπλέον, B μηνύματα από τον τρέχοντα round εισέρχονται στο mix. Συνολικά λοιπόν, σε κάθε round υπάρχουν B+b μηνύματα, εκ των οποίων θα αποσταλεί ένα υποσύνολο αυτών, μεγέθους B, όσο δηλαδή ορίζει το Threshold. [21] [29]

Σημαντική διαφορά με το Threshold Mix αποτελεί το γεγονός ότι πλέον τα rounds δεν είναι ανεξάρτητα μεταξύ τους. Ορίζουμε ως complete run του Pool Mix την κυκλική διαδικασία η οποία αρχίζει με άδειο pool, και ολοκληρώνεται όταν όλα τα μηνύματα του pool έχουν αποσταλεί στους αντίστοιχους παραλήπτες, με αποτέλεσμα αυτό να αδειάσει. Η αλληλεξάρτηση των rounds επιβάλλει την παρατήρηση κάθε complete run στο σύνολο του, ως ξεχωριστή οντότητα, όπως ακριβώς κάναμε με τα rounds στην περίπτωση του Threshold Mix.

Υποθέτουμε ξανά πως ο στόχος της επίθεσης στέλνει μηνύματα σε κάποιον παραλήπτη που ανήκει στο σύνολο M, και όλοι οι υπόλοιποι αποστολείς στέλνουν μηνύματα σε παραλήπτες που ανήκουν στο σύνολο N, ενώ ισχύει $M \subseteq N$. [30] Θεωρούμε ότι τα μηνύματα που ήδη βρίσκονται στο pool με την έναρξη της διαδικασίας κατανέμονται σύμφωνα με τη συνάρτηση κατανομής πιθανότητας u, εισερχόμενα από τον mix operaTor. Επιπλέον, θεωρούμε ότι ο επιτιθέμενος είναι σε θέση να παρατηρήσει ένα complete run του Pool Mix. Αυτό, αν και είναι δύσκολο να υλοποιηθεί επακριβώς, μπορεί να προσεγγιστεί με πολύ καλά αποτελέσματα εφόσον ο επιτιθέμενος έχει μεγάλο χρονικό περιθώριο παρατήρησης του εκάστοτε run.

Ορίζουμε ως O_i το σετ των παραληπτών και S_i το σετ των αποστολέων σε ένα round i. Ο στόχος ανήκει στο σύνολο S_i. Επιπλέον, ορίζουμε ως S_o κατάλληλο σετ τέτοιο ώστε να περιλαμβάνει όλα τα μηνύματα που βρίσκονται αρχικά στο pool και O_o κατάλληλο τέτοιο ώστε να περιλαμβάνεται το σύνολο των μηνυμάτων που έμειναν στο pool στο ακριβώς προηγούμενο round και εστάλησαν στον παρόντα round στους αντίστοιχους παραλήπτες. Επίσης, ορίζουμε ως l το σύνολο των rounds που παρατηρεί ο επιτιθέμενος, προκειμένου να αποκαλύψει την ταυτότητα του αποστολέα. Ισχύει ότι $|S_o|=|O_l|=B+b$ και $i \neq 0$ καθώς και $|S_i|=B$, $j \neq l$ και $|O_j|=B$. Κατασκευάζουμε τα σύνολα $O=\{r_i | r \in O_i\}$ και $S=\{s_i | s \in O_i\}$. [21] [22] [89] [90]

Εξετάζοντας μια παρατήρηση $O_{bs}=\{S,O\}$, υπάρχουν πολλές διαφορετικές εκδοχές σχετικά με τον τρόπο με τον οποίο οι αποστολείς έστειλαν τα μηνύματα τους στους παραλήπτες. Ορίζουμε ως σχέση λ το σενάριο σύμφωνα με το οποίο συνδέονται οι αποστολείς με τους παραλήπτες, σύμφωνα με τους κανόνες και τις παραδοχές που διέπουν το O_{bs}. Αν επί παραδείγματι έχουμε Pool Mix με Threshold 2 και ένα pool με ένα μήνυμα μέσα του, το οποίο είναι λειτουργικό (δηλαδή είναι σε διαδικασία run χωρίς να το έχει ολοκληρώσει) για δύο rounds. Το μήνυμα που βρίσκεται εντός του pool προήλθε από τον αποστολέα m ενώ τα υπόλοιπα δύο από τον αποστολέα-στόχο και κάποιον άλλον, τυχαίο

αποστολέα q. Έτσι, έχουμε S_0={m, A, q} και O_0={r,r'}. Στο επόμενο round, που τυχαίνει να είναι το τελευταίο του συγκεκριμένου run, ο mix operaTor έλαβε μηνύματα από τον αποστολέα-στόχο και από τυχαίο αποστολέα s, ενώ εστάλησαν μηνύματα προς τους παραλήπτες r, r', r''', αφήνοντας το mix κενό από μηνύματα. Έχουμε λοιπόν S_1={A, s}, O_1={r,r',r'''}, S={m_o,A_o,q_o,A_1,s_1} και O_1={r_0,r_0',r_1,r_1',r_1'''}. Με τη μέθοδο αυτή μπορούμε να εξετάσουμε όλα τα πιθανά σενάρια λ που είναι σύμφωνα με το O_{bs}. Ορίζουμε το σύνολο των πιθανών σεναρίων ως Λ και θεωρούμε σετ K τέτοιο ώστε |K|=|M|. Θεωρούμε συμβάν Y τέτοιο ώστε M=K. Αν το λ σενάριο συνέβη, τότε ο επιτιθέμενος θα παρατηρήσει το O_{bs} με αποτέλεσμα $Pr[O_{bs}|\lambda,K]=1$. Το πιθανό σενάριο λ συμβαίνει εφόσον όλοι οι αποστολείς επέλεξαν τους παραλήπτες των μηνυμάτων τους σύμφωνα με τους κανόνες του σεναρίου αυτού, καθώς και αν ο mix operaTor έστειλε σε όλους τους παραλήπτες τα μηνύματα που προοριζόταν για εκείνους, σύμφωνα με τους κανόνες που επιβάλλει το υπό εξέταση λ. Προκύπτει έτσι η εξής δεσμευμένη πιθανότητα:

$$\Pr[\lambda|Y] = \left(\prod_{s\in S} p_s\right) \frac{1}{\binom{B+b}{b}^t}$$

Στην παραπάνω πιθανότητα ισχύει ότι $p_s=\frac{1}{|N|}$ αν το s δεν είναι ο στόχος της επίθεσης και ότι $p_s=\frac{1}{|M|}$ στην αντίθετη περίπτωση. Η πιθανότητα αυτή βρίσκει εφαρμογή και στην περίπτωση που οι αποστολείς έχουν διαφορετικές συναρτήσεις κατανομής πιθανότητας, εφόσον αυτές είναι γνωστές στον επιτιθέμενο, ώστε να μπορέσει να προβεί στους κατάλληλους υπολογισμούς και τροποποιήσεις του μοντέλου. [23]

Έχοντας καθορίσει το $Pr[\lambda|M]$, μπορούμε να υπολογίσουμε το $Pr[O_{bs}|M]$ και από τον τύπο του Bayes για τις εξαρτημένες πιθανότητες, το $Pr[M|O_{bs}$.

$$\sum_{\lambda\in\Lambda} Pr[Obs|l,M] \; x \; Pr[\lambda|M] = \sum_{\lambda\in\Lambda} Pr[\lambda|M] = Pr[Obs|Y]$$

$$\Pr[\text{Obs}] = \sum_{K\, s.t.\, |K|=|M|} \sum_{\lambda\in\Lambda} \Pr[\text{Obs}|\lambda, Y]\Pr[Y]$$

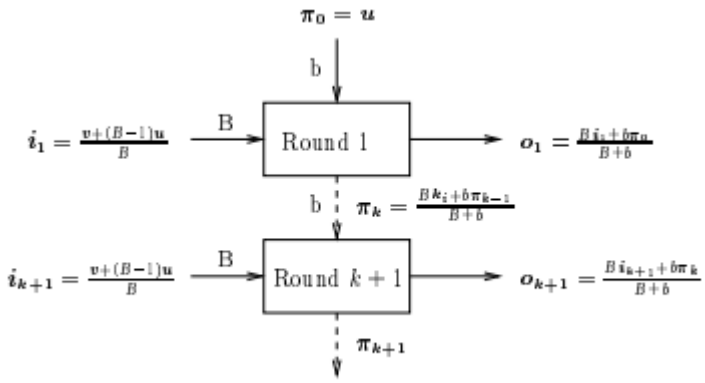
$$\Pr[Y|\text{Obs}] = \frac{\Pr[\text{Obs}|Y]\Pr[Y]}{\Pr[\text{Obs}]} = \frac{\sum_{\lambda\in\Lambda}\Pr[\lambda|M]\binom{|N|}{|M|}}{\sum_{K\, s.t.\,|K|=|M|}\sum_{\lambda\in\Lambda}\Pr[\lambda|Y]\binom{|N|}{|M|}}$$

Επομένως, έχουμε

Το οποίο μας δίνει τη δυνατότητα να υπολογίσουμε την πιθανότητα με την οποία ένα σετ K αποτελεί το σετ αποδεκτών των μηνυμάτων του στόχου. Αυτό βέβαια απαιτεί την εξέταση όλων των πιθανών σεναρίων Λ, το οποίο παρουσιάζει εκθετική πολυπλοκότητα τάξης τουλάχιστον Bk. Έτσι, δεν είναι βιώσιμη μια τέτοιου είδους επίθεση, ωστόσο με τις κατάλληλες προϋποθέσεις, μπορούν να εξαχθούν χρήσιμες πληροφορίες. [89] [92]

Στο παρακάτω σχήμα, απεικονίζεται η λειτουργία ενός Pool Mix Anonymity Network, με τις παραδοχές που καθιστούν μια Statistical Disclosure Attack εφικτή. Σε κάθε round, ο στόχος επιλέγει τυχαία έναν από τους N πιθανούς παραλήπτες του δικτύου, με συνάρτηση πυκνότητας πιθανότητας που καθορίζεται από το διάνυσμα v. Ο στόχος, αποστέλλει μηνύματα σε γύρους που καθορίζονται από τη συνάρτηση s(k). Σε περίπτωση που ο στόχος αποστέλλει κάποιο μήνυμα, τότε συμμετέχουν

στον ίδιο γύρο B-1 επιπλέον αποστολείς, ενώ σε περίπτωση που δε συμμετέχει, ο αριθμός αποστολέων που δεν αποτελούν στόχο της επίθεσης είναι συνολικά B. Οι υπόλοιποι αποστολείς επιλέγουν τους παραλήπτες των μηνυμάτων τους τυχαία, από το σύνολο N, σύμφωνα με τη συνάρτηση πυκνότητας πιθανότητας που καθορίζεται από το διάνυσμα u. Επιπροσθέτως, τα μηνύματα που αρχικά υπάρχουν στο pool, κατά την έναρξη του 1ου round, αποστέλλονται σε τυχαίους παραλήπτες από το σύνολο N, ακολουθώντας πάλι τη συνάρτηση πυκνότητας πιθανότητας που καθορίζεται από το διάνυσμα u. [21] [84]



Σχήμα 3.5: Εισερχόμενα και εξερχόμενα μηνύματα σε ένα Mix.

Στις παραδοχές που υιοθετούμε στο συγκεκριμένο μοντέλο επίθεσης, υποθέτουμε ότι κάθε παραλήπτης στο δίκτυο θα έχει, σε κάθε γύρο, εισερχόμενη ροή μηνυμάτων που θα προκύπτει ως συνδυασμός των διανυσμάτων u και v. Φυσικά, το v θα λαμβάνεται υπόψη παρόν μόνο σε rounds στους οποίους συμμετέχει ως αποστολέας ο στόχος της επίθεσης. Ορίζεται λοιπόν ένα νέο διάνυσμα, i_k που περιγράφει την κατανομή των μηνυμάτων μετά την παρέλευση ενός πολύ μεγάλου πλήθους rounds. Έτσι, έχουμε:

- $i_k = \frac{v+(B-1)u}{B}$ αν s(k)=1, δηλαδή αν ο στόχος στέλνει ένα μήνυμα στο εξεταζόμενο round
- $i_k=u$ αν $s(k) \neq 1$, δηλαδή ο στόχος δε συμμετέχει ως αποστολέας στο εξεταζόμενο round

Ταυτόχρονα, ορίζουμε ως o_k το αποτέλεσμα του round k. Η έξοδος αυτή είναι συνάρτηση της κατανομής εισόδου μηνυμάτων i_k και της π_{k-1}, δηλαδή της κατανομής παραληπτών από μηνύματα που βρίσκονται στο pool, σε ένα round k. Έτσι, η κατανομή εξόδου σε έναν γύρο k μπορεί να μοντελοποιηθεί ως εξής: $o_k= \frac{Bik+b\pi_{k-1}}{B+b}$. Επίσης, ισχύει ότι $\pi_k=o_k$. [21]

Σε αυτή την περίπτωση, ο επιτιθέμενος μπορεί να παρατηρεί το διάνυσμα s, που περιγράφει τη συμμετοχή του στόχου καθώς στέλνει μηνύματα στο δίκτυο ανωνύμων επικοινωνιών, καθώς και τη λίστα παραληπτών O_k, σε κάθε round. Η λίστα O_k αποτελείται από τυχαία δείγματα της κατανομής εξόδου o_k που περιγράφηκε παραπάνω, ενώ τα αποτελέσματα κάθε round είναι ανεξάρτητα από τους προηγούμενους.

Για δεδομένη s(k), μπορεί να επιτευχθεί επίλυση της $o_k= \frac{Bik+b\pi_{k-1}}{B+b}$ με αποτέλεσμα τον υπολογισμό όλων των πιθανών o_k. Δεδομένου ότι το o_k αποτελεί συνάρτηση των u και v, η o_k μπορεί να γραφεί ως εξής: $o_k=x_k\ v+(1-x_k)\ u$. Με απλή επίλυση του συστήματος εξισώσεων που περιγράφηκε, μπορεί να καθοριστεί το x_k ως εξής:

$$x_k = \sum_{i \le k, s(i)-1} \left(\frac{b}{B+b}\right)^{(i-1)} \frac{B}{B+b}\frac{1}{B}$$

Έτσι, ο επιτιθέμενος, έχει καταφέρει να καθορίσει τον παράγοντα x_k, ο οποίος εκφράζει τον συντελεστή βαρύτητας του στόχου στη συνομιλία, σε κάθε έξοδο O_k που παρατηρείται κατά τον k round.

Γίνεται εύκολα αντιληπτό πως με βάση τη μαθηματική ανάλυση που υλοποιήσαμε, στόχος της επίθεσης ειναι ο καθορισμός του διανύσματος v, το οποίο περιγράφει τη συνάρτηση κατανομής πιθανότητας επιλογής ενός παραλήπτη. Με το κλασικό από την κρυπτογραφία παράδειγμα των Bob και Alice, θεωρούμε ότι η Alice στέλνει μηνύματα σε διάφορους παραλήπτες, και ο επιτιθέμενος έχει στοχοποιήσει την Alice και θέλει να καθορίσει την πιθανότητα επιλογής του Bob ως παραλήπτη των μηνυμάτων της Alice. Αξιοποιόντας την παραπάνω ανάλυση σχετικά με τις ροές εξόδου o_k έχουμε τις εξής πιθανότητες. [89] [92]

$$\Pr[O_{ki} \to \text{Bob} | v_{\text{Bob}}, u_{\text{Bob}}, x_k] = (x_k v_{\text{Bob}} + (1 - x_k) u_{\text{Bob}})$$
$$\Pr[\neg O_{ki} \to \text{Bob} | v_{\text{Bob}}, u_{\text{Bob}}, x_k] = 1 - (x_k v_{\text{Bob}} + (1 - x_k) u_{\text{Bob}})$$

Το v_{Bob} καθορίζει την πιθανότητα να επιλεγεί ο Bob από την Alice ως παραλήπτης, και υποδηλώνει τη συμμετοχή του Bob στο συνολικό διάνυσμα v, το οποίο διαμορφώνεται από όλους τους πιθανούς παραλήπτες. Αντίστοιχα, το u_{Bob} εκφράζει την πθανότητα να έχει επιλεγεί ο Bob ως παραλήπτης μηνυμάτων από άλλους αποστολείς. Χρησιμοποιώντας το Θεώρημα του Bayes, έχουμε:

$$\Pr[v_{\text{Bob}} | O_{ki} \to \text{Bob}, u_{\text{Bob}}, x_k] =$$
$$\frac{\Pr[O_{ki} \to \text{Bob} | v_{\text{Bob}}, u_{\text{Bob}}, x_k] \Pr[v_{\text{Bob}} | u_{\text{Bob}}, x_k]}{\int_0^1 \Pr[O_{ki} \to \text{Bob} | v_{\text{Bob}}, u_{\text{Bob}}, x_k] \Pr[v_{\text{Bob}} | u_{\text{Bob}}, x_k] dv_{\text{Bob}}}$$
$$d \sim (x_k v_{\text{Bob}} + (1 - x_k) u_{\text{Bob}}) \Pr[\text{Prior } v_{\text{Bob}}]$$

$$\Pr[v_{\text{Bob}} | \neg O_{ki} \to \text{Bob}, u_{\text{Bob}}, x_k] =$$
$$\frac{\Pr[\neg O_{ki} \to \text{Bob} | v_{\text{Bob}}, u_{\text{Bob}}, x_k] \Pr[v_{\text{Bob}} | u_{\text{Bob}}, x_k]}{\int_0^1 \Pr[\neg O_{ki} \to \text{Bob} | v_{\text{Bob}}, u_{\text{Bob}}, x_k] \Pr[v_{\text{Bob}} | u_{\text{Bob}}, x_k] dv_{\text{Bob}}}$$
$$\sim (1 - (x_k v_{\text{Bob}} + (1 - x_k) u_{\text{Bob}})) \Pr[\text{Prior } v_{\text{Bob}}]$$

Εδώ, όρος Pr[Prior v_{Bob}] περιέχει πληροφορία σχετικά με το v_{Bob} πριν το διάστημα παρατήρησης. Μπορούμε λοιπόν να παρατηρήσουμε για κάθε μήνυμα, αν παραλήφθηκε από τον Bob και σε κάθε βήμα να υπολογίσουμε το v_{Bob} λαμβάνοντας υπόψη τα προηγούμενα δεδομένα και ερμηνεύοντας τα ως μια a priori κατανομή. Ο επιτιθέμενος λοιπόν μπορεί με αυτή τη μέθοδο να καθορίσει την κατανομή πιθανότητας λήψης ενός μηνύματος από τον Bob, έχοντας παρατηρήσει R_k μηνύματα που έχει λάβει ο Bob, σε k rounds αντίστοιχα.

$$\Pr[v_{\text{Bob}} | (x_1, R_1) \dots (x_l, R_l), u_{\text{Bob}}]$$
$$\sim \prod_k (x_k v_{\text{Bob}} + (1 - x_k) u_{\text{Bob}})^{R_k} (1 - (x_k v_{\text{Bob}} + (1 - x_k) u_{\text{Bob}}))^{(B - R_k)}$$

Η παραπάνω ανάλυση μπορεί να εφαρμοστεί για όλους τους παραλήπτες μηνυμάτων στο δίκτυο ανωνύμων επικοινωνιών, προκειμένου να καθορίσει ο επιτιθέμενος την ταυτότητα του παραλήπτη των μηνυμάτων της. Οι επιθέσεις αυτές, επειδή ακριβώς βασίζονται στη στατιστική ανάλυση της δικτυακής κίνησης και δεν απαιτούν την πλήρη ανάλυση της, ονομάζονται Statistical Disclosure Attacks. [21] [23] [84] [90]

Βελτιωμένο Μοντέλο των Statistical Disclosure Attacks

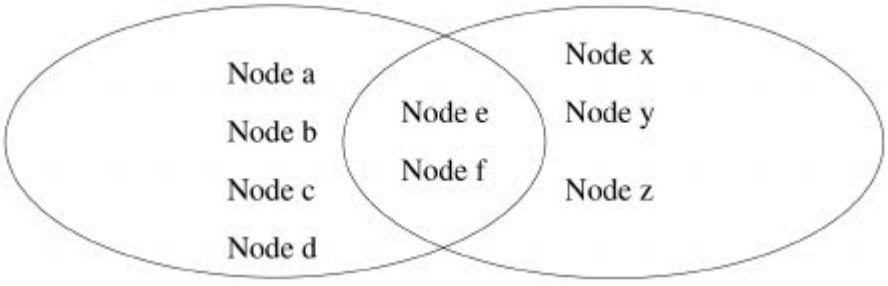
Οι Statistical Disclosure Attacks μπορούν να επεκταθούν και στα SG-Mix δίκτυα, τα οποία προσφέρουν καλό βαθμό εξασφάλισης της ανωνυμία των χρηστών σε συνδυασμό με μικρή καθυστέρηση στη δικτυακή κίνηση. Οι περισσότερες σύγχρονες διαδικτυακές εφαρμογές έχουν συγκεκριμένες και συχνά αυστηρές απαιτήσεις όσον αφορά το timeout περιθώριο, με την παρέλευση του οποίου διακόπτεται η σύνδεση, επομένως αξίζει να μελετηθούν οι Statistical Disclosure Attacks υπό το πρίσμα εφαρμογής τους σε low-latency δίκτυα ανωνύμων επικοινωνιών. [40] [89]

Στην περίπτωση αυτή, υποθέτουμε ότι ο στόχος της επίθεσης, δε στέλνει κάποιο άλλο μήνυμα προτού το προηγούμενο μήνυμα που έχει στείλει φτάσει στον τελικό του προορισμό, δηλαδή έχει εξέλθει του mix-net. Ένα SG-Mix δίκτυο μπορεί να παρασταθεί ως μια M/M/∞ σειρά. Με τη βοήθεια των Ανισοτήτων Chebychev,

$$\Pr(X + \mathrm{E}(X) \geq k\sigma) \leq \frac{1}{1+k^2}$$

προκύπτει ότι ως πιθανή καθυστέρηση ενός μηνύματος, στο SG-Mix, ορίζεται το $\tau = \frac{k+1}{\mu}$, όπου $\frac{1}{\mu}$ η τυπική απόκλιση της καθυστέρησης και k ο παράγοντας αισιοδοξίας. Στην ουρά αναμονής των μηνυμάτων είσοδο του SG-Mix, σε κάθε έλευση ενός νέου μηνύματος, υπάρχουν ήδη $\frac{\lambda}{\mu}$ μηνύματα, προκειμένου η ουρά να μη λειτουργεί ως FIFO και να εξασφαλίζεται η ανωνυμία των αποστολέων και παραληπτών. [22] Ο παράγοντας λ μπορεί να καθοριστεί με παρατήρηση των εισερχομένων στο SG-Mix δίκτυο μηνυμάτων σε ένα χρόνο T. Αν στον προαναφερθέντα χρόνο T εισέλθουν στο δίκτυο x νέα μηνύματα, τότε $\lambda = \frac{x}{T}$ και το λ ορίζεται ως ο ρυθμός εισόδου μηνυμάτων στο SG-Mix, στη μοναδα του χρόνου. [85]

Στόχος των βελτιωμένων Statistical Disclosure Attacks είναι ο σχηματισμός Sender-Sets και Receiver-Sets. Όλα τα σετς τα οποία περιέχουν μηνύματα από τον στόχο της επίθεσης σχηματίζουν το Receiver-Set, ενώ όλοι οι πιθανό αποστολείς που ανήκουν στο Receiver-Set που δημιουργήθηκε, σχηματίζουν το Sender-Set. [91]



Σχήμα 3.6: Intersection Sets.

Αν για παράδειγμα ο στόχος στείλει ένα μήνυμα, αυτό θα εισέλθει στο SG-Mix σε χρόνο t, το Receiver-Set συντίθεται από όλους τους συμμετέχοντες που λαμβάνουν τουλάχιστον ένα μήνυμα στο

χρονικό διάστημα W=[t,t+τ]. Καθώς η μέγιστη καθυστέρηση στο SG-Mix είναι τ, το μήνυμα που έστειλε ο στόχος θα φύγει από το δίκτυο σε χρόνο t+τ. Έτσι, κάθε συμμετέχοντας που θα παραλάβει τουλάχιστον ένα μήνυμα στο χρονικό διάστημα W, μπορεί να είναι ο συνομιλητής του στόχου και κατά συνέπεια θα ανήκει στο Receiver-Set. [92]

Αντίστοιχα, αν το μήνυμα του στόχου εισέλθει το SG-Mix σε χρόνο t, όλοι οι χρήστες που στέλνουν μήνυμα στο χρονικό διάστημα W2=[t-τ,t+τ] θα ανήκει στο Sender-Set. Με τον τρόπο αυτό σχηματίζεται το Sender-Set και πλέον, στόχος της επίθεσης, είναι να συσχετίσει το Sender-Set και το Receiver-Set. Καθώς η μέγιστη καθυστέρηση είναι τ, ένα μήνυμα που φεύγει από το SG-Mix σε χρόνο t, θα μπορεί να έχει αποσταλεί το νωρίτερο σε χρόνο t-τ, υπό το χειρότερο δυνατό σενάριο καθυστέρησης. [86] Αντίστοιχα, το μήνυμα που έφυγε σε χρόνο t+τ θα μπορούσε να έχει αποσταλεί τον ίδιο ακριβώς χρόνο, υπό το σενάριο μηδενικής καθυστέρησης. Έτσι, αναπόφευκτα, κάθε συμμετέχοντας που έχει στείλει κάποιο μήνυμα στο χρονικό διάστημα W2 θα ανήκει στο Sender-Set.

Τα βήματα για μια επιτυχημένη Βελτιωμένη Statistical Disclosure Attack μπορεί να καθοριστεί στα εξής βήματα:

1. Παρατήρηση του SG-Mix πρωτοκόλλου
2. Εκτίμηση της παραμέτρου λ
3. Υπολογισμός των διαστημάτων W1, W2 μέσω διαδοχικών παρατηρήσεων της λειτουργίας του δικτύου.
4. Καθορισμός των Sender-Set και Receiver-Set του στόχου της επίθεσης.
5. Καθορισμός της παραμέτρου b του Sender-Set, που καθορίζει το μέγεθος του.
6. Καθορισμός του διανύσματος o του Receiver-Set, που εκφράζει το διάνυσμα παρατηρήσεων σε κάθε round i. Σε μεγάλο βαθμό παρατηρήσεων, το διάνυσμα o συμπίπτει με το διάνυσμα u.
7. Καθορισμός των Cloak Users του Sender-Set. Ως Cloak Users ορίζονται οι συμμετέχοντες, των οποίων η συμπεριφορά έχει τη δυνατότητα να επηρεάσει την ανωνυμία του στόχου της επίθεσης.
8. Καθορισμός των Sender-Sets και Receiver-Sets των Cloak Users.
9. Καθορισμός των διανυσμάτων o για κάθε Cloak User αντίστοιχα.
10. Καθορισμός του διανύσματος CloakUsr
11. Καθορισμός του διανύσματος v.

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Disclosure Attacks

Όπως είδαμε, στην πιο ρεαλιστική περίπτωση των Pool Mix Anonymity Networks, οι Disclosure Attacks αποκτούν σημαντικό κόστος και πολυπλοκότητα. Πρόκειται ουσιαστικά για ένα NP-πρόβλημα, το οποίο ο επιτιθέμενος καλείται να αντιμετωπίσει, προκειμένου να αποκαλύψει την ταυτότητα των παραληπτών των μηνυμάτων που στέλνει ο στόχος της επίθεσης. Υιοθετώντας ωστόσο τις προσεγγίσεις που περιγράψαμε και υλοποιώντας την πιθανοτική ανάλυση, οι Statistical Disclosure Attacks καθίστανται βιώσιμες από άποψη απαιτήσεων πόρων, καθώς και εξαιρετικά επικίνδυνες για την προστασία της ταυτότητας των χρηστών. [23] Φυσικά, η πιθανοτική ανάλυση εισάγει ορισμένη αβεβαιότητα, καθώς ο επιτιθέμενος δεν είναι σε θέση να αναγνωρίσει την ταυτότητα των παραληπτών με απόλυτη βεβαιότητα, ωστόσο σε βάθος χρόνου και παρατηρήσεων, οι πιθανότητες επιτυχίας αυτού του είδους των επιθέσεων αυξάνεται σε σημαντικό βαθμό.

Ο βασικός περιορισμός των Statistical Disclosure Attacks, είναι φυσικά ο αριθμός των απαιτούμενων rounds προκειμένου να επιτευχθεί η ταυτοποίηση των παραληπτών των μηνυμάτων που στέλνει ο στόχος. Προς αυτή την κατεύθυνση, ο επιτιθέμενος μπορεί να ελέγχει κόμβους, να παρακολουθεί μηνύματα κατά μήκος της διαδρομής τους, με στόχο να εξάγει συμπεράσματα για τη σημαντικότητα τους σε σχέση με άλλα μηνύματα. [30] Οι βελτιωμένες Statistical Disclosure Attacks έχουν ακριβώς αυτό το σκοπό, να περιορίσουν δηλαδή αισθητά τον αριθμό των απαιτούμενων rounds προκειμένου να αποκαλύψουν την ταυτότητα του παραλήπτη των μηνυμάτων που στέλνει ο υπό παρακολούθηση στόχος.

Αντίστοιχα, προς την αντίθετη κατεύθυνση κινούνται οι αμυνόμενοι σε τέτοιες επιθέσεις. Κύριος και βασικός στόχος τους είναι η αποτροπή των επιτιθέμενων από το να αποκαλύψουν την ταυτότητα των χρηστών. Φυσικά, οι Disclosure Attacks είναι πρακτικά αδύνατο να αποτραπούν εντελώς, έτσι, τα πρωτόκολλα που χρησιμοποιούνται σε ανώνυμα δίκτυα επικοινωνιών δε μπορούν ποτέ να θεωρηθούν αδιαπέραστα από τέτοιου είδους επιθέσεις. [84] Στόχος λοιπόν των σχεδιαστών των πρωτοκόλλων αυτών είναι η καθυστέρηση του επιτιθέμενου, για όσο μεγαλύτερο χρονικό διάστημα γίνεται, προκειμένου να καταστήσουν το είδους των επιθέσεων αυτών ασύμφορο σε πόρους και χρόνο. Ο μόνος τρόπος για να επιτευχθεί αυτό είναι φυσικά να εφαρμοστούν διάφορες τεχνικές προκειμένου να αυξηθεί σημαντικά το απαιτούμενο πλήθος rounds που χρειάζεται ο επιτιθέμενος για να ταυτοποιήσει τον πιθανό παραλήπτη του στόχου, με μεγάλη πιθανότητα επιτυχίας.

Ο πιο διαδεδομένος τρόπος, που είδαμε και στις Predecessor Attacks, είναι η εισαγωγή dummy μηνυμάτων στη ροή , κάτι το οποίο όμως αυξάνει σημαντικά το φόρτο του δικτύου και την καθυστέρηση, γεγονός που έχει σημαντικές επιπτώσεις στην εμπειρία των χρηστών. Ακόμα μια μέθοδος επιβάλλει σε όλους τους χρήστες να στέλνουν μηνύματα σε κάθε round, είτε πραγματικά, είτε dummy, προκειμένου να καταστήσουν δυσχερέστερη την ανάλυση της δικτυακής κίνησης από πιθανές επιθέσεις. [22]

Η αύξηση της παραμέτρου b, που όπως είδαμε καθορίζει το πλήθος των μηνυμάτων που αναμιγνύονται σε κάθε round, μέσω της εισαγωγής dummy μηνυμάτων, αυξάνει τον αριθμό των rounds που απαιτούνται για την επιτυχή έκβαση της επίθεσης. Επίσης, μπορεί να αυξηθεί η διαφορετικότητα των επιλογών του στόχου, με αποτέλεσμα να καταστεί δυσχερέστερος ο εντοπισμος των πραγματικών παραληπτών του. Αυτό πρακτικά σημαίνει την αποστολή μηνυμάτων και τη δημιουργία κίνησης διαφορετικών πρωτοκόλλων και εφαρμογών, σε περισσότερους παραλήπτες, μέσω dummy μηνυμάτων.

Ακόμα ένας τρόπος είναι η συμμετοχή του στόχου με διαφορετικά n ψευδώνυμα στη διακίνηση μηνυμάτων. Τα ψευδώνυμα δε μπορούν να συσχετιστούν άμεσα με τον στόχο και κάθε ένα έχει διαφορετικό Receivers-Set. Σε κάθε round που ο στόχος θέλει να στείλει ένα μήνυμα, στέλνει μηνύματα από κάθε μια από τις n ταυτότητες. Καθώς κάθε ταυτότητα έχει διαφορετικό Receivers-Set, ο επιτιθέμενος δε μπορεί να προβεί σε συσχετίσεις προκειμένου να διαχωρίσει τα μηνύματα που ο στόχος στέλνει με την πραγματική του ταυτότητα, από τα μηνύματα που στέλνει από τα ψευδώνυμα του. [29] [30]

Οι βελτιωμένες Statistical Disclosure Attacks μπορούν να πετύχουν ένα πολύ ικανοποιητικό ποσοστό επιτυχούς αναγνώρισης των παραληπτών των μηνυμάτων που στέλνει ο στόχος, σε ποσοστό περί το 80%, σε ρεαλιστικά και εφαρμόσιμα δίκτυα ανωνύμων επικοινωνιών. Τα ποσοστά επιτυχίας αυτά

μπορούν να επιτευχθούν σε ένα πλήθος rounds περί τα 1000-2000. Αντίθετα, η χρήση ψευδωνύμων φαίνεται να περιορίζει σε πάρα πολύ μεγάλο βαθμό τις επιθέσεις αυτές.

3.1.2.3 Passive Timing Attacks

Εισαγωγικά Στοιχεία

Οι Timing Attacks αποτελούν μείζον πρόβλημα στις low-latency τεχνολογίες ανωνύμων επικοινωνιών. Αποτελούν μια υποκατηγορία των Traffic Analysis Attacks και έχουν παρατηρηθεί ήδη από την αρχή των ανωνύμων επικοινωνιών. Οι επιθέσεις αυτές βασίζονται στη δυνατότητα ενός χρήστη, έχοντας αποκτήσει τον έλεγχο ενός mix (δηλαδή ενός router) σε κάποιο δίκτυο ανωνύμων επικοινωνιών, να υλοποιεί ανάλυση των χρόνων (timing) των πακέτων που διακινούνται στο δίκτυο και να κάνει συσχετισμούς μεταξύ τους. Σε πολλές περιπτώσεις αρκεί ο επιτιθέμενος να ελέγχει δύο μόνο κόμβους στο δίκτυο, προκειμένου να έχει τη δυνατότητα να εξάγει συμπεράσματα με την παραπάνω μέθοδο για το ποια πακέτα ανήκουν σε συγκεκριμένη σύνδεση.

Πρόκειται για εξαιρετικά επικίνδυνες επιθέσεις οι οποίες απειλούν όλες τις τεχνολογίες ανωνύμων επικοινωνιών, ενώ είναι και αρκετά εύκολες και φθηνές, σε πόρους, να υλοποιηθούν. Ειδικότερα, επηρεάζουν τις low-latency ανώνυμες επικοινωνίες διότι καθίσταται ιδιαιτέρως δύσκολο να γίνει απόκρυψη των στατιστικών χαρακτηριστικών της ροής δεδομένων στο δίκτυο, με ταυτόχρονη διατήρηση του low latency που απαιτούν οι σύγχρονες δικτυακές εφαρμογές. Τα inter-packet intervals συνήθως δεν αποκρύπτονται, καθώς οι low-latency εφαρμογές απαιτούν την άμεση αποστολή των πακέτων, μετά τη δημιουργία τους. Έτσι, τα δίκτυα αυτά κινδυνεύουν από την υπονόμευση της ανωνυμίας των χρηστών τους από τέτοιου είδους επιθέσεις, μέσω της συσχέτισης των διαφόρων inter-packet intervals που παρατηρούνται στο δίκτυο.

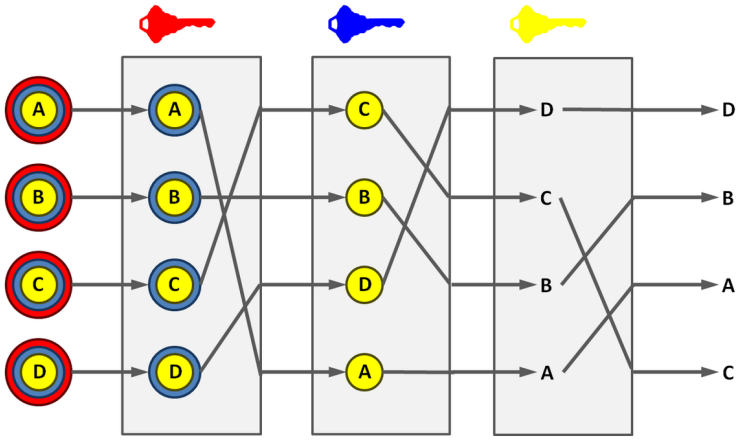
Οι Timing Analysis Attacks, όπως είναι το πλήρες όνομα τους, αποτελούν επιθέσεις που βασίζονται στην πιθανοτική ανάλυση της δικτυακής κίνησης. Ως εκ τούτου, σε κάθε επίθεση μπορεί να υπάρχουν τόσο ψευδώς θετικά όσο και ψευδώς αρνητικά αποτελέσματα. Το crossover error rate αποτελεί μετρική για την επιτυχία των Timing Attacks, δείχνοντας το σημείο στο οποίο τα ψευδώς θετικά αποτελέσματα είναι ίδια με τα ψευδώς αρνητικά. Φυσικά, όσο χαμηλότερο είναι το crossover error rate, τόσο πιο πιθανό είναι να καταστεί επιτυχής μια τέτοια επίθεση.

Η βασική μέθοδος προστασίας από Timing Attacks είναι η εισαγωγή dummy messages, τα οποία εισάγουν cover traffic σε κάθε σύνδεσμο του δικτύου. Ως αποτέλεσμα, ο επιτιθέμενος που έχει τον έλεγχο του συγκεκριμένου συνδέσμου (δηλαδή έχει τη δυνατότητα να παρακολουθεί και να αναλύει τη δικτυακή κίνηση μέσω εκείνου του σημείου), δεν έχει τη δυνατότητα να υλοποιήσει εύκολα τη στατιστική ανάλυση των διερχομένων πακέτων. Έχουν προταθεί επίσης άλλες μέθοδοι αντιμετώπισης τους, όπως η τεχνητή, σκόπιμη καθυστέρηση των πακέτων στο δίκτυο, προκειμένου να αποκρύπτονται τα identifying patterns στα πακέτα, κάτι που όμως εισάγει καθυστέρηση στο δίκτυο. Επίσης, έχουν προταθεί και λύσεις όπως το adaptive padding το οποίο δεν εισάγει επιπλέον καθυστέρηση στο δίκτυο, παρέχοντας ικανοποιητική προστασία έναντι των Timing Attacks.

Μοντέλο Επιθέσεων

Μια γενική περιγραφή των Timing Attacks μπορεί να γίνει μελετώντας ένα τυπικό Mix Network στο οποίο υπάρχει ο Initiator, ένας συμμετέχοντας-χρήστης δηλαδή που επιθυμεί να ξεκινήσει μια

ανώνυμη σύνδεση, ο Receiver που συνήθως είναι ένας destination web server που εξυπηρετεί κάποιο interactive web application και το ενδιάμεσο path, μια αλληλουχία κόμβων αποτελούμενο από M κόμβους. Το path μπορεί να είναι είτε μικρού μήκους, ήτοι να αποτελείται από 2-3 ενδιάμεσους κόμβους N, είτε να είναι μεγάλου μήκου, αποτελούμενο από 5-8 κόμβους. Θεωρούμε ότι όλα τα μηνύματα που αντιστοιχούν σε μια σύνδεση μπορεί να ακολουθούν ή και όχι το ίδιο ακριβώς μονοπάτι που έχει καθοριστεί από τον Initiator.

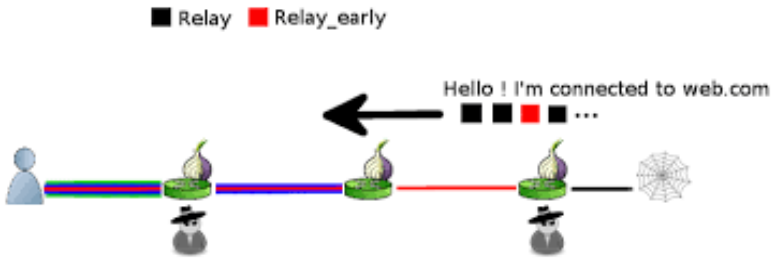


Σχήμα 3.7: Παράδειγμα σχηματισθέντος μονοπατιού.

Θεωρούμε επιτιθέμενο που έχει αποκτήσει έλεγχο σε δύο links του δικτύου, μέσω των οποίων έχει τη δυνατότητα να παρατηρεί τα inter-packet intervals, για παράδειγμα διαφορές στους χρόνους άφιξης/αναχώρησης δύο διαδοχικών πακέτων. Αυτό είναι δυνατό ακόμα και αν έχει προηγηθεί padding των πακέτων, καθώς τα inter-packet intervals τείνουν να παραμένουν αμετάβλητα και άμεσα συσχετισμένα με την IP Address του Initiator. Επιπροσθέτως, δικτυακή κίνηση που συνδέεται με συγκεκριμένες δικτυακές εφαρμογές τείνει να συμβαίνει σε ριπές (bursts). Τα bursts αυτά είναι ακόμα πιο εύκολο να γίνουν αναγνωρίσιμα από έναν επιτιθέμενο, αφού έχουν πολύ διαφορετικά inter-packet intervals από τις υπόλοιπες.

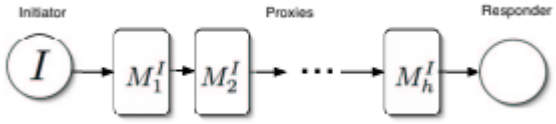
Η γενική μέθοδος που ακολουθεί ο επιτιθέμενος, προκειμένου να υλοποιήσει μια Timing Attack, είναι να καθορίσει time windows σταθερού μήκους και να καταγράφει τα πακέτα που διέρχονται σε αυτά. Αναλόγως του αριθμού των πακέτων που διέρχονται από κάθε window, μπορεί να υλοποιήσει στατιστική ανάλυση και συσχέτιση αυτών προκειμένου να ταυτοποιήσει τον Initiator αλλά και τον Receiver κάθε σύνδεσης. Σε περίπτωση που κατά τη διάρκεια της παρατήρησης ο συντελεστής συσχέτισης υπερβεί κάποιο συγκεκριμένο κατώφλι, ο επιτιθέμενος μπορεί να συσχετίσει τη συγκεκριμένη ροή με μια συγκεκριμένη σύνδεση. Όπως έχει προαναφερθεί, η μέθοδος αυτή μπορεί να παρουσιάσει ψευδώς θετικά ή ψευδώς αρνητικά αποτελέσματα. Αξίζει να τονιστεί ότι αν ο επιτιθέμενος επιλέξει υψηλό κατώφλι συσχέτισης, αυξάνεται το ποσοστό εμφάνισης ψευδώς αρνητικών αποτελεσμάτων και αντίστοιχα μειώνεται το ποσοστό ψευδώς θετικών αποτελεσμάτων, ενώ η επιλογή χαμηλού κατωφλίου συσχέτισης επιφέρει τα ακριβώς αντίθετα αποτελέσματα. Το crossover error rate διασφαλίζει ότι το ποσοστό ψευδώς θετικών αποτελεσμάτων θα είναι ίσο με αυτό των ψευδώς αρνητικών. Όσο πιο χαμηλό είναι το crossover error rate, τόσο πιο χαμηλά ποσοστά ψευδώς θετικών και ψευδώς αρνητικών αποτελεσμάτων εμφανίζονται. Υψηλό crossover error rate σημαίνει ότι υπάρχει ισχυρή άμυνα εναντίων των Timing Attacks στο δίκτυο. Η μεγαλύτερη δυνατή τιμή του που μπορεί να αντιμετωπίσει ένας επιτιθέμενος, προκειμένου να πετύχει το στόχο του είναι το 0.5. Τιμή υψηλότερη από αυτή σημαίνει ότι η επίθεση δε μπορεί να είναι επιτυχής.

Το παραπάνω μοντέλο επιθέσεων ονομάζεται Flow Correlation Attack. Μια άλλη παραλλαγή των Timing Attacks είναι οι Selective Cross Correlation Attacks, οι οποίες αποτελούν ένα πιο εξελιγμένο μοντέλο, προκειμένου να αντιμετωπίζουν τα dummy messages που εισέρχονται στο δίκτυο, για την προστασία του. Στην περίπτωση αυτή υποθέτουμε ότι η εισερχόμενη και η εξερχόμενη κίνηση είναι δύο διαφορετικές ροές. Στην εξερχόμενη κίνηση, αυτή δηλαδή που πηγάζει από τον Initiator, υπάρχει προσθήκη dummy messages, το οποίο φαίνεται στην ανάλυση. Έτσι, ο επιτιθέμενος μπορεί να απορρίψει τα windows στα οποία έχουν παρατηρηθεί προσθήκη dummy messages και να υλοποιήσει τις συγκρίσεις στα υπόλοιπα.



Σχήμα 3.8: Κακόβουλοι χρήστες στο Tor.

Θεωρώντας ότι ο Initiator επιλέγει M ενδιάμεσους κόμβους για το path, μπορούμε να μοντελοποιήσουμε το Path ως P^I, αποτελούμενο από τους διαδοχικούς κόμβους M_1^I , M_2^I , … M_h^I , όπως φαίνεται παρακάτω.



Σχήμα 3.9: Επικοινωνία του Initiator με τον Responder.

Ο M_1^I είναι ο κόμβος που λαμβάνει τα πακέτα από τον I και τα προωθεί στο δίκτυο ανωνύμων επικοινωνιών, ενώ ο M_h^I προωθεί τα πακέτα στον destination web server, δηλαδή τους Responders. Υποθέτουμε ότι κάθε link μεταφέρει μηνύματα από διάφορους Initiators ενώ το Path εγκαθίσταται πριν την αρχή της αποστολής πακέτων, με αποτέλεσμα ο κάθε Mix να γνωρίζει το επόμενο hop για κάθε σύνδεση. Αν ο επιτιθέμενος καταφέρει να αποκτήσει τον έλεγχο δύο κόμβων του δικτύου, για παράδειγμα των M_h^I και M_h^J σε δύο paths P^I και P^J αντίστοιχα, τότε μπορεί μέσω μιας Timing Attack αν I=J, δηλαδή να ταυτοποιήσει τους Responders του Initiator. Αυτό καθίσταται δυνατό λόγω του ότι αναλόγως της σύνδεσης, εμφανίζεται ένα συγκεκριμένο μοτίβο όσον αφορά την καθυστέρηση που παρουσιάζει κάθε πακέτο που ανήκει σε αυτή, η οποία μπορεί να παρατηρηθεί σε όλους τους κόμβους, καθώς αυτά διατρέχουν το δίκτυο.

Όσο ισχυρότερη είναι η συσχέτιση των χρόνων στα πακέτα που ο επιτιθέμενος παρατηρεί στα M_h^I και M_h^J, τόσο πιθανότερο είναι να ισχύει ότι I=J. Για τη μελέτη των συσχετισμών του χρόνου των πακέτων, ο επιτιθέμενος βασίζεται σε μια μεταβλητή που εκφράζει η χρονική διαφορά δ_i μεταξύ της άφιξης ενός πακέτου i και του αμέσως επόμενου που θα ακολουθήσει. Εφόσον ο επιτιθέμενος ελέγχει δύο κόμβους στο ίδιο path, τότε η διαφορά αυτή θα παρουσιάσει σημαντική συνάφεια,

παρατηρούμενη στους δύο αυτούς κόμβους. Αν για παράδειγμα παρατηρηθεί αυξημένη καθυστέρηση στον κόμβο M_1^I τότε πιθανότατα και η καθυστέρηση που θα παρατηρηθεί στον M_h^I θα είναι σημαντική. Η συσχέτιση αρκεί να είναι ισχυρότερη από άλλες, που παρατηρούνται μεταξύ διαφορετικών Initiators, προκειμένου να οδηγήσουν τον επιτιθέμενο με ασφάλεια στην εξαγωγή συμπερασμάτων.

Φυσικά, η ανάλυση αυτή είναι ευαίσθητη σε διάφορες ανωμαλίες του δικτύου, όπως είναι για παράδειγμα η απώλεια πακέτων, τα οποία μπορεί να επηρεάσουν σημαντικά τη μεταβλητή δ_i και να προκαλέσουν αποκλίσεις στη σύγκριση των χρόνων που παρατηρεί ο επιτιθέμενος. Για το λόγο αυτό εισήχθη η έννοια του time window, όπου εισάγεται ένα χρονικό παράθυρο σταθερής διάρκειας, που δεν επικαλύπτεται με το προηγούμενο η με το επόμενο, έτσι ώστε να γίνονται όσο πιο ακριβείς παρατηρήσεις είναι δυνατό. Έτσι, σε κάθε window καταγράφει έναν αριθμό πακέτων X_k^I για αυτά που έφτασαν από το P^I και αντίστοιχα για όλα τα υπόλοιπα. Έτσι, η αντιπαραβολή των αποτελεσμάτων γίνεται με τη σύγκριση των X_k^I και X_k^J που συλλέγονται από τους κόμβους που ελέγχει ο επιτιθέμενος.

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Timing Attacks

Όπως προαναφέρθηκε, ο πρώτος και πλέον γνωστός τρόπος αντιμετώπισης των Timing Attacks είναι η εισαγωγή dummy packets, μέσω των οποίων δημιουργείται cover traffic καθ όλο το μήκος του path. Αυτό μειώνει δραστικά τη δυνατότητα δημιουργίας συσχετίσεων μεταξύ των M_h^I και M_h^J καθώς και οι δύο κόμβοι θα καταγράψουν σχεδόν ίδιο αριθμό πακέτων σε κάθε χρονική στιγμή. Πλέον, οι διαφοροποιήσεις στις καθυστερήσεις των πακέτων πρέπει να συσχετιστούν, καθώς μια σημαντική καθυστέρηση μεταξύ δύο διαδοχικών πακέτων στο M_1^I θα πρέπει να ακολουθείται από μια μεγαλύτερη του μέσου όρου καθυστέρηση μεταξύ δύο πακέτων στον M_h^I κόμβο προκειμένου να αυξηθεί η συσχέτιση. Γενικότερα, η εισαγωγή dummy packets μειώνει δραστικά τη δυνατότητα του επιτιθέμενου να υλοποιήσει μια επιτυχημένη Timing Attack, εισάγωντας ωστόσο σημαντικό φόρτο στο δίκτυο, ειδικά αν αυτό εξυπηρετεί σημαντικό αριθμό χρηστών οι οποίοι συνδέονται με απαιτητικές δικτυακές εφαρμογές.

Επιπροσθέτως, οι άμυνες ενός δικτύου που χρησιμοποιεί cover traffic για την αντιμετώπιση των Timing Attacks αποδυναμώνονται σημαντικά λόγω περιστατικών όπως τα packet drops. Στην περίπτωση που συμβεί κάποια απώλεια πακέτων, πράγμα αρκετά συχνό στα δίκτυα, ο επιτιθέμενος θα παρατηρήσει ένα κενό στη δικτυακή κίνηση, γεγονός που αυξάνει τη συσχέτιση μεταξύ των M_1^I και M_h^I ενώ ταυτόχρονα τη μειώνει μεταξύ των M_h^I και M_h^J.

Μια ακόμη λύση η οποία έχει προταθεί είναι το defensive dropping. Ο Initiator κατασκευάζει dummy packets με τρόπο τέτοιο ώστε ένας ενδιάμεσος κόμβος M_m^I να τα κάνει drop. Η εντολή αυτή μπορεί να δοθεί με την εισαγωγή ενός μόνο bit στο κρυπτογραφημένο στρώμα. Έτσι, προκύπτουν σε τακτά, τυχαία και ανομοιογενή χρονικά διαστήματα packet drops έτσι ώστε να μειώνεται η συσχέτιση των παρατηρούμενων χρόνων στα πακέτα που καταγράφονται από τους κόμβους που ελέγχει ο επιτιθέμενος. Η άμυνα αυτή ενισχύεται σημαντικά αν επιλεχθούν περισσότεροι από ένας κόμβοι στο path που θα κάνουν drop τα dummy packets που δημιουργούνται. Η λύση αυτή έχει ισχυρή αποτρεπτική ικανότητα ενώ δεν εισάγει περαιτέρω επιβάρυνση στη δικτυακή κίνηση.

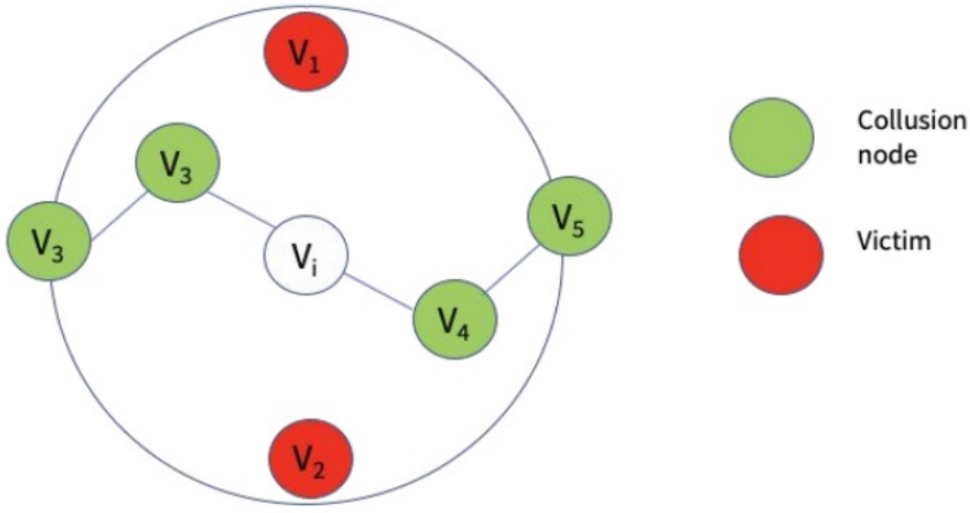
Μια ακόμα πιο εξελιγμένη παραλλαγή του defensive dropping είναι το adaptive padding, στο οποίο dummy messages εισάγονται στις ροές πακέτων από ενδιάμεσους κόμβους, με αποτέλεσμα να καταστρέφουν το οποιοδήποτε αποτύπωμα (fingerprint) που μπορεί να αφήνουν και μέσω του οποίου μπορούν να ταυτοποιηθούν. Σκοπός είναι να αποτρέψουν τον επιτιθέμενο να βγάλει συμπεράσματα σχετικά με το ποια συγκεκριμένη σύνδεση διακινεί πακέτα μέσω ενός συγκεκριμένου συνδέσμου του δικτύου και όχι να αποτρέψουν τον επιτιθέμενο να καταλάβει αν μια σύνδεση είναι ενεργή τη στιγμή της παρατήρησης ή όχι.

3.1.2.4 Collusion/Eclipse Attacks (Path Construction Attacks)

Εισαγωγικά Στοιχεία

Οι Collusion Attacks είναι επιθέσεις στις οποίες ένας κακόβουλος κόμβος κάνει μία συμφωνία με έναν άλλο κακόβουλο κόμβο, προκειμένου να υποκλέψει πληροφορίες ή να εισάγει κακόβουλο λογισμικό στη σύνδεση. Το ίδιο το όνομα παραπέμπει στον τρόπο λειτουργίας των επιθέσεων αυτών, καθώς Collusion σημαίνει Σκευωρία ή Συνωμοσία. [103] Αποτελεί έναν από τους πιο ρεαλιστικούς κινδύνους για τεχνολογίες ανωνύμων επικοινωνιών στις οποίες το μονοπάτι που δημιουργείται κατόπιν εντολής του Initiator για την εγκατάσταση μιας σύνδεσης δημιουργείται δυναμικά. Χαρακτηριστικότερο παράδειγμα είναι το δίκτυο MorphMix, στο οποίο το μονοπάτι δημιουργείται μέσω διαδοχικών επαναλήψεων, κατά τις οποίες ο κάθε κόμβος προτείνει το next hop επιλέγοντας έναν από τους γείτονες του. [83]

Στην περίπτωση αυτή, αν ένας κόμβος είναι κακόβουλος και επιλεγεί ως next hop, τότε θα έχει τη δυνατότητα να προτείνει μια σειρά από άλλους κακόβουλους κόμβους ως τον επόμενο κόμβο του anonymous tunnel, δημιουργώντας ένα malicious anonymous tunnel, επιτρέποντας έτσι τη συλλογή πληροφοριών από τον επιτιθέμενο, ο οποίος πλέον μπορεί να προβεί σε ανάλυση της δικτυακής κίνησης ή ακόμα και στην αποκρυπτογράφηση των πακέτων που διακινούνται.



Σχήμα 3.10: Δίκτυο με παρουσία Collusion nodes.

Σε γενικές γραμμές, είναι δύσκολο να εντοπιστούν κακόβουλοι κόμβοι στο δίκτυο, οι οποίοι κατά τα άλλα προσφέρουν καλές υπηρεσίες και συμμετέχουν όπως πρέπει. Τόσο ο Initiator όσο και οι

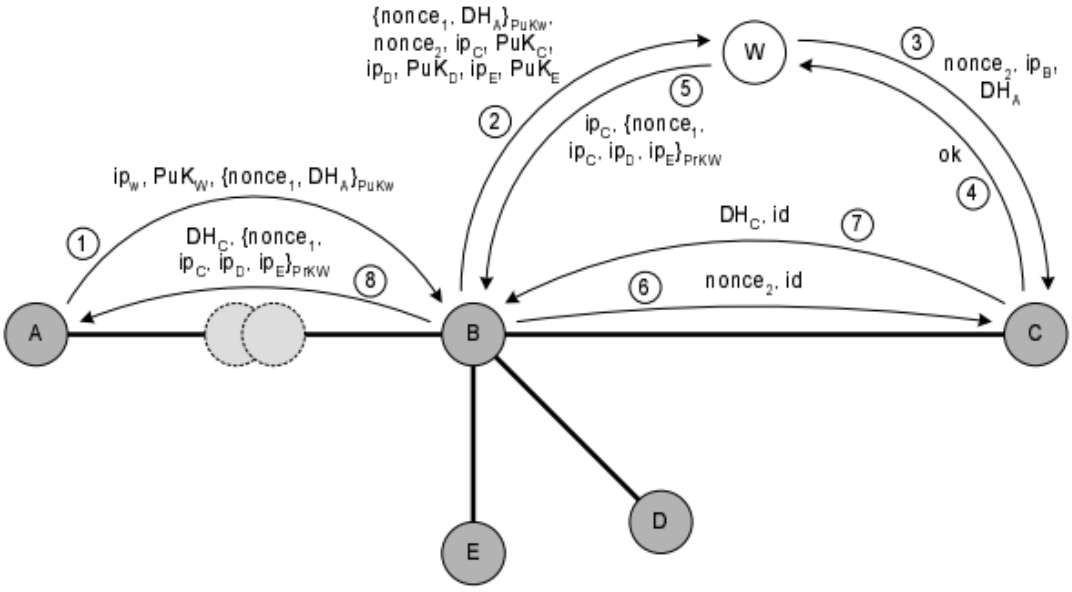
ενδιάμεσοι κόμβοι στο δίκτυο ανωνύμων επικοινωνιών δε μπορούν να γνωρίζουν αν κάποιος κόμβος συλλέγει και αναλύει δεδομένα. Κάτι που συνήθως διαφοροποιεί ένα σετ κακόβουλων, υποψήφιων ως next hop, κόμβων από άλλους honest nodes είναι το γεγονός ότι διαφημίζονται με τρόπο ώστε να έχουν περισσότερες πιθανότητες να επιλεχθούν. [104] [107] Έτσι, ενώ ένας honest κόμβος διαφημίζει με ίδιο τρόπο όλους τους υπόλοιπους κόμβους του, ένας malicious κόμβος που συμμετέχει σε μια Collusion Attack θα επιχειρήσει να προωθήσει περισσότερο τους κόμβους που συμμετέχουν στη “σκευωρία”.

Οι Collusion Attacks αποτελούν σημαντική πηγή κινδύνου για τα δίκτυα ανωνύμων επικοινωνιών, καθώς μπορούν να οδηγήσουν στην πλήρη απο-ανωνυμοποίηση της σύνδεσης, ταυτοποιόντας τόσο τον Initiator όσο και τον Receiver μιας σύνδεσης, καθώς και να επιτρέψουν στον επιτιθέμενο να αποκρυπτογραφήσει τα πακέτα που διακινούνται μέσω αυτής. [103] Οι επιθέσεις αυτού του τύπου δεν περιορίζονται μόνο στα δίκτυα ανωνύμων επικοινωνιών. Αντιθέτως, βρίσκουν πολύ μεγάλη εφαρμογή σε Online Social Networks, συστήματα αγοραπωλησιών, όπως τα Amazon και EBay, σε Blockchain Networks αλλά και σε Wireless Sensor Networks που χρησιμοποιούνται για την υλοποίηση του Internet of Things.

Οι επιθέσεις αυτές, όπως προαναφέρθηκε, μπορεί να επιστρατεύσουν μια σειρά κακόβουλων κόμβων όχι μόνο για να υλοποιήσουν ανάλυση της δικτυακής κίνησης, αλλά και για να εισάγουν κακόβουλο λογισμικό ή και πακέτα από μέρους του επιτιθέμενου. Αυτό παραπέμπει στις Sybil Attacks, οι οποίες αναλύονται παρακάτω. Η ουσιώδης διαφορά των Sybil με τους Collusion nodes είναι ότι στην πρώτη περίπτωση οι malicious κόμβοι που εμφανίζονται στο δίκτυο αποτελούν αντίγραφα της οντότητας του επιτιθέμενου, ενώ στη δεύτερη περίπτωση, οι Collusion nodes αποτελούν αντίγραφα κόμβων που εμπιστεύεται ο Initiator, ώστε αυτά να γίνουν μέρος του anonymous tunnel. [100]

Μοντέλο Επιθέσεων

Υποθέτουμε ότι ένας κακόβουλος κόμβος, ή ένα σύνολο κακόβουλων κόμβων, εισέρχεται στο δίκτυο, με σκοπό να απο-ανωνυμοποιήσει τη σύνδεση. Σαν σχήμα αναφοράς θα χρησιμοποιήσουμε τ παρακάτω:



Σχήμα 3.11: Διαδικασία επιλογής επόμενων κόμβων στο MorphMix.

Στην περίπτωση που ο κόμβος B είναι malicious, χωρίς να συνεργάζεται με άλλους κακόβουλος κόμβους, αλλά ο κόμβος W honest, τότε ο κόμβος B θα επιχειρήσει να σπάσει την ενθυλακωμένη κρυπτογράφηση μεταξύ των κόμβων A και C ώστε να έχει πρόσβαση στο περιεχόμενο των πακέτων που ανταλλάσσονται μεταξύ τους. Αυτό μπορεί να επιτευχθεί με δύο τρόπους. [83]

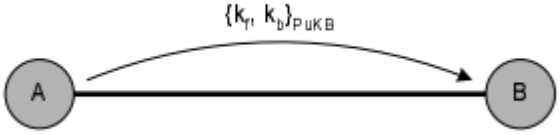
Ο πρώτος τρόπος είναι ο B να κάνει simulation του next hop μόνος του, οπότε θα ακολουθήσει τα εξής βήματα.

1. Αρχικά, στο μήνυμα 2 θα αντικαταστήσει τα public keys που σχετίζονται με τις IP Addresses με κλειδιά που θα δημιουργήσει μόνος του, για τα οποία γνωρίζει τα private keys. Στο βήμα αυτό, οι χρησιμοποιούμενες IP Addresses μπορεί να είναι είτε τέτοιες που αντιστοιχούν σε πραγματικούς, ενεργούς κόμβους του δικτύου, είτε σε κόμβους που δε συμμετέχουν, είτε ακόμα και σε κόμβους που δεν υπάρχουν καν στο δίκτυο.
2. Ο B θα υλοποιήσει interception του setup message που στέλνεται από τον W στον C για την εγκατάσταση κρυπτογραφημένης σύνδεσης στο συγκεκριμένο σύνδεσμο, με στόχο να μάθει το DHA του μηνύματος 3.
3. Ο B θα δημιουργήσει ένα ok-message το οποίο θα αποσταλεί από τον C στον W στο μήνυμα 4 προκειμένου να λάβει την απόδειξη αποστολής στο μήνυμα 5.
4. Ο B δημιουργεί το μισό του DH key-exchange και το εισάγει στο μήνυμα 8.

Ο B πλέον έχει καταφέρει να πλαστοπροσωπήσει τον C και να εμφανίζεται ως αυτός, χωρίς ο A να έχει κάποιο τρόπο να το εντοπίσει. Με παρόμοιο τρόπο, ο B μπορεί να κάνει spoofing και για τους υπόλοιπους κόμβους του anonymous tunnel. Ακόμα, ενδέχεται ο B να είναι ο τελευταίος κόμβος που επιλέγεται από τον A για τη δημιουργία του anonymous tunnel, με τα ίδια αποτελέσματα. [109] [110]

Ο δεύτερος τρόπος υλοποίησης της επίθεσης, αν ο B δρα μόνος του, είναι να χρησιμοποιήσει ως next hop έναν πραγματικό κόμβο και να υλοποιήσει μια Man-in-the-Middle Attack, ακολουθώντας τα εξής βήματα:

1. Αρχικά, στο μήνυμα 2 θα αντικαταστήσει τα public keys που σχετίζονται με τις IP Addresses με κλειδιά που θα δημιουργήσει μόνος του, για τα οποία γνωρίζει τα private keys. Στο βήμα αυτό, οι χρησιμοποιούμενες IP Addresses πρέπει υποχρεωτικά να είναι τέτοιες που αντιστοιχούν σε πραγματικούς, ενεργούς κόμβους του δικτύου.
2. Ο B θα υλοποιήσει interception του setup message που στέλνεται από τον W στον C για την εγκατάσταση κρυπτογραφημένης σύνδεσης στο συγκεκριμένο σύνδεσμο, υλοποιώντας μια Man-in-the-Middle Attack εκεί. Ο B υλοποιεί re-encyption του setup-message για την κρυπτογράφηση του link χρησιμοποιώντας το πραγματικό public key του C. Καθώς ο B γνωρίζει τα κλειδιά κρυπτογράφησης, μπορεί να υλοποιήσει interception του μηνύματος 3 και να μάθει το DHA.



Σχήμα 3.12: Interception μηνύματος.

3. Ο B αντικαθιστά το DHA με μια εκδοχή του που ο ίδιος δημιούργησε, την DHA' και το στέλνει στον κόμβο C μέσω του μηνύματος 3. Το πρωτόκολλο συνεχίζει τη λειτουργία του έως ότου ο B λάβει το μήνυμα 7.

4. Προτού στείλει το μήνυμα 8 στον A, ο B αντικαθιστά το DH_C με μια δική του εκδοχή, την οποία ο ίδιος δημιούργησε, την $DH_{C'}$.

Με τη μέθοδο που περιγράφηκε παραπάνω, ο B έχει καταφέρει πλέον να σπάσει το κρυπτογραφικό σχήμα μεταξύ των A και C, καθώς το έχει χωρίσει πλέον σε δύο μέρη. Μεταξύ των A, B τα πακέτα κρυπτογραφούνται με τα κλειδιά DH_A και $DH_{C'}$, ενώ παρόμοια κρυπτογράφηση γίνεται μεταξύ των B και C, χρησιμοποιώντας τα κλειδιά $DH_{A'}$ και DH_C. [108] [109]

Στην περίπτωση αυτή φυσικά, ο κόμβος B δεν έχει έλεγχο για τα επόμενα hops που θα επιλεχθούν για το anonymous tunnel, καθώς αυτοί θα επιλεγούν από τον C και αντίστοιχα από τους ακόλουθους κόμβους. Αν υποθέσουμε ότι ο επόμενος witness είναι ο V και επιλέγεται ως next hop ο κόμβος F, ο B θα μπορούσε να αντικαταστήσει το PuK_V στο μήνυμα 1 με ένα ψεύτικο κλειδί για το οποίο ο B γνωρίζει το private key. [83] Ομοίως με αυτά που περιγράφηκαν παραπάνω, ο B θα μπορούσε να κάνει interception του setup-message από τον C στον V, να διαβάσει τα κλειδιά κρυπτογράφησης, να δημιουργήσει ένα μήνυμα για τον V, χρησιμοποιώντας αυτή τη φορά το πραγματικό δημόσιο κλειδί του V. Στη συνέχεια ο B θα μπορούσε να κάνει interception του μηνύματος 2 και να αντικαταστήσει τα δημόσια κλειδιά που που αντιστοιχούν στις IP Addresses με τα δικά του δημόσια κλειδιά και επακόλουθα να κάνει interception του setup-message μεταξύ των V και F, να διαβάσει το DH_A από το μήνυμα 3 και ακολούθως να συνεχιστεί η επίθεση, με τα παραπάνω βήματα. Αξίζει να τονιστεί ότι αυτού του είδους η επίθεση είναι σαφώς πιο περίπλοκη από αυτή που ο B υλοποιεί spoofing των επόμενων κόμβων, καθώς ο επιτιθέμενος χρειάζεται να έχει τον έλεγχο πολύ περισσότερων κόμβων στο δίκτυο για να πετύχει το σκοπό του. [105]

Όσονα φορά την πρώτη επίθεση, στην οποία ο B μιμείται τους υπόλοιπους κόμβους, παρουσιάζει κι εκείνη αρκετές δυσκολίες, η κυριότερη εκ των οποίων είναι το γεγονός ότι ο επιτιθέμενος πρέπει να έχει τη δυνατότητα ελέγχου του συνδέσμου μεταξύ των W και C έτσι ώστε να μπορεί να κάνει intercept τα μηνύματα. Καθώς ο B δεν έχει τη δυνατότητα να προβλέψει ποιον witness κόμβο θα επιλέξει ο A, δεν είναι εύκολο να προετοιμαστεί εκ των προτέρων ώστε να είναι σε θέση να κάνει intercept τα μηνύματα από τον W. [101] Έτσι, ένα πιο ρεαλιστικό σενάριο θα ήταν να κάνει intercept τα μηνύματα από τον C, καθώς αυτός επιλέγει τη λίστα κόμβων στο μήνυμα 2. Ο B επί παραδείγματι θα μπορούσε να παρουσιάσει ως next hop, όσες IP Addresses είναι στο ίδιο δίκτυο με αυτόν, καθιστώντας σχετικά ευκολότερο να έχει πρόσβαση στα πακέτα που ανταλλάσσονται μεταξύ των W και C.

Σε περίπτωση που οι IP Addresses που παρουσιάζονται ως next hop από τον κόμβο B πρέπει να έχουν διαφορετικό prefix, η επίθεση καθίσταται δυσκολότερη, καθώς ο επιτιθέμενος αναγκάζεται πλέον να έχει τον έλεγχο σε διάφορες συνδέσεις (δηλαδή έλεγχο κόμβων σε διαφορετικά subnets) από τον W προς τους κόμβους τους οποίους παρουσιάζει ως υποψήφιους προς το next hop. Επιπροσθέτως, ο A, προκειμένου να εξασφαλίσει ότι δε θα εγκατασταθεί ένα malicious anonymous tunnel, μπορεί να απαιτήσει από τον κόμβο B να παρουσιάσει ένα ελάχιστο πλήθος υποψηφίων ως next hop κόμβων. Γίνεται εύκολα αντιληπτό ότι αν δεν υπάρχει ο παραπάνω περιορισμός, ο B, ως κακόβουλος κόμβος έχει τη δυνατότητα να παρουσιάσει ως next hop μόνο έναν υποψήφιο κόμβο, επίσης κακόβουλο, ο οποίος αναγκαστικά θα επιλεγεί. [103] [104] [105] Όσο πιο μεγάλο είναι το ελάχιστο πλήθος υποψηφίων next hop κόμβων που πρέπει να παρουσιάσει ένας κόμβος, τόσο δυσκολότερη καθίσταται η επίθεση. Παρόλα αυτά, αν κάποιος honest κόμβος δεν καταφέρει να παρουσιάσει το ελάχιστο αυτό πλήθος στον A, η εγκατάσταση του anonymous tunnel θα αποτύχει, επομένως πρέπει πάντα να επιλέγεται μια ισορροπημένη λύση για να διασφαλίζει τόσο την προστασία του δικτύου από Collusion Attacks, όσο και τη λειτουργικότητα του.

Ένας επιτιθέμενος ο οποίος έχει καταφέρει να αποκτήσει πρόσβαση σε πολλούς συνδέσμους του δικτύου, μπορεί να υλοποιήσει μια επιτυχημένη Collusion Attack και να υπονομεύσει την ασφάλεια του δικτύου. Στην περίπτωση που ο W είναι malicious κόμβος, τότε εκείνος μπορεί να χρησιμοποιηθεί για την υλοποίηση μιας Man-in-the-Middle Attack, αντικαθιστώντας το DHA στο μήνυμα 3 με ένα DHA' το οποίο ο ίδιος δημιούργησε. Στη συνέχεια κάνει intercept το μήνυμα 7 και αντικαθιστά το DHC με το DHC' το οποίο ο ίδιος δημιούργησε, σπάζοντας το κρυπτογραφικό σχήμα μεταξύ των A και C. Προκειμένου να μπορέσει να διαβάσει τα μηνύματα που ανταλλάσσονται μεταξύ των B και C πρέπει να υλοποιήσει Man-in-the-Middle Attack τη στιγμή εγκατάστασης της σύνδεσης μεταξύ τους. Η επίθεση αυτή είναι εξαιρετικά δύσκολο να πετύχει, καθώς ένας κόμβος δεν ξέρει αν και πότε θα επιλεχθεί ως witness node, ούτε και για ποιον τρίτο κόμβο θα είναι witness. Μια παραλλαγή του σεναρίου αυτού θα ήταν να προσπαθήσει ο W να μιμηθεί τον κόμβο C ώστε να κάνει intercept όλα τα μηνύματα που διακινούνται μεταξύ των B και C. Αυτό φυσικά απαιτεί ο επιτιθέμενος να έχει πρόσβαση σε πολλούς διαφορετικούς συνδέσμους στο δίκτυο και απαραιτήτως στο σύνδεσμο μεταξύ των B και C. Έτσι, καθίσταται ευκολότερο να υλοποιήσει μια επίθεση παρόμοια με αυτή όπου ο malicious κόμβος είναι ο B και προσπαθεί να κάνει impersonation όλους τους υπόλοιπους κόμβους του anonymous tunnel. [109]

Στη συνδυαστική περίπτωση των δύο παραπάνω επιθέσεων, όπου τόσο ο B όσο και ο W είναι ελεγχόμενοι από τον επιτιθέμενο, τότε ο B μπορεί πολύ εύκολα να υλοποιήσει impersonation του C, καθώς πλέον μπορεί να μάθει το DHA απευθείας από τον W. Επιπροσθέτως, ο W μπορεί να παρουσιάσει οποιαδήποτε IP Address θέλει, ως επόμενο υποψήφιο hop, στο μήνυμα 5. Φυσικά, καθώς ο κάθε witness επιλέγεται τυχαία από τον A, είναι εξαιρετικά δύσκολο να επιλέγονται συνεχώς witnesses κόμβοι που είναι στο ίδιο Collusion Attack με τους B και W, επομένως η επίθεση επί της ουσίας στα επόμενα στάδια, μέχρι την ολοκλήρωση του anonymous tunnel, είναι ίδια με την παραπάνω περίπτωση, όπου ο B είναι ο μόνος κακόβουλος κόμβος και προσπαθεί να κάνει impersonation του υπόλοιπους. [110]

Η πλέον επικίνδυνη μορφή των Collusion Attacks προκύπτει όταν ο B δεν δρα μόνος του, αλλά είναι μέρος ενός ευρύτερου γκρουπ κακόβουλων κόμβων. Στην περίπτωση αυτή, ο B μπορεί να παρουσιάσει τους συμμετέχοντες στο Collusion Attack κόμβους ως υποψήφιους για το next hop, γεγονός που θα οδηγήσει στην επιλογή ενός εξ αυτών. Φυσικά, ο περιορισμός που υπαγορεύει ο B να είναι σε διαφορετικό subnet από τους υποψήφιους next hop κόμβους που παρουσιάζει προσθέτει πολυπλοκότητα στην επίθεση, καθώς ο επιτιθέμενος πρέπει να διαθέτει κόμβους σε διαφορετικά γεωγραφικά σημεία. [106] Ωστόσο στην περίπτωση μιας συντονισμένης κυβερνοεπίθεσης προερχόμενης από στρατιωτικές/αστυνομικές υπηρεσίες ή ομάδες hackers, η επίθεση αυτή καθίσταται εύκολη και η επιτυχία της είναι βέβαιη.

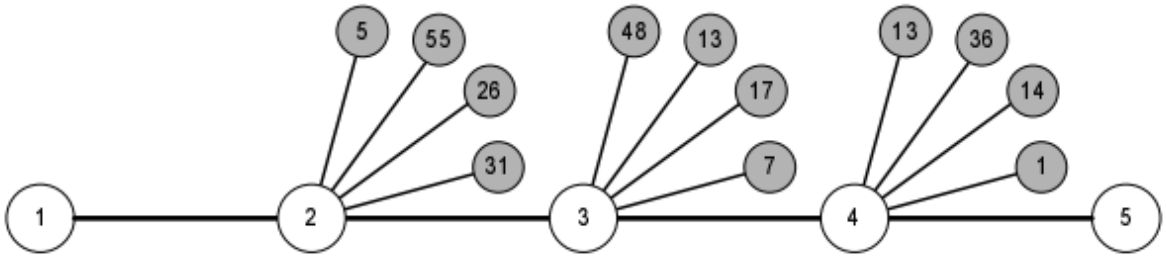
Από όλα τα παραπάνω σενάρια, η τελευταία περίπτωση είναι η πιο ισχυρή μορφή Collusion Attack, καθώς δύσκολα μπορεί να αντιμετωπιστεί, ενώ προσφέρει τον έλεγχο ολόκληρου του anonymous tunnel στον επιτιθέμενο. Η περίπτωση όπου τόσο ο B όσο και ο W είναι malicious nodes θα επιτρέψει στον επιτιθέμενο να ελέγξει ένα μέρος του anonymous tunnel, όχι όμως ολόκληρο. [98] [99] Τέλος, οι δύο πρώτες περιπτώσεις αποτελούν περισσότερο τη βάση πάνω στην οποία δουλεύουν οι Collusion Attacks, τα επιμέρους δηλαδή βήματα που υλοποιούνται στην τελευταία περίπτωση, παρά εάν ρεαλιστικό σενάριο επίθεσης. Συμπερασματικά, όπως προδίδει και το όνομα των επιθέσεων αυτών, όσο περισσότεροι κόμβοι αποτελούν τη “σκευωρία” (Collusion) στο δίκτυο, τόσο περισσότερες πιθανότητες έχει η επίθεση να καταστεί επιτυχής.

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Collusion Attacks

Το παραπάνω μοντέλο επιθέσεων μπορεί να επιφέρει πολλά προβλήματα στη λειτουργία των δικτύων ανωνύμων επικοινωνιών και εν τέλει να πλήξει την ανωνυμία των χρηστών. Στην περίπτωση μάλιστα που το δίκτυο δεχθεί επίθεση από μια ομάδα κακόβουλων κόμβων, υπάρχει η δυνατότητα να δημιουργηθεί ένα εξ ολοκλήρου malicious anonymous tunnel που θα δρομολογεί όλη τη δικτυακή κίνηση στον επιτιθέμενο.

Η προστασία ενός δικτύου ανωνύμων επικοινωνιών είναι εφικτή αν πραγματοποιείται ενδελεχής έλεγχος της συμπεριφοράς των κόμβων. Κατά κανόνα οι honest nodes όταν τους ζητηθεί τείνουν να διαφημίζουν τους άμεσα προς αυτούς συνδεδεμένους κόμβους με την ίδια συχνότητα. Αντίθετα, οι malicious nodes τείνουν να διαφημίζουν τους υπόλοιπους malicious nodes με τους οποίους είναι συνδεδεμένοι με μεγαλύτερη ένταση, προκειμένου να καταφέρουν να χτίσουν το malicious anonymous tunnel. Αν οι χρήστες των δικτύων χρησιμοποιούν τα διάφορα paths μόνο για περιορισμένο χρονικό διάστημα, υπάρχει η δυνατότητα να παρατηρηθούν οι κόμβοι οι οποίοι εμφανίζονται συχνά μαζί σε πολλά διαφορετικά paths, που σημαίνει ότι έχουν υψηλή συσχέτιση μεταξύ τους. Αυτή είναι μια σημαντική ένδειξη ότι ορισμένοι κόμβοι ανήκουν σε ένα Collusion και προσπαθούν να υλοποιήσουν ένα malicious anonymous tunnel. [108] Επιπλέον, σε περίπτωση που η χρήση του κάθε path γίνεται για περιορισμένο μόνο χρονικό διάστημα, εξασφαλίζεται ότι ακόμα κι αν ένας χρήστης παγιδευτεί σε ένα malicious tunnel, τότε θα το χρησιμοποιήσει για πολύ περιορισμένο όγκο δικτυακής κίνησης, ελαχιστοποιώντας τον κίνδυνο να αποκαλυφθεί η ταυτότητα και η δραστηριότητα του στο δίκτυο. [110]

Πάνω στη λογική αυτή βασίζεται και ο Collusion Detection Mechanism που χρησιμοποιείται από το MorphMix. Ο χρήστης παρατηρεί τα receipts που λαμβάνει από τους διάφορους witnesses κατά τη διάρκεια εγκατάστασης του anonymous tunnel, δηλαδή τα μηνύματα 5 και 8. Στο μήνυμα 2, περιέχονται οι IP Addresses των κόμβων που προσφέρονται ως next hop στον witness του κάθε βήματος. Ο πρώτος κόμβος στο receipt που λαμβάνει ο witness επιλέγεται ως next hop, έτσι, ο χρήστης γνωρίζει κάθε στιγμή ποιος κόμβος έχει προτείνει συγκεκριμένους κόμβους, σε κάθε στάδιο της δημιουργίας του anonymous tunnel. [105] [110]



Σχήμα 3.13: Προσφορά υποψήφιων κόμβων ως next hops.

Στην παραπάνω εικόνα παρουσιάζεται το σετ των κόμβων που παρουσιάζουν οι κόμβοι που συνθέτουν το anonymous tunnel. Κατά τη διάρκεια εγκατάστασης λοιπόν, μπορούμε να δούμε ότι ο κόμβος 2 προτείνει στον Initiator (κόμβο 1) το σετ {3, 5, 55, 26, 31} ως υποψήφια next hops. Ο witness του 2 επιλέγει τον κόμβο 3, για το λόγο αυτό στο σετ που βλέπει και καταγράφει ο κόμβος 1, ο επιλεχθείς κόμβος (εν προκειμένω περιπτώσει ο 3) παίρνει πάντα την πρώτη θέση. Έτσι, όταν

σχηματιστεί το anonymous tunnel, ο κόμβος 1 καταγράφει ότι το προτεινόμενο σετ από τον κόμβο 2 είναι το {3, 5, 55, 26, 31}, το προτεινόμενο σετ από τον κόμβο 3 είναι το [4, 48, 13, 17, 7} και το προτεινόμενο σετ από τον κόμβο 4 είναι το {5, 13, 36, 14, 1}. Ο συνδυασμός κόμβου και προτεινόμενου σετ ονομάζεται extended selection και αποθηκεύεται ως tuple στο table του αντίστοιχου tunnel, αφού ταξινομηθούν σε αύξουσα σειρά.

Το ζητούμενο στον συγκεκριμένο μηχανισμό είναι να εντοπιστούν κόμβοι οι οποίοι αλληλοδιαφημίζονται ως next hops. Ο παρακάτω αλγόριθμος έχει τη δυνατότητα να ελέγχει τη συσχέτιση μεταξύ των extended sets, προκειμένου να εντοπίσει ύποπτες συσχετίσεις. [110]

Algorithm 1 *Computing the correlation of an extended selection*

1. *Build a set ES_N consisting of the nodes of the new extended selection.*
2. *Define a result set ES_R which is empty at the beginning.*
3. *Compare each extended selection ES_T in the internal table with ES_N. If ES_N and ES_T have at least one element in common, then add the elements of ES_T to ES_R.*
4. *Count each occurrence of elements in ES_R that appear more than once and store the result in m.*
5. *Count the number of elements that appear only once in ES_R and store the result in s.*
6. *Compute the correlation c which is defined as $c = m/s$ if $s > 0$, or 0 otherwise.*

Σχήμα 3.14: Αλγόριθμος εντοπισμού colluding nodes.

Σε περίπτωση λοιπόν που παρατηρείται το φαινόμενο σε ένα extended set οι μη επιλεχθέντες ως next hop κόμβοι, να επαναλαμβάνονται στα επόμενα extended sets, αυτό αποτελεί μια σοβαρή ένδειξη ότι οι συγκεκριμένοι κόμβοι είναι Colluding nodes, καθώς παρουσιάζονται στους διάφορους witnesses εμφανώς περιορισμένες και επαναλαμβανόμενες επιλογές, πιθανότατα για να επιμηκυνθεί το malicious anonymous tunnel. [84] Όταν μάλιστα το φαινόμενο αυτό επαναλαμβάνεται για περισσότερα του ενός anonymous tunnel, δίνει συσχέτιση σημαντικά μεγαλύτερη από τις υπόλοιπες, γεγονός που είναι ισχυρή ένδειξη για μια υποκείμενη Collusion Attack στο δίκτυο.

Αξίζει να τονιστεί η σημασία της παρατήρησης και καταγραφής των extended sets για περισσότερα του ενός anonymous tunnels, καθώς έτσι εξασφαλίζεται ότι η υψηλή συσχέτιση που μπορεί να καταγραφεί μεταξύ κόμβων όντως ανταποκρίνεται, με μεγάλη πιθανότητα, σε colluding nodes και δεν είναι ψευδώς θετική. Είναι συχνό το φαινόμενο ορισμένοι κόμβοι να επαναλαμβάνονται εντός της δημιουργίας ενός anonymous tunnel, λόγω του αυξημένου bandwidth και των υπολογιστικών δυνατοτήτων που εκείνη τη στιγμή διαθέτει. [102] Ο κόμβος αυτός, αν ελέγχεται μόνο ένα table εσωτερικά για την εξαγωγή των συσχετίσεων μεταξύ κόμβων, μπορεί, λόγω της δημοφιλίας του τη δεδομένη στιγμή, να εκληφθεί ως colluding node και να απορριφθεί, δημιουργώντας προβλήματα και αστάθεια στη λειτουργία του δικτύου. Είναι σημαντικό λοιπόν να παρατηρείται η ποικιλία των προτεινόμενων κόμβων σε διαδοχικά anonymous tunnels. [99] Αυτό διασφαλίζεται από τον παράγοντα s στον παραπάνω αλγόριθμο, ο οποίος τείνει να είναι σημαντικά μεγαλύτερος του m όταν honest nodes παρουσιάζονται πολύ συχνά στα extended selections επειδή είναι δημοφιλείς, ενώ τείνει

να είναι σημαντικά μικρότερος του m, όταν συμβαίνει το αντίθετο, όταν δηλαδή οι συχνά εμφανιζόμενοι κόμβοι δεν είναι δημοφιλείς, αλλά malicious.

Με παρόμοιο τρόπο μπορεί να καθοριστεί και ένα tunnel αν είναι malicious, προκειμένου να απορριφθεί και να μη χρησιμοποιηθεί από τον χρήστη. Μπορεί έτσι να τεθεί ένα correlation limit για τους κόμβους, το οποίο δημιουργείται δυναμικά, από όλες τις καταγραφές που έχουν προηγηθεί, και υποδεικνύει αν ένας κόμβος είναι malicious (συσχέτιση άνω του correlation limit) ή honest (συσχέτιση κάτω του correlation limit). Σε περίπτωση που όλα τα extended selections έχουν συσχετίσεις κάτω του correlation limit, το tunnel θεωρείται honest, ενώ αν έστω και ένα extended selection υπερβεί το όριο, τότε το tunnel θεωρείται κακόβουλο και δε χρησιμοποιείται. Τα βήματα που ακολουθεί ο αλγόριθμος αυτός περιγράφονται συνοπτικά παρακάτω. [100]

Algorithm 2 *Determining if an anonymous tunnel is good or malicious*

1. *Initialize a variable rejectTunnel to false.*
2. *Get the next extended selection ES_N of the anonymous tunnel.*
3. *Compute the correlation c of ES_N according to algorithm 1.*
4. *Determine the limit correlation c_l from the correlation distribution.*
5. *If c is greater than c_l, set rejectTunnel to true.*
6. *Add c to the correlation distribution and add ES_N to the internal table.*
7. *If there are more intermediate nodes following in the tunnel, go to step 2.*
8. *If rejectTunnel is true, reject the tunnel. Otherwise it is considered good.*

Σχήμα 3.15: Αλγόριθμος εντοπισμού malicious tunnel.

Ο παραπάνω αλγόριθμος αποτυγχάνει μόνο στην περίπτωση που ο τελευταίος κόμβος είναι malicious, όμως σε αυτή την περίπτωση ο κόμβος αυτός δε μπορεί να συλλέξει πληροφορίες για την ταυτότητα ή τη δραστηριότητα του χρήστη. Ο καθορισμός του σωστού correlation limit είναι αρκετά σύνθετο ζήτημα, καθώς πολλές φορές οι honest nodes δεν είναι εύκολο να διαχωριστούν από τους malicious.

Εξελιγμένο Μοντέλο Collusion Attacks εναντίον του MorphMix

Οποιοσδήποτε χρήστης έχει πρόσβαση στο Internet και έχει εγκαταστήσει στο τερματικό του έναν MorphMix Client έχει τη δυνατότητα να συμμετέχει στο δίκτυο. Αυτό διευκολύνει σημαντικά την επεκτασιμότητα και την ευκολία χρήσης του συγκεκριμένου δικτύου ανωνύμων επικοινωνιών, ωστόσο καθίσταται εύκολο και στους επιτιθέμενους να συμμετέχουν σε αυτό, υλοποιώντας διάφορες επιθέσεις. Αξίζει να σημειωθεί ότι στις περισσότερες των περιπτώσεων, η μόνη ύποπτη και κακόβουλη συμπεριφορά των malicious nodes περιορίζεται στην προσπάθεια να επηρεάσουν τον σχηματισμό ενός anonymous tunnel. Κατά τα λοιπά, οι κόμβοι αυτοί συμπεριφέρονται και συμμετέχουν στο δίκτυο με τον ίδιο ακριβώς τρόπο όπως και οι υπόλοιποι. [104]

Θεωρούμε n το σύνολο των κόμβων που συμμετέχουν στο MorphMix και n_c ένα σύνολο Colluding nodes που ανήκουν σε διαφορετικά υποδίκτυα ο καθένας. Το n_c στην πραγματικότητα αντιπροσωπεύει τα διάφορα υποδίκτυα που έχουν colluding nodes, καθώς αν και ο πραγματικός αριθμός τους μπορεί να είναι σημαντικά μεγαλύτερος (καθώς ένα υποδίκτυο μπορεί να διαθέτει παραπάνω από έναν malicious node), ο Collusion Detection Mechanism που είδαμε προηγουμένως δεν λαμβάνει υπόψη του κόμβους εντός του ίδιου υποδικτύου για τον υπολογισμό των συσχετίσεων. [110]

Το σύνολο των malicious nodes αντιπροσωπεύουν ένα ποσοστό C σε σχέση με το σύνολο των διακριτών υποδικτύων που συμμετέχουν στο MorphMix. Το προαναφερθέν ποσοστό σε ρεαλιστικές τιμές μπορεί να κυμαίνεται από 0%, για ένα δίκτυο χωρίς malicious nodes, έως και 40%. Το ποσοστό αυτό καθορίζεται κατά κανόνα από το μέγεθος της επίθεσης, καθώς ένας μεμονωμένος επιτιθέμενος αντιπροσωπεύει ένα χαμηλό ποσοστό C, ενώ μια συντονισμένη κυβερνοεπίθεση από γκρουπ χακερς ή από κρατικές υπηρεσίες επιβολής του νόμου μπορούν να ανεβάσουν αρκετά υψηλά το ποσοστό, διαθέτοντας πόρους σε διαφορετικά υποδίκτυα. [109]

Στόχος της επίθεσης είναι η διασύνδεση ενός Initiator με κάποια συγκεκριμένη ροή δικτυακής κίνησης, κάτι που μπορεί να συμβεί αν ο επιτιθέμενος καταφέρει να αποκτήσει τον έλεγχο του πρώτου ενδιάμεσου, καθώς και του τελευταίου κόμβου από αυτούς που απαρτίζουν το anonymous tunnel. Η πιθανότητα να συμβεί αυτό είναι C^2. Έτσι, αν ένας επιτιθέμενος καταφέρει να αποκτήσει παρουσία, μέσω ελέγχου malicious nodes, στο 10% του συνόλου των υποδικτύων που συμμετέχουν εκείνη τη στιγμή στο MorphMix, έχει πιθανότητα 1% να ελέγξει τους δύο απαραίτητους για την επιτυχή έκβαση της επίθεσης κόμβους. Αντίστοιχα, παρουσία malicious nodes στο 40% των συμμετεχόντων υποδικτύων με αντίστοιχη συνεργασία μεταξύ τους, δίνει ποσοστό επιτυχούς έκβασης της επίθεσης 16%.

Οι επιτιθέμενοι όμως, μπορούν με έξυπνες επιλογές των extended selections να πετύχουν παρουσία σε κάθε anonymous tunnel που δημιουργείται, εισάγοντας μάλιστα μόνο malicious nodes σε αυτά χωρίς να εντοπίζονται από τον Collusion Detection Mechanism που έχει περιγραφεί. [107] [109] Πιο συγκεκριμένα, καθώς ο CDM κάθε κόμβου βασίζεται στις τοπικές εγγραφές του LEs, οι επιτιθέμενοι μπορούν να παραπλανήσουν τον μηχανισμό και να χειραγωγήσουν προς όφελος τους τη μήτρα των LEs.

Έτσι, οι colluding nodes θα πρέπει να προσφέρουν ως selection μόνο άλλους colluding nodes ενώ ταυτόχρονα τα selections αυτά να είναι οργανωμένα και δομημένα με τέτοιο τρόπο έτσι ώστε να παρουσιάζουν την ελάχιστη δυνατή επικάλυψη με άλλα malicious selections που ο κόμβος έχει αποθηκευμένα στο LEs του. Η στρατηγική αυτή εκμεταλλεύεται το γεγονός ότι ο Collusion Detection Mechanism σχεδιάστηκε ώστε να αντιμετωπίζει malicious nodes που προσφέρουν τυχαία selections από άλλους malicious κόμβους. Όταν όμως οι malicious selections προσφέρονται με τρόπο που να μην ενεργοποιούν το CDM, είναι εφικτή η παράκαμψη του. Τα ακόλουθα βήματα περιγράφουν το μοντέλο των εξελιγμένων Collusion Attacks στο MorphMix. [109]

1. Για κάθε victim u, σχεδιάζεται ένα σύνολο από selections S_u δομημένη κατά τρόπο τέτοιο, έτσι ώστε να μην υπάρχουν επικαλύψεις των υποδικτύων στα οποία ανήκουν οι κόμβοι, εντός του ίδιου συνόλου S_u.
2. Διατήρηση ενός global pointer p_g ο οποίος αποτελεί σημείο αναφοράς για το selection εντός του S_u το οποίο θα προσφερθεί στον επόμενο γύρο.

3. Όταν το victim u επιλέξει ως πρώτο ενδιάμεσο κόμβο έναν malicious node και ζητήσει ένα selection για να επιλεχθεί το next hop, παρέχεται το selection του S_u προς το οποίο δείχνει ο pointer p_g, ο οποίος στη συνέχεια αυξάνεται κατά 1. Σε περίπτωση που ο p_g δείχνει στο τελευταίο διαθέσιμο selection του S_u, παρέχεται αυτό και ο δείκτης επιστρέφει στην αρχή του.

Η παραπάνω επίθεση προϋποθέτει ότι ο κάθε malicious node γνωρίζει αν επιλέχθηκε ως ο πρώτος ενδιάμεσος κόμβος του anonymous tunnel. Αυτό είναι αρκετά δύσκολο να συμβεί στο MorphMix λόγω του ότι ο μηχανισμός επιλογής των witnesses είναι ο ίδιος σε κάθε επανάληψη. Επειδή ακριβώς ο malicious node πρέπει να καθορίσει αν είναι ο πρώτος ενδιάμεσος κόμβος προτού επιστρέψει το selection, είναι δύσκολο να καθορίσει αν είναι ο πρώτος ενδιάμεσος κόμβος μέσω Timing Attacks, καθώς μέχρι τότε έχουν ανταλλαχθεί ελάχιστα μηνύματα. [103] [106] Έτσι, ο παραπάνω αλγόριθμος επεκτείνεται για το σύνολο των βημάτων για τη δημιουργία ενός anonymous tunnel. Ο επιτιθέμενος μπορεί στη συνέχεια να καθορίσει αν ο πρώτος malicious κόμβος είναι και ο πρώτος ενδιάμεσος κόμβος του anonymous tunnel μετρώντας τους κόμβους μετά από αυτόν (καθώς όλοι θα είναι malicious και το μήκος μονοπατιού είναι σταθερό και εκ των προτέρων καθορισμένο. Έτσι, ο τελικός αλγόριθμος διαμορφώνεται ως εξής. [109]

1. Κάθε φορά που το victim u ζητάει ένα selection από έναν colluding node, η επίθεση ξεκινάει ορίζοντας έναν local pointer p_l ο οποίος δείχνει το selection που προσφέρεται σύμφωνα με τον global pointer p_g και στη συνέχεια προσφέρει το selection αυτό στον u.
2. Για κάθε επόμενο selection request που υλοποιεί ο victim από κάποιον malicious node, αυξάνουμε κατά ένα το p_l στο S_u και προσφέρεται το αντίστοιχο selection.
3. Μόλις δημιουργηθεί το anonymous tunnel, ο επιτιθέμενος καθορίζει αν ο πρώτος εν σειρά malicious node αποτελεί και τον πρώτο ενδιάμεσο κόμβο του, μετρώντας το μήκος του. Καθορίζεται με αυτό τον τρόπο αν ο κόμβος που αρχικά ζήτησε το selection ήταν το victim u ή κάποιος άλλος κόμβος u' που αποτελεί ενδιάμεσο κόμβο στο anonymous tunnel.
4. Εφόσον το anonymous tunnel δημιουργήθηκε από τον u, ο global pointer p_g λαμβάνει την τιμή που δείχνει ο local pointer p_l τη στιγμή εκείνη. Σε διαφορετική περίπτωση, ο p_g δε μεταβάλλεται, καθώς το malicious selection χρησιμοποιήθηκε από τον κόμβο u' και καταγράφηκε στο δικό του LES, επομένως μπορεί να χρησιμοποιηθεί στο victim u χωρίς να δημιουργήσει συσχετίσεις και να ενεργοποιήσει τον DCM.

Σε περίπτωση που η επίθεση απευθύνεται σε παραπάνω από ένα victims, θα πρέπει να δοθεί προσοχή έτσι ώστε να παρέχονται τα κατάλληλα selections στα κατάλληλα victims για να μην υπάρξει ενεργοποίηση του Collusion Detection Mechanism. Για την αποφυγή τέτοιων φαινομένων ο επιτιθέμενος θα πρέπει να χρησιμοποιεί διαφορετικές, τυχαίες μεταθέσεις του n_c όταν κατασκευάζει το S_u για κάθε διαφορετικό victim. Έτσι, είναι δυνατό να μετατεθεί τυχαία η σειρά των malicious nodes και να αποθηκευτεί στο S_u. [108] Στη συνέχεια επιλέγονται οι πρώτοι k κόμβοι και επαναλαμβάνεται κυκλικά η διαδικασία, με αποτέλεσμα να δημιουργούνται unique selections. Αυτό διασφαλίζει ότι τα misdirected selections δε θα αποτελέσουν κίνδυνο για την έκβαση της επίθεσης, καθώς τα unique selections αποτρέπουν τη δημιουργία ισχυρών συσχετίσεων στον Collusion Detection Mechanism. [100] [105]

Σε προσομοιώσεις επιθέσεων που έχουν γίνει, το βελτιωμένο μοντέλο επιθέσεων εξασφαλίζει μεγάλα ποσοστά επιτυχημένων Collusion Attacks. Αν ο επιτιθέμενος κατέχει κόμβους σε ποσοστό C=15% επί του συνόλου των διαφορετικών υποδικτύων που συμμετέχουν με κόμβους στο MorphMix, τότε μπορεί να δημιουργήσει τουλάχιστον 15% πλήρως malicious anonymous tunnels, ενώ αν το C φτάσει

στο 30% τότε ο επιτιθέμενος μπορεί να κάνει compromise σχεδόν το σύνολο των anonymous tunnels που δημιουργεί το victim, χωρίς να ενεργοποιήσει τον Collusion Detection Mechanism. [109]

Ένα αξιοσημείωτο πρόβλημα που αντιμετωπίζει ο επιτιθέμενος όταν διατηρεί κόμβους σε χαμηλό ποσοστό του συνόλου των διακριτών υποδικτύων (επιπέδου C=15%) που συνθέτουν το MorphMix είναι το γεγονός ότι έχουν πολύ περιορισμένους κόμβους να προσφέρουν στα πιθανά selections. Αυτό αναπόφευκτα οδηγεί στην επικάλυψη των προτεινόμενων selections, με αποτέλεσμα να ενεργοποιείται ο Collusion Detection Mechanism. [109] [110] Η λύση στο πρόβλημα αυτό προσφέρεται από τις έξυπνες επιλογές που προσφέρει το βελτιωμένο αυτό μοντέλο επιθέσεων. Έτσι, όταν ο επιτιθέμενος προσφέρει αρκετά unique selections, αποσύρεται για ορισμένο χρονικό διάστημα από την προσφορά selections προς τους υπόλοιπους κόμβους, προκειμένου να περιμένει έως ότου οι αντίστοιχες LEs τους γεμίσουν και γίνουν flushed. [108] Η συχνότητα αυτή εξαρτάται από το πόσο συχνά ένα victim δημιουργεί tunnels. Όπως έχουμε ήδη δει, κάθε κόμβος χρησιμοποιεί για πολύ περιορισμένο χρονικό διάστημα κάθε tunnel, με αποτέλεσμα το αντίστοιχο flushing της LEs του να συμβαίνει συχνά. Σε προσομοιώσεις επιθέσεων έχει παρατηρηθεί ότι ένας επιτιθέμενος με παρουσία στο C=10% των υποδικτύων του MorphMix, χρησιμοποιώντας την παραπάνω τεχνική μπορεί να κάνει compromise τα πενταπλάσια anonymous tunnels απ' ότι αν συνέχιζε να προσφέρει selections χωρίς διακοπή, έως ότου ανιχνευθεί από τον Collusion Detection Mechanism. Το ποσοστό C που απαιτείται να κατέχει ο επιτιθέμενος προκειμένου να μη χρειάζεται να σταματήσει την επίθεση έως ότου το LEs γίνει flushed έχει υπολογιστεί στο 15%. [101] Για $C \geq 15\%$ ο επιτιθέμενος μπορεί να συνεχίσει επ αόριστον την επίθεση του απρόσκοπτα, χωρίς να χρειάζεται να σταματήσει μόλις εξαντληθούν οι unique selections, ακριβώς γιατί το ποσοστό αυτό του εξασφαλίζει αρκούντως μεγάλο αριθμό κόμβων άρα και πιθανών unique selections που μπορεί να προσφέρει. [83] Μια ακόμα ενδιαφέρουσα προσέγγιση είναι αυτή στην οποία ο επιτιθεμενος προσφέρει selections που αποτελούνται από λίγους malicious και σημαντικά περισσότερους honest nodes, με αποτέλεσμα να μεγαλώνει σημαντικά ο παράγοντας u στον αλγόριθμο συσχέτισης, το οποίο έχει σαν αποτέλεσμα τη μείωση μελλοντικών συσχετίσεων και τη μείωση κινδύνου εντοπισμού. [104]

Ένα προφανές αντίμετρο στο βελτιωμένο μοντέλο επιθέσεων που περιγράφηκε παραπάνω είναι η αύξηση του μήκους του anonymous tunnel καθώς και του αριθμού των εγγραφών στο LEs. [109] Αυτό θα είχε ως αποτέλεσμα να εξαναγκάζεται ο επιτιθέμενος να προσφέρει περισσότερους κόμβους σε κάθε selection, κάτι που θα οδηγούσε στη συντομότερη πλήρωση του LEs και στη δημιουργία ισχυρών συσχετίσεων μεταξύ των malicious nodes προτού ο επιτιθέμενος καταφέρει να κάνει compromise μεγάλο αριθμό anonymous tunnels. Τα δύο αυτά μέτρα φυσικά δεν έρχονται χωρίς κόστος, καθώς η αύξηση του μήκους μονοπατιού οδηγεί αναπόφευκτα σε αυξημένο latency, ενώ η αύξηση των εγγραφών στο LEs οδηγεί σε αυξημένες αποθηκευτικές και υπολογιστικές ανάγκες τους κόμβους για την υλοποίηση του Collusion Detection Mechanism. [110]

Μια ακόμα λύση για την αντιμετώπιση αυτού του είδους των επιθέσεων είναι η εισαγωγή μεταβλητού μήκους μονοπατιού για το anonymous tunnel. Αυτό δυσκολεύει σημαντικά τον επιτιθέμενο στην προσπάθεια του να καθορίσει αν βρίσκεται στον πρώτο ενδιάμεσο ή στον τελευταίο κόμβο. Φυσικά, η πρόταση αυτή δεν αποτελεί πανάκεια, καθώς de facto ο αριθμός των ενδιάμεσων κόμβων που απαρτίζουν ένα anonymous tunnel είναι αυστηρά περιορισμένος ανάμεσα σε στενά όρια. Όπως έχουμε δει σε όλες σχεδόν τις τεχνολογίες ανωνύμων επικοινωνιών, οποιαδήποτε επιλογή μήκους μονοπατιού πάνω από ένα ρεαλιστικό όριο, όπως 8 ή 10 κόμβοι εισάγουν δυσβάστακτο latency στο δίκτυο, το οποίο καθίσταται πλέον ανίσχυρο να εξυπηρετήσει απαιτητικές διαδικτυακές εφαρμογές. [55] [73] [90] [109] Επιπροσθέτως, το δίκτυο καθίσταται πιο ευάλωτο σε failures σε περίπτωση που

ένας κόμβος, μέρος του tunnel αποχωρήσει από αυτό, κάτι που έχει αυξημένες πιθανότητες όταν το μήκος του μεγαλώνει. Επιπλέον, ακόμα και στην περίπτωση του μεταβλητού μήκους, ο επιτιθέμενος μπορεί να υλοποιήσει εκτιμήσεις της κατανομής των διαφόρων μηκών στο δίκτυο και να καθορίσει αν βρίσκεται στον πρώτο ή στον τελευταίο κόμβο. Το μεταβλητό μήκος των anonymous tunnels μπορεί να αποδυναμώσει σε κάποιο βαθμό τις Collusion Attacks αλλά όχι να τις αποτρέψει εξ ολοκλήρου. [104]

Στην περίπτωση του MorphMix οι νεοεισερχόμενοι στο δίκτυο χρήστες είναι ιδιαίτερα ευάλωτοι στις Collusion Attacks, καθώς έχουν κενό LES το οποίο μέχρι να γεμίσει για να γίνουν οι απαιτούμενες συσχετίσεις, δίνει αρκετό χώρο στους επιτιθέμενους να κάνουν compromise αρκετά anonymous tunnels. Ο μεγαλύτερος περιορισμός του Collusion Detection Mechanism είναι ότι λειτουργεί για κάθε κόμβο ξεχωριστά, χωρίς να λαμβάνει υπόψη του τις συσχετίσεις που δημιουργούνται στους υπόλοιπους κόμβους. Επιπλέον, ο επιτιθέμενος μπορεί εύκολα να καθορίσει το μέγεθος του LES, να υπολογίσει κάθε πότε γίνεται flushed, και να διακόπτει την επίθεση του στα κατάλληλα χρονικά διαστήματα προκειμένου να αποφύγει τον εντοπισμό. Οι παραπάνω λόγοι αποτελούν σημαντική τροχοπέδη για την ασφάλεια του δικτύου απέναντι σε Collusion Attacks κάτι που υπονομεύει σε μεγάλο βαθμό την ανωνυμία των χρηστών του. [109]

3.1.2.5 Latency Attacks

Εισαγωγικά Στοιχεία

Οι Latency Attacks αποτελούν μια από τις σημαντικότερες πηγές κινδύνου στις τεχνολογίες ανωνύμων επικοινωνιών και ίσως την πιο δύσκολη κατηγορία επιθέσεων, όσον αφορά την προστασία του δικτύου και των χρηστών του. Οι επιθέσεις αυτές βασίζονται στις θεμελιώδεις αρχές λειτουργίας των δικτύων, γι αυτό και είναι εξαιρετικά δύσκολο να εντοπιστούν και να αντιμετωπιστούν. Είναι γνωστό ότι τα πακέτα που διακινούνται μέσω διαφορετικών routes παρουσιάζουν διαφορετικό latency. Έτσι, ο επιτιθέμενος έχει τη δυνατότητα να παρατηρήσει, να καταγράψει τη δικτυακή κίνηση με απώτερο σκοπό να υπολογίσει τα διαφορετικά latencies που παρατηρούνται στο εκάστοτε δίκτυο ανωνύμων επικοινωνιών. Το latency λοιπόν αποτελεί από μόνο του μια εξαιρετικά σημαντική πηγή πληροφορίας για το δίκτυο, η οποία μπορεί να χρησιμοποιηθεί από κακόβουλους χρήστες προκειμένου να υπονομεύσουν την προστασία της ανωνυμίας των χρηστών του.

Οι Latency Attacks επηρεάζουν το σύνολο των τεχνολογιών ανωνύμων επικοινωνιών και είναι από τις πρώτες επιθέσεις που αναπτύχθηκαν εναντίον τους. Ήδη από τα πρώτα βήματα του Tor, αποδείχθηκε ότι ένας corrupt Tor node και ένας corrupt Web Server ο οποίος έχει υποστεί σημαντική αύξηση του φόρτου λόγω κίνησης που εξυπηρετεί, μπορούν να λειτουργήσουν συνδυαστικά προκειμένου να αποκαλύψουν τους υπάρχοντες κόμβους, οι οποίοι δρομολογούν τα πακέτα μιας σύνδεσης. Ο malicious Tor node μπορεί να στέλνει μηνύματα μέσω ενός loop σε όλους τους Web Servers, μετρώντας το χρόνο τον οποίο τα πακέτα βρίσκονται στο δίκτυο, καθώς διακινούνται. Στη συνέχεια, ο malicious web server, όταν θέλει να εντοπίσει τον Initiator μιας σύνδεσης, καθώς και το path που αυτός χρησιμοποιεί, μπορεί να μεταβάλει το throughput του σε ένα on/off burst μοτίβο, επιτρέποντας στον επιτιθέμενο να συσχετίσει την καθυστέρηση σε κάθε Tor Server, αντιπαραβάλοντας την με τις χρονικές στιγμές των on/off bursts. Με τον τρόπο αυτό, ο επιτιθέμενος μπορεί να παρατηρήσει αν δύο συνδέσεις χρησιμοποιούν το ίδιο path, εξάγοντας συμπεράσματα για τον Initiator τους.

Η παραπάνω είναι μια από τις πρώτες και πιο απλές Latency Attacks που εφαρμόστηκαν στο Tor. Η χρήση malicious web servers σε ένα δίκτυο ανωνύμων επικοινωνιών είναι σχετικά απλή και αυξάνει σημαντικά τις δυνατότητες του επιτιθέμενου. Αυτή είναι και η κύρια διαφοροποίηση των συγκεκριμένων επιθέσεων από τις Timing Attacks. Υπάρχουν διάφορες παραλλαγές των επιθέσεων που απασχολούν το παρόν κεφάλαιο. Μια από αυτές είναι η λεγόμενη Passive Linkability Attack, στην οποία latency noise προστίθεται στο δίκτυο, υπό τη μορφή επιπλέον καθυστέρησης που οφείλεται στο forwarding και στο mixing με άλλες ροές δεδομένων. Όταν ένας client επιχειρήσει να συνδεθεί σε δύο malicious web servers ή υλοποιήσει δύο συνδέσεις στον ίδιο malicious server, χρησιμοποιώντας την ίδια ανώνυμη σύνδεση, τα RTT των πακέτων μεταξύ client και server θα έχουν σαφή διαφοροποίηση από τα αντίστοιχα μεταξύ άλλων clients και του ίδιου server. Δύο colluding web servers μπορούν με τον τρόπο αυτό να συνδέσουν ροές πακέτων που χρησιμοποιούν το ίδιο Tor circuit. Η επίθεση αυτή δεν απαιτεί probing του δικτύου και έχει ελάχιστες απαιτήσεις σε bandwidth.

Μια άλλη παραλλαγή των Latency Attacks είναι η Analysis of noise-free anonymity leakage. Στην περίπτωση αυτή, το δίκτυο δε μπορεί να επιβάλλει οποιαδήποτε μορφή καθυστέρησης στο circuit. Έτσι, ο μόνος τρόπος να διαχωριστεί ένας client ο οποίος επικοινωνεί με έναν server μέσω του Internet και ενός client που επικοινωνεί χρησιμοποιώντας ένα δίκτυο ανωνύμων επικοινωνιών είναι ότι στη δεύτερη περίπτωση δεν εμφανίζεται η IP Address του client. Αυτή είναι και η πιο αντιπροσωπευτική μορφή επίθεσης που βασίζεται αποκλειστικά στην ανάλυση των RTTs.

Τέλος, αξίζει να σημειωθεί ότι οι Latency Attacks μπορούν να αποτελέσουν και Active Attacks, όπως στην περίπτωση των Active Client Identification Attacks. Είναι εξέλιξη της επίθεσης που περιγράφηκε στην αρχή της παρούσας ενότητας, η οποία ονομάζεται clogging attack. Η επίθεση αυτή απαιτεί πολύ περιορισμένους πόρους από την πλευρά των επιτιθέμενων, έναν corrupt Tor web server, έναν latency oracle που αναλαμβάνει τον υπολογισμό και τη σύγκριση των παρατηρούμενων RTTs μεταξύ των Tor servers και των nodes, χρησιμοποιώντας standard network protocols.

Οι επιθέσεις αυτές, λόγω της απλότητας στην υλοποίηση τους αλλά και της μεγάλης επικινδυνότητας για το δίκτυο, επιβάλλουν τη λήψη αντίμετρων, όπως την εισαγωγή τεχνητού latency προκειμένου να καταστεί δυσκολότερη η RTT ανάλυση στα διακινούμενα πακέτα. Απο προσομοιώσεις τέτοιου είδους επιθέσεων έχει αποδειχθεί ότι χωρίς να γίνει κάποιο optimization στα εν λόγω μοντέλα, ένας χρήστης μπορεί να ταυτοποιηθεί μετά από 50 περίπου επισκέψεις σε έναν ιστότοπο, το οποίο στην περίπτωση των σημερινών, υψηλής διαδραστικότητας διαδικτυακών εφαρμογών, αφορά λιγότερο από 8 ώρες παρατήρησης του δικτύου και της κίνησης έως ότου υπάρξει επιτυχής ταυτοποίηση του στόχου. Οι επιθέσεις αυτές είναι εξαιρετικά δύσκολο να εντοπιστούν και να αντιμετωπιστούν, καθώς βασίζεται σε μια πολύ απλή ανάλυση στοιχείων της δικτυακής κίνησης, ενώ αν συντονιστεί με άλλου είδους επιθέσεις, όπως Sybil και Collusion Attacks μπορεί να επιφέρει σημαντικά πλήγματα στην ανωνυμία και την ασφάλεια των χρηστών των τεχνολογιών ανωνύμων επικοινωνιών.

Μοντέλο Επιθέσεων

Όπως προαναφέρθηκε, οι Latency Attacks έχουν ευρύ πεδίο εφαρμογών. Τα proxy-based δίκτυα ανωνύμων επικοινωνιών περιπλέκουν σε κάποιο βαθμό τη διαδικασία ανάλυσης και υπολογισμού των RTTs που παρατηρούνται, σε σχέση με τα anonymous tunnels. Όταν ένας Tor exit node X λάβει TCP πακέτα από έναν server Y, υλοποιείται άμεσα η αναγνώριση του συμβάντος (acknowledgement), στέλνοντας τα δεδομένα πίσω στον client. Έτσι, οι συνήθεις TCP μηχανισμοί που χρησιμοποιούνται για τον υπολογισμό των RTTs μπορούν να υπολογίσουν μόνο το RTT από τον server στον proxy.

Αυτό φυσικά, από μόνο του, δεν αποτελεί αξιοποιήσιμο στοιχείο για την επίθεση. Για το λόγο αυτό, η επίθεση στοχεύει στους Web browsers προκειμένου να αποκτηθούν οι απαιτούμενες πληροφορίες.

Συγκεκριμένα, όταν ένας web server Y δέχεται ένα HTTP Request από έναν proxy node και θέλει να υλοποιήσει μια Latency Attack, στέλνει μια HTML σελίδα που περιέχει tags 1,000 <IMG height=1 width = 1 src= ...> τα οποία δείχνουν σε κενά αρχεία εικόνων. Αυτό έχει ως αποτέλεσμα οι web browsers που χρησιμοποιούν οι χρήστες να στείλουν επιπλέον 1000 ξεχωριστές συνδέσεις στον web server. Για κάθε μια από αυτές τις διακριτές συνδέσεις, ο Y θα λάβει ένα SYN μήνυμα από τον proxy node X και θα στείλει ένα SYN/ACK μήνυμα πίσω. Το πακέτο αυτό γίνεται ACK από τον X και στη συνέχεια ο X ειδοποιεί τον Initiator της σύνδεσης. Στην περίπτωση του Tor, ο proxy node X στέλνει στον Initiator ένα RELAY CONNECTED cell στον Initiator. Εν συνεχεία, ο Initiator A στέλνει ένα HTTP " GET " request στον X, ο οποίος το προωθεί στον web server Y. Ο χρόνος μεταξύ των ACK και GET πακέτων χρόνων άφιξης στον web server Y αποτελεί το δείγμα TAX το RTT δηλαδή μεταξύ του Initiator και του proxy.

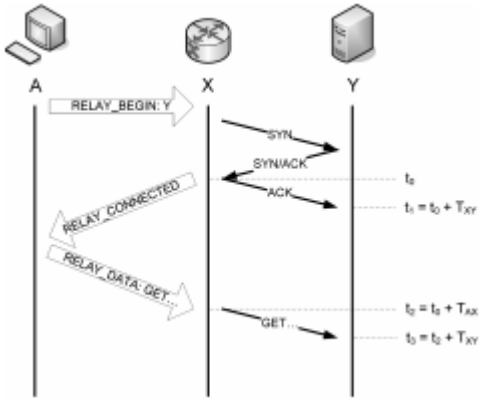
Η προαναφερθείσα μέθοδος επιτυγχάνει το στόχο της με δύο τρόπους. Ο πρώτος είναι με τη μέτρηση του χρόνου μεταξύ του serving μιας ιστοσελίδας και της λήψης ενός request για ένα embedded object. Ο δεύτερος αφορά τη μέτρηση του latency ενός κυκλώματος μέσω της παρατήρησης κάποιας συγκεκριμένης ιδιότητας (property) μιας ανώνυμης σύνδεσης. Και οι δύο μέθοδοι παρουσιάζουν σημαντικά προβλήματα όσον αφορά την αποδοτικότητα τους, καθώς χρειάζονται σημαντικό χρόνο έως ότου ολοκληρωθούν. Αυτό γίνεται προφανές όταν αναλογιστεί κάποιος ότι για την εξαγωγή ασφαλών συμπερασμάτων σχετικά με την καθυστέρηση σε ένα δίκτυο, θα πρέπει να υλοποιηθεί σημαντικός αριθμός μετρήσεων. Έτσι, στην περίπτωση μέσης καθυστέρησης t, ο επιτιθέμενος θα χρειαστεί να δαπανήσει n*t χρόνο, όπου n ο αριθμός των απαιτούμενων παρατηρήσεων. Επιπλέον, το μέγεθος του δείγματος μπορεί να μειωθεί σημαντικά σε αρκετές περιπτώσεις, μεταξύ των οποίων είναι και αυτή του Tor, στο οποίο γίνεται ανακύκλωση των χρησιμοποιούμενων κυκλωμάτων κάθε 10 λεπτά, εμποδίζοντας τον επιτιθέμενο να συλλέξει ικανό αριθμό μετρήσεων, ειδικά σε περίπτωση που το latency είναι μεγάλο.

Μια εξελιγμένη μορφή της επίθεσης αυτής περιλαμβάνει τον σχεδιασμό ενός application-level protocol από τον επιτιθέμενο, μέσω του pipelining, προκειμένου να καταφέρει να συλλέξει μεγαλύτερο αριθμό μετρήσεων και σε συντομότερο χρονικό διάστημα. Αυτό μπορεί να γίνει με τη χρήση ενός server που ελέγχει ο επιτιθέμενος, ο οποίος στέλνει περιοδικά timestamps στον client, ο οποίος τα κάνει echo πίσω στον server. Υποθέτοντας ότι η μεσολαβεί χρόνος i μεταξύ των διαδοχικών timestamps, ο επιτιθέμενος έχει τη δυνατότητα να συλλέξει n μετρήσεις σε χρόνο t+n*i, το οποίο μεταφράζεται σε αρκετές εκατοντάδες δείγματα, ακόμα και σε Tor δίκτυα με μεγάλο latency. Φυσικά, ένα πρόβλημα που προκύπτει είναι το κατά πόσον οι χρήστες που θα δεχθούν την επίθεση θα χρησιμοποιήσουν τον εν λόγω malicious server προκειμένου να καταστεί εφικτή η υλοποίηση της επίθεσης. Παρόλα αυτά, η πλειοψηφία των χρηστών του Tor χρησιμοποιεί τον περιηγητή ιστού Firefox, ο οποίος υποστηρίζει ταυτόχρονες συνδέσεις και persistent HTTP.

Το persistent HTTP μαζί με τη δυνατότητα ανακατεύθυνσης (redirect) προσφέρει τη δυνατότητα υλοποίησης του προαναφερθέντος timestamping, προκειμένου να καταφέρει ο επιτιθέμενος να συλλέξει στοιχεία για το latency του δικτύου. Η διαδικασία είναι εξαιρετικά απλή και υλοποιείται ως εξής. Το πρώτο request του χρήστη απαντάται με links σε k 1x1 εικόνες κάθε μια εκ των οποίων έχει ένα μοναδικό όνομα. Κάθε εικόνα όμως έχει ένα μοναδικό DNS name για τον server, αναγκάζοντας τον web browser του client να δημιουργήσει k persistent HTTP συνδέσεις με τον server. Όταν ο proxy

αιτηθεί ένα από αυτά τα αντικείμενα, ο server απαντάει με ένα HTTP/1.1 301 response—“Object Permanently Moved” μήνυμα, με ένα νέο URL του ίδιου server να έχει encoded το συγκεκριμένο timestamp. 19 επιπλέον μηνύματα με κωδικό 301 ακολουθούν, σε συγκεκριμένα, τακτά διαστήματα. Κάθε ένα από αυτά τα μηνύματα αποτελεί ένα response στο αντίστοιχο GET Request των timestamped μηνυμάτων που προηγήθηκαν. Ο client δεν απαιτείται να διαβάζει και να μεταφράσει επιτυχώς αυτά τα διαδοχικά μηνύματα. Αρκεί τα διαστήματα μεταξύ των διαδοχικών αποστολών να είναι μεγαλύτερα από το χρόνο επεξεργασίας των μηνυμάτων από τον client. Έτσι, ο client μόλις λάβει κάθε ένα από αυτά τα μηνύματα με κωδικό 301 θεωρούμε ότι αποκρίνεται άμεσα, στέλνοντας το GET Request για τη νέα τοποθεσία αμέσως.

Το εξελιγμένο αυτό μοντέλο επιθέσεων επιτρέπει όχι μόνο την ευκολότερη συλλογή πληροφοριών σχετικά με το latency του δικτύου, αλλά ταυτόχρονα είναι και ιδιαίτερα αποδοτική, καθώς δεν επιβαρύνει το δίκτυο. Ένα πλήρες HTTP Request/Response καταλαμβάνει περίπου 400 bytes από το bandwidth του δικτύου, ενώ το βελτιωμένο μοντέλο προσφέρει τη δυνατότητα υλοποίησης της επίθεσης με δέσμευση μόλις 4 bytes ανά μήνυμα με κωδικό 301. Στο παρακάτω σχήμα, παρουσιάζεται το βελτιωμένο μοντέλο της επίθεσης.

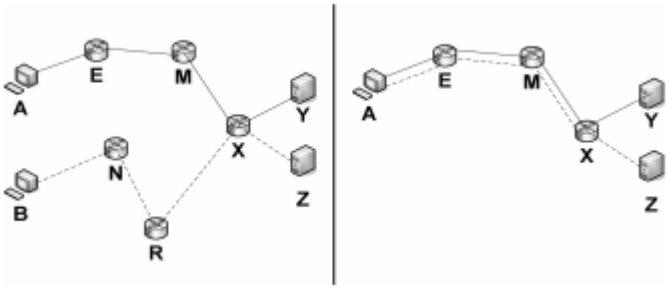


Σχήμα 3.16: Βελτιωμένο μοντέλο Latency Attacks.

Latency Attacks Case Studies

1. *Latency Attacks σε Διάφορα Δίκτυα Ανωνύμων Επικοινωνιών*

Μια συνήθης μορφή επίθεσης είναι αυτή στην οποία δύο malicious colluding servers Y και Z δέχονται συνδέσεις από τον proxy X με σκοπό να καθορίσουν αν τα μηνύματα που δέχονται προέρχονται από τον ίδιο ή διαφορετικούς clients. Ως βάση για την ανάλυση της επίθεσης θα χρησιμοποιήσουμε το παρακάτω σχήμα.



Σχήμα 3.17: Σχήμα αναφοράς για τις Latency Attacks.

Στο παραπάνω σχήμα υποθέτουμε ότι ο server Y επικοινωνεί με τον client A διαμέσου μιας ανώνυμης σύνδεσης η οποία τερματίζεται στον proxy X. Ο server Z επικοινωνεί με τον κόμβο B με τον ίδιο τρόπο, χρησιμοποιώντας μια διαφορετική ανώνυμη σύνδεση, η οποία επίσης τερματίζεται στον proxy X. Ορίζουμε ως T_{UV} την τυχαία μεταβλητή που συμβολίζει την καθυστέρηση μεταξύ των κόμβων U και V και ως T_U την αντίστοιχη μεταβλητή που συμβολίζει το χρόνο αναμονής στον κόμβο U. Η επίθεση υλοποιείται με τη συλλογή επαρκούς αριθμού δειγμάτων μεταξύ των $T_{AY} - T_{XY}$ και $T_{BZ} - T_{XZ}$, έτσι ώστε μέσω συγκρίσεων να καταλήξουμε σε συμπεράσματα σχετικά με το αν ανήκουν στην ίδια κατανομή πιθανότητας. Στο απλό proxy σύστημα ισχύει ότι $T_{AY} = T_{AX} + T_X + T_{XY}$ and $T_{BZ} = T_{BX} + T_X + T_{XZ}$, ενώ το αντίστοιχο κύκλωμα στα Tor δίκτυα περιλαμβάνει τους κόμβους E και M μεταξύ των A και X και N και R μεταξύ των B και X, δίνοντας τελικά $T_{AY} = T_{AE} + T_E + T_{EM} + T_M + T_{MX} + T_X + T_{XY}$ και $T_{BZ} = T_{BN} + T_N + T_{NR} + T_R + T_{RX} + T_X + T_{BZ}$. Αν ισχύει ότι A=B, δηλαδή ότι τα μηνύματα στην πραγματικότητα προέρχονται από έναν Initiator, τότε E=N και M=R, αφού το κάθε μονοπάτι στο Tor επιλέγεται εξ αρχής και δε μεταβάλλεται. Όπως είναι λογικό, οι μετρήσεις θα φαίνονται να προέρχονται από την ίδια κατανομή πιθανότητας.

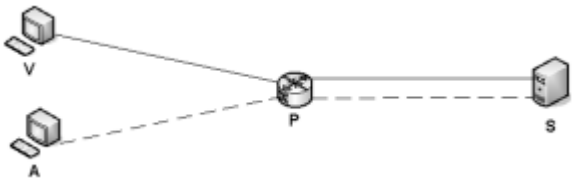
Με τη χρήση των Kolmogorov-Smirnov tests υπολογίζεται η μέγιστη διαφορά της συγκεντρωτικής πυκνότητας πιθανότητας μεταξύ δύο σετ δειγμάτων. Ορίζεται ένας παράγοντας απόρριψης, ο οποίος καθορίζει αν δύο σετ δειγμάτων αναφέρονται στον ίδιο Initiator (αν τα αποτελέσματα είναι μικρότερα από τον παράγοντα αυτό). Στην πραγματικότητα τα Kolmogorov-Smirnov tests έχουν μια περιοχή απόρριψης, επιτρέποντας στον επιτιθέμενο να επιλέξει την κατάλληλη τιμή, αναλόγως του tradeoff που θέλει να υλοποιήσει σχετικά με τα false-positive και false-negative error rates που θα παρουσιαστούν στην ανάλυση.

Το βασικό ερώτημα που προκύπτει από την ανάλυση των παραπάνω μοντέλων επιθέσεων είναι το κατά πόσο το latency ενός δικτύου μπορεί να αποτελέσει πηγή διαρροής πληροφοριών που μπορούν να αξιοποιηθούν σε κυβερνοεπιθέσεις. Η απάντηση στο ερώτημα αυτό δεν είναι απλή και εξαρτάται από πληθώρα παραγόντων. Ένα δίκτυο σε μορφή αστέρα για παράδειγμα, με ίσο μήκος καλωδίων μεταξύ των κόμβων δεν αποτελεί πρόσφορο έδαφος για την εξόρυξη πληροφοριών από το latency που παρατηρείται μεταξύ των διαφόρων κόμβων, ενώ στην περίπτωση ενός αμφίδρομου δακτυλίου, κάθε κόμβος μπορεί να αναγνωριστεί μοναδικά από το παρατηρούμενο latency. Σημαντικό ρόλο παίζει επίσης και το είδος του πρωτοκόλλου που χρησιμοποιείται, καθώς ο θόρυβος που προστίθεται στο δίκτυο μπορεί να καταστήσει την ανάλυση του latency αδύνατη.

Για το λόγο αυτό, έχει μελετηθεί το μέγεθος της πληροφορίας που μπορεί να εξαχθεί στην τοπολογία του Internet μέσω της παρατήρησης του latency, αν ένας επιτιθέμενος έχει ακριβή εικόνα για το RTT που εμφανίζεται σε έναν τυχαίο host. Ξεκινώντας από ένα σετ διακριτών υποψήφιων τοποθεσιών δικτύων {C1, C2, ... , CN }, σχηματίζεται μια τοποθεσία V, η οποία χαρακτηρίζει το θύμα, την οποία ο επιτιθέμενος θα προσπαθήσει να μαντέψει. Καθώς η τοποθεσία V επιλέγεται τυχαία, ο επιτιθέμενος έχει H0 = log2 N bits αβεβαιότητας σχετικά με την ακριβή πρόβλεψη της σωστής τοποθεσίας. Στη συνέχεια το περιβάλλον επιλέγει με ενιαίο τρόπο μια beacon τοποθεσία B1 και ένα μικρό δείγμα T1 από την κατανομή του latency μεταξώ των B1 και V και του επιτιθέμενου. Ο επιτιθέμενος μπορεί να υλοποιήσει ανάλυση δείγματος μεταξώ του B1 και όλων των Cis και καταλλήλως να ρυθμίσει την Pr[V = Ci] “belief” distribution. Πλέον, η νέα αβεβαιότητα είναι H1=i − Pr[V = Ci|T1] log Pr[V = Ci|T1], και η πληροφορία που εξήγαγε είναι H0 − H1. Καθώς η ανωτέρω διαδικασία επαναλαμβάνεται για τυχαία B2, B3, B4, ο επιτιθέμενος αυξάνει την αυτοπεποίθηση του και τη βεβαιότητα του για την ορθή αναγνώριση του στόχου. Η διαρροή πληροφορίας από m μετρήσεις είναι H0 − Hm, και αν το Hm είναι μικρό, τότε υπάρχει ένα μικρό σετ από υποψήφιες τοποθεσίες για το V.

Όταν οι clients εντοπίζονται μέσω μιας τοποθεσίας δικτύου, θα υπάρχουν μεγάλα σετ κόμβων τα οποία δε θα είναι διακριτά μεταξύ τους. Τυπικά, όλοι οι hosts εντός ενός δρομολογήσιμου IP prefix θα απέχουν μονάχα μερικά hops μεταξύ τους. Για 200,000 routable IP prefixes υπολογίζονται ως μέγιστο να υπάρχουν 2^{18} ξεχωριστές τοποθεσίες στο Internet. Σε πειράματα που έχουν πραγματοποιηθεί με 14,000 prefixes έχει υπολογιστεί ότι χρειάζονται περίπου 11.5 RTTs για την ορθή αναγνώριση μιας συγκεκριμένης φυσικής τοποθεσίας ενός host.

Οι προηγούμενοι παράγραφοι δείχνουν ότι η γνώση του latency μεταξύ ενός client και διαδοχικών hosts μπορεί να επιτρέψει σε έναν επιτιθέμενο να αναγνωρίσει ή να προσεγγίσει με μεγάλη ακρίβεια τις πιθανές τοποθεσίες ενός client. Στο πλαίσιο των ανυνώμων δικτύων τα οποία μελετά η παρούσα διπλωματική εργασία, θεωρούμε ότι στόχος είναι ένας client που θέλει να έχει ανώνυμη πρόσβαση στο δίκτυο, χρησιμοποιώντας διάφορες εφαρμογές. Κάθε φορά που ο client έχει πρόσβαση στο δίκτυο, υπάρχει η πιθανότητα να διαρρεύσουν πληροφορίες σχετικά με την τοποθεσία του δικτύου στο οποίο ανήκει. Ο ρόλος του malicious server είναι να ανακαλύψει την πιθανή αυτή τοποθεσία με τη μεγαλύτερη πιθανή βεβαιότητα και χρησιμοποιώντας τα ελάχιστα δυνατά anonymous links του δικτύου.



Σχήμα 3.18: Malicious Server.

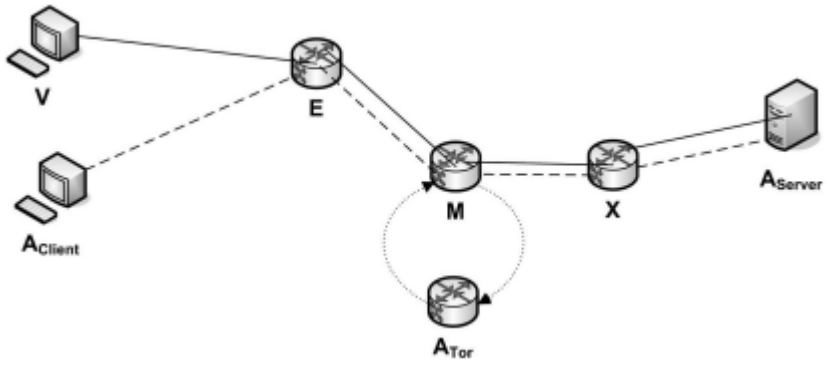
Η λειτουργία του δικτύου που βασίζεται σε proxy είναι πολύ απλή και παρουσιάζεται στο παραπάνω σχήμα. Ο client V συνδέεται στον server S μέσω του proxy. Τότε, μπορούμε να χρησιμοποιήσουμε timing analysis μεθόδους έτσι ώστε να υλοποιήσουμε ανάλυση δείγματος της κατανομής $T_{VS} = T_{VP} + T_P + T_{PS}$. Τα δείγματα αυτά περιλαμβάνουν τόσο το queuing delay από τον P όσο και τα network latencies T_{PS} and T_{VP}. Προκειμένου να γίνει δειγματοληψία από το T_P ο malicious server χρησιμοποιεί έναν συνεργαζόμενο client A για να συνδεθεί μέσω του P ανακτώντας δείγματα από το $T_{AS} = T_{AP} + T_P + T_{PS}$. Ο server υπολογίζει μια εκτίμηση της κατανομής του T_{VP} από τα παραπάνω δείγματα. Αν αυτή η εκτίμηση είναι ακριβής, δηλαδή έχει σε μεγάλο βαθμό κοινή πληροφορία με τη σωστή κατανομή, μπορεί να χρησιμοποιηθεί ως T1 χρόνος για να ενημερώσει την αυτοπεποίθηση του επιτιθέμενου ως προς τη σωστή αναγνώριση του στόχου.

Για τον υπολογισμό της κατανομής πιθανότητας του T1 μετράμε το RTT T_{AP} από κάθε δείγμα που συλλέχθηκε από το T_{AS}. Στη συνέχεια, για κάθε υποψήφιο RTT r χρησιμοποιούμε το MWW τεστ για να υπολογίσουμε την πιθανότητα $Pr[T_{VP} = \tau | T_{VS}, T_{AS} - T_{AP}]$. Ο υπολογισμός της εντροπίας αυτής της κατανομής μας δείχνει πόση αβεβαιότητα έχει ο επιτιθέμενος για το T_{VP} δεδομένων των παρατηρήσεων, ή πόση πληροφορία έχει χαθεί από τη χρήση της μεθόδου αυτής. Θα πρέπει να τονιστεί ότι, σε αντίθεση με την προηγούμενη μέθοδο, αυτή η μορφή επίθεσης δίνει μια διαρθρωμένη πληροφορία για το ποσό της πληροφορίας που διέρρευσε από το δίκτυο ανεξαρτήτως του set των υποψηφίων κόμβων. Μέσω πειραμάτων που έχουν διεξαχθεί προκύπτει ότι ένας επιτιθέμενος μπορεί να ανακτήσει μεγάλο μέρος πληροφορίας σχετικά με την τοποθεσία του victim, όταν αυτό χρησιμοποιεί έναν single-hop proxy server. Δεδομένου ότι χρειάζονται περίπου 11.5 RTTs κατά μέσο

όρο για την επιτυχή αναγνώριση της τοποθεσίας του victim, ορίζεται ως άνω όριο επισκέψεων οι 3.57 × 11.5 = 41 επισκέψεις.

2. Latency Attacks στο Tor Network

Κατόπιν της ανάλυσης των παραπάνω σεναρίων, μπορούμε να επεκτείνουμε την επίθεση κατά της τοποθεσίας του victim και στο Tor Network. Ο επιτιθέμενος εδώ απαρτίζεται από 3 logical entities. Αυτά είναι τα A_{Server}, ένας κακόβουλος δηλαδή Web server; A_{Client}, ένας κόμβος που παριστάνει έναν Tor client και A_{Tor}, έναν corrupted Tor server ο οποίος μπορεί να υλοποιήσει μια Murdoch-Danezis επίθεση. Η επίθεση αρχίζει όταν το victim V συνδέεται στον A_{Server} μέσω ενός Tor circuit που απαρτίζεται από τους κόμβους E, M, και X. Οι A_{Server} and A_{Tor} συνεργάζονται έτσι ώστε να υλοποιήσουν τη Murdoch-Danezis clogging attack και να αποκαλύψουν τους κόμβους E − M − X στο circuit. Τα ίδια entities συνεργάζονται προκειμένου να συλλέξουν πληροφορίες σχετικά με τη φυσική τοποθεσία του victim V. Στόχος της επίθεσης είναι, μετά από αρκετές επαναλήψεις, να αποκαλύψουν την ακριβή τοποθεσία του V με μεγάλη ακρίβεια.



Σχήμα 3.19: Latency Attack στο Tor.

Η βασική ιδέα πίσω από την επίθεση είναι να μετρηθεί, μέσω της χρήσης μιας Tor σύνδεσης T_{VE} το RTT μεταξύ του V και του entry node E. Ο επιτιθέμενος έτσι υπολογίζει, μέσω διαδοχικών υποψήφιων victim κόμβων C, το RTT T_{CE}. Χρησιμοποιώντας τις εκτιμήσεις αυτές ο επιτιθέμενος αυξάνει την αυτοπεποίθηση του σχετικά με την αποκάλυψη της φυσικής τοποθεσίας του victim node, επαναλαμβάνοντας τις επιθέσεις αυτές. Ύστερα από έναν ικανό αριθμό επαναλήψεων, ο επιτιθέμενος θα έχει μια πολύ καλή εικόνα σχετικά με τη φυσική τοποθεσία που αναζητά, έχοντας περιορίσει τις πιθανές τοποθεσίες δικτύων σε πολύ λίγες.

Από τη στιγμή που $T_{VX} = T_{VE} + T_E + T_{EM} + T_M + T_{MX} + T_X$, το circuit time περιλαμβάνει ορισμένες πληροφορίες σχετικά με το T_{VE} αλλά δε μπορεί να καθορίσει πλήρως το χρόνο που ενδιαφέρει τον επιτιθέμενο. Για το λόγο αυτό γίνεται αξιοποίηση της πληροφορίας που αποκτήθηκε από τη Murdoch-Danezis επίθεση. Όταν το V συνδέεται στον A_{Server} μέσω του Tor, υποθέτουμε ότι ο A_{Server} and A_{Tor} συνεργάζονται για να ανακαλύψουν τους κόμβους E − M − X που χρησιμοποιεί ο V για την ανώνυμη σύνδεση του. Η επίθεση αρχικά θα αποκαλύψει μόνο κόμβους του circuit αντί για την ακριβή σειρά με την οποία αυτοί εμφανίζονται στο μονοπάτι του V, όμως καθώς κάθε άλλος χρήστης του Tor Network χρησιμοποιεί μόνο 3 entry nodes και ο A_{Server} γνωρίζει τον exit node, ύστερα από αρκετές επαναλήψεις είναι εύκολο να καθοριστεί η σειρά των κόμβων στο μονοπάτι. Έως ότου συμβεί αυτό, ο επιτιθέμενος μπορεί να δοκιμάζει επιθέσεις με όλους τους πιθανούς συνδυασμούς και να απορρίψει τα λανθασμένα δεδομένα στη συνέχεια.

Χρησιμοποιώντας την παραπάνω ανάλυση, ο A_{Client} μπορεί να ανοίξει μια σύνδεση στον A_{Server} κάνοντας χρήση των ίδιων κόμβων E − M − X. Ο επιτιθέμενος μετράει το RTT των συνδέσεων αυτών, συλλέγοντας πολλαπλά δείγματα των T_{VX} και T_{AX}. Τα δείγματα αυτά, μαζί με τη γνώση του entry node time T_{AE} μπορούν να χρησιμοποιηθούν συνδυαστικά για τον υπολογισμό της κατανομής πιθανότητας T_{VE}. Εφόσον η κατανομή αυτή έχει μεγάλη εντροπία, μπορεί ο επιτιθέμενος να περιμένει και να χρησιμοποιήσει ένα άλλο circuit το οποίο χρησιμοποιεί σαν entry node τον E, έτσι ώστε να βελτιώσει την εκτίμηση του T_{VE}. Από πειράματα που έχουν υλοποιηθεί, εκτιμάται ότι χρειάζονται περίπου 50 server accesses προκειμένου να αναγνωριστεί η ακριβής τοποθεσία του δικτύου στο οποίο ανήκει το victim, αν δεν υπάρχει προηγουμένως οποιαδήποτε πληροφορία.

Έχοντας υπολογίσει το RTT από το victim προς τον Tor entry node E το επόμενο βήμα είναι η σύγκρισή του χρόνου στον κόμβο E με άλλους υποψήφιους κόμβους. Αν ελέγχουμε είτε κάποιον υποψήφιο κόμβο είτε τον E μπορούμε να τον υπολογίσουμε απευθείας, με τη χρήση του ping, ωστόσο αυτό είναι εκτός του πλαισίου του Tor Network που μελετάμε. Για να έχει η επίθεση πιθανότητες επιτυχίας πρέπει ο επιτιθέμενος να έχει μια μέθοδο εκτίμησης του RTT μεταξύ δύο hosts χωρίς να υπολογίζει στη συνεργασία τους. Για το λόγο αυτό γίνεται χρήση των network coordinates.

Ο όρος των network coordinates εισήχθη για τα peer-to-peer networks προκειμένου να γίνεται ευκολότερα αντιληπτό ποιοι hosts μπορούν να προσφέρουν καλύτερο routing ή downloading. Η βασική ιδέα πίσω από αυτό είναι η μέτρηση των RTTs μεταξύ κόμβων, έτσι ώστε να σχηματιστεί ένα ενιαίο σύστημα network coordinates που θα χαρακτηρίζει το δίκτυο, τέτοιο ώστε αν είναι γνωστές οι συντεταγμένες δύο κόμβων να μπορεί να προσδιοριστεί άμεσα το RTT μεταξύ τους. Το βασικό μειονέκτημα που παρουσιάζουν οι network coordinates αλγόριθμοι είναι ότι για να εξαχθεί επαρκής πληροφορία χωρίς τη χρήση συνεργαζόμενων κόμβων στο δίκτυο, πρέπει να χρησιμοποιηθούν διαδοχικοί κόμβοι για το service. Παρ όλα αυτά, διάφορες δωρεάν υπηρεσίες στο Internet, όπως το traceroute.org μπορούν να προσφέρουν RTT μετρήσεις από ένα γκρουπ hosts προς διάφορους τυχαίους hosts.

Από μετρήσεις που έχουν γίνει, έχει παρατηρηθεί πολύ μικρή απώλεια πληροφοριών, από την πλευρά του επιτιθέμενου, μέσω της χρήσης των network coordinates και τη μέτρηση του RTT. Η υλοποίηση της επίθεσης μπορεί να γίνει με τη χρήση διαφόρων τεχνικών, όπως αυτή του King, στην οποία μετράται το latency μεταξύ των A και B hosts υλοποιώντας ερωτήματα στον DNS server που είναι υπεύθυνος για το reverse DNS entry του A, ώστε να κάνει ένα recursive lookup στο DNS reverse entry του B. Άλλη πιθανή τεχνική είναι να γίνονται pings στους υποψήφιους κόμβους από τον entry node E, προσπαθώντας να επεκτείνει το circuit από το E σε ένα service που δεν υλοποιείται σε έναν υποψήφιο κόμβο κοντά στον A. Αν ο επιτιθέμενος υλοποιήσει το ίδιο service σε έναν corrupted κόμβο D και ζητήσει από τον E να επεκτείνει το circuit προς τον κόμβο D την ίδια στιγμή, τότε η διαφορά στους χρόνους των error messages των δύο requests αποτελεί μια πολύ καλή εκτίμηση των διαφορών στα αντίστοιχα RTTs.

Αξίζει να τονιστούν ορισμένοι περιορισμοί στο μοντέλο client location attack που αναπτύχθηκε στο παρόν κεφάλαιο. Ένας από αυτούς είναι το γεγονός ότι η επίθεση βασίζεται στην υπόθεση ότι το victim επισκέπτεται επανειλημμένως έναν server από την ίδια network location. Η πεποίθηση αυτή μπορεί να μην ισχύει, είτε λόγω κινητικότητας του host, είτε λόγω αστάθειας του route path. Η επίθεση μπορεί ακόμα να έχει επιτυχία αν τα Tor circuits προέρχονται από ένα μικρό αριθμό network

locations, όπως το σπίτι ή το μέρος εργασίας του victim, ωστόσο δεν έχει πιθανότητες επιτυχίας αν η τοποθεσία του αλλάζει συχνά και με μεγάλη αβεβαιότητα.

Ένας ακόμα περιορισμός που αφορά το client location attack αλλά όχι το linking attack, είναι η εξάρτηση της από τη Murdoch and Danezis attack. Οι επιθέσεις που βασίζονται στο redirection μπορούν να είναι επιτυχείς εφόσον ολοκληρωθούν εντός ενός εύλογου χρονικού διαστήματος. Έτσι, δεν έχει καταστεί ξεκάθαρο κατά πόσο οποιαδήποτε διάρκεια επίθεσης μπορεί να οδηγήσει σε επιτυχία, κάτι που έχει αντίκτυπο σε επιθέσεις που υλοποιούνται εντός μεγάλων Tor networks, που αναμφίβολα μεγαλώνουν και τη διάρκεια της επίθεσης.

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Latency Attacks

Οι παραπάνω επιθέσεις μπορούν να επεκταθούν σε όλα τα low latency δίκτυα ανωνύμων επικοινωνιών, όπως το Crowds και το I2P, καθώς προσφέρουν πολλαπλά entry points και relays με χαμηλή δικτυακή επιβάρυνση. Έτσι είναι δυνατή η συλλογή πιο στοχευμένων RTT μετρήσεων, επιτρέποντας στον επιτιθέμενο να εντοπίζει ένα victim με σημαντικά μεγαλύτερη ακρίβεια. Ορισμένα δίκτυα όπως το AN.ON μπορεί να παρουσιάζουν αυξημένη ανθεκτικότητα, ωστόσο κάποιο ποσο πληροφορίας είναι σίγουρο ότι θα φτάσει στα χέρια του επιτιθέμενου, μέσω της κατάλληλης ανάλυσης του latency. Επιπλέον, με τη χρήση κατάλληλων application-protocols, οι χρόνοι ολοκλήρωσης της επίθεσης μπορούν να βελτιωθούν σημαντικά. Χαρακτηριστικά παραδείγματα τέτοιων πρωτοκόλλων είναι τα IRC και SIP. Οι επιθέσεις αυτές μπορούν επίσης να ανακαλύπτουν τη φυσική τοποθεσία των servers που εξυπηρετούν hidden services. Ένας malicious Tor node και ένας hidden service client μπορούν να αναγνωρίσουν το second hop router (το πρώτο hop, όπως έχουμε δει γίνεται στον guard node ο οποίος είναι αξιόπιστος και δε μπορεί να χρησιμοποιηθεί από τον επιτιθέμενο) και να ανακτήσει πολύτιμες πληροφορίες σχετικά με το RTT μεταξύ του hidden service server και των guard nodes του. Αυτές οι εκτιμήσεις μπορούν να δώσουν με μεγάλη ακρίβεια την τοποθεσία του hidden service server, αν γίνουν συγκρίσεις με ήδη γνωστές network locations.

Υπάρχουν διάφορες τεχνικές προκειμένου να περιοριστεί ο αντίκτυπος των Latency Attacks στα δίκτυα ανωνύμων επικοινωνιών. Μια από αυτές είναι η ανάθεση συγκεκριμένου bandwidth για κάθε circuit, από τους onion routers, ανεξαρτήτως του αριθμού των circuits που βρίσκονται σε χρήση, καθώς και η δημιουργία ψεύτικης δικτυακής κίνησης. Αυτό φυσικά έχει κόστος στο συνολικό latency, άρα και το user experience στα ανώνυμα δίκτυα, ωστόσο παρέχει ένα σημαντικό βαθμό προστασίας έναντι αυτού του είδους των επιθέσεων.

Επιπλέον, οι Tor κόμβοι μπορούν να αποτρέψουν να γίνουν exploited ως RTT oracles με το να αρνούνται την επέκταση των circuits προς κόμβους που δεν περιλαμβάνονται στο directory. Επιπλέον, μπορούν να κάνουν drop τα ICMP ECHO REQUESTS έτσι ώστε να αυξήσουν το κόστος και το χρόνο δημιουργίας network coordinates από τον επιτιθέμενο, ενώ μπορούν να απενεργοποιηθούν τα recursive lookups από κόμβους εκτός του δικτύου. Είναι ακόμα δυνατή η απόρριψη όλης της δικτυακής κίνησης που δημιουργείται από pings. Τα παραπάνω δεν αποτρέπουν τη μέτρηση των RTTs ή το mapping που χρειάζεται για την υλοποίηση της επίθεσης, ωστόσο κάνουν τη διαδικασία υλοποίησης του network mapping ελαφρώς δυσκολότερη.

Ο πιο ασφαλής τρόπος αποτροπής τέτοιου είδους επιθέσεων είναι η προσθήκη επαρκούς delay έτσι ώστε τα RTT και timing χαρακτηριστικά του Tor network να γίνουν ανεξάρτητα του network topology. Αυτό μπορεί να επιτευχθεί με την τεχνητή καθυστέρηση των δεδομένων στον client. Έτσι,

η εισαγωγή delay με υψηλό ρυθμό μεταβλητότητας μπορεί να είναι ένα πολύ ισχυρό αντίμετρο στις Latency Attacks. Επίσης, οι circuit linking attacks μπορούν να αποτραπούν με την εισαγωγή delay σε κάθε Tor κόμβο, η οποία προέρχεται από την ίδια ακριβώς κατανομή.

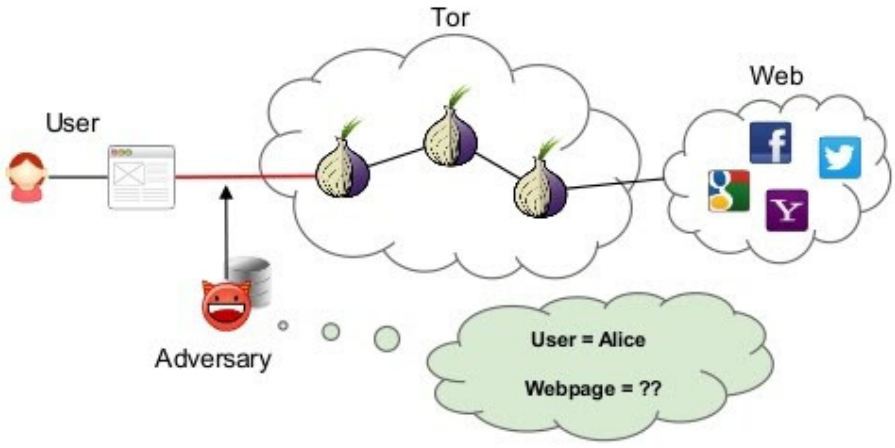
Παρ όλα αυτά, δεν πρέπει να ξεχνάμε ότι η χρήση των παραπάνω αντίμετρων, πρέπει να γίνεται λελογισμένα έτσι ώστε να διασφαλίζεται ότι δεν επηρεάζεται σημαντικά η λειτουργικότητα των low latency ανωνύμων δικτύων, έτσι ώστε αυτά να μπορούν να εξυπηρετούν ταυτόχρονα πολλαπλά requests προς latency-sensitive σύγχρονες δικτυακές εφαρμογές. Έτσι, για την αντιμετώπιση των παραπάνω επιθέσεων, θα μπορούσαν να εισαχθούν RTT-based circuits στα Tor δίκτυα, έτσι ώστε να παρατηρείται όσο το δυνατόν μικρότερη διαφορά στα RTTs, κάτι που δυσχεραίνει σημαντικά τις Latency Attacks.

3.1.2.6 Message Coding (Website Fingerprinting) Attacks

Εισαγωγικά Στοιχεία

Όταν ένας χρήστης επισκέπτεται έναν ιστότοπο, κατεβάζει μέσω του browser του πολλά διαφορετικά αρχείο τα οποία το απαρτίζουν. Τα αρχεία αυτά φιλοξενούνται στον web server και μπορεί να είναι HTML σελίδες, εικόνες, ακόμα και αρχεία πολυμέσων. Κάθε ένα από τα αρχεία αυτά έχει συγκεκριμένο μέγεθος. Σε έναν τυπικό browser, κάθε αρχείο λαμβάνεται από τον client σε μια ξεχωριστή TCP σύνδεση, σε διαφορετικό port. Έτσι, ο επιτιθέμενος μπορεί να υλοποιήσει συσχετίσεις των αρχείων που λαμβάνει κάποιος client από τον server, μετρώντας το μέγεθος των αρχείων που παραλήφθηκαν από κάθε διαφορετικό port.

Η ίδια ακριβώς τεχνική μπορεί να χρησιμοποιηθεί και ενάντια σε τεχνολογίες ανωνύμων επικοινωνιών, καθώς παρά την κρυπτογράφηση των αρχείων, συνήθως δεν υλοποιούνται τεχνικές obfuscation σε αυτά, για την αποφυγή δημιουργίας επιπλέον overhead στο δίκτυο. Έτσι, ο επιτιθέμενος μπορεί να παρατηρήσει το μέγεθος των πακέτων που φεύγουν από έναν web server τα οποία αποτελούν ουσιαστικά το ψηφιακό του αποτύπωμα (fingerprint). Στη συνέχεια, χρησιμοποιώντας τα fingerprints αυτά ο επιτιθέμενος μπορεί να παρακολουθήσει τη δραστηριότητα του δικτύου, καταλαβαίνοντας ποιους web servers και τι είδους περιεχόμενο λαμβάνουν τα victims της επίθεσης, ακόμα και αν δεν έχει καταφέρει να αποκαλύψει την ταυτότητα τους. Η επίθεση έχει πολύ χαμηλό κόστος υλοποίησης, είναι εύκολη να εφαρμοστεί σε ένα μεγάλο εύρος τεχνολογιών ανωνύμων επικοινωνιών και μπορεί να επιφέρει σημαντική υποβάθμιση της ανωνυμίας των χρηστών του δικτύου.



Σχήμα 3.20: Website Fingerprinting.

Το πλεονέκτημα των Website Fingerprinting Attacks είναι ότι ο επιτιθέμενος αρκεί να κάνει compromise το entry point του victim, καθιστώντας τες πολύ πιο αποδοτικές σε θέματα απαιτήσεων πόρων σε σχέση με άλλες επιθέσεις. Ο επιτιθέμενος στη συνέχεια παρατηρεί και καταγράφει όλη τη δικτυακή κίνηση από και προς το victim. Επειδή και ο ίδιος ο επιτιθέμενος, μέσω του compromised κόμβου αποτελεί μέρος του δικτύου, μπορεί και εκείνος να επικοινωνεί με τα διάφορα hidden services ή με κανονικούς ιστότοπους και να υλοποιήσει το website fingerprinting αναλόγως των αρχείων που λαμβάνει από τον καθένα. Υλοποιώντας σύγκριση των μεγεθών των αρχείων που παράγονται από τη δική του δραστηριότητα με αυτά που παρατηρεί από τη δικτυακή κίνηση που παράγει το victim, μπορεί με μεγάλη πιθανότητα να ανακαλύψει ποια services ακριβώς επισκέπτεται ο Initiator.

Οι συγκεκριμένες επιθέσεις υλοποιούνται κατά κύριο λόγο έναντι του Tor Network, ωστόσο θα μπορούσε να επεκταθεί και σε άλλες τεχνολογίες ανωνύμων επικοινωνιών. Ειδικότερα συστήματα που χρησιμοποιούν multiplexing των ροών πακέτων είναι ιδιαίτερα ευάλωτα σε τέτοιου είδους επιθέσεις.

Ενδιαφέρον παρουσιάζει το γεγονός ότι το fingerprinting είναι μια εξαιρετικά δημοφιλής πρακτική στον χώρο της κυβερνοασφάλειας, η οποία μπορεί να επεκταθεί και πέραν της δημιουργίας ενός αποτυπώματος για έναν ιστότοπο. Έτσι, η τεχνική αυτή μπορεί να επεκταθεί και για την ανάλυση και την εξαγωγή μοτίβων για τα χαρακτηριστικά του δικτύου. Εντάσσεται σε ένα συνολικότερο είδος επιθέσεων που βασίζονται στην ανάλυση της δικτυακής κίνησης και τη δημιουργία προφίλ των clients και των servers, προκειμένου να ανακαλύψουν την ταυτότητα τους. Το μοντέλο επιθέσεων αυτό μπορεί να είναι επιτυχές και όταν ο κακόβουλος χρήστης έχει τον έλεγχο του exit node στο μονοπάτι που συνδέει τον Initiator με τον Responder. Στην περίπτωση αυτή ο κίνδυνος αυξάνεται, καθώς είναι πολύ πιο εύκολο να καταγραφεί η κίνηση στον exit node και να υλοποιηθεί το fingerprint του μέσω καταγραφής της κίνησης που δημιουργούν ιδίως οι μη ανώνυμοι επισκέπτες.

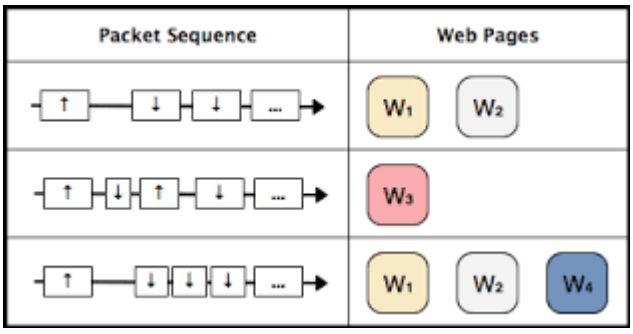
Website Fingerprinting Case Studies

1. *Website Fingerprinting Attacks στο Tor Network*

Ένα σημαντικό πρόβλημα που αντιμετωπίζουν οι εν λόγω επιθέσεις στο Tor Network είναι το γεγονός ότι η παρουσία του επιτιθέμενου σε ένα μόνο σημείο του δικτύου, και συγκεκριμένα στο entry point

του victim, καθιστά δύσκολη τη διάκριση κάθε μεγέθους αρχείου έτσι ώστε να σχηματιστεί το fingerprint για κάθε ένα από αυτά. [123]

Αν παρατηρήσει κάποιος τη δικτυακή κίνηση από και προς τον χρήστη, θα παρατηρήσει μια αλληλουχία πακέτων. Αν χρησιμοποιήσει την εκροή πακέτων από τον χρήστη, τότε μπορεί να ξεκινήσει να εξάγει ενδιαφέροντα συμπεράσματα σχετικά με το είδος των διακινούμενων αρχείων. Ορισμένα αρχεία μπορούν να έχουν πολύ σύντομα χρονικά διαστήματα μεταξύ τους, για παράδειγμα να παρατηρούνται 1 ή 2 εισερχόμενα πακέτα πριν εμφανιστεί ξανά κάποιο εξερχόμενο. Αυτό σημαίνει ότι ενδεχομένως τα πακέτα αυτά να αφορούν κάποιο πρωτόκολλο του δικτύου ή ορισμένα αρχεία πολύ μικρού μεγέθους, τα οποία έλαβε ο χρήστης από κάποιον server. Μεγαλύτερα χρονικά διαστήματα υποδηλώνουν μεγαλύτερα αρχεία. [121] Επίσης, πολύ σημαντική είναι η παρατήρηση των SYN, SYN-ACK και ACK μηνυμάτων που οριοθετούν τη λήψη νέων αρχείων από τον client. Έτσι, μέσω της παρατήρησης των αλληλουχιών αυτών μπορούν να σχηματιστούν σαφείς διαφοροποιήσεις μεταξύ των ιστοτόπων που επισκέπτεται το victim.



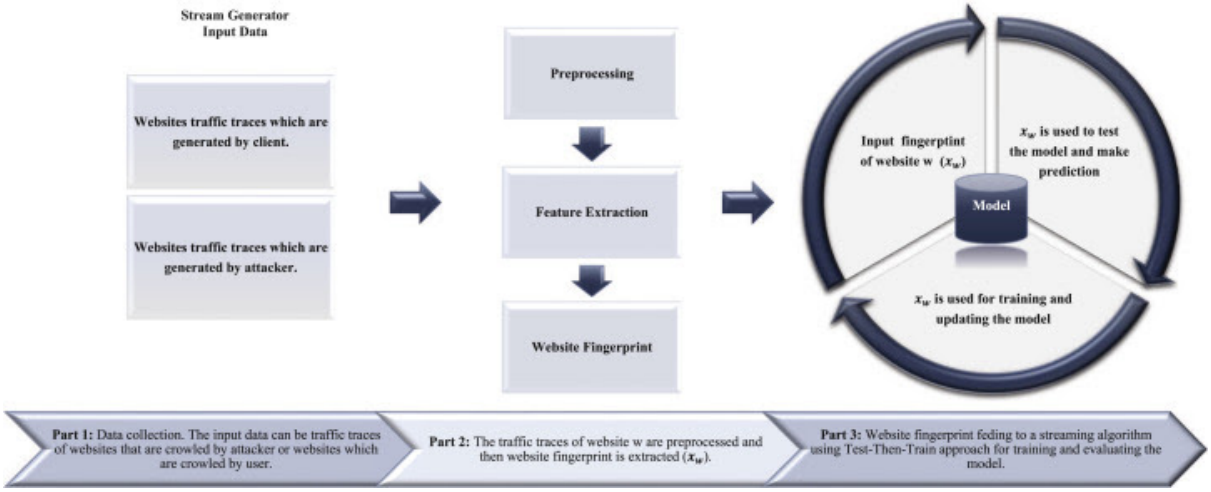
Σχήμα 3.21: Συσχέτιση αλληλουχίας πακέτων με τους αντίστοιχους ιστότοπους.

Έτσι, ως interval ορίζεται το χρονικό διάστημα κατά το οποίο υπάρχουν μόνο εισερχόμενα πακέτα και χρησιμοποιείται το διάνυσμα V=(v_1, v_2, v_3, …, v_n) που δηλώνει τον αριθμό των intervals με n πακέτα. Επίσης, εισάγεται το διάνυσμα F το οποίο ονομάζεται fingerprint vector. Η ομοιότητα S ορίζεται από τον τύπο: $S = \frac{V*F}{\|V\|*\|F\|}$ w . Αν υπάρχουν πολλά fingerprints τότε μπορεί ο επιτιθέμενος να υπολογίσει το V με κάθε F_i έτσι ώστε να πάρει τις ομοιότητες S_i και υλοποιώντας τις απαραίτητες συσχετίσεις του F με το μεγαλύτερο S_i να εξάγει συμπεράσματα σχετικά με τον ιστότοπο που επισκέπτεται το victim.

Στις συνηθεις Fingerprinting Attacks ένας ιστότοπος αποτελείται από περίπου 20 με 30 αρχεία, κάθε ένα από τα οποία έχει το δικό του μοναδικό μέγεθος. Έτσι, ο αριθμός των διακριτών ιστοτόπων στο δίκτυο είναι πάρα πολύ μεγάλος, κάτι που μπορεί να οδηγήσει σε μειωμένο detection rate της επίθεσης. Έτσι, όπως φαίνεται και στην παραπάνω εικόνα, η δικτυακή κίνηση σχετίζεται χρησιμοποιώντας σετ ιστοτόπων που έχουν αρχεία με παρόμοιο μέγεθος και παρόμοια patterns. Η ομαδοποίηση των ιστοτόπων και η χρήση των σετ που περιγράφηκαν επιταχύνουν και διευκολύνουν την υλοποίηση των επιθέσεων, δίνοντας πολύ καλά αποτελέσματα. [128]

Όσον αφορά την επιλογή του κατάλληλου fingerprint, οποιοσδήποτε vector μπορεί να χρησιμοποιηθεί ως fingerprint, λαμβάνοντας φυσικά υπόψη ότι και οι εκάστοτε θόρυβοι συμπεριλαμβάνονται σε αυτά. Η γενική αρχή είναι να χρησιμοποιούνται τα μικρότερα δυνατά μεγέθη που έχουν γίνει δειγματοληψία από τα αρχεία, καθώς αυτό ελαχιστοποιεί και την επίπτωση του θορύβου στο αποτύπωμα. Φυσικά, από τη στιγμή που τόσο ο επιτιθέμενος όσο και το victim

βρίσκονται στην ίδια περιοχή του δικτύου, το fingerprint θα πρέπει να περιλαμβάνει και πληροφορία που να αντικατοπτρίζει την κατάσταση του δικτύου.



Σχήμα 3.22: Διαδικασία Fingerprinting.

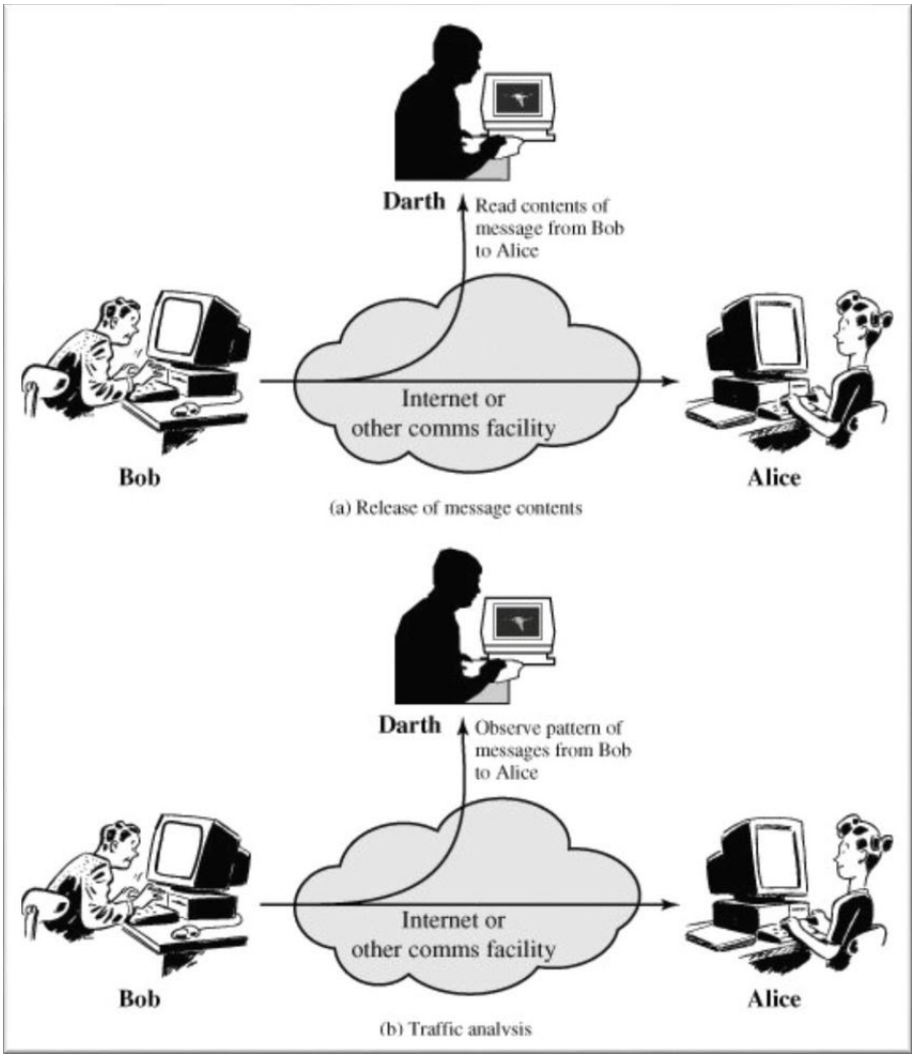
Τρόποι Αντιμετώπισης των Website Fingerprinting Attacks

Έχουν προταθεί διάφορες λύσεις για τη θωράκιση του Tor Network απέναντι στις συγκεκριμένες επιθέσεις. Η αύξηση του μεγέθους του cell φαίνεται να έχει πολύ μικρό αντίκτυπο στην ασφάλεια του δικτύου. Μια πρόταση είναι η υλοποίηση Odd Requests, δηλαδή requests που δεν έχουν κάποιον προορισμό ενδιαφέροντος προκειμένου να δημιουργήσουν επιπλέον δικτυακή κίνηση η οποία θα δυσκολέψει είτε τη δημιουργία του αποτυπώματος είτε στον υπολογισμό του similarity για τον συσχετισμό της κίνησης του θύματος με τα ήδη σχηματισθέντα fingerprints. [121] [123]

Κάτι τέτοιο θα μπορούσε να υλοποιηθεί με την ταυτόχρονη επίσκεψη σε ιστότοπους, έτσι ώστε ο επιτιθέμενος να βλέπει ένα συγκεντρωτικό vector, το οποίο θα είναι ίδιο με μια άλλη σελίδα που έχει αρχεία που αθροιστικά είναι του ίδιου μεγέθους με αυτά του συνδυασμού των διακριτών ιστοτόπων. Επίσης, οι χρήστες θα μπορούσαν να απενεργοποιήσουν τη λήψη αρχείων πολυμέσων, μέσω των web browsers τους, έτσι ώστε να δώσουν εσφαλμένους vectors στον επιτιθέμενο, δυσχεραίνοντας την ανάλυση που εκείνος υλοποιεί. [126] Η λύση αυτή προσφέρει όντως πολύ μεγάλο βαθμό προστασίας απέναντι σε Fingerprinting Attacks, ωστόσο έχουν το μειονέκτημα ότι ο βαθμός προστασίας που προσφέρει εξαρτάται από την εφαρμογή του από τους χρήστες του δικτύου, οι οποίοι δεν είναι βέβαιο ότι γνωρίζουν πώς να την υλοποιήσουν ή ακόμα μπορεί να μην είναι πρόθυμοι να το κάνουν. Υπάρχουν ορισμένα plugins όπως το TorButton που τυχαία απενεργοποιούν ορισμένα χαρακτηριστικά ενός ιστοτόπου, όπως εικόνες και scripts, ωστόσο πολλοί χρήστες είναι επιφυλακτικοί απέναντι σε τέτοιου είδους plugins και δεν είναι πρόθυμοι να τα χρησιμοποιήσουν.

Μια ακόμα χρήσιμη τεχνική αντιμετώπισης των επιθέσεων αυτών είναι η χρήση των Defensive Dropping τεχνικών, μέσω των οποίων δημιουργούνται dummy packets. Οι τεχνικές αυτές επιστρατεύονται από τις τεχνολογίες ανωνύμων επικοινωνιών για την αντιμετώπιση πολλών τύπων επιθέσεων, παθητικών και ενεργών. Τα πακέτα αυτά ενδέχεται να γίνουν dropped σε οποιονδήποτε κόμβο έτσι ώστε να καταφέρουν να καταστήσουν την ανάλυση του επιτιθέμενου αδύνατη. Ο μηχανισμός αυτός παρέχει πολύ υψηλά επίπεδα προστασίας, ωστόσο θεωρείται πολύ ακριβός μηχανισμός, ιδίως σε low-latency δίκτυα, καθώς δημιουργούν απαγορευτικά μεγάλο όγκο επιπλέον δικτυακής κίνησης. [121] [128] Σε περίπτωση που τα dummy πακέτα χρησιμοποιηθούν μόνο κατά τη διάρκεια διακίνησης ευαίσθητων πληροφοριών, ο επιτιθέμενος μπορεί να εντοπίσει την κορύφωση

του όγκου της δικτυακής κίνησης και να συμπεράνει ότι εκείνη τι στιγμή διακινούνται πληροφορίες υψηλής αξίας, επομένως η επιλεκτική χρήση των τεχνικών αυτών επίσης δε δίνει λύση στο πρόβλημα. Τα dummy packets είναι πράγματι η μόνη αξιόπιστη λύση για τη αντιμετώπιση των Fingerprinting Attacks, ωστόσο θα πρέπει να γίνει μελέτη ανάλογα με το μέγεθος του κάθε δικτύου, ώστε να εξασφαλιστεί ότι δε θα δημιουργήσει πρόβλημα διαθεσιμότητας των επικοινωνιών.



Σχήμα 3.23: Παράδειγμα Fingerprinting Attack.

3.1.3 Active Attacks

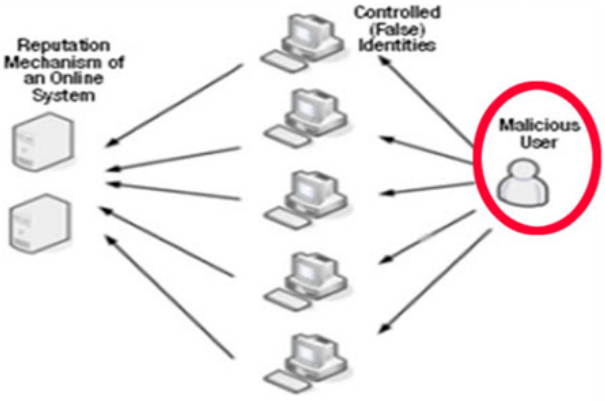
3.1.3.1 Sybil Attacks (Pseudospoofing)

Εισαγωγικά Στοιχεία

Οι Sybil Attacks είναι ένα ακόμα είδος επιθέσεων που καλούνται να αντιμετωπίσουν τα δίκτυα ανωνύμων επικοινωνιών, στο Στρώμα Δικτύου. Στόχος των Sybil Attacks είναι η υπονόμευση του χρησιμοποιηθέντος πρωτοκόλλου αξιοπιστίας των συμμετεχόντων ενός ή περισσοτέρων network services, σε ένα δίκτυο. Η γενική ιδέα πίσω από αυτές τις επιθέσεις είναι η δημιουργία ενός μεγάλου αριθμού ψευδωνύμων από τον επιτιθέμενο, με σκοπό αυτός να αποκτήσει δυσανάλογα μεγάλη επιρροή και αξιοπιστία στο δίκτυο ανωνύμων επικοινωνιών. [12] [32]

Οι επιθέσεις αυτές δανείστηκαν το όνομα τους από τη γνωστή περίπτωση της Sybil Dorsett, η οποία υπέφερε από Διαταραχή Πολλαπλής Προσωπικότητας (ψυχιατρική διαταραχή κατά την οποία μέσα σε ένα άτομο, στο πλαίσιο ποικίλων και διαφορετικών κοινωνικών και προσωπικών πλαισίων, συνυπάρχουν δύο, ή και περισσότερες, διακριτές ταυτότητες ή προσωπικότητες.). Η κλινική μελέτη της Sybil Dorsett (ψευδώνυμο της Shirley Ardell Mason) περιγράφηκε αναλυτικά στο βιβλίο της Flora Rheta Schreiber, Sybil. Το ευφάνταστο, αλλά πλήρως αντιπροσωπευτικό για το είδος των επιθέσεων, αυτό όνομα, προτάθηκε από τον Brian Zill της Microsoft Research. Το επίσημο όνομα των Sybil Attacks είναι Pseudospoofing ή αλλιώς Sock Puppetry. Σε αντίθεση με τις Predecessor και Disclosure Attacks που έχουμε εξετάσει, οι Sybil Attacks αποτελούν active attacks, αφού ο επιτιθέμενος δεν υλοποιεί απλώς παρατήρηση και ανάλυση της δικτυακής κίνησης, αλλά δημιουργεί ψεύτικες identities με σκοπό να αποκτήσει ενεργό επιρροή στις λειτουργίες των πρωτοκόλλων του. [38] [47]

Αυτού του είδους οι επιθέσεις είναι από τις πιο παλιές σε δίκτυα ανωνύμων επικοινωνιών, ενώ επεκτείνονται με πολύ μεγάλη συχνότητα και σε κοινωνικά, peer-to-peer δίκτυα που δεν έχουν στόχο τη διασφάλιση της ανωνυμίας των χρηστών τους. Οι επιθέσεις αυτές στοχεύουν στο reputation system του δικτύου. [50] Το reputation system είναι ουσιαστικά ένας αλγόριθμος, ο οποίος επιτρέπει την αξιολόγηση των peers ενός δικτύου από τους υπόλοιπους συμμετέχοντες, προκειμένου να εγκαθιδρυθεί εμπιστοσύνη μεταξύ των χρηστών. Έτσι, ένα δίκτυο ανωνύμων επικοινωνιών είναι ευπαθές σε αυτού του είδους επιθέσεις αναλόγως με το πόσο εύκολα επιτρέπει ο αλγόριθμος του reputation system που χρησιμοποιεί να δημιουργηθούν νέες ταυτότητες. [51] [54] Άλλοι παράγοντες που επηρεάζουν τις Sybil Attacks είναι το κατά πόσο οι οντότητες ενός δικτύου αντιμετωπίζονται ισάξια ως προς την αξιοπιστία τους, ανεξαρτήτως του αν ανήκουν στο δίκτυο για μεγάλο χρονικό διάστημα ή είναι πρόσφατες προσθήκες, καθώς και η αντιμετώπιση των οντοτήτων που δε συνδέονται ακόμα με έναν ήδη υπάρχοντα, αξιόπιστο peer. [61] Οι επιθέσεις αυτές είναι εξαιρετικά επικίνδυνες, καθώς μπορούν να υλοποιηθούν με σχετικά μικρό κόστος και να αποφέρουν αποτελέσματα με σημαντικά ποσοστά επιτυχίας.



Σχήμα 3.24: Παράδειγμα Sybil Attack.

Ως οντότητες ορίζονται οι συμμετέχοντες που έχουν πρόσβαση σε τοπικούς πόρους του δικτύου, και οι οποίες διαφημίζονται στους υπόλοιπους συμμετέχοντες παρουσιάζοντας μια ταυτότητα. [54] Ωστόσο, περισσότερες από μια ταυτότητες μπορούν να αντιστοιχούν σε μια μόνο οντότητα. Είναι μάλιστα σύνηθες, σε peer-to-peer δίκτυα να υπάρχει αντιστοίχιση πολλών ταυτοτήτων προς μια οντότητα για λόγους ασφάλειας, αξιοπιστίας, διαμοιρασμού πόρων του δικτύου και ακεραιότητας. Μάλιστα, όπως είδαμε και στις βελτιωμένες Statistical Disclosure Attacks, η χρήση ψευδώνυμων είναι και ένας εξαιρετικός τρόπος αντιμετώπισης τους. [67] Στην περίπτωση των Sybil Attacks, ο

επιτιθέμενος αξιοποιεί το χαρακτηριστικό αυτό των δικτύων προκειμένου να παρουσιάζεται αλλά και να συμμετέχει ενεργά στο δίκτυο υπό τη μορφή πολλών, διαφορετικών συμμετεχόντων και κόμβων. Με τον τρόπο αυτό, έχει τη δυνατότητα να αποκτά σημαντική επιρροή στο δίκτυο, επηρεάζοντας κατά το δοκούν την αξιοπιστία διαφόρων συμμετεχόντων, αυξάνοντας ψευδώς τη δική του, ακόμα και να εμποδίσει άλλους συμμετέχοντες να αποκτήσουν νέες ταυτότητες και να έχουν πρόσβαση στο δίκτυο.

Κατηγοριοποίηση των Sybil Attacks

Προκειμένου να κατανοηθούν καλύτερα οι μηχανισμοί μέσω των οποίων οι Sybil Attacks μπορούν να υπονομεύσουν την αξιοπιστία ενός δικτύου ανωνύμων επικοινωνιών. Έτσι, οι Sybil Attacks μπορούν να διαχωριστούν στις παρακάτω κατηγορίες.

- Direct vs Indirect Communication
  Οι Sybil Attacks εξαρτώνται άμεσα από το είδος των επικοινωνιών που εγκαθίσταται μεταξύ των legitimate (κανονικών) με τους Sybil κόμβους. Σε περίπτωση που ο επιτιθέμενος έχει τη δυνατότητα άμεσης επικοινωνίας, μέσω των Sybil κόμβων, με τους legitimate, τότε έχουμε direct (άμεση) επικοινωνία. Σε αντίθετη περίπτωση, ο επιτιθέμενος θα χρειαστεί να χρησιμοποιήσει τον δικό του legitimate κόμβο ως ενδιάμεσο, προκειμένου να επικοινωνήσει ένας Sybil με κάποιον άλλο legitimate κόμβο, γεγονός που συνιστά indirect (έμμεση) επικοινωνία. Όπως γίνεται εύκολα κατανοητό, οι Sybil Attacks που βασίζονται σε άμεση επικοινωνία είναι πολύ πιο απλές στην υλοποίηση τους αλλά και πολύ πιο δύσκολο να ανιχνευθούν.

- Busy vs Idle
  Σε P2P δίκτυα, συνηθίζεται να μένει ενεργός μόνο ένας πολύ μικρός αριθμός Sybil identities, ενώ οι υπόλοιπες παραμένουν αδρανείς. Σε περίπτωση που ο επιτιθέμενος μπορεί εύκολα να δημιουργεί νέες ψεύτικες identities, τότε έχει τη δυνατότητα να τις εισάγει και να τις αποσύρει αρκετά συχνά, με σκοπό να παρουσιάζονται ως αληθοφανείς, πραγματικές identities. Σε αντίθετη περίπτωση, ο επιτιθέμενος θα αναγκαστεί να χρησιμοποιήσει ταυτόχρονα τον περιορισμένο αριθμό Sybil identities που διαθέτει προκειμένου να επηρεάσει το σύστημα αξιολόγησης αξιοπιστίας του δικτύου, γεγονός που καθιστά πιο πιθανό να εντοπιστεί η επίθεση.

- Simultaneous vs. Non Simultaneous
  Ο επιτιθέμενος μπορεί να δημιουργήσει ταυτόχρονα όλες τις Sybil identities αλλά να τις παρουσιάσει στο δίκτυο ξεχωριστά, σε διαφορετικούς χρόνους. Στην περίπτωση αυτή, κάθε Sybil κόμβος αποκτά διαφορετικές ιδιότητες, με αποτέλεσμα να καθίσταται πολύ δύσκολος ο εντοπισμός τους, με κόστος βέβαια τόσο στην πολυπλοκότητα της διαδικασίας, όσο και στο χρόνο που χρειάζεται για να γίνει η διαδοχική εισαγωγή όλων των Sybil identities. Στις simultaneous επιθέσεις, όλοι οι Sybil κόμβοι συμμετέχουν ταυτόχρονα. Μια παραλλαγή τους είναι ένας φυσικός κόμβος να αλλάζει σε τακτά χρονικά διαστήματα τις identities του, προκειμένου να φαίνεται ότι όλες οι identities συμμετέχουν ταυτόχρονα στην επίθεση.

  Αντίθετα, στις Non Simultaneous επιθέσεις, ο επιτιθέμενος χρησιμοποιεί μέρος μόνο του συνόλου των Sybil identities κάθε φορά. Όπως προαναφέραμε και στη διάκριση μεταξύ των direct και indirect επιθέσεων, ο κακόβουλος χρήστης μπορεί να εισάγει ή να απομακρύνει τις identities αυτές από το δίκτυο, προκειμένου να δημιουργήσει μια ισχυρή ψευδαίσθηση ότι

πρόκειται για πραγματικές, υπαρκτές και legitimate οντότητες του δικτύου. Γενικότερα, οι legitimate οντότητες αποχωρούν και επανέρχονται στο δίκτυο με μεγάλη συχνότητα, έτσι οι Non Simultaneous επιθέσεις μπορούν πολύ αποτελεσματικά να παραπλανήσουν τους legitimate κόμβους ώστε αυτοί να αντιλαμβάνονται τους Sybil ως κανονικούς, δυσχαιρένοντας τον εντοπισμό τους. Επιπλέον, ο επιτιθέμενος έχει τη δυνατότητα ελέγχου πολλών διαφορετικών φυσικών κόμβων, που αποκτούν διαφορετικές identities, δίνοντας του τη δυνατότητα να πραγματοποιεί την επίθεση του εναλλάσοντας τες. Η τελευταία αυτή μέθοδος προσφέρει μεγάλα πλεονεκτήματα στον επιτιθέμενο όσονα φορά τη δυσκολία εντοπισμού των Sybil κόμβων, ωστόσο απαιτούν τον έλεγχο πολλών φυσικών κόμβων, κάτι που είναι απαιτητικό σε διαχειριστικούς πόρους, κοστοβόρο και δύσκολο να υλοποιηθεί, ειδικά από μεμονωμένους επιτιθέμενους. Τέτοιου είδους επιθέσεις μπορούν να πραγματοποιηθούν από ομάδες επιτιθέμενων, όπως κρατικές μυστικές υπηρεσίες ή ομάδες hackers.

- Insider vs. Outsider
  Εφόσον ο επιτιθέμενος είναι μέρος του δικτύου ανωνύμων επικοινωνιών και διατηρεί τουλάχιστον μια πραγματική identity, θεωρείται insider. Σε αντίθετη περίπτωση, θεωρείται outsider, ως προς το δίκτυο. Ο insider έχει πολύ περισσότερες δυνατότητες όσον αφορά την αλληλεπίδρασή του με το δίκτυο, καθώς μπορεί να εισάγει νέες ψεύτικες identities και να τις χρησιμοποιεί για να επικοινωνεί με legitimate κόμβους. Αντίθετα, οι outsiders έχουν πολύ περιορισμένη πρόσβαση στους πόρους και τις λειτουργίες του δικτύου που εξασφαλίζουν νέες identities, καθώς στην πλειοψηφία των περιπτώσεων, χρησιμοποιείται κάποιο είδος αυθεντικοποίησης των συμμετεχόντων, προκειμένου να δημιουργήσουν νέες ταυτότητες, όπως κωδικοί, tokens κλπ. Ο insider έχει πολύ μεγαλύτερη ελευθερία όσον αφορά τη διακίνηση δεδομένων και την επικοινωνία με άλλους κόμβους, καθώς συμμετέχει ως ομότιμος peer στο δίκτυο, τυγχάνοντας της εμπιστοσύνης των υπολοίπων κόμβων, προνόμια που δεν απολαμβάνει ένας επιτιθέμενος που δεν ανήκει στο δίκτυο (outsider). Γενικότερα, η επιπτώσεις των Sybil Attacks εξαρτώνται σε μεγάλο βαθμό από το αν ο επιτιθέμενος αποτελεί μέρος του δικτύου ή όχι, καθώς οι inside attacks μπορούν να προκαλέσουν σαφώς μεγαλύτερα προβλήματα. Υπο προϋποθέσεις, οι Sybil Attacks είναι δυνατό να εντοπιστούν μέσω της ανάλυσης δικτυακής κίνησης μεταξύ ενός ύποπτου κόμβου με έναν αξιόπιστο, κάτι που ωστόσο δε συνηθίζεται στα δίκτυα ανωνύμων επικοινωνιών, στα οποία η παρακολούθηση και η ανάλυση της δικτυακής κίνησης, ακόμα και για λόγους ασφαλείας των χρηστών, είναι αντίθετη στην αρχή λειτουργίας τους και το σκοπό για τον οποίο δημιουργήθηκαν και χρησιμοποιούνται.

Μοντέλο Επιθέσεων

Οι Sybil Attacks εμφανίζονται σε όλα σχεδόν τα P2P δίκτυα, είτε πρόκειται για συστήματα διαμοιρασμού αρχείων, όπως το BitTorrent, είτε σε ανώνυμα δίκτυα επικοινωνιών. Η αντιμετώπιση τους καθίσταται δύσκολη, ειδικά χωρίς την ύπαρξη κάποιας κεντρικής αρχής πιστοποίησης (CA-Certificate Authority) που θα αναλαμβάνει τη διαχείριση των χρηστών και τη δημιουργία και διαμοιρασμό νέων ταυτοτήτων μόνο σε μη κακόβουλους χρήστες. Αυτό ωστόσο, όπως έχουμε ήδη δει, αντιβαίνει τις αρχές λειτουργίας των ανωνύμων δικτύων, με αποτέλεσμα να απαιτούνται άλλου είδους τεχνικές. [57] [58] [60]

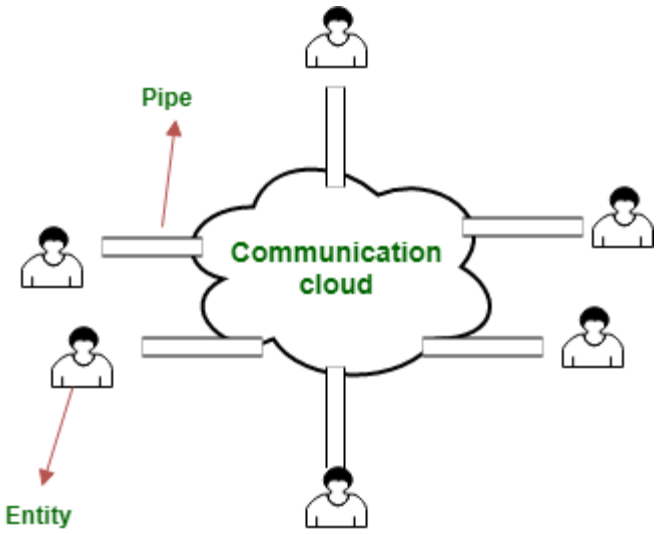
Η αποτελεσματικότητα των Sybil Attacks εξαρτάται από το μέρος της δικτυακής κίνησης που μπορεί να παρατηρήσει ο επιτιθέμενος, το οποίο ονομάζεται consensus weight. Όσο μεγαλύτερο είναι το

consensus weight του επιτιθέμενου, τόσο ευκολότερες καθίστανται και οι Sybil Attacks. Το πιο ευπαθές δίκτυο ανωνύμων επικοινωνιών είναι το Tor, ωστόσο το μεγαλύτερο πλήθος επιθέσεων, έχει στόχο τα Blockchain networks και τις συναλλαγές με κρυπτονομίσματα γενικότερα. [68]

Όπως ήδη αναφέραμε, η δημιουργία πολλαπλών identities από έναν φυσικό κόμβο είναι κάτι σύνηθες, καθώς μπορεί να προστατεύσει τόσο την ακεραιότητα, όσο και την ιδιωτικότητα των δεδομένων, μέσω του replication και του fragmentation των υπολογιστικών και δικτυακών πόρων. [38] [49] Ο επιτιθέμενος μπορεί να εκμεταλλευτεί το redundancy του δικτύου, καθώς στις περισσότερες φορές, οι φυσικές οντότητες (physical entities) δεν έχουν απευθείας σύνδεση ή γνώση των υπολοίπων, με αποτέλεσμα η επικοινωνία μεταξύ τους να βασίζεται αποκλειστικά στις identities που υιοθετούν στο παρόν δίκτυο.

Υπό φυσιολογικές συνθήκες, σε ένα οποιοδήποτε δίκτυο, είτε αφορά ανώνυμες επικοινωνίες είτε όχι, οι ήδη υπάρχουσες οντότητες εγγυώνται για οποιαδήποτε άλλη νεοεισελθείσα οντότητα, προκειμένου εκείνη να λάβει identity και να αποτελέσει μέλος των συμμετεχόντων. [37] Παρόλα ταύτα, ο μοναδικός τρόπος να εγγυηθεί κάποιος την ακεραιότητα μιας νέας οντότητας που εισέρχεται στο δίκτυο προϋποθέτει την ύπαρξη ενός CA, ο οποίος αναλαμβάνει τον έλεγχο των οντοτήτων και τη διανομή των identities, καθώς και τη διαχείριση τους καθ όλη τη λειτουργία του δικτύου.

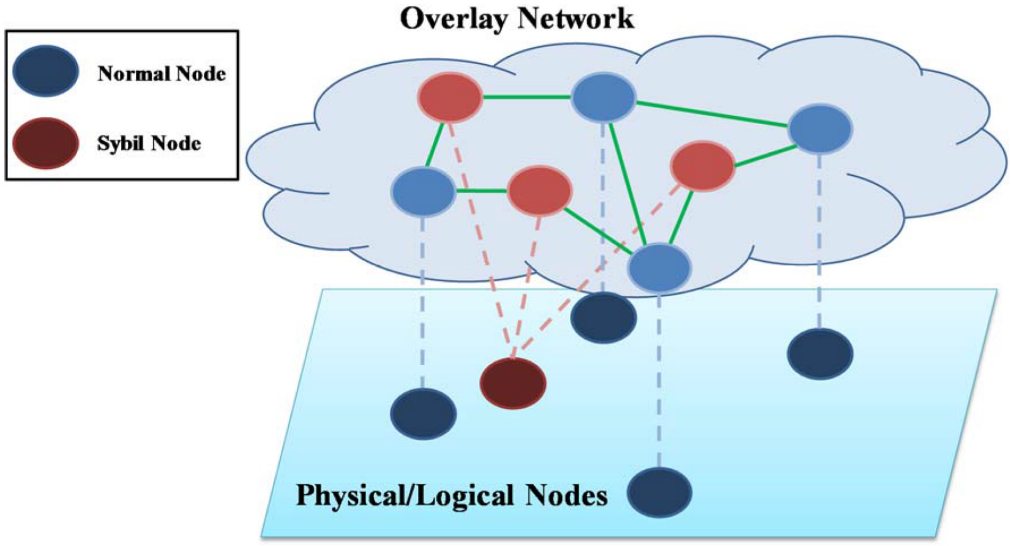
Υποθέτουμε ότι έχουμε το παρακάτω δίκτυο επικοινωνιών, στο οποίο δεν υφίσταται κάποιος CA. Το δίκτυο απαρτίζεται από τις οντότητες υποδομής e, το σύνολο των οποίων συνθέτει το Infrastructure Set *E*. Το σύνολο των επικοινωνιών λαμβάνει χώρα στο cloud, ενώ κάθε οντότητα συνδέεται στο cloud μέσω ενός pipe. Το cloud περιγράφει γενικά οποιαδήποτε δικτυακή τοπολογία υπάρχει, αποτελούμενη από routers, switches και άλλα μέρη, περιλαμβάνοντας φυσικά και τα δίκτυα ανωνύμων επικοινωνιών. [56]



Σχήμα 3.25: Communications Cloud.

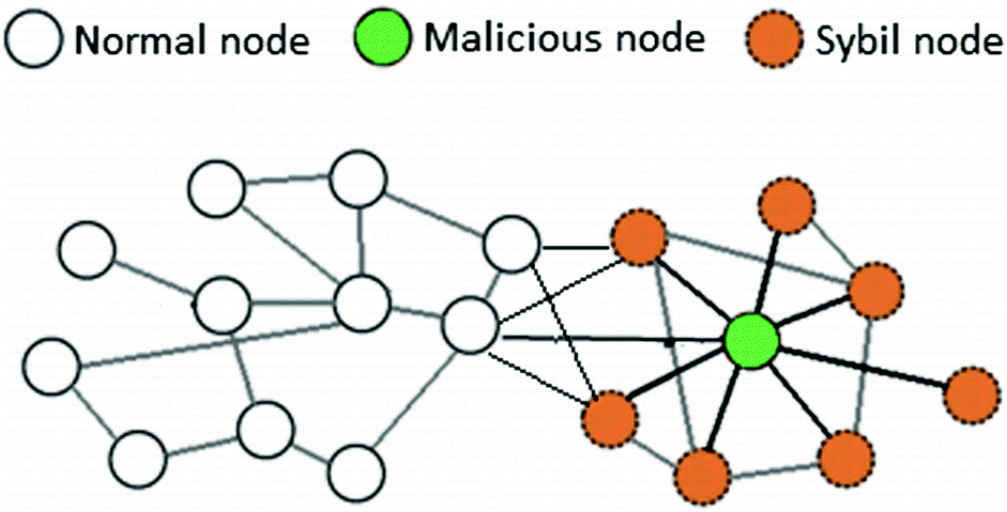
Το Infrastructure Set E μπορεί να διαιρεθεί σε δύο υποσύνολα, το C που περιλαμβάνει όλες τις οντότητες c (correct), αυτές δηλαδή που ακολουθούν όλα τα πρωτόκολλα που χρησιμοποιεί το δίκτυο και το F, το οποίο περιλαμβάνει τις οντότητες f (faulty), οι οποίες μπορούν να προβούν σε συμπεριφορά που αντιβαίνει τους κανόνες που ορίζουν τα πρωτόκολλα του δικτύου. [69] [71] Η επικοινωνία μεταξύ των οντοτήτων γίνεται με τη μορφή μηνυμάτων, τα οποία είναι σειρές bits, πεπερασμένου μήκους. Τα μηνύματα καθορίζονται είτε από τα πρωτόκολλα του δικτύου, είτε μετά

από συμφωνία μεταξύ των ίδιων των οντοτήτων που θέλουν να επικοινωνήσουν. Τα μηνύματα που προωθούνται μέσω των pipes, φτάνουν στο cloud, όπου γίνονται broadcasted σε όλες τις υπόλοιπες οντότητες. Υπάρχει εγγύηση παραλαβής των μηνυμάτων, αλλά όχι και της σειράς και του χρόνου με τα οποία θα φτάσουν αυτά. Ορίζεται ως παράγοντας ασφαλείας n, ο οποίος εκφράζει τον περιορισμό της πολυπλοκότητας εργασιών στο δίκτυο, σε πολυωνυμικό βαθμό, και πρόσβασης σε πόρους. Έτσι, κάθε οντότητα μπορεί να υλοποιήσει εργασίες χαμηλού βαθμού πολυωνυμικής πολυπλοκότητας n στο δίκτυο. Ο περιορισμός αυτός επιτρέπει στις οντότητες να να δημιουργούν εικονικά point-to-point μονοπάτια μεταξύ τους, στα οποία υπάρχει κρυπτογράφηση, με την προϋπόθεση πάντα ότι οι οντότητες που το απαρτίζουν έχουν αναγνωρίσει και εμπιστεύονται η μια την άλλη.



Σχήμα 3.26: Sybil Nodes στο Overlay Network.

Ο όρος identity αφορά τον τρόπο με τον οποίο μια οντότητα γίνεται αναγνωρίσιμη και της επιτρέπεται η επικοινωνία στο δίκτυο. Η identity έχει persistence στο χρόνο και παραμένει η ίδια σε όλα τα συμβάντα επικοινωνίας. Κάθε οντότητα e επιχειρεί να παρουσιάσει μια identity i στις υπόλοιπες. Εφόσον μια οντότητα e παρουσιάσει με επιτυχία την ταυτότητα του i σε μια άλλη οντότητα l (η οποία είναι correct), τότε η l αποδέχεται την identity i. Παράδειγμα ενός identity είναι το secure hash ενός public key. [56] [57] Κάθε correct οντότητα θα επιχειρήσει να παρουσιάσει μια μόνο legitimate identity, ενώ μια faulty οντότητα μπορεί να επιχειρήσει να παρουσιάσει εκτός από την legitimate identity που κατέχει στο δίκτυο, ακόμα μια ή και περισσότερες counterfeit (ψεύτικες) identities. Παρακάτω φαίνεται ο τρόπος με τον οποίο μια faulty οντότητα μπορεί να έχει υιοθετήσει αρκετές ψεύτικες identities, υλοποιώντας μια Sybil Attack. [66] [67] [68] [73]



Σχήμα 3.27: Δίκτυο παρουσία Sybil nodes.

Μια οντότητα μπορεί να έχει τρεις πιθανές πηγές πληροφόρησης σχετικά με τις άλλες οντότητες που ανήκουν στο δίκτυο. Μια έμπιστη πηγή, όπως η CA, τον εαυτό της ή άλλες οντότητες. Από τη στιγμή που δε χρησιμοποιείται κάποια CA, τότε μια οντότητα l αναγκαστικά επιλέγει να αποδεχτεί identities οντοτήτων που θεωρεί ότι μπορεί να εμπιστευτεί με κάποιον τρόπο (direct identity validation) ή identities οντοτήτων τις οποίες έχουν ήδη αποδεχθεί άλλες οντότητες, προς τις οποίες η οντότητα l έχει ήδη εμπιστοσύνη (indirect identity validation). Ακόμα και υπό τους περιορισμούς που θέτει ο παράγοντας ασφαλείας του δικτύου, n, μια faulty οντότητα μπορεί να υιοθετήσει έναν αριθμό identities. [74] Σε μεγάλης κλίμακας δίκτυα μάλιστα, όπου υπάρχουν ανομοιογένειες μεταξύ των οντοτήτων και της πρόσβασης που αυτές έχουν σε πόρους, αποδεικνύεται ότι ένας αρκούντως μεγάλος αριθμός faulty οντοτήτων μπορεί να υιοθετήσει και να χρησιμοποιήσει ένα απεριόριστο πλήθος ψευδών identities. [79]

Στην περίπτωση της direct identity validation, θεωρούμε ότι ο μόνος τρόπος για να επιτευχθεί ο διαχωρισμός δύο οντοτήτων βασίζεται στους πόρους δύο οντοτήτων, οι οποίοι μεταξύ τους μπορεί να διαφέρουν το πολύ από έναν σταθερό παράγοντα. Έτσι, η οντότητα l μπορεί να ζητήσει αποδείξεις σχετικά με τους πόρους μιας άλλης οντότητας, προτού αποδεχθεί την identity του. Θεωρώντας ότι μια faulty οντότητα f έχει λόγο ρ των δικών της πόρων, προς τους πόρους μιας οντότητας ελαχίστων υπολογιστικών δυνατοτήτων, έχει τη δυνατότητα τότε να παρουσιάσει g=|ρ| ξεχωριστές identities στην οντότητα l. Αυτό αποτελεί το άνω όριο των πιθανών identities που μπορεί να παρουσιάσει μια faulty οντότητα. [12]

Αν οι πόροι της επικοινωνίας μεταξύ των entities είναι περιορισμένοι, τότε η οντότητα l μπορεί να υλοποιήσει ένα broadcast στο οποία θα ζητάει identities από άλλες οντότητες και, λόγω ακριβώς των περιορισμών αυτών, να λάβει και να αποδεχθεί απαντήσεις που φτάνουν εντός καθορισμένου χρονικού διαστήματος, από την έναρξη της επικοινωνίας. Αν υπάρχουν περιορισμοί στους πόρους που αφορούν τον αποθηκευτικό χώρο, η οντότητα l μπορεί να απαιτήσει από τις υπόλοιπες προς αξιολόγηση οντότητες να αποθηκεύσουν ένα μεγάλο κομμάτι δεδομένων, επιβεβαιώνοντας αργότερα μέσω σύγκρισης, ότι όλες οι οντότητες, υπό τις identities που διαφήμιζαν τη στιγμή εκείνη, αποθήκευσαν ταυτόχρονα τα δεδομένα, επαληθεύοντας έτσι ότι πρόκειται για γνήσιες identities που ανήκουν σε ξεχωριστές οντότητες. Τέλος, σε περίπτωση περιορισμών σε υπολογιστικούς πόρους, η οντότητα l μπορεί να ζητήσει από τις προς αξιολόγηση οντότητες να λύσουν ένα υπολογιστικό

πρόβλημα, ελέγχοντας το χρόνο επίλυσης ταυτόχρονα από όλες τις identities που αποκρίνονται. [63] [64] [66]

Ακόμα ένα σημείο άξιο προσοχής, στην περίπτωση της direct identity validation, είναι ότι αν η οντότητα l αποδέχεται ως έμπιστες, οντότητες οι οποίες δεν έχουν επικυρωθεί ταυτόχρονα, μια faulty οντότητα f μπορεί να παρουσιάσει ένα μεγάλο πλήθος ψεύτικων identities σε αυτή. Το πρόβλημα αυτό δε μπορεί να αντιμετωπιστεί με τη χρήση επαλήθευσης που βασίζονται σε πόρους με χρονικούς περιορισμούς, όπως η υπολογιστική δύναμη ή το bandwidth, ωστόσο είναι εφικτό να περιοριστούν με τη χρήση μεθόδων που αφορούν την αποθήκευση δεδομένων, όπως έχουμε ήδη δει. Έτσι, σε περίπτωση που η οντότητα l αποδέχεται ως έμπιστες, οντότητες οι οποίες δεν έχουν επικυρωθεί ταυτόχρονα, μπορεί να ελέγχει συνεχώς τις οντότητες που εμπιστεύεται, ζητώντας τους να αποθηκεύουν συνεχώς, κομμάτια δεδομένων και προβαίνοντας σε συνεχείς επαληθεύσεις σε βάθος χρόνου, έχοντας περισσότερες πιθανότητες να εντοπίσει κάποια ψεύτικη identity και να την απορρίψει. Η μέθοδος αυτή ωστόσο περιορίζει σημαντικά τον αποθηκευτικό χώρο και τις ικανότητες εκτέλεσης εργασιών των προς επιβεβαίωση οντοτήτων. [37]

Ο δεύτερος πιο διαδεδομένος τρόπος με τον οποίο μια οντότητα μπορεί να αποδεχθεί identities άλλων οντοτήτων, από τη στιγμή που δεν υπάρχει κάποια κεντρική CA, είναι αυτός της indirect identity validation. Έτσι, αντί να αποδέχεται μια οντότητα l identities που έχει επαληθεύσει μέσω των computational challenges που περιγράφηκαν παραπάνω, μπορεί να δεχθεί ως αληθείς, έμπιστες identities αυτές τις οποίες εμπιστεύεται ήδη ένας ικανός αριθμός έμπιστων, ως προς το l, αριθμός οντοτήτων. [12] [69] Έτσι, αν μια οντότητα με identity i1 εμπιστεύεται και έχει αποδεχθεί την identity i2 μιας άλλης οντότητας, τότε θεωρείται ότι η i1 εγγυάται για την αξιοπιστία της i2. Ο προφανής κίνδυνος που προκύπτει εδώ είναι ότι, δεδομένου ενός ικανού αριθμού faulty entities, οι faulty identities μπορούν να αποκτήσουν σημαντική επιρροή στο σύστημα αξιοπιστίας και είτε να εγκρίνουν άλλες faulty identities, είτε να απορρίπτουν legitimate identities.

Σε περίπτωση λοιπόν που μια οντότητα l de facto αποδέχεται ως αξιόπιστη μια identity για την οποία εγγυώνται τουλάχιστον q άλλες οντότητες, τις οποίες ήδη η l εμπιστεύεται, τότε ένα σετ F που απαρτίζεται εξ ολοκλήρου από faulty οντότητες μπορεί να παρουσιάσει έναν τυχαία μεγάλο αριθμό διακριτών identities στην οντότητα l, αν ισχύει ότι $|F| \geq q$ ή αν οι αθροιστικές υπολογιστικές δυνατότητες του σετ F είναι ισάξιες ή ισχυρότερες από q+|F| οντότητες ελαχίστων δυνατοτήτων. [49] [50] Επιπροσθέτως, αν οι legitimate οντότητες του σετ C δεν συντονίζονται μεταξύ τους ώστε να αποδέχονται νέες identities ταυτόχρονα και σε σαφώς καθορισμένα για όλους χρονικά διαστήματα, τότε ακόμα και μια faulty οντότητα ελαχίστων υπολογιστικών δυνατοτήτων μπορεί να παρουσιάσει $g = ||C|/q|$ διακριτές identities στην οντότητα l. [61] Καθίσταται λοιπόν επιτακτικό τα challenges για την αποδοχή νέων identities να γίνονται ταυτόχρονα από όλες τις οντότητες του δικτύου, ώστε να ανιχνεύονται οι faulty. Αυτό φυσικά έχει διάφορους περιορισμούς. Όπως είδαμε για παράδειγμα στα challenges που αφορούν τη χωρητικότητα, μπορούν να δημιουργηθούν ζητήματα έλλειψεις πόρων σε μια οντότητα, ακόμα κι αν τα challenges προέρχονται από μια μόνο οντότητα. Σε περίπτωση που μια οντότητα κληθεί να αντιμετωπίσει πολλά τέτοια challenges από διαφορετικές οντότητες ταυτόχρονα, δε θα καταφέρει να ανταποκριθεί, ακόμα κι αν είναι legitimate. Όσον αφορά τα υπολογιστικά challenges, αυτά μπορούν συνήθως να λυθούν συνδυαστικά, αν προέρχονται από διαφορετικές οντότητες. [64]

Όλες οι παραπάνω παρατηρήσεις μας δίνουν το περίγραμμα μιας Sybil Attack. Θα πρέπει να τονιστεί ότι δεδομένων συγκεκριμένων συνθηκών, και κυριότερα ελλείψει κεντρικής CA, μια faulty οντότητα

μπορεί να αυξήσει σημαντικά την επιρροή της στο δίκτυο, παρουσιάζοντας πολλές ψεύτικες identities. Ένα δίκτυο, δεδομένου ότι έχει τη δυνατότητα να λειτουργεί με την παρουσία ενός μέρους φ, ως προς το σύνολο, ψεύτικων identities, μπορεί να συνεχίσει να λειτουργεί μόνο υπό την προϋπόθεση ότι το πολύ φ/g οντότητες εντός του είναι faulty.

Τέλος, αξίζει να παρατεθούν ορισμένα χαρακτηριστικά παραδείγματα Sybil nodes που έχουν εντοπιστεί έως σήμερα και να αναλυθεί σύντομα ο τρόπος λειτουργίας τους.

1. Re-write Sybils: Οι συγκεκριμένοι Sybil relays έχουν στόχο να υποκλέψουν συναλλαγές Bitcoin που λαμβάνουν χώρα στο Tor. Αυτό επιτυγχάνεται μέσω της αλλαγής των Bitcoin διευθύνσεων, χρησιμοποιώντας relayed HTML. Οι Sybil relays έχουν όλοι το Exit flag και ουσιαστικά αλλάζουν το onion domain που βρίσκεται στο HTTP Response του Web Server προκειμένου να ανακατευθύνουν τη δικτυακή κίνηση σε κάποιο κακόβουλο ιστότοπο που ελέγχεται από τον επιτιθέμενο. Για να καταστεί επιτυχής η επίθεση, πρέπει τα ψεύτικα domains έχουν ίδιο ένα μέρος του προθέματος με το κανονικό site, καθώς με αυτό τον τρόπο είναι δυνατό να δημιουργηθεί ένα Base32-encoded SHA-1 hash του δημοσίου κλειδιού του ψεύτικου domain το οποίο να είναι σχεδόν ίδιο με αυτό του κανονικού site, κάτι το οποίο επιτρέπει την ανακατεύθυνση της κίνησης στο κακόβουλο site. Η διαδικασία αυτή είναι εξαιρετικά απλή καθώς μια χαμηλών δυνατοτήτων κάρτα γραφικών έχει τη δυνατότητα να υλοποιήσει τη διαδικασία δημιουργίας onion domains σε μόλις λίγα λεπτά. Οι ανακατευθύνσεις αυτές επιτρέπουν στους επιτιθέμενους να υποκλέψουν στοιχεία των συνδέσεων που αφορούν σε συναλλαγές Bitcoins και λοιπών κρυπτονομισμάτων, αλλάζοντας το αποτέλεσμα τους.
2. Redirect Sybils: Τα Redirect Sybils δεν έχουν μεγάλη διαφορά με τα Re-write, καθώς διαφοροποιούνται κυρίως στο σκοπό τον οποίο εξυπηρετούν, χρησιμοποιώντας τις ίδιες τεχνικές. Αποτελούν Exit relays τα οποία κάνουν redirect τα Respones/Requests των χρηστών σε impersonating websites, προκειμένου να κλέψουν login credentials από τους χρήστες του Tor. Χρησιμοποιούνται πολλές φορές σε συνδυασμό με τους Re-write relays, προκειμένου να υποκλέψουν login credentials από websites που χρησιμοποιούνται για συναλλαγές κρυπτονομισμάτων. Από Redirect Sybils που έχουν εντοπιστεί, παρατηρείται ότι η συνήθης τακτική που χρησιμοποιείται είναι η σταδιακή εισαγωγή τους στο Tor με σκοπό να αυξηθεί το μέγεθος του Sybil group σε βάθος χρόνου, χωρίς όμως να παρουσιάζουν τα μέλη του ικανοποιητικό αριθμό κοινών χαρακτηριστικών, που θα διευκόλυνε τον εντοπισμό τους από ευριστικά εργαλεία.
3. FDCservers Sybils: Χρησιμοποιούνται για το deanonymization των χρηστών onion services στο Tor και είναι από τους πιο συχνά χρησιμοποιούμενους Sybil relays. Οι relays αυτοί μπορούν να χρησιμοποιηθούν σαν guard relays και σαν onion service directories με αποτέλεσμα να ελέγχει ο επιτιθέμενος και τα δύο άκρα του δικτύου και να μπορεί να παρατηρεί πλήρως τη δικτυακή κίνηση ορισμένων χρηστών. Έτσι, μπορεί να εξάγει συμπεράσματα για τα είδη των onion services που χρησιμοποιεί ένας χρήστης. Σε προγενέστερες επιθέσεις έχουν παρατηρηθεί έως και 121 FDCservers Sybils στο Tor.
4. Default Sybils: Ο όρος default προέρχεται από το κοινό nickname των Sybil κόμβων, που είναι “default”. Πρόκειται για relays που τρέχουν σε Windows machines, με onion routing port το 443 και directory port το 9030. Οι Sybil relays αυτοί παρουσιάζουν συχνές μεταβολές στο status τους, δηλαδή εισέρχονται και εξέρχονται συχνά στο Tor, ενώ παρουσιάζουν και μικρό uptime, που υποδηλώνει ότι πρόκειται για κόμβους οι οποίοι είναι συνήθως

προσωπικοί υπολογιστές οι οποίοι έχουν μολυνθεί με malware εν αγνοία των χρηστών τους και λειτουργούν ως μέρος ενός botnet στο Tor.

5. Trotsky Sybils: Ομοίως με τους Default Sybils, οι Trotsky relays αποτελούν μέρη ενός botnet και εντοπίζονται κυρίως στην Ανατολική Ευρώπη. Αποτελούν κυρίως Exit relays και οι περισσότεροι πλέον έχουν ταυτοποιηθεί ως Sybil nodes και έχουν αποκλειστεί από το Tor.
6. Amazon EC2 Sybils: Οι relays αυτοί χρησιμοποιούν τυχαία παραγόμενα nicknames μήκους 16-17 γραμμάτων, GNU/Linux και έχουν IP Addresses που αντλούνται από το EC2 δίκτυο της Amazon (εξού και το όνομα τους). Σε 88 IP Addresses που έχουν παρατηρηθεί, έχει βρεθεί ένα μοτίβο ενεργειών σύμφωνα με το οποίο κάθε relay άλλαζε τακτικά το fingerprint του, υλοποιώντας ελάχιστες, συγκεκριμένες μεταβολές. Μετά από 24 ώρες λάμβαναν το HSDir flag ενώ μετά από 48 ώρες είχαν καταστεί ανενεργοί. Πρόκειται για κόμβους που στόχο έχουν το exploitation του DHT του Tor.
7. Anonpoke Sybils: Relays που είχαν όλοι το όνομα Anonpoke και είχαν στόχο να λειτουργήσουν ως onion service directories, καθώς ήταν middle relays και διαφημιζόταν στο Tor ως directory mirrors. Μοιραζόταν όλοι το nickname Anonpoke και βρισκόταν σε έναν VPS provider του U.S Rackspace. Εντοπίστηκαν εγκαίρως και αποσύρθηκαν από το Tor.
8. Planetlab Sybils: Χρησιμοποιούσαν παραλλαγές των planet και labs ως nicknames, όπως pl, planet, plab κλπ. Είχαν σκοπό να χρησιμοποιηθούν ως Exit relays αλλά αφαιρέθηκαν από το Tor μετά από τρεις μέρες, χωρίς να καταφέρουν να υλοποιήσουν την επίθεση.
9. LizardNSA Sybils: Περιλάμβαναν τόσο Middle όσο και Exit relays με στόχο να πάρουν την HSDir flag και να λειτουργήσουν ως onion services directories. Τα μηχανήματα φιλοξενούνταν στο Google Cloud, αποτελούσαν σημαντικό αριθμό του συνόλου των Tor relays συγκριτικά με το σύνολο τους και κατάφεραν να παραμείνουν μόνο δέκα ώρες στο Tor.
10. FuzIVZTOR Sybils: Χρησιμοποιήθηκαν ως Middle relays, ανήκαν στο δίκτυο 212.38.181.0/24 και απερρίφθησαν σχεδόν πέντε ώρες μετά την είσοδο τους στο Tor. [103]

Sybil Attacks Case Studies

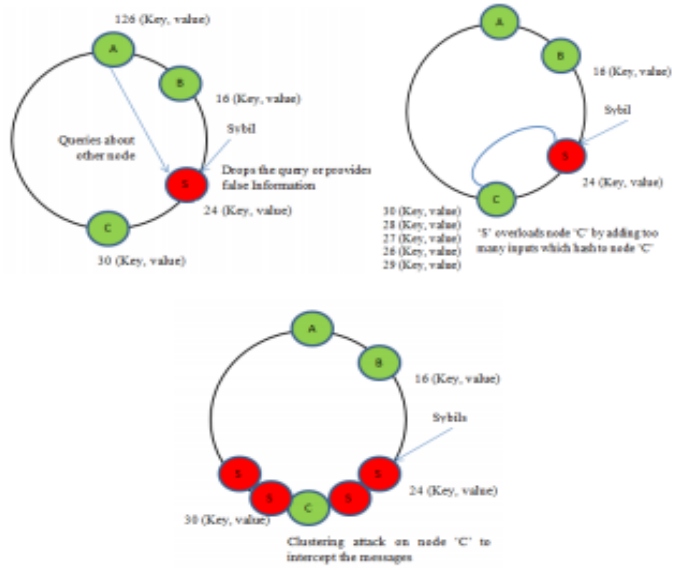
1. Sybil Attacks στο Tor Network

Όπως αναφέραμε, οι Sybil Attacks περιγράφουν μια ευρεία γκάμα κακόβουλων ενεργειών που σκοπό έχουν να ενισχύσουν τη θέση του επιτιθέμενου σε ένα δίκτυο συμμετεχόντων (peers) ώστε αυτός να έχει τη δυνατότητα να το επηρεάζει, σύμφωνα πάντα με το consensus weight που έχει καταφέρει να αποκτήσει. Το Tor Network είναι ιδιαίτερα επιρρεπές και ευάλωτο σε τέτοιου είδους επιθέσεις, καθώς δεν υφίσταται κάποια κεντρική αρχή CA. [48] Οι Sybil Attacks, αν και ενεργητικού τύπου επιθέσεις, δεν αρκούν μόνες τους πάντα για να επιτευχθεί ο στόχος του κακόβουλου χρήστη. Πολλές φορές είναι απλά ένα μέσο ώστε ο επιτιθέμενος να φτάσει πιο εύκολα στο στόχο του. Φυσικά, είναι δυνατό, όπως είδαμε, με τη χρήση πολλαπλών identities να καταφέρει ακόμα και DoS επιθέσεις, αποκτώντας μεγάλη επιρροή στο σύστημα αξιοπιστίας και ανάθεσης identities του δικτύου, με αποτέλεσμα να μπορεί να αρνείται identities σε νέες, legitimate οντότητες. [37] Παρ ολ αυτά, οι Sybil Attacks μπορούν να επηρεάσουν με πιο ήπιο τρόπο τα δίκτυα ανωνύμων επικοινωνιών, υπονομεύοντας έτσι την αξιοπιστια τους και κυρίως την ταυτότητα των χρηστών τους. Ανάλογα με το consensus weight που κατέχει ο επιτιθέμενος, μπορεί να υλοποιήσει ευκολότερα τις ακόλουθες επιθέσεις:

- Exit traffic tampering: όπως είδαμε και στην ανάλυση των δικτύων ανωνύμων επικοινωνιών, κατά την έξοδο της δικτυακής κίνησης από το Tor Network διέρχεται μέσω των κόμβων εξόδου. Ο επιτιθέμενος, ελέγχοντας τους κόμβους αυτούς μπορεί να υλοποιήσει παρακολούθηση των πακέτων, να συλλέξει πληροφορίες και συνθηματικά από μη

κρυπτογραφημένες συνδέσεις ή ακόμα και να εισάγει κακόβουλο περιεχόμενο στη σύνδεση. [37]

- Website fingerprinting: στο Tor Network, όλοι οι κόμβοι που ανήκουν στο σχηματισθέν μονοπάτι γνωρίζουν μόνο τον κόμβο προέλευσης του μηνύματος καθώς και το επόμενο άλμα (hop), δηλαδή τον κόμβο στον οποίο θα προωθήσουν το μήνυμα. [61] Ο πρώτος κόμβος στο μονοπάτι, που λαμβάνει το μήνυμα απευθείας από την πηγή ονομαζεται guard relay και χαρακτηρίζεται από ισχυρή κρυπτογράφηση προκειμένου να προστατεύεται η ταυτότητα και η δραστηριότητα της πηγής. [53] [54] Ο επιτιθέμενος μπορεί να μην έχει τη δυνατότητα να αποκρυπτογραφήσει το μήνυμα, ωστόσο μπορεί να υλοποιήσει ανάλυση της δικτυακής κίνησης, βασιζόμενος στο μέγεθος των πακέτων και το χρόνο διέλευσης τους, προκειμένου να εξάγει συμπεράσματα σχετικά με το είδος των ιστότοπων που επισκέπτεται ο στόχος.
- Bridge address harvesting: χρήστες του διαδικτύου που υπόκεινται σε περιορισμούς πρόσβασης σε περιεχόμενο λόγω λογοκρισίας, συχνά χρησιμοποιούν private Tor relays τα οποία καλούνται bridges. Το Tor εφαρμόζει περιορισμούς στη διανομή bridges προκειμένου να μην είναι σε θέση αυτοί που επιβάλλουν τη λογοκρισία (κρατικοί μηχανισμοί, πανεπιστήμια, εργοδότες) να ανακτήσουν όλες τις bridge addresses. [50] Παρόλα αυτά, ο επιτιθέμενος μπορεί να χρησιμοποιήσει ένα middle relay και να παρατηρήσει την κίνηση που δεν προέρχεται από ήδη γνωστούς guard relays, αποκαλύπτοντας έτσι τις κρυφές bridge addresses.
- End-to-end correlation: αν ο επιτιθέμενος καταφέρει να αποκτήσει πρόσβαση στο guard και exit relay ταυτόχρονα, μπορεί να υλοποιήσει Timing Attacks και να αποκαλύψει πλήρως τη δικτυακή κίνηση του στόχου.
- Onion services manipulation: με τη χρήση ορισμένου αριθμού Sybils, ο επιτιθέμενος έχει τη δυνατότητα να θέσει offline έναν TCP onion server.



Σχήμα 3.28: Sybil Attack στο Tor.

Η ρύθμιση ενός relay ώστε αυτό να δρομολογεί περισσότερη κίνηση, μπορεί να αυξήσει το consensus weight του επιτιθέμενου, διευκολύνοντας τον να υλοποιήσει κάποιες από τις παραπάνω επιθέσεις. Παρόλα αυτά, υπάρχουν εν γένει περιορισμοί όσον αφορά τη δικτυακή κίνηση που μπορεί ένα relay να διαχειριστεί, περιορισμοί που επιβάλλονται τόσο από το bandwidth των links, όσο και από τους υπολογιστικούς του πόρους, λόγω των υψηλών απαιτήσεων σε πόρους για τις λειτουργίες κρυπτογράφησης/αποκρυπτογράφησης των μηνυμάτων. [49] Εν τέλει, ο επιτιθέμενος, προκειμένου

να αυξήσει το consensus weight του σε ικανοποιητικά επίπεδα, θα αναγκαστεί να εισάγει περισσότερα relays στο δίκτυο, τα οποία αποκαλούνται Sybils.

Το Tor Network ήδη χρησιμοποιεί ορισμένους τρόπους άμυνας από Sybil Attacks. Αρχικά, οι direcTory authorities αποδέχονται το πολύ δύο relays ανά IP Address προκειμένου να αποτρέψουν Sybil Attacks που χρειάζονται λίγους πόρους. Ο αλγόριθμος επιλογής μονοπατιού αποτρέπει τους Tor clients από το να επιλέξουν δύο relays στο ίδιο /16 δίκτυο. Επιπλέον, οι direcTory authorities χρησιμοποιούν flags (σημαίες) για να χαρακτηρίζουν τα relays. Οι flags αυτές σχετίζονται με το status και το QoS (Quality of Service) που παρέχουν οι relays και είναι οι εξής:

- Valid: λειτουργικό relay
- HSDir: το relay αποτελεί onion service direcTory. Αποκτά το flag αυτό αφού παρέλθουν κατ ελάχιστο 7 μέρες μετά την είσοδο του (όριο ασφαλείας).
- Exit: το relay αποτελεί exit relay
- BadExit: το exit relay είναι misconfigured ή πιθανώς κακόβουλο και δεν πρέπει να χρησιμοποιείται από τους Tor clients.
- Stable: σταθερό relay, αποκτά το flag αυτό αφού παρέλθουν κατ ελάχιστο 7 μέρες μετά την είσοδο του (όριο ασφαλείας).
- Guard: το πρώτο hop των Tor clients.
- Running: relay στον οποίο οι direcTory authorities συνδέθηκαν εντός των τελευταίων 45 λεπτών, επιβεβαιώνοντας ότι είναι εν λειτουργία. [8] [53] [55] [57]

Τα όρια ασφαλείας για τα HSDir και Stable flags αποτελούν μια δικλείδα ασφαλείας για το Tor Network, καθώς οι direcTory authorities έχουν στη διάθεση τους περισσότερο χρόνο για να ανιχνεύσουν και να απορρίψουν Sybil relays, προτού αυτά γίνουν ομότιμα και ισάξια μέρη του δικτύου. Τα relays στο Tor είναι αναγνωρίσιμα με μοναδικό τρόπο μέσω του fingerprint (αποτυπώματος) τους, το οποίο αποτελείται από το Base32-encoded SHA-1 hash του δημοσίου κλειδιού του. [96] Επιπροσθέτως, ο διαχειριστής του κάθε relay μπορεί να του αναθέσει ένα nickname ώστε να είναι ευκολότερο στην απομνημόνευση του. Φυσικά, τα nicknames δεν είναι μοναδικά στο δίκτυο.

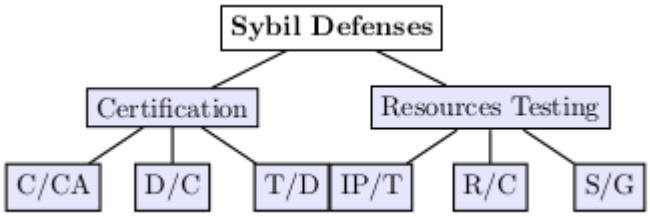
Οι κόμβοι εξόδου διαθέτουν μια exit policy (πολιτική εξόδου), η οποία καθορίζει τις IP Addresses και τα ports με τα οποία καθίσταται δυνατή η σύνδεση του και η μεταφορά δεδομένων. Σε περίπτωση που ένας χρήστης έχει και διαχειρίζεται πάνω από έναν relay στο δίκτυο, τότε η βέλτιστη πρακτική είναι να τους συνενώσει σε ένα relay family, έτσι ώστε οι χρήστες να μη χρησιμοποιούν πάνω από ένα relay σε κάθε family, προκειμένου να αποφύγουν Correlation Attacks. [100] Ενδιαφέρον προκύπτει από το γεγονός ότι αν κάποιος χρήστης με πάνω από ένα relays στο δίκτυο δεν τα οργανώσει σε κάποιο relay family, τότε αυτά θεωρούνται benign Sybil relays. Παρ όλα αυτά, οι benign Sybil relays δεν αποτελούν πρόβλημα ασφαλείας στο δίκτυο.

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Sybil Attacks

Οι Sybil Attacks αποτελούν σημαντικό κίνδυνο για τα δίκτυα ανωνύμων επικοινωνιών καθώς μπορούν να υπονομεύσουν σημαντικά την ασφάλεια ενός δικτύου, είτε πρόκειται για κοινωνικό δίκτυο είτε για δίκτυο ανωνύμων επικοινωνιών. [37] Μέχρι στιγμής, δεν υπάρχει κάποιος καθολικός τρόπος προστασίας των δικτύων από τέτοιου είδους επιθέσεις, καθώς κάθε επίθεση διαφοροποιείται σημαντικά από τις υπόλοιπες και εξατομικεύεται στα πρωτόκολλα του δικτύου που θέλει να πλήξει.

Στόχος των μέτρων προστασίας είναι να εντοπίσουν έγκαιρα τυχόν Sybil nodes στο δίκτυο και να τους απομονώσουν εισάγοντας το ελάχιστο δυνατό overhead στο δίκτυο, ώστε να διατηρείται η λειτουργικότητα του και το UX. Δεν υπάρχει τρόπος να εξαλειφθούν πλήρως οι Sybil Attacks, ούτε φυσικά και να θωρακιστεί σε απόλυτο βαθμό ένα δίκτυο από αυτές. [49] [50] Ακόμα και σε αυστηρές μεθόδους προστασίας, υπάρχουν περιπτώσεις false positives, όπου legitimate κόμβοι θα απορριφθούν ως πιθανώς κακόβουλοι, διαταράσσοντας τη λειτουργία του συστήματος, καθώς και περιπτώσεις false negatives, όπου Sybil nodes δεν αναγνωρίζονται ως κακόβουλοι, με αποτέλεσμα να συνεχίζεται η παρουσία τους στο δίκτυο, υπονομεύοντας την ασφάλεια του.

Οι μέθοδοι προστασίας από Sybil Attacks παρουσιάζονται συνοπτικά στο παρακάτω διάγραμμα.



Σχήμα 3.29: Sybil Attack Defenses.

Η πιστοποίηση των χρηστών ενός δικτύου αποτελεί τον πλέον δοκιμασμένο τρόπο προστασίας από Sybil Attacks, καθώς μπορεί να αποτρέψει μη αξιόπιστους χρήστες από το να εισέλθουν στο δίκτυο και να δημιουργούν νέες identities. [53] Βασίζεται στην ύπαρξη μιας αξιόπιστης Certifying Authority (CA) η οποία αναλαμβάνει να διασφαλίσει την ένα προς ένα αντιστοιχία μιας οντότητας με μια identity στο δίκτυο. Έτσι επιλύεται το ζήτημα ανάγκης εγκατάστασης εμπιστοσύνης μεταξύ των συμμετεχόντων του δικτύου, το οποίο μετατίθεται ολοκληρωτικά στη CA. [12] [55] Είναι ίσως η μοναδική μέθοδος που μπορεί να εξασφαλίσει πλήρως ένα δίκτυο έναντι των συγκεκριμένων επιθέσεων, ωστόσο μπορεί να εισάγει σημαντικό performance overhead στο δίκτυο, ειδικά σε μεγάλης κλίμακας δίκτυα. Στην περίπτωση των ανωνύμων δικτύων επικοινωνιών, η χρήση μιας CA είναι αδύνβατη καθώς η ύπαρξη της αντιβαίνει τόσο στη λογική χρήσης τους, όσο και θέτει πρακτικά προβλήματα για την προστασία της ταυτότητας των χρηστών τους.

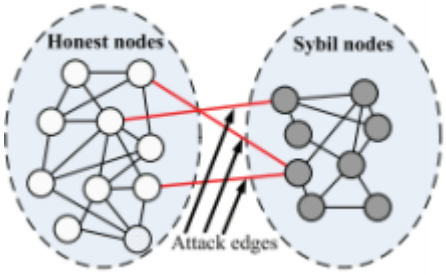
Η μέθοδος του Resources Testing είναι η μόνη βιώσιμη λύση για τα δίκτυα που μελετά η παρούσα εργασία. [94] Βασίζεται στο γεγονός ότι η πρόσβαση σε πόρους που έχει η κάθε οντότητα στο δίκτυο είναι περιορισμένη και ως εκ τούτου, μπορούν να χρησιμοποιηθούν διάφορα computational challenges στα identities που εμφανίζονται στο δίκτυο, προκειμένου να επαληθευτεί αν πρόκειται για μεμονωμένες οντότητες ή Sybils. Τα αρχικά challenges βασιζόταν σε υπολογιστικούς, αποθηκευτικούς ή δικτυακούς πόρους, οι οποίοι ωστόσο πλέον κρίνονται ανεπαρκείς, καθώς υπάρχουν επιτιθέμενοι με σημαντικές υπολογιστικές δυνατότητες που μπορούν να εισάγουν πολλαπλές identities στο δίκτυο. [97] [98] [99]

Η μέθοδος των Recurring Costs είναι μια υποκατηγορία των Resources Testing, εισάγοντας resource tests σε τακτά χρονικά διαστήματα με σκοπό να εισάγει σημαντικό computational overhead σε μόνιμη βάση, σε τυχόν επιτιθέμενους που προσπαθούν να εισάγουν και να ελέγξουν πολλαπλές identities στο δίκτυο. Μια ακόμη ενδιαφέρουσα παραλλαγή των Recurring Costs είναι αυτη που υλοποιείται με Turing Tests, χαρακτηριστικό εκ των οποίων είναι τα CAPTCHA. [100] Η μέθοδος των Recurring Costs παρουσιάζει αδυναμίες, ειδικά όταν ο επιτιθέμενος επιστρατεύσει κάποιο botnet για την επίθεση του, ενώ ακόμα και τα CAPTCHAs μπορούν να αντιμετωπιστούν είτε ανακατευθύνοντας τα

προβλήματα σε πραγματικούς χρήστες, είτε χρησιμοποιώντας τεχνικές και μεθόδους επεξεργασίας εικόνας.

Το IP Testing επιστρατεύει την ανάλυση της τοποθεσίας των χρηστών ενός δικτύου, μέσω της συσχέτισης τους με τις IP Addresses, προκειμένου να ανιχνευθούν πολλαπλές ταυτότητες που βασίζονται σε μια μόνο οντότητα. Σημαντικός φόρτος εργασιών που εντοπίζεται σε μια συγκεκριμένη γεωγραφική περιοχή μπορεί να υποδηλώνει την ύπαρξη ορισμένων Sybil identities. Χαρακτηριστικό παράδειγμα τεχνολογίας ανωνύμων επικοινωνιών που χρησιμοποιούν εξ αρχής τη μέθοδο αυτή είναι το Tarzan, το οποίο περιορίζει την ύπαρξη Sybil identities ελέγχοντας ενδελεχώς τις IP Addresses των συμμετεχόντων αντιπαραβάλλοντάς τες με το γεωγραφικό στίγμα τους. Η μέθοδος αυτή είναι αξιόπιστη, ωστόσο η ύπαρξη botnets μπορεί να δώσει τη δυνατότητα στον επιτιθέμενο να ελέγξει πολλαπλούς υπολογιστές και να εισάγει πάρα πολλές ταυτότητες στο δίκτυο, κάτι το οποίο καθιστά τη μέθοδο IP Testing ανεπαρκή. [95]

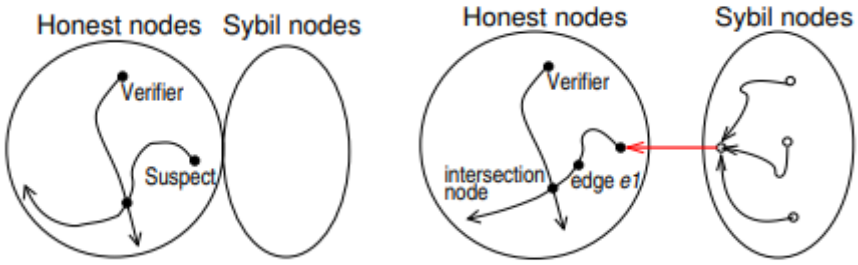
Πέραν των παραπάνω λύσεων αξίζει να μελετηθούν και οι μέθοδοι που βασίζονται στα Social Networks. Αποτελούν αποκεντρωμένες μεθόδους που δουλεύουν πάρα πολύ καλά σε μεγάλου μεγέθους, κατανεμημένα δίκτυα, ενώ η απουσία κάποιας κεντρικής CA διασφαλίζει ότι είναι συμβατές με τις τεχνολογίες ανωνύμων επικοινωνιών. Αποτελούν εύκολα υλοποιήσιμες λύσεις με χαμηλό κόστος όσον αφορά τις επιδόσεις του δικτύου και μπορούν να αξιοποιηθούν ως components σε πολλές τεχνολογίες χωρίς να εισάγουν σημαντική πολυπλοκότητα. [94] Τα παραπάνω πρωτόκολλα βασίζονται στην P2P δομή των κοινωνικών δικτύων, όπου όλοι οι κόμβοι μαζί συνθέτουν το social graph και κάθε φορά που δύο κόμβοι επικοινωνούν μεταξύ τους, σχηματίζεται ένα edge.



Σχήμα 3.30: Sybil Attack Edges.

Μια λύση αποτελεί το SybilGuard. Στο συγκεκριμένο εργαλείο, υπάρχουν δύο φάσεις, αυτή της αρχικοποίησης και αυτή του online εντοπισμού Sybil nodes. Σε πρώτη φάση, οι συμμετέχοντες κόμβοι σχηματίζουν με τυχαίο τρόπο routing tables τόσο για την εισερχόμενη όσο και για την εξερχόμενη κίνηση. Στη συνέχεια κάθε κόμβος σχηματίζει ένα walk μήκους $w = O(\sqrt{n} \log n)$ το οποίο ανακοινώνει στους γειτονικούς κόμβους βάσει του ήδη σχηματισθέντος routing table. Κάθε κόμβος πορ βρίσκεται στο εν λόγω walk καταχωρεί το δημόσιο κλειδί του δημιουργού του walk και στην ουσία λειτουργεί ως “μάρτυρας” και “εγγυητής” για τη συμπεριφορά του. Κάθε walk originator έχει με αυτό τον τρόπο μια λίστα από ”μαρτυρες”. [51] Κατά την online φάση εντοπισμού, τα μονοπάτια που έχουν σχηματιστεί, που αποκαλούνται verifiers, βοηθούν κάθε κόμβο να καταλάβει αν τα αιτήματα για διαμετακόμιση της δικτυακής κίνησης προέρχονται από αξιόπιστες πηγές. Έτσι, ο κάθε verifier ελέγχει τη λίστα των witnesses του ύποπτου κόμβου με τη δική του λίστα και αν υπάρχει διασταύρωση (intersection) μεταξύ των δύο, τότε ο ύποπτος κόμβος θεωρείται ασφαλής. Σε διαφορετική περίπτωση, ο κόμβος θεωρείται Sybil node και η κίνηση απορρίπτεται. [103] Η επιτυχία του SybilGuard βασίζεται στο γεγονός ότι οι Attack Edges είναι περιορισμένες, καθώς οι Sybil nodes δεν έχουν εγκαταστήσει αρκετές συνδέσεις με Honest nodes στο δίκτυο. Έτσι, walks που προέρχονται

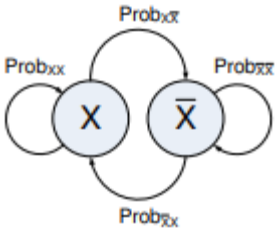
από Sybil nodes δε θα καταφέρουν να έχουν αρκετά intersections με verifiers και σύντομα θα ταυτοποιηθούν ως κακόβουλοι κόμβοι. [56] Στις παρακάτω εικόνες φαίνεται παραστατικά τι συμβαίνει στην περίπτωση που κάποιος ύποπτος κόμβος επιχειρήσει σύνδεση και πώς γίνεται ο εντοπισμός του και η ταυτοποίηση του ως Honest node (πρώτη εικόνα) ή ως Sybil node (δεύτερη εικόνα).



Σχήμα 3.31: Παράδειγμα Sybil Attack Edges.

Το SybilLimit αποτελεί εργαλείο παρεμφερές με το SybilGuard, αλλά βασίζεται στην ύπαρξη πολλών μικρότερων σε μήκος walks, ενώ η καταχώρηση των δημοσίων κλειδιών των walks originators γίνεται στα edges που δημιουργούνται στο δίκτυο. [52] Το μήκος των σχηματισθέντων walks είναι w = O(log n). Με τον ίδιο τρόπο όπως και παραπάνω, σχηματίζονται οι verifiers του δικτύου και στη φάση της online φάσης εντοπισμού γίνονται έλεγχοι για τους originators της κίνησης, όταν πρόκειται για ύποπτους κόμβους, προκειμένου να ελεγχθεί αν υπάρχουν intersections στα εξεταζόμενα walks. Αξίζει να τονιστεί ότι τόσο στο SybilGuard όσο και στο SybilLimit πρέπει να δοθεί η δέουσα προσοχή στην επιλογή του παράγοντα w, καθώς υποτίμηση ή υπερτίμηση του μπορεί να δημιουργήσει προβλήματα. [51] Τα παραπάνω πρωτόκολλα μπορούν να λειτουργήσουν σε πλήρως αποκεντροποιημένα δίκτυα, ωστόσο μπορούν να ανιχνεύουν μόνο έναν Sybil node σε κάθε στιγμή.

Το SybilInfer αποτελεί ένα πιθανοτικό μοντέλο εντοπισμού Sybil nodes, που ελέγχει κατά πόσο ένα γκρουπ κόμβων που σχηματίζει μονοπάτια (traces) είναι αξιόπιστο. Κάθε ένας από τους n κόμβους υλοποιεί s traces στο δίκτυο. [50] [103] Το πρωτόκολλο καθορίζει το αν ένας κόμβος είναι Sybil ή όχι υπολογίζοντας τη δεσμευμένη πιθανότητα, με το Θεώρημα του Bayes, να είναι κάποιος κόμβος αξιόπιστος, δεδομένων των traces που έχει σχηματίσει, δηλαδή την P (X = Honest|T).



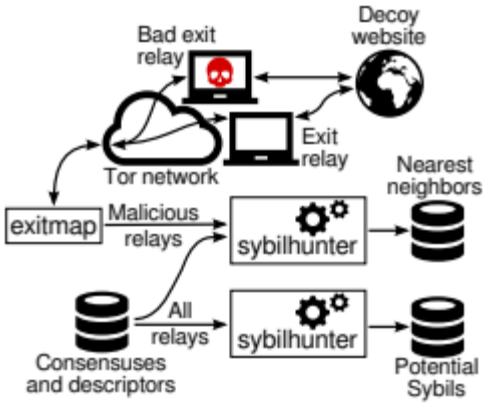
Σχήμα 3.32: Πιθανοτικό μοντέλο στις Sybil Attacks.

Το SybilDefender βασίζεται στην community detection approach για τον εντοπισμό των Sybil nodes. Είναι από τους πιο ευρέως διαδεδομένους τρόπους εντοπισμού τέτοιων επιθέσεων, καθώς δεν περιορίζεται στον εντοπισμό μόνο ορισμένων μεμονωμένων Sybil nodes αλλά από τη στιγμή που εντοπίσει κάποιο, ερευνά το community γύρω από αυτόν, θεωρόντας ότι οι κόμβοι γύρω από αυτόν είναι πολύ πιθανό να είναι επίσης Sybil nodes. [74] Για την εύρεση ενός Sybil node το πρωτόκολλο ξεκινά από έναν Honest node και βρίσκει τους k-hop εγγύτερους γείτονες που θεωρούνται αξιόπιστοι, οι οποίοι οριοθετούν και την περιοχή ασφαλείας, που δεν περιλαμβάνει δηλαδή κάποιον ύποπτο

κόμβο. Στη συνέχεια, κάθε ένας από αυτούς τους κόμβους σχηματίζει τυχαία μονοπάτια μεταβλητού μήκους και καταγράφεται η συχνότητα παρουσίας κάθε κόμβου σε αυτά. Σε περίπτωση που η συχνότητα εμφάνισης ενός κόμβου στα σηματισθέντα μονοπάτια είναι μικρή, σημαίνει ότι ο κόμβος αυτός είναι Sybil node και κατά συνέπεια απορρίπτεται. [103] Με τον εντοπισμό ενός Sybil node, σχηματίζονται μονοπάτια που περιλαμβάνουν τους γειτονικούς του κόμβους, περιλαμβάνοντας τους μια μόνο φορά. [56] Με τον ήδη εντοπισμένο Sybil node ως κόμβο αναφοράς, υλοποιείται ένα τυχαίο partial walk το οποίο φτάνει ως έναν κόμβο γύρω από τον οποίο όλοι οι υπόλοιποι κόμβοι συμμετέχουν ήδη σε κάποιο walk και το μονοπάτι θεωρείται πλέον νεκρό. Καθώς εντοπίζονται πολλά dead paths, αποκαλύπτεται και η Sybil κοινότητα στο δίκτυο.

Το Symon αποτελεί λύση στην οποία κάθε κόμβος σχετίζεται με έναν non-Sybil κόμβο που ονομάζεται Symon. Η εκχώρηση των Symons σε κάθε κόμβο είναι δυναμική και ελαχιστοποιεί την πιθανότητα να υπάρχει ένα ζεύγος από Sybil nodes. Κάθε Symon παρακολουθεί τις δραστηριότητες του κόμβου που του ανατίθεται, με αποτέλεσμα να γίνεται εξαιρετικά δαπανηρό να δημιουργήσει κάποιος ψεύτικες identities. [103]

Το SybilHunter αποτελεί μια επιλογή για την ανάλυση της αξιοπιστίας των κόμβων ενός δικτύου, βάσει της ανάλυσης της συμπεριφοράς τους και τη σύγκρισή τους με καταγεγραμμένη δικτυακή κίνηση στο Tor. Μπορεί έτσι να εντοπίσει αν ένας ασυνήθιστα μεγάλος όγκος relays έφυγαν ή εισήλθαν στο Tor, ποιοι relays αλλάζουν συχνά τα κλειδιά τους καθώς και ποιοι κόμβοι έχουν σχεδόν ίδιες ρυθμίσεις και πόρους. [54]



Σχήμα 3.33: SybilHunter.

Ακόμα μερικά εργαλεία, τα οποία λειτουργούν με παρόμοιο τρόπο και δε θα αναλυθούν στην παρούσα εργασία είναι τα SybilShield, Sum Up και Gatekeeper. Παρακάτω παρατίθενται τα αποτελέσματα σύγκρισης ορισμένων εργαλείων σχετικά την αποδοτικότητα των μοντέλων, όσον αφορά τα απαιτούμενα walks για τον εντοπισμό Sybil nodes. [12] [51] [103]

Scheme	Maximum g	Accepts	w	# walks
SybilGuard	$O(\sqrt{n}/\log n)^1$	$O(\sqrt{n}\log n)$	$O(\sqrt{n}\log n)$	1
SybilLimit	$O(n/\log n)$	$O(\log n)$	$O(\log n)$	$O(\sqrt{m})$
SybilInfer	—	—	$O(\log n)$	c^3
SumUp	$O(n)^2$	$O(1)$	—	—
Gatekeepr	$O(n/\log n)$	$O(\log k)$	$O(\log n)$	c^3
Whanau	$O(n/\log n)$	$O(\log n)$	$O(\log n)$	$O(\sqrt{cn}\log n)$
MobID	—	—	—	—

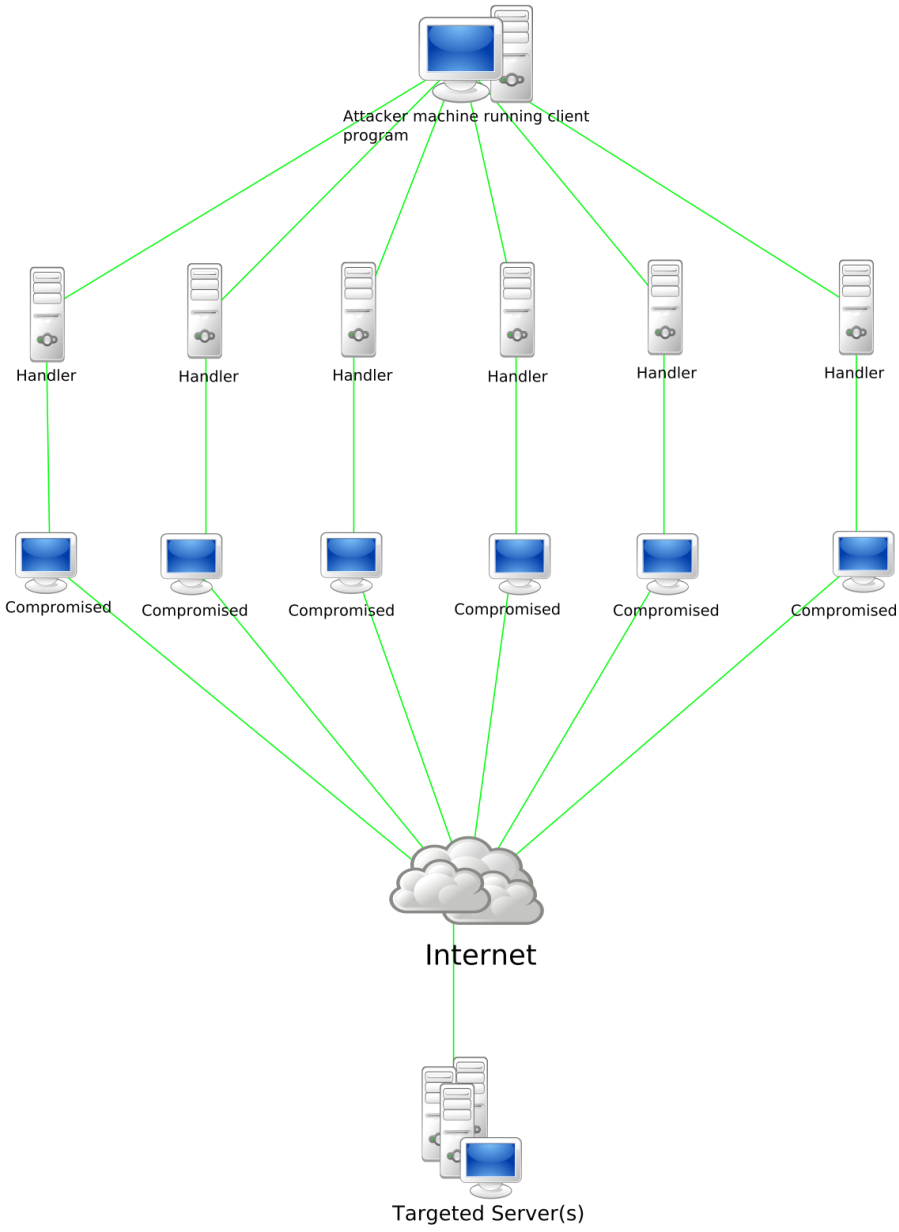
3.1.3.2 Denial of Service Attacks

Εισαγωγικά Στοιχεία

Τα δίκτυα ανωνύμων επικοινωνιών, όπως και τα υπόλοιπα δίκτυα, είναι ευάλωτα σε Denial of Service (DoS) Attacks. Ως Denial of Service Attack ορίζεται το είδος κυβερνοεπίθεσης στο οποίο ο επιτιθέμενος καθιστά μη προσβάσιμους ορισμένους πόρους ενός συστήματος (για παράδειγμα την επεξεργαστική ισχύ) ή ενός δικτύου (όπως το bandwidth) στους χρήστες του. Στην περίπτωση των δικτύων, οι επιθέσεις γίνονται είτε εναντίων ορισμένων services ή hosts του δικτύου, με αποτέλεσμα εκείνοι να μη μπορούν να εξυπηρετήσουν την υφιστάμενη δικτυακή κίνηση, είτε εναντίων πόρων του ίδιου του δικτύου, υλοποιώντας flooding το οποίο εξαντλεί το bandwidth του δικτύου και καθιστώντας το μη λειτουργικό.

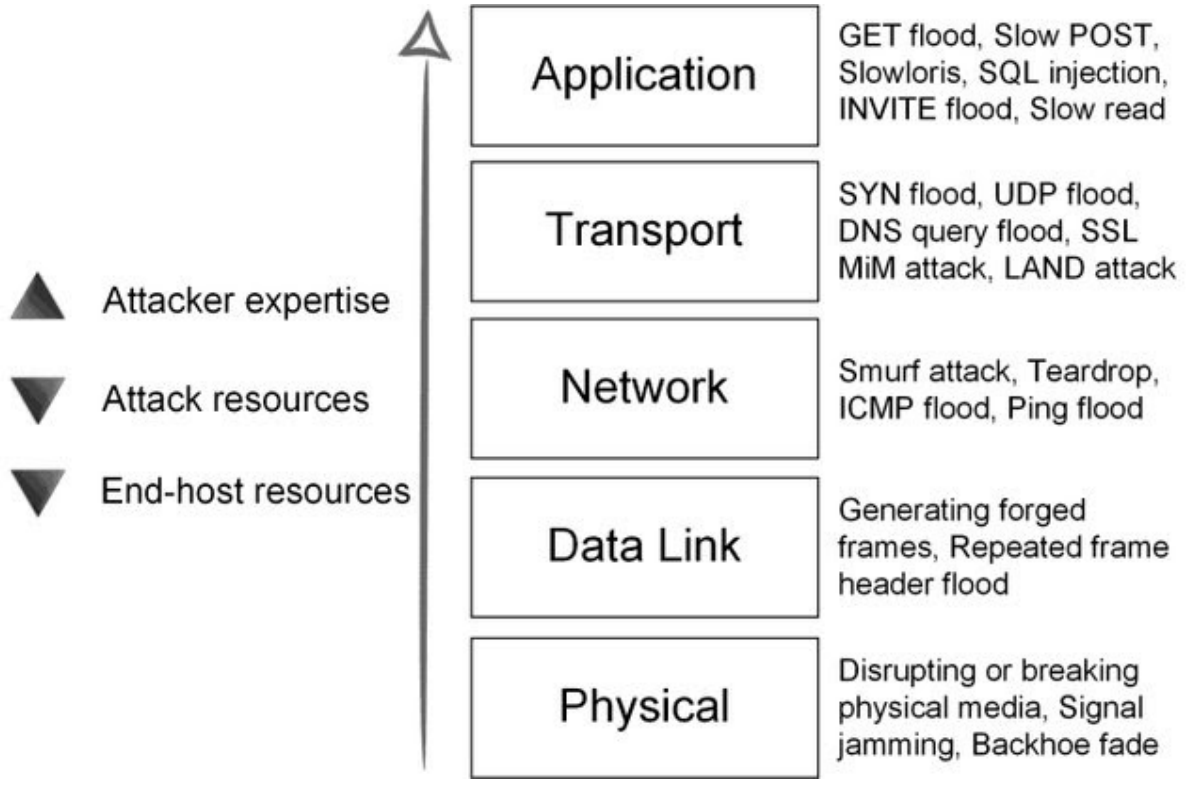
Σχήμα 3.34: Denial of Service Attack.

Μια πολύ προσφιλής παραλλαγή των DoS Attacks είναι οι Distributed DoS (DDoS Attacks), στις οποίες ο επιτιθέμενος με τη χρήση ενός botnet, μπορεί να υλοποιήσει flooding του victim από δικτυακή κίνηση που προέρχεται από πολλές διαφορετικές πηγές, σε διαφορετικά γεωγραφικά σημεία. [115] [120] [132] [140] Το δίκτυο αυτό των botnets μπορεί να υλοποιηθεί με πολλούς τρόπους και αξιοποιείται από τον επιτιθέμενο μέσω ενός Command and Control (C&C) software. Ο επιτιθέμενος συνήθως μολύνει έναν αριθμό hosts στο διαδίκτυο χρησιμοποιώντας ένα exploit kit και στη συνέχεια το payload που χρησιμοποιεί υλοποιεί τη σύνδεση με τον C&C server. Εν συνεχεία ο επιτιθέμενος μπορεί να χρησιμοποιήσει τους hosts αυτούς για διάφορες επιθέσεις. Στις DDoS Attacks η χρήση του botnet διασφαλίζει ότι ακόμα και αν ο αμυνόμενος καταφέρει να μπλοκάρει μια ή περισσότερες πηγές που παράγουν κακόβουλη κίνηση, η υπερεπάρκεια και η γεωγραφική διασπορά των διαθέσιμων bots καθιστούν ουσιαστικά την αντιμετώπιση της επίθεσης αδύνατη. [135]



Σχήμα 3.35: Distributed Denial of Service Attack.

Οι DoS επιθέσεις μπορούν να ταξινομηθούν σε τρεις μεγάλες κατηγορίες. Η πρώτη είναι η Application-layer DDOS attack, στις οποίες στοχεύονται ευπάθειες σε λογισμικά όπως τα Windows, Apache, OpenBSD κ.α, για να εκτελέσει την επίθεση και να εξαντλήσει τους πόρους του server. Οι Protocol DDOS attack στοχεύουν σε επίπεδο πρωτοκόλλου. Αυτή η κατηγορία περιλαμβάνει Synflood, Ping of Death και πολλά άλλα. Τέλος, οι Volume-based DDOS Attacks περιλαμβάνουν ICMP floods, UDP floods και άλλα είδη. Στην παρακάτω εικόνα παρουσιάζονται συνοπτικές λεπτομέρειες σχετικά με τις DoS Attacks που λαμβάνουν χώρα σε διαφορετικα layers του OSI μοντέλου. [116] [117] [118]



Σχήμα 3.36: Μοντέλο επιτιθέμενων σε μια Denial of Service Attack.

Μοντέλο Επιθέσεων

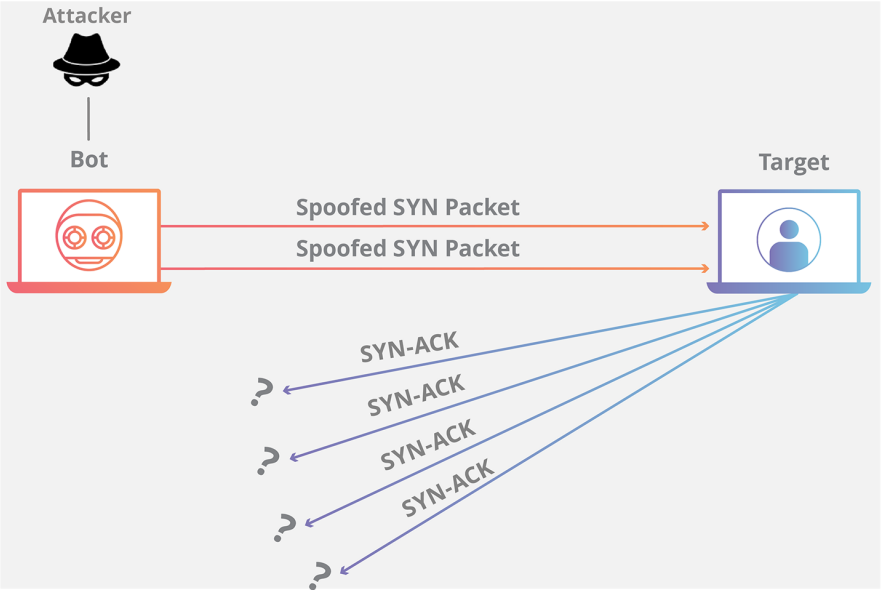
Τα δίκτυα ανωνύμων επικοινωνιών είναι ιδιαίτερα ευάλωτα σε ένα συγκεκριμένο είδος Denial of Service Attacks, και συγκεκριμένα στις Selective DoS Attacks. Η ιδέα πίσω από τις επιθέσεις αυτές είναι η άρνηση παροχής υπηρεσίας σε honest κόμβους προκειμένου το δίκτυο να εξαναγκαστεί στη δημιουργία νέων anonymous tunnels, σε μια επαναλαμβανόμενη διαδικασία έως ότου οι κόμβοι αυτοί συνδεθούν με άλλους compromised κόμβους. Οι malicious κόμβοι, επιχειρούν σε τακτά χρονικά διαστήματα να διακόψουν την παροχή υπηρεσίας προς άλλους honest nodes, όταν το anonymous tunnel στο οποίο συμμετέχουν δεν έχει γίνει ακόμα compromised. Η άρνηση υπηρεσίας αυτή είναι πολύ απλή, καθώς οι malicious κόμβοι μπορούν απλά να διακόπτουν την κίνηση στα tunnels στα οποία συμμετέχουν σα να έχουν βγει εκτός υπηρεσίας. [132] [139]

Ουσιαστικά ο επιτιθέμενος εκτελεί επιλεκτικές Denial of Service επιθέσεις στα tunnels στα οποία δεν έχει ακόμα πρόσβαση, ενώ αφήνει τα tunnels στα οποία διαθέτει compromised κόμβους άθικτα, υλοποιώντας ανάλυση της δικτυακής κίνησης προκειμένου να ταυτοποιήσει τον Initiator και τον Destination. Οι επιθέσεις αυτές μπορούν να δώσουνα ποτελέσματα μόνες τους ή να συνδυαστούν με άλλου είδους επιθέσεις, όπως είναι οι Predecessor, οι Collusion και οι Sybil Attacks επιφέροντας πολλαπλάσια πλήγματα στην ανωνυμία των εκάστοτε χρηστών του δικτύου. Ο γενικός αλγόριθμος της επίθεσης είναι ο ακόλουθος:

if anonymous tunnel is compromised **then**
  do nothing and proceed with information gathering and analysis techniques
else
  perform Selective DoS Attack and force the anonymous network to rebuild the anonymous tunnel until tunnel is compromised

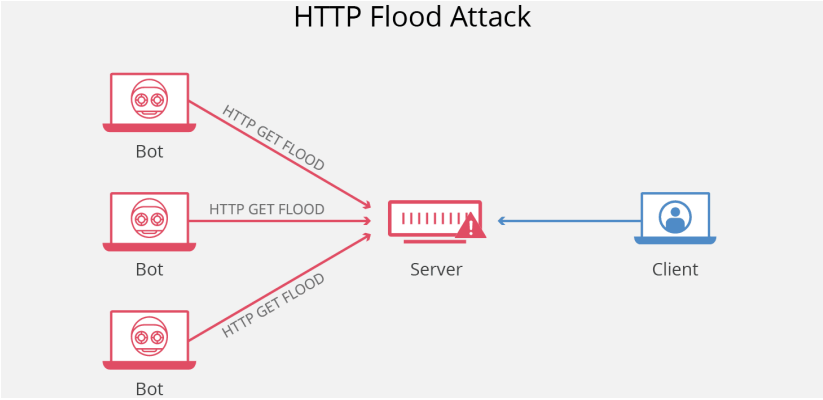
end if

Υπάρχουν δύο μέθοδοι με τις οποίες υλοποιούνται οι Denial of Service Attacks στα δίκτυα ανωνύμων επικοινωνιών. Ο πρώτος είναι μέσω του TCP Syn Flooding. Σε αυτή την περίπτωση ο επιτιθέμενος χρησιμοποιεί μια πλαστή IP Address προκειμένου να στείλει ένα SYN Request στον στόχο της επίθεσης. [111] Όταν ο στόχος λάβει το μήνυμα αυτό στέλνει ως απάντηση το SYN-ACK μήνυμα του και περιμένει την τελική απόκριση ACK από τον επιτιθέμενο, προκειμένου να ολοκληρωθεί επιτυχώς το TCP handshake. Το μήνυμα αυτό ωστόσο δεν φτάνει ποτέ, καθώς η IP Address που φαίνεται στο SYN μήνυμα είναι ψευδής. Ο επιτιθέμενος στέλνει έναν πολύ μεγάλο όγκο τέτοιων παραποιημένων TCP μηνυμάτων στον στόχο, εξαντλώντας τους πόρους του και οδηγώντας τον σε αδυναμία να λειτουργήσει, θέτοντας τον εκτός λειτουργίας. [128]



Σχήμα 3.37: TCP Flooding.

Η δεύτερη μεθοδος που χρησιμοποιείται είναι η Query Flooding Attack, η οποία εκτυλίσσεται στο Application Layer. [140] [142] Ο κόμβος στον οποίο απευθύνεται το query σε πολλές περιπτώσεις θα χρειαστεί να προωθήσει το query σε όλους τους υπόλοιπους κόμβους του γκρουπ του ή ακόμα και του δικτύου, όπως συμβαίνει σε πάρα πολλές peer-to-peer τεχνολογίες ανωνύμων επικοινωνιών, ιδιαίτερα δε σε αυτές που απευθύνονται σε file sharing εφαρμογές. Έτσι, ο επιτιθέμενος εκμεταλευόμενος την ιδιότητα αυτή του δικτύου αποστέλλει μεγάλο όγκο queries, εξαντλώντας σε πολύ σύντομο χρονικό διάστημα τους πόρους του.



Σχήμα 3.38: HTTP Flooding.

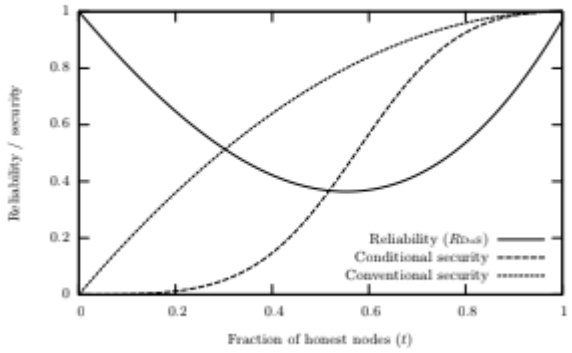
Denial of Service Attacks Case Studies

1. *Denial of Service Attacks στο Tor*

Όπως έχει ήδη αναλυθεί και σε προηγούμενες επιθέσεις, το Tor είναι ιδιαίτερα ευάλωτο αν ο πρώτος και ο τελευταίος router από αυτούς που απαρτίζουν το εκάστοτε μονοπάτι ελέγχονται από τον επιτιθέμενο, καθώς με κατάλληλη ανάλυση της δικτυακής κίνησης μπορούν να επιβεβαιώσουν αν οι εξεταζόμενες ροές πακέτων ανήκουν στο ίδιο data stream, ταυτοποιώντας ουσιαστικά τόσο τον Initiator όσο και τον Responder της εκάστοτε διαδικτυακής συνομιλίας. Κάτι τέτοιο δύναται να επιφέρει σημαντικό πλήγμα στην ανωνυμία των χρηστών του και να επιτρέψει στους επιτιθέμενους να συλλέξουν κρίσιμες πληροφορίες σχετικά με αυτούς. Η αξιοπιστία του Tor Network είναι πολύ εύκολο να προσδιοριστεί, καθώς αν ένα μονοπάτι αποτελείται από l routers τότε αν έστω ένας από αυτούς τεθεί εκτός λειτουργίας, τότε το ολόκληρο το μονοπάτι καθίσταται ανενεργό. Θεωρώντας λοιπόν f την πιθανότητα ένας router να είναι αξιόπιστος, τότε ως $R = f^l$ ορίζεται η πιθανότητα να είναι ολόκληρο το tunnel στο οποίο ανήκει αξιόπιστο. [112] [113] [116] Εδώ θα πρέπει να τονιστεί ότι ο όρος reliable αναφέρεται σε ένα tunnel το οποίο επιτυγχάνει να προωθήσει τη δικτυακή κίνηση, ενώ ο όρος secure για tunnel το οποίο δεν περιέχει κάποιον compromised node.

Το Tor Network είναι ιδιαίτερα ευπαθές ενάντια στις Selective Denial of Service Attacks, οι οποίες είναι εύκολο να υλοποιηθούν, επιφέροντας σημαντικά πλήγματα στη συνολική αξιοπιστία του δικτύου. Η επίθεση μπορεί να υλοποιηθεί όταν ο επιτιθέμενος έχει αποκτήσει τον έλεγχο του πρώτου ή του τελευταίου router ενός tunnel. Μέσω των routers αυτών, έχει τη δυνατότητα να πραγματοποιήσει παρατήρηση της διερχόμενης από αυτούς δικτυακής κίνησης και στη συνέχεια να κάνει συγκρίσεις με αυτές που διέρχονται από άλλους routers τους οποίους ελέγχει, οι οποίοι αποτελούν επίσης τον πρώτο ή τον τελευταίο router σε άλλα μονοπάτια. Αν υπάρχει σύγκληση στα αποτελέσματα τότε η δικτυακή κίνηση μπορεί να ταυτοποιηθεί και να αναγνωριστεί ο Initiator και ο Responder. [117] Αν δεν υπάρξει σύγκληση, τότε ο επιτιθέμενος υλοποιεί Denial of Service Attack στο συγκεκριμένο μονοπάτι, απαγορεύοντας στον router που έχει υπό έλεγχο να προωθήσει οποιασδήποτε μορφής δικτυακής κίνησης. Υποθέτουμε ότι οι compromised routers διακόπτουν την προώθηση πακέτων για οποιοδήποτε μονοπάτι δεν καταφέρουν να ταυτοποιήσουν επιτυχώς. Επιπροσθέτως, σε περίπτωση που ο επιτιθέμενος καταφέρει να αποκτήσει τον έλεγχο ενος router που λειτουργεί ως ενδιάμεσο hop τότε μέσω αυτού διακόπτει οποιαδήποτε δικτυακή κίνηση διέρχεται από αυτό, εκτός από την περίπτωση που τόσο το προηγούμενο όσο και το επόμενο router αποτελούν colluding nodes.

Υπό το πρίσμα της επίθεσης που περιγράφηκε, η συνολική αξιοπιστία ενός anonymous tunnel είναι $R < DoS >= (1-t)^2 + (tf)^2$. Παρατηρείται λοιπόν το φαινόμενο να θεωρείται reliable ένα tunnel το οποίο έχει τόσο τον πρώτο όσο και τον τελευταίο κόμβο compromised ή αν αποτελείται από non-compromised κόμβους εξ ολοκλήρου. Στο διάγραμμα που ακολουθεί παρουσιάζεται η αξιοπιστία ενός Tor Network υπό την απειλή μιας Selective DoS Attack όταν f=0.99. [138] [140]



Σχήμα 3.39: Σύγκριση αξιπιστίας και ασφάλειας του δικτύου.

Γίνεται εμφανές ότι η αξιοπιστία (reliability) του δικτύου μειώνεται καθώς αυξάνεται το πλήθος των compromised nodes στο δίκτυο, έως ότου φτάσει στο 0.55, από όπου ξεκινάει και αυξάνεται ξανά. [135] Αυτό μπορεί να φαίνεται παράδοξο, ωστόσο συμβαίνει διότι στο σημείο αυτό ο όρος $(1-t)^2$ κυριαρχεί. Αυτό σημαίνει ότι πλέον οι compromised nodes υλοποιούν Denial of Service Attacks σε λιγότερα tunnels, καθώς έχουν ήδη ταυτοποιήσει αρκετά. [130] Το διάγραμμα μας δίνει επιπλέον σημαντικές πληροφορίες σχετικά με το πλήθος των secure tunnels ως μέρος των reliable, για παράδειγμα την εξαρτημένη πιθανότητα του να είναι ένα tunnel secure, δεδομένου ότι είναι reliable. Η πληροφορία αυτή είναι εξαιρετικά χρήσιμη καθώς στο Tor Network όταν ένα tunnel καθίσταται μη λειτουργικό, κάτι το οποίο γίνεται μέσω των DoS Attacks, επιχειρεί να σχηματίσει ένα νέο μονοπάτι, επαναλαμβάνοντας τη διαδικασία αυτή έως ότου δημιουργηθεί ένα reliable tunnel. [128] [129] Η εξαρτημένη πιθανότητα που παρουσιάζεται στο διάγραμμα δείχνει την πιθανότητα να είναι ένα tunnel ασφαλές και αξιόπιστο, δηλαδή ασφαλές και λειτουργικό. Φαίνεται ότι για υψηλές τιμές του t οι τιμές είναι πολύ κοντά στις συμβατικές τιμές για την ασφάλεια ενός Tor Network που δεν υποφέρει από DoS Attacks, ωστόσο όσο αυξάνεται ο αριθμός των compromised κόμβων, τόσο μεγαλύτερη απόκλιση υπάρχει. Για t=0.5 υπό φυσιολογικές συνθήκες λειτουργίας, στο Tor Network έχουμε ασφαλές το 75% όλων των tunnels, ενώ στην περίπτωση που λάβουμε υπόψη τις Selective Denial of Service Attacks τότε μόνο το 33% των σχηματισθέντων tunnels παραμένουν ελεύθερα από compromised nodes. [138]

Στην παραπάνω ανάλυση καθοριστικό ρόλο παίζει ο παράγοντας t, ο οποίος εκφράζει το ποσοστό των συνολικών κόμβων στο Tor Network που είναι non-compromised, δηλαδή honest. Στις παραπάνω αναλύσεις φαίνεται ότι για t=0.5 θα υπήρχαν μεν σημαντικές επιπτώσεις στη ασφάλεια του δικτύου λόγω των Selective DoS Attacks, ωστόσο ταυτόχρονα φαίνεται εξαιρετικά δύσκολο οι μισοί κόμβοι στο Tor Network να είναι κακόβουλοι, επομένως ένα τέτοιο σενάριο φαντάζει εξαιρετικά δύσκολο να γίνει πραγματικότητα. [139] Πράγματι, το σενάριο αυτό είναι δύσκολο να υλοποιηθεί υπό φυσιολογικές συνθήκες λειτουργίας του δικτύου, ωστόσο το Tor Network δέχεται συνεχώς νέες προσθήκες κόμβων χωρίς ιδιαίτερο έλεγχο για την αξιοπιστία τους. Σε περίπτωση που υλοποιηθεί μια τέτοια προσπάθεια από κάποιον οργανισμό που έχει πρόσβαση σε πόρους, τότε είναι δυνατό οργανισμός αυτός να προσφέρει ένα μεγάλο πλήθος νέων compromised κόμβων στο δίκτυο, με πολλές διαφορετικές identities και μεγάλη γεωγραφική κατανομή οι οποίοι θα καταφέρουν να υλοποιήσουν με μεγάλη ευκολία μια σειρά επιθέσεων, συμπεριλαμβανομένων και των Selective DoS Attacks. [141] Το Tor Network εξάλλου έχει αποτελέσει πολλές φορές στόχο διαφόρων κρατικών cybersecurity agencies ανά τον κόσμο, τα οποία διαθέτουν υπερεπάρκεια πόρων για να υλοποιήσουν τέτοιου είδους επιθέσεις, τόσο για την ταυτοποίηση της δικτυακής κίνησης που σχετίζεται με

εγκληματικές δραστηριότητες, όσο και για τη λογοκρισία του Internet και την απαγόρευση πρόσβασης σε περιεχόμενο μέσω του δικτύου.

Οι Selective DoS Attacks δημιουργούν ιδιαίτερο πρόβλημα διότι συνδυάζονται με τις Predecessor Attacks προκειμένου να επιταχύνουν την επίτευξη των στόχων τους. Όπως αναφέρεται και στο αντίστοιχο κεφάλαιο, η συνεχής δημιουργία νέων μονοπατιών οδηγεί μετά από $O((1-t)^2 ln(n))$ rounds στη δημιουργία ενός compromised tunnel, όπου n το σύνολο των κόμβων που υπάρχει στο Tor Network. [118] [132] [142] Η χρήση Guard nodes συμβάλει στην αντιμετώπιση των Predecessor Attacks ενώ μπορούν να συμβάλλουν και στη θωράκιση του δικτύου απέναντι στις Selective DoS Attacks. Αυτό φυσικά έχει επιπτώσεις στο reliability των χρηστών, καθώς σε αρκετές περιπτώσεις λόγω των DoS Attacks θα έχουν διακοπή υπηρεσίας, ωστόσο θωρακίζονται εξ ολοκλήρου από τυχόν compromised tunnels. Η θωράκιση ωστόσο που προσφέρουν οι Guard nodes προϋποθέτει την ύπαρξη αρκετών τέτοιων κόμβων. [138] Έτσι, ο χρήστης θα πρέπει να έχει μια ευρεία επιλογή Guard nodes για να επιλέξει ως πρώτο κόμβο του μονοπατιού, κάτι που δεν είναι πάντα εφικτό. Σε αντίθετη περίπτωση, η χρήση Guard nodes μπορεί να οδηγήσει στα ακριβώς αντίθετα αποτελέσματα, δηλαδή στην ενίσχυση της Selective DoS Attack, καθώς η πιθανότητα να γίνει compromised ένα tunnel είναι μεγαλύτερη αν χρησιμοποιείται πολύ μικρό πλήθος Guard nodes. Για παράδειγμα, η χρήση ενός μόνο Guard node θα έχει ως αποτέλεσμα (1-t) όλων των tunnels να γίνουν compromised. Με χρήση 3 Guard nodes, η οποία είναι και η εφαρμογή του Tor Network, έχουμε επίσης σημαντικά αυξημένο αριθμό compromised tunnels. [115]

Σε κάθε περίπτωση, η παραπάνω ανάλυση δείχνει ότι το Tor Network είναι ιδιαίτερα ευάλωτο ενάντια σε τέτοιου είδους επιθέσεις. Ο επιτιθέμενος, εκμεταλλευόμενος τους μηχανισμούς δημιουργίας των anonymous tunnels στο πρωτόκολλο του Tor Network επιφέρει πλήγματα, μέσω επιλεκτικών Denial of Service Attacks στα tunnels που δεν έχει κάνει ακόμα compromised, στην αξιοπιστία του δικτύου, προκειμένου να εξαναγκάσει το δίκτυο να δημιουργεί συνεχώς νέα tunnels, έως ότου αυτά περιέχουν compromised κόμβους, οι οποίοι θα επιτρέψουν στον επιτιθέμενο να υλοποιήσει ανάλυση της δικτυακής κίνησης. [135] [136]

2. Denial of Service Attacks σε Mix Networks

Τα Mix Networks όπως το MixMaster και το MixMinion είναι δίκτυα που χρησιμοποιούνται κατά κόρον για εξυπηρέτηση high latency ανωνύμων επικοινωνιών, όπως είναι η ανταλλαγή ανώνυμης ηλεκτρονικής αλληλογραφίας. Τα δίκτυα αυτά, παρ' όλο που αδυνατούν να υποστηρίξουν σύγχρονες διαδικτυακές εφαρμογές που απαιτούν low latency, είναι πολύ πιο ισχυρές στην αντιμετώπιση Timing και Latency Attacks καθώς κατά τη διάρκεια του batching εισάγουν μεγάλες, μεταβλητές και ανομοιογενείς μεταξύ τους καθυστερήσεις, καθιστώντας τις παραπάνω αναλύσεις εξαιρετικά δύσκολες.

Τα παραπάνω δίκτυα αντιμετώπισαν εξ αρχής ζητήματα αξιοπιστίας (reliability) καθώς τα mixes αποτελούνται κατά κόρον από κόμβους που συνεισφέρουν στο δίκτυο οι συμμετέχοντες χρήστες, με αποτέλεσμα αυτοί να μην είναι συνεχώς διαθέσιμοι. [132] Μια λύση που εφαρμόστηκε ήταν η εισαγωγή pingers στο δίκτυο, οι οποίοι επιφορτίζονται με την αξιολόγηση της διαθεσιμότητας των κόμβων. Οι pingers δημιουργούν κίνηση προς όλα τα mixes και καταγράφουν τη συνολική διαθεσιμότητα των κόμβων, μέσω της καταγραφής του uptime και της δυνατότητας παράδοσης μηνυμάτων, σχηματίζοντας rankings στα οποία φαίνεται η αξιοπιστία τους. Προκειμένου να αποφευχθεί το φαινόμενο malicious κόμβοι να επηρεάζουν το ranking των honest κόμβων τα pings δρομολογούνται μέσω ενός ανώνυμου δικτύου επικοινωνιών. [133] Στη συνέχεια, οι clients επιλέγουν

τα mixes μέσω των οποίων θα δρομολογήσουν τη δικτυακή τους κίνηση βασιζόμενοι στα reliability rankings που έχουν δημιουργήσει και κοινοποιήσει στο δίκτυο οι pingers. Η κοινοποιημένη πληροφορία αυτή ωστόσο μπορεί να είναι εύκολα προσβάσιμη και στους επιτιθέμενους, οι οποίοι μπορούν να καταλάβουν ποια είναι τα συχνότερα χρησιμοποιούμενα mixes και να τα στοχεύσουν, δημιουργώντας έτσι κινδύνους για την ανωνυμία του δικτύου.

Μια άλλη λύση για την αξιολόγηση της αξιοπιστίας των mixes είναι ο κατακερματισμός των μηνυμάτων σε fragments, τα οποία θα αποστέλλονται στον τελικό προορισμό μέσω διαφορετικών paths. [115] Τα mixes που ανήκουν σε διαφορετικά paths δεν έχουν καμία επικοινωνία μεταξύ τους και τα διαφορετικά fragments των μηνυμάτων δεν αλληλεπιδρούν μεταξύ τους. Επιπλέον, τα διαφορετικά fragments δε μπορούν να συσχετιστούν, καθιστώντας την ανάλυση της δικτυακής κίνησης από κάποιο κακόβουλο χρήστη δύσκολη. [117] Τέλος, η αξιοπιστία του δικτύου επιτυγχάνεται στέλνοντας πολλαπλά αντίγραφα του ίδιου μηνύματος μέσω διαφορετικών mixes προκειμένου να εξασφαλιστεί ότι αυτά θα παραδοθούν σε κάθε περίπτωση. [120]

Ο παρακάτω πίνακας δείχνει ορισμένες σημαντικές παραμέτρους που θα χρησιμοποιηθούν στην ανάλυση των Selective Denial of Service Attacks στα Mix Networks. [138]

Variable	Description
l	The *length* of all paths. We assume all copies of the message travel over paths of the same length.
w	(for *width*) The number of independent paths over which a copy of the message is transmitted.
t	The probability a mix is honest. Its converse $\bar{t} = 1 - t$ is the probability a node is in the hands of the adversary. We assume that all nodes when chosen have the same probability of being corrupt, independently of the number of previously honest or corrupt nodes selected.
f	The probability an honest node is reliable. Its converse $\bar{f} = 1 - f$ is the probability it is unreliable. This does not apply to corrupt nodes, which are reliable or not depending on the attack strategy—a reliable node relays the message correctly, while an unreliable one is simply offline, and behaves as if it does not exist in the network.

Για να γίνει ένα μήνυμα compromised θα πρέπει τουλάχιστον ένα πλήρες route να αποτελείται εξ ολοκλήρου dishonest mixes. Ένα route διαθέτει τουλάχιστον ένα honest mix με πιθανότητα $1 - \bar{t}^{l}$, ενώ η πιθανότητα να έχουν όλα τα routes τουλάχιστον ένα honest mix είναι αντίστοιχα $(1 - \bar{t}^{l})^{w}$. Η αύξηση του παράγοντα l, ο οποίος όπως βλέπουμε αντικατοπτρίζει το μήκος των μονοπατιών, αυξάνει εκθετικά τον βαθμό ασφαλείας ενός Mix Network. [138] Έτσι, τα Mix Networks υπερτερούν σημαντικά σε θέματα ασφαλείας από τα αντίστοιχα low latency δίκτυα ανωνύμων επικοινωνιών όπως το Tor Network. Στο Mixminion ο παράγοντας l έχει καθοριστεί να ισούται με 5, επομένως ακόμα και αν το 50% των mixes γίνει compromised, μόνο το 3% του συνόλου των διακινούμενων στο δίκτυο μηνυμάτων θα μπορέσει να διαβαστεί από τον επιτιθέμενο. Η αύξηση ή η μείωση του παράγοντα l είναι και που καθορίζεται από τον εκάστοτε χρήστη, επομένως σε πιο επισφαλή δίκτυα οι χρήστες μπορούν να αυξήσουν έτι περαιτέρω το βαθμό ασφαλείας τους και να θωρακίσουν την ανωνυμία τους. Όσον αφορά τη αξιοπιστία ενός Mix Network, ένα μήνυμα μπορεί να παραδοθεί στον τελικό προορισμό του αν ένα τουλάχιστον full route δεν έχει malicious mixes εντός του. Η πιθανότητα να συμβεί αυτό είναι $(\bar{t} + t * f)^{l}$, ενώ η πιθανότητα να μην είναι όλα τα routes reliable ορίζεται $1 - [1 - (\bar{t} + t * f)^{w}$ [138] [139] [140] [141]

Ο επιτιθέμενος μπορεί να επιλέξει να υλοποιήσει μια Selective Denial of Service Attack έτσι ώστε να μεγιστοποιήσει τις πιθανότητες του να κάνει compromise ορισμένα μηνύματα. Στην περίπτωση αυτή, ένας compromised mix επιλέγει να κάνει relay μόνο τα μηνύματα τα οποία μπορεί να κάνει trace, δηλαδή να παρακολουθήσει καθ όλη τη διαδρομή τους στο μονοπάτι. Τα mixes αποκρυπτογραφούν όσα μηνύματα μπορούν, με τη βοήθεια των υπολοίπων colluding mixes, προκειμένου να καθορίσουν

αν κατά τη διαδρομή υπάρχουν honest mixes. Τα μηνύματα τα οποία δε θα μπορέσουν να αποκρυπτογραφηθούν με τον τρόπο που περιγράφηκε παραπάνω είτε θα απορριφθούν εξ ολοκλήρου από τα malicious mixes, είτε θα τροποποιηθούν ελαφρώς ώστε να μη μπορούν να ανακτηθούν από τον τελικό προορισμό. Αυτό οδηγεί στον Initiator να στείλει περισσότερα αντίγραφα του μηνύματος που χάθηκε, από διαφορετικά routes, κάτι που αυξάνει τις πιθανότητες να γίνει compromised και να αποκρυπτογραφηθεί από τον επιτιθέμενο. [112]

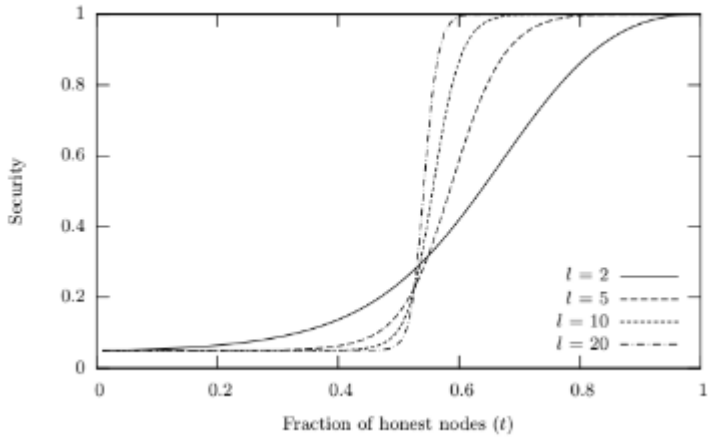
Έτσι, υπό το πρίσμα ενός Mix Network στο οποίο λαμβάνει χώρα μια Selective DoS Attack διακρίνουμε δύο πιθανά σενάρια για την επιτυχή παράδοση ενός μηνύματος από τον Initiator στον τελικό προορισμό. Το πρώτο είναι το route να αποτελείται εξ ολοκλήρου από honest mixes και το δεύτερο, να αποτελείται εξ ολοκλήρου από compromised mixes. Η πιθανότητα να συμβεί αυτό είναι $r = (1-t)^l + (t*f)^l$. Τουλάχιστον ένα μονοπάτι εντός του εύρους w πρέπει να επιλεχθεί, κάτι που συμβαίνει με πιθανότητα $1-(1-r)^w$. Η αξιοπιστία επομένως για ένα Mix Network το οποίο υφίσταται μια >Selective DoS Attack ορίζεται $1-(1-[\bar{t}+(t*f)^l])^w$. Η Selective DoS Attack δεν επηρεάζει την πιθανότητα ένα μήνυμα να είναι secure. Η διαφορά με την τακτική που εφαρμόζεται στις αντίστοιχες επιθέσεις στα low latency anonymous networks είναι ότι εδώ εξαναγκάζεται ο χρήστης να στείλει περισσότερα αντίγραφα ενός μηνύματος προκειμένου αυτό να παραδοθεί επιτυχώς, κάτι που αυξάνει σημαντικά τις πιθανότητες να γίνει compromised από τον επιτιθέμενο. [138]

Σε ένα Mix Network με παραμέτρους (l, w_{DoS}, t, f), το οποίο υφίσταται μια Selective DoS Attack, για να επιτύχει τα ίδια αξιοπιστία με ένα Mix Network που υφίσταται μια οποιαδήποτε άλλη Passive Attack και έχει παραμέτρους (l, w_{pas}, t, f) θα πρέπει να σταλούν w_{DoS} αντίγραφα μηνυμάτων, όπου

$$w_{DoS} = \frac{\log(1-(\bar{t}+t\cdot f)^l)}{\log(1-(\bar{t}^l+(t\cdot f)^l))} w_{pas}$$

Προκύπτει ότι οι Selective DoS Attacks παρέχουν σαφές πλεονέκτημα στον επιτιθέμενο όσον αφορά την πιθανότητα επιτυχίας αποκρυπτογράφησης ενός μηνύματος, καθώς ο Initiator θα χρειαστεί να στείλει έναν πολύ μεγάλο αριθμό αντιγράφων έως ότου αυτό παραδοθεί επιτυχώς. Γίνεται πολύ εύκολα αντιληπτό ότι με μεγάλο αριθμό compromised mixes στο δίκτυο, η διαθεσιμότητα λαμβάνει τις ίδιες υψηλές τιμές με το αν η πλειοψηφία των mixes είναι honest. Έτσι, καθίσταται σαφές ότι η ασφάλεια ενός δικτύου επ ουδενί δε θα πρέπει να θεωρείται συνυφασμένη με τη διαθεσιμότητα και την αξιοπιστία του.

Η αύξηση του μήκους μονοπατιού στα Mix Networks είναι μια από τις ενδεδειγμένες λύσεις για την αύξηση της ασφάλειας τους. Όπως έχει αναφερθεί ήδη, η αύξηση του παράγοντα l οδηγείσ ε εκθετική αύξηση της ασφάλειας του δικτύου απέναντι σε Passive Attacks. Στο παρακάτω διάγραμμα φαίνεται το επίπεδο ασφαλείας που επιτυγχάνεται από τον κατάλληλο συνδυασμό των παραγόντων του Mix Network.



Σχήμα 3.40: Σύγκριση αξιοπιστίας και ασφάλειας του δικτύου βάσει του ποσοστού των honest nodes.

Για μεγάλες τιμές του t, υψηλές τιμές του l εγγυώνται την ασφάλεια του δικτύου απέναντι σε Selective DoS Attacks. Αντίθετα, για χαμηλές τιμές του t, οι υψηλές τιμές του l δρουν επιβαρυντικά για την ασφάλεια του δικτύου, καθώς στην περίπτωση που πολλά mixes γίνουν compromised, η αύξηση του μήκους μονοπατιού οδηγεί σε περισσότερα malicious mixes να ενταχθούν σε αυτό. Αυτό δείχνει ότι τα Mix Networks αν και είναι γενικά πιο αξιόπιστα στην αντιμετώπιση επιθέσεων, έχουν ένα συγκεκριμένο όριο όσον αφορά το πλήθος των compromised mixes που βρίσκονται σε αυτά, πάνω από το οποίο το δίκτυο καθίσταται μη ασφαλές. [136] [137] [138]

3. *Denial of Service Attacks σε Reliability-Oriented Anonymous Networks*

Το Cashmere, όπως έχει αναλυθεί και στο αντίστοιχο κεφάλαιο είναι μια τεχνολογία ανωνύμων επικοινωνιών προσανατολισμένη στην αύξηση της αξιοπιστίας του δικτύου, έτσι ώστε να διασφαλίζεται η παράδοση των διακινούμενων μηνυμάτων στον τελικό προορισμό ακόμα και υπό τις δυσμενέστερες συνθήκες. Υπό την παρουσία ενός παθητικού κακόβουλου χρήστη, τόσο οι honest όσο και οι dishonest κόμβοι του δικτύου θα δρομολογήσουν κατάλληλα τα μηνύματα στο δίκτυο. Αυτό συμβαίνει διότι, όπως έχει ήδη αναφερθεί, αρκεί ένας μόνο ενεργός κόμβος root relay group, ο οποίος μπορεί να λειτουργεί ως root relay group και να προωθεί τα μηνύματα. Καθώς τα μηνύματα διακινούνται σε όλους τους κόμβους του relay group, αρκεί μόνο ένας compromised κόμβος εντός ενός αυτού ώστε να καταστεί μη ασφαλές. Φυσικά, επειδή ο τελικός προορισμός δεν αποκαλύπτεται στο αποκρυπτογραφημένο μήνυμα αλλά επιλέγεται ανάμεσα σε όλα τα μέλη του relay group, για να θεωρηθεί ένα μήνυμα compromised θα πρέπει και ο προορισμός να είναι compromised κόμβος. [113]

Θεωρώντας (l, w, t, f) τις παραμέτρους του Cashmere με τους κακόβουλους κόμβους να δρομολογούν όλη τη δικτυακή κίνηση, μπορούμε να υπολογίσουμε την πιθανότητα να είναι ένα relay group αξιόπιστο. Όπως έχει τονιστεί προηγουμένως, η αξιοπιστία στην παρούσα ανάλυση αναφέρεται στη διαθεσιμότητα, συνεπώς η πιθανότητα να υπάρχει ένας honest, reliable ή dishonest κόμβος στο relay group είναι $1 - (t * \bar{f})^{w}$. [138] Φυσικά γίνεται αντιληπτό ότι για να παραδοθεί ένα μήνυμα επιτυχώς στον προορισμό του πρέπει όλα τα relay groups από τα οποία θα διέλθει να είναι επίσης αξιόπιστα. Η πιθανότητα ένα relay group να είναι ο τελικός προορισμός είναι 1/l, έτσι, ένα μήνυμα παραδίδεται με πιθανότητα:

$$\sum_{i=0}^{l-1} \frac{1}{l} \left(1 - (t\bar{f})^{w}\right)^{i} (\bar{t} + tf)$$

Όσον αφορά την ασφάλεια του Cashmere, προκύπτει αβίαστα το συμπέρασμα ότι για να καταφέρει ένας επιτιθέμενος να πλήξει την ανωνυμία των επικοινωνιών και να αποκαλύψει την ταυτότητα του Initiator σε ένα μήνυμα θα πρέπει κάθε relay group μέσω του οποίου αυτό διέρχεται, συμπεριλαμβανομένου και του τελικού προορισμού, να είναι compromised. Η πιθανότητα να υπάρχει τουλάχιστον ένας compromised κόμβος σε κάθε relay group είναι $1 - t^{w}$. [138] [142] Η τελική πιθανότητα που έχει λοιπόν ένα μήνυμα να παραδοθεί επιτυχώς, χωρίς να πληγεί η ανωνυμία του αποστολέα του είναι:

$$1 - \sum_{i=0}^{l-1} \frac{1}{l} (1 - t^{w})^{i} \bar{t}$$

Υπό το πρίσμα των selective DoS Attacks, το Cashmere επηρεάζεται αν οποιοδήποτε relay group είναι compromised. Ακολουθώντας τον αλγόριθμο της επίθεσης, ο κακόβουλος χρήστης θα κάνει drop οποιαδήποτε δικτυακή κίνηση διέρχεται μέσω του relay root που ελέγχει, εκτός αν έχει καταφέρει να κάνει compromised ολόκληρο το path, κάτι που θα του δώσει πρόσβαση στην ταυτοποίηση του Initiator και του προορισμού του μηνύματος. Αυτό πρακτικά σημαίνει πως όταν τα μηνύματα παραδίδονται κανονικά, είτε ολόκληρο το μονοπάτι αποτελείται από honest κόμβους, είτε αποτελείται εξολοκλήρου από compromised και η ανωνυμία έχει πάψει πλέον να υφίσταται. [113]

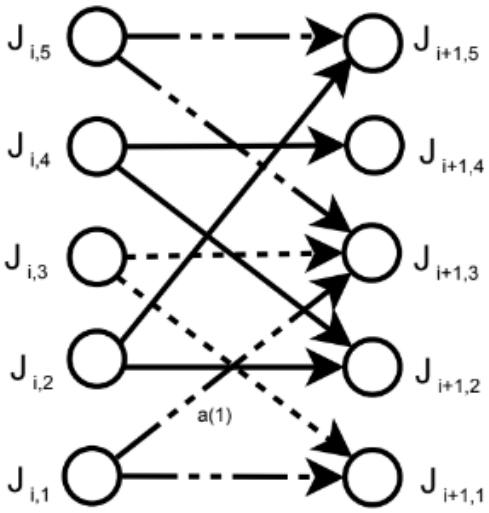
Ένας κόμβος επιλέγεται ως root relay μόνο αν είναι αξιόπιστος, επομένως η πιθανότητα να είναι τόσο αξιόπιστος, δηλαδή διαθέσιμος, όσο και ασφαλής, είναι $\frac{t*f}{(t*f+\bar{t})}$. Η τελική πιθανότητα να παραδοθεί ένα μήνυμα με ασφάλεια, υπό την απειλή ενός επιτιθέμενου που υλοποιεί μια Selective DoS Attack είναι:

$$\sum_{i=0}^{l-1} \frac{1}{l} \left((1 - t^{w})^{i} \bar{t} + \left(\frac{tf}{tf + \bar{t}} \right)^{i} tf \right)$$

Η αύξηση της αξιοπιστίας του Cashmere μέσω της αύξησης του w δεν είναι δυνατή καθώς ο επιτιθέμενος αρκεί να έχει τον έλεγχο μόνο του root node για να μπλοκάρει τη διέλευση των μηνυμάτων. Οι Selective DoS Attacks είναι πολύ ισχυρές στην ταχύτατη μείωση των ασφαλών μονοπατιών στο δίκτυο. [138] Έτσι, το Cashmere είναι σαφώς υποδεέστερο από τα Mix Networks όσον αφορά την προστασία από τέτοιου είδους επιθέσεις, καθώς εκεί απαιτείται ο επιτιθέμενος να έχει έναν compromised κόμβο σε κάθε path. Έτσι, οι Selective DoS Attacks αποτελούν ίσως τον κυριότερο κίνδυνο για τη συγκεκριμένη τεχνολογία ανωνύμων επικοινωνιών, υπονομεύοντας σε μεγάλο βαθμό την ασφάλεια τους. [112]

Μια ακόμα εφαρμογή ανωνύμων επικοινωνιών που έχει μελετηθεί υπό το πρίσμα των Selective DoS Attacks είναι το Hydra-Onions. Είναι μια παραλλαγή του Onion Routing ειδικά σχεδιασμένη ώστε να είναι ανθεκτική στις Onion Dropping Attacks. Το πρωτόκολλο λειτουργεί με παρόμοιο τρόπο με τα Mix Networks, μόνο που στη συγκεκριμένη εφαρμογή, σε κάθε βήμα, θα δημιουργηθούν δύο

αντίγραφα του μηνύματος και θα προωθηθούν σε δύο διαφορετικούς επόμενους mixes. Ενδεικτικά η λειτουργία του φαίνεται στην παρακάτω εικόνα. [115]



Σχήμα 3.41: Λειτουργία των Mixes σε reliability-focused τεχνολογίες ανωνύμων επικοινωνιών.

Κάθε ένα από τα mixes στο εκάστοτε μονοπάτι μπορεί να αποκρυπτογραφήσει τα μηνύματα που διακινούνται σε αυτό. Αν σε κάθε βήμα υπάρχει ένας compromised mix τότε το Hydra-Onion είναι μη ασφαλές. Η πιθανότητα λοιπόν ένα μήνυμα να είναι ασφαλές είναι $1-(1-t^w)^l$. Η εν λόγω τεχνολογία ανωνύμων επικοινωνιών επιτυγχάνει θεαματικά αποτελέσματα όσον αφορά τη διασφάλιση της αξιοπιστίας του δικτύου. Ακόμα και όταν βρίσκεται υπό μεγάλης έντασης DoS Attacks καταφέρνει να επιτύχει reliability της τάξης του 95% με παράγοντα w=6. Παρ όλα αυτά, αυτό γίνεται με μεγάλο κόστος στην ασφάλεια του δικτύου, καθώς η αύξηση του παράγοντα w οδηγεί σε πολύ αυξημένες πιθανότητες να γίνει compromised το δίκτυο, αφού ο επιτιθέμενος χρειάζεται μόνο έναν κόμβο. Ενδεικτικά, με 15% των κόμβων να είναι compromised μόλις το 5% των onions θα γίνουν compromised, ωστόσο όταν το ποσοστό ανέβει στο 30%, τα μισα onions θα γίνουν compromised. Παρατηρείται λοιπόν εκθετική αύξηση του insecurity του δικτύου όσο αυξάνουν οι compromised κόμβοι στο δίκτυο. [138]

Το Hydra-Onions λοιπόν είναι μια τεχνολογία ιδιαίτερα ευάλωτη στις Selective DoS Attacks όταν στο δίκτυο συμμετέχουν πολλοί compromised κόμβοι, ωστόσο παρέχουν σημαντικά πλεονεκτήματα όταν ο επιτιθέμενος έχει περιορισμένο αριθμό πόρων, καθώς επιτυγχάνουν μεγάλα ποσοστά αξιοπιστίας και μπορούν να αντιμετωπίσουν επιτυχώς μια συμβατική, εξωτερική Denial of Service Attack.

4. Denial of Service Attacks στο Salsa

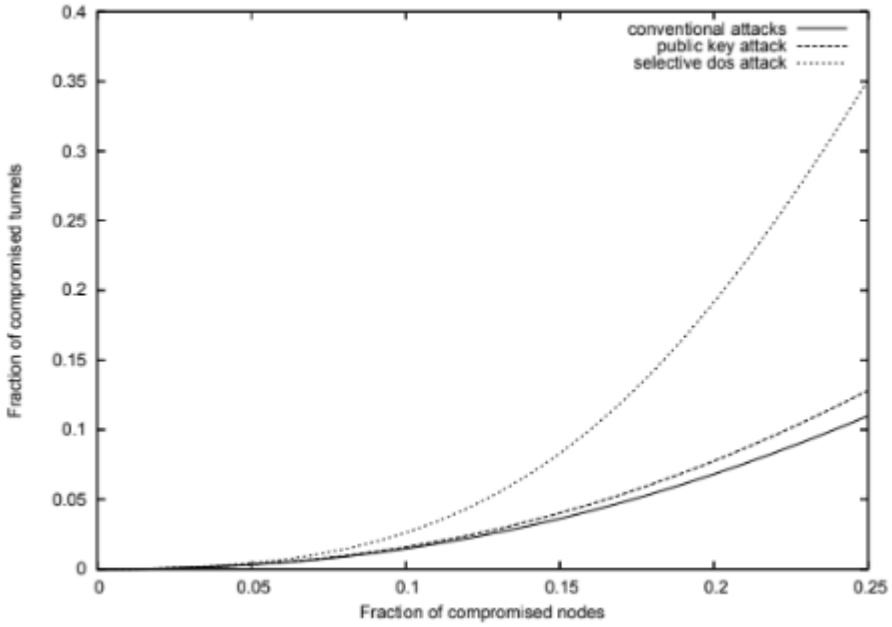
Στο Salsa ένα tunnel θεωρείται compromised αν υπάρχει ένας τουλάχιστον, ελεγχόμενος από τον επιτιθέμενο, κόμβος σε κάθε στάδιο του. Επίσης, το tunnel θεωρείται compromised αν τόσο ο πρώτος όσο και ο τελευταίος κόμβος ελέγχονται από τον επιτιθέμενο. Ο μηχανισμός δημιουργίας tunnels είναι ευάλωτος σε Public Key Modification Attacks. Αν όλοι οι r κόμβοι σε ένα στάδιο γίνουν compromised, ο επιτιθέμενος μπορεί να μεταβάλλει τα keys που χρησιμοποιούνται για το lookup του επόμενου σταδίου, κάτι που αποτρέπει το Salsa να ελέγξει αν η IP Address είναι εντός του σωστού πεδίου, ώστε να συνεχίσει την προώθηση των πακέτων. Η διαδικασία αυτή συνεχίζεται με τον ίδιο τρόπο που υλοποιείται μια Collusion Attack, με αποτέλεσμα το tunnel να χτίζεται εξ ολοκλήρου με κακόβουλους κόμβους. Με τον τρόπο αυτό οι επιτιθέμενοι μπορούν να υλοποιήσουν interception των μηνυμάτων και να αποκαλύψουν την ταυτότητα του Initiator. [113]

Οι Selective Denial of Service Attacks χρησιμοποιούνται για να εξαναγκάσουν το δίκτυο να χτίσει καινούρια tunnels, έως ότου αυτά περιλαμβάνουν compromised κόμβους. Η απόρριψη της σύνδεσης γίνεται εύκολα, με τον κακόβουλο κόμβο να επιστρέφει τυχαία αποτελέσματα σε lookups που υλοποιούνται από tunnels που δεν έχουν γίνει compromised ακόμα. Η επίθεση γίνεται σε δύο φάσεις. Αρχικά η DoS Attack γίνεται όταν ο τελευταίος κόμβος του tunnel είναι honest ενώ στο αμέσως προηγούμενο tunnel υπάρχει ένας compromised κόμβος αλλά οι υπόλοιποι είναι honest. Στη δεύτερη φάση, ο επιτιθέμενος διακόπτει την δικτυακή κίνηση προς οποιονδήποτε κόμβο αν το tunnel δεν είναι compromised. [126]

Οι κακόβουλοι κόμβοι υλοποιούν ανάλυση της δικτυακής κίνησης στο πρώτο τμήμα του stream και συσχετίζουν τα αποτελέσματα με αυτά όλων των υπολοίπων streams. Αν η ανάλυση οδηγήσει σε σαφή σύνδεση ενός Initiator και ενός Recipient, τότε η προώθηση των μηνυμάτων συνεχίζεται κανονικά. Σε αντίθετη περίπτωση, διακόπτεται η σύνδεση ώστε να δημιουργηθούν νέα tunnels. Ο αλγόριθμος υλοποίησης της επίθεσης είναι ο παρακάτω:

if a stage is completely compromised **then**
  emulate remaining hops via public key modification attack
else
  if the second-to-last stage has an attacker and the last node being looked is honest **then**
    return arbitrary information to DoS the tunnel
  else
    return correct results
  end if
end if
if attacker selected to forward traffic **then**
  perform traffic analysis
end if
if attackers cannot identify the source and destination of the tunnel after a timeout **then**
  stop forwarding traffic on that tunnel
end if

Το Salsa είναι εξαιρετικά ευάλωτο απέναντι σε Selective Denial of Service Attacks, οδηγώντας σε δραματική μείωση τα επίπεδα προστασίας της ανωνυμίας των χρηστών. Οι μηχανισμοί που αποτρέπουν τις Public Key Modification Attacks, ορίζοντας στο δίκτυο συγκεκριμένες τιμές στις ιδιότητες του, διευκολύνουν σημαντικά τον επιτιθέμενο στο να αποκτήσει πρόσβαση σε κάθε στάδιο της δημιουργία του tunnel. Στο παρακάτω διάγραμμα παρουσιάζεται ο κίνδυνος για τις συνηθέστερες επιθέσεις στο δίκτυο, ανάλογα με το ποσοστό των compromised κόμβων που βρίσκονται σε αυτό.



Σχήμα 3.42: Ποσοστό compromised κόμβων στο Salsa.

Οι ιδανικές τιμές για το l είναι 2 και 3, προκειμένου να επιτευχθεί το μέγιστο δυνατό επίπεδο προστασίας απέναντι στις Selective DoS Attacks. Αύξηση της παραμέτρου αυτής πέραν των τιμών αυτών δεν έχει κανένα απολύτως αποτέλεσμα. Μια λύση για την προστασία του δικτύου θα ήταν η επίλυση των conflicts να γίνεται μέσω της συμμετοχής της πλειοψηφίας των κόμβων και όχι ομόφωνα, καθώς στην παρούσα υλοποίηση, ένας μόνο κόμβος αρκεί για να αρνηθεί την υπηρεσία σε ένα tunnel, αναγκάζοντας το δίκτυο να δημιουργήσει νέο, κάτι που διευκολύνει το έργο του επιτιθέμενου. [138]

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Selective Denial of Service Attacks

Οι Selective Denial of Service Attacks είναι ιδιαιτέρως επικίνδυνες και μπορούν να επιφέρουν σημαντικά πλήγματα στη διατήρησης της ανωνυμίας των χρηστών. Η αξιοπιστία του δικτύου λοιπόν διαμορφώνεται συνολικά από δύο παράγοντες, τη διαθεσιμότητα, η οποία πλήττεται από τις DoS Attacks και την ασφάλεια των επικοινωνιών. Ευρέως χρησιμοποιούμενα δίκτυα όπως το Tor αποδεικνύονται πολύ ευάλωτα σε τέτοιου είδους επιθέσεις. Μάλιστα, οι τεχνολογίες που δίνουν βάρος στην υψηλή διαθεσιμότητα της υπηρεσίας φαίνεται να ενισχύουν το μηχανισμό της επίθεσης, διευκολύνοντας τον επιτιθέμενο να κάνει compromise ένα tunnel. [114] [125]

Η προστασία του πρώτου και του τελευταίου tunnel είναι ζωτικής σημασίας, αφού είναι κόμβοι που μπορούν να υπονομεύσουν σημαντικά τη ανωνυμία των χρηστών, ενώ αποτελούν και πρόσφορο έδαφος για την υλοποίηση και άλλων επιθέσεων, όπως είναι οι Predecessor Attacks. Η χρήση διαφόρων reputation systems θα μπορούσε επίσης να δρα ανασταλτικά για τυχόν κακόβουλους κόμβους στο δίκτυο, υποχρεώνοντας τους να αποχωρήσουν από αυτό αν γίνει αντιληπτή μη φυσιολογική συμπεριφορά τους όσον αφορά τη δρομολόγηση μηνυμάτων. [111] Κάτι τέτοιο ωστόσο δεν είναι πάντα απλό, καθώς για μεγάλα μήκη μονοπατιού, δεν είναι πάντα ευδιάκριτο ποιο router/mix είναι υπεύθυνο για την απόρριψη της δικτυακής κίνησης.

Σε κάθε περίπτωση, μηχανισμοί που εγγυώνται ότι οι μη αξιόπιστοι κόμβοι θα ανιχνεύονται εγκαίρως ή ότι η πλειοψηφία των κόμβων του δικτύου θα είναι honest θα πρέπει να εισαχθούν σε όλες τις τεχνολογίες ανωνύμων επικοινωνιών, προκειμένου να αντιμετωπιστούν οι σοβαρές συνέπειες των DoS επιθέσεων και να διασφαλιστεί η ανωνυμία των χρηστών του. Ειδικότερα οι peer-to-peer εφαρμογές, λόγω της πολυπλοκότητας που τις χαρακτηρίζει, μπορούν να δώσουν περισσότερους attack vectors στους επιτιθέμενους.

3.1.3.3 Message Tagging/Replay Attacks

Εισαγωγικά Στοιχεία

Σε πολλές από τις Passive Attacks γίνεται προφανές ότι ο επιτιθέμενος προσπαθεί να εκμεταλλευτεί τις πληροφορίες που διαρρέουν από το δίκτυο μέσω της καθυστέρησης (latency) που παρατηρείται στο δίκτυο ή μέσω της μέτρησης των χρόνων αναχώρησης και άφιξης των διαφόρων μηνυμάτων. Οι Message Tagging Attacks είναι στην ουσία η εξέλιξη της κατηγορίας αυτής επιθέσεων σε Active Attacks.

Στην προκειμένη περίπτωση ο επιτιθέμενος δεν περιορίζεται απλά στην παθητική παρατήρηση των διακινούμενων στο δίκτυο πακέτων, αλλά προκαλεί ο ίδιος μικρές μεταβολές σε αυτά με σκοπό να είναι σε θέση να τα ανιχνεύσει ευκολότερα κατά τη διαδρομή τους στο δίκτυο, καθιστώντας έτσι την ανάλυση της δικτυακής κίνησης μη αναγκαία προκειμένου να ταυτοποιήσει είτε τον Initiator είτε τον Responder. Το tagging των μηνυμάτων μπορεί να γίνει είτε τροποποιώντας ελαφρά συγκεκριμένα τμήματα της επικεφαλίδας τους, είτε εξαναγκάζοντας τα μηνύματα σε επανάληψη, εξού και η εναλλακτική ονομασία των επιθέσεων αυτών ως Replay Attacks. [4] [8] [35] [101]

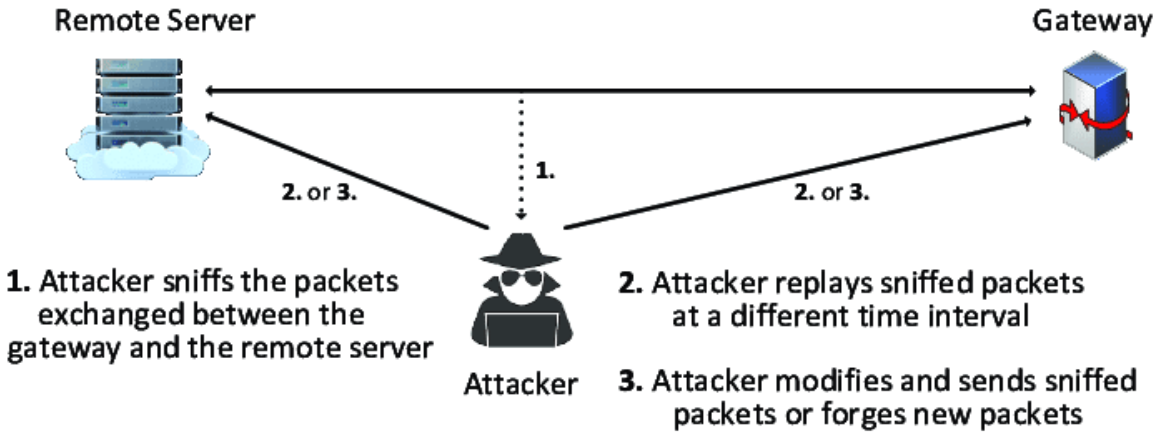
Οι επιθέσεις αυτές απαιτούν από τον επιτιθέμενο να έχει τον έλεγχο του πρώτου κόμβου στο μονοπάτι, ο οποίος και υλοποιεί το tagging, καθώς και του τελευταίου, ο οποίος ανιχνεύει τα τροποποιηθέντα μηνύματα και υλοποιεί τη μαθηματική ανάλυση της δικτυακής κίνησης. Η υλοποίηση τέτοιων επιθέσεων επηρεάζει, σε διαφορετικό βαθμό, σχεδόν όλες τις τεχνολογίες ανωνύμων επικοινωνιών και αποτελούν σημαντικό παράγοντα της υποβάθμισης της ανωνυμίας των χρηστών τους. [40] Η αντιμετώπιση τους είναι εφικτή μέσω της εισαγωγής μιας πολύ αυστηρής δομής στα μηνύματα που διακινούνται στο δίκτυο, τέτοια ώστε να καθιστά το tagging τους ανέφικτο, ωστόσο τέτοιες τεχνικές έχουν υψηλό κόστος ενώ δεν είναι πάντα δυνατό να εφαρμοστούν. [98]

Θα πρέπει να τονιστεί ότι οι επιθέσεις αυτές δεν εντάσσονται στις Traffic Analysis Attacks, καθώς το tagging επιτρέπει στον επιτιθέμενο να συσχετίσει τη δικτυακή κίνηση μεταξύ των Initiator και Responder πολύ εύκολα και γρήγορα. Επίσης, άξιο αναφοράς είναι ότι στην περίπτωση που το tagging υλοποιείται μέσω του playback των μηνυμάτων, δηλαδή έχουμε μια Replay Attack τότε εκτός από την υπονόμευση της ανωνυμίας των χρηστών πλήττεται και η διαθεσιμότητα των δικτύων ανωνύμων επικοινωνιών. [120]

Μοντέλο Επιθέσεων

Στόχος των Message Tagging Attacks είναι να επιβεβαιώσει ο επιτιθέμενος ότι ένας Initiator συνομιλεί με έναν Responder. Η συνομιλία αυτή αναφέρεται σε ένα ευρύ πλήθος εφαρμογών και τεχνολογιών ανωνύμων επικοινωνιών. Έτσι, ο επιτιθέμενος μπορεί να επαληθεύσει με τις επιθέσεις αυτές ότι δύο χρήστες ανταλλάσουν ηλεκτρονική αλληλογραφία, σε δίκτυα high-latency, είτε δύο

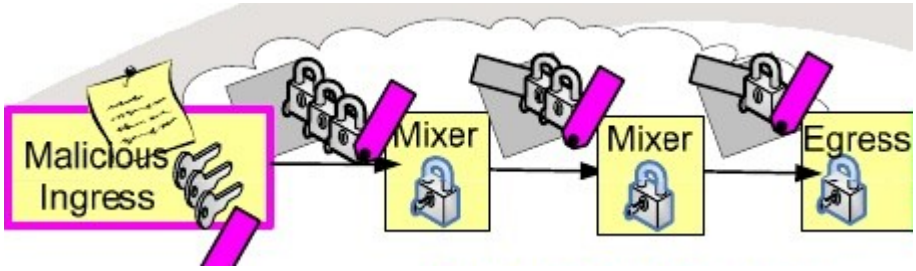
χρήστες που χρησιμοποιούν anonymous chatting υπηρεσίες μέσω κάποιου από τα πρωτόκολλα ανωνύμων επικοινωνιών που έχουν αναλυθεί στο πρώτο μέρος της παρούσας εργασίας, είτε να ανιχνεύσει την ανταλλαγή πακέτων και να επαληθεύσει τη χρήση ενός hidden ή μη service από έναν χρήστη του Tor Network. [130] [142]



Σχήμα 3.43: Replay Attack.

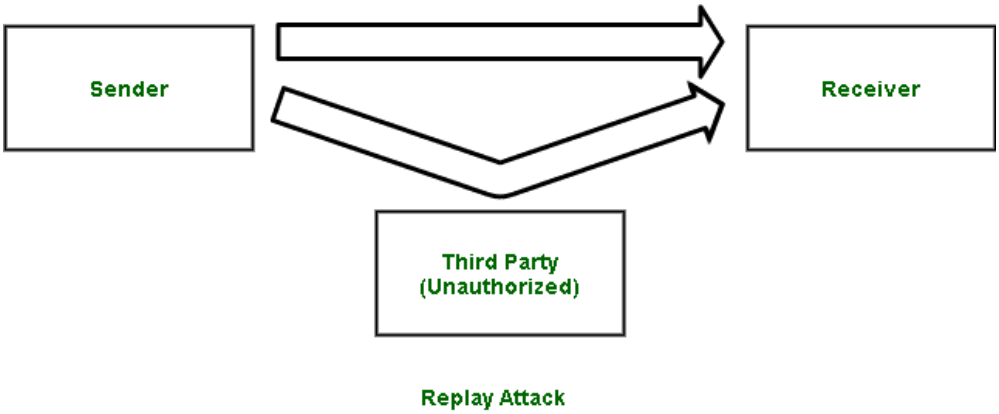
Βασική προϋπόθεση για την επιτυχία τέτοιων επιθέσεων είναι να είναι σε θέση ο επιτιθέμενος να έχει τον έλεγχο του entry και exit κόμβου του εκάστοτε δικτύου. Η επίθεση ξεκινάει από τον entry node. Ο επιτιθέμενος αρχικά επιδιώκει να ταυτοποιήσει ένα πακέτο από το TCP stream στο κύκλωμα και να τροποποιήσει την επικεφαλίδα του είτε να δημιουργήσει ένα αντίγραφο του. [10] Η επίθεση αυξάνει τις πιθανότητες επιτυχίας της αναλόγως των κόμβων που ελέγχει ο επιτιθέμενος στο δίκτυο, καθως αυτό του επιτρέπει να έχει μεγαλύτερο έλεγχο στους μηχανισμούς ελέγχου και επεξεργασίας της επικεφαλίδας ή των αντιγράφων των μηνυμάτων. [63]

Σε περίπτωση που ο επιτιθέμενος επιλέξει την τροποποίηση των μηνυμάτων (tagging), υπάρχουν διάφορες παραλλαγές τους, ανάλογα με τα στοιχεία που τροποποιούνται σε αυτά. Έτσι, ο επιτιθέμενος μπορεί να τροποποιήσει ορισμένα τμήματα του ciphertext και στη συνέχεια να χρησιμοποιήσει διάφορα integrity checks, βασισμένο για παράδειγμα σε ένα hash, το οποίο περιέχεται στο μήνυμα. [80] [86] Η τροποποίηση θα μπορούσε επίσης να ανιχνευθεί στην τελική αποκρυπτογράφηση του μηνύματος, καθώς αν έχει τροποποιηθεί ελαφρώς το ciphertext και το τελικό αποκρυπτογραφημένο μήνυμα παρουσιάζει ανωμαλίες, ο επιτιθέμενος μπορεί να επιβεβαιώσει τη συνομιλία μεταξύ των δύο συμμετεχόντων. Οι παραπάνω επιθέσεις είναι ιδιαίτερα χρήσιμες σε high-latency email exchange πρωτόκολλα ανωνύμων επικοινωνιών, καθώς το plaintext των μηνυμάτων είναι πολύ πιο εύκολο να ελεγχθεί για την ορθότητα του. [90]



Σχήμα 3.44: Message Tagging Attacks σε Email Exchange Anonymous System.

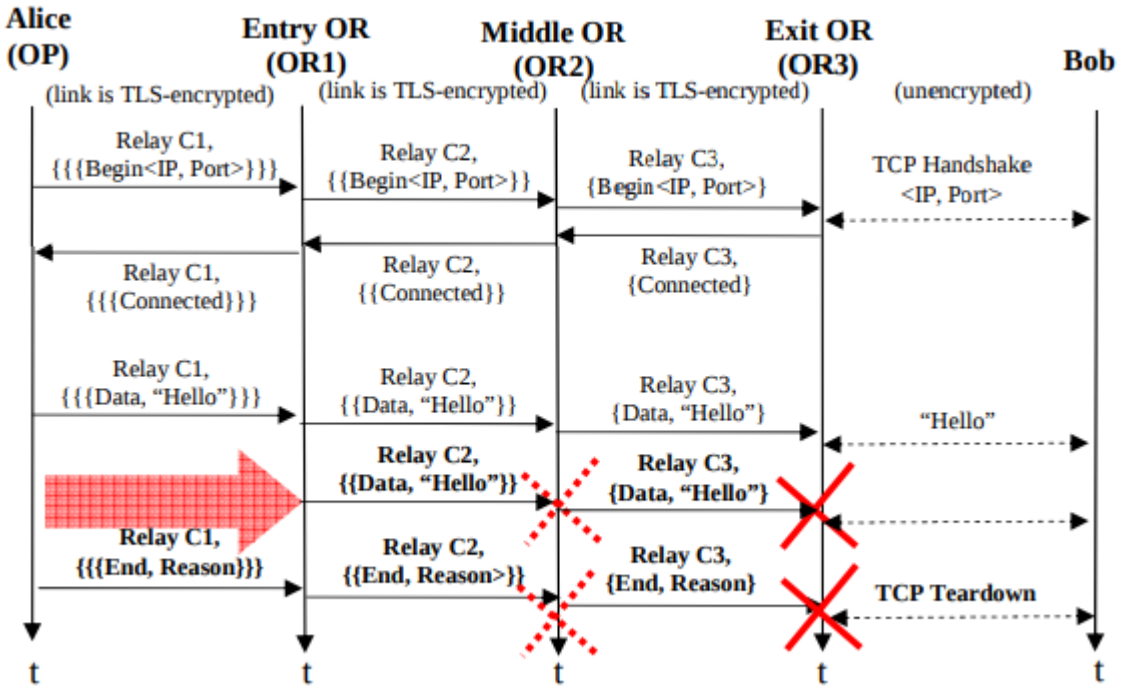
Στην άλλη παραλλαγή των επιθέσεων αυτών, όπου ο επιτιθέμενος επιλέγει να δημιουργήσει αντίγραφο ενός μηνύματος, τότε κατά τη διάρκεια δημιουργίας του καταγράφονται τόσο η IP Address της πηγής όσο και το timestamp του. Όταν το μήνυμα διασχίσει το δίκτυο και φτάσει στον exit node τότε εκείνος θα παρατηρήσει δύο ίδια μηνύματα με διαφορετικά timestamps, κάτι που θα οδηγήσει σε error. [58] Μέσω του error αυτού ο επιτιθέμενος είναι σε θέση να καταγράψει την ώρα δημιουργίας του καθώς και την IP Address και το Port του αυθεντικού μηνύματος. Έτσι επιβεβαιώνει με αυτό τον τρόπο την επικοινωνία των δύο μερών, αφού ο entry node γνωρίζει τον Initiator, και ο exit node γνωρίζει τον Responder. [62]



Σχήμα 3.45: Παράδειγμα Replay Attack.

Στην παραπάνω περίπτωση, το error δημιουργείται γιατί στους κόμβους από τους οποίους διέρχεται ένα μήνυμα και οι οποίοι είναι υπεύθυνοι για τη διαδοχική κρυπτογράφηση/αποκρυπτογράφηση των μηνυμάτων, διατηρείται ένα counter των μηνυμάτων που διακινούνται από την ίδια πηγή με τα ίδια χαρακτηριστικά (ουσιαστικά ως πηγή εκλαμβάνεται ο προηγούμενος κόμβος και ως χαρακτηριστικά συγκεκριμένα πεδία της επικεφαλίδας του που αντιστοιχούν σε συγκεκριμένο data flow), με κάθε μήνυμα να το αυξάνει κατά ένα. Γίνεται λοιπόν αντιληπτό ότι η χρήση διπλότυπων μηνυμάτων δημιουργεί αποσυγχρονισμό της διαδικασίας κρυπτογράφησης/αποκρυπτογράφησης των μηνυμάτων, δημιουργώντας errors. [96]

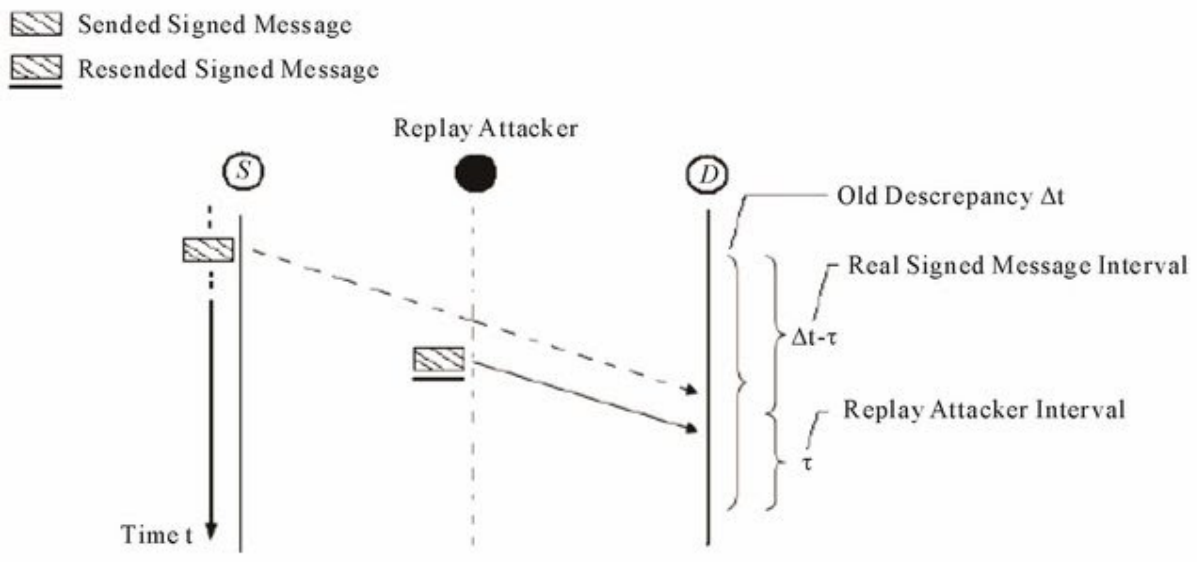
Μεγάλη προσοχή θα πρέπει να δοθεί στην επιλογή των μηνυμάτων τα οποία θα μεταβληθούν ή θα γίνουν πηγή αντιγράφων. Αν επιλεχθούν μηνύματα τα οποία ανταλλάσονται κατά τη διάρκεια δημιουργίας του anonymous tunnel τότε τόσο η τροποποίηση τους όσο και η δημιουργία και διακίνηση στο δίκτυο αντιγράφων τους θα προκαλέσουν errors τα οποία θα οδηγήσουν στη διακοπή χρήσης του εν λόγω tunnel, καθιστώντας το μη λειτουργικό. Είναι εξαιρετικά σημαντικό τα πακέτα αυτά να αποτελούν μέρος του TCP stream. [102] [120] Τα μηνύματα αυτά κρυπτογραφούνται κατά τη διαδρομή τους προς τον τελικό προορισμό, επομένως τα μόνα στοιχεία που είναι γνωστά είναι το circuit ID και το είδος του μηνύματος (control/relay). Καθίσταται λοιπόν προφανές ότι κατά κύριο λόγο τα relay πακέτα είναι αυτά που κατεξοχίν μπορούν να χρησιμοποιηθούν σε τέτοιου είδους επιθέσεις. Ορισμένες Message Tagging Attacks μπορούν να χρησιμοποιήσουν την τροποποίηση control πακέτων, ωστόσο πρόκειται για εξειδικευμένες περιπτώσεις. Παράδειγμα των επιθέσεων αυτών στο Tor Network παρουσιάζεται στην παρακάτω εικόνα:



Σχήμα 3.46: Παράδειγμα ανταλλαγής μηνυμάτων σε μια Replay Attack.

Ο επιτιθέμενος είναι συνήθως σε θέση να γνωρίζει πότε έχει δημιουργηθεί ένα anonymous tunnel, μετά το πέρας του οποίου μπορεί να ξεκινήσει να υλοποιεί μια Message Tagging Attack, γνωρίζοντας τη διαδικασία δημιουργία τους και τι ακριβώς μηνύματα ανταλλάσσονται. [42] Αυτό προϋποθέτει καλή γνώση του πρωτοκόλλου και παρατήρηση των μηνυμάτων που διακινούνται στο δίκτυο. Η παρατήρηση του TCP stream μπορεί να γίνει αν ο επιτιθέμενος εντοπίσει μια σύνδεση από τον exit node προς έναν server, καθώς μια τέτοια σύνδεση σημαίνει ότι ένας client επικοινωνεί με έναν server και έχει ήδη εγκατασταθεί το anonymous tunnel. [50] Αντίστοιχα, η διακοπη επικοινωνίας ενός exit node με έναν server σηματοδοτεί τη λήξη του διαύλου αυτού.

Στην περίπτωση που ο επιτιθέμενος επιλέξει τη δημιουργία και διακίνηση αντιγράφων στο δίκτυο, τότε μπορεί να χρησιμοποιήσει τον compromised exit node για να υλοποιήσει buffering των μηνυμάτων, τα οποία θα μπορέσει να διακινήσει αργότερα, δημιουργώντας πάλι τα αντίστοιχα errors μέσω των οποίων μπορεί να επαληθεύσει την επικοινωνία μεταξύ των δύο στόχων του. Επιπλέον, στην περίπτωση αυτή σημαντική είναι η επιλογή του χρόνου που θα διακινηθούν στο δίκτυο τα αντίγραφα. [70] [112] Η διαδικασία αυτή, όπως έχει ήδη αναφερθεί, προκαλεί διαταραχή στη λειτουργία του δικτύου, η χρήση του συγκεκριμένου tunnel θα διακοπεί και θα επιλεχθούν άλλα για τη συνέχιση της επικοινωνίας. Έτσι, τα αντίγραφα θα πρέπει να αποστέλλονται ενώ δεν υπάρχει κάποια ενεργή TCP σύνδεση και πριν αυτή διακοπεί. Οι επιθέσεις αυτές έχουν ελάχιστο αντίκτυπο στις επιδόσεις του δικτύου και συνεπώς είναι δύσκολο να εντοπιστούν. [130]



Σχήμα 3.47: Παράδειγμα αποστολής αντιγράφων μηνύματος σε μια Replay Attack.

Η επιβεβαίωση της σύνδεσης ενός Initiator με έναν Responder γίνεται με τη χρήση του Network Time Protocol (NTP), μέσω του οποίου συγχρονίζονται οι ώρες των entry και exit nodes. Έτσι, με τη δημιουργία των συσχετίσεων που περιγράφηκαν παραπάνω, μπορεί ο επιτιθέμενος να επιβεβαιώσει ότι δύο χρήστες του δικτύου ανωνύμων επικοινωνιών συνομιλούν μεταξύ τους. Η επιβεβαίωση αυτή είναι ταχύτατη, δεν έχει το υψηλό κόστος που ενδέχεται να έχουν ορισμένες Traffic Analysis Attacks ενώ είναι ιδιαίτερα ανθεκτική απέναντι σε διάφορες τεχνικές προστασίας και ανεξάρτητη από το μέγεθος του δικτύου. [35]

Οι συγκεκριμένες επιθέσεις μπορούν να προκαλέσουν σημαντικά προβλήματα σε διάφορες λειτουργίες των δικτύων ανωνύμων επικοινωνιών, ειδικότερα δε σε αυτές που αποτελούν τους βασικούς πυλώνες για τη διασφάλιση της ανωνυμίας των χρηστών τους. Μια πολύ σημαντική λειτουργία της επίθεσης είναι ότι μπορεί να χρησιμοποιηθεί για την τυχαία δημιουργία προφίλ διαφόρων χρηστών και hidden servers στα δίκτυα. [58] Ο επιτιθέμενος μπορεί να χτίσει ολόκληρο το προφίλ της διαδικτυακής συμπεριφοράς ενός χρήστη, συλλέγοντας πληροφορίες σχετικά με τους ιστότοπους και τις υπηρεσίες που χρησιμοποιεί, καταργώντας ουσιαστικά την ανωνυμία που του προσφέρουν τα συγκεκριμένα δίκτυα. Επιπλέον, οι επιθέσεις αυτές μπορούν να χρησιμοποιηθούν και υποστηρικτικά προς άλλες επιθέσεις, όπως οι Denial of Service και οι Sybil Attacks. [100] [106] [123] [142] Πολλές Message Tagging Attacks δημιουργούν connection errors, τα οποία εκμεταλλεύεται ο επιτιθέμενος. Τα ίδια αυτά errors σηματοδοτούν τη διακοπή χρήσης του συγκεκριμένου tunnel, κάτι που αν γίνεται συνεχώς και εσκεμμένα μετατρέπεται σε Denial of Service Attack. Μάλιστα, όπως έχει αναφερθεί και στο αντίστοιχο κεφάλαιο, η κακόβουλη τροποποίηση μηνυμάτων είναι ο κυριότερος τρόπος πρόκλησης διακοπής συνδέσεων στην περίπτωση των Selective DoS Attacks. [148]

Τέλος, αξίζει να αναλυθεί η επίδραση του θορύβου των δικτύων στις συγκεκριμένες επιθέσεις, καθώς και ο αντίκτυπος που αυτός έχει στα αποτελέσματα τους. Ως θόρυβος στις Message tagging Attacks ορίζεται το σύνολο των decryption errors ή των taggings που έγιναν όχι υπευθύνη του επιτιθέμενου, αλλά λόγω σφαλμάτων που συμβαίνουν στους διάφορους κόμβους του δικτύου. [23] Τα τυχαία σφάλματα αυτά είναι πράγματι σπάνια, καθώς τα δίκτυα ανωνύμων επικοινωνιών στο σύνολο τους επιστρατεύουν ισχυρά πρωτόκολλα που διασφαλίζουν την ακεραιότητα των μηνυμάτων και την

προστασία της από τυχαία σφάλματα του δικτύου. Ειδικότερα στην περίπτωση των Replay Attacks ο επιτιθέμενος μπορεί να αυξήσει έτι περαιτέρω το ποσοστό επιτυχίας των επιθέσεων αυτών επιλέγοντας το κατάλληλο πλήθος μηνυμάτων που πρέπει να στείλει στο δίκτυο. [90]

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Message Tagging Attacks

Το Mixmaster είναι από τα πρώτα δίκτυα που εισήγαγε τρόπους αντιμετώπισης των συγκεκριμένων επιθέσεων. Οι μέθοδοι αυτοί επικεντρώνονται στην ανίχνευση πιθανών μεταβολών στα μηνύματα που διακινούνται μέσω του δικτύου, έτσι ώστε αυτά να απορρίπτονται σε περίπτωση που υπάρξει τροποποίηση σε αυτά από κάποιον επιτιθέμενο. [33] Αυτό πρακτικά γίνεται με την ντετερμινιστική δημιουργία των μηνυμάτων, δημιουργώντας το απαιτούμενο padding χρησιμοποιώντας ένα διαμοιραζόμενο (shared) κλειδί και στέλνοντας ένα hash που χαρακτηρίζει ολόκληρο το μήνυμα σε όλα τα ενδιάμεσα mixes. Αυτό φυσικά προϋποθέτει να υλοποιείται έλεγχος της ακεραιότητας των μηνυμάτων σε κάθε ενδιάμεσο κόμβο του δικτύο. Ο έλεγχος της ακεραιότητας μόνο στον τελευταίο κόμβο δεν είναι η βέλτιστη πρακτική ασφάλειας για την αντιμετώπιση των συγκεκριμένων επιθέσεων, καθώς αυτός μπορεί να είναι compromised και να ελέγχεται από κάποιον επιτιθέμενο. [51] Έτσι, η αντιμετώπιση των Message Tagging Attacks προϋποθέτει μια κατανεμημένη, peer-to-peer προσέγγιση ώστε να υπάρχει έλεγχος καθ όλο το μονοπάτι.

Φυσικά, οι μέθοδοι αυτοί δεν είναι πάντα δυνατό να εφαρμοστούν κατ απόλυτο τρόπο. Το Mixmaster επί παραδείγματι υποστηρίζει μη-διακριτά (indistinguishable) απαντήσεις, επομένως η παραπάνω στρατηγική δε δύναται να χρησιμοποιηθεί για την ανίχνευση αλλαγών στο σώμα του μηνύματος, αφού αυτό τροποποιείται έτσι ώστε να φέρει το περιεχόμενο της απάντησης. [46] Έτσι, η μέθοδος αυτή χρησιμοποιείται για την προστασία των headers του μηνύματος, ωστόσο δε μπορεί να χρησιμοποιηθεί και για την προστασία της ακεραιότητας του ίδιου του σώματος. [47] Πολύ σημαντικό επίσης είναι να προστατεύεται η ακεραιότητα τόσο του forward όσο και του reply path, έτσι ώστε να αποκλειστεί κάθε ενδεχόμενο να τροποποιηθεί από κάποιον κακόβουλο χρήστη που ενδεχομένως ελέγχει έναν ενδιάμεσο κόμβο.

Το Mixminion επιστρατεύει μια ελαφρως τροποποιημένη εκδοχή της παραπανω στρατηγικής προκειμένου να προστατευθεί από τέτοιου είδους επιθέσεις. Αν το σώμα του μηνύματος έχει τροποποιηθεί, το μήνυμα μπορεί να υποστεί σωστή επεξεργασία, ωστόσο το τελικό περιεχόμενο δε θα είναι σε θέση να δώσει πληροφορίες στον επιτιθέμενο σχετικά με το περιεχόμενο του ή τον τελικό του προορισμό. [65] [67] Αυτό πρακτικά σημαίνει ότι αν και ο επιτιθέμενος είναι σε θέση να τροποποιήσει το μήνυμα με τρόπο τέτοιο ώστε να μην ανιχνεύεται από τους μηχανισμούς του δικτύου, η αλλοίωση του μηνύματος είναι τόσο μεγάλη που πρακτικά είναι αδύνατο να εξάγει πληροφορίες σχετικά με το περιεχόμενο ή ακόμα και τον αρχικό ή τελικό προορισμό του. [70]

Το παραπάνω επιτυγχάνεται με τη χρήση large block ciphers για την κωδικοποίηση του δεύτερου header και του σώματος του μηνύματος, δημιουργώντας τη μέγιστη δημιουργία λαθών σε αυτά, σε περίπτωση που τροποποιηθούν από έναν κακόβουλο χρήστη. [6] Επιπροσθέτως, η κωδικοποίηση των παραπάνω στοιχείων είναι διασυνδεδεμένη, με αποτέλεσμα η τροποποίηση του ενός να μετατρέπει το σύνολο του μηνύματος ουσιαστικα σε τυχαίο θόρυβο. Τόσο το πρώτο όσο και το δεύτερο header του μηνύματος είναι αδύνατο να τροποποιηθούν, καθώς περιέχουν ένα gigest που ανιχνεύει τυχόν τροποποιήσεις σε αυτά. [12] Οποιαδήποτε τροποποίηση στους headers ενός πακέτου αυτομάτως οδηγείσ την απόρριψη τους. Αυτό φυσικά περιορίζεται στους headers μόνο του μηνύματος, σε αντίθεση με το Mixmaster στο οποίο περιλαμβάνει και το σώμα του.

Αν ο επιτιθέμενος επιλέξει να τροποποιήσει το σώμα του μηνύματος, τότε επιστρατεύονται οι counter-intuitive swap λειτουργίες του δικτύου. Έτσι, αν ο επιτιθέμενος τροποποιήσει το σώμα του μηνύματος πριν υλοποιηθεί η swap λειτουργία, τότε το δεύτερο header που περιέχει τον τελικό προορισμό και το σώμα του κειμένου θα αλλοιωθούν σημαντικά, τόσο ώστε να μετατραπούν σε τυχαίο δικτυακό θόρυβο, όπως περιγράφηκε και πιο πάνω. Αν ο επιτιθέμενος τροποποιήσει το σώμα μετά τη swap λειτουργία τότε το μήνυμα έχει αποκτήσει ήδη επαρκή ανωνυμία και δεν κινδυνεύει να γίνει compromised. [99]

Θα πρέπει να τονιστεί ότι το σύνολο των τεχνικών αυτών, που αφορούν στην προστασία μεμονωμένων μηνυμάτων, δεν επεκτείνονται και στην περίπτωση που ο επιτιθέμενος επιχειρήσει να κάνει tagging πολλαπλών μηνυμάτων που ανήκουν στην ίδια ροή πακέτων. [45] [49] [58] Στην περίπτωση αυτή, αν και το πρώτο τροποποιημένο μήνυμα μπορεί να χάσει την πληροφορία που φέρει, τα υπόλοιπα μηνύματα που ανήκουν στην ίδια ροή μπορούν να φέρουν ευδιάκριτες πληροφορίες. Οι επιθέσεις αυτές είναι πιθανό να συμβούν σε όλες τις τεχνολογίες ανωνύμων επικοινωνιών που χρησιμοποιούν forward error-correction κώδικες (FEC codes) για τη διασφάλιση της ακεραιότητας των μηνυμάτων. [60]

Τέλος, θα πρέπει να γίνει σαφές ότι δεν παρέχουν όλες οι Message Tagging Attacks την ίδια ποιότητα και ποσότητα πληροφορίας στον επιτιθέμενο. Η χρήση κρυπτογραφικού σχήματος παίζει πρωτεύοντα ρόλο στην αποτελεσματικότητα των επιθέσεων αυτών. Η χρήση BEAR κρυπτογραφικών σχημάτων διασφαλίζει ότι σε τυχόν τροποποίηση ενός μηνύματος, είτε στους headers είτε στο σώμα, η τελική αποκρυπτογράφηση οδηγεί σε ένα τελείως τυχαίο αποτέλεσμα το οποίο δεν είναι δυνατό να παρέχει πληροφορίες στον επιτιθέμενο. [70] Αυτό μάλιστα σημαίνει ότι τα tagged messages δε μπορούν να συσχετιστούν μεταξύ τους, με αποτέλεσμα κάθε στιγμή να μπορεί να συμβεί στο δίκτυο μόνο μια Message Tagging Attack, αφού ακόμα και μια επίθεση σε όλα τα μηνύματα μια ροής δεδομένων θα παράγει εντελώς διαφορετικά αποτελέσματα μεταξύ των μηνυμάτων. [71] [72] [73]

Η χρήση και μόνο του BEAR διασφαλίζει ότι σε περίπτωση εκδήλωσης τέτοιων επιθέσεων θα υπάρχει η ελάχιστη δυνατή διαρροή πληροφοριών που δύσκολα θα επιφέρει κάποιο όφελος στον επιτιθέμενο. Τεχνικές όπως η εισαγωγή δύο headers και swap point ενισχύουν την ασφάλεια του δικτύου αν και έχουν επιπτώσεις στις επιδόσεις του. [91]

Το Tor Network, όντας ευάλωτο σε end-to-end επιθέσεις αντιμετωπίζει προβλήματα από τις Message Tagging Attacks. [8] Η εφαρμογή των παραπάνω τεχνικών δεν είναι εφικτές στο συγκεκριμένο δίκτυο, αφού οι Onion Routers δε μπορούν να υλοποιήσουν τα παραπάνω hashes που χρησιμοποιούνται για τον έλεγχο ακεραιότητας, καθώς δε γνωρίζουν τα session keys των υπολοίπων routers στο δίκτυο. Ο έλεγχος ακεραιότητας των μηνυμάτων μέσω των παραπάνω μεθόδων θα οδηγούσε σε μεγέθυνση του μηνύματος σε κάθε hop, κάτι που επιβαρύνει σημαντικά το δίκτυο. Για τον περιορισμό της επιβάρυνσης αυτής είτε θα έπρεπε να αποκαλύπτεται εξ αρχής το όνομα του μονοπατιού, είτε να γίνεται padding μέχρι ένα προκαθορισμένο επίπεδο. [10] [18]

Έτσι, η ακεραιότητα των μηνυμάτων ελέγχεται μόνο στα άκρα του κάθε data stream. Κάθε φορά που δημιουργείται ένα νέο hop, δημιουργείται ένα SHA-1 digest με ένα παράγωγο του κλειδιού που χρησιμοποιείται, με αποτέλεσμα να προστίθενται σε αυτό όλα τα relay cells που δημιουργούνται. Το SHA-1 digest αυτό χρησιμοποιείται για την επιβεβαίωση της ακεραιότητας των μηνυμάτων που ανταλλάσσονται. [14] [15] Για να είναι σε θέση ο επιτιθέμενος να γνωρίζει ποια cells πρέπει να τροποποιήσει πρέπει να γνωρίζει το digest state. Ο επιτιθέμενος δεν είναι σε θέση να τροποποιήσει το

hash με τρόπο τέτοιο ώστε να παραχθεί ένα νέο, έγκυρο hash, καθώς αυτά υπόκεινται σε end-to-end κρυπτογράφηση κατά μήκος του δικτύου. Επίσης, οι Onion Routers και οι Onion Proxies θα σταματήσουν τη χρήση ενός anonymous tunnel όταν εντοπίσουν ένα τροποποιημένο hash. [23]

Η αντιμετώπιση των Replay Attacks στα δίκτυα ανωνύμων επικοινωνιών μπορεί να γίνει με την ελαχιστοποίηση των κακόβουλων entry nodes. [111] Ο path selection αλγόριθμος θα πρέπει να είναι πολύ αυστηρός στην επιλογή των κόμβων που θα τοποθετηθούν πρώτοι στο μονοπάτι, διασφαλίζοντας την ακεραιότητα τους. Επίσης, σημαντική είναι η θωράκιση του δικτύου από Sybil Attacks, οι οποίες μπορούν να ανεβάσουν τη δημοτικότητα ορισμένων malicious nodes, διαφημίζοντας μη αληθές bandwidth, με αποτέλεσμα να επιλέγονται οι κόμβοι αυτοί ως Guard nodes. [2] [10] Η εισαγωγή ενός reputation system επίσης θα βοηθούσε στην αντιμετώπιση των επιθέσεων αυτών. Ακόμα μια επιλογή αποτελεί η παρακολούθηση του δικτύου για τυχόν ύπαρξη duplicate cells. Το buffering των cells σε έναν ενδιάμεσο κόμβο και η σύγκριση με τα διερχόμενα από αυτόν μηνύματα θα μπορούσε να δώσει λύση σε αυτό το πρόβλημα, ωστόσο τίθεται ζήτημα επιπλέον overhead στο δίκτυο. [18] [20] [26] Τέλος, μια ακόμα λύση που χρησιμοποιείται σε πολλές περιπτώσεις επιθέσεων είναι η παρακολούθηση του δικτύου για συχνές αλλαγές των χρησιμοποιούμενων anonymous tunnels, που σαφώς υποδεικνύει ότι ενδεχομένως να υπάρχει κάποια κακόβουλη δραστηριότητα στο δίκτυο. Επίσης, συχνά decryption errors μπορούν να είναι αποτέλεσμα μιας τέτοιας επίθεσης.

3.1.3.4 Active Timing Attacks

Εισαγωγικά Στοιχεία

Οι Timing Attacks, όπως έχει ήδη αναλυθεί και στο κεφάλαιο των Passive Attacks, αποτελούν μια από τις πιο χαρακτηριστικές Traffic Analysis Attacks στα δίκτυα ανωνύμων επικοινωνιών και είναι ικανές να επιφέρουν σημαντικά πλήγματα στην ασφάλεια τους. Ο επιτιθέμενος επιχειρεί να παρατηρήσει τις εισερχόμενες και τις εξερχόμενες ροές πακέτων σε κάποιον χρήστη και προς κάποιον compromised κόμβο του δικτύου, έτσι ώστε υλοποιήσει συσχετίσεις των timing patterns των πακέτων που διακινούνται μέσω αυτού.

Οι επιθέσεις, εκτός από την Passive μορφή τους, μπορούν πολύ εύκολα να μετατραπούν σε Active Attacks αυξάνοντας σημαντικά την αποτελεσματικότητα τους, αντιμετωπίζοντας μάλιστα σημαντικές γραμμές άμυνας του δικτύου, όπως η παραγωγή dummy packets και η εισαγωγή τεχνητής καθυστέρησης στα πακέτα που διακινούνται σε αυτό. Στην περίπτωση αυτή, ο επιτιθέμενος εισάγει ο ίδιος τα δικά του timing patterns στη δικτυακή κίνηση που διέρχεται μέσω των compromised routers που εκείνος ελέγχει. [201]

Αποτέλεσμα της συγκεκριμένης παραλλαγής των Timing Attacks είναι οι τεχνολογίες ανωνύμων επικοινωνιών, ιδιαίτερα δε εκείνες που εστιάζονται σε low-latency εφαρμογές , να αντιμετωπίζουν σοβαρά προβλήματα ασφαλείας, καθώς καμία εξ αυτών δεν είναι σε θέση να τις αντιμετωπίσει. Στην περίπτωση που ο επιτιθέμενος καταφέρει να ελέγξει κάποιους routers με τους οποίους επικοινωνεί απευθείας ο Initiator ή εκείνοι επικοινωνούν απευθείας με τον Destination, μπορεί να χρησιμοποιήσει τις επιθέσεις αυτές για να επιφέρει σημαντικά πλήγματα στην προστασία της ανωνυμία των χρηστών του.

Αξίζει να αναφερθεί ότι υπάρχουν διάφοροι τρόποι υλοποίησης των συγκεκριμένων επιθέσεων. Εκτός από την απλή προσθήκη καθυστέρησης στα πακέτα που διέρχονται από έναν compromised router, ο

επιτιθέμενος μπορεί να στέλνει ριπές πακέτων (bursts of traffic) στους routers, προκειμένου να προσδώσει ορισμένα delay patterns στα πακέτα, ώστε να καταφέρει να αναγνωρίσει επιτυχώς τους routers που απαρτίζουν ένα συγκεκριμένο μονοπάτι. Επιπλέον, το ping μπορεί επίσης να χρησιμοποιηθεί για την αναγνώριση των timing patterns σε διάφορους routers. [194] [195]

Εξαιρετικά ενδιαφέρουσα είναι επίσης η περίπτωση στην οποία χρησιμοποιούνται Denial of Service επιθέσεις, προκειμένου να εξαναγκαστεί ο χρήστης, μέσω της απόρριψης των πακέτων, να χρησιμοποιήσει κυκλώματα στα οποία ο επιτιθέμενος έχει compromised routers. Επιπλέον, μπορούν να συνδυαστούν με Latency Attacks, καθώς μέσω τεχνητού congestion που προέρχεται από τον επιτιθέμενο, μπορεί να αναγνωριστούν διακριτά latencies μεταξύ των διαφορετικών χρηστών του δικτύου.

Μοντέλο Επιθέσεων

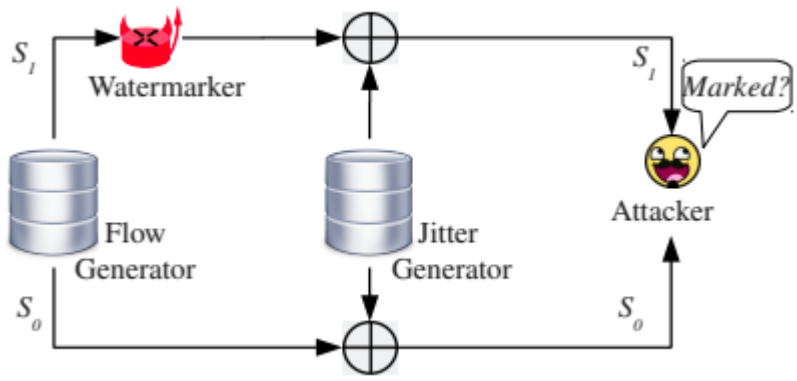
Στο συγκεκριμένο μοντέλο επίθεσης, θεωρούμε ότι ο χρήστης δεν έχει τη δυνατότητα να παράγει νέα πακέτα ή να αντιγράφει ήδη υπάρχοντα, κάτι που υλοποιείται ουσιαστικά στις Message Tagging/Replay Attacks. Στις συγκεκριμένες επιθέσεις, ο επιτιθέμενος επιχειρεί την απλή εισαγωγή του δικού του, διακριτού timestamp στα διακινούμενα πακέτα, προκειμένου να μπορέσει να τα διακρίνει σε άλλους συνδέσμους ή routers του δικτύου. Οι επιθέσεις αυτές μπορούν να υλοποιηθούν με τρεις μορφές, οι οποίες αναλύονται συνοπτικά παρακάτω:

- Χρήση Artificial Gaps
  Στην περίπτωση αυτή, ο επιτιθέμενος μπορεί να υλοποιήσει dropping διαδοχικών πακέτων σε μια ροή δεδομένων, προκειμένου να δημιουργήσει ένα μεγάλο κενό σε αυτή. Στη συνέχεια, έχει τη δυνατότητα να παρατηρήσει το μεγάλο αυτό κενό στους επόμενους routers οι οποίοι είναι compromised, με αποτέλεσμα να είναι σε θέση να προβεί στις απαραίτητες συσχετίσεις. [198] Ο επιτιθέμενος μπορεί εύκολα να υλοποιήσει την απόρριψη των πακέτων με ορισμένες απλές DoS Attacks, όπως έχουν περιγραφεί το αντίστοιχο κεφάλαιο.

  Οι επιθέσεις αυτές μάλιστα μπορούν εύκολα να συνδυαστούν, έτσι ώστε ο επιτιθέμενος να δημιουργεί, μέσω των gaps, εμφανή σημεία συσχέτισης της δικτυακής κίνησης, και ταυτόχρονα να εξαναγκάζει συνεχώς τον χρήστη να χρησιμοποιήσει κάποιο νέο anonymous tunnel, έως ότου καταλήξει σε αυτό που ελέγχεται πλήρως από τον επιτιθέμενο.

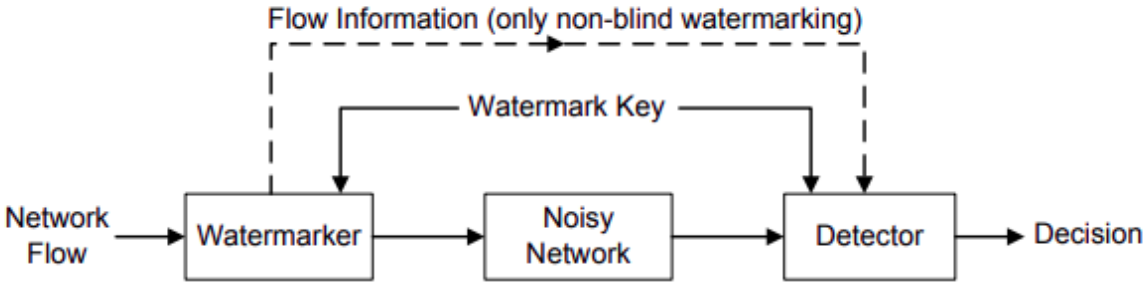
  Πολλά δίκτυα ανωνύμων επικοινωνιών επιχειρούν, για την καλύτερη προστασία της ανωνυμίας των χρηστών τους, να έχουν ένα συνεχή ρυθμό αποστολής μηνυμάτων στο δίκτυο, προκειμένου να δυσχεραίνεται η ανάλυση της δικτυακής κίνησης. Μέσω της παραπάνω επίθεσης, ακόμα και μικρές τεχνητές απώλειες πακέτων είναι διακριτές σε πολύ μεγάλο βαθμό, διευκολύνοντας σημαντικά το έργο του επιτιθέμενου. [200]
- Χρήση Artificial Bursts
  Ο επιτιθέμενος μπορεί να προκαλέσει τεχνητή καθυστέρηση ενός σημαντικού όγκου πακέτων σε κάποιον router που ο ίδιος ελέγχει και στη συνέχεια να τα απελευθερώσει όλα μαζί, με αποτέλεσμα να πραγματοποιήσει μια τεχνητή ριπή πακέτων. Η τεχνητή καθυστέρηση πακέτων δε μπορεί να είναι υπερβολικά μεγάλη καθώς θα οδηγήσει αναπόφευκτα στη διακοπή της TCP σύνδεσης, όπως ακριβώς ορίζεται από το πρωτόκολλο. Οι επιθέσεις αυτές μπορούν να αντιμετωπιστούν με Adaptive Padding αντίμετρα, ωστόσο το Defensive Dropping των πακέτων δε μπορεί να βοηθήσει, όπως θα αναλυθεί στο επόμενο μέρος. [196]
- Εισαγωγή Watermark

Οι συγκεκριμένες επιθέσεις ονομάζονται Network Flow Watermarking Attacks. Αποτελεί συνήθη πρακτική στις τεχνολογίες ανωνύμων επικοινωνιών να υλοποιείται κάποιας μορφής Flow Transformation, δηλαδή να μεταβάλλονται τα χαρακτηριστικά μιας δικτυακής ροής από τους μηχανισμούς του δικτύου έτσι ώστε να καταστεί δυσδιάκριτη σε πιθανές απόπειρες ανάλυσης της κίνησης από κάποιον κακόβουλο χρήστη. [198] [199] Πολλές από αυτές τις τεχνικές έχουν αναλυθεί ήδη στην παρούσα εργασία, καθώς αποτελούν αντίμετρα για πολλά είδη επιθέσεων. Χαρακτηριστικό παράδειγμα είναι η εισαγωγή dummy traffic ώστε να αποκρύπτονται τα χαρακτηριστικά κάθε ροής δεδομένων.



Σχήμα 3.48: Σύστημα απόφασης για την αναγνώριση ενός watermark σε μια Watermarking Attack.

Η εισαγωγή ενός watermark εντός του inter-packet timing domain μιας ροής πακέτων μπορεί να την κάνει διακριτή ακόμα και αν προστατεύεται από ισχυρούς μηχανισμούς cover traffic, υπόκειται σε πολυπλεξία με άλλες παρόμοιες ροές, διαχωρίζεται σε υπο-ροές, υπάρχουν ισχυροί packet dropping μηχανισμοί και έχει τυχαίες καθυστερήσεις, τεχνητές ή φυσικές. [196] Η επιτυχία των επιθέσεων αυτών δεν προϋποθέτει να υπάρχει κάποιος global adversary, απλά να είναι σε θέση ο επιτιθέμενος να ελέγχει συγκεκριμένους κόμβους του δικτύου ώστε αφενός να μπορεί να μεταβάλει το timestamp των πακέτων, αφετέρου να μπορεί να ανιχνεύει το συγκεκριμένο watermark κατά μήκος της διαδρομής.

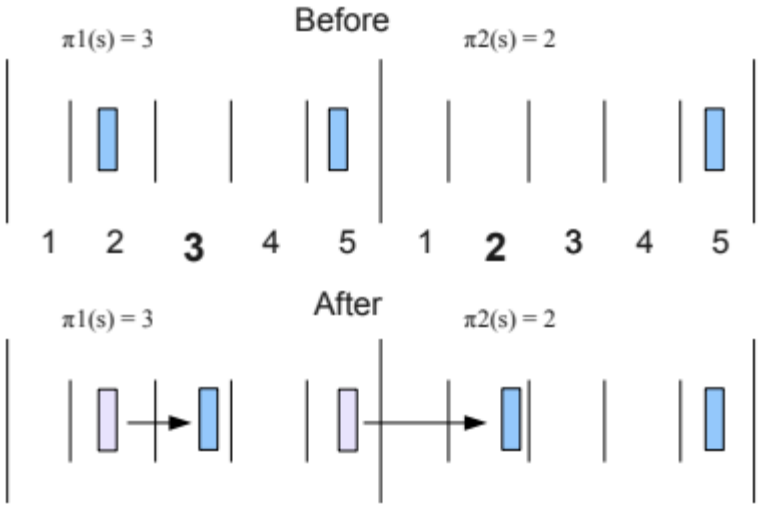


Σχήμα 3.49: Παράδειγμα Watermarking Attack.

Στις επιθέσεις αυτές εμπλέκονται δύο οντότητες, ο encoder και ο decoder. Αυτοί είναι δύο boundary routers (δηλαδή routers που επικοινωνούν απευθείας είτε με τον Initiator είτε με τον Destination) τους οποίους ελέγχει ο επιτιθέμενος. Ο encoder ενσωματώνει το watermark στις εισερχόμενες ροές, συνήθως καθυστερώντας συγκεκριμένα πακέτα. Από την άλλη, ο decoder ελέγχει κάθε εξερχόμενη ροή προκειμένου να εντοπίσει το αντίστοιχο watermark. [200] [202]

Υπάρχουν διάφοροι τρόποι εισαγωγής του watermark στα πακέτα, με τρόπο τέτοιο ώστε να μπορεί ο decoder να τα εντοπίσει πολύ εύκολα, αλλά να φαίνονται ακίνδυνα στους υπόλοιπους routers του δικτύου, προκειμένου να μην ενεργοποιήσουν κάποιο μηχανισμό προστασίας. Το watermark μπορεί να είναι είτε υπό τη μορφή network jitter είτε interval-based. Στην πρώτη περίπτωση το watermark εισάγεται στα ίδια τα πακέτα, ενώ στη δεύτερη ενσωματώνεται στα intervals τα οποία περιέχουν ομάδες πακέτων.

Οι πλέον εξελιγμένες μορφές watermarking είναι το SWIRL και το RAINBOW. Το μεν πρώτο εισάγει διαφορετικό blind watermark σε κάθε ροή δεδομένων, προκειμένου να προστατευθεί από Multi-Flow αντίμετρα. Ο χρόνος χωρίζεται σε διαστήματα (intervals) στα οποία εισάγεται το εκάστοτε watermark. Αποτελεί μια πολύ ισχυρή επίθεση, ενώ το watermark είναι τόσο ανθεκτικό στο network jitter, όσο και δυσδιάκριτο στους κανονικούς χρήστες αλλά και σε εξελιγμένες μεθόδους προστασίας. Έχει πολύ χαμηλά error rates και μπορεί να οδηγήσει στην ταυτοποίηση των ροών δεδομένων την ταυτότητα των στόχων της επίθεσης σε πολύ μικρό χρονικό διάστημα. Η εισαγωγή των watermarks παρουσιάζεται στην παρακάτω εικόνα. [194]



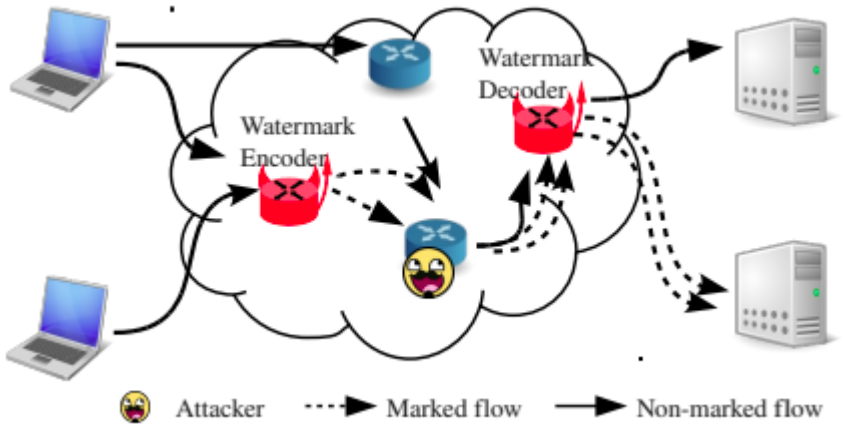
Σχήμα 3.50: SWIRL Watermarking Attack.

Αντίστοιχα, το RAINBOW αποτελεί μια ακόμα πιο εξελιγμένη τεχνική watermarking στην οποία ο encoder και ο decoder μοιράζονται μια βάση δεδομένων στην οποία καταγράφονται τα inter-arrival timings των πακέτων. Επίσης, εισάγεται ένα watermark που παίρνει τιμή α ή -α με πιθανότητα ½ έκαστο. Οι αλγόριθμοι τόσο στον encoder όσο και στον encoder έχουν την παρακάτω μορφή. [195]

Input: v, w, n
  for $j = 1 \rightarrow n$ **do**
    if $v[j] + w[j] \geq 0$ **then**
      $v[j] = v[j] + w[j]$
    end if
  end for
  return v

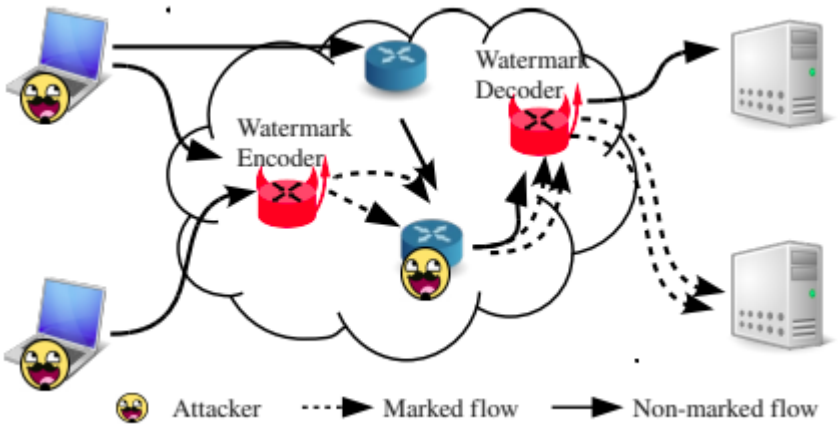
Input: $v, DB = \{v_1, v_2, \cdots, v_m\}, w, \zeta$
  $isDetected = FALSE$
  for $i = 1 \rightarrow m$ **do**
    $d_i = v_i - v$
    $r = \cos(d_i, w)$
    if $r > \zeta$ **then**
      $isDetected = TRUE$
    end if
  end for
  return $isDetected$

Το μοντέλο του επιτιθέμενου μπορεί να κατηγοριοποιηθεί ως εξής. Στην πρώτη περίπτωση υπάρχουν οι Isolated adversaries οι οποίοι βασίζονται στο Output-only detection, καθώς ο επιτιθέμενος έχει πρόσβαση μόνο στο περιεχόμενο της εξόδου του encoder. Έχουν περιορισμένες δυνατότητες όσον αφορά την αποτελεσματικότητα των επιθέσεων τους, χωρίς ωστόσο αυτό να σημαίνει ότι δε μπορούν να επιφέρουν πλήγματα στην ανωνυμία των χρηστών. Παρακάτω παρουσιάζεται συνοπτικά το είδος αυτό των επιτιθέμενων. [197] [198] [199]



Σχήμα 3.51: Output-only Detection Watermarking Attack.

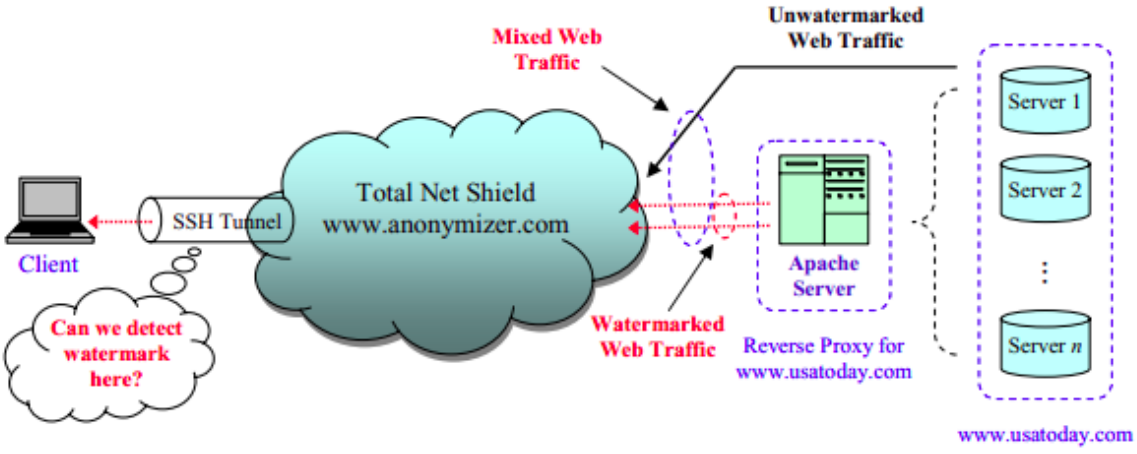
Το δεύτερο μοντέλο ονομάζεται Chosen Flow Adversaries. Στην περίπτωση αυτή ο επιτιθέμενος έχει αυξημένες δυνατότητες παρατήρησης της δικτυακής ροής, τόσο πριν όσο και μετά τη διαδικασία του watermarking. Έτσι, ο επιτιθέμενος έχει τη δυνατότητα να παρατηρήσει το network jitter τόσο πριν όσο και μετά το watermarking με αποτέλεσμα να έχει σημαντικά μικρότερα false-negative και false-positive αποτελέσματα στην αναγνώριση των ροών. Το μοντέλο παρουσιάζεται παρακάτω. [195] [201]



Σχήμα 3.52: Chosen Flow Watermarking Attack.

Αποτελεσματικότητα και Τρόποι Αντιμετώπισης των Timing Attacks

Οι επιθέσεις αυτές αποτελούν σημαντικό κίνδυνο για τις τεχνολογίες ανωνύμων επικοινωνιών. Εντάσσονται σε ένα πλαίσιο διαρκούς έρευνας πιο αποτελεσματικών παραλλαγών των επιθέσεων αυτών αλλά και πιο αποτελεσματικών τρόπων προστασίας. Πολλές από τις μεθόδους που χρησιμοποιούνται για την άμυνα των δικτύων από επιθέσεις αποτυγχάνουν να αντιμετωπίσουν τη συγκεκριμένη κατηγορία επιθέσεων. Ταυτόχρονα, η εισαγωγή deep learning αλγορίθμων μπορεί να ενισχύσει αφενός τους επιτιθέμενους, προκειμένου να ανακαλύψουν προηγμένες μεθόδους εντοπισμού των watermarks, αφετέρου μπορεί να βοηθήσει τους σχεδιαστές των δικτύων να αναλύσουν την κίνηση προκειμένου να εντοπίσουν ύποπτες καθυστερήσεις και εν γένει ανωμαλίες στην αλληλουχία των πακέτων. Παρακάτω παρουσιάζεται ένα case study μιας τέτοιας επίθεσης στο Anonymizer.

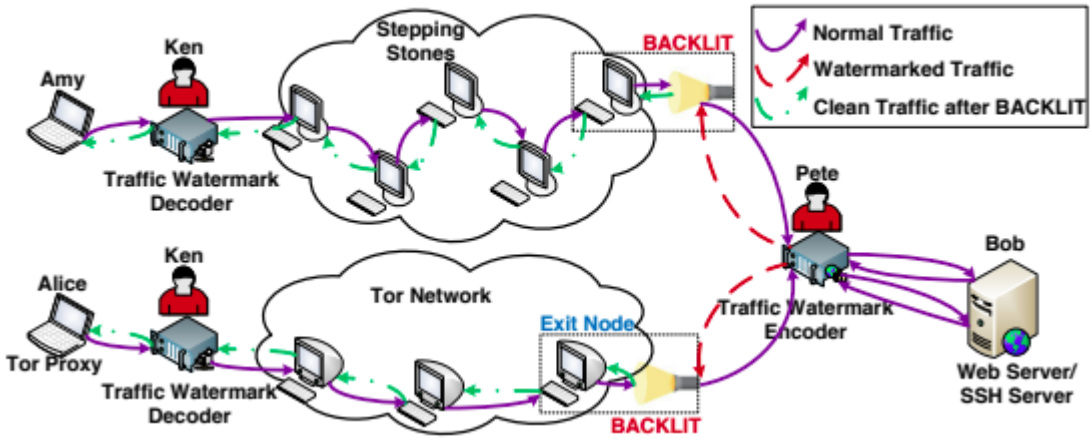


Σχήμα 3.53: Watermarking Attack στο Anonymizer.

Διάφορα padding schemes μπορούν να αντιμετωπίσουν αποτελεσματικά τις επιθέσεις αυτές. Όπως έχει αναλυθεί, οι συγκεκριμένες τεχνικές είναι πολύ αποτελεσματικές στην προστασία του δικτύου από διάφορες επιθέσεις, ωστόσο μπορούν να εισάγουν σημαντικό latency στο δίκτυο, με αποτέλεσμα να μην καθίσταται πάντα εφικτή η εφαρμογή τους, ειδικά όταν πρόκειται για low-latency δίκτυα. Άλλες μέθοδοι αντιμετώπισης των επιθέσεων αυτών είναι το PNR, το MFA και το BACKLIT. [201] [202]

Το PNR είναι μια μέθοδος εισαγωγής controlled timing στα πακέτα που αποστέλλονται, με αποτέλεσμα να καθίσταται εύκολος ο εντοπισμός των watermarks με τη χρήση στατιστικών και data mining εργαλείων. Το MFA αποτελεί μια παθητική μέθοδο εντοπισμού η οποία παρατηρεί διαδοχικές ροές που έχουν υποστεί εισαγωγή watermark, με σκοπό να παρατηρήσει συγκεκριμένες κοινές περιόδους δραστηριότητας ή αδράνειας στο δίκτυο. Αποτελεί μια εξαιρετικά αποτελεσματική μέθοδο εντοπισμού των επιθέσεων αυτών, έχοντας οδηγήσει στη δημιουργία των πιο εξελιγμένων μορφών επιθέσεων, από πλευράς επιτιθέμενων, όπως είναι το RAINBOW και το SWIRL τα οποία αναλύθηκαν πιο πάνω. [195] [198]

Τέλος, μια από τις πιο σύγχρονες μεθόδους αντιμετώπισης είναι το BACKLIT, όπου ο αμυνόμενος χρησιμοποιεί έναν server ο οποίος αποστέλλει δικτυακή κίνηση στον encoder, έτσι ώστε να αναλύσει το watermarking scheme που χρησιμοποιεί ο επιτιθέμενος και να κάνει μια ευκολότερη αντιπαραβολή των “καθαρών” και των watermarked ροών δεδομένων. Είναι ένα επίσης εξαιρετικά επιτυχημένο μοντέλο αντιμετώπισης των επιθέσεων αυτών, ωστόσο βασίζεται στο συγκεκριμένο μοντέλο επιτιθέμενου. Η λειτουργία του παρουσιάζεται στην παρακάτω εικόνα. [196] [197]



Σχήμα 3.54: Λειτουργία του BACKLIT.

Συμπερασματικά, οι εν λόγω επιθέσεις αποτελούν σημαντικό πεδίο έρευνας, καθώς με την έλευση νέων τεχνολογιών, όπως τα Machine Learning και η AI αναπτύσσονται σημαντικές δυνατότητες τόσο για τους επιτιθέμενους όσο και για τους σχεδιαστές των δικτύων.

3.2 Tor Network Attacks and Defenses

Το second-generation Onion Routing αποτελεί την πιο διαδεδομένη τεχνολογία ανωνύμων επικοινωνιών, καθώς υπολογίζεται ότι καθημερινά πάνω από 2 με 2,5 εκατομμύρια χρήστες παγκοσμίως το χρησιμοποιούν για την πλοήγηση τους στο Internet διατηρώντας την ανωνυμία τους. Αξίζει μάλιστα να σημειωθεί ότι μετά τις αποκαλύψεις του σκάνδαλου Schnowden το 2013, το ενδιαφέρον των χρηστών για τρόπους που θα διασφαλίσουν την ανωνυμία τους στο Internet αυξήθηκε κατακόρυφα, με αποτέλεσμα οι χρήστες του Tor Network να πολλαπλασιαστούν.

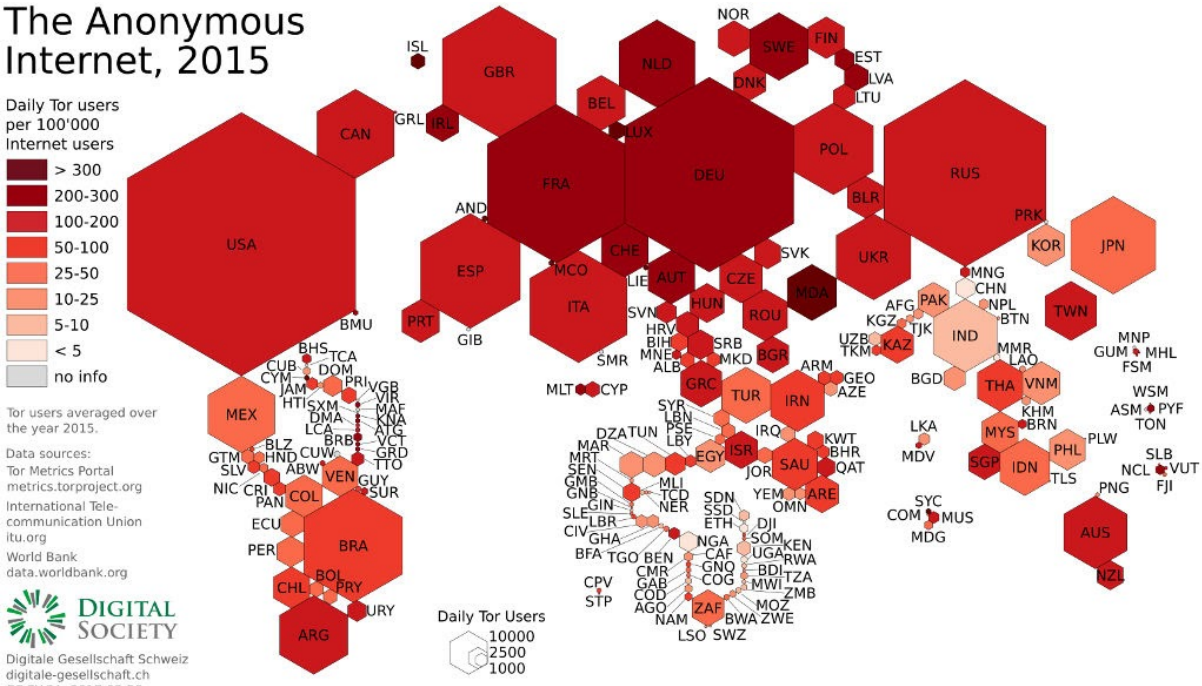
Φυσικά, το Tor Network απευθύνεται σε μια ευρεία γκάμα χρηστών, από εκείνους που επιθυμούν να πλοηγηθούν στο διαδίκτυο διατηρώντας την ανωνυμία τους, χρήστες που επιθυμούν να έχουν πρόσβαση σε λογοκριμένο περιεχόμενο αλλά και χρήστες που θέλουν να έχουν πρόσβαση στο Dark

Web για την υλοποίηση παράνομων δραστηριοτήτων. Υπολογίζεται ότι υπάρχουν πάνω από 7000 servers στο δίκτυο, οι οποίοι προσφέρουν πρόσβαση στο δίκτυο.

Σε κάθε περίπτωση, το Tor Network επικρατεί την κυρίαρχη λύση για τους χρήστες που επιθυμούν να διατηρήσουν την ανωνυμία τους. Μάλιστα, επιτυγχάνει πολύ καλύτερες επιδόσεις από τη δεύτερη σε δημοτικότητα λύση, που είναι η χρήση ενός VPN, σχετικά με την πρόσβαση σε περιεχόμενο που λογοκρίνεται. Επιπλέον, είναι προφανές ότι αποτελεί τη μόνη λύση για χρήστες που θέλουν να έχουν πρόσβαση σε παράνομο περιεχόμενο. Τα πλεονεκτήματα του Tor Network μπορούν να αναλυθούν επιγραμματικά τα παρακάτω:

- Κρύβει αποτελεσματικά τη δραστηριότητα των χρηστών στο διαδίκτυο.
- Anti-spy προστασία. Το δίκτυο αποτρέπει τους υπόλοιπους συμμετέχοντες από το να γνωρίζουν ποιους ιστότοπους επισκέπτεται κάποιος.
- Anonymous identity. Όλοι οι χρήστες έχουν κοινά χαρακτηριστικά με αποτέλεσμα να μην είναι δυνατό να διακρίνονται μεταξύ τους μέσω των συσκευών που χρησιμοποιούν.
- Multi-layer encryption. Η διαστρωματωμένη κρυπτογράφηση και η πολλαπλή δρομολόγηση των πακέτων μέσω πολλών routers διασφαλίζει, υπό φυσιολογικές συνθήκες, την ανωνυμία των χρηστών.
- Ελεύθερη πρόσβαση σε περιεχόμενο. Το Tor Network μέσω του browser που παρέχεται από το Tor Project επιτρέπει την πρόσβαση σε περιεχόμενο που έχει λογοκριθεί στο δίκτυο.
- Δωρεάν χρήση. Οποιοσδήποτε μπορεί να συμμετέχει στο Tor Network χωρίς να πληρώνει κάποια συνδρομή, είτε ως Tor Relay είτε ως τελικός χρήστης.

Τα τελευταία δεδομένα που υπάρχουν για τους χρήστες του Tor Network παρουσιάζονται στο παρακάτω γράφημα. Τα δεδομένα ανήκουν στο έτος 2015 και παρουσιάζονται τόσο ο απόλυτος αριθμός χρηστών, όσο και ο σχετικός αριθμός που υποδεικνύει το ποσοστό των χρηστών εν συγκρίσει με το σύνολο κάθε χώρας. Άξιο παρατήρησης είναι ότι η Κίνα έχει ελάχιστο ποσοστό χρηστών, καθώς τα μέτρα καταπολέμησης του Tor Network μέσω του Big Firewall of China απέδωσαν και κατάφεραν να αντιμετωπίσουν αποτελεσματικά την πρόσβαση των χρηστών σε αυτό. Πολλές από τις επιθέσεις που έχουν περιγραφεί παραπάνω έχουν κατ’ επανάληψη επιστρατευτεί από την Κινεζική Κυβέρνηση προκειμένου να εντοπίσουν χρήστες του δικτύου. Κρίνεται λοιπόν σκόπιμο να αναλυθούν οι κυριότερες απειλές εναντίον του δικτύου, καθώς δυνητικά επηρεάζουν πάρα πολλούς χρήστες καθημερινά.



3.2.1 Passive Attacks

3.2.1.1 Observing user traffic patterns

Οι επιθέσεις αυτές ανήκουν στην κατηγορία των Message Coding Attacks. Ο επιτιθέμενος μπορεί να παρατηρεί τη σύνδεση ενός χρήστη, και ενώ δεν είναι δυνατό να ανακαλύψει τον τελικό προορισμό των μηνυμάτων τους, μπορεί να εντοπίσει συγκεκριμένα traffic patterns. Τα patterns αυτά απαρτίζονται από εισερχόμενα και εξερχόμενα πακέτα και ο επιτιθέμενος μπορεί να υλοποιήσει περαιτέρω επεξεργασία και συσχετίσεις προκειμένου να κάνει profiling του χρήστη-στόχου της επίθεσης. [10]

3.2.1.2 Observing user content

Σε περίπτωση που ο ιστότοπος τον οποίο επισκέπτεται ένας χρήστης είναι κακόβουλος, τότε ο επιτιθέμενος μπορεί να έχει πρόσβαση στο περιεχόμενο που στέλνει ο χρήστης. Συνήθως συνδυάζεται με Phishing Attacks, όπου ο στόχος της επίθεσης χρησιμοποιεί εν αγνοία του ένα counterfeit site το οποίο έχει δημιουργήσει και ελέγχει ο επιτιθέμενος, προκειμένου να αποκτήσει πρόσβαση σε credentials ή σε περιεχόμενο που έχει ο χρήστης. [20]

3.2.1.3 Option distinguishability

Όπως έχει ήδη αναλυθεί, πολλές τεχνολογίες ανωνύμων επικοινωνιών παρέχουν δυνατότητες παραμετροποίησης των μηχανισμών ανωνυμίας στους χρήστες, προκειμένου να εξασφαλίζεται το βέλτιστο trade-off ανωνυμίας και επιδόσεων, ανάλογα με τις ανάγκες τους. Το Tor Network παρέχει επίσης τη δυνατότητα αυτή, επιτρέποντας στους χρήστες να επιλέξουν πόσο συχνά θα αλλάζουν τα χρησιμοποιούμενα μονοπάτια και άλλες λειτουργίες. [17] Παρ’ όλο που η λειτουργία αυτή επιτρέπει

στους χρήστες να προσαρμόζουν το Tor Network στις ανάγκες τους, τα διακριτά χαρακτηριστικά αυτά μπορούν να είναι attack vector καθώς κάνουν διακριτή τη σύνδεση από τις υπόλοιπες.

3.2.1.4 End-to-end timing correlation

Οι Timing Attacks αποτελούν μια εξαιρετικά σημαντική αλλά και δύσκολα αντιμετωπίσιμη πηγή απειλών για το Tor Network και κατ επέκταση για το σύνολο των τεχνολογιών ανωνύμων επικοινωνιών. Η ανάλυση και η συσχέτιση των χρόνων άφιξης και αναχώρησης πακέτων αλλά και του latency στο δίκτυο μπορεί να επιτρέψει στον επιτιθέμενο να υλοποιήσει συσχετίσεις των ροών δεδομένων με μεγάλη μάλιστα πιθανότητα επιτυχίας. [20] Το Tor Network προσπαθεί να αντιμετωπίσει τις επιθέσεις αυτές μέσω της απόκρυψης της σύνδεσης μεταξύ του Onion Proxy και του Tor node. Αυτό επιτυγχάνεται είτε με τη χρήση firewall είτε με την ενσωμάτωση του Onion Proxy μέσα στο Tor node. Ένας global observer μπορεί να αντιμετωπίσει αποτελεσματικά τα αντίμετρα αυτά, διαχωρίζοντας την κίνηση που πηγάζει από έναν Onion Router από αυτή που απλώς διέρχεται μέσω αυτού.

3.2.1.5 End-to-end size correlation

Η καταμέτρηση πακέτων από τον επιτιθέμενο μπορεί επίσης να χρησιμοποιηθεί για την ταυτοποίηση των endpoints του anonymous tunnel. Ο leaky pipe μηχανισμός του Tor Network προσφέρει ένα επίπεδο προστασίας στο δίκτυο αφού ο αριθμός εισερχομένων και εξερχομένων πακέτων σε ένα κύκλωμα δεν είναι πάντα ο ίδιος. [18]

3.2.1.6 Website fingerprinting

Οι επιθέσεις αυτές αποτελούν στην ουσία εξέλιξη των Observing user traffic patterns Attacks, μέσω των οποίων ο επιτιθέμενος δημιουργεί ο ίδιος fingerprints των ιστοτόπων που υποπτεύεται ότι επισκέπτεται ο στόχος του και στη συνέχεια επιχειρεί να υλοποιήσει συσχετίσεις σχετικά με το μέγεθος των πακέτων και την αλληλουχία που παρατηρείται σε αυτά. [29] [41] Μπορεί με τον τρόπο αυτό να ανακαλυψει ποιους ιστότοπους επισκέπτεται ένας χρήστης. Ο πολυπλεξία ροών δεδομένων εντός των κυκλωμάτων αποτελεί μια πρώτη γραμμή άμυνας, ενώ επιπλέον αντίμετρα, όπως έχει αναφερθεί και στην αντίστοιχη ανάλυση είναι η χρήση dummy traffic και η εισαγωγή μεγαλύτερου μεγέθους cells.

3.2.2 Active Attacks

3.2.2.1 Compromise Keys

Ένας επιτιθέμενος ο οποίος θα καταφέρει να μαθει το key του TLS session μπορεί να έχει πρόσβαση στα control cells και στα κρυπτογραφημένα relay cells σε κάθε κύκλωμα ης συγκεκριμένης σύνδεσης. Αυτό συμβαίνει διότι, όπως έχει αναφερθεί και στην ανάλυση του Onion Routing, όταν ο επιτιθέμενος γνωρίζει το κλειδί (key) ενός circuit session τότε είναι σε θέση να αποκρυπτογραφήσει και το αντίστοιχο στρώμα κρυπτογράφησης. [57]

Επίσης, ένας επιτιθέμενος που γνωρίζει το ιδιωτικό κλειδί TLS ενός Onion Router είναι σε θέση να υποδυθεί τον συγκεκριμένο κόμβο καθ όλη τη διάρκεια ισχύος του συγκεκριμένου κλειδιού. Φυσικά, θα χρειαστεί επίσης να γνωρίζει και το onion key για να είναι σε θέση να αποκρυπτογραφήσει τα cells που φτάνουν στον router. [8]

Η περιοδική ανακύκλωση των κλειδιών περιορίζει τον κίνδυνο αυτό, καθώς μειώνει το χρονικό παράθυρο στο οποίο μπορούν να εκτελεστούν επιτυχώς τέτοιου είδους επιθέσεις. Από την άλλη, ένας επιτιθέμενος που έχει κάνει compromised, με τον παραπάνω τρόπο, έναν κόμβο, είναι σε θέση να υποδύεται ες αεί τον συγκεκριμένο κόμβο, αφού μπορεί να στέλνει ψεύτικους descriptors στους directory servers του Tor Network.

3.2.2.2 Iterated Compromise

Ένας επιτιθέμενος που συμμετέχει στο δίκτυο μπορεί να κάνει compromisation τους Onion Routers σε βαθμό τέτοιο ώστε να καταφέρει να κάνει compromise όλο το circuit, ελέγχοντας ουσιαστικά πλήρως το anonymous tunnel. Ο τρόπος με τον οποίο μπορεί να γίνει αυτό είναι είτε χρησιμοποιώντας system intrusion τεχνικές, είτε με μεθόδους νομικού εξαναγκασμού ή μη. [69] Χαρακτηριστικό είναι το γεγονός ότι σε αρκετές περιπτώσεις, ορισμένες δικαστικές αποφάσεις υποχρέωσαν διάφορα δίκτυα ανωνύμων επικοινωνιών, όπως το Java Anon Proxy, να εισάγουν backdoors στο δίκτυο προκειμένου να καταφέρουν διάφορες κρατικές υπηρεσίες να εντοπίσουν παράνομη δραστηριότητα που λάμβανε χώρα εκεί. [70]

Ο επιτιθέμενος για να είναι σε θέση στο Tor Network να έχει αποτελέσματα από αυτές τις επιθέσεις θα πρέπει να καταφέρει να τις ολοκληρώει εντός του χρόνου ζωής του συγκεκριμένου κυκλώματος. Σε διαφορετική περίπτωση οι Onion Routers θα έχουν απορρίψει την απαραίτητη στον επιτιθέμενο πληροφορία. Επιπροσθέτως, η χρήση cross-jurisdictions κυκλωμάτων μπορούν να αποτρέψουν τέτοιου είδους επιθέσεις, ειδικά όταν προκύπτουν μέσω νομικού εξαναγκασμού.

3.2.2.3 Run a Recipient

Οι επιθέσεις αυτές βασίζονται στη μεθοδολογία των Latency Attacks. Ο επιτιθέμενος τρέχει στο Tor Network έναν webserver, μέσω του οποίου μπορεί εύκολα να μάθει τα timing patterns των χρηστών που συνδέονται σε αυτόν, αλλά και να υλοποιήσει μια end-to-end latency ανάλυση του δικτύου. Επίσης, είναι σε θέση να εισάγει τεχνητή καθυστέρηση στα πακέτα, να υλοποιήσει message tagging τεχνικές, διευκολύνοντας περαιτέρω την ανάλυση της δικτυακής κίνησης.

Ο webserver αυτός μπορεί να περιέχει περιεχόμενο που ενδιαφέρει μια συγκεκριμένη ομάδα χρηστών, με απώτερο σκοπό να τραβήξει το ενδιαφέρον τους ώστε να συνδεθούν σε αυτόν. Με τον

τρόπο αυτό, ο επιτιθέμενος καταφέρνει να ελέγχει το ένα άκρο της σύνδεσης. Τα πρωτόκολλα που χρησιμοποιεί το web application θα μπορούσαν επίσης να αξιοποιηθούν για την αποκάλυψη πληροφοριών σχετικά με την ταυτότητα του Initiator, κάτι που το Tor Network αντιμετωπίζει με τη χρήση του Privoxy και διαφόρων άλλων protocol cleaners. [55]

3.2.2.4 Run an Onion Proxy

Στην πλειοψηφία των περιπτώσεων, οι χρήστες τρέχουν το δικό τους Onion Proxy τοπικά, κάτι που ωστόσο δεν ισχύει σε μερικές περιπτώσεις, εισάγοντας τον κίνδυνο, αν αυτός γίνει compromised, να υπονομεύονται όλες οι μελλοντικές συνδέσεις οι οποίες υλοποιούνται μέσω αυτού. [8]

3.2.2.5 DoS Non-Observed Nodes

Πρόκειται για τις Selective Denial of Service Attacks, στις οποίες ο επιτιθέμενος υλοποιεί DoS Attacks σε κυκλώματα που δεν ελέγχει ο ίδιος, προκειμένου να τα εξαναγκάσει σε ανασχηματισμό, να πλήξει την αξιοπιστία τους ή απλώς να πλήξει συνολικά τη διαθεσιμότητα του δικτύου. [17]

3.2.2.6 Run a Hostile Onion Router

Ένας κακόβουλος κόμβος στο δίκτυο, εκτός από παθητικές παρατηρήσεις του δικτύου, μπορεί να συμμετέχει και ο ίδιος ενεργά στον σχηματισμό μονοπατιών ή να τροποποιήσει τα traffic patterns των cells προς άλλους κόμβους που διέρχονται μέσω αυτού. Για να επηρεάσει φυσικά την ανωνυμία του δικτύου, θα πρέπει να γειτνιάζει με ένα από τα δύο endpoints του κυκλώματος. Η ύπαρξη hostile routers στο Tor Network μπορεί να αποτελέσει πηγή πολλών επιθέσεων, όπως έχει αναλυθεί και στους κινδύνους που διατρέχουν συνολικά οι ανώνυμες επικοινωνίες. Έτσι, οι κακόβουλοι αυτοί κόμβοι μπορούν να συνεργάζονται και να συμμετέχουν σε Collusion, Latency, Sybil και DoS Attacks στο Tor Network. [14]

3.2.2.7 Introduce Timing into Message

Πρόκειται στην ουσία για της Active Timing Attacks, οι οποίες έχουν αναλυθεί στο αντίστοιχο κεφάλαιο. [86]

3.2.2.8 Tagging Attack

Πρόκειται για τις Message Tagging Attacks, όπως έχουν αναλυθεί στο αντίστοιχο κεφάλαιο. [90]

3.2.2.9 Replace Contents of Unauthenticated Protocols

Μη ασφαλή πρωτόκολλα όπως το HTTP μπορούν να γίνουν compromised, έτσι ώστε ο επιτιθέμενος να καταφέρει να υποδυθεί τον server που είναι στόχος του. Έτσι, η χρήση secure protocols είναι επιβεβλημένη για την αποτροπή τέτοιων επιθέσεων. [8]

3.2.2.10 Replay Attacks

Πρόκειται για μια αρκετά επικίνδυνη παραλλαγή των Message Tagging Attacks όπου, όπως έχει αναλυθεί στο αντίστοιχο κεφάλαιο, στέλνονται πολλαπλά αντίγραφα του ίδιου cell προκειμένου να

δημιουργηθεί error στο δίκτυο, κάτι που βοηθάει τον επιτιθέμενο να επιβεβαιώσει τη συνομιλία δύο μερών. [23] Το Tor Network είναι αρκετά ανθεκτικό σε τέτοιου είδους επιθέσεις, καθώς η επανάληψη ενός μηνύματος οδηγεί σε καινούριο handshake, άρα και διαφορετικό session key.

3.2.2.11 Smear Attacks

Οι επιθέσεις αυτές έχουν στόχο να πλήξουν την αξιοπιστία του δικτύου στο ευρύ κοινό, κυρίως μέσω της υλοποίησης παράνομων δραστηριοτήτων σε αυτό, με αποτέλεσμα να ληφθούν μέτρα για την απαγόρευση χρήσης του. [40]

3.2.2.12 Distribute Hostile Code

Στο διαδίκτυο κυκλοφορούν πολλές κακόβουλες εκδόσεις του Tor software οι οποίες αντί για την προστασία της ανωνυμίας των χρηστών, καθιστούν τις συνδέσεις ευάλωτες σε επιθέσεις. Οι επίσημες και ασφαλείς εκδόσεις του συγκεκριμένου λογισμικού υπογράφονται με το επίσημο δημόσιο κλειδί του Tor Project. [41]

3.2.3 Directory Attacks

3.2.3.1 Destroy Directory Servers

Η ύπαρξη πολλών Directory Servers δημιουργεί υπερεπάρκεια πόρων, έτσι ώστε ακόμα και στην περίπτωση που ορισμένοι από αυτούς τεθούν εκτός λειτουργίας, το δίκτυο να συνεχίσει να λειτουργεί κανονικά. Σε περίπτωση που υπάρχει έστω ένας ενεργός, το δίκτυο μπορεί να λειτουργήσει, ωστόσο όταν τεθούν εκτός λειτουργίας πάνω από το 50% των servers τότε το directory δε θα διαθέτει αρκετές υπογραφές στο consensus ώστε να το χρησιμοποιούν οι χρήστες αυτόματα, έτσι οι χρήστες θα πρέπει να επιλέξουν οι ίδιοι αν εμπιστεύονται τον εκάστοτε server. [11]

3.2.3.2 Subvert a Directory Server

Αν ένας επιτιθέμενος έχει τον έλεγχο ενός Directory Server τότε μπορεί να επηρεάσει το Final Directory. Οι Onion Routers συμμετέχουν ή όχι στο δίκτυο με βάση ενός πλειοψηφικού συστήματος, συνεπώς ένας κακόβουλο directory μπορεί να επηρεάσει το σύστημα ώστε να συμπεριληφθούν και κακόβουλοι κόμβοι που οριακά είχαν απορριφθεί. [47]

3.2.3.3 Subvert a Majority of Directory Servers

Ένας κακόβουλος χρήστης ο οποίος ελέγχει άνω του 50% των Directory Servers μπορεί να συμπεριλάβει όσους κακόβουλους Onion Routers επιθυμεί εκείνος στο Final Directory. [8]

3.2.3.4 Encourage Directory Server Dissent

Ένας επιτιθέμενος ο οποίος μπορεί να πείσει κάποιους από τους Directory Servers operators να μην εμπιστεύονται κάποιον άλλο μπορεί να δημιουργήσει δύο διαφορετικά αντιμαχόμενα γκρουπ, με

αποτέλεσμα να διαχωριστούν και οι χρήστες του δικτύου σε δύο διαφορετικά γκρουπ, αναλογως των Directory που χρησιμοποιούν. [15]

3.2.3.5 Trick the Directory Servers into Listing a Hostile Onion Router

Οι operators των Directory Servers οφείλουν να μεριμνούν για την απόρριψη τυχόν κακόβουλων Onion Routers. [2]

3.2.3.6 Convince the Directories that a Malfunctioning OR is Working

Ένας κακόβουλος Onion Router μπορεί να αποδέχεται TLS συνδέσεις από έναν Onion Router, απορρίπτοντας ταυτόχρονα όλα τα cells από αυτόν, με αποτέλεσμα να εμφανίζεται ως ενεργός και διαθέσιμος στο δίκτυο. Οι Directory Servers οφείλουν να υλοποιούν αναλυτικό έλεγχο των Onion Routers προκειμένου να αποφεύγονται τέτοιου είδους κίνδυνοι. [55]

3.2.4 Attacks Against Rendezvous Points

3.2.4.1 Make many Introduction Requests

Ένας επιτιθέμενος μπορεί να αρνηθεί την πρόσβαση σε χρήστες με το να υλοποιήσει flooding των introduction points με requests. Ως αντίμετρο, ο χρήστης μπορεί να περιορίσει τον αριθμό των requests που λαμβάνει. [20]

3.2.4.2 Attack an Introduction Point

Είναι δυνατόν ένα hidden service να τεθεί εκτός λειτουργίας αν ένας επιτιθέμενος καταφέρει να θέσει εκτός λειτουργίας τα introduction points του. Για να πετύχει η επίθεση ο επιτιθέμενος θα χρειαστεί να απενεργοποιήσει όλα τα πιθανά introduction points καθώς το hidden service θα μπορούσε απλά να διαφημίσει καινούρια ή να χρησιμοποιεί διαφορετικά για την εκάστοτε κατηγορία clients. [23]

3.2.4.3 Compromise an Introduction Point

Σε περίπτωση που ένα introduction point βρίσκεται υπό τον έλεγχο ενός κακοβουλου χρήστη τότε αυτός μπορεί είτε να κάνει flooding με introduction requests σε έναν χρήστη ή να αποτρέψει από τα μη κακόβουλα requests από το να φτάσουν σε εκείνον. Ο client μπορεί να διακόψει τη λειτουργία του κυκλώματος αν εντοπίσει το flooding αυτό. Ο περιοδικός έλεγχος της σύνδεσης μπορεί επίσης να εντοπίσει για τυχόν valid requests που μπλοκάρονται από τον επιτιθέμενο. [29]

3.2.4.4 Compromise a Rendezvous Point

Το Rendezvous Point είναι το μόνο που γνωρίζει την ακριβή ταυτότητα ενός hidden service, επομένως τυχόν επίθεση εναντίον του μπορεί να οδηγήσει στην πλήρη ταυτοποίηση της υπηρεσίας και του παρόχου της. [41]

Μέρος IV

Συμπεράσματα

Σκοπός της παρούσας διπλωματικής εργασίας ήταν η συγκέντρωση και καταγραφή όλων των τεχνολογιών ανωνύμων επικοινωνιών οι οποίες αναπτύχθηκαν από τις απαρχές της έρευνας πάνω στο συγκεκριμένο πεδίο, καθώς και η αναλυτική παρουσίαση όλων των επιθέσεων οι οποίες έχουν στόχο να πλήξουν την προστασία της ανωνυμίας των χρηστών τους.

Αναμφίβολα, η ιδιωτικότητα των χρηστών και η απόκρυψη της δραστηριότητας τους στο διαδίκτυο αποτελεί μείζον θέμα τα τελευταία χρόνια, έχοντας απασχολήσει τους απλούς χρήστες, τους τεχνολογικούς κολοσσούς αλλά και τις κυβερνήσεις και τα δικαστικά όργανα. Οι χρήστες γίνονται ολοένα και πιο ευαίσθητοι όσον αφορά την προστασία των ευαίσθητων προσωπικών δεδομένων τους, συνειδητοποιώντας ότι η ελεύθερη χρήση πολλών υπηρεσιών έχει ως πραγματικό αντίτιμο τα δεδομένα αυτά τα οποία σιωπηλά συλλέγονται από διάφορους οργανισμούς και αποτελούν αντικείμενο κοινωνικής, πολιτικής και κυρίως οικονομικής εκμετάλλευσης.

Για το λόγο αυτό, τα τελευταία χρόνια έχει αναπτυχθεί πληθώρα τεχνολογιών που δίνουν βάρος στη διασφάλιση της ανωνυμίας και της ιδιωτικότητας των χρηστών, προσφέροντας μάλιστα υψηλού επιπέδου υπηρεσίες και επιδόσεις οι οποίες μπορούν να ανταποκριθούν ακόμα και στις σύγχρονες, απαιτητικές διαδικτυακές εφαρμογές. Η έρευνα γύρω από το συγκεκριμένο πεδίο έχει συγκεντρώσει πλήθος επιστημόνων και σχεδιαστών δικτύων επικοινωνιών οι οποίοι αντιλαμβάνονται ότι οι χρήστες πλέον τοποθετούν ψηλά σε προτεραιότητα την προστασία των δεδομένων τους, ιδιαίτερα σε μια εποχή όπου τα πάντα είναι διασυνδεδεμένα μεταξύ τους.

Οι τεχνολογίες αυτές εφάρμοσαν διάφορες αρχιτεκτονικές και κάθε μια από αυτές επιχείρησε να δώσει λύσεις σε συγκεκριμένα προβλήματα ή να αντιμετωπίσει ορισμένους τύπους επιθέσεων. Όπως είναι φυσικό, καμία λύση δεν είναι τέλεια. Ακόμα και το Tor Network, το οποίο αποτελεί σήμερα την πιο δημοφιλή λύση για την προστασία της ανωνυμίας των χρηστών και την πρόσβαση σε λογοκριμένο περιεχόμενο, παρουσιάζουν σημαντικές αδυναμίες σε συγκεκριμένα μοντέλα επιθέσεων. Ταυτόχρονα, οι τεχνολογίες αυτές έχουν και άλλες σημαντικές προκλήσεις να αντιμετωπίσουν. Σε πολλές περιπτώσεις η επεκτασιμότητα μιας τεχνολογίας δε μπορεί να εφαρμοστεί ώστε να ικανοποιήσει μεγάλο αριθμό χρηστών, ενώ άλλες τεχνολογίες που βασίζονται σε Peer-to-Peer αρχιτεκτονικές δεν είναι εύκολο να υλοποιηθούν, καθώς απαιτούν την εθελοντική συμμετοχή πολλών χρηστών παγκοσμίως για να λειτουργήσουν. Τέλος, οι διαρκώς αυξανόμενες ανάγκες των διαδικτυακών εφαρμογών για high bandwidth και low latency δυσκολεύουν πολλές τεχνολογίες στο να ανταποκριθούν στις απαιτήσεις των χρηστών, εισάγοντας σημαντική καθυστέρηση στο δίκτυο.

Ταυτόχρονα, οι τεχνολογίες αυτές παρουσιάζουν πρόσφορο έδαφος επιθέσεων, καθώς η ανωνυμία που προσφέρουν σε πολλές περιπτώσεις αποτέλεσαν, και συνεχίζουν να αποτελούν, πεδίο υλοποίησης παράνομων δραστηριοτήτων, ενώ σε πολλές περιπτώσεις απολυταρχικά καθεστώτα επιχειρούν να λογοκρίνουν συγκεκριμένο περιεχόμενο που υπάρχει στο διαδίκτυο προκειμένου οι πολίτες μιας χώρας να μην έχουν πρόσβαση σε αυτό.

Η υλοποίηση των επιθέσεων αυτών βασίζεται κατά κύριο λόγο σε Traffic Analysis τεχνικές, στις οποίες το επιτιθέμενο μέρος παρατηρεί τη δραστηριότητα του δικτύου και επιχειρεί, μέσω συσχετισμών να προβεί σε συμπεράσματα σχετικά με την ταυτότητα και τη διαδικτυακή δραστηριότητα του στόχου του. Επιπροσθέτως, παραδοσιακές επιθέσεις κατά των δικτύων, όπως οι Denial of Service Attacks εξελίχθηκαν και προσαρμόστηκαν ώστε να εξυπηρετούν τους σκοπούς των επιθέσεων κατά της ανωνυμίας των χρηστών. Οι επιθέσεις φυσικά πολλές φορές συνδυάζονται μεταξύ τους, προκειμένου να επιφέρουν τα βέλτιστα δυνατά αποτελέσματα. Σπανίως πλέον υλοποιείται μια μόνο επίθεση, καθώς οι επιτιθέμενοι, ιδιαίτερα όσοι διαθέτουν επάρκεια πόρων, προσπαθούν να αυξήσουν την επιφάνεια επίθεσης του στόχου τους και να επιφέρουν πολλαπλά πλήγματα στην ανωνυμία του.

Έως σήμερα έχει αναπτυχθεί πλήθος επιθέσεων, καθώς η διαρκής εξέλιξη των τεχνολογιών ανωνύμων επικοινωνιών ανάγκασε τους επιτιθέμενους να εξελίξουν τις ήδη υπάρχουσες αλλά και να προσθέσουν νέες στο οπλοστάσιο τους, προκειμένου να αντιμετωπίσουν τα εξελιγμένα μέτρα προστασίας και αποτροπής των σύγχρονων δικτύων. Πολλά μοντέλα επιθέσεων μάλιστα επικεντρώνονται αποκλειστικά σε μια συγκεκριμένη τεχνολογία. Το σύνολο των επιθέσεων αυτών μπορεί να επιφέρει, όπως έχει αποδειχθεί, σημαντικά πλήγματα στις τεχνολογίες αυτές και να υπονομεύσει σοβαρά την ασφάλεια και την ανωνυμία των χρηστών τους.

Βεβαίως, όσο οι επιθέσεις εξελίσσονται, τόσο οι μηχανικοί δικτύων επικεντρώνουν την έρευνα τους για την ανάπτυξη προστατευτικών μηχανισμών οι οποίοι μπορούν να αντιμετωπίσουν επιτυχώς τυχόν ύποπτη δραστηριότητα εντός του δικτύου και να υποβάλλουν εγκαίρως τους κακόβουλους χρήστες. Σε όλα αυτά τα αντίμετρα φυσικά, υπάρχει ένας κοινός παρονομαστής. Αυτός δεν είναι άλλος από το trade-off, που σε κάθε περίπτωση πρέπει να επιτευχθεί, μεταξύ της ασφάλειας και της λειτουργικότητας του δικτύου. Είναι αυταπόδεικτο ότι, όσο προσθέτονται μηχανισμοί προστασίας, είτε ενεργοί είτε παθητικοί, σε ένα δίκτυο, τόσο μεγαλώνει το διαχειριστικό overhead και το latency, με αποτέλεσμα όχι μόνο να μειώνεται το UX αλλά πολλές φορές ακόμα και να καθίσταται αδύνατη η χρήση του δικτύου. Έτσι, θα πρέπει πάντα να αναζητείται η λεπτή ισορροπία μεταξύ της προστασίας της ανωνυμίας και της ικανότητας του δικτύου να εξυπηρετεί μεγάλο πλήθος χρηστών και απαιτητικές διαδικτυακές εφαρμογές.

Αντίστοιχα διλήμματα φυσικά υπάρχουν και στην πλευρά των επιτιθέμενων. Και στην περίπτωση αυτή θα πρέπει να σταθμιστεί το κόστος σε πόρους και χρόνο μιας επίθεσης σε σχέση με το προσδοκώμενο αποτέλεσμα. Θα πρέπει εξάλλου να τονιστεί ότι στόχος των μέτρων προστασίας δεν είναι η εξ ολοκλήρου αποτροπή των επιθέσεων, αλλά σε πολλές περιπτώσεις η αποθάρρυνση του επιτιθέμενου, μέσω εισαγωγής μεγάλου κόστους και πολυπλοκότητας υλοποίησης τους.

Όπως έχει αναλυθεί και στο αντίστοιχο κεφάλαιο των επιθέσεων, οι δυνατότητες του επιτιθέμενου είναι το σημείο κλειδί για την επιτυχή έκβαση μιας τέτοιας επίθεσης. Δε θα ήταν υπερβολή να αναφερθεί ότι ο κύριος αντίπαλος των τεχνολογιών αυτών, η κύρια δηλαδή πηγή επιθέσεων, είναι οι κυβερνήσεις και οι μυστικές υπηρεσίες. Οι οντότητες αυτές έχουν αυξημένες δυνατότητες σε πόρους αλλά και πρόσβασης στη δικτυακή υποδομή πάνω στην οποία υλοποιούνται οι τεχνολογίες ανωνύμων επικοινωνιών, με αποτέλεσμα να είναι σε θέση να επιφέρουν σημαντικά πλήγματα σε αυτές και να μπορούν να ταυτοποιήσουν τους χρήστες τους. Φυσικά, διάφορες εγκληματικές οργανώσεις που διαπράττουν κυβερνοεγκλήματα είναι επίσης σε θέση να υπονομεύσουν την ανωνυμία που παρέχουν

αυτά τα δίκτυα, εξαπολύοντας εξελιγμένες επιθέσεις, κυρίως εναντίον δικτύων που χρησιμοποιούνται για ανώνυμες επικοινωνίες για κρατικούς, στρατιωτικούς και διπλωματικούς σκοπούς.

Αξίζει επιπλέον να γίνει μια αναφορά στα ηθικά ζητήματα που προκύπτουν από τη χρήση των ανωνύμων επικοινωνιών και των επιθέσεων εναντίον τους. Σε πολλές περιπτώσεις, οι τεχνολογίες αυτές έχουν χρησιμοποιηθεί για τη διενέργεια παράνομων δραστηριοτήτων, όπως η διακίνηση όπλων, ναρκωτικών ουσιών, παιδικής πορνογραφίας αλλά και για την επικοινωνία μεταξύ μελών εγκληματικών και τρομοκρατικών οργανώσεων. Παράλληλα, τα δίκτυα αυτά αποτελούν μια μόνιμη πηγή κυβερνοεπιθέσεων διαφόρων ειδών, καθώς αποκρύπτουν ικανοποιητικά τη δραστηριότητα και την ταυτότητα των hackers, με αποτέλεσμα να καθίσταται εξαιρετικά δύσκολος ο εντοπισμός τους. Πολλές από τις επιθέσεις που έχουν περιγραφεί στην παρούσα διπλωματική εργασία έχουν χρησιμοποιηθεί για την αποκάλυψη τέτοιων δραστηριοτήτων, βοηθώντας σημαντικά στην καταπολέμηση του οργανωμένου εγκλήματος. Στον αντίποδα, πολλές επιθέσεις έχουν χρησιμοποιηθεί από απολυταρχικά καθεστώτα για τη λογοκρισία περιεχομένου και την απαγόρευση πρόσβασης των πολιτών σε νόμιμους στον υπόλοιπο κόσμο ιστοτόπων. Τέλος, οι επιθέσεις εναντίων των δικτύων αυτών από μυστικές υπηρεσίες αποτελεί πολλές φορές προϊόν κατασκοπείας, παραβιάζοντας διεθνείς συμβάσεις και νόμους.

Τα δίκτυα ανωνύμων επικοινωνιών εν γένει συγκεντρώνουν ένα μεγάλο, ετερόκλητο πλήθος χρηστών, οι οποίοι επιθυμούν την κάλυψη συγκεκριμένων αναγκών. Από απλούς χρήστες που επιθυμούν να περιηγηθούν στο διαδίκτυο με ένα μεγαλύτερο βαθμό ανωνυμίας, έως χρήστες που προσπαθούν να αποκτήσουν πρόσβαση σε λογοκριμένο περιεχόμενο, ακόμα και χρήστες που επιθυμούν να υλοποιήσουν παράνομες συναλλαγές.

Σε κάθε περίπτωση το ζήτημα της ιδιωτικότητας και της ανωνυμίας στο διαδίκτυο αναμένεται να απασχολήσει σημαντικά όλους τους εμπλεκόμενους φορείς, καθώς ήδη έχει ξεκινήσει η αντιπαράθεση μεταξύ των υποστηρικτών των δικαιωμάτων των χρηστών για πλήρη διαφάνεια στις επικοινωνίες και των κυβερνήσεων και παρόχων υπηρεσιών διαδικτύου που υποστηρίζουν ότι πρέπει να έχουν ένα βαθμό ελέγχου πάνω στη δραστηριότητα που συντελείται στο διαδίκτυο. Επιπλέον, οι μεγάλοι τεχνολογικοί κολοσσοί επηρεάζονται επίσης, καθώς η χρήση τέτοιων δικτύων τους στερεί τα πολύτιμα δεδομένα των χρηστών-πελατών τους, τα οποία τους επιφέρουν έσοδα δισεκατομμυρίων, με νόμιμους ή και όχι, μερικές φορές, τρόπους.

Ήδη έχει παρατηρηθεί διχογνωμία όσον αφορά τη χρήση των κρυπτονομισμάτων, η φύση των οποίων φέρει σημαντικές ομοιότητες, ορισμένες ως προς τις χρησιμοποιούμενες τεχνολογίες, αλλά σίγουρα και ως προς τον σκοπό τους. Ήδη αρκετές βιομηχανίες και κυβερνήσεις αντιδρούν σθεναρά ως προς τη χρήση των κρυπτονομισμάτων, καθώς δεν έχουν κανέναν απολύτως έλεγχο πάνω σε αυτά, κάτι που ανατρέπει πλήρως το έως τώρα οικονομικό μοντέλο. Αυτό φυσικά διασφαλίζει τους χρήστες τους από κρατικό παρεμβατισμό και διάφορες απαγορεύσεις. Από την άλλη, τα κρυπτονομίσματα αποτελούν πλέον το κύριο μέσο συναλλαγών για παράνομες δραστηριότητες στο διαδίκτυο, ενώ υπόκεινται και σε τρομερές μεταβολές όσον αφορά την αξία τους, κάτι που μπορεί να οδηγήσει σε σημαντικές απώλειες τους χρήστες τους.

Ομοίως με το παραπάνω παράδειγμα, η εντεινόμενη αναζήτηση της ανωνυμίας από πλευράς των χρηστών δημιουργεί παρόμοια ζητήματα στις κυβερνήσεις και τους τεχνολογικούς κολοσσούς, που πλέον παρατηρούν ότι χάνουν τον έλεγχο που είχαν έως τώρα σχετικά με τη δραστηριότητα των χρηστών το διαδίκτυο. Έτσι, οι τεχνολογίες αυτές διασφαλίζουν μεν τα θεμελιώδη δικαιώματα των

χρηστών, μπορούν όμως εύκολα να αποτελέσουν πεδίο μηδενικού ελέγχου από πλευράς των μηχανισμών ελέγχου εκτινάσσοντας τις παράνομες δραστηριότητες, όπως οι κυβερνοεπιθέσεις.

Τέλος, αξίζει να γίνει αναφορά στην εξέλιξη των παραπάνω τεχνολογιών και επιθέσεων. Η σημερινή εποχή είναι μια εποχή μετάβασης στο Internet of Everything και την Τεχνητή Νοημοσύνη. Ήδη τέτοιες τεχνολογίες χρησιμοποιούνται σε κάποιο βαθμό και αναμένεται να αυξηθούν κατακόρυφα τα επόμενα χρόνια. Οι επιθέσεις εναντίον των δικτύων ακολουθούν τις εξελίξεις αυτές, επιστρατεύοντας νέες Deep Learning τεχνικές για την ταχύτερη και ακριβέστερη ανάλυση της δικτυακής κίνησης. Τα νέα αυτά μοντέλα επιθέσεων έχουν ήδη μελετηθεί, ως ένα βαθμό, με τα αποτελέσματα να δείχνουν ότι οι αλγόριθμοι αυτοί μπορούν να μελετήσουν εύκολα και γρήγορα εκατομμύρια δείγματα network traces και να προβούν σε συσχετίσεις με παλαιότερα αποτελέσματα ερευνών, προκειμένου να υλοποιήσουν ακριβέστερα Website Fingerprints ή Timing και Latency Analysis του δικτύου. Νευρωνικά Δίκτυα επίσης επιστρατεύονται για την υλοποίηση τέτοιων επιθέσεων, δίνοντας νέα μοντέλα τα οποία παρουσιάζουν συντριπτικά ποσοστά επιτυχίας, της τάξης του 96%.

Φυσικά, οι ίδιες τεχνολογίες μπορούν να χρησιμοποιηθούν και από τους σχεδιαστές των δικτύων για να αναπτύξουν νέα μοντέλα αμυντικών μηχανισμών που θα είναι σε θέση να αποτρέψουν τις προαναφερθείσες επιθέσεις. Οι Deep Learning μέθοδοι μπορούν να επιστρατευτούν για την ανάλυση κακόβουλης δικτυακής κίνησης που έχει συγκεντρωθεί, προκειμένου να εκπαιδευτούν οι μηχανισμοί αποτροπής για τον ταχύτερο εντοπισμό επιθέσεων και τη θωράκιση των δικτύων. Επιπλέον, οι παραπάνω μέθοδοι μπορούν να ενισχύσουν σημαντικά τις ικανότητες των adaptive αμυντικών μηχανισμών, προκειμένου εκείνοι να λαμβάνουν γρήγορες αποφάσεις για την αυστηρότητα και το επίπεδο προστασίας του δικτύου, αναλόγως του περιβάλλοντος και του ρίσκου επίθεσης.

Συμπερασματικά, οι τεχνολογίες ανωνύμων επικοινωνιών αποτελούν ένα εξαιρετικά ευρύ πεδίο έρευνας το οποίο θα συνεχίσει να αναπτύσσεται δυναμικά, λαμβανοντας ώθηση από τις σύγχρονες τεχνολογίες. Ο αέναος αγώνας μεταξύ των επιτιθέμενων και των σχεδιαστών του δικτύου οδηγεί σε συνεχείς καινοτομίες, οι οποίες ωστόσο δεν είναι πάντα εύκολα εφαρμόσιμες και είναι καταδικασμένες να παραμείνουν σε πειραματικό επίπεδο. Έχοντας ευρύ πεδίο εφαρμογής, από απλούς χρήστες έως και άκρως απόρρητες στρατιωτικές επικοινωνίες, είναι βέβαιο ότι θα αποτελέσουν ένα από τα πλέον ανερχόμενα τεχνολογικά πεδία στο μέλλον, τόσο στο κομμάτι της έρευνας και ανάπτυξης νέων τεχνολογιών, όσο και στην εξέλιξη των επιθέσεων εναντίον τους.

Βιβλιογραφία

[1] Kesdogan, D., Egner, J., & Büschkes, R. (1998). *Stop-and-Go-MIXes providing probabilistic anonymity in an open system.* In D. Aucsmith (Ed.), Information hiding (pp. 83-98). LNCS 1525, Berlin: Springer-Verlag.
[2] Marques, R., & Zuquete, A. (2011). *A social networking for anonymous communication systems: A survey.* Proceedings of the International Conference on Computational Aspects of Social Networks CASoN, 249 – 254.

[3] Nambiar, A., & Wright, M. (2006). Salsa: *A structured approach to large-scale anonymity.* Proceedings of the 13th ACM Conference on Computer and Communications Security CCS'06, New York, NY, USA: ACM, 17–26.
[4] Mittal, P., & Borisov, N. (2012). *Information leaks in structured peer-to-peer anonymous communication systems.* ACM Transactions on Information and System Security, 15(1), 5:1-5:28
[5] Danezis, G., & Serjantov, A. (2005). *Statistical disclosure or intersection attacks on anonymity systems.* Information Hiding, LNCS 3200, Berlin: Springer-Verlag, 293-308.
[6] Corrigan-Gibbs, H., & Ford, B. (2010). *Dissent: Accountable anonymous group messaging.* Proceedings of the 17th ACM Conference on Computer and Communications Security CCS'10, pp. 340-350. ACM.
[7] Clarke, I., Sandberg, O., Wiley, B., & Hong, T. W. (2001). *Freenet: A distributed anonymous information sTorage and retrieval system.* Proceeding of the International Workshop on Designing Privacy Enhancing Technologies: Design Issues in Anonymity and Unobservability, New York: Springer-Verlag, 46-66.
[8] Dingledine, R., Mathewson, N., & Syverson, P. (2004). *Tor: The second-generation onion router.* Naval Research Lab, Washington DC.
[9] Freedman, M. J., Sit, E. Cates, J., & Morris, R. (2002). *Introducing Tarzan, a Peer-to-Peer Anonymizung Network Layer.* Electronic Proceedings for the 1st International Workshop on Peer-to-Peer Systems IPTPS'02, Cambridge, MA, USA.
[10] Goldschlag, D. M., Reed, M. G., & Syverson, P. F. (1996). *Hiding routing information.* Proceedings of Information Hiding: First International Workshop, 137–150.
[11] Abbott, T. G., Lai, K. J., Lieberman, M. R., & Price, E. C. (2007). *Browser-based attacks on Tor.* PET'07 Proceedings of the 7th International Conference on Privacy Enhancing Technologies, pp. 184-199. Berlin, Heidelberg: Springer-Verlag.
[12] Balachandran, N., & Sanyal, S. (2012). *A review of techniques to mitigate Sybil attacks.* International Journal of Advanced Networking and Applications, 4(1), 1514-1518.
[13] Chaum, D. L. (1988). *The dining cryptographers problem.* Journal of Cryptology 1(1), 65-75.
[14] Chen, T. M., & Wang, V. (2010). *Web filtering and censoring.* Computer, 43(3), 94-97.
[15] Goel, S., Robson, M., Polte, M., & Sirer, E. G. (2003). *Herbivore: A scalable and efficient protocol for anonymous communication.* Technical Report TR2003-1890. Ithaca, New York: Cornell University, Computing and Information Science.
[16] Reiter, M. K., & Rubin, A. D. (1998) *Crowds: Anonymity for web transactions.* ACM Transactions on Information System Security, 1(1), 66–92.
[17] Reed, M. G., Syverson, P. F., & Goldschlag, D. M. (1998). *Anonymous connections and onion routing.* IEEE Journal on Selected Areas in Communications, 16(4), 482–494.
[18] Syverson, P., Tsudik, G., Reed, M., & Landwehr, C. (2000). *Towards an analysis of onion routing security.* In H. Federrath (Ed.), Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, Berlin: Springer-Verlag, 96-114.
[19] Shmatikov, V., & Wang, M.-S. (2006). *Timing analysis in low-latency mix networks: Attacks and defenses.* Proceedings of the 11th European Symposium on Research in Computer Security ESORICS, Hamburg, Germany: Springer-Verlag, LNCS 4189, 18-33.
[20] Wright, M., Adler, M., Levine, B. N., & Shields, C. (2004). *The predecessor attack: An analysis of a threat to anonymous communications systems.* ACM Transactions on Information and System Security (TIS-SEC), 4, 489–522.
[21] Wolinsky, D. I., Syta, E., & Ford, B. (2013). *Hang with your buddies to resist intersection attacks.* Proceedings of the ACM Conference on Computer and Communications Security CCS, ACM.

[22] Kesdogan, D., Egner, J., and Buschkes, R. 1998. *Stop-and-go-mixes providing probabilistic anonymity in an open system.* In Information Hiding (April 1998).
[23] Levine, B. N., Reiter, M., Wang, C., and Wright, M. 2004. *Stopping timing attacks in low-latency mix-based systems.* In Proc. Financial Cryptography (February 2004).
[24] Scarlatta, V., Levine, B., and Shields, C. 2001. *Responder anonymity and anonymous peer-to-peer file sharing.* In Proc. IEEE International Conference on Network Protocols (ICNP) (November 2001).
[25] Schneier, B. 1996 . *Applied Cryptography.* J. Wiley and Sons.
[26] Wright, M., Adler, M., Levine, B., and Shields, C. 2002. *An analysis of the degradation of anonymous protocols.* In ISOC Symposium on Network and Distributed System Security (February 2002).
[27] J. Brickell and V. Shmatikov. *Efficient anonymity-preserving data collection.* In 12th KDD, pages 76–85, Aug. 2006.
[28] O. Berthold, H. Federrath, and M. Kohntopp. *Project "anonymity and unobservability in the internet".* In CFP, April 2000.
[29] O. Berthold and H. Langos. *Dummy traffic against long term intersection attacks.* In 2nd PET, 2002.
[30] O. Berthold, A. Pfitzmann, and R. Standtke. *The disadvantages of free MIX routes and how to overcome them.* In Workshop on Design Issues in Anonymity and Unobservability, pages 30–45, July 2000.
[31] P. Golle and A. Juels. *Dining cryptographers revisited.* Eurocrypt, pages 456–473, May 2004.
[32] S. Han et al. *Expressive privacy control with pseudonyms.* In SIGCOMM, Aug. 2013.
[33] D. Chaum, A. Fiat, and M. Naor. *Untraceable electronic cash.* In CRYPTO, Aug. 1988.
[34] D. J. Kelly. *A taxonomy for and analysis of anonymous communications networks.* PhD thesis, Wright Patterson AFB, OH, USA, 2009. AAI3351544.
[35] A. Pfitzmann and M. Hansen. *A terminology for talking about privacy by data minimization:Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management.* Aug. 2010.
[36] N. S. Evans, R. Dingledine, and C. Grothoff. *A practical congestion attack on Tor using long paths.* In 18th USENIX Security, Aug. 2009.
[37] J. R. Douceur. *The Sybil attack.* In 1st International Workshop on Peer-to-Peer Systems, pages 251–260, Mar. 2002.
[38] B. Ford and J. Strauss. *An offline foundation for online accountable pseudonyms.* In 1st International Workshop on Social Network Systems (SocialNets), 2008.
[39] C. Diaz, S. Seys, J. Claessens, and B. Preneel. *Towards measuring anonymity.* In Proceedings of the 2nd international conference on Privacy enhancing technologies, PET'02, 2003.
[40] V. Shmatikov and M.-H. Wang. *Measuring relationship anonymity in mix networks.* In WPES, Oct. 2006.
[41] J.-F. Raymond. *Traffic analysis: Protocols, attacks, design issues and open problems.* In Workshop on Design Issues in Anonymity and Unobservability, pages 10–29, 2000.
[42] Andreas Pfitzmann and Marit Hansen. *Anonymity, Unobservability, and Pseudonymity: A Consolidated Proposal for Terminology.* July 2000.
[43] C. A. Neff. *A verifiable secret shuffle and its application to e-voting.* In CCS, pages 116–125, Nov. 2001.
[44] S. J. Murdoch and G. Danezis. *Low-cost traffic analysis of Tor.* In IEEE Security and Privacy, pages 183–195, May 2005.

[45] E. G. Sirer, S. Goel, M. Robson, and D. Engin. *Eluding carnivores: File sharing with strong anonymity.* In SIGOPS EW, Sept. 2004.
[46] N. Tran, B. Min, J. Li, and L. Submaranian. *Sybil-resilient online content voting.* In 6th NSDI, pages 15–28, Apr. 2009.
[47] M. K. Wright, M. Adler, B. N. Levine, and C. Shields. *Passive-logging attacks against anonymous communications systems.* TISSEC, May 2008.
[48] H. Gao, J. Hun. *Security Issues in Online Social Networks.* In Proc of IEEE Internet Computing, Volume 15, No.4, 2011.
[49] R. Sherwood, B. Bhattacharjee, and A. Srinivasan, *P5: A Protocol for Scalable Anonymous Communication.* Proc. IEEE Symp. Security and Privacy (S&P '02), pp. 53-65, May 2002.
[50] G. Danezis, P. Mittal, *SybilInfer: Detecting Sybil Nodes using Social Networks.* in: NDSS, 2009.
[51] H. Yu, M. Kaminsky, P. B. Gibbons, A. D. Flaxman, *Sybilguard: defending against sybil attacks via social networks.* IEEE/ACM Trans.Netw. 16 (3) (2008) 576 589.
[52] H. Yu, P. B. Gibbons, M. Kaminsky, F. Xiao, *Sybillimit: a near-optimal social network defense against sybil attacks.* IEEE/ACM Trans.Netw. 18 (3) (2010) 885 898.
[53] N. Danner, D. Krizanc, M. LiberaTore, *Detecting denial of service attacks in Tor.* in: R. Dingledine, P. Golle (Eds.), Financial Cryptography and Data Security, Vol. 5628 of Lecture Notes in Computer Science, Springer Berlin Heidelberg, 2009, pp. 273 284.
[54] Liang Wang and Jussi Kangasharju. *Real-World Sybil Attacks in BitTorrent Mainline DHT.* In: Globecom. IEEE, 2012. URL: https: / / nymity. ch / sybilhunting / pdf /Wang2012a. pdf (cit. On p. 1).
[55] Philipp Winter et al. *Spoiled Onions: Exposing Malicious Tor Exit Relays.* In: PETS. Springer, 2014. URL: https://nymity.ch/sybilhunting/pdf/Winter2014a.pdf (cit. on pp. 1, 3, 4).
[56] H. Yu, *Sybil defenses via social networks: A tutorial and survey.* SIGACT News, vol. 42, no. 3, pp. 80–101, 2011.
[57] Alex Biryukov, Ivan Pustogarov, and Ralf-Philipp Weinmann. *Trawling for Tor Hidden Services: Detection, Measurement, Deanonymization.* In: Security & Privacy. IEEE, 2013. URL:https://nymity.ch/sybilhunting/pdf/Biryukov2013a.pdf (cit. On pp. 2, 7, 9, 10, 13).
[58] Kevin Bauer and Damon McCoy. *No more than one server per IP address.* Mar. 2007. URL: https : / / gitweb . Torproject . org /Torspec.git/tree/proposals/109-no-sharing-ips.txt (cit. on p. 3).
[59] Herrmann, M., Grothoff, C.: *Privacy-implications of performance-based peer selection by onion-routers: a real-world case study using I2P.* In: Proceedings of the 11th international conference on Privacy enhancing technologies. PETS'11, Berlin, Heidelberg, Springer-Verlag (2011) 155–174
[60] Timpanaro, J.P., Chrisment, I., FesTor, O.: *MoniToring the I2P network.*
[61] Wolchok, S., Hofmann, O.S., Heninger, N., Felten, E.W., Halderman, J.A., Rossbach, C.J., Waters, B., Witchel, E.: *Defeating Vanish with low-cost Sybil attacks against large DHTs.* In: Proc. of NDSS. (2010)
[62] [21]L. Lamport, R. Shostak, M. Pease, *The Byzantine Generals Problem.* TPLS 4(3), 1982.
[63] D. Dean, A. Stubblefield, *Using Client Puzzles to Protect TLS.* 10th USENIX Security Symp., 2001.
[64] C. Ellison, *Establishing Identity Without Certification Authorities.* 6th USENIX Security Symposium, 1996, pp. 67-76.
[65] A. Fiat, A. Shamir, *How to Prove Yourself: Practical Solutions of Identification and Signature Problems.* Crypto '86, 1987, pp. 186-194.
[66] D. Chaum, *Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms.* CACM 4 (2), 1982.
[67] T. Aura, P. Nikander, J. Leiwo, *DoS-Resistant Authentication with Client Puzzles.* Cambridge Security Protocols Workshop, Springer, 2000.

[68] G. Bissias, A. P. Ozisik, B. N. Levine, and M. LiberaTore. *Sybil-resistant mixing for bitcoin.* In Proceedings of the 13th Workshop on Privacy in the Electronic Society, pages 149–158. ACM, 2014.
[69] B. Viswanath, A. Post, K. P. Gummadi, and A. Mislove. *An analysis of social network-based sybil defenses.* ACM SIGCOMM Computer Communication Review, 41(4):363–374, 2011.
[70] J. E. Holt and K. E. Seamons. *Nym: Practical pseudonymity for anonymous networks.* Internet Security Research Lab Technical Report, 4:1–12, 2006.
[71] W. Chang, J. Wu, C. Tan, and F. Li, *Sybil defenses in mobile social networks.* in Proc. IEEE Conf. Global Commun. (GLOBECOM), 2013, pp. 1–6.
[72] A. Cheng and E. Friedman, *Sybilproof reputation mechanisms.* in Proc. SIGCOMM Workshop, 2005, pp. 128–132.
[73] L. Shi, S. Yu, W. Lou, and Y. T. Hou, *SybilShield: An agent aided social network-based Sybil defense among multiple communities.* in Proc. IEEE Conf. Comput. Commun. (INFOCOM), 2013, pp. 1034–1042.
[74] W. Wei, F. Xu, C. Tan, and Q. Li, SybilDefender: *Defend against Sybil attacks in large social networks.* in Proc. IEEE Conf. Comput. Commun. (INFOCOM), 2012, pp. 1951–1959.
[75] Q. Cao and X. Yang, *SybilFence: Improving social-graph-based Sybil defenses with user negative feedback.* Duke Univ., Comput. Sci., Tech. Rep. CS-TR-2012-05, Mar. 2012 [Online]. Available: http://arxiv.org/abs/1304.3819
[76] L. Bilge, T. Strufe, D. Balzarotti, and E. Kirda, *All your contacts are belong to us: Automated identity theft attacks on social networks.* in Proc. 18th Int. Conf. World Wide Web (WWW), 2009.
[77] D. Quercia and S. Hailes, *Sybil attacks against mobile users: Friends and foes to the rescue.* in Proc. IEEE IEEE Conf. Comput. Commun. (INFOCOM), 2010, pp. 336–340.
[78] Z. Yang et al., *Uncovering social network Sybils in the wild.* in Proc. Int. Microelectron. Conf. (IMC), 2011, pp. 259–268.
[79] L. Alvisi, A. Clement, A. Epasto, S. Lattanzi, and A. Panconesi, *SoK: The evolution of Sybil defense via social networks.* in IEEE Symp. Security Privacy, 2013, pp. 382–396.
[80] B. Yu, C. Xu, and B. Xiao, *Detecting Sybil attacks in VANETs.* J. Parallel Distrib. Comput., vol. 73, no. 6, pp. 746–756, 2013.
[81] K. J., Forss, T., & Pulkkis, G. (2014). *Anonymous communication on the internet.* Proceedings of Informing Science & IT Education Conference (InSITE) 2014 (pp. 103-120). Retrieved from http://Proceedings.InformingScience.org/InSITE2014/InSITE14p103-120Grahn0483.pdf
[82] *SmartHide Overview* (2013). Retrieved from http://smarthide.com/overview
[83] Levine, B. N., & Shields, C., (2002). *Hordes – A multicast based protocol for anonymity.* Journal of Computer Security, 10(3), 213-240.
[84] Berthold, O., Pfitzmann, A., and Standtke, R. (2000). *The disadvantages of free MIX routes and how to overcome them.* In Designing Privacy Enhancing Technologies, LNCS Vol. 2009, pages 30–45. Springer-Verlag. http://www.tik.ee.ethz.
[85] Serjantov, A. and Danezis, G. (2002). *Towards an information theoretic metric for anonymity.* In Proceedings of the Privacy Enhancing Technologies Workshop 2002, San Francisco, CA.
[86] Agrawal, D., Kesdogan, D., Penz, S.: *Probabilistic Treatment of MIXes to Hamper Traffic Analysis.* In: Proceedings of the 2003 IEEE Symposium on Security and Privacy (May 2003)
[87] Berthold, O., Pfitzmann, A., Standtke, R.: *The disadvantages of free MIX routes and how to overcome them.* In: Federrath, H. (ed.) *Designing Privacy Enhancing Technologies.* LNCS, vol. 2009, pp. 30–45. Springer, Heidelberg (2000)
[88] Danezis, G.: *Mix-networks with restricted routes.* In: Dingledine, R. (ed.) PET 2003. LNCS, vol. 2760, Springer, Heidelberg (2003)

[89] Danezis, G.: *Statistical disclosure attacks.* In: Samarati, K.G., Vimercati (eds.) Proceedings of Security and Privacy in the Age of Uncertainty (SEC2003), Athens, May 2003. IFIP TC11, pp. 421–426. Kluwer, Dordrecht (2003)
[90] Diaz, C., Serjantov, A.: *Generalising mixes.* In: Dingledine, R. (ed.) PET 2003. LNCS, vol. 2760, Springer, Heidelberg (2003)
[91] Kesdogan, D., Agrawal, D., Penz, S.: *Limits of anonymity in open environments.* In: Petitcolas, F.A.P. (ed.) IH 2002. LNCS, vol. 2578, Springer, Heidelberg (2003)
[92] Serjantov, A., Dingledine, R., Syverson, P.: *From a trickle to a flood: Active attacks on several mix types.* In: Petitcolas, F.A.P. (ed.) IH 2002. LNCS, vol. 2578, Springer, Heidelberg (2003)
[93] Serjantov, A., Newman, R.E.: *On the anonymity of timed pool mixes.* In: Proceedings of the Workshop on Privacy and Anonymity Issues in Networked and Distributed Systems, Athens, Greece, May 2003, pp. 427–434. Kluwer, Dordrecht (2003)
[94] P. Piyawongwisal, P. Xia. *Sybil Attack and Defense in P2P Networks*, In Advanced Computer Networks, CS 238, University of Illinois, 2011.
[95] W. Luo, J. Liu, J.L. Liu, C. Fan. *An Analysis of Security in Social Networks.* In IEEE Dependable, Autonomic and Secure Computing, 2009.
[96] B. Wellman, *Computer networks as social networks.* Science 293: 2031-2034, 2001.
[97] A.A. Hasib. *Threats of Online Social Networks.* In IJCSNS, 2009.
[98] G. Wang et al. *You are how you click: Clickstream analysis for Sybil detection*, In Proc of 22nd USENIX Security Symp, 2013.
[99] G. Wang et al. *Social turing tests: Crowdsourcing Sybil detection.* In Proc of Netw. Distrib Syst security symp (NDSS), 2012.
[100] H. Yu, P. B. Gibbons, and M. Kaminsky. *Brief announcement: Toward an optimal social network defense against sybil attacks.* In ACM PODC, 2007.
[101] N. B. Margolin and B. N. Levine. *Quantifying and discouraging sybil attacks.* Technical report, U. Mass. Amherst, Computer Science, 2005.
[102] G. Danezis, C. Lesniewski-Laas, M. F. Kaashoek, and R. Anderson. *Sybil-resistant DHT routing.* In ESORICS, 2005. Springer-Verlag LNCS 3679.
[103] R. John, Jacob P. Cherian, Jubilant J. Kizhakkethottam *A survey of techniques to prevent sybil attacks* 2015 International Conference on Soft-Computing and Networks Security (ICSNS)
[104] *eDonkey File Sharing System*, 2003.
[105] R. Bhagwan, S.Savage, and G. Voelker. *Understanding Availability.* In 2nd International Workshop on Peer-to-Peer Systems, 2003.
[106] Fabrizio Cornelli, Ernesto Damiani, Sabrina De Capitani di Vimercati, Stefano Paraboschi, and Pierangela Samarati. *Choosing Reputable Servents in a P2P Network.* In WWW, pages 376–386, 2002.
[107] George Danezis, Roger Dingledine, and Nick Mathewson. *Mixminion: Design of a Type III Anonymous Remailer Protocol.* In Proceedings of the 2003 Symposium on Security and Privacy, pages 2–15. IEEE Computer Society, May 11–14 2003.
[108] Sepandar D. Kamvar, Mario T. Schlosser, and Hector Garcia-Molina. *The Eigentrust Algorithm for Reputation Management in P2P Networks.* In WWW, pages 640–651, 2003.
[109] Parisa Tabriz, Nikita Borisov. *Breaking the Collusion Detection Mechanism of MorphMix*
[110] Marc Rennhard. *MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection.* January 2002
[111] R. Dingledine, M. J. Freedman, D. Hopwood, and D. Molnar. *A reputation system to increase MIX-net reliability.* In I. S. Moskowitz, editor, Information Hiding, volume 2137 of Lecture Notes in Computer Science, pages 126–141, Pittsburgh, PA, 2001. Springer Berlin / Heidelberg.

[112] R. Dingledine and N. Mathewson. *Anonymity loves company: Usability and the network effect.* In R. Anderson, editor, Fifth Workshop on the Economics of Information Security (WEIS), Cambridge, UK, June 2006.
[113] L. Zhuang, F. Zhou, B. Y. Zhao, and A. Rowstron. *Cashmere: Resilient anonymous routing.* In USENIX Symposium on Networked Systems Design and Implementation (NSDI), Boston, MA, May 2005.
[114] C. Park, K. Itoh, and K. Kurosawa. *Efficient anonymous channel and all/nothing election scheme.* In T. Helleseth, editor, Advances in Cryptology (EUROCRYPT), volume 765 of Lecture Notes in Computer Science, pages 248–259, Lofthus, Norway, 23-27 May 1993. Springer Berlin / Heidelberg.
[115] L. Øverlier and P. Syverson. *Valet services: Improving hidden servers with a personal touch.* In Sixth Workshop on Privacy Enhancing Technologies (PET), volume 4258 of Lecture Notes in Computer Science, pages 223–244, Cambridge, UK, June 2006. Springer Berlin / Heidelberg.
[116] M. Jakobsson, A. Juels, and R. L. Rivest. *Making mix nets robust for electronic voting by randomized partial checking.* In D. Boneh, editor, USENIX Security Symposium, pages 339–353, San Francisco, CA, Aug. 2002. USENIX Association.
[117] P. H. O'Neill. Tor's Ex-director: *'The Criminal Use of Tor has Become Overwhelming'.* https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop, May 2017. Cyberscoop Online News Article.
[118] V. Pappas, E. Athanasopoulos, S. Ioannidis, and E. P. Markatos. *Compromising Anonymity using Packet Spinning.* In International Conference on Information Security, 2008.
[119] K. Poulsen. *Feds Are Suspects in New Malware That Attacks Tor Anonymity.* https://www.wired.com/2013/08/freedom-hosting, August 2013. Wired Online News Article.
[120] A. Johnson, R. Jansen, N. Hopper, A. Segal, and P. Syverson. *Peer-Flow: Secure Load Balancing in Tor.* Proceedings on Privacy Enhancing Technologies (PoPETs), 2017(2), April 2017.
[121] S. Li, H. Guo, and N. Hopper. *Measuring Information Leakage in Website Fingerprinting Attacks and Defenses.* In Conference on Computer and Communications Security (CCS), 2018.
[122] R. Wails, Y. Sun, A. Johnson, M. Chiang, and P. Mittal. *Tempest: Temporal Dynamics in Anonymity Systems.* Proceedings on Privacy Enhancing Technologies (PoPETS), 2018(3), 2018.
[123] T. Wang and I. Goldberg. *Improved Website Fingerprinting on Tor.* In Workshop on Privacy in the Electronic Society (WPES), 2013.
[124] M. Mathis, J. Semke, J. Mahdavi, and T. Ott. *The Macroscopic Behavior of the TCP Congestion Avoidance Algorithm.* ACM Computer Communication Review, 27(3):67–82, 1997.
[125] R. Jansen, P. Syverson, and N. Hopper. *Throttling Tor Bandwidth Parasites.* In USENIX Security Symposium, 2012.
[126] R. Jansen, K. S. Bauer, N. Hopper, and R. Dingledine. *Methodically Modeling the Tor Network.* In Workshop on Cyber Security Experimentation and Test (CSET), 2012.
[127] J. Hayes and G. Danezis. *k-fingerprinting: a Robust Scalable Website Fingerprinting Technique.* In USENIX Security Symposium, 2016.
[128] D. Herrmann, R. Wendolsky, and H. Federrath. *Website Fingerprinting: Attacking Popular Privacy Enhancing Technologies with the Multinomial Naive-Bayes Classifier.* In Workshop on Cloud Computing Security, 2009.
[129] R. Jansen. *New Tor Denial of Service Attacks and Defenses.* https://blog.torproject.org/new-tor-denial-service-attacks-and-defenses, January 2014. Blog Post.
[130] R. Jansen and N. Hopper. *Shadow: Running Tor in a Box for Accurate and Efficient Experimentation.* In Network and Distributed System Security Symposium (NDSS), 2012.

[131] D. Gopal and N. Heninger. *Torchestra: Reducing Interactive Traffic Delays over Tor.* In Workshop on Privacy in the Electronic Society (WPES), 2012.
[132] D. Goulet. *Ongoing DDoS on the Network.* Tor-Project Email 001604, December 2017. https://lists.torproject.org/pipermail/tor-project/2017-December/001604.html.
[133] D. Fifield, C. Lan, R. Hynes, P. Wegmann, and V. Paxson. *Blocking-resistant Communication through Domain Fronting.* In Privacy Enhancing Technologies Symposium (PETS), 2015.
[134] R. Dingledine, N. Hopper, G. Kadianakis, and N. Mathewson. *OneFast Guard for Life (or 9 Months).* In Privacy Enhancing Technologies Symposium (PETS), 2014.
[135] M. AlSabah and I. Goldberg. *PCTCP: Per-circuit TCP-over-IPsec Transport for Anonymous Communication Overlay Networks.* In Conference on Computer and Communications Security (CCS), 2013.
[136] M. Alsabah and I. Goldberg. *Performance and Security Improvements for Tor: A Survey.* ACM Comput. Surv., 49(2):32:1–32:36, September 2016.
[137] M. V. Barbera, V. P. Kemerlis, V. Pappas, and A. D. Keromytis. *CellFlood: Attacking Tor Onion Routers on the Cheap.* In European Symposium on Research in Computer Security (ESORICS), 2013.
[138] N. Borisov, G. Danezis, P. Mittal, and P. Tabriz. *Denial of Service or Denial of Security?* In Conference on Computer and Communications Security (CCS), 2007.
[139] X. Cai, X. C. Zhang, B. Joshi, and R. Johnson. *Touching from a Distance: Website Fingerprinting Attacks and Defenses.* In Conference on Computer and Communications Security (CCS), 2012.
[140] H. Darir, H. Sibai, N. Borisov, G. Dullerud, and S. Mitra. *TightRope: Towards Optimal Load-balancing of Paths in Anonymous Networks.* In Workshop on Privacy in the Electronic Society (WPES), 2018.
[141] D. Goulet. *Circuit cell queue can fill up memory.* Tor Trac Ticket 25226, 2018. https://trac.torproject.org/projects/tor/
ticket/25226.
[142] B. Schneier. *Attacking Tor: how the NSA targets users' online anonymity.* https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity, October 2013. The Guardian Online News Article.
[143] Michael A. Padlipsky, David W. Snow, and Paul A. Karger. *Limitations of End-to-End Encryption in Secure Computer Networks.* The MITRE Corporation: Bedford MA, HQ Electronic Systems Division technical report ESD-TR-78-158, August 1978.
[144] Paul A. Karger. *Non-Discretionary Access Control for Decentralized Computing Systems*. Laboratory for Computer Science, Massachusetts Institute of Technology S. M. amp; E. E. thesis MIT/LCS/TR-179, May 1977.
[145] Ian Goldberg, David Wagner, and Eric Brewer. *Privacy-enhancing Technologies for the Internet.* In the Proceedings of the 42nd IEEE Spring COMPCON, February 1997.
[146] Lim, Dongwon & Zo, Hangjung & Lee, Dukhee. (2011). *The Value of Anonymity on the Internet.* 6629. 452-464. 10.1007/978-3-642-20633-7_33.
[147] Sardá, Thais & Natale, Simone & Sotirakopoulos, Nikos & Monaghan, Mark. (2019). *Understanding online anonymity. Media, Culture & Society.* 41. 016344371984207. 10.1177/0163443719842074.
[148] Marc Liberatore and Brian Neil Levine. *Inferring the Source of Encrypted HTTP Connections.* Proceedings of the 13th ACM conference on Computer and Communications Security (CCS 2006), November 2006, pages 255-263.

[149] Richard Clayton, Steven J. Murdoch, and Robert N. M. Watson. *Ignoring the Great Firewall of China.* In the Proceedings of the Sixth Workshop on Privacy Enhancing Technologies (PET 2006), Cambridge, UK, June 2006, pages 20-35.
[150] Andreas Pashalidis and Bernd Meyer. *Linking Anonymous Transactions: The Consistent View Attack.* In the Proceedings of the Sixth Workshop on Privacy Enhancing Technologies (PET 2006), Cambridge, UK, June 2006, pages 384-392.
[151] Ben Adida and Douglas Wikström. *How to Shuffle in Public.* In the Proceedings of the Theory of Cryptography 2007, February 2007.
[152] M. Edman, F. Sivrikaya, and B. Yener. *A Combinatorial Approach to Measuring Anonymity.* In Intelligence and Security Informatics, 2007 IEEE, May 2007, pages 356-363.
[153] Parvathinathan Venkitasubramaniam, Ting He, and Lang Tong. *Anonymous Networking amidst Eavesdroppers.* Pre-print available as arXiv:0710.4903v1 at arxiv.org, October 2007.
[154] Matthew Edman and Bülent Yener. *On anonymity in an electronic society: A survey of anonymous communication systems.* In ACM Computing Surveys 42(1), 2009, pages 1-35
[155] Prateek Mittal, Femi Olumofin, Carmela Troncoso, Nikita Borisov, and Ian Goldberg. *PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval.* In the Proceedings of the 20th USENIX Security Symposium, August 2011.
[156] Nguyen Phong Hoang, Panagiotis Kintis, and Manos Antonakakis. *An Empirical Study of the I2P Anonymity Network and its Censorship Resistance.* In the Proceedings of the Internet Measurement Conference 2018 (IMC '18), October 2018.
[157] Marc Rennhard and Bernhard Plattner. *Introducing MorphMix: Peer-to-Peer based Anonymous Internet Usage with Collusion Detection.* In the Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2002), Washington, DC, USA, November 2002.
[158] Wei Dai. *PipeNet 1.0* Post to Cypherpunks mailing list, January 1998. First written in 1996 based on cypherpunks posts in 1995.
[159] Jon McLachlan, Andrew Tran, Nicholas Hopper, and Yongdae Kim. *Scalable onion routing with Torsk.* In the Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 2009.
[160] Prateek Mittal and Nikita Borisov. *ShadowWalker: Peer-to-peer Anonymous Communication using Redundant Structured Topologies.* In the Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 2009.
[161] Andriy Panchenko, Arne Rache, and Stefan Richter. *NISAN: Network Information Service for Anonymization Networks.* In the Proceedings of the 2009 ACM Conference on Computer and Communications Security, CCS 2009, Chicago, Illinois, USA, November 2009.
[162] Roger Dingledine, Michael J. Freedman, and David Molnar. *The Free Haven Project: Distributed Anonymous Storage Service.* In the Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, July 2000.
[163] I. Stoica et al. *Chord: a scalable peer-to-peer lookup protocol for Internet applications.* IEEE/ACM Transactions on Networking, vol. 11, no. 1, pp. 17-32, Feb. 2003, doi: 10.1109/TNET.2002.808407.
[164] Rowstron, A. and P. Druschel. *Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer.* (2001).
[165] Zhao, Ben & Kubiatowicz, John & Joseph, Anthony. (2002). *Tapestry: a fault-tolerant wide-area application infrastructure.* Computer Communication Review. 32. 81.
[166] Dobzinski, Oren & Talmy, Anat. (2004). *Viceroy - on the implementation of a Peer to Peer network.*

[167] Kaashoek, M. & Karger, David. (2004). *Koorde: A Simple Degree-Optimal Distributed Hash Table.* Lecture Notes in Computer Science. 10.1007/978-3-540-45172-3_9.
[168] Nick Feamster, Magdalena Balazinska, Greg Harfst, Hari Balakrishnan, and David Karger. *Infranet: Circumventing Web Censorship and Surveillance.* In the Proceedings of the 11th USENIX Security Symposium, August 2002.
[169] Diogo Barradas, Nuno Santos, Luis Rodrigues, and Vítor Nunes. *Poking a Hole in the Wall: Efficient Censorship-Resistant Internet Communications by Parasitizing on WebRTC.* In the Proceedings of the 27th ACM Conference on Computer and Communications Security (CCS '20), November 2020.
[170] Milad Nasr, Hadi Zolfaghari, Amir Houmansadr, and Amirhossein Ghafari. *MassBrowser: Unblocking the Censored Web for the Masses, by the Masses.* In the Proceedings of the 27th Symposium on Network and Distributed System Security (NDSS '20), February 2020.
[171] Sajin Sasy and Ian Goldberg. *ConsenSGX: Scaling Anonymous Communications Networks with Trusted Execution Environments.* In Proceedings on Privacy Enhancing Technologies 2019(3), July 2019.
[172] Ludovic Barman, Mahdi Zamani, Italo Dacosta, Joan Feigenbaum, Bryan Ford, Jean-Pierre Hubaux, and David Wolinsky. *PriFi: Low-Latency Anonymity for Organizational Networks.* April 2021.
[173] Frederick Douglas, Rorshach, Weiyang Pan, and Matthew Caesar. *Salmon: Robust Proxy Distribution for Censorship Circumvention.* In Proceedings on Privacy Enhancing Technologies 2016(4), October 2016.
[174] Paul Vines and Tadayoshi Kohno. *Rook: Using Video Games as a Low-Bandwidth Censorship Resistant Communication Platform.* In the Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2015), October 2015.
[175] Jelle van den Hooff, David Lazar, Matei Zaharia, and Nickolai Zeldovich. *Vuvuzela: Scalable Private Messaging Resistant to Traffic Analysis.* In the Proceedings of the 25th ACM Symposium on Operating Systems Principles (SOSP 2015), Monterey, California, October 2015.
[176] Stevens Le Blond, David Choffnes, William Caldwell, Peter Druschel, and Nicholas Merritt. *Herd: A Scalable, Traffic Analysis Resistant Anonymity Network for VoIP Systems.* In the Proceedings of the ACM SIGCOMM 2015 Conference, August 2015.
[177] Nikita Borisov, George Danezis, and Ian Goldberg. *DP5: A Private Presence Service.* In Proceedings on Privacy Enhancing Technologies 2015(2), June 2015.
[178] Henry Corrigan-Gibbs, Dan Boneh, and David Mazières. *Riposte: An anonymous messaging system handling millions of users.* In the Proceedings of the 36th IEEE Symposium on Security and Privacy (S&P 2015), San Jose, California, USA, May 2015, pages 321-338.
[179] Shuai Li, Mike Schliep, and Nick Hopper. *Facet: Streaming over Videoconferencing for Censorship Circumvention.* In the Proceedings of the Workshop on Privacy in the Electronic Society (WPES 2014), November 2014.
[180] Shuai Li and Nicholas Hopper. *Mailet: Instant Social Networking under Censorship.* In Proceedings on Privacy Enhancing Technologies 2016(2), April 2016.
[181] Richard McPherson, Amir Houmansadr, and Vitaly Shmatikov. *CovertCast: Using Live Streaming to Evade Internet Censorship.* In Proceedings on Privacy Enhancing Technologies 2016(3), July 2016.
[182] Albert Kwon, David Lazar, Srinivas Devadas, and Bryan Ford. *Riffle: An Efficient Communication System With Strong Anonymity.* In Proceedings on Privacy Enhancing Technologies 2016(2), April 2016, pages 115-134.

[183] Sandra Siby, Marc Juarez, Claudia Diaz, Narseo Vallina-Rodriguez, and Carmela Troncoso. *Encrypted DNS -> Privacy? A Traffic Analysis Perspective.* In the Proceedings of the 27th Symposium on Network and Distributed System Security (NDSS '20), February 2020.
[184] Chad Brubaker, Amir Houmansadr, and Vitaly Shmatikov. *CloudTransport: Using Cloud Storage for Censorship-Resistant Networking.* In the Proceedings of the 14th Privacy Enhancing Technologies Symposium (PETS 2014), July 2014.
[185] Qiyan Wang, Xun Gong, Giang T. K. Nguyen, Amir Houmansadr, and Nikita Borisov. *CensorSpoofer: Asymmetric Communication using IP Spoofing for Censorship-Resistant Web Browsing.* In the Proceedings of the 19th ACM conference on Computer and Communications Security (CCS 2012), October 2012.
[186] Masoud Akhoondi, Curtis Yu, and Harsha V. Madhyastha. *LASTor: A Low-Latency AS-Aware Tor Client.* In the Proceedings of the 2012 IEEE Symposium on Security and Privacy, May 2012.
[187] Hsu-Chun Hsiao, Tiffany Hyun-Jin Kim, Adrian Perrig, Akira Yamada, Sam Nelson, Marco Gruteser, and Wei Ming. *LAP: Lightweight Anonymity and Privacy.* In the Proceedings of the 2012 IEEE Symposium on Security and Privacy, May 2012.
[188] Amir Houmansadr, Giang T. K. Nguyen, Matthew Caesar, and Nikita Borisov. *Cirripede: Circumvention Infrastructure using Router Redirection with Plausible Deniability.* In the Proceedings of the 18th ACM conference on Computer and Communications Security (CCS 2011), October 2011.
[189] Eric Wustrow, Scott Wolchok, Ian Goldberg, and J. Alex Halderman. *Telex: Anticensorship in the Network Infrastructure.* In the Proceedings of the 20th USENIX Security Symposium, August 2011.
[190] Brandon Wiley. *Dust: A Blocking-Resistant Internet Transport Protocol.* School of Information, University of Texas at Austin technical report , 2011.
[191] Kirill Levchenko and Damon McCoy. *Proximax: Fighting Censorship With an Adaptive System for Distribution of Open Proxies.* In the Proceedings of Financial Cryptography and Data Security (FC'11), February 2011.
[192] George Danezis, Claudia Diaz, Carmela Troncoso, and Ben Laurie. *Drac: An Architecture for Anonymous Low-Volume Communications.* In the Proceedings of the 10th Privacy Enhancing Technologies Symposium (PETS 2010), Berlin, Germany, July 2010.
[193] Eric Wustrow, Colleen M. Swanson, and J. Alex Halderman. *TapDance: End-to-Middle Anticensorship without Flow Blocking.* In the Proceedings of 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, August 2014.
[194] A. Houmansadr and N. Borisov. *SWIRL: A scalable watermark to detect correlated network flows.* In Network and Distributed System Security Symposium. Internet Society, Feb 2011.
[195] A. Houmansadr, N. Kiyavash, and N. Borisov. *RAINBOW: A robust and invisible non-blind watermark for network flows.* In Network and Distributed System Security Symposium. Internet Society, Feb 2009.
[196] Y. Pyun, Y. Park, X. Wang, D. S. Reeves, and P. Ning. *Tracing traffic through intermediate hosts that repacketize flows.* In G. Kesidis, E. Modiano, and R. Srikant, editors, IEEE Conference on Computer Communications (INFOCOM), pages 634– 642, May 2007.
[197] X. Wang, S. Chen, and S. Jajodia. *Network flow watermarking attack on low-latency anonymous communication systems.* In Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP ’07, pages 116–130, Washington, DC, USA, 2007. IEEE Computer Society.
[198] X. Wang and D. S. Reeves. *Robust correlation of encrypted attack traffic through stepping stones by manipulation of interpacket delays.* In Proceedings of the 10th ACM conference on Computer and communications security, CCS ’03, pages 20–29, New York, NY, USA, 2003. ACM.

[199] X. Wang, D. S. Reeves, and S. F. Wu. *Inter-packet delay based correlation for tracing encrypted connections through stepping stones.* In Proceedings of the 7th European Symposium on Research in Computer Security, ESORICS '02, pages 244–263, London, UK, UK, 2002. Springer-Verlag.
[200] W. Yu, X. Fu, S. Graham, D. Xuan, and W. Zhao. *Dsss-based flow marking technique for invisible traceback.* In Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP '07, pages 18– 32, Washington, DC, USA, 2007. IEEE Computer Society.
[201] N. Kiyavash, A. Houmansadr, and N. Borisov. *Multiflow attacks against network flow watermarking schemes.* In P. van Oorschot, editor, USENIX Security Symposium. USENIX, July 2008.
[202] P. Peng, P. Ning, and D. S. Reeves. *On the secrecy of timingbased active watermarking trace-back techniques.* In V. Paxson and B. Pfitzmann, editors, IEEE Symposium on Security and Privacy, pages 334–349. IEEE Computer Society Press, May 2006.
[203] Andriy Panchenko, Lexi Pimenidis. *Towards Practical Attacker Classification for Risk Analysis in Anonymous Communication.* Springer Berlin Heidelberg.
[204] Chen, Chen & Asoni, Daniele & Barrera, David & Danezis, George & Perrig, Adrian. *HORNET: High-speed Onion Routing at the Network Layer.* https://netsec.ethz.ch/publications/papers/chen_hornet_ccs15.pdf
[205] Chen, Chen & Asoni, Daniele & Perrig, Adrian & Barrera, David & Danezis, George & Troncoso, Carmela. *TARANET: Traffic-Analysis Resistant Anonymity at the Network Layer.* 137-152. 10.1109/EuroSP.2018.00018.
[206] Jody Sankey and Matthew Wright. *Dovetail: Stronger Anonymity in Next-Generation Internet Routing.* In the Proceedings of the 14th Privacy Enhancing Technologies Symposium (PETS 2014), July 2014.