Δίκτυα Υπολογιστών
Διδάσκων: Καθηγητής Οικονομίδης Αναστάσιος

Τίτλος:

Ομότιμα Δίκτυα – Θέματα ασφάλειας, επιθέσεων και αντίμετρα

P2P Networks - Security, Attacks and Countermeasures

Μέλη ομάδας εργασίας :

Παπαθαναήλ Γεώργιος (mis 16003)

Τσολαρίδης Χρήστος (mis 16039)

Περίληψη

Τα δίκτυα P2P ή αλλιώς δίκτυα ομότιμων εφαρμογών είναι ιδιαίτερα διαδεδομένα τα τελευταία χρόνια, κυρίως λόγω των εφαρμογών τους στο διαμοιρασμό αρχείων και στην επικοινωνία σε πραγματικό χρόνο. Αυτό που τα διακρίνει είναι η απουσία κεντρικού server και ότι κάθε κόμβος λειτουργεί ως πελάτης και ως server ταυτόχρονα. Ανάλογα με τη δομή τους διακρίνονται τα P2P σε δομημένα και αδόμητα, ενώ ανάλογα με την ύπαρξη ή μη κεντρικής διεύθυνσης σε συγκεντρωμένα, αποκεντρωτικά και σε τρίτης γενιάς. Η δημοφιλία των P2P δικτύων αλλά και το στοιχείο της ανωνυμίας που τα χαρακτηρίζει, τα καθιστά ελκυστικό στόχο για κακόβουλους χρήστες που δρουν επιθετικά με στόχο την εξαπάτηση των άλλων κόμβων του δικτύου, την αλλοίωση των μεταδιδόμενων πακέτων και τη γενικότερη δυσλειτουργία του συστήματος. Οι πιο γνωστές επιθέσεις είναι η άρνησης παροχής υπηρεσιών σε απλή και γενικευμένη μορφή (Dos& DDos), η εξάπλωσης κακόβουλου λογισμικού, η "Query flooding", η "Man in the middle", οι επιθέσεις στο ευρετήριο και στον πίνακα δρομολόγησης "Index poisoning" και "Routing table poisoning" αντίστοιχα, καθώς και η "Sybil" και η "Eclipse". Άλλες εντάσσονται στην κατηγορία των γενικών επιθέσεων και άλλες με βάση τον τύπο του δικτύου χαρακτηρίζονται ως ειδικές επιθέσεις. Υπάρχουν αμυντικές τεχνικές που μπορούν να εφαρμοστούν ανάλογα με την κάθε περίπτωση, οι οποίες βασίζονται είτε στη δράση μίας κεντρικής αρχής είτε σε διαδικασίες ελέγχου αυθεντικότητας και εγκυρότητας των κόμβων του δικτύου και των μεταδιδόμενων μηνυμάτων.

Abstract

In the late years P2P Networks have been used for many purposes, such as file sharing and real time communication. What distinguishes them from Client-Server Networks is the absence of a central server, which means that each node behaves both as a client and as a server. Depending on their structure P2P are divided into structured and unstructured networks, while the existence of a central authority or not divides them into centralized, decentralized and third generation. Their popularity and the fact that most peers stay anonymous make P2P networks an attractive target for malicious users, who attack against them in order to fool other good nodes, to modify the transmitted package and make the system collapse. The most common attacks are the Denial of Service and the Distributed Denial of Service, Worm Propagation, Query Flooding, Man in the middle, Index poisoning and Routing Table poisoning attack, Sybil and Eclipse. Some of them belong to general attacks and others to specific attacks based on the network type. For each type of attack there are defense techniques which can be used, counting either on a central authority action or on authentication and validation procedures for the nodes and for the transmitted messages as well.

ΕΙΣΑΓΩΓΗ

Οι τεχνολογίες Peer-to-Peer (P2P) παρουσιάζουν μια συνεχώς αυξανόμενη τάση και έχουν πολύ σημαντικό ρόλο σε εφαρμογές διαμοιρασμού αρχείων, στα social media, σε online πλατφόρμες που παρέχουν υπηρεσίες livestreaming και υπηρεσίες online αποθήκευσης. Επιπλέον τα P2P δίκτυα συνεισφέρουν σημαντικά σε τεχνολογίες όπως το Cloud Computing και το Internet of Things. Ο μεγαλύτερος όγκος δεδομένων στο Internet στις μέρες μας προέρχεται από εφαρμογές που δουλεύουν πάνω σε P2P δίκτυα.

Τα P2P δίκτυα παρέχουν μεγάλη ταχύτητα διαμοιρασμού δεδομένων σε σύγκριση με τα κλασσικά δίκτυα Client-Server. Τα P2P δίκτυα χωρίζονται σε δομημένα (structured) και αδόμητα(unstructured). Τα πρώτα P2P δίκτυα δεν είχαν δομή και αυτό είχε σαν αποτέλεσμα να έχουν μεγάλο κόστος και να μην είναι αποδοτικά όσο αυξάνονταν οι κόμβοι. Από την άλλη μεριά τα δομημένα P2P δίκτυα παρέχουν καλύτερη απόδοση όσοι κόμβοι και αν προστεθούν στο δίκτυο. Σε αντίθεση με τα Client-Server δίκτυα, η τεχνολογία P2P μας προσφέρει μια αποκέντρωση (decentralisation) των αρχείων(τα αρχεία δε βρίσκονται σε ένα σημείο, αλλά σε πολλά), αυτοοργάνωση, ανοχή στα σφάλματα (fault tolerance), και load balancing.

Όπως αναφέραμε και πιο πάνω τα P2P δίκτυα καλύπτουν μια ευρεία γκάμα εφαρμογών με πιο γνωστή το διαμοιρασμό αρχείων(Bittorent protocol), άλλα και το online gaming. Η αρχιτεκτονική πάνω στην οποία έχουν "χτιστεί" τα P2P δίκτυα είναι ότι επιτρέπεται σε δύο ή παραπάνω υπολογιστές (nodes) να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Όπως είναι φυσικό μια τέτοια δομή δικτύου είναι επιρρεπής στις κακόβουλες επιθέσεις και έχει κάποια ζητήματα ασφάλειας που θα πρέπει να ληφθούν σοβαρά υπόψη.

Στην παρούσα εργασία γίνεται μια συνοπτική παρουσίαση των P2P δικτύων, καθώς και παρουσίαση των βασικών κακόβουλων επιθέσεων και τρόπων αντιμετώπισης σε έναν P2P δίκτυο.

1 Ομότιμα Δίκτυα(Peer-to-Peer)

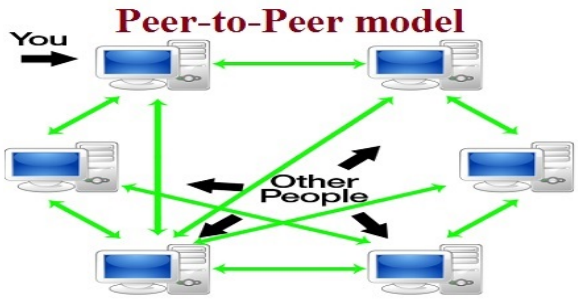
Σύμφωνα με τον ορισμό που δίνει η Wikipedia *:"Ένα δίκτυο υπολογιστών P2P είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης (bandwidth) των κόμβων. Οι πληροφορίες που βρίσκονται στον έναν κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα."*

Peer: Με τον όρο peer χαρακτηρίζουμε έναν κόμβο του δικτύου που μπορεί να συμπεριφερθεί και σαν πελάτης και σαν εξυπηρετητής, με ή χωρίς κεντρική διαχείριση και με ή χωρίς συνεχή συνδεσιμότητα.

Node: Με τον όρο node χαρακτηρίζουμε έναν υπολογιστή που είναι συνδεδεμένος σε κάποιο δίκτυο. Οι κόμβοι μπορεί να είναι υπολογιστές γενικής χρήσης ή μπορούν να κάνουν κάποια εξειδικευμένη εργασία.

Στα ομότιμα δίκτυα το κάθε peer μπορεί να συνδεθεί απευθείας με κάποιο άλλο και να μπει στο σύστημα χωρίς τη συμμετοχή άλλων συνδέσεων. Κάθε κόμβος είναι σε θέση να παίξει είτε το ρόλο του διακομιστή ή του πελάτη ανάλογα με την περίσταση. (Nima Jafari Navimipour, 2015)

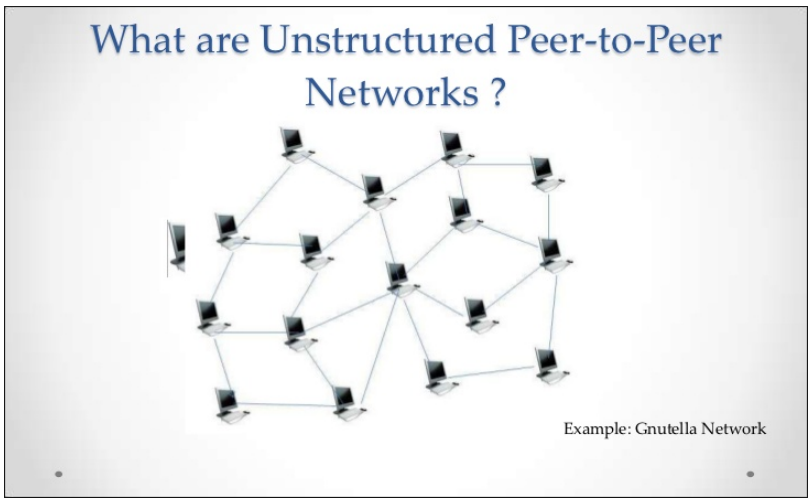
Μπορούμε να κατηγοριοποιήσουμε τα P2P συστήματα με δύο τρόπους. Λαμβάνοντας υπόψη την προέλευση των δεδομένων, μπορούμε να ξεχωρίσουμε δύο βασικές κατηγορίες 1)Αδόμητα και 2)Δομημένα. Επιπλέον τα δομημένα μπορούμε να τα χωρίσουμε σε χαλαρά δομημένα(loosely structured) (Freenet) και αυστηρά δομημένα(highly structured)(Chord). Μια επιπλέον κατηγοριοποίηση που θα μπορούσε να γίνει είναι με βάση τον βαθμό αποκεντροποίησης. Σύμφωνα με τη Wikipedia με αυτή τη ταξινόμηση τα P2P δίκτυα χωρίζονται σε 1)Συγκεντρωτικά (Centralized), 2) Αποκεντρωτικά (Decentralized) και Υβριδικά(Hybrid). Στη συνέχεια θα γίνει μια συνοπτική παρουσίαση των παραπάνω κατηγοριών.



Εικόνα 1: P2P Δίκτυο (Wikipedia)

1.1 Αδόμητα (Unstrutctured) P2P

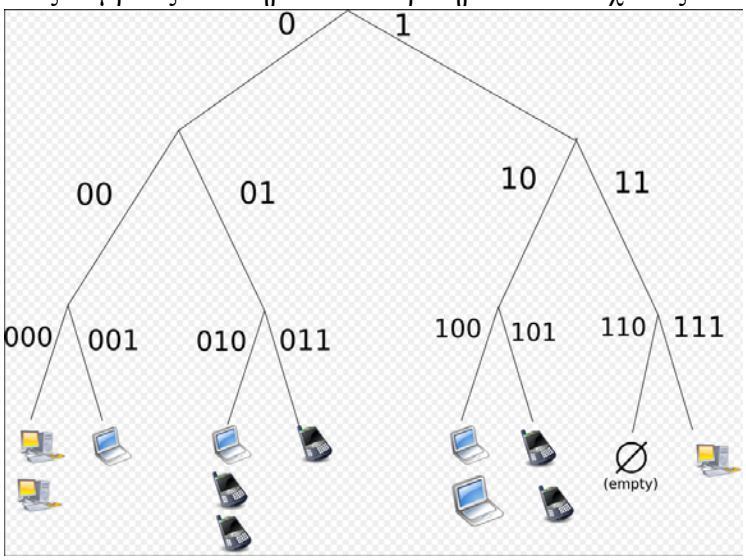
Τα αδόμητα P2P δίκτυα είναι τα πρώτα συστήματα P2P που δημιουργήθηκαν. Το πιο γνωστό ήταν το σύστημα Napster το οποίο είχε ως σκοπό το διαμοιρασμό αρχείων μουσικής στο internet. Μετά το Napster υπήρξε μια ανάπτυξη και άλλων τέτοιον συστημάτων που εκτός από μουσική μπορούσαν να διαμοιράσουν εικόνες και video (Kazaa,Gnutella) (Zulhasnine, 2013).Σε ένα αδόμητο P2P σύστημα οι κόμβοι(nodes) που αποτελούν το σύστημα είναι συνδεδεμένα τυχαία μεταξύ τους (Hameurlain, 2011) και έχουν ως βασική λειτουργία την εύρεση του κόμβου που έχει το αρχείο που χρειάζεται ο χρήστης. Επειδή δεν υπάρχει κάποια προκαθορισμένη δομή, τα αδόμητα P2P δίκτυα είναι πολύ εύκολο να δημιουργηθούν και έχουν χαμηλό κόστος. Ένα βασικό μειονέκτημα των αδόμητων P2P δικτύων είναι ότι πολλές φορές ένα "ερώτημα" μπορεί να μην "απαντηθεί". Δηλαδή να μην μπορούμε να βρούμε τα κατάλληλα peers για να κατεβάσουμε ένα αρχείο που δεν είναι δημοφιλές (Tatsuaki Hamai, 2009).



Εικόνα 2 : Αδόμητο P2P δίκτυο (slideshare.net)

1.2 Δομημένα (Structured) P2P

Τα δομημένα P2P συστήματα, βοήθησαν στο να ξεπεραστούν τα όποια προβλήματα υπήρχαν στα αδόμητα. Στα δομημένα P2P δίκτυα το σύστημα οργανώνεται σε μία συγκεκριμένη τοπολογία, και ένα πρωτόκολλο δεσμεύει ότι κάθε κόμβος μπορεί να ψάξει και να βρει στο δίκτυο οποιοδήποτε αρχείο ή πηγή θέλει ακόμη και αν η πηγή είναι πολύ σπάνια. Ο πιο συνηθισμένος τύπος δομημένου P2P δικτύου βασίζεται στον κατανεμημένο πίνακα κατακερματισμού (DHT) (Tatsuaki Hamai, 2009). Μέσα σε αυτό τον πίνακα τοποθετούνται όλα τα αρχεία και οι κόμβοι, και ο κάθε κόμβος είναι "υπεύθυνος" για κάποιο συγκεκριμένο κομμάτι του δικτύου. Όταν ένας χρήστης θέλει να ψάξει για κάποιο αρχείο ανατρέχει στον πίνακα. Για να υπάρχει γρήγορη δρομολόγηση μέσα σε ένα δομημένο δίκτυο, πρέπει να υπάρχει μια λίστα με όλους τους κόμβους που τηρούνε τα κριτήρια. Αυτό έχει ως αποτέλεσμα τα



Εικόνα 3:Δομημένο Δίκτυο P2P (Wikipedia)

δομημένα συστήματα να μην είναι τόσο ανθεκτικά σε σχέση με τα αδόμητα. Το Bittorent είναι ένα γνωστό δομημένο P2P πρωτόκολλο.

1.3 Συγκεντρωτικά P2P δίκτυα

Η συγκεκριμένη κατηγορία ομότιμων δικτύων θα μπορούσε να χαρακτηριστεί και ως ομότιμα δίκτυα "πρώτης γενιάς."Έχουν κοινά χαρακτηριστικά με τις τοπολογίες Πελάτη/Εξυπηρετητή. Δηλαδή υπάρχει ένας κοινός server ο οποίος συμπεριφέρεται σαν directory server. Μέσα σε αυτόν τον server υπάρχουν όλες οι πληροφορίες που θα χρειαστεί ο χρήστης για τον εντοπισμό κάποιου αρχείου. Όταν βρεθεί το αρχείο γίνεται η σύνδεση μεταξύ χρήστη και εξυπηρετητή. Το μειονέκτημα αυτής της αρχιτεκτονικής είναι ότι σε περίπτωση που δημιουργηθεί κάποιο πρόβλημα στον server, αυτόματα "κρεμάει" όλο το δίκτυο (http://p2pfoundation.net/P2P_Computing).Στην κατηγορία των συγκεντρωτικών ομότιμων δικτύων ανήκει το γνωστό σε όλους Napster.

1.3.1 Αποκεντρωτικά P2P δίκτυα

Η φιλοσοφία εδώ είναι εντελώς διαφορετική. Κάθε peer συνδέεται απευθείας με τα άλλα peers χωρίς να μεσολαβεί κάποιος εξυπηρετητής(server) δηλαδή είναι ταυτόχρονα και πελάτης και εξυπηρετητής. Αυτές οι συνδέσεις μπορεί να είναι άπειρες, και θεωρητικά να δημιουργήσουν ένα τεράστιο δίκτυο. Σε αυτή την κατηγορία ανήκουν το Kazaa και το Gnutella.(www.slideshare.net)

1.3.2 Υβριδικά P2P δίκτυα

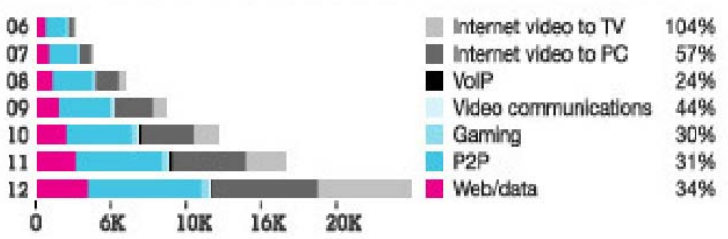
Τα υβριδικά P2P δίκτυα είναι ένας συνδυασμός ομότιμων δικτύων και δικτύων πελάτη εξυπηρετητή. Ένα τυπικό υβριδικό ομότιμο δίκτυο έχει έναν κεντρικό εξυπηρετητή, που βοηθάει τα peers να βρίσκονται μεταξύ τους.(Darlagiannis,2005)

2 Θέματα ασφάλειας, επιθέσεων και αντίμετρων σε δίκτυα Peer to Peer (P2P)

Λόγω των πολλών πλεονεκτημάτων τους, που αναφέρθηκαν παραπάνω, τα δίκτυα P2P έχουν καταστεί ιδιαίτερα δημοφιλή μεταξύ των χρηστών του διαδικτύου τα τελευταία χρόνια όπως φαίνεται και στην Εικόνα 4. Εξαιτίας αυτού του μεγάλου αριθμού των χρηστών τους αλλά και εξαιτίας του γεγονότος πως κόμβοι εισχωρούν και αποχωρούν από το δίκτυο χωρίς κάποιο κεντρικό έλεγχο, έχουν ανακύψει σημαντικά θέματα ασφάλειας των δικτύων αυτού του είδους. Η ασφάλεια, άλλωστε, αποτελεί σημαντική παράμετρο που πρέπει να ληφθεί υπόψη κατά την επιλογή της αρχιτεκτονικής ενός δικτύου. Σε γενικές γραμμές το επίπεδο της ασφάλειας ενός P2P δικτύου εξαρτάται σε μεγάλο βαθμό από την αξιοπιστία των χρηστών του ή διαφορετικά από το ποσοστό των κόμβων του που συμπεριφέρεται κακόβουλα. Στην ιδανική περίπτωση όπου όλοι οι χρήστες είναι «πιστοποιημένοι» και «άξιοι εμπιστοσύνης» και κανένας δεν αναμένεται να δράσει με κακόβουλο τρόπο, όπως για παράδειγμα εκτοξεύοντας επιθέσεις ή στέλνοντας αρχεία με παράνομο υλικό ή εμποδίζοντας άλλους χρήστες να έχουν πρόσβαση στο επιθυμητό αρχείο, το παρεχόμενο επίπεδο ασφάλειας θα είναι υψηλό.

Στη συγκεκριμένη ενότητα της εργασίας αναπτύσσονται τα συχνότερα είδη εμφανιζόμενων επιθέσεων σε δίκτυα P2P, οι οποίες κατηγοριοποιούνται σε γενικές, που έχουν δηλαδή συχνή

εμφάνιση και στο Internet, και σε ειδικότερες ανάλογα και με την υποκατηγορία του δικτύου, ενώ επίσης παρουσιάζονται και οι κατάλληλοι αμυντικοί μηχανισμοί – αντίμετρα, με βάση τη βιβλιογραφία.



Εικόνα 4: Global traffic trends (IBM Support Group: Smarter Communication, 2013)

Μετά το πέρασμα από τα δίκτυα Πελάτη/Εξυπηρετητή(Client/Server) στα ομότιμα δίκτυα αυξήθηκε κατακόρυφα η επικινδυνότητα της χρήσης του διαδικτύου. Είναι πολύ πιθανό ο χρήστης κατά την αναζήτηση κάποιου αρχείου να πέσει θύμα κακόβουλων λογισμικών (Trojans) αλλά και ιών που μπορούν να βλάψουν σημαντικά το σύστημα του. (Xiaowen Chu, Xiaowei Chen, Kaiyong Zhao and Jiangchuan Liu (2010)).Για να μπορέσει ο χρήστης να προστατευτεί έχουν αναπτυχθεί αμυντικοί μηχανισμοί όπως η κρυπτογράφηση, το φιλτράρισμα των αρχείων η εισαγωγή κωδικών ασφαλείας.

2.1 Γενικές επιθέσεις (General attacks)

2.1.1 Επίθεση άρνησης παροχής υπηρεσιών (Denial-of-Service Dos attack)

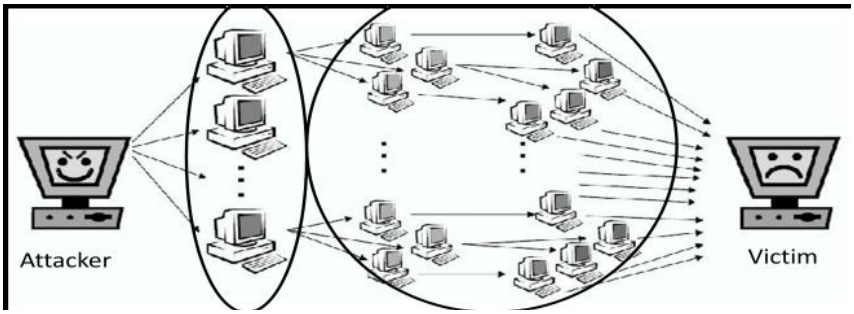
Η επίθεση τύπου Dos αποσκοπεί στο να καταστήσει το δίκτυο μη διαθέσιμο και προσβάσιμο από άλλους υποψήφιους χρήστες, μέσω εξάπλωσης σε αυτό ψεύτικων ή πλαστών πακέτων (bogus packets), με αποτέλεσμα να επιβαρύνεται μέσω μεγάλης κίνησης και εν τέλει να αποτρέπεται η «νόμιμη» κυκλοφορία εντός του δικτύου αλλά και να μη μπορούν να εξυπηρετηθούν άλλοι πελάτες. (Washbourne, 2015). Εναλλακτικός τρόπος εφαρμογής αυτής της επίθεσης είναι με το να υποβάλλει ο κακόβουλος χρήστης τον κόμβο-θύμα σε σχολαστικούς υπολογισμούς, έτσι ώστε να δυσκολεύεται να απαντήσει σε αιτήματα άλλων κόμβων. (Yang & Yang ,nd) Στην ουσία γίνεται σπατάλη των πόρων του δικτύου (εύρος ζώνης, buffer) καθώς και υπολογιστικών πόρων, όπως η μνήμη. (Eleni Koutrouli, 2012)

Κατάλληλο είδος άμυνας που παρεμποδίζει τέτοιες επιθέσεις είναι το λεγόμενο «pricing», δηλαδή η υποβολή ενός παζλ στους ενδιαφερόμενους κόμβους πριν την εξυπηρέτηση των αιτημάτων τους. Συνεπώς, όταν ένας κακόβουλος χρήστης σκοπεύει να δράσει, πρέπει να λύσει πρώτα ένα παζλ και έτσι καθίσταται δυσκολότερο για εκείνον να εκτοξεύσει επίθεση αυτού του είδους. (Pretre, 2005)

2.1.2 Γενικευμένη επίθεση άρνηση παροχής υπηρεσιών (Distributed Denial-of-Service Dos attack)

Η συγκεκριμένη επίθεση, η οποία βασίζεται στη Dos, επιχειρείται όταν η επιτιθέμενη πηγή δεν είναι μόνο μία, αλλά πολύ περισσότερες και αυτό συμβαίνει μέσα από τον έλεγχο του

επιτιθέμενου ενός μεγάλου πλήθους άλλων υπολογιστών τύπου «zombie», δηλαδή κόμβων οι οποίοι είτε έχουν μολυνθεί με κακόβουλο λογισμικό είτε έχουν κυριευτεί από τους κακόβουλους χρήστες χωρίς οι ίδιοι να το γνωρίζουν (Tefera, 2014). Το τελικό θύμα-κόμβος αυτής της μεθόδου δέχεται επίθεση όχι από τον επιτιθέμενο αλλά από τους κόμβους που έχει υπό τον έλεγχό του (τα «zombies»). Αυτή ακριβώς η έμμεση ανάμειξή του καθιστά δύσκολο τον εντοπισμό του. Χαρακτηριστική είναι η ακόλουθη εικόνα αναπαράστασης της επίθεσης.



Εικόνα 5: Επίθεση DDoS

Ιδιαίτερα ευάλωτα στην επίθεση DDoS είναι τα συγκεντρωτικά δίκτυα P2P, εξαιτίας ακριβώς του χαρακτήρα τους, της ύπαρξης δηλαδή ενός και μόνο κεντρικού server. Αν ο κεντρικός server αποτύχει να αμυνθεί έναντι της επίθεσης, τότε όλο το σύστημα θα καταρρεύσει. Αντίθετα, στα αποκεντρωτικά δίκτυα P2P λόγω της τοπολογίας τους η εν λόγω επίθεση προκαλεί μικρότερη ζημιά, καθώς πλήττεται ένα μόνο τμήμα του δικτύου.

Οι επιθέσεις DDos λόγω του μεγάλου όγκου τους είναι αρκετά δύσκολο να αντιμετωπιστούν και επίσης μπορούν να πλήξουν το γόητρο αλλά και να προκαλέσουν ζημιά πολλών εκατομμυρίων ευρώ (Singh, 2014). Χαρακτηριστικά αναφέρεται πως το 2013, όταν το site της Amazon κατέρρευσε για 15 λεπτά, υπολογίστηκε απώλεια εσόδων γύρω στα 66.000$ το λεπτό. (Shawn, 2013) Για αυτό το λόγο έχουν αναπτυχθεί από εταιρείες τηλεπικοινωνιών (Verizon) και ασφάλειας (Akamai) κατάλληλα αμυντικά συστήματα για την απόκρουση των DDos. (Verizon business, Major Online Stock Broker Turns to Verizon Business to Help Stop a Potentially Devastating DDoS Attack. Verizon business, 2008).

2.1.3 Επίθεση κακόβουλου λογισμικού (Worm propagation)

Το κακόβουλο λογισμικό εξαπλώνεται από τον έναν κόμβο στον άλλον μέσω του δικτύου και πιο συγκεκριμένα μέσω αρχείων ή emails. Πρόκειται, σύμφωνα με κάποιες πηγές (Sans Institute ,2004) για ένα πρόγραμμα ή κάποιον αλγόριθμο που αντιγράφεται από μόνο του και στις περισσότερες περιπτώσεις προκαλεί κακόβουλες επιθέσεις ή διαφορετικά είναι ένας ιός με δυνατότητα αυτόνομης παραγωγής.

Προτεινόμενα αντίμετρα που μπορούν να εφαρμοστούν είναι αυτά που χρησιμοποιούνται ήδη ευρέως σε πολλά υπολογιστικά συστήματα, δηλαδή το τείχος προστασίας (firewall) και τα διάφορα αντιικά λογισμικά (antivirus software). Το μεν τείχος προστασίας μπλοκάρει εκείνη τη θύρα (port) που χρειάζεται το worm για να μολύνει τον κόμβο, το δε antivirus περιλαμβάνει την υπογραφή του ιού και αν ορισμένα χαρακτηριστικά ενός προς διανομή αρχείου συμπίπτουν με την υπογραφή του ιού, το λογισμικό διαγράφει ή απομονώνει το αρχείο.

2.1.4 Επίθεση τύπου πλημμύρας ερωτημάτων (Query flooding attack)

Σύμφωνα με τη βιβλιογραφία (Chaudhari, Gamit, 2014), πρόκειται για υποπερίπτωση των επιθέσεων τύπου Dos, η οποία λαμβάνει χώρα στο επίπεδο εφαρμογής ("application layer"). Προκειμένου να αποκτήσει το επιθυμητό αρχείο, ο ενδιαφερόμενος κόμβος αποστέλλει αιτήματα-ερωτήματα στους γειτονικούς του. Ο κακόβουλος κόμβος τότε θα παράξει όσο το δυνατόν περισσότερα τέτοια αιτήματα, έτσι ώστε να «πλημμυρίσει» το δίκτυο. Επίθεση Query flooding έχει πραγματοποιηθεί στο παρελθόν στο Napster και στο Gnutella, με αποτέλεσμα τη δυσλειτουργία των δικτύων.

Η συγκεκριμένη επίθεση δεν είναι ιδιαίτερα επικίνδυνη για το σύστημα, καθώς στην περίπτωση του Gnutella ο κάθε κόμβος μπορεί να δεχτεί ένα μέγιστο αριθμό αιτημάτων από έναν αιτούμενο κόμβο και κατά συνέπεια να αγνοήσει τα επιπλέον εισερχόμενα ερωτήματα που καταλήγουν σε εκείνον με τη μορφή «πλημμύρας». Αυτός ο μηχανισμός δύναται να μειώσει το βαθμό επικινδυνότητας της επίθεσης. (Wang, 2006) (Chaudhari, Gamit, 2014)

2.1.5 Επίθεση Man in the middle (Man in the middle attack)

Επίθεση «Man in the middle» ονομάζεται η κατάσταση στην οποία ο επιτιθέμενος μπορεί να έχει πρόσβαση και να διαφοροποιήσει τα μηνύματα μεταξύ δύο κόμβων, χωρίς κάθε κόμβος να γνωρίζει ότι ο σύνδεσμος μεταξύ τους έχει παραβιαστεί. (Hamai, Masahiro, & Yu, 2009) Για την αποδοτική λειτουργία των P2P χρειάζεται οι κόμβοι να βασίζονται σε αξιόπιστους ενδιάμεσους χρήστες, για να προωθήσουν τα αιτήματά τους. Κατά την εκδήλωση της επίθεσης οι επιτιθέμενοι, οι οποίοι αποτελούν τους ενδιάμεσους μεταξύ των χρηστών, αλλοιώνουν τα αιτήματα αυτά. (Eleni Koutrouli, 2012)

Η χρήση ψηφιακών υπογραφών και κρυπτογραφημένων μηνυμάτων θεωρείται αποτελεσματική άμυνα. Τα κρυπτογραφημένα μηνύματα δυσχεραίνουν το έργο του επιτιθέμενου, ακόμα και αν εκείνος τα έχει υποκλέψει, ενώ οι ψηφιακές υπογραφές περιλαμβάνουν τεχνικές αυθεντικότητας και εγκυρότητας-αξιοπιστίας των χρηστών ώστε να υπάρξει διαχωρισμός μεταξύ καλών και κακόβουλων. (Yang & Yang ,nd).

2.2 Ειδικές επιθέσεις (Specific attacks)

2.2.1 Index poisoning attack (Επίθεση αλλοίωσης του ευρετηρίου)

Τα περισσότερα P2P δίκτυα που εξυπηρετούν τη διανομή αρχείων διαθέτουν ευρετήρια («index»), επιτρέποντας έτσι στους χρήστες τους να εντοπίσουν τον κόμβο που διαθέτει το προς κατέβασμα αρχείο. Η επίθεση αλλοίωσης του ευρετηρίου («index poisoning») έχει στόχο να προσβάλλει αυτή τη διαδικασία αναζήτησης μέσω του ευρετηρίου και το επιτυγχάνει με την εισαγωγή από πλευράς επιτιθέμενου μεγάλου αριθμού μη έγκυρων πληροφοριών (bogus information) μέσα σε αυτό, έτσι ώστε να εμποδίσει τους χρήστες να εντοπίσουν τις σωστές πηγές.(Yang & Yang ,nd) Στην ουσία μια index poisoning attack διαφημίζει σκόπιμα μια μεγάλη ποσότητα μη έγκυρων πληροφοριών που δεν αντιστοιχεί σε καμία διεύθυνση IP ή αριθμό θύρας(Yuan, 2014). Αλλοιώνει τις πληροφορίες στο ευρετήριο ενός δικτύου P2P, με σκοπό οι πληροφορίες να μη μπορούν να διαμοιραστούν στους πελάτες. Ιδιαίτερα ευάλωτη σε αυτού του είδους την επίθεση είναι η δημοφιλής εφαρμογή δικτύου P2P BitTorrent. Στο BitTorrent αρχικά πρέπει να κατεβάσει ο χρήστης ένα αρχείο γνωστό ως seed με την κατάληξη

.torrent. Το αρχείο αυτό περιέχει πληροφορίες, όπως το μέγεθος και το όνομα του αρχείου, αλλά και ένα ανιχνευτή (tracker), ο οποίος λειτουργεί σαν ένα κέντρο ανταλλαγής πληροφοριών από το οποίο οι κόμβοι αποκτούν χρήσιμες πληροφορίες σχετικά με άλλους υπολογιστές που κατεβάζουν το ίδιο αρχείο. Κατά την αναζήτηση στο BitTorrent ένας κόμβος διαφημίζει τις πληροφορίες του στον ανιχνευτή και εν συνεχεία παίρνει μία λίστα με πληροφορίες για τους άλλους κόμβους. Σε αυτή τη διαδικασία ο ανιχνευτής δεν πιστοποιεί την αυθεντικότητα του κόμβου ούτε ελέγχει αν το περιεχόμενο του αρχείου είναι πράγματι διαθέσιμο, όπως διαφημίζει ο κόμβος. Ο επιτιθέμενος σκοπίμως διαφημίζει μεγάλη ποσότητα μη έγκυρων πληροφοριών για κόμβους, που διαθέτουν το αρχείο, οπότε όσο ο χρήστης προσπαθεί να κατεβάσει το αρχείο από τους κόμβους αυτούς, το BitTorrent αποτυγχάνει να δημιουργήσει συνδέσεις εξαιτίας της μεγάλης πιθανότητας να συνδεθεί με μη έγκυρους κόμβους. (Kong, 2010)

Για τη συγκεκριμένη επίθεση μπορούν να εφαρμοστεί η τεχνική άμυνας μέσω της βαθμολόγησης των πηγών. Όσοι κόμβοι διαφημίζουν και ανεβάζουν αρχεία στο δίκτυο, που όντως διαθέτουν, θα λαμβάνουν υψηλή βαθμολογία. Από την άλλη, κόμβοι οι οποίοι δρουν κακόβουλα και προσπαθούν να πλήξουν το σύστημα μέσω του ευρετηρίου, θα καταχωρούνται σε μία μαύρη λίστα.

2.2.2 Routing table poisoning attack (Επίθεση αλλοίωσης του πίνακα δρομολόγησης)

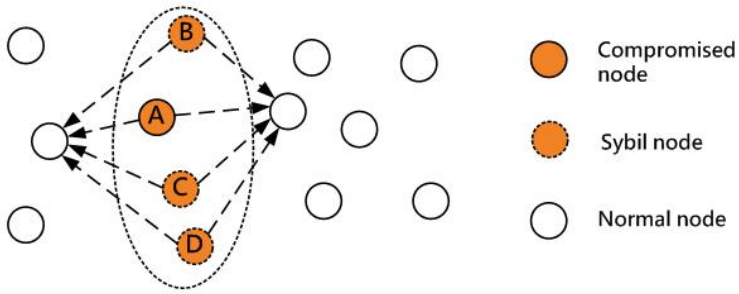
Η συγκεκριμένη επίθεση εφαρμόζεται σε δίκτυα P2P, τα οποία βασίζονται σε κατανεμημένους πίνακες κατακερματισμού (DHT) (Tatsuaki Hamai, 2009). *"Ως DHT ορίζεται ο πίνακας που παρέχει μία υπηρεσία αναζήτησης μέσα σε ένα αποκεντρωμένο κατανεμημένο σύστημα."*(Wikipedia) Σύμφωνα με την Wikipedia, ο πίνακας χρησιμοποιεί μία συνάρτηση κατατεμαχισμού για γρήγορη εύρεση εγγραφών σε βάσεις δεδομένων. Όπως ένα λεξικό έχει τις λέξεις-κλειδιά και τους αντίστοιχους ορισμούς-περιγραφές, έτσι και η συνάρτηση κατατεμαχισμού μπορεί να εξυπηρετήσει αντιστοιχώντας τις λέξεις-κλειδιά (keys) με τις αντίστοιχες τιμές κατατεμαχισμού (values). Ζεύγη δηλαδή κλειδιών-τιμών (key-value) αποθηκεύονται μέσα στον πίνακα και έτσι κάθε συμμετέχων κόμβος μπορεί να ανακτήσει αποτελεσματικά την τιμή που συνδέεται με ένα δεδομένο κλειδί. Με αυτό τον τρόπο λειτουργίας ο DHT μπορεί μέσα σε ένα δίκτυο να διαχειριστεί τις συνεχείς αφίξεις και αναχωρήσεις κόμβων αλλά και τις αποτυχίες. Ως προς τον πίνακα δρομολόγησης (routing table), πρόκειται για μια βάση δεδομένων που βρίσκεται αποθηκευμένη σε ένα δρομολογητή ή ένα δικτυωμένο υπολογιστή. Οι πίνακες δρομολόγησης χρησιμοποιούνται από τους αλγόριθμους δρομολόγησης, οι οποίοι δίνουν ως αποτέλεσμα τον επόμενο σταθμό στον οποίο πρέπει να μεταφερθεί ένα πακέτο IP. Τότε ο δρομολογητής δρομολογεί το πακέτο IP στον επόμενο σταθμό. Ο πίνακας δρομολόγησης αποθηκεύει όλες τις διαδρομές (και σε ορισμένες περιπτώσεις, μετρήσεις που σχετίζονται με αυτές τις γραμμές) προς άλλους σταθμούς του δικτύου. Η κατασκευή των πινάκων δρομολόγησης είναι ο πρωταρχικός στόχος των πρωτοκόλλων δρομολόγησης όταν χρησιμοποιούνται στατικές διαδρομές.(Wikipedia)

Κατά την επίθεση αυτή οι κακόβουλοι χρήστες προσθέτουν την IP διεύθυνση του υπολογιστή του υποψήφιου θύματος μέσα στους πίνακες δρομολόγησης μιας ομάδας κόμβων ως μία γειτονική τους. Με αποστολή ψεύτικων μηνυμάτων από πλευράς επιτιθέμενων γνωστοποιείται η ύπαρξη της IP διεύθυνσης του θύματος σε διαφορετικούς κόμβους, οι οποίοι πλέον συμπεριλαμβάνουν το θύμα στους γείτονές τους και στη συνέχεια του αποστέλλουν πακέτα με πληροφορίες. Στην περίπτωση πάρα πολλών τέτοιων εξαπατημένων κόμβων το θύμα μπορεί εύκολα να τεθεί εκτός λειτουργίας. (Wang,2006)

Σε γενικές γραμμές η περιγραφόμενη επίθεση δεν αποτελεί ιδιαίτερη απειλή για τα συστήματα P2P, διότι μπορούν να αναβαθμίσουν τον πίνακα δρομολόγησης αυτόματα. Επίσης, όταν οι κόμβοι δε λαμβάνουν απάντηση από τους γειτονικούς, μπορούν να διαγράψουν τις ψεύτικες IP διευθύνσεις από τους πίνακες δρομολόγησης.

2.2.3 Sybil attack

Η επίθεση Sybil ανήκει στις επιθέσεις που βασίζονται στην αδυναμία απόδοσης έγκυρων ταυτοτήτων στους συμμετέχοντες ενός δικτύου (“Identity assignment attacks”) . (Yang & Yang ,nd) Τα δίκτυα P2P είναι εικονικά δίκτυα επικάλυψης (“overlay networks”) χτισμένα πάνω σε ένα δίκτυο υποστρώματος (όπως άλλωστε το Internet το οποίο δουλεύει πάνω στο τηλεπικοινωνιακό δίκτυο), το οποίο σημαίνει πως κάθε οντότητα στο υπόστρωμα έχει μία αντίστοιχη ταυτότητα στο δίκτυο επικάλυψης. Η Sybil Attack αναφέρεται σε μια επίθεση ταυτοποίησης, στην οποία ένας κακόβουλος χρήστης αποκτά ψεύτικες ταυτότητες και δημιουργεί ψεύτικους κόμβους τους οποίους τοποθετεί μεταξύ των έμπιστων κόμβων. Έτσι αποκτά τον έλεγχο ενός μεγάλου κομματιού του δικτύου. (Haowen Liu, 2013). Η Sybil attack μπορεί να εμφανιστεί σε όλα τα δίκτυα που απαιτούν αυτή τη σχέση μεταξύ οντότητας και ταυτότητας, άρα πέρα από τα P2P και σε δίκτυα ad-hoc και αισθητήρων. Ο κύριος στόχος της Sybil attack είναι να πλήξει την απόδοση του συστήματος λήψης εφεδρικών αντιγράφων (“redundant backup mechanism”), που διαθέτουν τα δίκτυα με σκοπό να προστατέψουν την ακεραιότητα και την ιδιωτικότητά τους.



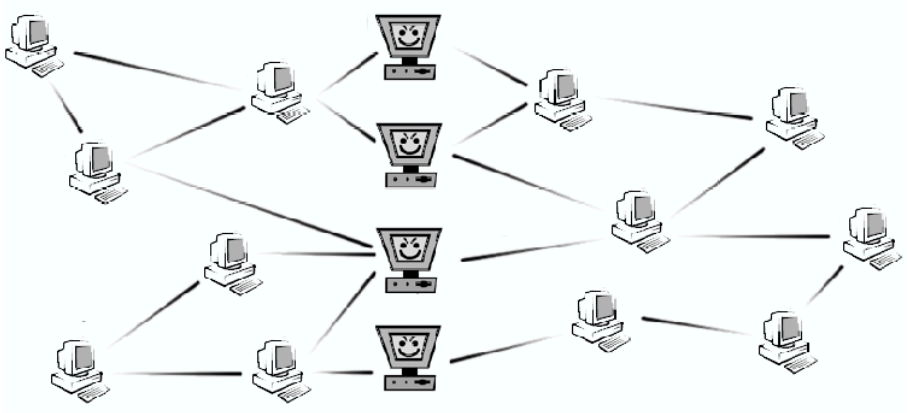
Εικόνα 6:Επίθεση Sybil (Yang & Yang,nd)

Αντίμετρο εδώ είναι μία διαδικασία που ονομάζεται εγγραφή (“self-registration”) (Vestola, 2010) . (Yang & Yang ,nd) και λειτουργεί ως ακολούθως. Για κάθε νέο κόμβο με βάση την IP διεύθυνση και το port του εκδίδεται η ταυτότητά του και στη συνέχεια κάνει εγγραφή και αιτείται να συμμετέχει στο δίκτυο. Την ευθύνη και τη δυνατότητα της πιστοποίησης της ταυτότητας του νέου χρήστη έχουν οι ήδη εγγεγραμμένοι κόμβοι του συστήματος. Αν η πλειοψηφία αυτών του επιτρέψει να συμμετέχει στο δίκτυο, αν δηλαδή μέσα από τον έλεγχο της ταυτότητάς του προκύψει ότι ο νέος κόμβος δεν είναι ψεύτικος, γίνεται δεκτός. Μειονέκτημα της μεθόδου self-registration είναι το γεγονός πως το κόστος της απόκτησης μιας IP διεύθυνσης συνεχώς φθίνει. Εξάλλου, οι επιτιθέμενοι μπορούν να διαθέτουν ένα μεγάλο αριθμό IP διευθύνσεων έχοντας υπό τον έλεγχό τους μια συλλογή από υπολογιστές τύπου “zombies”, όπως εξηγήθηκε παραπάνω.

Μία δεύτερη πιο αποτελεσματική αμυντική μέθοδος που χρησιμοποιείται είναι το σύστημα ελέγχου πρόσβασης (admission control system ACS) , το οποίο βασίζεται στη λογική ενός κρυπτογραφικού παζλ που πρέπει να επιλύσει κάθε νέος κόμβος, εφόσον επιθυμεί να συμμετέχει στο δίκτυο. Το παζλ πρέπει να επιλυθεί κατόπιν πρόκλησης από τους άλλους χρήστες. Σύμφωνα με τη βιβλιογραφία(Vestola 2010), απαιτούνται μέρες ή και εβδομάδες προσπάθειας από έναν κακόβουλο χρήστη προκειμένου να αποκτήσει ένα μικρό ποσοστό κόμβων σε ένα περιορισμένο δίκτυο.

2.2.4 Eclipse attack

Η επίθεση Eclipse ανήκει στις επιθέσεις που στόχο έχουν να εκμεταλλευτούν τις αδυναμίες στους μηχανισμούς δρομολόγησης των δικτύων (“Routing level attacks”). Σε μία επίθεση Eclipse ο επιτιθέμενος ελέγχει ένα μεγάλο τμήμα των γειτονικών κόμβων ενός καλού χρήστη. Αυτή η ομάδα των κακόβουλων κόμβων επιδιώκει να εξαπατήσει τον καλό χρήστη περνώντας τις διευθύνσεις τους στη λίστα των γειτονικών του κόμβων. Μέσω της επίθεσης ο επιτιθέμενος μπορεί να ελέγξει ένα σημαντικό τμήμα του δικτύου, αν όχι όλο το δίκτυο, (Chirag Parmar, 2015) καθώς αν οι κακόβουλοι κόμβοι βρίσκονται σε μεγάλη κλίμακα δύνανται να επισκιάσουν τους καλούς. Κατά συνέπεια οι χρήστες δε μπορούν να προωθήσουν μηνύματα σωστά και το δίκτυο συνολικά υπολειτουργεί. Η επίθεση τύπου Sybil, που παρουσιάστηκε παραπάνω, θεωρείται ειδική περίπτωση της επίθεσης Eclipse, εφόσον ο επιτιθέμενος δημιουργεί μεγάλη ποσότητα από στοιχεία ταυτοποίησης για να δράσουν ως γείτονες του καλόβουλου χρήστη. (Yang & Yang,nd) Όπως φαίνεται και στην ακόλουθη εικόνα, οι κακόβουλοι κόμβοι έχουν διαχωρίσει το δίκτυο σε δύο υποδίκτυα. Ό,τι μέθοδοι επικοινωνίας και αν χρησιμοποιηθούν στα δύο υποδίκτυα, οι καλοί κόμβοι δε μπορούν να αποφύγουν τη σύνδεση με έναν από τους κακόβουλους, οπότε όλο το δίκτυο είναι υπό τον έλεγχό τους.



Εικόνα 7:Eclipse Attack (Yang & Yang,nd)

Ως προς τους μηχανισμούς άμυνας ενάντια στην επίθεση Eclipse μπορεί καταρχάς να αναφερθεί η ιδέα της δέσμευσης των απευθείας διαδρομών που έρχονται προς τον κακόβουλο κόμβο (όρος “indegree”) και των απευθείας διαδρομών που φεύγουν από αυτόν (όρος “outdegree”) . Αυτό το αντίμετρο εφαρμόζεται πρώτα στην επίθεση τύπου Sybil, έτσι ώστε να αποκλειστεί το ενδεχόμενο μίας επίθεσης Eclipse βασιζόμενης σε επίθεση Sybil. (Gera Jaideep, 2016) Στη συνέχεια για κάθε κόμβο του δικτύου P2P ζητείται να εξετάσει περιοδικά τη λίστα των γειτόνων των κόμβων με τους οποίους συνορεύει. Αν ο αριθμός των κόμβων στην επιστρεφόμενη λίστα

γειτόνων είναι μεγαλύτερος του ορίου "indegree" ή αν ο αυτός ο κόμβος δεν είναι στη λίστα, σημαίνει πως έχει γίνει επίθεση τύπου Eclipse.

Ένας άλλος τρόπος άμυνας σε αυτήν την επίθεση βασίζεται στον ανώνυμο έλεγχο των γειτονικών ομάδων των κόμβων. Αν δηλαδή ένας κόμβος διαθέτει ένα σημαντικά μεγαλύτερο αριθμό συνδέσεων σε σχέση με το μέσο όρο, ενδέχεται να ετοιμάζει μία επίθεση Eclipse. Όταν όλοι οι υπολογιστές του δικτύου εκτελούν αυτόν τον έλεγχο τακτικά, οι κακόβουλοι χρήστες ανακαλύπτονται και μπορούν να απομακρυνθούν από τις γειτονικές ομάδες των καλών χρηστών.

Η πιο αποτελεσματική άμυνα θεωρείται ο έλεγχος των στοιχείων ταυτότητας των κόμβων που μπορούν να χρησιμοποιηθούν στους πίνακες δρομολόγησης. Ένας τέτοιος έλεγχος όμως μπορεί να υλοποιηθεί μόνο από μία έμπιστη κεντρική αρχή, η οποία αν υπολειτουργήσει τότε όλο το δίκτυο θα καταρρεύσει. Δίκτυα δηλαδή συγκεντρωτικά (Centralized) μπορούν από μόνα τους να αποτύχουν.

Αντίμετρο κατάλληλο για αποκεντρωμένα (Decentralized) δίκτυα P2P είναι η μέθοδος "induced churn" (όπου churn ο ρυθμός με τον οποίο κόμβοι έρχονται και φεύγουν από το δίκτυο) (Vestola ,2010). Σύμφωνα με αυτή κάθε κόμβος εξαναγκάζεται περιοδικά να αποχωρεί από το δίκτυο και να επιστρέφει με μία νέα ταυτότητα, ενώ παράλληλα γίνεται περιοδική αρχικοποίηση (reset) των πινάκων δρομολόγησης των κόμβων, έτσι ώστε να αποφεύγεται η κακή χρήση τους από hacking με την εγγραφή σε αυτούς κακόβουλων IP διευθύνσεων. Έτσι ο πίνακας δρομολόγησης γίνεται λιγότερο αποδοτικός αλλά πιο ανθεκτικός στην επίθεση. Οι εξαναγκασμένες απρόβλεπτες αλλαγές στα στοιχεία ταυτότητας θα μειώσουν τις πιθανότητες ενός επιτιθέμενου να πραγματοποιήσει επιθέσεις Eclipse. Η μέθοδος υποστηρίζεται πως παρέχει ένα επαρκές επίπεδο ασφάλειας ενάντια στις επιθέσεις Eclipse.

Ακολουθεί πίνακας στον οποίο παρατίθενται περιληπτικά οι προαναφερθείσες επιθέσεις (με την αγγλική τους ονομασία), η κατάλληλη αμυντική στρατηγική για την κάθε μία αλλά και ο βαθμός επικινδυνότητάς τους.

Πίνακας 1: Συγκεντρωτικός πίνακας επιθέσεων και τρόποι αντιμετώπισης.

Όνομα Επίθεσης	**Τρόπος εκδήλωσης**	**Βαθμός επικινδυνότητας**	**Αντίμετρα**	**Δυνατότητα άμυνας του δικτύου**
Denial-of-Service Dos	1. Εξάπλωση στο δίκτυο πλαστών πακέτων 2. Υποβολή του θύματος σε σχολαστικούς υπολογισμούς	Μέτριος	Pricing	Μεγάλη
Distributed Denial-of-Service Dos	Μέσω ελέγχου ενός πλήθους υπολογιστών τύπου "zombies"	Υψηλός (κυρίως για τα συγκεντρωτικά δίκτυα)	Αμυντικοί μηχανισμοί από εταιρείες ασφάλειας	Μικρή

			δικτύων	
Worm propagation	Εξάπλωση από τον ένα κόμβο στον άλλο μέσω αντιγραφής	Μέτριος	Τοίχος προστασίας, αντιικό λογισμικό	Μέτρια
Man in the middle	Υποκλοπή και αλλοίωση δεδομένων μεταξύ δύο σταθμών	Μικρός	Κρυπτογράφηση Ψηφιακές υπογραφές.	Μεγάλη
Index poisoning	Αλλοίωση των πληροφοριών του ευρετηρίου με στόχο το δυσχερή εντοπισμό του σωστού πακέτου	Υψηλός	Βαθμολόγηση πηγών	Μέτρια
Routing table poisoning	Μέσω αλλοίωσης των πληροφοριών του πίνακα δρομολόγησης	Μέτριος	Αυτόματη αναβάθμιση του πίνακα δρομολόγησης	Μεγάλη
Sybil	Κατοχή πολλών IP διευθύνσεων από πλευράς επιτιθέμενου	Υψηλός	Διαδικασία “self-registration”	Μικρή
Eclipse	Συνεργασία των κακόβουλων κόμβων προς εξαπάτηση των καλών χρηστών	Υψηλός	Έλεγχος των στοιχείων ταυτότητας των χρηστών από ένα κεντρικό κόμβο, Μέθοδος “induced churn”	Μικρή

3 Συμπεράσματα και προτάσεις για μελλοντική έρευνα

Στην παρούσα εργασία έγινε μία συνοπτική παρουσίαση των P2P δικτύων. Τα P2P δίκτυα έχουν αρκετά πλεονεκτήματα και έτσι έχουν γίνει αρκετά δημοφιλή. Μερικά από τα πλεονεκτήματα τους είναι: 1) Η απλή δομή 2)Το μηδαμινό κόστος 3)Ελεύθερη ροή πληροφορίας 4)Η αποθήκευση των αρχείων σε υπολογιστές των χρηστών αντί σε κάποιον κεντρικό Server. Επισημάνθηκαν οι κυριότερες κατηγορίες ταξινόμησής τους, αναφέρθηκαν ορισμένα πολύ γνωστά δίκτυα τέτοιου τύπου (Napster, Kazaa, Gnutella, BitTorrent, FreeNet) και παρουσιάστηκαν οι πιο βασικές και συχνές εκδηλωμένες επιθέσεις σε αυτά μαζί με τους γνωστότερους μηχανισμούς άμυνας. Οι επιθέσεις κατηγοριοποιήθηκαν σε γενικές, με πεδίο εμφάνισης πέρα από τα δίκτυα P2P το κλασσικό Internet και σε εξειδικευμένες επιθέσεις.

Αντίμετρα για την κάθε απειλή παρατέθηκαν και αναλύθηκαν. Κάποιες ειδικές επιθέσεις όπως η Sybil και η Eclipse είναι υψηλής επικινδυνότητας για το σύστημα, καθώς σχετίζονται με τα στοιχεία ταυτότητας των κόμβων του δικτύου. Επομένως, θέματα απόδοσης ταυτότητας και η πρόληψη επιθέσεων απόδοσης ταυτότητας θα πρέπει να αποτελούν πρώτιστη προτεραιότητα. Απειλές όπως η Index poisoning attack καθιστούν τρωτά τόσο τα δομημένα όσο και τα αδόμητα δίκτυα. Το κοινό στοιχείο όλων των επιθέσεων που παρουσιάστηκαν στην εργασία, είναι πως είναι σχετικά εύκολο να πραγματοποιηθούν και στην πράξη, με δεδομένο ότι θα υπάρχουν πάντα χρήστες που θα θέλουν να δράσουν κακόβουλα και επιθετικά.

Συμπερασματικά, διαπιστώνεται πως τα δίκτυα P2P θα συνεχίσουν να εξελίσσονται και να είναι ιδιαίτερα δημοφιλή, ωστόσο ταυτόχρονα εμφανίζουν θέματα ασφάλειας και μάλιστα σοβαρά. Τα προτεινόμενα αντίμετρα ενώ δείχνουν αποτελεσματικά έναντι των διάφορων απειλών, συχνά κατακρίνονται από την άποψη πως δεν είναι ιδιαίτερα πρακτικά καθώς επιβάλλουν αυστηρούς περιορισμούς στο δίκτυο και διαδικασίες δύσκολα εφαρμόσιμες. Το δεύτερο συμπέρασμα, επομένως, που προκύπτει είναι πως οι δύο έννοιες ασφάλεια και αποδοτικότητα του συστήματος έρχονται συχνά σε σύγκρουση. Την ίδια στιγμή που οι αμυντικές διατάξεις καλύπτουν και ενισχύουν την άμυνα του δικτύου, μειώνουν την απόδοσή του.

Άρα, η ανάπτυξη εργαλείων ασφάλειας που θα συνδυάζουν αποτελεσματικότητα αλλά και απλότητα στη χρήση τους είναι το ζητούμενο και η επόμενη τεχνολογική πρόκληση. Μόνο μέσα από την εφαρμογή τέτοιων εργαλείων μπορούν να σχεδιαστούν δίκτυα P2P ασφαλή και αποδοτικά.

Βιβλιογραφία

Ανάκτηση από http://p2pfoundation.net/P2P_Computing: http://p2pfoundation.net/P2P_Computing

Avinash Chaudhari, P. G. (2014, Φεβρουάριος). Analysis of various attacks on P2P networks. *IJETTCS Vol.3 Issue 1*, σσ. 217-220.

Chirag Parmar, C. J. (2015, Ιανουάριος 1). A Survey On Peer-to-Peer Network Attacks and Defenses. *International Journal for Innovative Research in Science & Technology| Volume 1 | Issue 7*, σσ. 136-141.

Eleni Koutrouli, A. T. (2012, 1 2). Taxonomy of attacks and defense mechanisms in P2P reputation systems-Lessons for reputation system designers. *ELSEVIER*, σσ. 47-70.

Gera Jaideep, D. B. (2016). Survey on the Present State-of-the-Art of P2P Networks, Their Security. *International Journal of Applied Engineering Research ISSN 0973-4562 Volume 11, Number 1 (2016)* , σσ. 616-620.

Darlagiannis, Vasilios (2005). "Hybrid Peer-to-Peer Systems". In Steinmetz, Ralf; Wehrle, Klaus. *Peer-to-Peer Systems and Applications*. Springer.

Hameurlain, A. (2011). "A Survey of Structured P2P Systems for RDF Data Storage and Retrieval". Στο A. K. Hameurlain, *Transactions on Large-Scale Data- and Knowledge-Centered Systems III: Special Issue on Data and Knowledge Management in Grid and PSP Systems* (σ. 21). Springer.

Haowen Liu, C. M. (2013). AN ADAPTIVE MEMBERSHIP PROTOCOL AGAINST SYBILATTACK IN UNSTRUCTURED P2P NETWORKS. *Information and Communications Technologies (IETICT 2013)* (σσ. 29 - 34). Beijing: IET.

Kong, C. (2010). The Evaluation of Index Poisoning in BitTorrent. *Second International Conference on Communication Software and Networks* (σσ. 382-386). Singapore: IEEE

Nima Jafari Navimipour, F. S. (2015, Μάιος). A comprehensive study of the resource discovery techniques. *Peer-to-Peer Networking and Applications*, σσ. 474-492.

Pretre, B. (2005). *Master Thesis: Attacks on Peer-to-Peer Networks.* ETH University,Zurich.

Shawn, H. (2013, August 19). *Smallbiztrends.com*. Ανάκτηση από smallbiztrends.com/2013/08/amazon-down-custom-error-page.html

Singh, G. T. (2014, Μάρτιος 11). Big Data Analytics framework for Peer-to-Peer Botnet detection using Random Forests. *ELSEVIER*.

Tatsuaki Hamai, M. F. (2009). ITU-T Recommendations on. (σσ. 1-6). Αθήνα : IEEE.

Vestola, M. (2010, Μάιος 10). Security Issues in Structured P2P Overlay Networks. Helsinki.

Wang, L. (2006, Δεκέμβριος 11). Attacks Against Peer-to-Peer Networks and Countermeasures. Ελσίνκι.

Washbourne, L. (2015, Απρίλιος 6). A Survey of P2P Network Security.

www.wikipedia.org. (n.d.). Ανάκτηση από Peer to peer from Wikipedia: http://en.wikipedia.org/wiki/Peer_to_peer

www.slideshare.net

Yang, Y. Y. (n.d.). *A Survey of Peer-to-Peer Attacks and Counter Attacks.* CSE Department, California State Polytechnic University, Pamona.

Yuan, L. K. (2014). A STUDY OF INDEX POISONING IN PEER-TOPEER. *International Journal on Cybernetics & Informatics (IJCI) Vol. 3, No. 6, December 2014* , (σσ. 11-23).

Zulhasnine, M. (2013). "P2P Streaming Over Cellular Networks: Issues, Challenges, and Opportunities". Στο *Building Next-Generation Converged Networks: Theory and Practice* (σ. 99). CRC Press.

Tefera, M.(2014). *Master Thesis: Attacks on structured P2P Networks:Simulating Sybil Attack.* Mittuniversited. Sundsvall, Sweden.

SANS Institute (2004). *Worm Propagation and countermeasures*, Glenn Gebbhart.

.

.