Τμήμα Τεχνολογία Πληροφορικής και Τηλεπικοινωνιών

« Peer to Peer Security Issues »

Επιβλέπων Καθηγητής : Μακροδημήτρης Γεώργιος

Φοιτήτριες :

Γεωργκή Αθηνά

Πανταζοπούλου Ευσταθία

Οκτώβριος 2011

Σπάρτη

PEER TO PEER SECURITY ISSUES

Ευχαριστίες

Θα θέλαμε να ευχαριστήσουμε θερμά τον επιβλέποντα καθηγητή της πτυχιακής μας εργασίας, κ. Μακροδημήτρη Γεώργιο. Οι οδηγίες του, οι υποδείξεις του και η κατανόηση που έδειξε κατά τη συγγραφή της εργασίας αποτέλεσαν καθοριστικά στοιχεία για την εκπόνησή της.

Θα θέλαμε επίσης να εκφράσουμε την ευγνωμοσύνη μας στις οικογένειες μας και στους ανθρώπους που είχαμε δίπλα μας όλοι αυτήν την περίοδο.

Περίληψη

Με αφορμή την έξαρση των εφαρμογών Peer to Peer, γίνεται σε αυτή την πτυχιακή μια παρουσίαση της κατάστασης σε παγκόσμια κλίμακα των εν λόγω εφαρμογών. Γίνεται μια ιστορική αναδρομή σε περιόδους ακμής αλλά και παρακμής των Peer to Peer εφαρμογών και της χρησιμότητας τους στην παγκόσμια διαδικτυακή κοινότητα. Παρουσιάζονται και αναλύονται δύο από τις κύριες αρχιτεκτονικές τους, η Κεντρικοποιημένη και η μη κεντρικοποιημένη.

Η πρώτη έχει σαφώς πιο καλά αποτελέσματα όσον αφορά την ταχύτητα στις αναζητήσεις αλλά παρουσιάζει σημαντικά μειονεκτήματα όπως ότι αν χαλάσει ο κεντρικός server τότε καταρρέει όλο το σύστημα. Αντίθετα η αρχιτεκτονική που βασίζεται στη μη κεντρικοποιημένη, δηλαδή χωρίς να υπάρχει κάποιος κεντρικός υπολογιστής σίγουρα εγγυάται την σταθερότητα του συστήματος ενώ μπορεί και να προσφέρει ανωνυμία που μπορεί να είναι ζητούμενο για πολλούς χρήστες. Σε άλλο Κεφάλαιο αναλύονται διάφορα ζητήματα ασφάλειας που προκύπτουν από την χρήση των Peer to Peer.

Έχοντας μια Peer to Peer εφαρμογή εγκατεστημένη αφήνετε εκτεθειμένος ενδεχομένως ο υπολογιστή και προσωπικές πληροφορίες σε αγνώστους. Επιτρέποντας στους ξένους να έχουν πρόσβαση σε αρχεία στον υπολογιστή, αλλα και σε άλλες ευαίσθητες πληροφορίες. Έτσι στην παρούσα πτυχιακή αναλύονται μηχανισμοί ασφάλειας, που προσπαθούν να επιτύχουν μυστικότητα αλλά και να παρέχουν όλες τις βασικές υπηρεσίες ασφαλείας. Επίσης αναλύονται διάφορα νομικά ζητήματα που έχουν προκύψει από την πρώτη στιγμή της εμφάνισης τους, διάφορες δικαστικές διαμάχες που έχουν προκύψει σε διεθνές επίπεδο, αλλά καθώς και τρόποι αντιμετώπισης τους.

Περιεχόμενα

Εισαγωγή

Η γέννηση νέων αναγκών και η συνεχώς αυξανόμενη και ευρέως διαδεδομένη διαθεσιμότητα δεδομένων από πηγές πληροφοριών του διαδικτύου έχει δημιουργήσει μεγάλο ενδιαφέρον όσον αφορά στις δυνατότητες ανταλλαγής πληροφοριών. Στα πλαίσια αυτά δημιουργήθηκαν το μοντέλο Peer to Peer (P2P) ή αλλιώς δίκτυα ομότιμων κόμβων. Τα P2P δίκτυα είναι μια κατηγορία δικτύων στην οποία κάθε υπολογιστής (κόμβος) που μετέχει είναι ισότιμος, έχει ίδια δικαιώματα και υποχρεώσεις. Δεν υπάρχει, δηλαδή, η έννοια του πελάτη και του εξυπηρετητή, καθώς κάθε κόμβος μπορεί να έχει και τους δύο ρόλους. Με τον τρόπο αυτό μεταφέρουμε την "ευφυΐα" του δικτύου στα άκρα του και όχι σε κάποιους συγκεκριμένους κόμβους. Ένας πιο τυπικός ορισμός θα έλεγε ότι τα δίκτυα ομότιμων είναι μια κλάση αρχιτεκτονικής δικτύου και εφαρμογών που χρησιμοποιούν κατανεμημένους πόρους με στόχο να πραγματοποιήσουν εργασίες δρομολόγησης και δικτύωσης με ένα αποκεντρωμένο και αυτό-οργανονούμενο τρόπο. Τα συστήματα P2P, για μια πιο συνεκτική περιγραφή, διακρίνονται από τα εξής ιδιαίτερα χαρακτηριστικά:

Το δίκτυο P2P διευκολύνει την μεταφορά δεδομένων ή άμεσων μηνυμάτων σε πραγματικό χρόνο μεταξύ των απομακρυσμένων χρηστών προσωπικών υπολογιστών στην περιφέρεια του διαδικτύου. Πιο συγκεκριμένα, μετά την σύνδεση δύο τερματικών εντός του δικτύου P2P δικτύου, ότι επακολουθεί συμβαίνει σε πραγματικό χρόνο. Επίσης, λόγω της άμεσης σύνδεσης που έχει εφαρμοστεί, δεν παρεμβάλλεται κανένας μεσάζοντας, που θα μπορούσε να κατακρατά και να αποθηκεύει δεδομένα, ή να καθυστερεί την μεταφορά δεδομένων ή μηνυμάτων μεταξύ των συνδεδεμένων τερματικών. Τα μεταφερόμενα δεδομένα μπορεί να αποτελούν απλά μηνύματα κειμένου, φωνητικά μηνύματα, ακόμα και ολόκληρα αρχεία.

Οι ομότιμοι υπολογιστές κατέχουν την ιδιότητα τόσο του εξυπηρετητή όσο και του πελάτη, εφόσον κάθε προσωπικός υπολογιστής μπορεί να στείλει αλλά και να

λάβει περιεχόμενο εντός του συστήματος P2P. Εκμεταλλευόμενο την διπλή αυτή αποστολή που υπηρετούν οι χρήστες, το σύστημα κοινής χρήσης αρχείων καταφέρνει να αποκεντρώσει τα αποθηκευμένα στο σύστημα αρχεία. Μάλιστα, αυτή η τροποποίηση των συστημάτων P2P οδηγεί σε ένα πολύ πιο συνεκτικό και αξιόπιστο δίκτυο. Αυτό συμβαίνει διότι, ενώ στην αρχιτεκτονική πελάτη – εξυπηρετητή (Client - Server Model), πιθανή δυσλειτουργία του εξυπηρετητή θέτει εκτός λειτουργίας όλο το σύστημα, στα συστήματα διαμοιρασμού αρχείων, πιθανή βλάβη σε έναν από τους προσωπικούς υπολογιστές δεν έχει αξιοσημείωτη επίπτωση στο δίκτυο.

Σε ένα δίκτυο πελάτη – εξυπηρετητή (Client - Server Model), η μεγάλη πλειοψηφία του περιεχομένου αποθηκεύεται στον κεντρικό εξυπηρετητή (server). Οι πελάτες μπορούν να έχουν πρόσβαση σε αυτό το περιεχόμενο, αλλά οποιαδήποτε ευθύνη αποθήκευσης περιεχομένου εναπόκειται στον κεντρικό εξυπηρετητή. Σε ένα σύστημα P2P το περιεχόμενο βρίσκεται εγκατεστημένο σε μεμονωμένους υπολογιστές. Ένας χρήστης του συστήματος μπορεί να λάβει αυτά τα περιεχόμενα ή κομμάτι τους, αποκτώντας πρόσβαση στον ίδιο τον προσωπικό υπολογιστή που τα διατηρεί. Σε αντάλλαγμα ο χρήστης δίνει την άδειά του για ελεύθερη πρόσβαση των υπόλοιπων ομότιμων στον δικό του υπολογιστή και κατ' επέκταση στα δεδομένα του. Κατά αυτό τον τρόπο, το περιεχόμενο αποκεντρώνεται (ανεξαρτητοποιείται από τον κεντρικό εξυπηρετητή) και βρίσκεται πια κατανεμημένο στο δίκτυο.

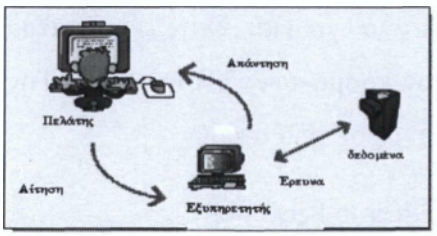
Το δίκτυο παρέχει μεγάλη αυτονομία στους χρήστες και ουσιαστικά τους δίνει πλήρως τον έλεγχο. Σε ένα πραγματικό σύστημα P2P, κάθε ομότιμος λειτουργεί ανεξάρτητα και οργανώνει μόνος του κάθε του κίνηση. Όπως γίνεται προφανές, αυτό έρχεται σε πλήρη αντίθεση με την παραδοσιακή αρχιτεκτονική του εξυπηρετητή / πελάτη, όπου ο πελάτης εξαρτάται σε μεγάλο βαθμό από τον εξυπηρετητή.

Το δίκτυο φιλοξενεί ομότιμους υπολογιστές που δεν βρίσκονται πάντα συνδεδεμένοι και που μπορεί να μην διαθέτουν μόνιμες διευθύνσεις IP (Internet Protocol: Πρωτόκολλο Διαδικτύου). Τα παραδοσιακά δίκτυα server/client δίκτυα ήταν εξοικειωμένα με τερματικούς κόμβους που κατείχαν μόνιμες διευθύνσεις. Η εκ των προτέρων γνώση των μόνιμων διευθύνσεων, ήταν απαραίτητη για την αμφίδρομη επικοινωνία μεταξύ εξυπηρετητή και πελάτη. Ωστόσο, σε ένα δίκτυο P2P, οι ομότιμοι

υπολογιστές δεν χρειάζονται σταθερές διευθύνσεις IP, καθώς η αναγνώριση του υπολογιστή δεν έγκειται σε διάκριση τοποθεσίας ή μηχανήματος, αλλά στην αναγνώριση του χρήστη. Μάλιστα αυτή η αυτονομία των συστημάτων κοινού διαμοιρασμού αντικειμένων από την IP διευθυνσιοδότηση κρίνεται απαραίτητη για την λειτουργία του. Η αποκεντρωμένη φύση των ομότιμων υπολογιστών, σε συνδυασμό με το γεγονός του ότι οι Παροχείς Υπηρεσιών Δικτύου (ISP: Internet Service Provider) παρέχουν διευθύνσεις IP δυναμικά, καθιστούν απαραίτητο για τις εφαρμογές P2P εφαρμογές να λειτουργούν εκτός του Συστήματος Ονοματοδοσίας Δικτύων (DNS: Domain Name System).

Τα δίκτυα αυτά είναι χρήσιμα για ποικίλους σκοπούς. Ο διαμοιρασμός αρχείων που περιέχουν ήχο, εικόνα, δεδομένα ή οτιδήποτε άλλο σε ψηφιακή μορφή είναι πολύ συνηθισμένος, ενώ και δεδομένα πραγματικού χρόνου, όπως η τηλεφωνική κίνηση, μπορούν να περαστούν χρησιμοποιώντας τεχνολογία ομότιμων.

Πρέπει να αναφερθεί ότι το αρχικό Internet είχε σχεδιαστεί σαν ένα σύστημα peer to peer. Με τον καιρό όμως εξελίχθηκε σε τύπου client-server όπου οι πελάτες ήταν εκατομμύρια και επικοινωνούσαν με ένα περιορισμένο αριθμό servers. Έτσι οι σημερινές εφαρμογές χρησιμοποιούν το Internet όπως αρχικά είχε σχεδιασθεί δηλαδή σαν ένα μέσο επικοινωνίας για υπολογιστές που μοιράζονται πόρους, αρχεία και ότι άλλο απευθείας ο ένας με τον άλλο. Είναι χαρακτηριστικό ότι στην Γερμανία ένα 70% της κίνησης στο ερευνητικό δίκτυο προέρχεται από εφαρμογές P2P.



Μοντέλο client/server[1]

Μοντέλο Peer to Peer[2]

[1] Φώτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων". 2007.

[2] Φώτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων".

Κεφάλαιο 1ο

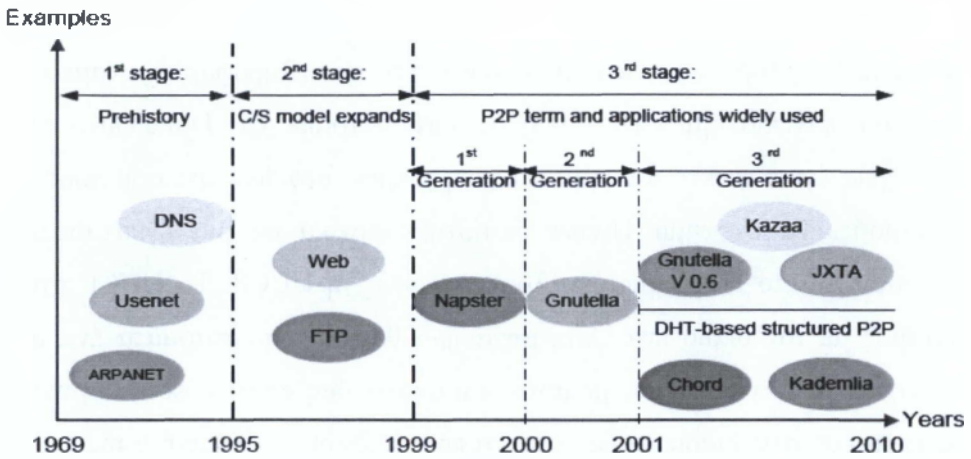
1. Ιστορική αναδρομή και η εξέλιξη των P2P

Πριν συζητήσουμε την ιστορία των υπολογιστών Peer to Peer (P2P), πρέπει πρώτα να καταλάβουμε τι είναι. Ο όρος P2P δημιουργήθηκε για να περιγράψει τα δίκτυα εκείνα τα οποία έχουν την απαίτηση οι χρήστες τους να μοιράζονται με τα υπόλοιπα μέλη του δικτύου τα αρχεία τους, τους υπολογιστικούς τους πόρους ή οτιδήποτε άλλο απαιτηθεί για κάποιο κοινό σχέδιο.

Πριν δημιουργηθεί αυτός ο όρος και εφαρμοστεί στην πράξη, οι χρήστες του Internet αλληλεπιδρούσαν μεταξύ τους μεν αλλά με δύσχρηστους και αργούς τρόπους όπως πχ με τα mail και μέσω ομάδων συζητήσεων(newsgroups). Μπορούσαν να στείλουν ο ένας στον άλλο αρχεία χωρίς να γίνεται έλεγχος των συναλλαγών αυτών από κάποιον κεντρικό φορέα. Δεν μπορούσαν όμως να συζητήσουν σε πραγματικό χρόνο πάνω σε αυτά, να τα οργανώσουν σε κατηγορίες ή να σημειώνουν σχόλια πάνω σε αυτά. Η εισαγωγή αυτού του τρόπου αλληλεπίδρασης στο διαδίκτυο θα βελτίωνε τον τρόπο με τον οποίο οι χρήστες επικοινωνούσαν μεταξύ τους.

Αν και ο όρος αυτός υπάρχει εδώ και λίγο καιρό ο τρόπος λειτουργίας του και η αρχιτεκτονική του υπάρχουν εδώ και πολλά χρόνια. Στην πραγματικότητα η αρχιτεκτονική αυτή είναι η παλαιότερη στον κόσμο των επικοινωνιών. Την ιστορία των P2P δικτύων μπορούμε να την διαιρέσουμε σε τρία στάδια:

- (1969-1995) Προϊστορία Peer to Peer
- (1995-1999) Έκρηξη του Διαδικτύου
- (1999 -;) Σύγχρονες εφαρμογές



Χάρτης Πορείας της P2P ιστορίας[3]

1.1 Προϊστορία Peer to Peer (1960-1995)

Κατά τη διάρκεια της προϊστορίας των P2P δικτύων (1960-1995), η σκέψη του P2P άνθισε μέσα από διάφορα συστήματα, αν και ο όρος αυτός δεν έγινε δεκτός εκείνη την εποχή.

Μπορούμε να πούμε ότι η ομότιμη δικτύωσης άρχισε να καλλιεργείτε από την εποχή του Ψυχρού πολέμου στις αρχές της δεκαετίας του '60. Το Υπουργείο Εθνικής Άμυνας των Ηνωμένων Πολιτειών προσπαθούσε να αναπτύξει ένα δίκτυο επικοινωνιών και διοίκησης το οποίο θα ήταν ικανό να επιβιώσει από μια ενδεχόμενη επίθεση με πυρηνικά όπλα από τη Σοβιετική Ένωση. Τότε, ιδρύθηκε η Υπηρεσία Προηγμένων Ερευνητικών Έργων (Advanced Research Projects Agency-ARPA), η οποία με τη σειρά της δημιούργησε το ARPANET, τον πρόγονο του σημερινού internet. Το APRANET δεν χρησιμοποιούσε το μοντέλο Πελάτη - Εξυπηρετητή (client – server), κάθε host ήταν ίσης μεταχείρισης. Σκοπός του ARPANET, ήταν η μεταγωγή πακέτων ανάμεσα σε ένα πλήθος ομότιμων υπολογιστών.

Usenet ήταν ένα άλλο παράδειγμα, κατά το πρώτο στάδιο το οποίο παρέχει τοπικό έλεγχο και σχετικά απλή διαχείριση. Usenet είναι ουσιαστικά ο παππούς του P2P. Το

[3] Zhonchong Ou."Structuted P2P, Hierarchical Architrcture And Performance Evaluation" http://herkules.oulu.fi/isbn9789514262487/isbn9789514262487.pdf

Usenet για πρώτη φορά σχεδιάστηκε το 1979, αρχικά δημιουργήθηκε ως ένα δίκτυο με το οποίο θα μπορούσαν να μεταδίδονται νέα και πληροφορίες ανάμεσα στους φοιτητές των πανεπιστημίων University of North Carolina και Duke University, ενώ στη συνέχεια έγινε εφικτή και η ανταλλαγή μικρών αρχείων με αρκετούς, όμως, περιορισμούς. Το σύστημα Usenet βασίστηκε αρχικά σε μια εγκατάσταση που ονομάζεται Unix to Unix πρωτόκολλο αντιγραφής, ή UUCP. Το UUCP ήταν ένας μηχανισμός με τον οποίο ένα Unix μηχάνημα θα καλούσε αυτόματα ένα άλλο με σκοπό την ανταλλαγή αρχείων με αυτό, και ακολούθως αποσύνδεση. Ο μηχανισμός αυτός επέτρεψε στις διαδικτυακές Unix τοποθεσίες την ανταλλαγή e-mail, αρχείων, patches του συστήματος, ή άλλα μηνύματα. Το Usenet σήμερα χρησιμοποιεί πρωτόκολλο με βάση TCP / IP που είναι γνωστό ως Network News Transport Protocol (NNTP), το οποία επιτρέπει σε δύο υπολογιστές στο δίκτυο Usenet να ανακαλύψουν νέες ομάδες συζήτησης με αποτελεσματικότητα και να προβούν σε ανταλλαγή μηνυμάτων μεταξύ τους.

Το βασικό μοντέλο του Usenet παρέχει τοπικό έλεγχο και σχετικά απλή διαχείριση. Ένα site Usenet ενώνεται με τον υπόλοιπο κόσμο, με τη δημιουργία μιας σύνδεσης ανταλλαγής ειδήσεων με ένα τουλάχιστον άλλο sever στο δίκτυο Usenet. Σήμερα, η ανταλλαγή παρέχεται συνήθως από την εταιρία ISP(Internet Service Provider). Ο διαχειριστής της εταιρείας μπορεί να ελέγχει το μέγεθος των μεταφερόμενων δεδομένων, προσδιορίζοντας ποιος server θα τα μεταφέρει. Επιπλέον, ο διαχειριστής μπορεί να καθορίσει μια στιγμή λήξης αναλόγως την ομάδα ή την ιεραρχία, έτσι ώστε τα άρθρα σε μια ομάδα συζήτησης να ανακτώνται για ένα ορισμένο χρονικό διάστημα. Οι έλεγχοι αυτοί επιτρέπουν σε κάθε οργανισμό να συμμετάσχει εθελοντικά στο δίκτυο με τους δικούς του όρους. Πολλοί οργανισμοί αποφασίζουν να μην μεταφέρονται για παράδειγμα newsgroups που μεταδίδουν σεξουαλικό περιεχόμενο ή παράνομο υλικό. Αυτή είναι μια ειδοποιός διαφορά από το Freenet, το οποίο (ως επιλογή του σχεδιασμού) δεν επιτρέπει σε έναν χρήστη να ξέρει τι υλικό έχει λάβει.

Ακόμη και στην φυσική ιεραρχική Domain Name System (DNS), θα μπορούσαμε να δούμε την σκιά των P2P δικτύων, καθώς και κατά τις πρώτες ημέρες του Internet, ο τρόπος να χαρτογραφήσεις ένα πιο ανθρώπινα φιλικό όνομα όπως BBN σε μια

διεύθυνση IP (όπως 4.2.49.2) ήταν μέσω ενός και μόνο απλού αρχείου, hosts.txt το οποίο διανεμόταν παντού. Δεδομένου ότι το δίκτυο αυξήθηκε σε χιλιάδες hosts και η διαχείριση αυτού του αρχείου κατέστη αδύνατη, το DNS εξελίχθηκε ως ένας τρόπος για να διανέμονται τα δεδομένα σε ολόκληρο το τότε P2P Internet.

Το DNS στο σύνολό του λειτουργεί εκπληκτικά καλά, έχοντας κλίμακα έως 10.000 φορές το αρχικό του μέγεθος. Υπάρχουν πολλά βασικά στοιχεία σχεδιασμού του DNS που έχουν αναπαραχθεί σε πολλά κατανεμημένα συστήματα σήμερα. Ένα στοιχείο είναι ότι οι hosts μπορούν να λειτουργήσουν τόσο ως πελάτες όσο και ως servers, διανέμοντας αιτήσεις όταν χρειαστεί. Το δεύτερο στοιχείο είναι η φυσική μέθοδος διανομής requests σε όλο το δίκτυο. Κάθε DNS server μπορεί να θέσει ερωτήματα σε οποιοδήποτε άλλο, αλλά σε κανονική λειτουργία υπάρχει ένα πρότυπο μονοπάτι μέσω της αλυσίδας ιεραρχίας. Το φορτίο κατανέμεται φυσικά σε όλο το δίκτυο DNS, έτσι ώστε κάθε name server να εξυπηρετεί μόνο τις ανάγκες των πελατών του και του namespace που διαχειρίζεται ατομικά.

Έτσι, από πρώτα στάδια του, το Internet χτίστηκε βασισμένο σε P2Pμορφές επικοινωνίας. Ένα πλεονέκτημα αυτής της ιστορίας είναι ότι έχουμε την εμπειρία να αντλήσουμε για το σχεδιασμό νέων P2Pσυστημάτων.

1.2 Η έκρηξη του Διαδικτύου (1995-1999)

Κατά το δεύτερο στάδιο της έκρηξης του Διαδικτύου (1995-1999). Το διαδίκτυο απομακρύνθηκε από την λογική της ''όμοιος-προς-όμοιο'' αρχιτεκτονικής. και σταδιακά έδωσε τη θέση του στο μοντέλο πελάτη – εξυπηρετητή (client – server). Αυτό προέκυψε λόγο ο τι όταν τα πρώτα δίκτυα P2P άρχισαν να αναπτύσσονται, στις αρχές της δεκαετίας του 90, είχαν άκρως περιορισμένη εφαρμογή, σε εσωτερικές διαδικασίες εταιριών ή στην ανταλλαγή πληροφοριών μεταξύ συνεργαζόμενων ερευνητών. Έτσι ένα τεράστιο σύνολο καθημερινών ανθρώπων άρχισε να χειρίζεται το διαδίκτυο ως μέσο για να ανταλλάσσει γράμματα ηλεκτρονικού ταχυδρομείου, να αποκτά πρόσβαση σε ιστοσελίδες και να αγοράζει αγαθά.

Η ιδέα του ισόνομου διαμοιρασμού αρχείων στο διαδίκτυο, άρχισε να ξεθωριάζει και το διαδίκτυο γρήγορα έγινε ένα μέσο παρόμοιο με την τηλεόραση και τις εφημερίδες. Έτσι, θεωρώντας αυτή την εικόνα του διαδικτύου ως μόνιμη, οι σχεδιαστές του ανέπτυξαν συστήματα που δεν υποστήριζαν την λογική P2P, αλλά μια αρχιτεκτονική σχεδίαση που ονομάστηκε B2C (Business-to-Consumer: Εταιρεία-προς-καταναλωτή). Καθώς όμως τα συστήματα κοινού διαμοιρασμού αρχείων ήδη υπήρχαν, η περαιτέρω ανάπτυξή τους φάνταζε εμπόδιο στην εξάπλωση του διαδικτύου, η οποία είχε βασιστεί στην λογική πελάτης - εξυπηρετητής.

1.3 Σύγχρονες εφαρμογές Peer to Peer (1999 -;)

Το τρίτο στάδιο των P2P δικτύων (1999 -;) είναι το στάδιο κατά το οποίο η έννοια των P2P, επισήμως χρησιμοποιείται και ευρέως αποδεκτή. Αυτό το στάδιο μπορούμε να χωρίσουμε σε 3 γενιές.

1.3.1 Το πρώτο Peer to Peer δίκτυο

Η μεγάλη επανάσταση στον διαμοιρασμό αρχείων έγινε το 1999 όταν εμφανίστηκε το πρώτο P2P δίκτυο, το περίφημο πλέον Napster, δημιουργός του οποίου ήταν ο, μόλις δεκαοκτώ τότε ετών, Shawn Fanning. Αυτή η πρωτοποριακή τεχνολογία επέτρεπε σε χρήστες από όλο τον κόσμο να αναζητούν και να «κατεβάζουν» τραγούδια, σε μορφή Mp3, τα οποία ήταν αποθηκευμένα σε υπολογιστές άλλων χρηστών της υπηρεσίας. Μερικούς μήνες αργότερα, η Napster Inc. μετρούσε πάνω από 21 εκατομμύρια χρήστες. Ο 18 χρόνος τότε μαθητής δεν μπορούσε να φανταστεί σε καμιά περίπτωση ότι το δημιούργημα του θα άλλαζε τον τρόπο με τον οποίο απολαμβάνουμε πολυμεσικές εφαρμογές και γενικά επικοινωνούμε.

Για να είναι εφικτή η αναζήτηση των αρχείων αυτών, το Napster χρησιμοποιούσε έναν κεντρικό server, στον οποίο ήταν αποθηκευμένοι οι τίτλοι όλων των τραγουδιών, τα οποία οι χρήστες της υπηρεσίας διέθεταν για διαμοιρασμό, αλλά και οι ηλεκτρονικές διευθύνσεις των χρηστών αυτών.

Όταν ένας χρήστης συνδέεται στο δίκτυο τότε το πρόγραμμα-πελάτης που είναι εγκατεστημένο στον υπολογιστή του ενημερώνει τον server για τα αρχεία δηλ. τα

τραγούδια που διατηρεί ο χρήστης. Παρομοίως όταν ένας χρήστης φεύγει ο server ενημερώνεται κατάλληλα. Όταν ένας χρήστης ζητήσει ένα αρχείο τότε ο server ψάχνει μέσω της μηχανής αναζήτησης που διατηρεί για τους χρήστες που έχουν το συγκεκριμένο αρχείο και ενημερώνει τον χρήστη.

Από κει και πέρα τον έλεγχο αναλαμβάνει το πρόγραμμα που είναι εγκατεστημένο στον χρήστη. Το πρόγραμμα αναλαμβάνει την επικοινωνία με τους άλλους χρήστες για να αρχίσει η διαδικασία αντιγραφής του αρχείου. Δηλ. το σύστημα ξεκινάει σαν κεντρικό στην πορεία όμως γίνεται αποκεντρωμένο.

Καθώς το Napster αποκτούσε όλο και μεγαλύτερη φήμη αλλά και περισσότερους συνδρομητές, ένα σύνολο δισκογραφικών εταιριών, καλλιτεχνών και η Ένωση της Δισκογραφικής Βιομηχανίας της Αμερικής (RIAA), με τον ισχυρισμό της παραβίασης των πνευματικών δικαιωμάτων των ανταλλασσόμενων στο Napster μουσικών κομματιών, ξεκίνησαν μια εκστρατεία για την κατάργηση του προγράμματος. Μετά από μεγάλης διάρκειας νομικών αγώνων, η λειτουργία του Napster διακόπηκε τον Ιούλιο του 2001, αρκετά σύντομα μετά την εμφάνισή του, αλλά έχοντας πρώτα ενισχύσει όσο κανείς άλλος την μόδα της αρχιτεκτονικής P2P.

Με τη Napster έκλεισε ένα κεφάλαιο μόνο από τη μεγάλη εξέλιξη του downloading η οποία ακολούθησε. Προσπερνώντας τον κεντρικό εξυπηρετητή του Napster, που ήταν και ο πιο εύκολος στόχων νομικών κυρώσεων, τα δεύτερης γενιάς P2P δίκτυα δημιούργησαν σταδιακά την εικόνα και την πληθώρα επιλογών που υπάρχει σήμερα.

1.3.2 Τα συστήματα κοινής χρήσης αρχείων δεύτερης γενιάς

Μετά την πρώτη εμφάνιση του Napster η AOL ανέθεσε σε δύο προγραμματιστές της να φτιάξουν κάτι παρόμοιο. Οι Justin Frankel και Tom Pepper που δούλευαν στη Nullsoft, έγραψαν ένα καθαρά P2Pπρωτόκολλο το οποίο και ανακοίνωσαν πως θα διέθεταν δωρεάν στο διαδίκτυο. Μόλις εκδόθηκε η πρώτη έκδοση του προγράμματος στις 14 Μαρτίου του 2000, η AOL φοβισμένη από τις μηνύσεις κατά του Napster αποφάσισε να το αποσύρει. Ήταν όμως ήδη αργά καθώς ικανοί προγραμματιστές που

είχαν αποκτήσει το αρχείο κατάφεραν να το δημιουργήσουν από την αρχή και να το προσφέρουν στον κόσμο, αυτή τη φορά με ανοιχτό τον κώδικα. Το όνομά του: Gnutella, που είναι ο βασικός εκπρόσωπος της δεύτερης γενιάς. Η μεγάλη διαφοροποίηση σε σχέση με το Napster ήταν η απουσία ενός κεντρικού server, και πλέον κάθε κόμβος θεωρούταν ισάξιος. Η σχεδίαση αυτή όμως γρήγορα δημιούργησε προβλήματα στένωσης του συστήματος, λόγω της εκτεταμένης χρήσης του (οι περισσότεροι ήταν πρώην χρήστες του Napster) και της τεχνικής της πλημμύρας που χρησιμοποιούσε στις αναζητήσεις αντικειμένων.

Το σύστημα FastTrack έλυσε αυτό το πρόβλημα παρέχοντας την δυνατότητα σε κάποιους κόμβους να είναι περισσότερο ίσοι από τους άλλους. Αυτό γινόταν με το να επιλέγονται κάποιοι κόμβοι με μεγαλύτερη χωρητικότητα (σε αποθηκευτικό χώρο, εύρος δικτύου κτλπ) για να κρατάνε τις λίστες και με τους λιγότερης χωρητικότητας να συνδέονται σε αυτούς, παρέχοντας ένα δίκτυο το οποίο μπορούσε να εξαπλωθεί σε μεγαλύτερο μέγεθος. Το FastTrack αποτέλεσε ένα άκρως κλιμακούμενο δίκτυο.

Αργότερα το Gnutella αλλά και οι περισσότερες σημερινές P2P εφαρμογές υιοθέτησαν αυτό το μοντέλο, για να οδηγηθούμε σε μεγαλύτερα αλλά και πιο αποτελεσματικά δίκτυα.

Τα καλύτερα παραδείγματα συστημάτων κοινής χρήσης αρχείων δεύτερης γενιάς αποτελούν τα Gnutella, Kazaa και Emule/Kademlia. Τα eDonkey2000/Overnet, Gnutella, FastTrack και Ares Galaxy έχουν συγκεντρώσει γύρω στους 10,3 εκατομμύρια χρήστες. Λεγεται ότι σήμερα ένα πολύ μεγάλο μερίδιο των P2P δικτύων χρησιμοποιούν το πρωτόκολλο BitTorrent.

Το πρωτόκολλο αυτό έκανε την εμφάνιση του το 2002 και χρησιμοποιείται κυρίως για την μεταφορά αρχείων μεγάλου μεγέθους. Ο τρόπος λειτουργίας των P2P δικτύων που χρησιμοποιούν αυτό το πρωτόκολλο παρουσιάζει πολλές διαφορές σε σχέση με τα υπόλοιπα P2P δίκτυα. Κάθε αρχείο δεδομένων, που διατίθεται για διαμοιρασμό σε ένα τέτοιο δίκτυο, «σπάει» σε πολλά μικρά τμήματα. Για να πραγματοποιηθεί το "κατέβασμα" αυτού του αρχείου, θα πρέπει πρώτα ο χρήστης να κατεβάσει ένα πολύ μικρό αρχείο με κατάληξη.torrent, το οποίο στην συνέχεια πρέπει να ανοιχθεί με την βοήθεια κάποιου torrent client, όπως για παράδειγμα το

utorrent. Το αρχείο αυτό περιέχει πληροφορίες σχετικά με το μέγεθος του αρχείου που θέλει να κατεβάσει ο χρήστης, το πλήθος τον τμημάτων που αποτελούν αυτό το αρχείο και τον tracker στον οποίο πρέπει να συνδεθεί ο χρήστης. Με τον όρο tracker εννοούμε έναν κεντρικό server, η αποκλειστική λειτουργία του οποίου είναι να ενημερώνει τον client που χρησιμοποιεί ο χρήστης, σχετικά με το ποιοι κόμβοι έχουν εκείνη την στιγμή ολόκληρο ή κάποια τμήματα του επιθυμητού αρχείου και μπορούν να το διαμοιράσουν

Σε αντίθεση με τα άλλα δίκτυα P2P, που έχουν μια δενδροειδή δομή και όπου η ανταλλαγή των αρχείων γίνεται κυρίως ανάμεσα σε δύο υπολογιστές, σε ένα δίκτυο που χρησιμοποιεί το BitTorrent πρωτόκολλο, οι χρήστες που διαμοιράζονται ένα αρχείο σχηματίζουν τα λεγόμενα «κοπάδια» (swarm). Κάθε χρήστης που έχει ολόκληρο το αρχείο ονομάζεται seed ή αλλιώς seeder, ενώ οι χρήστες που δεν έχουν ακόμη ολόκληρο το αρχείο ονομάζονται peers ή, αλλιώς, leechers. Όταν κάποιος leecher αποκτήσει ολόκληρο το αρχείο, μετατρέπεται σε seeder και μπορεί να συνεχίσει να μεταβιβάζει τμήματα του αρχείου στα υπόλοιπα μέλη του swarm. Με τον τρόπο αυτό μεγιστοποιείται η πιθανότητα των πιθανών leecher να αποκτήσουν τελικά το αρχείο.

Ένα άλλο πλεονέκτημα αυτού του πρωτοκόλλου είναι πως ακόμα και οι χρήστες οι οποίοι δεν έχουν ακόμα ολόκληρο το αρχείο, μπορούν να δίνουν σε άλλους χρήστες τα τμήματα του αρχείου τα οποία έχουν ήδη κατεβάσει, αυξάνοντας με τον τρόπο αυτό την ταχύτητα με την οποία διαμοιράζεται τελικά ένα αρχείο. Όταν το αρχείο αποκτηθεί από μερικούς peers, ο αρχικός seeder, δηλαδή αυτός ο οποίος δημιούργησε το.torrent αρχείο και που ήταν ο πρώτος που άρχισε το «ανέβασμα» του αρχείου μπορεί να σταματήσει το ανέβασμα του συγκεκριμένου αρχείου και να αρχίσει να ανεβάζει κάποιο άλλο. Σε αυτό το πρωτόκολλο, δηλαδή, δεν υπάρχει μεγάλη εξάρτηση από τον αρχικό seeder, κάτι που διασφαλίζει, εκτός των άλλων, και την μεγάλη βιωσιμότητα των αρχείων.

Με την εξέλιξη αυτού του πρωτοκόλλου δημιουργήθηκαν και περισσότερο αποκεντρωτικά δίκτυα, τα οποία δεν βασίζονται σε κάποιον tracker. Σε αυτά τα δίκτυα η εύρεση των κόμβων που μοιράζονται κάποιο αρχείο και η σύνδεση με αυτά

γίνεται μέσω της τεχνολογίας κατανεμημένων πινάκων κατακερματισμού DHT (Distributed Hash Tables),οι οποία βοήθησε στην αντιμετώπιση του προβλήματος της διαθεσιμότητας καθώς μέσω της αντιγραφής και διατήρησης αρχείων σε γειτονικούς κόμβους από κάποιον κόμβο η αναζήτηση γινόταν γρήγορα και αποτελεσματικά.

1.3.3 Τα συστήματα κοινής χρήσης αρχείων τρίτης και τέταρτης γενιάς

Ως γνωστόν πολλοί θέλουν το κλείσιμο των P2P δικτύων, έτσι προσπαθούν με μηνύσεις να μας φοβίσουν, αλλά έρχεται και μια ακόμα λύση επί αυτού του θέματος. Η 3η γενιά!

Η τρίτης γενιάς είναι παρόμοια με την δεύτερη μόνο που εισαγάγει την έννοια της ανωνυμίας (anonymity). Ένας βαθμός ανωνυμίας δημιουργείται με το να δρομολογείται ή κίνηση μας μέσω κόμβων άλλων χρηστών πράγμα που κάνει δύσκολο για κάποιον να προσδιορίσει ποιος κατεβάζει και ποιος προσφέρει αρχεία στο δίκτυο. Επιπρόσθετα τα περισσότερα δίκτυα διαθέτουν μηχανισμούς κωδικοποίησης του ανταλλασσόμενου περιεχομένου, ενώ σε πολλές περιπτώσεις η ανωνυμία των προσωπικών υπολογιστών επιτυγχάνεται με την απόδοση εικονικών διευθύνσεων IP στους χρήστες από τα δίκτυα P2P.

Αποτέλεσμα της επιβάρυνσης των ''ανώνυμων'' δικτύων με επιπρόσθετες λειτουργίες που συχνά επιβαρύνουν και καθυστερούν το σύστημα, αποτέλεσε η περιορισμένη χρήση των δικτύων τρίτης γενιάς για διαμοιρασμό αντικειμένων. Χαρακτηριστικά παραδείγματα αποτελούν τα WASTE, JetiANts, Tor και I2P. Τα περισσότερα των προγραμμάτων αυτών έχουν δυνατή κρυπτογράφηση και προστασία από traffic sniffing (υποκλοπή κίνησης πακέτων).

Επίσης ένας ακόμα τύπος ομότιμων δικτύων τρίτης γενιάς που εμφανίστηκε είναι αυτός του φίλου προς φίλο (Friend to Friend) επικοινωνίας. Αυτό το μοντέλο επιτρέπει απευθείας σύνδεση για την προώθηση αρχείων αιτήσεων των κόμβων των οποίων οι χρήστες γνωρίζονται μεταξύ τους και την επιτρέπουν ο ένας στον άλλο. Παραδείγματα ''ανώνυμων'' δικτύων αποτελούν τα ANts P2P, RShare, Freenet, I2P, GNUnet και Entropy.

Πέρα από την παραδοσιακή λειτουργία της ανταλλαγής αρχείων υπάρχουν σήμερα υπηρεσίας που στέλνουν ροές δεδομένων αντί για αρχεία εντός ενός ομότιμου δικτύου. Έτσι μπορεί κάποιος να ακούσει ράδιο ή να δει τηλεόραση χωρίς κάποιον εξυπηρετητή να παρεμβάλλεται. Ένα δημοφιλές παράδειγμα τέτοιου δικτύου είναι το Justin.tv (www.justin.tv) όπου κανείς μπορεί να δει online αθλητικά γεγονότα, ταινίες, διάφορες τηλεοπτικές εκπομπές καθώς και να δημιουργήσει το δικό του προσωπικό κανάλι στο οποίο μπορούν να συνδεθούν και να παρακολουθούσουν άλλοι χρήστες.

Σχήμα 1: Συσχετισμός ταχύτητας ανώνυμων και μη, δικτύων P2P [4]

[4] Φώτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων". 2007.

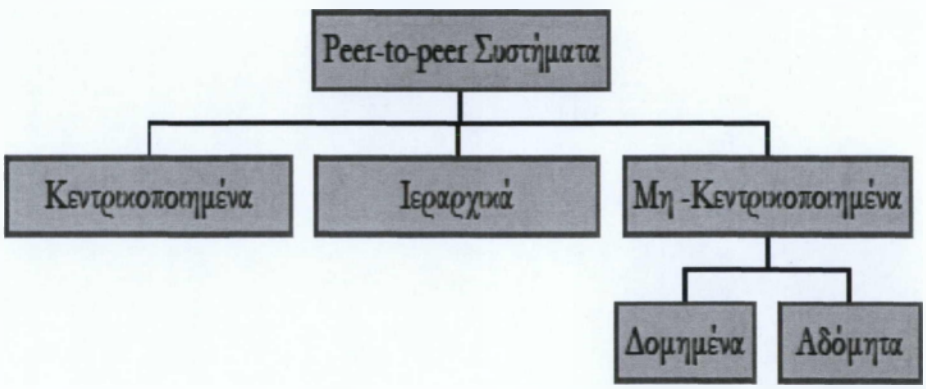
Κεφάλαιο 2ο

2 Αρχιτεκτονικές P2P δικτύων

Τα συστήματα P2P όπως όλα τα δίκτυα έχουν συγκεκριμένες τοπολογίες και αρχιτεκτονικές. Οι κόμβοι που μετέχουν σε ένα P2P σύστημα σχηματίζουν ένα δίκτυο επικάλυψης (overlay network) πάνω από την υπάρχουσα υποδομή του διαδικτύου. Διασυνδέονται, επικοινωνούν και ανταλλάσσουν πληροφορίες μεταξύ τους σε τοπολογίες ανεξάρτητα από το δίκτυο υποδομής (IP network) διατηρώντας την αυτονομία τους.

Η αρχιτεκτονική του δικτύου επηρεάζει τον μηχανισμό δρομολόγησης μηνυμάτων αναζήτησης, την απόδοση, την ικανότητα κλιμάκωσης, την προσαρμοστικότητα ανοχή σε σφάλματα, κλπ. και στοχεύει στην υποστήριξη λειτουργιών όπως διαμοιρασμό αρχείων (file sharing), κατανεμημένο υπολογισμό (distributed computing), επικοινωνία – συνεργασία μεταξύ των χρηστών (collaboration network).

Υπάρχουν διάφορες αρχιτεκτονικές για τον σχηματισμό του overlay δικτύου :



Σχήμα 2.1: Peer to Peer Αρχιτεκτονικές[5]

[5] Μαργαρίτη, "Data Management in Peer`to`Peer Systems", Technical report, Πανεπιστήμιο Ιωαννίνων, 2005.

2.1 Κεντρικοποιημένη P2P Αρχιτεκτονική (Centralized P2P)

Σχήμα 2.2: Αρχιτεκτονική κεντρικού καταλόγου [6]

Στην κεντρικοποιημένη αρχιτεκτονική οι υπολογιστές- κόμβοι συνδέονται μεταξύ τους αλλά και με έναν κεντρικό εξυπηρετητή (server). Ο κεντρικός αυτός server είναι και ο αποκλειστικός υπεύθυνος για τον συντονισμό των συμμετεχόντων στο σύστημα χρηστών και για την διατήρηση ενός δείκτη για κάθε διαθέσιμο προς διαμοιρασμό αρχείο. Όταν ένας χρήστης εκκινεί την εφαρμογή κοινής χρήσης αρχείων P2P, η εφαρμογή έρχεται σε επαφή με τον εξυπηρετητή καταλόγου. Ειδικά, η εφαρμογή που εκτελείται στον ομότιμο πληροφορεί τον εξυπηρετητή καταλόγου για την διεύθυνσή IP της και για τα αντικείμενα στον τοπικό της δίσκο, τα οποία κάνει διαθέσιμα για κοινή χρήση (π.χ. τους τίτλους όλων των αποθηκευμένων αρχείων MP3).

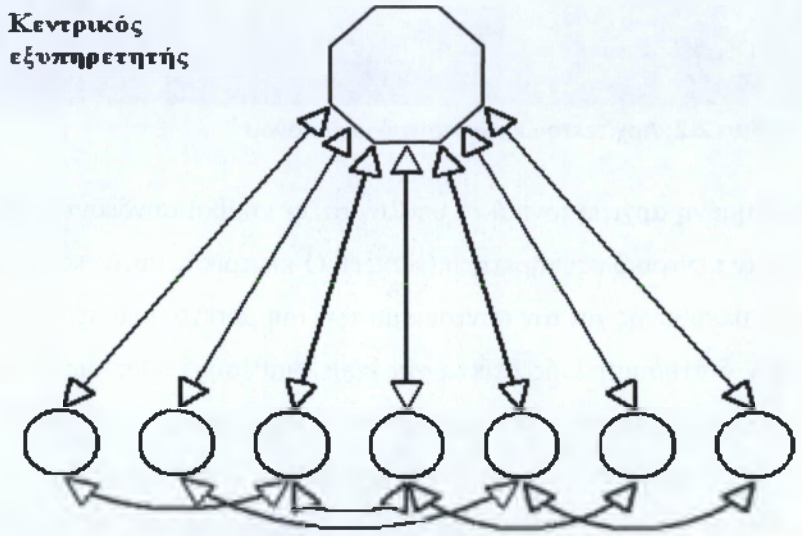
Με αυτόν τον τρόπο, ο εξυπηρετητής καταλόγου ξέρει ποια αντικείμενα έχει διαθέσιμα για κοινή χρήση ο ομότιμος υπολογιστής. Ο εξυπηρετητής καταλόγου συλλέγει αυτές τις πληροφορίες από κάθε ενεργό ομότιμο, και έτσι δημιουργεί μια

---

[6] Φώτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων". 2007.

κεντρικοποιημένη δυναμική βάση δεδομένων, που αντιστοιχίζει κάθε όνομα αντικειμένου σε ένα σύνολο διευθύνσεων IP. Όταν ένας ενεργός ομότιμος πάρει ένα νέο αντικείμενο ή αφαιρέσει ένα αντικείμενο, πληροφορεί τον εξυπηρετητή καταλόγου, έτσι ώστε αυτός με την σειρά του να ενημερώσει την βάση δεδομένων του για την εν λόγω ενέργεια.

Για να ανιχνεύσει ένα αρχείο, ο ομότιμος στέλνει μια αίτηση στον κεντρικό εξυπηρετητή, ο οποίος πραγματοποιεί μια αναζήτηση στην κεντρικοποιημένη βάση δεδομένων του και εντέλει αποκρίνεται με μια λίστα των χρηστών που διαθέτουν το επιθυμητό αρχείο.



Σχήμα 2.3: Κεντρικοποιημένη Αρχιτεκτονική[7]

Για να παραμένει η βάση δεδομένων του ενημερωμένη, ο εξυπηρετητής καταλόγου πρέπει να είναι σε θέση να καθορίσει πότε αποσυνδέεται ένας ομότιμος. Ένας ομότιμος μπορεί να αποσυνδεθεί κλείνοντας την εφαρμογή πελάτη P2P ή απλώς αποσυνδεόμενος από το διαδίκτυο. Ένας τρόπος παρακολούθησης του ποιοι ομότιμοι παραμένουν συνδεδεμένοι είναι να στέλνονται περιοδικά μηνύματα προς ομότιμους, για να διαπιστώσει ο εξυπηρετητής αν αποκρίνονται. Ένας άλλος τρόπος

[7] Φωτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων" 2007.

παρακολούθησης από τον εξυπηρετητή των συνδεδεμένων ομότιμων είναι η διατήρηση μιας μόνιμης TCP σύνδεσης μεταξύ του εξυπηρετητή και του κάθε συνδεδεμένου ομότιμου. Αν η TCP σύνδεση κλείσει, τότε ο ομότιμος έχει αποσυνδεθεί και ο εξυπηρετητής καταλόγου αφαιρεί τα ονόματα αντικειμένων και τις αντίστοιχες διευθύνσεις IP του ομότιμου από την βάση δεδομένων του.

Αυτή η αρχιτεκτονική είχε χρησιμοποιηθεί από το Napster.

Τέτοια συστήματα είναι απλά και λειτουργούν γρήγορα και αποτελεσματικά για την εύρεση πληροφοριών. Οι αναζητήσεις είναι περιεκτικές και μπορούν να παρέχουν την εγγύηση στις αναζητήσεις. Το βασικότερο πλεονέκτημα της χρήσης κεντρικοποιημένου καταλόγου είναι η απλότητα της συγκεκριμένης αρχιτεκτονικής. Υπάρχουν όμως και αρκετά μειονεκτήματα, τα βασικότερα εκαιτων οποίων είναι:

- *Ένα μόνο σημείο αποτυχίας:* Αν ο κεντρικός εξυπηρετητής καταλόγου καταρρεύσει για οποιονδήποτε λόγο τότε καταρρέει μαζί του όλη η εφαρμογή P2P. Ακόμη και αν χρησιμοποιείται μια φάρμα εξυπηρετητών με πλεονάζοντες εξυπηρετητές, οι συνδέσεις διαδικτύου προς την φάρμα μπορούν να αποτύχουν, κάνοντας όλη την εφαρμογή να καταρρεύσει.

- *Συμφόρηση απόδοσης:* Σε ένα μεγάλο σύστημα Peer to Peer, με εκατοντάδες χιλιάδες συνδεδεμένων χρηστών, ένας κεντρικοποιημένος εξυπηρετητής πρέπει να διατηρεί μια τεράστια βάση δεδομένων καθώς και να αποκρίνεται σε χιλιάδες ερωτήματα ανά δευτερόλεπτο. Πράγματι το έτος 2000, όταν ήταν ακόμα η δημοφιλέστερη εφαρμογή Peer to Peer, το Napster βασανιζόταν από προβλήματα κίνησης στον κεντρικοποιημένο του εξυπηρετητή.

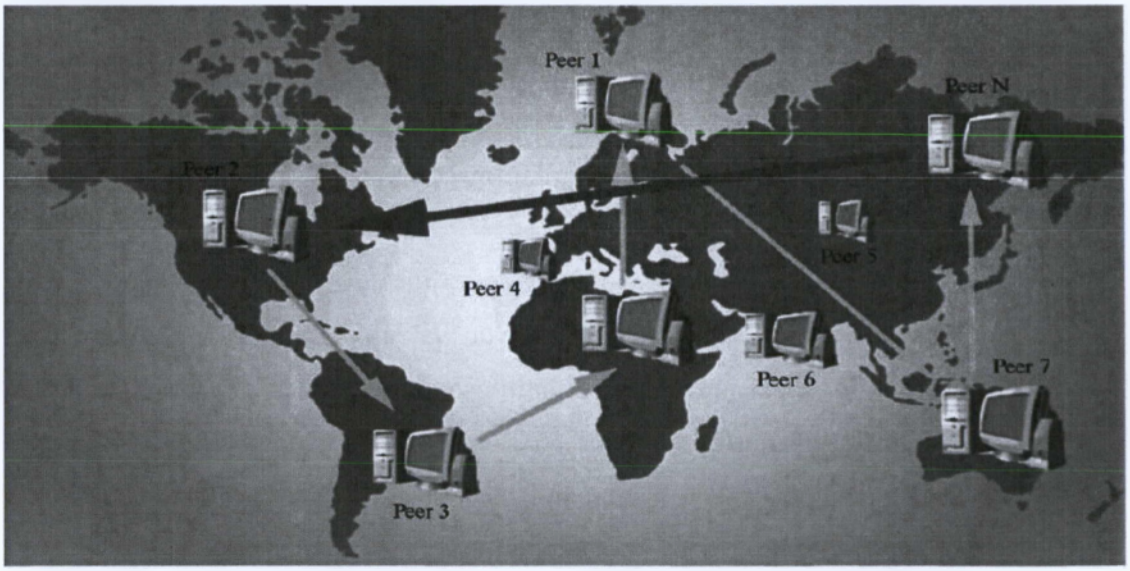
- *Παραβίαση πνευματικών δικαιωμάτων:* Η παγκόσμια βιομηχανία παραγωγής δίσκων προβληματίζεται έντονα από το γεγονός ότι τα συστήματα κοινής χρήσης αρχείων P2P επιτρέπουν σε χρήστες να λαμβάνουν δωρεάν περιεχόμενο που καλύπτεται από πνευματικά δικαιώματα. Όταν μια εταιρεία P2P έχει έναν κεντρικοποιημένο εξυπηρετητή καταλόγου, νομικά προβλήματα μπορούν να αναγκάσουν την εταιρεία να τον απενεργοποιήσει. Σαφώς, είναι

πιο δύσκολο να κλείσουν οι περισσότερο αποκεντρωμένες αρχιτεκτονικά εφαρμογές.

2.2 Ιεραρχική P2P Αρχιτεκτονική

Οι κομβόι οργανώνονται σε ιεραρχική δομή όπως γίνεται με τους DNS στο διαδίκτυο. Στα ιεραρχικά P2P συστήματα εισάγεται ή έννοια των "super-peers" (FastTrack),δηλαδή, οι ομότιμοι κόμβοι χωρίζονται σε δύο κατηγορίες, στους υπερ-κόμβος (super-peers) και στους πελάτες (clients). Η δομή τους μπορεί να είναι κεντρικοποιημένη ή μη.

2.3 Μη κεντρικοποιημένη P2P αρχιτεκτονική (Un- Centralized P2P)



Σχήμα 2.4: Αρχιτεκτονική μη-κεντρικοποιημένου καταλόγου[8]

Μια άλλη κατηγορία αρχιτεκτονικών είναι οι μη-κεντρικοποιημένες όπου οι κόμβοι συγκροτούν το overlay δίκτυο είτε δομημένα ακολουθώντας κανόνες για τον

[8] Φώτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων". 2007.

σχηματισμό του δικτύου, είτε αδόμητα όπου δεν υπάρχει ούτε κεντρικό directory ούτε ακριβείς οδηγίες για τον σχηματισμό τοπολογίας του δικτύου και την τοποθέτηση των περιεχομένων. Αυτό που διαφοροποιεί τα μη κεντρικοποιημένα P2P δίκτυα από αυτά της προηγούμενης ενότητας είναι ότι δε διαθέτουν κάποιον κεντρικό κατάλογο-ευρετήριο.

2.3.1 Αδόμητα Συστήματα

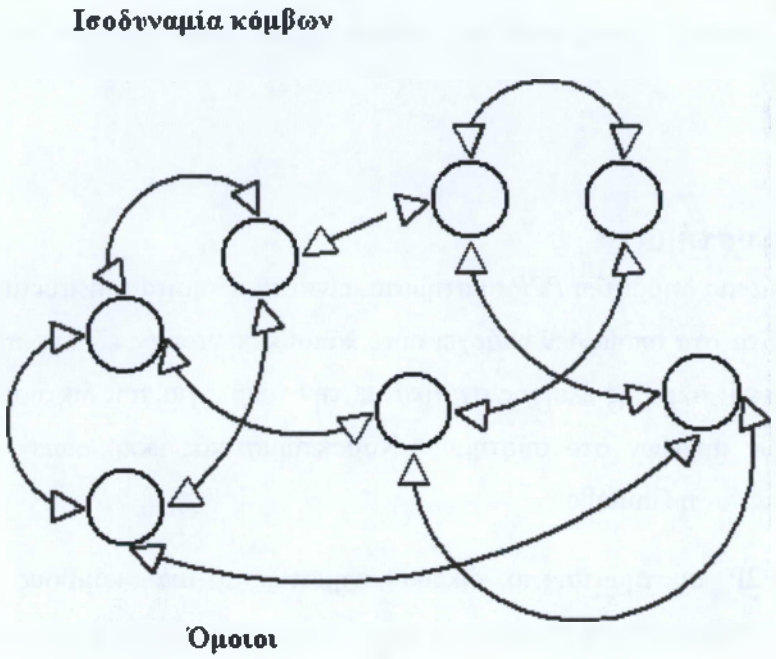
Στις μέρες μας, τα πιο δημοφιλή *P2P* συστήματα, είναι τα αδόμητα (unstructured). Αυτά είναι συστήματα στα οποία δεν υπάρχει ούτε κάποιος κεντρικός εξυπηρετητής (server), άλλα ούτε και ακριβής έλεγχος σχετικά με την τοπολογία του δικτύου και την τοποθέτηση των αρχείων στο σύστημα. Χαρακτηριστικός εκπρόσωπος των συστημάτων αυτών είναι η Gnutella.

Στα αδόμητα P2P συστήματα, το δίκτυο σχηματίζεται από κόμβους που συνδέονται χωρίς συγκεκριμένους κανόνες. Η προκύπτουσα τοπολογία έχει κάποιες ιδιότητες, αλλά η τοποθέτηση των αρχείων στο σύστημα είναι ανεξάρτητη από αυτή, σε αντίθεση με τα δομημένα P2P συστήματα. Τα αδομητα P2P δίκτυα για την αναζήτηση αρχείων χρησιμοποιούν το πρωτόκολλο πλημμύρας (Flooding protocol).

Ένας ομότιμος συνδέεται στο δίκτυο επικάλυψης, ερχόμενος δηλαδή σε επαφή με έναν κόμβο εκκίνησης, ο οποίος και του παρέχει την διεύθυνση IP ενός ή περισσοτέρων υφιστάμενων ομότιμων μέσα στο δίκτυο. Κάθε ομότιμος ξέρει μόνο τους γειτονικούς του ομότιμους, δηλαδή τους χρήστες με τους οποίους διατηρεί μια γραμμή σύνδεσης μέσα στο δίκτυο επικάλυψης.. Όπως με το ιεραρχικό δίκτυο επικάλυψης απαιτείται ένα αρκετά πολύπλοκο πρωτόκολλο για την συντήρηση του δικτύου, δεδομένης της απρόβλεπτης συμπεριφοράς των χρηστών σε ότι αφορά την συχνότητα σύνδεσης και αποσύνδεσης.

Τα P2P συστήματα αυτής της μορφής, είναι πολύ ανθεκτικά στις εισόδους και τις αποχωρήσεις κόμβων, ωστόσο παρουσιάζουν και σημαντικά μειονεκτήματα. Βασικό μειονέκτημα τους είναι ότι το ερωτήματα που τίθεται δεν μπορεί πάντα να απαντηθεί. Δημοφιλές περιεχόμενο μπορεί να είναι διαθέσιμο σε διάφορους χρήστες

αλλά αν ένας ομότιμος ψάχνει για σπάνια αντικείμενα ή μοιράζετε μόνο μερικά άλλα τους ομόλογους του, τότε είναι μάλλον απίθανο ότι η αναζήτηση θα είναι επιτυχείς.



Σχήμα 2.5: Αδόμητα Συστήματα[9]

Δεδομένου ότι δεν υπάρχει συσχετισμός μεταξύ ομότιμων και το περιεχόμενο που αυτή διαχειρίζονται, δεν υπάρχει εγγύηση ότι οι πλημμύρες θα βρουν ένα ομότιμο που έχει τα επιθυμητά στοιχεία. Έτσι τα αδόμητα συστήματα έχουν πολύ κακή απόδοση αναζήτησης.

Αδόμητα Peer to Peer δίκτυα είναι: Gnutella, FastTrack, KaZaA,BitTorrent κ.α.

2.3.2 Δομημένα Συστήματα

Στα δομημένα συστήματα, η τοπολογία του δικτύου ελέγχεται αυστηρά. Επίσης, κάθε αρχείο τοποθετείται σε συγκεκριμένο κόμβο και όχι τυχαία, με στόχο να γίνει η αναζήτηση μέσα στο σύστημα πιο αποτελεσματική. Αυτό επιτυγχάνεται με τη χρήση

[9] Φώτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων". 2007.

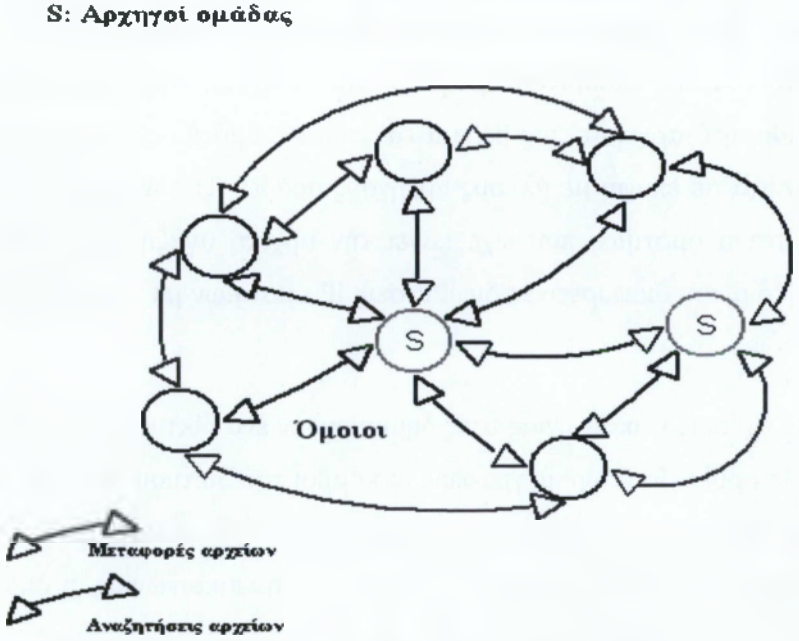
ενός μηχανισμού απεικόνισης, των αρχείων στους κόμβους, που συνήθως είναι μία συνάρτηση κατακερματισμού (***hashing***).

Ένας αριθμός χρηστών χρίζονται αρχηγοί ομάδων. Όταν ένας ομότιμος συνδέεται στην εφαρμογή P2P, ο ομότιμος εκχωρείται σε έναν από τους αρχηγούς ομάδων. Αφού μάθει την διεύθυνση IP του αρχηγού της ομάδας του ο ομότιμος έρχεται σε επαφή μαζί του και τον πληροφορεί για όλα τα τοπικά προς αυτόν περιεχόμενα που είναι έτοιμος να μοιραστεί. Ό αρχηγός ομάδας διατηρεί μια βάση δεδομένων που αντιστοιχεί ονόματα περιεχομένου με διευθύνσεις IP, για όλους τους ομότιμους που έχουν εκχωρηθεί σε αυτή την ομάδα. Με αυτόν τον τρόπο κάθε ομάδα γίνεται ένα συρρικνωμένο σύστημα κοινής χρήσης αρχείων, με τον αρχηγό της ομάδας να έχει έναν αντίστοιχο ρόλο με αυτόν του κεντρικοποιημένου εξυπηρετητή καταλόγου της Κεντρικοποιημενης αρχιτεκτονικής. Είναι σημαντικό να αναφερθεί ότι ο αρχηγός ομάδας, που είναι ένας συνηθισμένος ομότιμος και όχι αποκλειστικά εξυπηρετητής, ενημερώνει την βάση δεδομένων του μόνο για τα περιεχόμενα των μελών της ομάδας του, μη γνωρίζοντας οτιδήποτε για χρήστες εκτός της ομάδας αυτής.

Για να ανιχνεύσει ένας χρήστης ένα συγκεκριμένο αρχείο απευθύνεται στον αρχηγό της ομάδας του. Αυτός αποκρίνεται με μια λίστα ομότιμων της ίδιας ομάδας που κατέχουν το επιθυμητό αρχείο εκτός βέβαια εάν τέτοιος ομότιμος δεν υπάρχει, οπότε ο αρχηγός έρχεται σε επαφή με άλλους αρχηγούς ομάδων ζητώντας τους την αντίστοιχη λίστα. Έτσι ο ομότιμος που είχε κάνει την αρχική αναζήτηση μπορεί εντέλει να έχει στα χέρια του διαφορετικές διευθύνσεις IP ομότιμων με το επιθυμητό αρχείο στην κατοχή τους.

Οι ομότιμοι και οι σχέσεις επικοινωνίας τους δημιουργούν ένα δίκτυο επικάλυψης (overlay network). Με ορολογία θεωρίας γράφων, οι κόμβοι του δικτύου επικάλυψης είναι οι ομότιμοι. Μεταξύ των ομότιμων και του αρχηγού της ομάδας, αλλά και μεταξύ των αρχηγών ομάδας ανά δύο υπάρχει εικονική ζεύξη επικοινωνίας, η οποία και παριστάνεται στο δίκτυο επικάλυψης με μια γραμμή. Για παράδειγμα ακόμα και αν ένας ομότιμος και ο αρχηγός της ομάδας του βρίσκονται σε διαφορετικούς παροχείς ISPs σε διαφορετικούς ηπείρους, συνδέονται απ' ευθείας με μια γραμμή στο δίκτυο επικάλυψης και έτσι αποτελούν δύο εικονικούς γείτονες.

Επειδή οι ομότιμοι συνδέονται και αποσυνδέονται συνεχώς και με απρόβλεπτη συχνότητα (περιλαμβανομένων και των ομότιμων-αρχηγών ομάδων), το δίκτυο επικάλυψης είναι αναπτυσσόμενο και άκρως δυναμικό. Για να συνδεθεί ένας χρήστης στο δίκτυο επικάλυψης πρέπει να καθορίσει τουλάχιστον μια γραμμή ανάμεσα στον εαυτό του και έναν άλλο χρήστη που βρίσκεται ήδη στο σύστημα. Αυτό συνεπάγεται ότι ο ομότιμος πρέπει να λάβει γνώση της διεύθυνσης IP κάποιου άλλου ομότιμου στο σύστημα. Έτσι το σύστημα P2P κοινής χρήσης αρχείων πρέπει να διαθέτει έναν κόμβο εκκίνησης (ή πολλαπλούς κόμβους εκκίνησης). Όταν ένας ομότιμος εισέρχεται στο σύστημα έρχεται σε επαφή με αυτόν τον κόμβο εκκίνησης. Ο κόμβος με την σειρά του αποκρίνεται με την διεύθυνση IP ενός από τους αρχηγούς ομάδων και ο ομότιμος καθορίζει μια γραμμή μαζί του. Επίσης υπάρχει η πιθανότητα ο κόμβος εκκίνησης να χρίσει τον ομότιμο νέο αρχηγό ομάδας, οπότε στην περίπτωση αυτή ο ομότιμος χρειάζεται τις διευθύνσεις IP κάποιων άλλων αρχηγών ομάδων.



Σχήμα 2.6: Δομημένα Συστήματα[10]

[10] Φώτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων". 2007.

Ένα από τα ελκυστικά χαρακτηριστικά αυτής της προσέγγισης αποκεντρωμένου καταλόγου είναι ότι δεν υπάρχει ένας αποκλειστικός εξυπηρετητής για την βάση δεδομένων καταλόγου, αλλά η βάση δεδομένων είναι τώρα κατανεμημένη επάνω σε ένα υποσύνολο ομότιμων, τους αρχηγούς ομάδων. Αν συνυπολογίσει κανείς ότι κάθε αρχηγός ομάδας παρακολουθεί μόνο τα περιεχόμενα της ομάδας του, οι βάσεις δεδομένων καταλόγου είναι πια σχετικά μικρές σε μέγεθος. Επιπρόσθετα, επειδή οι βάσεις δεδομένων βρίσκονται κατανεμημένες επάνω σε συνηθισμένους ομότιμους, είναι πιο δύσκολο να πραγματοποιηθούν νομικές ενέργειες με σκοπό την παύση του συστήματος κοινής χρήσης αρχείων P2P (π.χ. λόγω παραβίασης πνευματικών δικαιωμάτων), σε σχέση με την απλή παύση ενός κεντρικοποιημένου εξυπηρετητή καταλόγου. Και αυτή η αρχιτεκτονική όμως χαρακτηρίζεται από σοβαρά μειονεκτήματα:

- *Πολυπλοκότητα:* Ένα αρκετά πολύπλοκο πρωτόκολλο πρέπει να χρησιμοποιηθεί για την κατασκευή και συντήρηση του δικτύου επικάλυψης. Για παράδειγμα, στην περίπτωση που ένας αρχηγός ομάδας αποσυνδεθεί από το σύστημα, το δίκτυο επικάλυψης αφού αναγνωρίσει την αποσύνδεση πρέπει να εκχωρήσει όλους τους ομότιμους της ομάδας σε έναν νέο αρχηγό ομάδας. Τέτοια και άλλα παρόμοια ζητήματα καθιστούν την συντήρηση του δικτύου επικάλυψης πολύπλοκη εργασία.

- *Ιεραρχία:* Ακόμα και σε αυτήν την άκρως αποκεντρωμένη προσέγγιση οι ομότιμοι που είναι αρχηγοί ομάδων δεν χαρακτηρίζονται ισότιμοι με τους απλούς ομότιμους-μέλη μιας ομάδας. Σε ένα πραγματικά αποκεντρωμένο και κατανεμημένο σύστημα όλοι οι ομότιμοι θα έπρεπε να ήταν ίσοι. Επειδή οι αρχηγοί ομάδων έχουν περισσότερες αρμοδιότητες, αναλαμβάνουν ένα μεγάλο κομμάτι εργασίας και έτσι μπορεί να προκληθούν συμφορήσεις.

- *Κόμβος εκκίνησης:* Το σύστημα δεν είναι ένα γνήσιο σύστημα χωρίς εξυπηρετητή, μιας και ο κόμβος εκκίνησης πρέπει να βρίσκεται σε έναν εξυπηρετητή που βρίσκεται πάντα σε λειτουργία. Αν και οι αρμοδιότητες αυτού του κόμβου εκκίνησης είναι λίγες όπως είδαμε (εκχώρηση ομότιμων

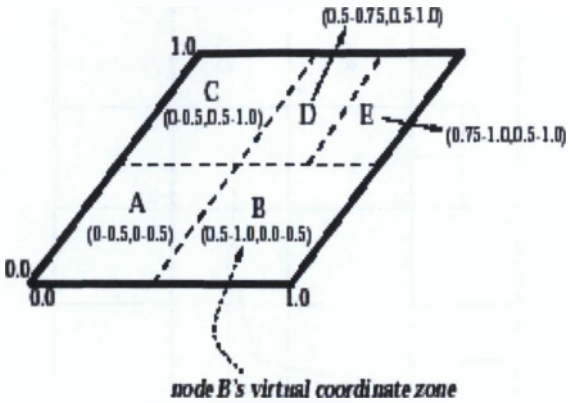
που συνδέονται σε αρχηγούς ομάδων, καθορισμός αρχηγών ομάδων και συντήρηση του δικτύου επικάλυψης), ένας ή περισσότεροι κόμβοι εκκίνησης πρέπει να είναι πάντα και μόνιμα παρόντες.

Στη συνέχεια περιγράφονται δύο από τα γνωστότερα δομημένα συστήματα, το Chord και το CAN.

2.3.2.1 CAN (Content-Addressable Network)

Το δίκτυο CAN συμπεριφέρεται σαν ένας πίνακας κατακερματισμού ο οποίος αντιστοιχεί κλειδιά ("keys") σε τιμές ("values"). Οι τρεις βασικές λειτουργίες του είναι η εισαγωγή, η αναζήτηση και η διαγραφή δεδομένων. Πρόκειται για ένα πλήρως κατανεμημένο δίκτυο από ανεξάρτητους κόμβους, καθένας από τους οποίους κατέχει ένα κομμάτι-ζώνη (που ονομάζεται "zone") του πίνακα κατακερματισμού και αποθηκεύει πληροφορίες για τους γειτονικούς του κόμβους. Η οργάνωση του δικτύου περιστρέφεται γύρω από ένα εικονικό σύστημα συντεταγμένων d διαστάσεων με τη μορφή ενός d-torus. Το σύστημα αυτό συντεταγμένων αναφέρεται και με τον όρο "reality".

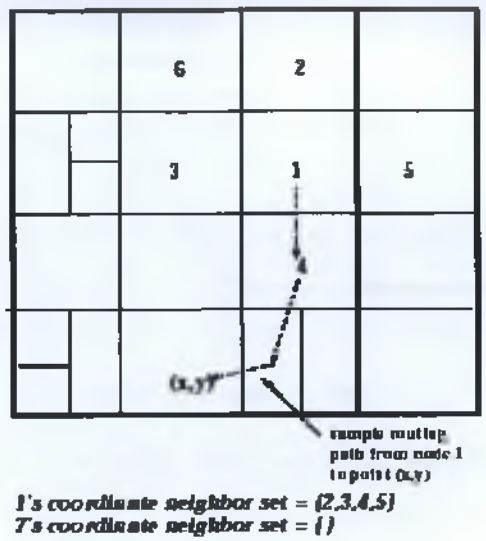
Σε κάθε στιγμή, το σύστημα συντεταγμένων διαμερίζεται δυναμικά σε όλους τους κόμβους που υπάρχουν στο δίκτυο έτσι ώστε κάθε κόμβος να κατέχει τη δική του ανεξάρτητη ζώνη σε αυτό. Έτσι στο Σχήμα 2.7 ο δισδιάστατος χώρος διαμερίζεται σε πέντε κόμβους και για παράδειγμα ο κόμβος B κατέχει το κομμάτι-ζώνη με συντεταγμένες (0.5-1.0,0.0-0.5). Το σύστημα συντεταγμένων αποθηκεύει ζεύγη (κλειδί, τιμή) όπου το κλειδί κάθε ζεύγους αντιστοιχίζεται σε ένα σημείου P αυτού του χώρου με μια ομοιόμορφη συνάρτηση κατακερματισμού. Τελικά ένα ζεύγος αποθηκεύεται στον κόμβο που κατέχει τη ζώνη με το σημείο P στο οποίο αντιστοιχίζεται το κλειδί του.



Σχήμα 2.7: Παράδειγμα ενός χώρου 2-διαστάσεων με πέντε κόμβους[11]

Ένα τέτοιο δίκτυο οργανώνεται ως εξής με τις συνεχείς εισαγωγές νέων κόμβων. Ένας κόμβος που επιθυμεί να εισαχθεί στο δίκτυο επιλέγει τυχαία ένα σημείο P στο χώρο. Στη συνέχεια ο νέος κόμβος γνωρίζοντας έναν κόμβο που υπάρχει ήδη στο δίκτυο αναλαμβάνει να στείλει μέσω αυτού ένα μήνυμα στον κόμβο που κατέχει τη ζώνη με το συγκεκριμένο σημείο P. Η δρομολόγηση του μηνύματος γίνεται με το μηχανισμό δρομολόγησης που περιγράφεται στη συνέχεια. Όταν το μήνυμα φτάσει στον προορισμένο κόμβο, ο τελευταίος διαιρεί τη ζώνη που κατέχει στα δύο, κατά μήκος μιας διάστασης και ο νέος κόμβος αναλαμβάνει το ένα από τα δύο τμήματα που προκύπτουν καθώς και τα δεδομένα που είναι αποθηκευμένα σε αυτό. Τέλος πρέπει να ενημερωθούν οι γείτονες του νέου και του διαιρεμένου κόμβου για τις αλλαγές.

[11] Ν. Κρεμμύδας, "Επισκόπηση στα Συστήματα Ομότιμων Κόμβων", Ε.Μ Π., 2005.



Σχήμα 2.8: Παράδειγμα δικτύου CAN και αναζήτησης σε αυτό ενός δεδομένου[12]

Ένας κόμβος που θέλει να ανακτήσει κάποιο δεδομένο που αντιστοιχίζεται σε ένα κλειδί εφαρμόζει την ίδια συνάρτηση κατακερματισμού (που αντιστοιχίζει δεδομένα σε ζώνες) πάνω στο κλειδί και προκύπτει το σημείο P όπου αποθηκεύεται το ζεύγος (κλειδί, τιμή). Αν το P δεν ανήκει στον κόμβο που έκανε την αίτηση τότε αυτή δρομολογείται προς την κατεύθυνση του P μέσω των γειτόνων του εφαρμόζοντας ένα "greedy" αλγόριθμο, δρομολογείται δηλαδή στο γείτονα με τις πιο κοντινές συντεταγμένες με τον προορισμό. Στο παράδειγμα του Σχήματος 2.8 ο κόμβος 1 επιθυμεί να ανακτήσει το δεδομένο που αντιστοιχίζεται στο σημείο (x,y). Επειδή ο ίδιος δεν κατέχει αυτό το σημείο δρομολογεί την ερώτηση στον κοντινότερο προς το σημείο γείτονά του, τον κόμβο 4 ο οποίος με τη σειρά του επιλέγει έναν κατάλληλο γείτονα για τη δρομολόγηση της ερώτησης που τελικά φτάνει στο σημείο (x,y).

2.3.2.1.1 Δρομολόγηση στο CAN

Κάθε κόμβος στο CAN, διατηρεί ένα πίνακα δρομολόγησης στον οποίο αποθηκεύει τις IP διευθύνσεις και τις συντεταγμένες των ζωνών των γειτόνων του. Οι

[12] Ν. Κρεμμύδας, "Επισκόπηση στα Συστήματα Ομότιμων Κόμβων", Ε.Μ.Π., 2005.

πληροφορίες αυτές είναι αρκετές για τη δρομολόγηση ενός μηνύματος μεταξύ δύο οποιωνδήποτε σημείων στο χώρο συντεταγμένων. Ένα μήνυμα στο CAN περιλαμβάνει και τις συντεταγμένες του σημείου προορισμού του. Έτσι, κάθε κόμβος χρησιμοποιώντας τις συντεταγμένες των γειτόνων του, προωθεί το μήνυμα σε εκείνο το γείτονα με συντεταγμένες πλησιέστερες στο σημείο προορισμού. Για ένα χώρο d διαστάσεων, διαμερισμένο σε n ίσες ζώνες, το μέσο μήκος μονοπατιού δρομολόγησης είναι $(d/4)(n^{1/d})$, ενώ κάθε κόμβος έχει 2d γείτονες.

2.3.2.1.2 Εισαγωγή κόμβου στο CAN

Όταν ένας κόμβος εισέρχεται στο σύστημα, πρέπει να αποκτήσει τη δική του ζώνη στο χώρο συντεταγμένων. Αυτό επιτυγχάνεται με τη διαίρεση της ζώνης ενός κόμβου στη μέση. Η διαδικασία περιλαμβάνει τρία βήματα:

- Ο εισερχόμενος κόμβος εντοπίζει ένα κόμβο στο CAN
- Χρησιμοποιώντας τους μηχανισμούς δρομολόγησης, βρίσκει ένα κόμβο του οποίου η ζώνη θα διαιρεθεί
- Οι γείτονες της ζώνης που διαιρέθηκε ενημερώνονται για την παρουσία του νέου κόμβου

Πιο συγκεκριμένα, ο κόμβος προς εισαγωγή, επιλέγει τυχαία ένα σημείο P και στέλνει ένα μήνυμα συνένωσης με προορισμό το σημείο αυτό. Το μήνυμα δρομολογείται στο CAN μέχρι να φτάσει στον κόμβο στον οποίο ανήκει το P. Στη συνέχεια ο κόμβος αυτός, διαιρεί τη ζώνη του σε δύο ίσα μέρη, κρατάει ένα και δίνει το άλλο στον νέο κόμβο. Επίσης τα αντίστοιχα ζεύγη (K, V), μεταφέρονται στο νέο κόμβο. Για να ολοκληρωθεί η διαδικασία εισαγωγής, θα πρέπει η πληροφορία που κρατάει κάθε κόμβος για τους γείτονές του να είναι έγκυρη. Αυτό επιτυγχάνεται με μηνύματα που στέλνονται περιοδικά από κάθε κόμβο, τα οποία περιλαμβάνουν τις συντεταγμένες της ζώνης του.

2.3.2.1.3 Αποχώρηση κόμβου από το CAN

Όταν ένας κόμβος αποχωρεί από το CAN, τότε η ζώνη του πρέπει να καταληφθεί από κάποιον από τους εναπομείναντες κόμβους. Η τυπική διαδικασία δηλώνει ότι όταν ένας κόμβος θέλει να αποχωρήσει, πρέπει να παραδώσει τη ζώνη και τα ζεύγη του σε έναν από τους γείτονές του. Αν η ζώνη κάποιου εκαιτων γειτόνων του μπορεί να συνενωθεί με τη δική του ζώνη, τότε αυτό γίνεται. Διαφορετικά, η ζώνη παραδίδεται προσωρινά στο γείτονα με τη μικρότερη ζώνη.

Το CAN περιλαμβάνει επίσης και μηχανισμούς ανάκαμψης από αποτυχίες κόμβων. Σε φυσιολογικές συνθήκες, κάθε κόμβος στέλνει περιοδικά μηνύματα στους γείτονές του, με τις συντεταγμένες της ζώνης του και μια λίστα με τους γείτονες του. Η απουσία ενός τέτοιου μηνύματος δηλώνει ότι ο κόμβος έχει αποτύχει. Σε μια τέτοια περίπτωση οι γείτονες του κόμβου αυτού, ξεκινούν ένα αλγόριθμο άμεσης κατάληψης, που εξασφαλίζει ότι η ζώνη του κόμβου που απέτυχε, θα δεσμευθεί από το γείτονα με τη μικρότερη ζώνη.

2.3.2.1.4 Βελτιώσεις του CAN

Βελτιώσεις μπορούν να γίνουν πάνω στις προδιαγραφές του CAN, που περιγράψαμε παραπάνω, με στόχο τη γρηγορότερη δρομολόγηση. Οι σημαντικότερες από αυτές τις βελτιώσεις είναι:

- *Αύξηση του αριθμού των διαστάσεων:* Αυξάνοντας τον αριθμό των διαστάσεων, μειώνεται το μήκος του μονοπατιού δρομολόγησης, με κόστος τη μικρή αύξηση στο μέγεθος του πίνακα δρομολόγησης που διατηρεί κάθε κόμβος.

- *Πολλαπλοί χώροι συντεταγμένων (realities):* Οι κόμβοι καταλαμβάνουν μία ζώνη σε κάθε *reality*. Τα περιεχόμενα του πίνακα κατακερματισμού αναπαράγονται σε κάθε *reality*, αυξάνοντας έτσι τη διαθεσιμότητα των αρχείων.

- *Χρήση πολλαπλών συναρτήσεων κατακερματισμού:* Ένα κλειδί απεικονίζεται σε k σημεία στο χώρο, με χρήση k συναρτήσεων κατακερματισμού, αυξάνοντας έτσι τη διαθεσιμότητα των αρχείων.

- *Τοπολογίες σύμφωνες με την IP τοπολογία των κόμβων:* Κόμβοι που βρίσκονται κοντά στο φυσικό δίκτυο, τοποθετούνται κοντά και στο χώρο συντεταγμένων, μειώνοντας το χρόνο δρομολόγησης.

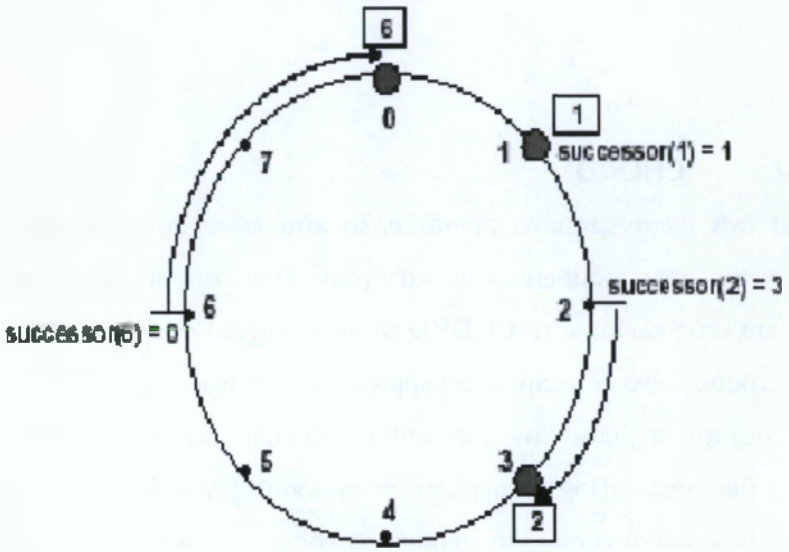
- *Υπερφόρτωση ζωνών:* Μία ζώνη καταλαμβάνεται από περισσότερους του ενός κόμβους, βελτιώνοντας έτσι την αντοχή σε αποτυχίες κόμβων.

2.3.2.2 CHORD

Είναι ένα κατανεμημένο πρωτόκολλο που λύνει το πρόβλημα της αποδοτικής τοποθέτησης των κόμβων που κατέχουν ένα συγκεκριμένο αντικείμενο. Έτσι δεδομένου ενός κλειδιού το CHORD το αντιστοιχίζει σε έναν κόμβο. Το πρωτόκολλο αυτό εφαρμόζει ένα συνεπή κατακερματισμό που εξισορροπεί το φορτίο, αφού κάθε κόμβος δέχεται περίπου τον ίδιο αριθμό κλειδιών. Σε ένα σύστημα με N κόμβους, καθένας διατηρεί O(logN) περίπου πληροφορίες για άλλους κόμβους τις οποίες χρησιμοποιεί στη συνέχεια για τη δρομολόγηση.

Το δίκτυο με βάση αυτό το πρωτόκολλο οργανώνεται ως εξής. Η συνάρτηση κατακερματισμού που χρησιμοποιείται αντιστοιχίζει σε κάθε κόμβο και κλειδί ένα αναγνωριστικό (id) μεγέθους m bits. Το αναγνωριστικό του κόμβου και του κλειδιού προκύπτει εφαρμόζοντας τη συνάρτηση πάνω στην IP διεύθυνση του κόμβου και στο κλειδί αντίστοιχα. Τα αναγνωριστικά ταξινομούνται σε έναν κύκλο με 2^m στοιχεία, όπως φαίνεται στο Σχήμα 2.9 που αποτελεί παράδειγμα ενός CHORD δικτύου με τρεις κόμβους, τον μηδέν(0), ένα(1) και τρία(3). Ένα κλειδί αποθηκεύεται στον πρώτο κόμβο που το αναγνωριστικό του είναι ίσο με αυτό του κλειδιού ή στον επόμενο κόμβο πάνω στον κύκλο. Αυτός ο κόμβος ονομάζεται "successor" του κλειδιού.

Έτσι στο Σχήμα 2.9 ο "successor" του κλειδιού1 είναι ο κόμβος ένα(1), του κλειδιού2 ο κόμβος τρία(3) και του κλειδιού6 ο μηδέν(0). Όταν ένας κόμβος εισέρχεται στο δίκτυο μοιράζεται κάποια από τα κλειδιά που κατείχε ο "successor" του, ενώ όταν το εγκαταλείπει δίνει όλα τα κλειδιά στο "successor" του. Κάθε κόμβος εκτός από τη γνώση που έχει για τον "successor" του πάνω στον κύκλο διατηρεί και έναν πίνακα δρομολόγησης με m εγγραφές το πολύ, καθεμιά από τις οποίες περιλαμβάνει το αναγνωριστικό και την IP διεύθυνση ενός κόμβου s. Ο κόμβος της i^{th} εγγραφής είναι ο πρώτος για τον οποίο ισχύει η σχέση: $s=successor(n+2^{i-1})$ όπου $1 \leq i \leq m$ και n ο αριθμός κόμβων.



Σχήμα 2.9: Παράδειγμα δικτύου CHORD[13]

Η δρομολόγηση σε ένα τέτοιο δίκτυο επιτυγχάνεται λαμβάνοντας υπόψη τον πίνακα δρομολόγησης. Ένας κόμβος n που θέλει να ανακτήσει κάποιο δεδομένο πρέπει να βρει τον κόμβο που το κατέχει. Η ιδέα είναι να βρεθεί το id του προηγούμενου κόμβου (predecessor) από αυτόν που κατέχει το ζητούμενο δεδομένο. Από εκεί με ένα βήμα φτάνει στον προορισμό. Αν ο n είναι ο "predecessor" του ζητούμενου κόμβου τότε η διαδικασία τελείωσε. Αν όχι τότε ο κόμβος n με βάση τον

[13] Ν Κρεμμύδας, "Επισκόπηση στα Συστήματα Ομότιμων Κόμβων", Ε.Μ.Π., 2005.

πίνακα που διατηρεί, με πληροφορίες για κάποιους κόμβους, βρίσκει τον κοντινότερο κόμβο στον "predecessor". Η διαδικασία αυτή επαναλαμβάνεται μέχρι να βρεθεί ο ζητούμενος κόμβος.

2.3.2.2.1 Εισαγωγή κόμβου στο CHORD

Για να είναι εφικτός, κάθε στιγμή, ο εντοπισμός ενός κλειδιού μέσα στο δίκτυο, πρέπει να τηρούνται οι εξής δύο προϋποθέσεις: κάθε κόμβος να κρατάει σωστά τον successor του και υπεύθυνος για ένα κλειδί k να είναι ο successor του k. Επιπλέον, για να γίνονται γρήγορα οι αναζητήσεις, θα πρέπει τα finger tables των κόμβων να είναι πάντα σωστά ενημερωμένα. Έτσι, κατά την εισαγωγή ενός κόμβου στο σύστημα θα πρέπει να διατηρούνται οι παραπάνω προϋποθέσεις. Για την διευκόλυνση της εισαγωγής, οι κόμβοι κρατάνε επίσης και ένα δείκτη στον *predecessor* τους, στον κόμβο δηλαδή, που είναι ο αμέσως προηγούμενος τους στον κύκλο. Η διαδικασία της εισαγωγής έχει ως εξής: αρχικά ο κόμβος που πρόκειται να εισαχθεί, εντοπίζει έναν κόμβο που βρίσκεται ήδη στο σύστημα και αυτός αναλαμβάνει να βρει τον predecessor και τους fingers του νέου κόμβου. Στη συνέχεια, ενημερώνονται οι fingers των υπαρχόντων κόμβων, αφού ο νέος κόμβος πρέπει να προστεθεί στα finger tables κάποιων από αυτών και τέλος, μεταφέρονται στο νέο κόμβο τα αρχεία με κλειδιά για τα οποία θα είναι πλέον υπεύθυνος αυτός.

2.3.2.2.2 Ταυτόχρονες εισαγωγές και αποτυχίες κόμβων

Όπως αναφέρθηκε στην προηγούμενη ενότητα, για να εξασφαλιστεί η ορθότητα των αναζητήσεων, θα πρέπει οι successors των κόμβων να είναι σωστά ενημερωμένοι. Για το λόγο, αυτό το CHORD, τρέχει περιοδικά ένα πρωτόκολλο *σταθεροποίησης* (stabilization protocol), το οποίο ανανεώνει τους successors και τα finger tables των κόμβων. Στην περίπτωση τώρα αποτυχιών κάποιων κόμβων, είναι πιθανό, ένας κόμβος να μη γνωρίζει το νέο του successor. Για να αποφευχθεί αυτή η κατάσταση, κάθε κόμβος εκτός από την πληροφορία για το ποιος είναι ο successor του, διατηρεί και μία λίστα με τους r κόμβους που έπονται του successor του, όπου r

μία παράμετρος του συστήματος.. Έτσι, όταν ο successor ενός κόμβου δεν ανταποκρίνεται, ο κόμβος επικοινωνεί με τον επόμενο successor στη λίστα του.

2.3.2.3 Διαφορές CAN-CHORD

Το CAN και το CHORD αποτελούν δύο αρχιτεκτονικές δομημένων *peer-to-peer* συστημάτων, που βασίζονται στη χρήση κατανεμημένου πίνακα κατακερματισμού. Ο πίνακας 2 συνοψίζει τα χαρακτηριστικά των δύο αρχιτεκτονικών, που παρουσιάστηκαν σε αυτή την ενότητα. Όπως μπορούμε να παρατηρήσουμε, το CAN υπερέχει σημαντικά σε δύο χαρακτηριστικά. Η πληροφορία που διατηρεί κάθε κόμβος είναι ανεξάρτητη από τον συνολικό αριθμό των κόμβων στο σύστημα και είναι της τάξης του 2d, όπου d ο αριθμός των διαστάσεων, ενώ στο CHORD κάθε κόμβος διατηρεί πληροφορία για logN κόμβους, όπου N το πλήθος των κόμβων. Επιπλέον, στο CAN η εισαγωγή ή αποχώρηση ενός κόμβου απαιτεί μόλις 2d μηνύματα για την διατήρηση της δομής, ενώ στο CHORD $(logN)^2$.

	Αρχιτεκτονική	**Πρωτόκολλο αναζήτησης**	**Παράμετροι συστήματος**	**Δρομολόγηση**	**Πληροφορία δρομολόγησης**	**Εισαγωγή/ αποχώρηση κόμβων**
CAN	Εικονικός πολύ-διάστατος χώρος συντεταγμένων	Απεικόνιση ζεύγους (κλειδί, τιμή) σε σημείο του χώρου	N: αριθμός κόμβων στο δίκτυο d: αριθμός διαστάσεων	$O(dN^{1/d})$	2d	2d
CHORD	Εικονικός χώρος αναγνωριστικών οργανωμένος σε δακτύλιο	Απεικόνιση κλειδιού σε κόμβο του δακτυλίου	N: αριθμός κόμβων στο δίκτυο	O(logN)	logN	$(logN)^2$

Πίνακας 2: Χαρακτηριστικά των CAN και CHORD

Κεφάλαιο 3ο

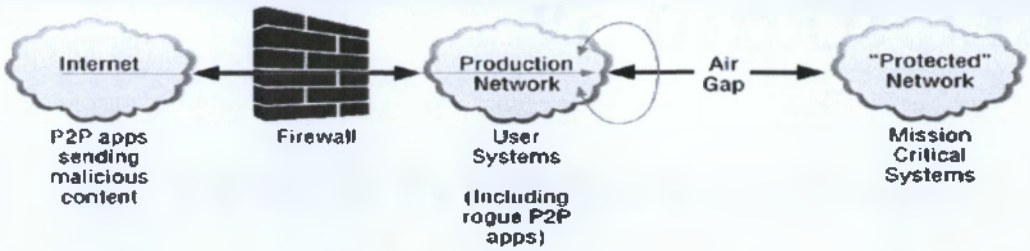
3 Ζητήματα Ασφάλειας P2P δικτύων

Η ασφάλεια είναι ένα ουσιαστικό συστατικό οποιουδήποτε συστήματος ηλεκτρονικών υπολογιστών, και είναι απαραίτητη για τα P2P συστήματα. Στα εξής τμήματα θα περιγράψουμε τα κύρια ζητήματα P2P ασφάλειας.

3.1 Ανάγκη για την ασφάλεια

Σε αυτούς τους ταραχώδεις καιρούς θα πίστευε κανείς ότι τα P2P ζητήματα ασφάλειας θα είναι το μικρότερο από τα προβλήματά του κόσμου. Εντούτοις οι εταιρικές απάτες και η απώλεια εισοδήματος λόγω των επιθέσεων στα εσωτερικά δίκτυά τους έχουν φέρει στην πρώτη γραμμή στον κόσμο της πληροφορικής παγκοσμίως. Το Napster όπως αναφέραμε ήταν το πρώτο P2P δίκτυο και παρόλο που προκάλεσε πολλές δικαστικές αποφάσεις όλο και περισσοτερες εφόρμαγες δημιουργήθηκαν μετά από αυτό, με αποτέλεσμα να προκαλέσουν εταιρικούς παγκόσμιους πονοκεφάλους. Όμως με τα καλύτερα πρωτόκολλα ασφάλειας αυτός ο πονοκέφαλος θα μπορούσε να μετατραπεί σε πολύτιμο προτέρημα για τον εταιρικό κόσμο και για τον κόσμο γενικά.

Το παρακάτω διάγραμμα επεξηγεί τα χάσματα στην ασφάλεια κατά χρησιμοποίηση των P2P εφαρμογών. Μπορούμε να δούμε ότι αφήνουμε αυτές τις εφαρμογές να μπουν μέσα στα δίκτυά μας. Η ασφάλεια του «ασφαλούς» δικτύου μας είναι τώρα στη διακινδύνευση.



14

Εξαιτίας αυτού, εμείς είμαστε αυτοί που θα πρέπει να προστατέψουμε τον εαυτό μας. Πρέπει να περιγράψουμε τα στοιχεία που είναι σημαντικά για εμάς να χρησιμοποιήσουμε, προτού αντιμετωπίσουμε το ζήτημα της ασφάλειας. Τα κύρια σημεία είναι ο έλεγχος σύνδεσης, έλεγχος προσπέλασης, έλεγχος λειτουργίας και φυσικά η προστασία των στοιχείων που αποθηκεύονται στις μηχανές μας.

Η σύνδεση, η πρόσβαση, και ο έλεγχος λειτουργίας είναι τα ζητήματα προτεραιότητας εδώ. Εάν μπορούμε να καταστήσουμε αυτά ασφαλή, τα άλλα δύο σημεία προκύπτουν από αυτά.

3.2 Συνέπειες της κακής Ασφαλείας

Η P2P δικτύωση επιτρέπει στο δίκτυό να είναι ανοικτό στις διάφορες μορφές επίθεσης, διάρρηξης, κατασκοπείας, και κακόβουλης αναστάτωσης, δεν φέρνει νέες απειλές στο δίκτυο, αλλά γνωστές απειλές όπως τα σκουλήκια και οι επιθέσεις ιών.

Τα P2P δίκτυα μπορούν επίσης να επιτρέψουν σε έναν υπάλληλο να μεταφορτώσουν και να χρησιμοποιήσουν το υλικό με τέτοιο τρόπο που παραβιάζει τους νόμους πνευματικής ιδιοκτησίας, και να μοιραστούν τα αρχεία με έναν τρόπο που παραβιάζει τις πολιτικές ασφαλείας οργανώσεων. Οι εφαρμογές όπως Napster, Kazaa, Grokster και άλλες είναι αρκετά δημοφιλείς στους χρήστες του internet, λόγω ότι οι χρήστες μπορούν να μεταφέρουν μεταξύ τους μουσική αλλα και αλλα αρχεία.

Έτσι πολλοί χρήστες εκμεταλλεύονται τους εργοδότες τους που έχουν μεγάλες συνδέσεις για να μεταφορτώνουν αρχεία στην εργασία. Αυτό παρουσιάζει τα

[14] "P2P Ασφαλεία", http://ntrg.cs.tcd.ie/undergrad/4ba2.02-03/p10.html

πολυάριθμα προβλήματα για το εταιρικό δίκτυο όπως η χρησιμοποίηση του ακριβού εύρους ζώνης και την προσβολή από ιούς, μια επίθεση μέσω ενός μολυσμένου αρχείου μεταφορτωμένου.

Κλοπή:

Το πρόβλημα με τα P2P δίκτυα κοινής χρήσης αρχείων είναι ότι αθελά μας μπορούμε να μοιραστούμε πάρα πολύ περισσότερο από ό, τι νομίζουμε ότι μοιραζόμαστε.

Με το ανέβασμα και το κατέβασμα υλικού που προστατεύεται από πνευματικά δικαιώματα σε δίκτυα P2Pδεν παραβιάζετε μόνο ο νόμος, αλλα και εκθέτουμε ενδεχομένως τον υπολογιστή ,προσωπικές πληροφορίες αλλα και άλλες ευαίσθητες πληροφορίες, όπως τα τραπεζικά στοιχεία και αριθμούς κοινωνικής ασφάλισης. Με αποτέλεσμα σημαντικές πληροφορίες να έχουν εκτεθεί σε μη εξουσιοδοτημένα άτομα. Επίσης η διαθεσιμότητα αυτών των πληροφοριών μπορεί να αυξήσει και τον κίνδυνο της κλοπής ταυτότητας.

Trojans, ιοί, worms :

Ένας χρήστης θα μπορούσε να μεταφορτώσει και να εγκαταστήσει μια παγιδευμένη P2P εφαρμογή που θα μπορούσε να επιβάλει σοβαρή ζημιά, να θέσει εκτός λειτουργίας έναν υπολογιστή, για να εξαλείψει ή να τροποποιήσει δεδομένα. Εάν ένας τέτοιος υπολογιστής που έχει προσβληθεί είναι μέρος του δικτύου διαχείρισης, μπορεί η δυσλειτουργία του να έχει εκτεταμένες επιπτώσεις. Ο ιός είναι μια μορφή κακόβουλου λογισμικού. Πρόκειται για ένα πρόγραμμα που αναπαράγει τον κώδικά του προσκολλώμενο σε άλλα προγράμματα, με τρόπο ώστε ο κώδικας του ιού να εκτελείται κατά την εκτέλεση προγράμματος του υπολογιστή που έχει προσβληθεί. Υπάρχουν πολλοί άλλοι τύποι κακόβουλου λογισμικού: ορισμένοι βλάπτουν μόνο τον υπολογιστή όπου έχουν αντιγραφεί, ενώ άλλοι μεταδίδονται σε άλλα δικτυωμένα προγράμματα. Υπάρχουν λ.χ. προγράμματα (με την ονομασία "λογικές βόμβες") που παραμένουν αδρανή μέχρι την ενεργοποίησή τους από κάποιο γεγονός, όπως μια συγκεκριμένη ημερομηνία, π.χ. Τρίτη και 13. Άλλα προγράμματα εμφανίζονται ως καλοήθη, όταν όμως ανοίγουν εκδηλώνουν κακόβουλη επίθεση (για το λόγο αυτό αποκαλούνται "Δούρειοι Ίπποι" - Trojans). Άλλα προγράμματα

(ονομαζόμενα "σκουλήκια" - worms) δεν προσβάλλουν άλλα προγράμματα όπως ο ιός, αλλά δημιουργούν αντίγραφά τους, τα οποία με τη σειρά τους αναπαράγονται, κατακλύζοντας τελικά ολόκληρο το σύστημα.

Απόφραξη εύρους ζώνης και ο διαμοιρασμός αρχείων:

Οι P2P εφαρμογές όπως Kazaa,Gnutella και FreeNet επιτρέπουν σε έναν υπολογιστή να μοιράζετε αρχεία με έναν άλλο υπολογιστή που βρίσκεται κάπου αλλού στο διαδίκτυο. Ένα σοβαρό πρόβλημα που προκύπτει λόγο αυτής της λειτουργιάς τους είναι ότι οδηγούν στη βαριά κυκλοφορία, η οποία φράζει το δίκτυο. Τα πλούσια ακουστικά και τηλεοπτικά αρχεία που οι P2Pχρήστες μοιράζονται είναι πολύ μεγάλα. Με αποτέλεσμα αυτό να οδηγεί σε άσκοπη καθυστέρηση δικτύου εις βάρος άλλων εργαζόμενων-χρηστών. καθώς επίσης και για τους πελάτες ηλεκτρονικού εμπορίου. Κατασπατάληση εύρους (bandwidth).

Bugs:

Software bug είναι ένα λάθος, σφάλμα, αποτυχία, ή ελάττωμα σε ένα πρόγραμμα λογισμικού που το οδηγεί σε ανεπιθύμητη συμπεριφορά. Τα περισσότερα bugs προέρχονται από ανθρώπινα λάθη ή σφάλματα που γίνονται είτε στον πηγαίο κώδικα είτε στον σχεδιασμό/αρχιτεκτονική του προγράμματος, και μερικά προέρχονται από την εσφαλμένη παραγωγή κώδικα από έναν μεταγλωττιστή. Γεια να λειτουργήσει μια P2P εφαρμογή κοινής χρήσης αρχείων θα πρέπει το κατάλληλο λογισμικό να εγκατασταθεί στο σύστημα των χρηστών. Εάν αυτό το λογισμικό περιέχει ένα bug,τότε θα μπορούσε να εκθέσει το δίκτυο σε έναν αριθμό κινδύνων, με διάφορα επίπεδα δυσχέρειας προς τον χρήστη του προγράμματος. Μερικά bugs έχουν μόνο μια λεπτή επίδραση στην λειτουργικότητα του προγράμματος, και μπορούν έτσι να παραμείνουν μη ανιχνευμένα για πολύ καιρό. Μερικά άλλα όμως έχουν πιο σοβαρές επιπτώσεις όπως σύγκρουση με τις επιχειρησιακές εφαρμογές ή ακόμα και κατάρρευση του συστήματος.

Πρόσβαση Backdoor:

Είναι κομμάτια κώδικα που γράφονται μέσα σε εφαρμογές ή λειτουργικά συστήματα έτσι ώστε να δώσουν στους προγραμματιστές πρόσβαση σε προγράμματα

χωρίς να χρειάζεται αυτοί να περάσουν από τις συνήθεις, χρονοβόρες διαδικασίες ασφάλειας της πρόσβασης. Στην ουσία είναι "τρύπες" ασφάλειας που δημιουργούνται εσκεμμένα. Τυπικά γράφονται από προγραμματιστές εφαρμογών που χρειάζονται κάποιο μέσο εξφαλμάτωσης ή ελέγχου του κώδικα που αναπτύσσουν. Αρκετά συχνά αποτελούν τροποποίηση νόμιμου λογισμικού με κακόβουλο σκοπό.

Οι P2P εφαρμογές όπως KazaA, Morpheus ή Gnutella επιτρέπουν στους ανθρώπους όλου του κόσμου να μοιράζονται μεταξύ τους εφαρμογές μουσικής, βίντεο και λογισμικού. Αυτές οι εφαρμογές εκθέτουν τα στοιχεία όσον αφορά τον υπολογιστή του χρήστη σε χιλιάδες ανθρώπους στο διαδίκτυο. Αυτές οι P2Pεφαρμογές δεν σχεδιάστηκαν για τη χρήση στα εταιρικά δίκτυα και κατά συνέπεια εισάγουν σοβαρές αδυναμίες στην ασφάλεια του εταιρικού δικτύου, εάν εγκατασταθεί στα δικτυωμένα PC. Παραδείγματος χάριν εάν ένας χρήστης ξεκινήσει το Gnutella και στη συνέχεια κάνει κλικ στο εταιρικό Intranet να ελέγξει το email, ένας εισβολέας θα μπορούσε να χρησιμοποιήσει αυτό ως backdoor για να αποκτήσουν πρόσβαση στο εταιρικό δίκτυο LAN.

Μη- Κρυπτογραφημένο ΙΜ:

Οι στιγμιαίες εφαρμογές μηνύματος όπως εκείνους που παρέχονται από τη AOL, τη Microsoft και το Yahoo, αποτελούν επίσης απειλή πληροφοριών για μια επιχείρηση. Πολλοί χρήστες χρησιμοποιούν αυτές τις εφαρμογές προκειμένου να επικοινωνήσουν με φίλους, να στείλουν ή να δεχθούν αρχεία, μηνύματα, καθώς αυτές οι εφαρμογές προσπαθούν να ξεγελάσουν τα προγράμματα που φιλτράρουν τις πληροφορίες που εισέρχονται και εξέρχονται από ένα δίκτυο, ώστε να περάσουν και δεδομένα που μπορεί να περιέχουν κακόβουλο λογισμικό. Ωστόσο οι χρήστες δεν συνειδητοποιούν τους κινδύνους που κρύβουν αυτές οι εφαρμογές και την πιθανή καταστροφή που μπορεί να επιφέρουν. Ποτέ δεν μπορούμε να είμαστε σίγουροι για το ποιος είναι στο άλλο άκρο της γραμμής. Μπορεί πράγματι να είναι κάποιος φίλος μας ή ένας κακόβουλος χρήστης. Οι περισσότερες από αυτές τις εφαρμογές περιέχουν τρωτά σημεία, η εκμετάλλευση των οποίων από γνώστες του είδους θα μπορούσε να δημιουργήσει σοβαρά προβλήματα. Ένα αρχείο που θα πάρουμε μπορεί να είναι μολυσμένο και να οδηγήσει με η σειρά του στη μόλυνση του συστήματος και του δικτύου γενικότερα. Λόγω της εύκολης επικοινωνίας, είναι επίσης δυνατό για

τους μη-πιστούς υπαλλήλους να συνομιλούν στους ανταγωνιστές και να αποκαλύπτουν ευαίσθητα μυστικά της επιχείρησής. Επίσης εάν αυτές οι εφαρμογές χρησιμοποιούνται για να συζητήσουν την ευαίσθητη πληροφορία, ένας επιτιθέμενος μπορεί να διαβάσει όλα τα μηνύματα που στέλνονται πέρα δώθε μέσω το δίκτυο ή το Διαδίκτυο με τη χρησιμοποίηση ενός προγράμματος διαμοιρασμού αρχείων.

Εμπιστευτικότητα:

Το Kazaa και Gnutella δίνουν σε όλους τους πελάτες την άμεση πρόσβαση στα αρχεία που αποθηκεύονται στο σκληρό δίσκο ενός χρήστη. Κατά συνέπεια είναι δυνατό για έναν χάκερ να αποκτήσει πρόσβαση στους φακέλους και τις πληροφορίες που είναι εμπιστευτικές. Η εμπιστευτικότητα σημαίνει πρόληψη μη εξουσιοδοτημένης αποκάλυψης πληροφοριών, δηλαδή, πρόληψη από μη εξουσιοδοτημένη ανάγνωση. Επομένως, σημαίνει ότι τα δεδομένα που διακινούνται μεταξύ των υπολογιστών ενός δικτύου, αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Αυτό αφορά όχι μόνο την προστασία από μη εξουσιοδοτημένη αποκάλυψη των δεδομένων αυτών καθαυτών αλλά ακόμη και από το γεγονός ότι τα δεδομένα απλώς υπάρχουν. Έτσι για παράδειγμα, το γεγονός ότι κανείς έχει φάκελο εγκληματία είναι συχνά το ίδιο σημαντικό όπως και οι λεπτομέρειες για το έγκλημα που διαπράχθηκε.

Αυθεντικότητα:

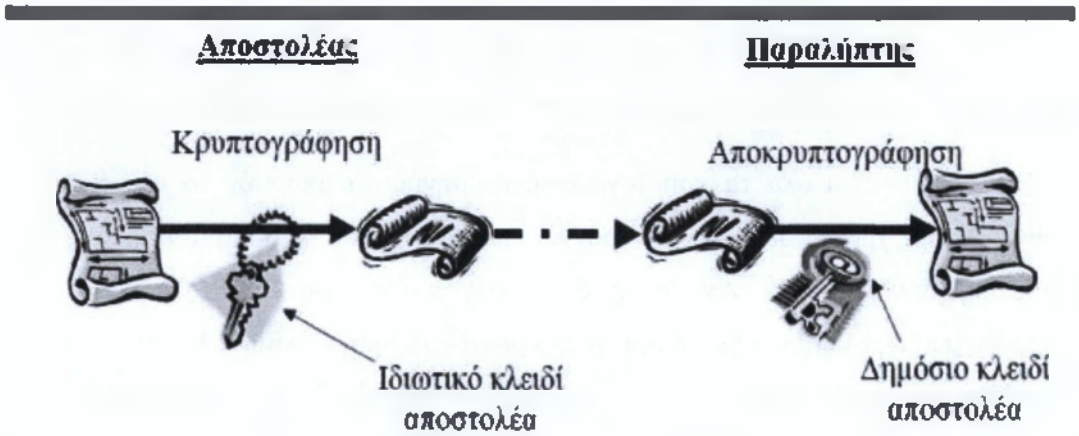
Υπάρχει επίσης το ζήτημα της αυθεντικότητας. Όταν χρησιμοποιούνται τα P2Pθα πρέπει εξασφαλίζετε ότι η πρόσβαση σε πληροφορίες από ομότιμους είναι αυτοί που πραγματικά λένε ότι είναι και ότι έχουν πρόσβαση μόνο στις εξουσιοδοτημένες πληροφορίες. Αφορά στην εξασφάλιση ότι τα δεδομένα είναι απαλλαγμένα από ατέλειες και ανακρίβειες κατά τις εξουσιοδοτημένες τροποποιήσεις. Η αυθεντικότητα και η ακεραιότητα των στοιχείων μπορεί να εγγυηθεί μόνο μέσω της χρήσης των απαραίτητων διαδικασιών οι οποίες θα έχουν συμφωνηθεί ανάμεσα στους ενδιαφερόμενους οργανισμούς.

3.3 Υφιστάμενα πρότυπα ασφαλείας σε δίκτυα P2P

Όλοι οι μηχανισμοί ασφαλείας έχουν αναπτυχθεί σήμερα, με βάση είτε συμμετρική / μυστικού κλειδιού ή ασύμμετρη / κρυπτογραφία δημόσιου κλειδιού, ή μερικές φορές έναν συνδυασμό των δύο. Εδώ θα παρουσιάσουμε τις βασικές πτυχές τους και τα κύρια χαρακτηριστικά τους.

3.3.1 Κρυπτογραφία μυστικού Κλειδιού (Secret-Key Cryptography)

Στην κρυπτογράφηση μυστικού κλειδιού, το κλειδί χρησιμοποιείται για κωδικοποίηση και αποκωδικοποίηση του μηνύματος, οπότε λέγεται ότι είναι συμμετρική - επειδή και τα δύο, κλειδιά είναι ίδια. Η κρυπτογράφηση μυστικού κλειδιού, απαιτεί και τα δύο μέρη να γνωρίζουν τον αλγόριθμο και το κλειδί για να αποκωδικοποιήσουν το μήνυμα. Μέχρι την ανάπτυξη της κρυπτογράφησης δημοσίου κλειδιού από τους κρυπτογράφους, κατά την δεκαετία του 70, η κρυπτογράφηση μυστικού κλειδιού ήταν ο μόνος διαθέσιμος τύπος κρυπτογράφησης.



Σχήμα 3.1: Η διαδικασία κρυπτογράφησης συμμετρικού κλειδιού.[15]

Η κρυπτογράφηση μυστικού κλειδιού λειτουργεί καλά για να κρατά μυστικά, αλλά και τα δύο μέρη πρέπει να γνωρίζουν το ίδιο μυστικό κλειδί για να αποκωδικοποιήσουν το μήνυμα. Δεν υπάρχει ασφαλής τρόπος μεταφοράς του

[15] Μάρκος Σελλής, "Ασφάλεια Ιατρικών Εγγράφων XML Με Την Χρήση Ψηφιακής Υπογραφής" ΕΜΠ

κλειδιού από το ένα μέρος στο άλλο, χωρίς να προηγηθεί κάποια επίπονη διαδικασία, π.χ. και τα δύο μέρη να συναντηθούν στην ίδια συμφωνημένη περιοχή, ώστε να ανταλλάξουν κλειδιά. Σίγουρα δεν υπάρχει τρόπος ανταλλαγής κλειδιών μέσω ενός ηλεκτρονικού μέσου, χωρίς να υπάρχει η πιθανότητα ένας υποκλοπέας να τα υποκλέψει.

Για να αποφεύγονται οι αποκαλούμενες επιθέσεις εκτενών αναζητήσεων πρέπει το πλήθος των πιθανών διαφορετικών συνδυασμών κλειδιών για έναν κρυπτογραφικό αλγόριθμο να είναι μεγάλο, καθώς σε περίπτωση που ο κρυπταναλυτής αποκτήσει ένα αντίστοιχο ζεύγος αρχικού και κρυπτογραφημένου κειμένου μπορεί προσπαθώντας με όλα τα πιθανά κλειδιά να βρει ποιο ταιριάζει και να το χρησιμοποιήσει κατόπιν για να αποκρυπτογραφεί άλλα κρυπτογραφημένα κείμενα που έχουν κρυπτογραφηθεί με το ίδιο κλειδί. Διαφορετικά, σε περίπτωση που απλά κατάφερε να υποκλέψει ένα κρυπτογραφημένο κείμενο, μπορεί να το αποκρυπτογραφήσει με διάφορους συνδυασμούς κλειδιών μέχρι να βρει ένα αρχικό κείμενο που έχει σημασία, δηλαδή λογική, οπότε τότε αποκτά στην ουσία και το σωστό κλειδί ή κάτι πολύ κοντά σε αυτό και στη συνέχεια μπορεί να το χρησιμοποιήσει για την αποκρυπτογράφηση επόμενων κρυπτογραφημένων κειμένων.

Έχει ειπωθεί ότι όλα τα κρυπτογραφημένα μηνύματα μπορούν να σπάσουν, αν δοθεί αρκετός χρόνος σε έναν ηλεκτρονικό υπολογιστή που θα δοκιμάσει όλους τους πιθανούς συνδυασμούς. Αν όμως ο χρόνος αυτός είναι τόσο μεγάλος (για παράδειγμα, 1.014 χρόνια για συμμετρική κρυπτογράφηση με κλειδί 128-bit), τότε το 'σπάσιμο' του κρυπτογραφημένου μηνύματος θα έχει πιθανότατα ελάχιστη σημασία. Όσο οι ηλεκτρονικοί υπολογιστές γίνονται ισχυρότεροι και ταχύτεροι, τόσο τα κλειδιά γίνονται μεγαλύτερα και οι αλγόριθμοι κρυπτογράφησης πολυπλοκότεροι.

Τυπικά, τα κλειδιά είναι σειρές από bits και ως εκ τούτου η απαίτηση για μεγάλο πλήθος κλειδιών έχει την έννοια της χρησιμοποίησης πολλών bits, δηλαδή περισσότερα από κάποιο κάτω όριο. Η χρησιμοποίηση 64 bits αποτελεί ένα τυπικό μήκος κλειδιού το οποίο παρέχει $264 \approx 1019$ διαφορετικά κλειδιά. Οπότε, αν μπορούσαμε να δοκιμάζουμε όλους τους πιθανούς συνδυασμούς κλειδιών με ρυθμό ένα κλειδί κάθε δισεκατομμυριοστό του δευτερολέπτου, δηλαδή να δοκιμάζουμε

1.000.000.000 κλειδιά ανά δευτερόλεπτο, τότε θα χρειαζόμασταν περίπου 300 χρόνια για να δοκιμάσουμε όλους τους πιθανούς συνδυασμούς κλειδιών.

3.3.2 Κρυπτογραφία Δημόσιου Κλειδιού (Public Key Cryptography)

Η κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιεί ένα κλειδί για κρυπτογράφηση ενός μηνύματος και ένα διαφορετικό κλειδί για την αποκρυπτογράφησή του, οπότε καλούνται ασύμμετροι αλγόριθμοι. Σε ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού, το κλειδί κρυπτογράφησης καλείται δημόσιο κλειδί, επειδή μπορεί να ανακοινωθεί δημόσια. Το κλειδί αποκρυπτογράφησης καλείται ιδιωτικό κλειδί, επειδή πρέπει να κρατηθεί ιδιωτικό, για να παραμείνει ασφαλές.

Σχήμα 3.2: Η διαδικασία κρυπτογράφησης δημόσιου κλειδιού.[16]

Το πρόβλημα με την κρυπτογράφηση μυστικού κλειδιού είναι το εξής: Ο αποστολέας και ο παραλήπτης πρέπει να έχουν το ίδιο κλειδί για να ανταλλάξουν κρυπτογραφημένα μηνύματα επάνω σε ένα ανασφαλές μέσο. Αν δύο μέρη αποφασίσουν να ανταλλάξουν ιδιωτικά μηνύματα ή αν οι συσκευές δικτύου ή τα προγράμματα δύο υπολογιστών πρέπει να καθορίσουν ένα ασφαλές κανάλι, τα δύο μέρη πρέπει να αποφασίσουν για ένα κοινό κλειδί. Καθένα από τα δύο μέρη μπορεί να αποφασίσει απλώς για ένα κλειδί, αλλά αυτό το μέρος δεν θα έχει κάποιο τρόπο να το στείλει στο άλλο μέρος, χωρίς τον κίνδυνο να υποκλαπεί καθ' οδών.

16 Μάρκος Σελλής, "Ασφάλεια Ιατρικών Εγγράφων XML Με Την Χρήση Ψηφιακής Υπογραφής". ΕΜΠ

Με την κρυπτογράφηση δημόσιου κλειδιού, ο παραλήπτης μπορεί να στείλει ένα δημόσιο κλειδί κρυπτογράφησης στον αποστολέα. Δεν υπάρχει ανάγκη το δημόσιο κλειδί να κρατηθεί μυστικό, επειδή μπορεί να χρησιμοποιηθεί μόνο για κρυπτογράφηση μηνυμάτων και όχι για αποκρυπτογράφησή τους. Όταν ο παραλήπτης λάβει ένα μήνυμα που έχει κωδικοποιηθεί με το δημόσιο κλειδί του, μπορεί να χρησιμοποιήσει το ιδιωτικό του κλειδί για να αποκωδικοποιήσει το μήνυμα. Η αποκάλυψη του δημόσιου κλειδιού για κωδικοποίηση δεν επιτρέπει σε κανέναν άλλο να αποκωδικοποιήσει τα ιδιωτικά του μηνύματα. Η κρυπτογραφία δημόσιου κλειδιού είναι μια νέα σχετικά εξέλιξη στην κρυπτογραφία, που επιλύει πολλά μακροχρόνια προβλήματα που έχουν σχέση με τα κρυπτογραφικά συστήματα - ειδικά το πρόβλημα που σχετίζεται με την ανταλλαγή μυστικών κλειδιών.

Το 1976, οι Witfield Diffe και Martin Hellman βρήκαν ένα τρόπο για να επιλύσουν το πρόβλημα του ασφαλούς καναλιού. Βρήκαν ότι ορισμένες μονόδρομες συναρτήσεις μπορούν να αναιρεθούν χρησιμοποιώντας ένα διαφορετικό κλειδί για αποκρυπτογράφηση, από αυτό που χρησιμοποιείται για κρυπτογράφηση. Η λύση τους, που ονομάστηκε κρυπτογραφία δημόσιου κλειδιού, εκμεταλλεύεται ένα χαρακτηριστικό των πρώτων και των σχεδόν πρώτων αριθμών, συγκεκριμένα, το πόσο δύσκολο είναι να βρείτε δύο παράγοντες ενός μεγάλου αριθμού που έχει δύο μόνο παράγοντες, όπου και οι δύο είναι πρώτοι. Από την ώρα που οι Diffie και Hellman ανέπτυξαν το σύστημά τους, έχουν εισαχθεί και μερικοί άλλοι κρυπτοθετήρες δημόσιου κλειδιού, που χρησιμοποιούν ακόμη πιο δύσκολες μονόδρομες συναρτήσεις.

3.3.3 Υβριδική Κρυπτογραφία Ψηφιακού Φακέλου

Αν και είναι πολύ βραδύτερο από τα συμμετρικά συστήματα, το σύστημα δημόσιου κλειδιού/ιδιωτικού κλειδιού επιλύει έξυπνα το πρόβλημα που ταλανίζει τα συμμετρικά κρυπτοσυστήματα - την ανταλλαγή μυστικών κλειδιών.

Δεν υπάρχει όμως ανάγκη να χάσουμε την ταχύτητα των κρυπτοσυστημάτων μυστικού κλειδιού, απλώς επειδή τα μυστικά κλειδιά δεν μπορούν να ανταλλαγούν με ασφάλεια. Τα υβριδικά κρυπτοσυστήματα χρησιμοποιούν κρυπτογράφηση δημόσιου

κλειδιού για να ανταλλάσσουν μυστικά κλειδιά και μετά χρησιμοποιούν τα μυστικά κλειδιά για να καθορίσουν ένα κανάλι επικοινωνίας. Σχεδόν όλα τα σύγχρονα κρυπτοσυστήματα λειτουργούν με αυτόν τον τρόπο.

Όταν δύο άνθρωποι ή συσκευές πρέπει να καθορίσουν ένα ασφαλές κανάλι για επικοινωνία, ο ένας τους πρέπει να παράγει ένα τυχαίο μυστικό κλειδί και μετά να κρυπτογραφήσει το μυστικό κλειδί χρησιμοποιώντας το δημόσιο κλειδί του παραλήπτη. Το κρυπτογραφημένο κλειδί στέλνεται κατόπιν στον παραλήπτη. Ακόμη και αν υποκλαπεί το κλειδί, μόνο ο πραγματικός παραλήπτης, χρησιμοποιώντας το δικό του ιδιωτικό κλειδί, μπορεί να αποκρυπτογραφήσει το μήνυμα που περιέχει το μυστικό κλειδί.

Όταν και τα δύο μέρη έχουν το μυστικό κλειδί, μπορούν να αρχίσουν να χρησιμοποιούν ένα ταχύτερο κρυπτοσύστημα μυστικού κλειδιού για να ανταλλάσσουν μυστικά μηνύματα.

3.4 Πρωτόκολλα

Ένα πρωτόκολλο είναι μια σειρά κανόνων που πρέπει να ακολουθηθούν για την εκτέλεση μιας δεδομένης εργασίας. Τα πρωτόκολλα ασφάλειας δεδομένων συχνά περιέχουν την χρήση κάποιων αλγορίθμων κρυπτογράφησης αλλά σε γενικές γραμμές αυτό που προσπαθούν να επιτύχουν δεν είναι μόνο η μυστικότητα αλλά και να παρέχουν όλες τις βασικές υπηρεσίες ασφαλείας.

3.4.1 Πρωτόκολλο SSL (Secure Sockets Layer)

Για την προστασία των πληροφοριών που μεταδίδονται μέσω P2P ορισμένα δίκτυα χρησιμοποιούν το βιομηχανικό πρότυπο Secure Sockets Layer (SSL). Αναπτύχθηκε από την εταιρεία Netscape και σχεδιάστηκε για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων στο διαδίκτυο. Η έκδοση 3.0 του πρωτοκόλλου κυκλοφόρησε από την Netscape το 1996 και αποτέλεσε την βάση για την μετέπειτα ανάπτυξη του πρωτοκόλλου TLS (Transport Layer Security), το οποίο

πλέον τείνει να αντικαταστήσει το SSL. Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται ευρέως για ηλεκτρονικές αγορές και χρηματικές συναλλαγές μέσω του διαδικτύου.

Το SSL χρησιμοποιεί μεθόδους κρυπτογράφησης των δεδομένων που ανταλλάσσονται μεταξύ δύο συσκευών (συνηθέστερα Ηλεκτρονικών Υπολογιστών) εγκαθιδρύοντας μία ασφαλή σύνδεση μεταξύ τους μέσω του διαδικτύου. Το πρωτόκολλο αυτό χρησιμοποιεί το TCP/IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιεί ο τελικός χρήστης. Για τον λόγο αυτό μπορεί να παρέχει υπηρεσίες ασφαλούς μετάδοσης πληροφοριών σε πρωτόκολλα ανώτερου επιπέδου όπως για παράδειγμα το HTTP, το FTP, το Telnet κοκ.

Η μετάδοση πληροφοριών μέσω του διαδικτύου γίνεται ως επί το πλείστον χρησιμοποιώντας τα πρωτόκολλα TCP/IP (Transfer Control Protocol / Internet Protocol). Το SSL λειτουργεί πριν το TCP/IP και μετά τις εφαρμογές υψηλού επιπέδου, όπως είναι για παράδειγμα το HTTP (προβολή ιστοσελίδων), το FTP (μεταφορά αρχείων) και το IMAP (e-mail). Άρα λοιπόν αυτό που ουσιαστικά κάνει το SSL είναι να παίρνει τις πληροφορίες από τις εφαρμογές υψηλότερων επιπέδων, να τις κρυπτογραφεί και στην συνέχεια να τις μεταδίδει στο Internet προς τον Η/Υ που βρίσκεται στην απέναντι πλευρά και τις ζήτησε.

Το SSL προσφέρει συνοπτικά τις ακόλουθες υπηρεσίες:

- Πιστοποίηση του server από τον client.
- Πιστοποίηση του client από τον server.
- Εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.

Οι κρυπτογραφικοί αλγόριθμοι που υποστηρίζονται από το πρωτόκολλο είναι οι εξής: DES - Data Encryption Standard, DSA - Digital Signature Algorithm, KEA - Key Exchange Algorithm, MD5 - Message Digest, RC2/RC4, RSA, SHA-1 - Secure Hash Algorithm, SKIPJACK, Triple-DES.

3.4.1.1 Λειτουργία του SSL

Το πρωτόκολλο SSL χρησιμοποιεί έναν συνδυασμό της κρυπτογράφησης δημοσίου και συμμετρικού κλειδιού. Η κρυπτογράφηση συμμετρικού κλειδιού είναι πολύ πιο γρήγορη και αποδοτική σε σχέση με την κρυπτογράφηση δημοσίου κλειδιού, παρόλα αυτά όμως η δεύτερη προσφέρει καλύτερες τεχνικές πιστοποίησης. Κάθε σύνδεση SSL ξεκινά πάντα με την ανταλλαγή μηνυμάτων από τον server και τον client έως ότου επιτευχθεί η ασφαλής σύνδεση, πράγμα που ονομάζεται χειραψία (handshake). Η χειραψία επιτρέπει στον server να αποδείξει την ταυτότητά του στον client χρησιμοποιώντας τεχνικές κρυπτογράφησης δημοσίου κλειδιού και στην συνέχεια επιτρέπει στον client και τον server να συνεργαστούν για την δημιουργία ενός συμμετρικού κλειδιού που θα χρησιμοποιηθεί στην γρήγορη κρυπτογράφηση και αποκρυπτογράφηση των δεδομένων που ανταλλάσσονται μεταξύ τους. Προαιρετικά η χειραψία επιτρέπει επίσης στον client να αποδείξει την ταυτότητά του στον server. Αναλυτικότερα, η διαδικασία χειραψίας έχει ως εξής:

- Αρχικά ο client στέλνει στον server την έκδοση του SSL που χρησιμοποιεί, τον επιθυμητό αλγόριθμο κρυπτογράφησης, μερικά δεδομένα που έχουν παραχθεί τυχαία και οποιαδήποτε άλλη πληροφορία χρειάζεται ο server για να ξεκινήσει μία σύνδεση SSL.

- Ο server απαντά στέλνοντας παρόμοιες πληροφορίες συμπεριλαμβανομένου όμως και του ψηφιακού πιστοποιητικού, το οποίο τον πιστοποιεί στον client. Προαιρετικά μπορεί να ζητήσει και το ψηφιακό πιστοποιητικό του client.

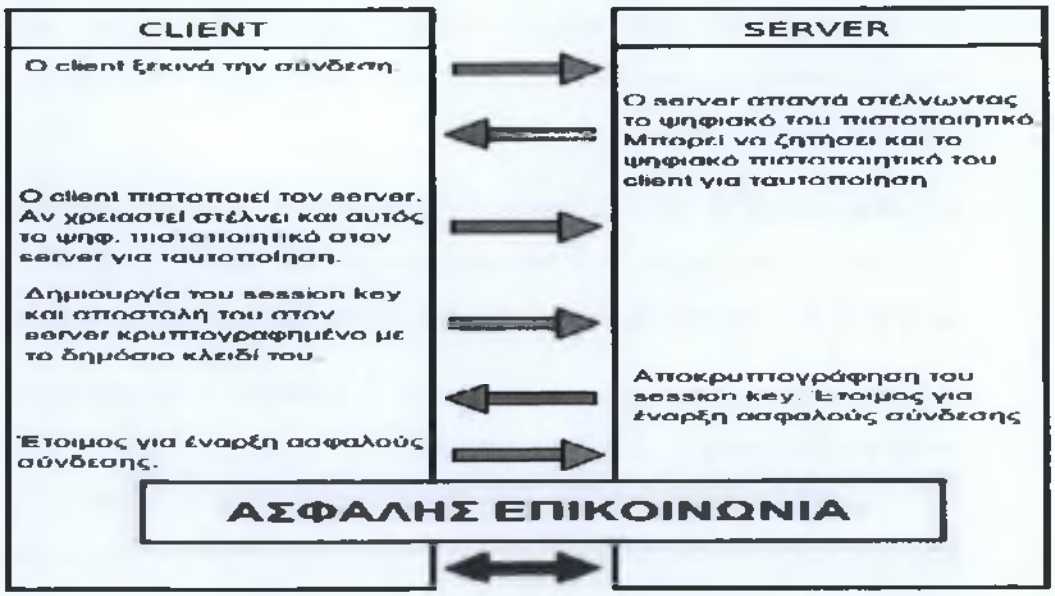
- Ο client λαμβάνει το ψηφιακό πιστοποιητικό του server και το χρησιμοποιεί για να τον πιστοποιήσει. Εάν η πιστοποίηση αυτή δεν καταστεί δυνατή, τότε ο χρήστης ενημερώνεται με ένα μήνυμα σφάλματος και η σύνδεση SSL ακυρώνεται. Εάν η πιστοποίηση του server γίνει χωρίς προβλήματα, τότε η διαδικασία της χειραψίας συνεχίζεται στο επόμενο βήμα.

- Ο client συνεργάζεται με τον server και αποφασίζουν τον αλγόριθμο κρυπτογράφησης που θα χρησιμοποιηθεί στην ασφαλή σύνδεση SSL. Επίσης ο client δημιουργεί το συμμετρικό κλειδί που θα χρησιμοποιηθεί στον αλγόριθμο κρυπτογράφησης και το στέλνει στον server κρυπτογραφημένο,

χρησιμοποιώντας την τεχνική κρυπτογράφησης δημοσίου κλειδιού. Ηλαδή χρησιμοποιεί το δημόσιο κλειδί του server που αναγράφεται πάνω στο ψηφιακό του πιστοποιητικό για να κρυπτογραφήσει το συμμετρικό κλειδί και να του το στείλει. Στην συνέχεια ο server χρησιμοποιώντας το ιδιωτικό του κλειδί μπορεί να αποκρυπτογραφήσει το μήνυμα και να αποκτήσει το συμμετρικό κλειδί που θα χρησιμοποιηθεί για την σύνδεση.

- Ο client στέλνει ένα μήνυμα στον server ενημερώνοντάς τον ότι είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
- Ο server στέλνει ένα μήνυμα στον client ενημερώνοντάς τον ότι και αυτός είναι έτοιμος να ξεκινήσει την κρυπτογραφημένη σύνδεση.
- Από εδώ και πέρα η χειραψία έχει ολοκληρωθεί και τα μηνύματα που ανταλλάσσουν τα δύο μηχανήματα (client - server) είναι κρυπτογραφημένα.

Η διαδικασία της χειραψίας φαίνεται πιο παραστατικά στο σχήμα που ακολουθεί.



Σχήμα 3.3:Η SSL Επικοινωνία βήμα βήμα[17]

[17] Γιακουμιδάκης Ανδρέας," Ασφάλεια σε διομότιμα δίκτυα"

3.4.2 Ipsec Τεχνολογίες (IP Security)

Τα πρωτόκολλα TCP/IP δεν παρέχουν μηχανισμούς κρυπτογράφησης. Συνεπώς, για την ασφαλή μετάδοση πάνω σε δίκτυο IP υπήρξε η ανάγκη νέου πρωτοκόλλου με μηχανισμούς κρυπτογράφησης, το οποίο θα είναι εφαρμόσιμο σε IP δίκτυα. Το IPSec (IP Security) αποτελεί ένα σύνολο πρωτοκόλλων ανεπτυγμένων από το Internet Engineering Task Force (IETF) με στόχο την ασφαλή μετάδοση και ανταλλαγή δεδομένων (packets) μέσω του στρώματος IP. Το IPSec σήμερα αποτελεί έναν από τους πιο διαδεδομένους τρόπους υλοποίησης των δικτύων VPN. Ως προς τα επίπεδα του OSI, αντιστοιχίζεται στο επίπεδο 3 (επίπεδο δικτύου).Αυτό σημαίνει πως μπορεί να προστατεύσει οποιαδήποτε ροή δεδομένων (πρωτόκολλα και εφαρμογές) ανώτερων επιπέδων.

Ο βασικός στόχος στην ανάπτυξη του προτύπου IPSec είναι η αντιμετώπιση των απειλών χωρίς να απαιτείται πρόσθετος εξοπλισμός, ούτε να υπάρχει ανάγκη για ένα σύνολο τροποποιήσεων και αλλαγών σε διάφορες εφαρμογές.

Έτσι οι υπηρεσίες που προσφέρει το πρωτόκολλο IPSec είναι:

- *Ακεραιότητα των δεδομένων* (Integrity), που διασφαλίζει ότι τα πακέτα των δεδομένων κατά την διάρκεια της μεταφοράς τους δεν έχουν αλλοιωθεί ή παραποιηθεί, είτε από «εισβολείς» είτε από τυχόν σφάλματα επικοινωνίας.
- *Εξακρίβωση γνησιότητας της προέλευσης των δεδομένων* (Authentication) ή πιστοποίηση ταυτότητας, που επαληθεύει ότι τα δεδομένα στάλθηκαν πράγματι από το χρήστη που ισχυρίζεται ότι τα έστειλε.
- *Εμπιστευτικότητα* (Confidentiality), που προσφέρει τη δυνατότητα αναγνώρισης και επεξεργασίας των δεδομένων μόνο από εγκεκριμένους χρήστες.

Το IPSec αναφέρεται σε μια σειρά πρωτοκόλλων όπως ορίζεται στα RFC 2401-2411 και RFC 2451. Αυτά τα πρωτόκολλα χωρίζονται σε δύο κύριες κατηγορίες:

- *Πρωτόκολλα σχετικά με την ασφάλεια*, τα οποία καθορίζουν την πληροφορία που πρέπει να προστεθεί σε ένα IP πακέτο για να ενεργοποιηθούν οι έλεγχοι

εμπιστευτικότητας, ακεραιότητας και πιστοποίησης ταυτότητας. Επίσης καθορίζεται και το πως πρέπει να γίνει η κρυπτογράφηση των δεδομένων του πακέτου.

- *Πρωτόκολλα σχετικά με την ανταλλαγή κλειδιών*, τα οποία διαπραγματεύονται το συσχετισμό ασφάλειας μεταξύ των δυο υποψήφιων προς επικοινωνίας οντοτήτων (θα επεξηγηθεί παρακάτω).

3.4.2.1 Πακέτα IPSec

Η IPSec ορίζει ένα νέο σετ επικεφαλίδων το οποίο προστίθεται στα IP διαγράμματα. Αυτές οι νέες επικεφαλίδες τοποθετούνται μετά την επικεφαλίδα IP και πριν το πρωτόκολλο επιπέδου 4 (τυπικά το TCP ή το UDP). Αυτές οι νέες επικεφαλίδες παρέχουν πληροφορίες για την ασφάλεια του φορτίου των IP πακέτων όπως αναλύεται παρακάτω:

- *Επικεφαλίδα πιστοποίησης ταυτότητας* (AH–Authentication Header)–αυτή η επικεφαλίδα όταν προστίθεται σε ένα IP διάγραμμα διασφαλίζει την ακεραιότητα και την ταυτότητα των δεδομένων. Δεν παρέχει ασφάλεια πιστότητας. Η επικεφαλίδα αυτή χρησιμοποιεί μια keyed-hash συνάρτηση αντί ψηφιακών υπογραφών διότι η τεχνολογία ψηφιακών υπογραφών είναι πολύ αργή και θα μείωνε την απόδοση του δικτύου.

- *Φορτίο ασφαλείας ενθυλάκωσης* (ESP–Encapsulating Security Payload)–αυτή η επικεφαλίδα όταν προστίθεται σε ένα IP διάγραμμα προστατεύει την ακεραιότητα και την ταυτότητα των δεδομένων. Αν ηESP χρησιμοποιείται για την επικύρωση της ακεραιότητας των δεδομένων δεν περιλαμβάνει τα αμετάβλητα πεδία της IP επικεφαλίδας.

Οι AH και οι ESP μπορούν να χρησιμοποιηθούν ανεξάρτητα ή μαζί, αν και για τις περισσότερες εφαρμογές μια από τις δυο είναι αρκετή. Και για τα δυο αυτά πρωτόκολλα οι IPSec δεν καθορίζει συγκεκριμένους αλγόριθμους που πρέπει να χρησιμοποιηθούν αλλά παρέχει ένα ανοικτό πλαίσιο για βιομηχανική υλοποίηση με

παραγωγή ανεξάρτητων αλγορίθμων. Αρχικά οι περισσότερες υλοποιήσεις της IPSec θα περιλαμβάνουν υποστήριξη για το MD5 από την RSA Data Security ή για την SHA (Secure Hash Algorithm) όπως ορίζεται από την κυβέρνηση των Η. Π. Α. για την ακεραιότητα και την πιστοποίηση της ταυτότητας. Το DES (Data Encryption Standard) είναι προς το παρόν ο πιο κοινά προσφερόμενος αλγόριθμος κρυπτογράφησης αν και υπάρχουν και άλλοι όπως οι IDEA, Blowfish και RC4.

3.4.2.2 Καταστάσεις λειτουργίας

Η IPSec παρέχει δυο καταστάσεις λειτουργίας, την transport και την tunnel:

Στην κατάσταση transport μόνο το IP φορτίο κρυπτογραφείται ενώ οι αρχικές επικεφαλίδες μένουν ανέπαφες. Αυτή η κατάσταση λειτουργίας έχει το πλεονέκτημα της πρόσθεσης μόνο μερικών Bytes σε κάθε πακέτο. Επιπλέον επιτρέπουν σε συσκευές στο δημόσιο δίκτυο να βλέπουν την τελική πηγή και προορισμό του πακέτου. Αυτή η δυνατότητα επιτρέπει ειδική επεξεργασία (για παράδειγμα QoS) στο ενδιάμεσο δίκτυο βασισμένη στην πληροφορία που βρίσκεται στην IP επικεφαλίδα. Ωστόσο η επικεφαλίδα του επιπέδου 4 θα κρυπτογραφηθεί περιορίζοντας τη δυνατότητα έρευνας των πακέτων. Βεβαίως αφήνοντας την IP επικεφαλίδα χωρίς κρυπτογράφηση η κατάσταση λειτουργίας transport επιτρέπει στον επιτιθέμενο να κάνει ανάλυση κίνησης (traffic analysis). Για παράδειγμα ο επιτιθέμενος θα μπορούσε να δει πότε ένα CEO της Cisco έστειλε πολλά πακέτα σε ένα άλλο CEO. Ωστόσο ο επιτιθέμενος θα γνώριζε μόνο την αποστολή των IP πακέτων και δεν θα ήταν στη θέση να καθορίσει αν αυτά ήταν πακέτα e-mail ή κάποιας άλλης εφαρμογής.

Στην κατάσταση tunnel, το IPSEC διασφαλίζει ολόκληρο το πακέτο IP, δηλαδή επικεφαλίδα και δεδομένα. Στη συνέχεια προστίθεται μια επιπλέον επικεφαλίδα IP, για τη δομολόγηση του πακέτου. Οι υπηρεσίες ασφάλειας που προσφέρονται σε λειτουργία tunnel, εξαρτώνται από το πρωτόκολλο που υλοποιεί το IPSEC (AH ή ESP). Το IPSEC σε λειτουργία tunnel χρησιμοποιείται συνήθως για την (end to end)

σύνδεση μεταξύ δύο δρομολογητών - firewalls, στα πλαίσια ενός Εικονικού Ιδιωτικού δικτύου VPN.

3.4.2.3 Εικονικά Ιδιωτικά Δίκτυα (Virtual Private Networks – VPNs)

Εκτός από τη διασύνδεση δικτύων, το IPSec υποστηρίζει την ασφαλή επικοινωνία μεταξύ δύο hosts (host - to - host), μεταξύ LAN (lan - to - lan), καθώς και συνδέσεις (user - to - LAN) όπου ο απομακρυσμένος χρήστης μπορεί να συνδεθεί ασφαλώς στο περιβάλλον του τοπικού δικτύου. Ένα δίκτυο VPN περιλαμβάνει ένα σύνολο από τεχνολογίες που επιτρέπουν την ασφαλή επικοινωνία διαμέσου μη ασφαλών δικτύων όπως είναι το Internet και τα δημόσια τηλεφωνικά δίκτυα. Η ασφάλεια ενός δίκτυου VPN δεν επιτυγχάνεται με μισθωμένες γραμμές (leased lines) αλλά με κρυπτογραφικούς μηχανισμούς ασφάλειας που επιτρέπουν μόνον σε εξουσιοδοτημένες οντότητες την πρόσβαση σε εμπιστευτικά δεδομένα. Έτσι, για παράδειγμα, ένας απομακρυσμένος client με εγκατεστημένο λογισμικό VPN μπορεί να συνδεθεί σε έναν server (VPN - enabled), και να εκτελέσει οποιαδήποτε λειτουργία (π.χ. telnet, mail, κοινή χρήση αρχείων, κ.λ.π), καθώς η επικοινωνία θα προστατεύεται από το IPSEC. Αυτό έρχεται σε αντίθεση με άλλες τεχνολογίες (π.χ. OpenSSH, SSL), οι οποίες επειδή ανήκουν σε υψηλότερα επίπεδα, μπορούν να προστατέψουν συγκεκριμένες εφαρμογές και πρωτόκολλα.

3.4.3 Υποδομή Δημόσιου Κλειδιού (PKI)

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure, PKI) αποτελεί ένα συνδυασμό λογισμικού, τεχνολογιών ασύμμετρης κρυπτογραφίας και διαδικασιών, ο οποίος κατά βάση πιστοποιεί την εγκυρότητα κάθε εμπλεκόμενου σε μια ψηφιακή συναλλαγή. Η ΥΔΚ πιστοποιεί την ταυτότητα μιας πιστοποιημένης οντότητας υπογράφοντας το δημόσιο κλειδί της και δημοσιεύοντάς το, μαζί με πληροφορίες σχετικά με την ταυτότητα της οντότητας, σε ένα πιστοποιητικό. Παράλληλα διατηρεί καταλόγους με τα έγκυρα, τα ληγμένα αλλά και τα ανακληθέντα πιστοποιητικά.

Οι κυριότεροι μηχανισμοί ασφάλειας τους οποίους καλύπτει η Υποδομή Δημόσιου Κλειδιού είναι η εξής:

- *Απόρρητο της επικοινωνίας* (Confidentiality): Τα δεδομένα προστατεύονται από μη εξουσιοδοτημένη πρόσβαση με μηχανισμούς ελέγχου πρόσβασης στην περίπτωση αποθήκευσης δεδομένων και μέσω κρυπτογράφησης κατά την αποστολή τους.

- *Ακεραιότητα* (Integrity): Τα δεδομένα προστατεύονται από μη εξουσιοδοτημένη τροποποίηση μέσω μηχανισμών κρυπτογράφησης όπως οι ηλεκτρονικές υπογραφές.

- *Πιστοποίηση* (Authentication): Πραγματοποιείται επιβεβαίωση της ταυτότητας ενός ατόμου ή της πηγής αποστολής δεδομένων.

- *Μη Άρνηση Αποδοχής* (Non - Repudiation): Η Μη Άρνηση Αποδοχής συνδυάζει τις υπηρεσίες της Πιστοποίησης και της Ακεραιότητας και διασφαλίζει ότι μία συναλλαγή η οποία πραγματοποιήθηκε ηλεκτρονικά δε μπορεί να αμφισβητηθεί από τα συμβαλλόμενα μέρη. Για παράδειγμα ο αποστολέας δεδομένων δεν μπορεί να αρνηθεί ότι δημιούργησε και απέστειλε το μήνυμα.

3.4.3.1 Το πρότυπο X.509

Το X.509 είναι ένα διεθνές πρότυπο που καθορίζει τον τρόπο λειτουργίας των Υποδομών Δημοσίου Κλειδιού (Public Key Infrastructure/PKI). Προδιαγράφει τις μορφές διάθεσης της σχετικής πληροφορίας (κλειδιά, πιστοποιητικά, λίστες ανάκλησης), καθώς και τους αλγορίθμους επαλήθευσης του κύρους ενός πιστοποιητικού.

3.4.3.2 Πιστοποιητικά και επαλήθευση

Στο X.509, η Αρχή Πιστοποίησης (Certification Authority — CA) εκδίδει ένα πιστοποιητικό, το οποίο περιλαμβάνει πληροφορίες για μια οντότητα-υποκείμενο (subject). Το υποκείμενο του πιστοποιητικού μπορεί να είναι ένα όνομα

(common name) ή κάποια άλλη οντότητα (alternative name), όπως μια διεύθυνση e-mail, μια διεύθυνση IP ή ένα όνομα DNS.

Ένα πιστοποιητικό X.509 περιέχει τις ακόλουθες πληροφορίες:

- ✓ Πιστοποιητικό
- ✓ Έκδοση X.509 (π.χ. 3)
- ✓ Αύξων Αριθμός
- ✓ Αλγόριθμος
- ✓ Εκδούσα Αρχή Πιστοποίησης
- ✓ Περίοδος έγκυροτητας
- ✓ Όχι νωρίτερα από
- ✓ Όχι αργότερα από
- ✓ Υποκείμενο
- ✓ Πληροφορίας δημόσιου κλειδιού υποκειμένου
- ✓ Αλγόριθμος δημόσιου κλειδιού
- ✓ Τιμή δημόσιου κλειδιού
- ✓ Προαιρετικές πληροφορίες…
- ✓ Επεκτάσεις (extensions)…
- ✓ Αλγόριθμος υπογραφής πιστοποιητικού

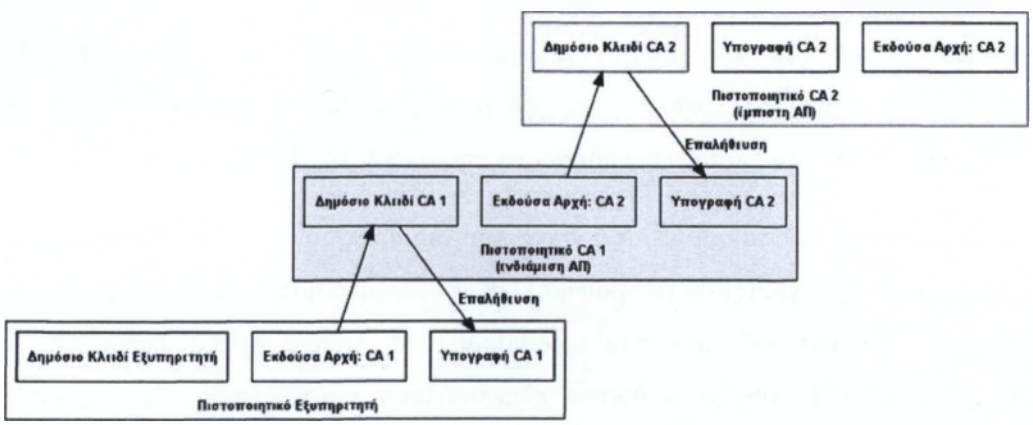
Υπογραφή πιστοποιητικού

Η Αρχή Πιστοποίησης υπογράφει ψηφιακά τις πληροφορίες του πιστοποιητικού, ώστε όποιος διαθέτει το δημόσιο κλειδί της, να μπορεί να επαληθεύσει την ισχύ των πληροφοριών που φέρει το πιστοποιητικό. Κάθε Αρχή Πιστοποίησης διαθέτει με τη σειρά της ένα δικό της πιστοποιητικό, υπογεγραμμένο από κάποια άλλη αρχή πιστοποίησης (σε αυτή την περίπτωση μιλάμε για ενδιάμεση αρχή πιστοποίησης — intermediate CA) ή από τον εαυτό της (οπότε μιλάμε για αρχική αρχή

πιστοποίησης — root CA). Επομένως η επαλήθευση της εγκυρότητας ενός πιστοποιητικού μπορεί να γίνει ακολουθώντας μια αλυσίδα Αρχών Πιστοποίησης, μέχρι να φτάσουμε σε μια έμπιστη Αρχή Πιστοποίησης (trusted CA).

Κάθε λειτουργικό σύστημα ή πρόγραμα περιήγησης του διαδικτύου (browser), διανέμεται με έναν κατάλογο έμπιστων αρχικών και ενδιάμεσων Αρχών Πιστοποίησης, πράγμα το οποίο σημαίνει ότι μπορεί να επαληθεύσει την εγκυρότητα ενός μεγάλου αριθμού πιστοποιητικών.

Έστω, για παράδειγμα, ότι συνδεόμενοι σε έναν Εξυπηρετητή (server), παρουσιάζεται ένα πιστοποιητικό υπογεγραμμένο από την αρχή πιστοποίησης «CA 1». Η «CA 1» είναιενδιάμεση αρχή πιστοποίησης και δεν υπάρχει εγκατεστημένη στο λειτουργικό σύστημα, όμως ο Εξυπηρετητής μας παρέχει το πιστοποιητικό της μαζί με το δικό του. Ελέγχοντας την υπογραφή, διαπιστώνεται ότι, σύμφωνα με τη «CA 1», το πιστοποιητικό του εξυπηρετητή είναι έγκυρο, ωστόσο η «CA 1» δεν είναι έμπιστη Αρχή Πιστοποίησης. Το πιστοποιητικό της «CA 1» φέρει υπογραφή από την «CA 2», η οποία βρίσκεται στον κατάλογο με τις έμπιστες Αρχές Πιστοποίησης του λειτουργικού συστήματος που χρησιμοποιούμε. Επομένως, επαληθεύοντας το πιστοποιητικό της «CA 1» χρησιμοποιώντας το δημόσιο κλειδί από το πιστοποιητικό της «CA 2», καταλήγουμε σε μια έμπιστη αρχή πιστοποίησης. Κατ' αυτόν τον τρόπο σχηματίζεται η αλυσίδα πιστοποίησης (certification chain) όπως φαινεται στο Σχήμα



Σχήμα 3.4:Αλυσίδα πιστοποίησης[18]

18 "Υποδομή Δημόσιου Κλειδιού (PKI)", http://pki.grnet.gr/help

Επομένως το *δημόσιο κλειδί* που βρίσκεται στο πιστοποιητικό του Εξυπηρετητή μπορεί να χρησιμοποιηθεί με ασφάλεια για την κρυπτογράφηση δεδομένων προς αυτόν, αφού η έμπιστη «CA 2» έχει επιβεβαιώσει (μέσω της «CA 1») ότι το πιστοποιητικό αυτό (και επομένως και το δημόσιο κλειδί) *όντως* ανήκει στον Εξυπηρετητή.

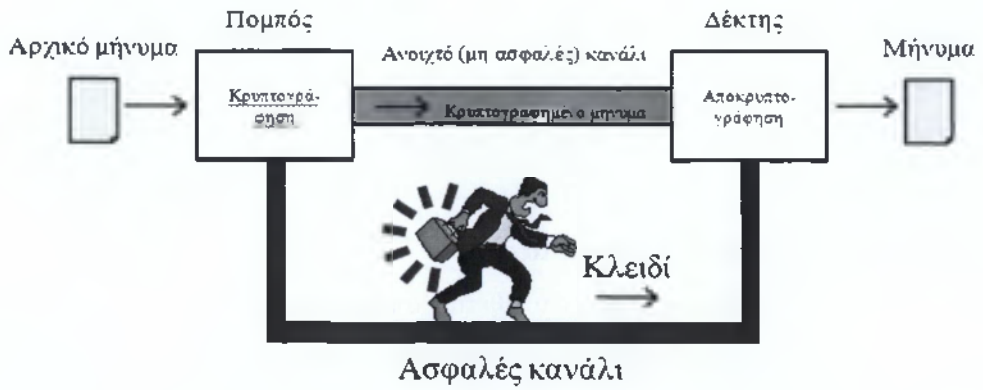
3.4.4 Η κβαντική κρυπτογραφία

Η πληροφορία κωδικοποιείται σε φωτόνια που μεταδίδονται μέσω οπτικών ινών. Η κβαντική κρυπτογραφία διαφέρει ριζικά από τα συστήματα ασφάλειας που χρησιμοποιούν τα σημερινά δίκτυα και τα οποία, παρά τις πολύπλοκες διαδικασίες στις οποίες βασίζονται, μπορούν τελικά να παραβιαστούν από όποιον έχει στα χέρια του χρόνο, χρήμα και μεγάλη υπολογιστική δύναμη.

3.4.4.1 Η μυστική δύναμη των φωτονίων

Η κβαντική κρυπτογραφία χρησιμοποιεί τους νόμους της κβαντικής φυσικής, οι οποίοι θεωρούνται εγγενώς απαραβίαστοι. Η αρχική ιδέα της κβαντικής κρυπτογραφίας ξεκίνησε πριν 25 χρόνια από τον Bennet της IBM και τον Brassard του πανεπιστημίου του Μόντρεαλ. Βασίζεται στη γνωστή κβαντική «αρχή της απροσδιοριστίας» του Heisenberg, δηλαδή στο γεγονός ότι ένας παρατηρητής δεν μπορεί να μετρήσει την κβαντική πληροφορία χωρίς να την αλλοιώσει. Η νέα τεχνολογία λειτουργεί στέλνοντας δέσμες σωματιδίων φωτονίων, οι οποίες διαταράσσονται αν κάποιος επιχειρήσει να υποκλέψει το μήνυμα.

Το σύστημα χρησιμοποιεί «κλειδιά» που δημιουργούνται και διανέμονται μέσω τεχνολογιών κβαντικής κρυπτογράφησης. Κάθε μεταδιδόμενο φωτόνιο μεταφέρει ένα απόλυτα μυστικό «κλειδί» που κωδικοποιεί τα μεταφερόμενα δεδομένα, όπως συμβαίνει στα συνηθισμένα δίκτυα ηλεκτρονικών υπολογιστών. Το πλεονέκτημα είναι ότι κανείς (πέρα από τους δύο χρήστες στο συγκεκριμένο επικοινωνιακό κανάλι) δεν μπορεί να «κρυφακούσει» για να μάθει το κλειδί, χωρίς να αποκαλύψει τον εαυτό του.



Σχήμα 3.4: διανομή κλειδιού[19]

Όπως αποδείχτηκε και στην επίδειξη που έγινε στη Βιέννη, όταν ένας εισβολέας προσπαθεί να υποκλέψει την κβαντική επικοινωνία, τα φωτόνια αλλοιώνονται και οι ανιχνευτές του δικτύου καταγράφουν την επίθεση, ενώ το σύστημα αυτόματα κλείνει για αυτοπροστασία χωρίς να έχει παραβιαστεί. Η επικοινωνία επαναλαμβάνεται αργότερα με ένα νέο «κλειδί». Αν εξάλλου, για κάποιο λόγο, ένας κβαντικός σύνδεσμος σταματήσει να λειτουργεί, τα φωτόνια στέλνονται από εναλλακτικούς δρόμους αυτόματα μέσω του τηλεπικοινωνιακού δικτύου, έτσι ώστε οι δύο χρήστες παραμένουν σε συνεχή ασφαλή επικοινωνία.

Μέχρι σήμερα είχαν γίνει και άλλες απόπειρες για κβαντική κρυπτογράφηση, αλλά βασικά αφορούσαν μόνο την επικοινωνία ανάμεσα σε δύο άτομα (αποστολέα-λήπτη) και στο πλαίσιο αυτό ήδη υπάρχουν εμπορικές εφαρμογές από αρκετές εταιρίες. Οι λύσεις αυτές έχουν περιορισμένη εφαρμογή και αυξημένους κινδύνους (αν π.χ. κοπεί το καλώδιο οπτικής ίνας, η επικοινωνία διακόπτεται).

Αντίθετα, η εφαρμογή που παρουσιάστηκε στη Βιέννη, είναι η πρώτη που αξιοποιεί την κβαντική κρυπτογραφία σε περιβάλλον δικτύου, με ό,τι θετικό αυτό συνεπάγεται (μεγαλύτερη γεωγραφική κάλυψη, εναλλακτικές οδοί επαφής αποστολέα-λήπτη για συνεχή επικοινωνία κλπ).

[19] "Σύγχρονες τάσεις – Κβαντική Κρυπτογραφία", cgi.di.uoa.gr/

Η πρώτη δημόσια εφαρμογή της κβαντικής κρυπτογραφίας έγινε το 2007 στις εκλογές στο καντόνι της Γενεύης στην Ελβετία, όπου το νέο σύστημα εγγυήθηκε ότι η ηλεκτρονική ψηφοφορία ήταν ασφαλής και ότι δεν χάθηκε καμία ψήφος στη μετάδοση από τα εκλογικά κέντρα.

3.4.4.2 Είναι όμως όντως απαραβίαστη;

Η κβαντική κρυπτογραφία είναι, υποτίθεται, απαραβίαστη και μερικές τράπεζες ήδη την χρησιμοποιούν για να μεταφέρουν δεδομένα. Όμως είχε ανακοινώθηκε από το Νορβηγικό Πανεπιστήμιο Επιστήμης και Τεχνολογίας στο Trondheim, σύμφωνα με δημοσίευμα της ηλεκτρονικής υπηρεσίας New Scientist, ότι ένας «ωτακουστής» μπορεί να την παραβιάσει χωρίς να αφήσει κανένα ίχνος, εκμεταλλευόμενος ένα πρόβλημα στον χρησιμοποιούμενο τεχνολογικό εξοπλισμό.

Ο καθηγητής Vadim Makarof του νορβηγικού πανεπιστημίου και συνεργάτες του από τη Σουηδία και τη Ρωσία υποστηρίζουν ότι τυχόν κακόβουλοι τρίτοι μπορούν να ελέγξουν από μακριά τον εξοπλισμό του λήπτη και να αποκωδικοποιούν τα σήματα που, μέσω των φωτονίων, στέλνει ο αποστολέας. Όπως δήλωσαν, έχουν ανακαλύψει ότι δύο από τις τρεις συχνότερα χρησιμοποιούμενες συσκευές κβαντικής κρυπτογραφίας είναι ευάλωτες από άποψη ασφάλειας και μελετούν πώς θα ξεπεράσουν το πρόβλημα.

Άλλοι ερευνητές πάντως, όπως ο Norbert Litkenchaous από το Ινστιτούτο Κβαντικής Πληροφορικής του Καναδά, δήλωσε ότι δεν θεωρεί πως το παραπάνω κενό ασφαλείας είναι σοβαρό. Το μέλλον θα δείξει αν οι αποκρυπτογράφοι θα μείνουν χωρίς δουλειά.

Κεφάλαιο 4ο

4. Νομικά ζητήματα P2P δικτύων

Από την πρώτη στιγμή της ανάπτυξης των P2P δικτύων ανέκυψαν σοβαρά νομικά ζητήματα. Όπως αναφέραμε και στα προηγούμενα κεφάλαια η ανταλλαγή αρχείων μέσω του διαδικτύου επιτυγχάνεται χάρη κυρίως στη χρήση της τεχνολογίας P2P. Έτσι τα νομικά ζητήματα στα P2P δίκτυα συνεπάγουν παραβίαση των δικαιωμάτων πνευματικής ιδιοκτησίας. Θέματα παραβίασης της πνευματικής ιδιοκτησίας θα μπορούσε να είναι το μεγαλύτερο πρόβλημα για P2P δίκτυα κοινής χρήσης αρχείων. Τα Νομικά ζητήματα αυξάνονται κάθε χρόνο με όλο και περισσότερους ανθρώπους να χρησιμοποιούν τα P2P δίκτυα κοινής χρήσης αρχείων.

4.1 Πνευματική ιδιοκτησία και P2P

Θέματα πνευματικής ιδιοκτησίας είναι το πιο συχνό πρόβλημα για τα P2P δίκτυα κοινής χρήσης αρχείων. Σύμφωνα με την ισχύουσα νομοθεσία για την πνευματική ιδιοκτησία τόσο σε εθνικό όσο και σε ευρωπαϊκό και διεθνές επίπεδο στο πλαίσιο των Συνθηκών του Παγκόσμιου Οργανισμού για τη Διανοητική Ιδιοκτησία (WIPO) του 1996, η χωρίς άδεια θέση ενός έργου στη διάθεση άλλων χρηστών μέσω ενός δικτύου P2P αποτελεί προσβολή του αποκλειστικού δικαιώματος του δημιουργού.

Γιατί με τον ελεύθερο διαμοιρασμό τους στο διαδίκτυο, παραβιάζονται τα δικαιώματα που έχουν οι δημιουργοί τους πάνω σε αυτά να επιτρέπει ή να απαγορεύει την ψηφιακή διάχυση του έργου του. Ενώ η εμφάνιση στην οθόνη του υπολογιστή του χρήστη ή το «κατέβασμα» (downloading) του αρχείου από ένα τέτοιο δίκτυο αποτελούν αναπαραγωγές, για τις οποίες χρειάζεται η άδεια του δημιουργού ή τυχόν άλλου δικαιούχου. Το «κατέβασμα» ενός προστατευόμενου έργου από το Διαδίκτυο εντάσσεται στην ευρεία περίμετρο του *δικαιώματος αναπαραγωγής*.

Πρόκειται για αναπαραγωγή του έργου στο σκληρό δίσκο του υπολογιστή του χρήστη του δικτύου, η οποία στα δίκτυα P2P συνοδεύεται από την ταυτόχρονη διάθεση του έργου σε έναν απροσδιόριστο αριθμό χρηστών, καθώς η φιλοσοφία των δικτύων P2P είναι ότι κάθε έργο που λαμβάνεται από το χρήστη πρέπει να προσφέρεται για ανταλλαγή στο δίκτυο. Πρόκειται για εξουσία ψηφιακής διάχυσης του έργου, δεδομένου ότι η πρόσβαση στα έργα μέσω του δικτύου P2Pπραγματοποιείται από το χώρο και στο χρόνο που έχει επιλέξει ο χρήστης. Στις περιπτώσεις που η διάθεση του έργου στο κοινό και η αναπαραγωγή πραγματοποιούνται ταυτόχρονα, αυτό που προκύπτει είναι αν η διάθεση του έργου – που τελείται αναγκαστικά και αυτόματα με το «κατέβασμα» - προσβάλλει το δικαίωμα ψηφιακής διάχυσης του δημιουργού. Σύμφωνα με μία άποψη, όταν το λογισμικό που χρησιμοποιείται δεν αφήνει στο χρήστη τη δυνατότητα να επιλέξει αν θα διαθέσει το έργο που «κατεβάζει» στο κοινό, αλλά η διάθεση πραγματοποιείται αυτόματα κατά τη διάρκεια της αναπαραγωγής και ενόσω αυτή δεν έχει ακόμη ολοκληρωθεί, πρόκειται για παθητική διάθεση, η οποία δεν αποτελεί προσβολή της πνευματικής ιδιοκτησίας, δεδομένου ότι συχνά ο χρήστης αγνοεί τη διενέργεια της διάθεσης του έργου ή τουλάχιστον δεν μπορεί να την ελέγξει, οπότε λείπει το στοιχείο της βούλησης και της πρόθεσης του χρήστη.

Επιπλέον – κατά την ίδια πάντοτε άποψη – όταν ο χρήστης διαθέτει το έργο σε άλλους χρήστες την ώρα που το «κατεβάζει», δε διαθέτει το ίδιο έργο ακέραιο ως ένα προστατευόμενο άυλο αγαθό, αλλά διάσπαρτα πακέτα δεδομένων σε πολλούς διαφορετικούς άλλους χρήστες, τα οποία από μόνα τους δεν μπορούν να εκληφθούν ως έργο ή ως αποσπάσματα έργου. Ορθότερη, ωστόσο, φαίνεται η αντίθετη άποψη, η οποία δέχεται την ύπαρξη προσβολής της πνευματικής ιδιοκτησίας εξαιτίας της χωρίς άδεια διάθεσης του έργου στο κοινό, άσχετα από το αν αυτή έχει επιλεγεί από το χρήστη ή αν αποτελεί τεχνική συνέπεια της χρήσης του λογισμικού P2P, την οποία δεν μπορεί να ελέγξει ο χρήστης.

Η σύγκρουση ανάμεσα στα συμφέροντα των πνευματικών δικαιούχων, όπως αυτά ορίζονται από το δίκαιο της πνευματικής ιδιοκτησίας και των δικαιωμάτων των χρηστών του διαδικτύου στην ενημέρωση και την πρόσβαση σε πληροφορίες, έχει

δημιουργήσει προβληματισμούς σχετικά με τις νομοθετικές ρυθμίσεις που απαιτούνται για την εναρμόνιση των παραπάνω δικαιωμάτων στην σύγχρονη εποχή.

4.2 Προστασία προσωπικών δεδομένων και P2P

Λαμβάνοντας υπόψη τη συνεχή αύξηση της πειρατείας προστατευμένου υλικού, οι κάτοχοι των πνευματικών δικαιωμάτων προσπαθούν να βρουν νέους τρόπους, έτσι ώστε να προστατεύσουν τα δικαιώματα που έχουν πάνω στα έργα τους. Οι πρώτες προσπάθειες των δικαιούχων ήταν επικεντρωμένες στο να αναγκάσουν τους παρόχους να εγκαταστήσουν φίλτρα και άλλα τεχνολογικά μέσα, για τον περιορισμό της πρόσβασης σε ηλεκτρονικές διευθύνσεις, οι οποίες έδιναν την δυνατότητα στους χρήστες να κατεβάζουν προστατευμένο υλικό, αλλά και για την χρήση προγραμμάτων ανταλλαγής αρχείων τύπου P2P.

Στην συνέχεια, σε μια προσπάθεια να μειωθεί η ανταλλαγή αρχείων μέσω του internet, οι δικαιούχοι άρχισαν να πιέζουν τους παρόχους υπηρεσιών Internet (Internet Service Providers, ISP), έτσι ώστε να αποσπάσουν από αυτούς τα στοιχεία των πελατών τους, και τις διευθύνσεις IP τους, προκειμένου να μπορούν στη συνέχεια να καταθέτουν μηνύσεις σε βάρος αυτών που κατεβάζουν προστατευμένα αρχεία, κυρίως μέσα από P2P προγράμματα. Όπως είναι φανερό, προκύπτουν κάποια σοβαρά νομικά ζητήματα, καθώς η απαίτηση αυτή των δικαιούχων έρχεται αντιμέτωπη με κάποια από τα θεμελιώδη δικαιώματα των πολιτών, όπως είναι το δικαίωμα της επικοινωνίας, αλλά και το δικαίωμα προστασίας των προσωπικών δεδομένων.

Η ανταλλαγή προστατευόμενων έργων μέσω δικτύων P2P αποτελεί μια ιδιαίτερη μορφή ηλεκτρονικής επικοινωνίας, η οποία καλύπτεται από τον ευρύ ορισμό της επικοινωνίας στο άρθρο 2 της Οδηγίας 2002/58/ΕΚ, σύμφωνα με τον οποίο ως επικοινωνία νοείται κάθε πληροφορία που ανταλλάσσεται ή διαβιβάζεται μεταξύ ενός πεπερασμένου αριθμού μερών μέσω μιας διαθέσιμης στο κοινό υπηρεσίας ηλεκτρονικών επικοινωνιών.

Η κάλυψη των διευθύνσεων IP από την προστασία του απορρήτου της επικοινωνίας σημαίνει ότι προκειμένου να είναι νόμιμη η συλλογή των διευθύνσεων IP, πρέπει να τηρούνται οι νόμιμες προϋποθέσεις άρσης του απορρήτου. Επομένως, η διεύθυνση IP έχει διπλή ιδιότητα: από τη μια αποτελεί προσωπικό δεδομένο και από την άλλη στοιχείο συστατικό της επικοινωνίας.

4.3 Ιστορικές δικαστικές αποφάσεις και νομολογίες

Από την πρώτη στιγμή της εμφάνισης των δικτύων P2P όπως προαναφέραμε, οι πνευματικοί δημιουργοί, έσπευσαν να διασφαλίσουν τα δικαιώματα τους μέσω δικαστικών αγώνων. Στόχος τους ήταν η παρεμπόδιση του διαμοιρασμού των έργων τους στο διαδίκτυο χωρίς άδεια, κάτι που έβλαπτε τα οικονομικά και ηθικά τους συμφέροντα. Τα πρώτα χρόνια οι δικαιούχοι κινήθηκαν νομικά εναντίων των δημιουργών των P2P προγραμμάτων, ενώ στη συνέχεια αποφάσισαν να στραφούν και ενάντια των χρηστών, οι οποίοι αντάλλασαν προστατευμένα έργα, προσβάλλοντας με τον τρόπο αυτό το δικαίωμα της αναπαραγωγής, αλλά και της διάθεσης στο κοινό.

4.3.1 Διώξεις κατά των δημιουργών των P2P προγραμμάτων

Η πιο γνωστή υπόθεση υπήρξε η υπόθεση «Napster». Όπως έχει ήδη αναφερθεί, τον Ιούνιο του 1999 εμφανίστηκε το Napster, λογισμικό για P2P δίκτυα. Το Napster αμέσως κατηγορήθηκε πως παραβίαζε τα πνευματικά δικαιώματα των δημιουργών των τραγουδιών και πως χρησιμοποιούταν για την παράνομη ανταλλαγή προστατευμένων αρχείων. Άμεσα η αμερικάνικη ένωση δισκογραφικών εταιρών (RIAA), κινήθηκε νομικά εναντίων του Napster, με την αιτιολογία πως η υπηρεσία παρείχε την δυνατότητα στους χρήστες του προγράμματος να ανταλλάσουν προστατευμένα αρχεία μέσω ενός κεντρικού καταλόγου που επέτρεπε την αναζήτηση τραγουδιών, αλλά και την επικοινωνία μεταξύ των χρηστών.

Συγκεκριμένα στην δίκη η οποία είναι γνωστή ως A&M Records, Inc. v. Napster, Inc., η μουσική βιομηχανία κατήγγειλε:

- Πως οι χρήστες του προγράμματος Napster μέσω της ανταλλαγής προστατευμένων έργων, πρόσβαλλαν άμεσα τα πνευματικά δικαιώματα των δημιουργών.
- Πως το Napster ευθυνόταν για τη δευτερεύουσα προσβολή των πνευματικών δικαιωμάτων των δικαιούχων
- Το Napster ήταν υπεύθυνο και για την έμμεση προσβολή των πνευματικών δικαιωμάτων των δημιουργών.

Μετά την τελική απόφαση του δικαστηρίου, οι υπεύθυνοι του Napster καταδικάστηκαν σε καταβολή χρηματικού ποσού της τάξεως των 36 εκατομμυρίων ευρώ στις δισκογραφικές εταιρίες και στους δικαιούχους των πνευματικών δικαιωμάτων, ως αποζημίωση για τις απώλειες που είχαν υποστεί. Παράλληλα έγινε μια προσπάθεια, έτσι ώστε να συνεχίσει να λειτουργεί το πρόγραμμα με συνδρομή, διανέμοντας νέο υλικό από τις δισκογραφικές εταιρίες έναντι κάποιου οικονομικού ανταλλάγματος. Από τότε έχει ακολουθήσει μια σειρά εξαγορών του Napster με τελευταία αυτή της Best Buy έναντι 121 εκατομμυρίων δολαρίων.

Ο κυριότερος λόγος για τον οποίο το Napster καταδικάστηκε ήταν η ύπαρξη του κεντρικού καταλόγου στον οποίο αποθηκεύονταν οι IP των χρηστών και μέσω του οποίου μπορούσαν οι χρήστες να αναζητούν τραγούδια, αλλά και να επικοινωνούν με άλλους χρήστες. Κατανοώντας ότι ο κεντρικός ρόλος της «Napster» στην παράνομη ανταλλαγή μουσικών αρχείων οδήγησε στην καταδίκη της εταιρίας, οι εταιρίες που παρείχαν παρόμοια τεχνολογία αποφάσισαν να μεταβάλουν τα τεχνολογικά δεδομένα για να αποφύγουν μελλοντικές καταδίκες για προσβολή πνευματικής ιδιοκτησίας.

Τα πρώτα προγράμματα P2P, που υιοθετούσαν την αποκεντρωτική προσέγγιση, ήταν το Grokster, το Morpheus της Streamkast Networks και το Kazaa. Όπως θα φανεί παρακάτω, η στάση των δικαστηρίων ήταν ευνοϊκότερη απέναντι στις εταιρίες ανάπτυξης αυτών των προγραμμάτων, σε σχέση με τη στάση τους απέναντι στο Napster. Πράγματι, στην διαμάχη ανάμεσα στην MGM Studios και τις εταιρίες Grokster και Streamkast, η πρωτόδικη απόφαση του αμερικάνικου δικαστηρίου απάλλαξε τις δύο εταιρίες ανάπτυξης των P2P προγραμμάτων από τις κατηγορίες της δευτερεύουσας και έμμεσης προσβολής της πνευματικής ιδιοκτησίας. Κατά την

διάρκεια της δίκης οι εκπρόσωποι των δύο εταιριών επικαλέστηκαν την απόφαση του Ανωτάτου Δικαστηρίου της Αμερικής το 1984 στην διαμάχη της Sony Corp Of America με την Universal City Studios.

Το δικαστήριο έκρινε πως τα προγράμματα αυτά δεν προσφέρονταν μόνο για παράνομη ανταλλαγή αρχείων, αλλά είχαν και άλλες νόμιμες χρήσεις, ενώ παράλληλα αναγνώρισε πως λόγω της έλλειψης κεντρικού καταλόγου, οι δύο αυτές εταιρίες δεν συμμετείχαν άμεσα στην ανταλλαγή προστατευμένων έργων.

Ένα άλλο πρόγραμμα P2P, αποκεντρωτικού χαρακτήρα, ήταν το Kazaa, το οποίο δημιουργήθηκε το 2001 από την ολλανδική εταιρία Consumer Empowerment. Η εταιρία αμέσως δέχτηκε μήνυση από την ολλανδική εταιρία παραγωγής μουσικής Buma/Stemra για την άμεση και έμμεση προσβολή πνευματικών δικαιωμάτων και οδηγήθηκε στα ολλανδικά δικαστήρια. Αν και πρωτοδίκως καταδικάστηκε, το εφετείο της Ολλανδίας αθώωσε τελικά την Consumer Electronics. Στη συνέχεια, στα πλαίσια της δικαστικής διαμάχης ανάμεσα στην εταιρία MGM Studios και τις εταιρίες Grokster και Streamkast, απαγγέλθηκαν κατηγορίες και κατά των νέων ιδιοκτητών του Kazaa (Sharman Networks). Τελικά οι κατηγορίες απορριφθήκαν από το εφετείο Ninth Circuit Court of Appeals της Αμερικής.

Οι παραπάνω αποφάσεις αντικατοπτρίζουν τη σημαντική αλλαγή που υπήρξε στην αντιμετώπιση από τα δικαστήρια της ευθύνης των εταιριών που αναπτύσσουν προγράμματα, όταν αυτά P2P δεν περιλαμβάνουν κεντρικό κατάλογο αναζήτησης. Ωστόσο, τη στάση αυτή δεν την υιοθέτησε το σύνολο των δικαστηρίων. Στις 25 Ιουνίου του 2005, το Ανώτατο δικαστήριο της Αμερικής ανέτρεψε την αρχική απόφαση του πρωτοβάθμιου και δευτεροβάθμιου δικαστηρίου στην δίκη «MGM Studios Inc. εναντίων Grokster Ltd», κρίνοντας πως τα προγράμματα Grokster και Morpheus είναι υπεύθυνα για την προσβολή των πνευματικών δικαιωμάτων των δημιουργών. Το Ανώτατο δικαστήριο απεφάνθη τελικώς πως δεν μπορεί να γίνει χρήση της δικαστικής απόφασης στην διαμάχη της Sony Corp Of America με την Universal City Studios.

Ο κυριότερος λόγος καταδίκης των δύο εταιριών ήταν η παρακίνηση, των χρηστών, να χρησιμοποιήσουν τα προγράμματα αυτά για να προβούν σε παράνομη

ανταλλαγή αρχείων, προσβάλλοντας έτσι τα πνευματικά δικαιώματα των δημιουργών.

Αμέσως μετά την απόφαση του Ανωτάτου δικαστηρίου, η Grokster Ltd ανέστειλε την διανομή του προγράμματος και κατέβαλε ποσό ίσο με 50 εκατομμύρια δολάρια σε εταιρίες της μουσικής βιομηχανίας. Επιπρόσθετα, το Φεβρουάριο του 2004 και πριν ακόμα την λήξη της δίκης Grokster, η Αυστραλιανή Ένωση Δισκογραφικών Εταιριών (ARIA) κατέθεσε ασφαλιστικά μέτρα ενάντιον της εταιρίας Sharman Networks, για προσβολή πνευματικών δικαιωμάτων μέσω του προγράμματος Kazaa. Στις 5 Σεπτεμβρίου του 2005, το Ομοσπονδιακό Δικαστήριο της Αυστραλίας έκρινε πως, αν και η ίδια η εταιρία δεν προσέβαλλε η ίδια τα πνευματικά δικαιώματα των δημιουργών, ωστόσο επέτρεπε σε άλλους να το πράξουν.

Για τον λόγο αυτό διέταξε την εταιρία να τροποποιήσει το πρόγραμμα Kazaa εντός δύο μηνών. Εντούτοις η Sharman Networks δεν έπραξε ως όφειλε, με αποτέλεσμα, στις 5 Δεκεμβρίου του 2005 να αναγκαστεί να διακόψει την διανομή του προγράμματος. Παράλληλα στα πλαίσια του συμβιβασμού με την RIAA, η Sharman Networks κατέβαλε το ποσό των 100 εκατομμυρίων δολαρίων στις τέσσερις μεγαλύτερες δισκογραφικές εταιρίες της Αμερικής. Εξετάζοντας τη νομολογία Grokster και την απόφαση του Αυστραλιανού δικαστηρίου στην υπόθεση Kazaa, εξάγεται το συμπέρασμα πως, παρά την ύπαρξη νόμιμων χρήσεων για τα P2P προγράμματα δεύτερης γενιάς, αλλά και της έλλειψης άμεσης συμμετοχής στην προσβολή των πνευματικών δικαιωμάτων, λόγω της απουσίας κεντρικού καταλόγου, εντούτοις, οι διανομείς τέτοιου λογισμικού είναι υπεύθυνοι για τις παράνομες ανταλλαγές αρχείων από τους χρήστες τους.

Οι διανομείς τέτοιων προγραμμάτων θα πρέπει να χρησιμοποιούν μέτρα για την πρόληψη της προσβολής της πνευματικής ιδιοκτησίας, όπως εγκατάσταση φίλτρων για τον έλεγχο των αρχείων που ανταλλάσσονται, ενώ σε καμιά περίπτωση δεν θα πρέπει να ενθαρρύνουν τους χρήστες να τελέσουν παράνομες πράξεις με την χρήση των προγραμμάτων τους.

4.3.2 Διώξεις κατά των χρηστών των P2P δικτύων

Η αβεβαιότητα ως προς το αποτέλεσμα της δικαστικής κρίσης στις δίκες κατά των εταιριών που διανέμουν το λογισμικό P2P υπήρξε η αιτία της αλλαγής στρατηγικής από τους δικαιούχους των πνευματικών δικαιωμάτων, οι οποίοι εγκαταλείπουν μερικώς την τακτική του προσδιορισμού και της δίωξης ενός κεντρικού υπευθύνου για τις προσβολές και αρχίζουν πλέον να στρέφονται κατά των τελικών χρηστών.

Οι λόγοι για την αλλαγή της στάσης των δικαιούχων είναι πολλαπλοί και περιλαμβάνουν:

- Την συνεχή εξέλιξη των P2P δικτύων, εξέλιξη η οποία κάποια στιγμή θα καθιστούσε δυσχερή την ενοχοποίηση των διανομέων τους.
- Τον εκφοβισμό των χρηστών μέσω της παραδειγματικής τιμωρίας μερικών από αυτούς

Σε πολλές περιπτώσεις οι δικαιούχοι, στις δικαστικές διαμάχες με χρήστες, εμπλέκουν και τους παρόχους internet, ζητώντας από αυτούς τα στοιχεία των πελατών τους, με αποτέλεσμα να εγείρονται ζητήματα σχετικά με την προστασία των προσωπικών δεδομένων, κάτι με το οποίο θα ασχοληθούμε εκτενώς στην επόμενη ενότητα. Οι απλοί χρήστες αυτών των προγραμμάτων, προσβάλλουν τα δικαιώματα των πνευματικών δημιουργών με δύο τρόπους.

1. Πρώτον, με το ανέβασμα ενός προστατευμένου έργου σε κάποιο δίκτυο P2P, χωρίς άδεια, προσβάλλουν το δικαίωμα του δημιουργού στην διάθεση του έργου του στο κοινό.
2. Δεύτερον, όταν κάποιος χρήστης κατεβάζει κάποιο προστατευμένο έργο στον υπολογιστή του, προσβάλλει το δικαίωμα της αναπαραγωγής του έργου, αφού δημιουργεί παράνομα ένα αντίγραφο αυτού στον σκληρό του δίσκο.

Οι περισσότερες αγωγές κατά χρηστών γίνονται εναντίον χρηστών που διαθέτουν τα προστατευμένα έργα σε κάποιο P2P δίκτυο με την διαδικασία του uploading. Όπως αναφέραμε είναι τέτοια η αρχιτεκτονική των δικτύων P2P, που ακόμη και όταν

ένας χρήστης απλά κατεβάζει κάποιο αρχείο, ταυτόχρονα ανεβάζει και τμήματα αυτού του αρχείου ακόμα και παρά την θέληση του ή εν αγνοία του. Συνήθως, μάλιστα, υποχρεώνεται να το κάνει έτσι ώστε να του επιτρέπεται να συμμετάσχει στην P2P κοινότητα. Επιπρόσθετα δεν χρειάζεται να ολοκληρωθεί το κατέβασμα του αρχείου για να αρχίσει το πρόγραμμα να ανεβάζει μέσω αυτοματοποιημένης διαδικασίας τμήματα του αρχείου.

Οι χρήστες των P2P προγραμμάτων στις πρώτες αγωγές εναντίον τους, αμύνθηκαν προβάλλοντας το δικαίωμα τους για αναπαραγωγή στα πλαίσια της ιδιωτικής χρήσης. Παρόλα αυτά, οι αποφάσεις των δικαστηρίων στις πρώτες αγωγές κατά των χρηστών ήταν καταδικαστικές, αφού απέρριπταν την εξαίρεση της αναπαραγωγής για ιδιωτική χρήση, ενώ ταυτόχρονα καταδίκαζαν τους χρήστες και για την παράνομη διάθεση του υλικού στο διαδίκτυο, αφού αυτή γινόταν δίχως άδεια. Μάλιστα το γεγονός πως η αναπαραγωγή γινόταν από ένα αντίτυπο το οποίο διατέθηκε στο κοινό χωρίς άδεια, ήταν το κύριο επιχείρημα για το οποίο οι δικαστικές αρχές δεν δέχονταν και την εφαρμογή της εξαίρεσης της αναπαραγωγής για ιδιωτική χρήση.

Το αρνητικό κλίμα προς τους χρήστες P2P δικτύων άρχισε να ανατρέπεται το όταν, στις 13 Οκτωβρίου του 2004, το Πλημμελειοδικείο της πόλης Rodez της Γαλλίας, αθώωσε έναν χρήστη για την παράνομη αναπαραγωγή κινηματογραφικών ταινιών. Το δικαστήριο έκρινε πως εφαρμόζεται η εξαίρεση της αναπαραγωγής για ιδιωτική χρήση, ενώ ταυτόχρονα ο χρήστης απαλλάχθηκε και από κατηγορίες για διάθεση του έργου μέσω του προγράμματος. Την απόφαση του Πλημμελειοδικείου επικύρωσε και το Εφετείο του Montpellier στις 10 Μαρτίου του 2005.

Μάλιστα σε μια παρόμοια υπόθεση που εκδικάστηκε τον Δεκέμβριο του 2005, γαλλικό δικαστήριο όχι μόνο αθώωσε χρήστη από την κατηγορία της παράνομης αναπαραγωγής, αλλά ταυτόχρονα απέρριψε τις κατηγορίες εναντίον του για παράνομη διάθεση του έργου στο κοινό. Ο λόγος ήταν πως λόγω της αρχιτεκτονικής των δικτύων όταν ο χρήστης «κατέβασε» το προστατευμένο αρχείο και χωρίς να προβεί σε κάποια άλλη ενέργεια, έγινε ταυτόχρονα και uploader, με αποτέλεσμα άλλοι χρήστες του δικτύου να έχουν πρόσβαση στο αρχείο αυτό.

Το δικαστήριο έκρινε πως δεν υπήρξε δόλος στις ενέργειες του χρήστη. Έτσι, η διάθεση του έργου στο κοινό ήταν απλά μια συνέπεια της αναπαραγωγής του έργου στον σκληρό δίσκο του χρήστη, πράξη η οποία ήταν νόμιμη λόγω της εξαίρεσης για ιδιωτική χρήση. Ταυτόχρονα το P2P πρόγραμμα που είχε χρησιμοποιηθεί, δεν έδινε κάποια επιλογή στον χρήστη, έτσι ώστε να ενημερώσει τους άλλους χρήστες του δικτύου πως το αντίγραφο διανεμόταν χωρίς την άδεια του δημιουργού. Ο χρήστης, δηλαδή, δεν προέτρεπε άλλους χρήστες να κατεβάσουν ένα παράνομο αντίγραφο του έργου.

Η εφαρμογή της εξαίρεσης της αναπαραγωγής εφαρμόστηκε και στην δικαστική διαμάχη μεταξύ της Ένωσης Δισκογραφικών Εταιριών του Καναδά (CRIA) και πέντε παροχών internet του Καναδά. Η CRIA ζήτησε από τους συγκεκριμένους παρόχους να της παραδώσουν στοιχεία για 29 πελάτες τους που αντάλλασαν παράνομα προστατευμένα αρχεία μέσω P2Pδικτύων.Οι δικαστικές αρχές έκριναν πως οι πάροχοι δεν είναι υποχρεωμένοι να παραδώσουν τα στοιχεία αυτά και πως η αναπαραγωγή των έργων είναι νόμιμη λόγω της εξαίρεσης για ιδιωτική χρήση. Παράλληλα, αθώωσαν του χρήστες και για την πράξη της διάθεσης των έργων δίχως άδεια, δεχόμενοι πως η διάθεση τους ήταν απλά συνέπεια της αναπαραγωγής του αρχείου και της αυτόματης τοποθέτησης στον φάκελο με τα προς διανομή αρχεία.

Η προσωρινή (όπως αποδείχθηκε) αυτή ευνοϊκή στάση των δικαστικών αρχών υπέρ των χρηστών των P2Pδικτύων ανατράπηκε απότομα όταν, τον Μάιο του 2006, το γαλλικό Ακυρωτικό δικαστήριο κατήργησε την νομολογία του Εφετείου του Montpellier, την νομολογία δηλαδή πάνω στην οποία στηρίχθηκαν πολλές μεταγενέστερες αθωωτικές δικαστικές αποφάσεις.

Ο λόγος της ακύρωσης της συγκεκριμένης νομολογίας ήταν πως Εφετείο δεν είχε δώσει επαρκείς εξηγήσεις για το εάν ο χρήστης που διέθετε το αρχείο στο δίκτυο το είχε αποκτήσει από νόμιμη πηγή, ενώ ταυτόχρονα δεν αντίκρουσε τους ισχυρισμούς της πολιτικής αγωγής πως «η εξαίρεση της αναπαραγωγής για ιδιωτική χρήση αποτελεί απόκλιση από το μονοπώλιο του δημιουργού και συνεπώς για να τύχει εφαρμογής πρέπει η αναπαραγωγή να πραγματοποιείτε από κάποια νόμιμη πηγή του έργου και αναγκαστικά να μην προκαλεί βλάβη στα δικαιώματα των δικαιούχων

πνευματικής ιδιοκτησίας επί των έργων». Η υπόθεση παραπέμφθηκε στο Εφετείο του Aix-en-Provence, το οποίο επίσης απέρριψε την περίπτωση εξαίρεσης της αναπαραγωγής για ιδιωτική χρήση, δεν έλαβε όμως θέση γύρω από το πόσο σημαντικό είναι να είναι νόμιμη η πηγή από την οποία ο χρήστης απέκτησε το αρχείο προς διάθεση.

Το κριτήριο της «νομιμότητας της πηγής» έχει διχάσει τις δικαστικές αρχές, για το εάν μπορεί να εφαρμοστεί στην περίπτωση της εξαίρεσης της αναπαραγωγής για ιδιωτική χρήση. Είναι όμως γενικά αποδεκτή η άποψη, πως, από την στιγμή που η απόδειξη της νομιμότητας της πηγής του αρχείου είναι πολλές φορές αδύνατη, είναι προτιμότερο να αποφεύγετε αυτός ο περιορισμός στην εφαρμογή της εξαίρεσης στα πλαίσια της ιδιωτικής χρήσης.

Μέχρι σήμερα πολλοί ακόμη χρήστες βρέθηκαν ενώπιον των δικαστικών αρχών για παράνομη ανταλλαγή αρχείων μέσω διαδικτύου. Παρόλα αυτά οι αποφάσεις των δικαστηρίων διαφοροποιούνται ανάλογα πάντα και με τις συνθήκες που περιβάλλουν την κάθε υπόθεση. Για τον λόγο αυτό, είναι επιτακτική η ανάγκη δημιουργίας ενός ενιαίου νομικού πλαισίου γύρω από την χρήση P2P δικτύων ή η εύρεση μιας κοινά αποδεκτής λύσης που να διασφαλίζει σε ικανοποιητικό βαθμό τα δικαιώματα των πνευματικών δημιουργών, αλλά και τις ελευθερίες των πολιτών.

4.3.3 Διώξεις κατά των trackers και των ιστοσελίδων αναζήτηση αρχείων torrent

Η μεγάλη διάδοση των P2P δικτύων που ακολουθούσαν το πρότυπο BitTorrent και ο, συνεχώς αυξανόμενος, αριθμός των χρηστών τους, έστρεψαν τις ενώσεις των δισκογραφικών εταιριών και των κινηματογραφικών στούντιο εναντίων των trackers που φιλοξενούσαν αρχεία σε μορφή torrent, αλλά και των ιστοσελίδων που προσέφεραν δυνατότητες αναζήτησης τέτοιων αρχείων.

Πολύ γρήγορα η Ένωση Κινηματογραφικών Εταιριών της Αμερικής (Motion Picture Association of America, MPAA) άσκησε διώξεις σε πολλούς trackers, αλλά και σε σελίδες αναζήτησης αρχείων torrent, συμπεριλαμβανομένων και των

TorrentSpy, IsoHunt και TorrentBox, για συστηματική προσβολή πνευματικών δικαιωμάτων.

4.3.3.1 Pirate Bay

Το The Pirate Bay είναι η ποιο δημοφιλής ιστοσελίδα αναζήτησης αρχείων torrent παγκοσμίως και σύμφωνα με τους ιδιοκτήτες του, αριθμεί πάνω από 25 εκατομμύρια χρήστες. Η δημιουργοί του μάλιστα φημίζονταν για την αλαζονική και ειρωνική τους στάση απέναντι στις αντί-πειρατικές οργανώσεις και τις αρχές.

Το 2006 η Σουηδική αστυνομία, μετά από πιέσεις της MIAA, με οργανωμένη επιχείρηση κατάσχεσε 186 servers που άνηκαν στο Pirate Bay. Παρόλα αυτά, η ιστοσελίδα έμεινε εκτός λειτουργίας για τρεις μόνο ημέρες, ενώ με την επαναλειτουργία της οι χρήστες της διπλασιάστηκαν.

Τον Ιανουάριο του 2008 η οργάνωση International Federation of the Phonographic Industry (IFPI), υπέβαλε μήνυση στους Fredrik Neij, Gottfrid Svartholm και Peter Sunde, δημιουργούς της ιστοσελίδας ThePirateBay.org, αλλά και στον επιχειρηματία Carl Lundstrom, ιδιοκτήτη της εταιρίας Rix Telecom AB, που παρείχε υπηρεσίες φιλοξενίας στην ιστοσελίδα.

Οι παραπάνω κατηγορήθηκαν για έμμεση και δευτερεύουσα προσβολή πνευματικής ιδιοκτησίας μέσω της ιστοσελίδας, και πιο συγκεκριμένα κατηγορήθηκαν για «υποβοήθηση τρίτων στην προσβολή πνευματικών δικαιωμάτων», παραβιάζοντας με τον τρόπο αυτό τον Σουηδικό νόμο.

Η πολύκροτη δίκη του The Pirate Bay ξεκίνησε στις 16 Φεβρουαρίου του 2009, στο δικαστήριο της Στοκχόλμης στην Σουηδία. Στην δίκη έγινε χρήση υλικού από τους servers που είχαν κατασχεθεί το 2006 από την Σουηδική αστυνομία, ως αποδεικτικών στοιχείων.

Οι κατηγορούμενοι μέσω των δικηγόρων τους υποστήριξαν πως οι ίδιοι δεν διενεργούν κάποια παράνομη πράξη, αφού στην ιστοσελίδα τους απλώς παρέχουν μια μηχανή αναζήτησης για αρχεία torrent. Έτσι, υποστήριξαν πως θα πρέπει να αντιμετωπίζονται σαν μια μηχανή αναζήτησης, όπως είναι η Google. Άλλωστε, δεν διαθέτουν οι ίδιοι προστατευμένα αρχεία στους servers τους και η διάθεση και αναπαραγωγή έργων γίνεται αποκλειστικά ανάμεσα στους χρήστες.

Μόλις την δεύτερη μέρα της δίκης, οι μισές κατηγορίες εναντίον του The Pirate Bay απορρίφθηκαν. Συγκεκριμένα, απορρίφθηκαν οι κατηγορίες που σχετίζονταν με την «υποβοήθηση της δημιουργία προστατευμένου υλικού», δηλαδή οι ιδιοκτήτες της ιστοσελίδας απαλλαχθήκαν από τις κατηγορίες σχετικά με την υποβοήθηση στην αναπαραγωγή των πνευματικών έργων. Μετά από την εξέλιξη αυτή, οι κατηγορίες που απέμειναν αφορούσαν μόνο την υποβοήθηση στην διάθεση των προστατευμένων έργων στο κοινό.

Η ακρόαση της δίκης κράτησε συνολικά εννιά ημέρες, ενώ η τελική απόφαση του δικαστηρίου ανακοινώθηκε στις 17 Απριλίου του 2009. Το δικαστήριο έκρινε ένοχους τους τέσσερις κατηγορούμενους για συνέργεια στην προσβολή πνευματικής ιδιοκτησίας και τους καταδίκασε σε ένα χρόνο φυλάκιση έκαστο και στην καταβολή προστίμου ύψους 3,5 εκατομμυρίων δολαρίων. Σημαντικό ρόλο στην λήψη αυτής της απόφασης, έπαιξε η οργανωμένη φύση των δραστηριοτήτων των κατηγορουμένων και η εμπορική χρήση της ιστοσελίδας, μέσω της οποίας αποκόμιζαν οικονομικά οφέλη, κυρίως από διαφημιστικές αφίσες (banners).

Η ιστοσελίδα συνεχίζει να λειτουργεί, όμως πλέον, αντί για αρχεία τύπου torrent, υπάρχουν τα λεγόμενα magnet links. Τα magnet links είναι μια τεχνολογία που επιτρέπει την έναρξη της ανταλλαγής ενός αρχείου χωρίς την ύπαρξη ενός tracker και μάλιστα απ' ευθείας από κάποιον εξυπηρετητή (π.χ. το πρόγραμμα utorrent). Με τον τρόπο αυτό, τα αρχεία αναζητούνται με βάση το περιεχόμενο τους και όχι με βάση τον τίτλο τους, κάνοντας χρήση ενός Hash Value. Η χρήση αυτής της τεχνολογίας καθιστά πολύ δυσκολότερο τον εντοπισμό των χρηστών που ανταλλάσουν αρχεία μέσω P2P δικτύων.

4.3.3.2 Torrent Spy

Το TorrentSpy ήταν μια δημοφιλής ιστοσελίδα, η οποία προσέφερε μια μηχανή αναζήτησης για αρχεία torrent με χρήση των οποίων οι χρήστες P2Pπρογραμμάτων μπορούσαν να κατεβάσουν προστατευμένο υλικό. Τον Φεβρουάριο του 2006 η MPAA υπέβαλε μήνυση στους ιδιοκτήτες της ιστοσελίδας, αφού πολλά από τα αρχεία torrent αφορούσαν κινηματογραφικές ταινίες που προστατεύονταν από τα πνευματικά δικαιώματα.

Ένα από τα κυριότερα επιχειρήματα που προέταξαν οι ιδιοκτήτες της ιστοσελίδας, ήταν πως στους servers τους δεν υπήρχαν αποθηκευμένα αρχεία torrent, ούτε προστατευμένο υλικό και πως η ιστοσελίδα λειτουργούσε απλά ως μια μηχανή αναζήτησης αρχείων torrent στο διαδίκτυο.

Τον Δεκέμβριο του 2007 το δικαστήριο κατηγόρησε το TorrentSpy πως εσκεμμένα κατάστρεφε συστηματικά αποδεικτικά στοιχεία εναντίων της ιστοσελίδας και των χρηστών της, ενώ ταυτόχρονα ψευδομαρτυρούσε στο δικαστήριο σχετικά με την πράξη αυτή. Για τον λόγο αυτό, το δικαστήριο έκρινε πως ήταν αδύνατο να πραγματοποιηθεί μια δίκαιη δίκη. Τελικά τον Μάιο του 2008 και παρά το γεγονός πως το TorrentSpy είχε ήδη σταματήσει την λειτουργία του, ο ομοσπονδιακός δικαστής έδωσε εντολή στους ιδιοκτήτες του TorrentSpy να καταβάλλουν ως αποζημίωση 110 εκατομμυρίων δολαρίων στην MPAA για προσβολή πνευματικών δικαιωμάτων από την διάθεση χιλιάδων κινηματογραφικών ταινιών και τηλεοπτικών σειρών.

4.4 Κατάσταση στην Ελλάδα

Για την προστασία των πνευματικών δικαιωμάτων των δημιουργών έχουν δραστηριοποιηθεί στην Ελλάδα αρκετοί αρμόδιοι οργανισμοί. Ο πλέον ενεργός σήμερα είναι η Εταιρεία Προστασίας Οπτικοακουστικών Έργων (ΕΠΟΕ), η οποία λειτουργεί ως οργανισμός συλλογικής προστασίας πνευματικών και συγγενικών

δικαιωμάτων. Και κατά καιρούς έχει προβεί σε καταγγελίες σε περιπτώσεις προσβολής της πνευματικής ιδιοκτησίας.

4.4.1 Greek-Fun.com

Στα τέλη του 2009, μετά από καταγγελία της ΕΠΟΕ, ο Αντεισαγγελέας Πλημμελειοδικών της Ρόδου, άσκησε ποινική δίωξη στους ιδιοκτήτες της ιστοσελίδας Greek-Fun.com, για προσβολή πνευματικής ιδιοκτησίας και μάλιστα σε βαθμό κακουργήματος. Η ιστοσελίδα προσέφερε συνδέσμους που παρέπεμπαν τους χρήστες σε ιστοσελίδα με προστατευμένο υλικό και έδινε στους χρήστες την δυνατότητα να αναπαράγουν το υλικό αυτό στον υπολογιστή τους, κυρίως μέσω «άμεσου κατεβάσματος» (direct download).

Παράλληλα, η ιστοσελίδα είχε και εμπορικό χαρακτήρα, αφού αποκόμιζε ωφέλη από διαφημίσεις που προβάλλονταν στην ιστοσελίδα, ενώ ταυτόχρονα, προφασιζόμενη το υψηλό κόστος συντήρησής της, ζητούσε από τους χρήστες της οικονομική ενίσχυση μέσω δωρεάς. Η ΕΠΟΕ στην καταγγελία της ανέφερε, πως η ζημιές που υπέστη από την λειτουργία της ιστοσελίδας, ανέρχονται στο ποσό των 1.800.000 ευρώ.

Αν και δεν υπήρξε χρήση του πρωτοκόλλου peer to peer, η συγκεκριμένη υπόθεση παρουσιάζει ενδιαφέρον, αφού αποτελεί την πρώτη, στην Ελλάδα, περίπτωση άσκησης κατηγοριών για παράνομη διάθεση προστατευόμενων έργων μέσω διαδικτύου.

4.4.5 Gamato.info

Στις 10 Μαρτίου του 2010 πραγματοποιήθηκε η πρώτη σύλληψη ιδιοκτητών ελληνικού tracker από την δίωξη ηλεκτρονικού εγκλήματος. Η ιστορία ξεκινά από τον Δεκέμβρη 2009, όταν το gamato.info έλαβε προειδοποίηση-εξώδικο να σταματήσει τη δραστηριότητά του που έχει σχέση με πνευματικά δικαιώματα. Το site έκλεισε μέχρι τον Φεβρουάριο, οπότε και ξανάνοιξε, έχοντας απλώς προσθέσει ένα disclaimer, σύμφωνα με το οποίο «οι χρήστες είναι αποκλειστικά υπεύθυνοι για το

περιεχόμενο των links που postάρουν στον tracker». Η λειτουργία συνεχίστηκε κανονικά, μέχρι και τις 10 μαρτίου του 2011. Η Εταιρεία Προστασίας Οπτικοακουστικών Εργων (ΕΠΟΕ) κατέθεσε μήνυση στο Τμήμα Δίωξης Ηλεκτρονικού Εγκλήματος Αθηνών κατά των διαχειριστών της σελίδας για παραβίαση του νόμου περί πνευματικής ιδιοκτησίας, επειδή στο gamato.info διακινούνταν χωρίς έγκριση ταινίες, τραγούδια, παιχνίδια και άλλο copyrighted υλικό.

Παράλληλα, η διαχειριστές της ιστοσελίδας αποκόμιζαν μεγάλα χρηματικά οφέλη από τα διαφημιστικά που προβάλλονταν στην ιστοσελίδα, αλλά και από τις δωρεές των χρηστών. Τα κέρδη αυτά, σύμφωνα με τις καταγγελίες της ΕΠΟΕ, ανέρχονται σε εκατομμύρια ευρώ. Η ιστοσελίδα ήταν ιδιαίτερα δημοφιλής, αφού αριθμούσε 850.000 μέλη και δεχόταν καθημερινά 16.000.000 επισκέψεις από χρήστες από όλο τον κόσμο. Στις 9 Μαρτίου η Δίωξη Ηλεκτρονικού Εγκλήματος Αθηνών και Θεσσαλονίκης έκανε κατ' οίκον έρευνες και σχημάτισε δικογραφίες για 11 Ελληνες ως moderators του site, από τους οποίους συνελήφθησαν οι 6, σχηματίστηκε δικογραφία εναντίον τους και οδηγήθηκαν στους εισαγγελείς για τα περαιτέρω. Επίσης ειδοποιήθηκε η Ιντερπόλ προκειμένου να συλλάβει και να εκδώσει στη χώρα άλλους δύο moderators που διαμένουν εκτός Ελλάδας..

Ωστόσο, μέχρι σήμερα στην Ελλάδα δεν έχουν γίνει διώξεις κατά μεμονωμένων χρηστών για την χρήση P2P προγραμμάτων και την ανταλλαγή αρχείων μέσω αυτών. Παρόλα αυτά, είναι άξιο αναφοράς πως το 2005, σύμφωνα με καταγγελίες σε γνωστά και έγκυρα forum, η εταιρία ALTEC, η οποία λειτουργούσε ως εναλλακτικός πάροχος internet, διέκοψε την σύνδεση ενός συνδρομητή της, για το λόγο ότι αυτός κατέβαζε μέσω P2P δικτύου και συγκεκριμένα μέσω του πρωτοκόλλου BitTorrent, μια κινηματογραφική ταινία. Παρόλα αυτά, από τότε δεν έχει επαναληφθεί κάτι παρόμοιο από κανέναν ελληνικό πάροχο.

Κεφάλαιο 5ο

5 Αντιμετώπιση Νομικών Ζητημάτων

Η καθημερινή ανταλλαγή προστατευμένων αρχείων μέσω P2P προγραμμάτων είναι μια πραγματικότητα, η οποία είναι δύσκολα αναστρέψιμη. Επί το πλείστον, οι δικαιούχοι επιλέγουν την νομική οδό για την διασφάλιση των οφελών που μπορούν να αποκομίσουν από την κανονική εκμετάλλευση των έργων τους. Αυτό έχει ως αποτέλεσμα την έναρξη αναρίθμητων και πολύχρονων δικαστικών διαμαχών κατά δημιουργών και χρηστών P2P προγραμμάτων, αλλά και κατά δημιουργών ιστοσελίδων και παρόχων υπηρεσιών internet. Πολλές φορές τα χρηματικά πρόστιμα που επιβάλλουν τα δικαστήρια σε χρήστες προγραμμάτων p2p, είναι υπερβολικά υψηλά, κάτι που καθιστά αδύνατη την αποπληρωμή τους. Όμως η παραδειγματική τιμωρία λίγων ατόμων μέσα από ένα πολύ ευρύ σύνολο, με τόσο αυστηρές ποινές, σίγουρα δεν αποτελεί την λύση του προβλήματος. Είναι λοιπόν φανερό πως θα πρέπει να εξεταστούν εναλλακτικές προτάσεις για την εξεύρεση μιας κοινά αποδεκτής λύσης στο μείζον αυτό ζήτημα.

5.1 Global License

Μια τέτοια λύση προτάθηκε για πρώτη φορά το 2005 στο γαλλικό κοινοβούλιο και είναι γνωστή ως "Global License" ή "Legal License". Σύμφωνα με την πρόταση αυτή, ο διαμοιρασμός προστατευμένου υλικού με χρήση των P2P προγραμμάτων θα μπορούσε να γίνει νόμιμος, με αντάλλαγμα οι χρήστες να πληρώνουν κάποια μηνιαία συνδρομή στον πάροχο τους. Τα χρήματα από τη συνδρομή αυτή των χρηστών θα κατέληγαν στην συνέχεια στους δικαιούχους. Με τον τρόπο αυτό οι χρήστες των P2P προγραμμάτων θα μπορούσαν να «κατεβάζουν» όποια αρχεία επιθυμούσαν, δίχως τον φόβο κάποιας καταγγελίας.

Η ιδέα του Global License γρήγορα απέκτησε πολλούς υποστηρικτές, όπως, για παράδειγμα, οργανώσεις διάφορες χρηστών του διαδικτύου, καταναλωτών και οικογενειών, αλλά και οργανώσεις μουσικών και άλλων καλλιτεχνών. Παράλληλα, είχε την υποστήριξη και αρκετών πολιτικών προσώπων. Οι υποστηρικτές της ιδέας ανέφεραν πως η χρήση του Global License είναι μια εφαρμόσιμη και ρεαλιστική λύση, η οποία θα μπορούσε να προσφέρει αρκετά έσοδα στους δικαιούχους. Αναλυτικά, κάποια από τα πλεονεκτήματα του Global License, όπως τα παρουσιάζουν οι υποστηρικτές της ιδέας αυτής, είναι τα ακόλουθα:

- Οι βιομηχανίες της μουσικής και του κινηματογράφου και οι δικαιούχοι θα λαμβάνουν συνεχή και ικανοποιητικά έσοδα από την συνδρομή των χρηστών. Τα έσοδα θα μοιράζονται ανάλογα με την δημοτικότητα των καλλιτεχνών ή την πραγματική διακίνηση των αρχείων, αν αυτή μπορεί να καταγραφεί λεπτομερώς
- Οι χρήστες του διαδικτύου θα μπορούν να ανταλλάσουν μουσικά και άλλα αρχεία χωρίς φόβο, από μια μεγάλη βιβλιοθήκη. Όσο περισσότεροι χρήστες ανταλλάσουν αρχεία, τόσο περισσότερες επιλογές θα υπάρχουν
- Θα υπάρξει πραγματική ανάπτυξη στην ευρυζωνικότητα και τις τεχνολογίες του διαδικτύου, αφού περισσότεροι χρήστες θα ζητούν καλύτερες ταχύτητες στο internet και θα δέχονται να πληρώσουν περισσότερα για αυτές.
- Νέοι καλλιτέχνες και παραγωγοί θα μπορούν να διαφημίζουν τη δουλειά τους και να αποκομίζουν έσοδα από αυτή, χωρίς την ανάγκη των δισκογραφικών εταιριών και των κινηματογραφικών στούντιο
- Θα ελαχιστοποιηθεί η παρέμβαση των δικαστικών αρχών.

Βέβαια η εφαρμογή της λύσης του Global License ενέχει αρκετές δυσκολίες, όπως είναι, για παράδειγμα, η εύρεση ενός τρόπου για τον σωστό διαμοιρασμό των εσόδων στους δικαιούχους, αλλά και η εξασφάλιση πως τα έσοδα θα είναι αρκετά, έτσι ώστε να αποζημιώνονται επαρκώς οι δικαιούχοι για την ελεύθερη ανταλλαγή των έργων τους.

Αν και η ιδέα του Global License που προτάθηκε το 2005 στο γαλλικό κοινοβούλιο δεν μετουσιώθηκε σε κάποιο νόμο, εξακολουθεί μέχρι και σήμερα να έχει πολλούς υποστηρικτές και θα μπορούσε μελλοντικά να διαμορφώσει την υπόσταση της ανταλλαγής προστατευμένων αρχείων στο διαδίκτυο.

5.2 Ο Γαλλικός Νόμος HADOPI

Σε μια προσπάθεια να μειωθεί η ανταλλαγή προστατευμένων έργων μέσω του διαδικτύου και να προστατευθούν οι δικαιούχοι, η γαλλική κυβέρνηση παρουσίασε, στα μέσα του 2009, ένα νομοσχέδιο με την ονομασία HADOPI. Το νομοσχέδιο αυτό στην αρχική του μορφή, προέβλεπε πως σε περίπτωση που γινόταν αντιληπτό πως κάποιος χρήστης του διαδικτύου «κατέβαζε» παράνομα προστατευμένο υλικό μέσω κάποιου P2P προγράμματος, τότε ο χρήστης αυτός αρχικά θα λάμβανε ένα προειδοποιητικό email από μια αρμόδια αρχή με την ονομασία HADOPI (the Haute Autorit pour la Diffusion des Oeuvres et la Protection des droits sur Internet), μέσω του παρόχου του. Σε περίπτωση που ο χρήστης συνέχιζε την παράνομη αυτή δραστηριότητα, θα λάμβανε μια προειδοποιητική επιστολή στην διεύθυνση κατοικίας του. Εάν, παρόλα αυτά, ο χρήστης δε συμμορφωνόταν με τις παραπάνω υποδείξεις, τότε θα γινόταν διακοπή της σύνδεσης του στο internet για ένα χρόνο, με απόφαση της νεοσύστατης αρχής. Μάλιστα ο χρήστης θα ήταν υποχρεωμένος να συνεχίσει να καταβάλλει την συνδρομή του στον πάροχο του, παρά την διακοπή της σύνδεσης.

Από την πρώτη στιγμή της παρουσίασης του νομοσχεδίου, υπήρξαν έντονες αντιδράσεις, τόσο από οργανισμούς για την υπεράσπιση των δικαιωμάτων των πολιτών, όσο και από συντηρητικούς βουλευτές της Γαλλίας, οι οποίοι χαρακτήρισαν τα μέτρα αυτά «δρακόντεια» και υπερβολικά.

Το νομοσχέδιο Hadopi ή αλλιώς ο νόμος των τριών χτυπημάτων, που φέρει το όνομα του από τα τρία στάδια προειδοποίησης των χρηστών που κατεβάζουν

παράνομα υλικό από το διαδίκτυο, φαίνεται πως υπακούει στην μοίρα του ονόματος του:

- Την πρώτη φορά που κατατέθηκε προς ψήφιση καταψηφίστηκε αιφνιδιαστικά στην Εθνοσυνέλευση, χαρίζοντας μια δυσάρεστη στιγμή για το κυβερνών κόμμα του Γάλλου Προέδρου αφού η καταψήφιση οφειλόταν σε απουσίες της κυβερνητικής κοινοβουλευτικής ομάδας.
- Την δεύτερη φορά υπερψηφίστηκε από τα αρμόδια νομοθετικά όργανα, αλλά ακυρώθηκε η βασική διάταξη στο Συνταγματικό Δικαστήριο. Οι Γάλλοι Ανώτατοι Δικαστικοί ευθυγραμμίστηκαν με το ψήφισμα του Ευρωπαϊκού Κοινοβουλίου όπως αυτό υιοθετήθηκε στις αρχές Μαΐου, σύμφωνα με το οποίο η πρόσβαση στο διαδίκτυο είναι θεμελιώδες ανθρώπινο δικαίωμα και πως για οποιαδήποτε επιβαλλόμενη διακοπή πρέπει να έχει προηγηθεί δικαστική διαδικασία μετά από σχετική ακρόαση.
- Είναι πλέον η τρίτη φορά που ο νόμος HADOPI έρχεται ενώπιον των γαλλικών νομοθετικών οργάνων.

Η απόφαση του Δικαστηρίου είχε ως αποτέλεσμα την επανεξέταση και αναθεώρηση του νομοσχεδίου από την κυβέρνηση της Γαλλίας. Σύμφωνα με το νέο νομοσχέδιο, η αρχή HADOPI θα μπορεί να παρακολουθεί και να συλλέγει στοιχεία για χρήστες που ανταλλάσουν παράνομα προστατευμένο υλικό μέσω internet και στην συνέχεια θα παραδίδει τα στοιχεία αυτά στη δικαιοσύνη.

Στη συνέχεια το δικαστήριο θα είναι σε θέση να υποβάλλει κυρώσεις στο χρήστη και πιο συγκεκριμένα θα μπορεί :

- Να διακόπτει την σύνδεση του χρήστη στο internet για ένα χρόνο, ή να υποβάλλει στον χρήστη πρόστιμο έως 300.000 ευρώ ή και ποινή φυλάκισης με ανώτατο όριο τα δύο χρόνια
- Να υποβάλλει πρόστιμο ως 1.500 ευρώ σε χρήστες που ηθελημένα, ή εν αγνοία τους, αφήνουν τρίτους να «κατεβάζουν» υλικό παράνομα μέσα από

την σύνδεση τους ή να διακόπτει την σύνδεση τους στο διαδίκτυο για ένα μήνα

Η νέα μορφή του νομοσχεδίου εγκρίθηκε από την Γερουσία και στη συνέχεια στις 22 Σεπτεμβρίου υπερψηφίστηκε και από την γαλλική βουλή με 258 ψήφους υπέρ και 131 ψήφους κατά.

Το σοσιαλιστικό κόμμα της Γαλλίας προσέφυγε για δεύτερη φορά στο Συνταγματικό Δικαστήριο, το οποίο όμως στις 22 Οκτωβρίου του 2009 ενέκρινε τελικά τον νέο νόμο, μετά τις αλλαγές που έγιναν στο νομοσχέδιο.

Ο νόμος, ο οποίος σήμερα είναι γνωστός με το όνομα HADOPI 2, η αλλιώς «νόμος των τριών χτυπημάτων», είχε προγραμματιστεί να τεθεί σε ισχύ από την πρωτοχρονιά του 2010. Παρόλα αυτά η ισχύς του νόμου έχει ανασταλεί προσωρινά, αφού η Εθνική Επιτροπή για την πληροφορική και τις θεμελιώδεις ελευθερίες της Γαλλίας (Commission nationale de l'informatique et des libertés - CNIL) αρνήθηκε να υπογράψει τα απαραίτητα έγγραφα που απαιτούνται, έτσι ώστε να αρχίσει η εφαρμογή του νόμου. Συγκεκριμένα, η αρχή ζήτησε από την κυβέρνηση της χώρας περισσότερες πληροφορίες σχετικά με τον τρόπο με τον οποίο η αρχή HADOPI θα παρακολουθεί και θα καταγράφει τις κινήσεις των χρηστών του internet, αλλά και τον τρόπο και τα μέσα με τα οποία θα αρχειοθετούνται αυτά τα στοιχεία.

Σκοπός της CNIL είναι να λάβει τις απαραίτητες διαβεβαιώσεις πως η συλλογή των στοιχείων θα γίνεται με τρόπο που δεν θα παραβιάζει τα δικαιώματα των χρηστών και πως θα εξασφαλίζεται η ιδιωτικότητα τους.

Παρά τις ποικίλες αντιδράσεις και τις δυσκολίες που αντιμετώπισε η γαλλική κυβέρνηση, τελικά ο νόμος HADOPI αποτελεί γεγονός και είναι πλέον θέμα χρόνου η έναρξη της ισχύος του. Ο υπερψήφιση του νόμου αποτελεί σημείο ορόσημο στην μακρόχρονη διαμάχη ανάμεσα στους δικαιούχους των πνευματικών δικαιωμάτων και τους υπέρμαχους της ελευθερίας της επικοινωνίας και του δικαιώματος στην ενημέρωση.

Είναι σχεδόν βέβαιο πως και άλλες χώρες θα ακολουθήσουν το παράδειγμα της Γαλλίας, επηρεαζόμενες μάλιστα και από τις πιέσεις που δέχονται από τις ενώσεις τις μουσικής και κινηματογραφικής βιομηχανίας. Ανεξάρτητα το πόσο επιτυχής θα κριθεί τελικά ο νόμος, είναι γεγονός πως με την ψήφιση του θα πρέπει να επανεξεταστεί και να αναπροσαρμοστεί και το καθεστώς της πνευματικής ιδιοκτησίας γενικότερα, αλλά και ειδικότερα, σε ο,τι αφορά το διαδίκτυο.

5.3 Digital Economy Bill

Ακολουθώντας την πολιτική της γαλλικής κυβερνήσεως, οι κυβερνήσεις άλλων κρατών μελών της Ευρωπαϊκής Ένωσης φαίνεται να είναι διατεθειμένες να παρουσιάσουν νομοσχέδια,τα οποία θα υιοθετούν τα πρότυπα του νόμου HADOPI, για την αποτροπή της προσβολής της πνευματικής ιδιοκτησίας μέσω του διαδικτύου. Στα μέσα του 2009, στο Ηνωμένο Βασίλειο, κατά την διάρκεια της Βασιλικής Ομιλίας στο κοινοβούλιο παρουσιάστηκε ένα νέο νομοσχέδιο γνωστό ως Digital Economy Bill.

Το νομοσχέδιο αυτό περιέχει ρυθμίσεις για πολλούς τομείς που περιλαμβάνουν την χρήση της τεχνολογίας και των ψηφιακών δεδομένων. Μεταξύ αυτών αναφέρεται πως η βρετανική κυβέρνηση θα λάβει τα απαραίτητα μέτρα, έτσι ώστε να εξασφαλιστεί η καθολική πρόσβαση στο διαδίκτυο μέσω ευρυζωνικής σύνδεσης σε όλους του κατοίκους της Μεγάλης Βρετανίας. Η δέσμευση αυτή είναι πολύ σημαντική, καθώς συμβαδίζει με την τάση της Ευρωπαϊκής Ένωσης σχετικά με το δικαίωμα της πρόσβασης στο διαδίκτυο. Παρόλα αυτά το νομοσχέδιο περιλαμβάνει και ένα αντικρουόμενο, στα παραπάνω, τμήμα, το οποίο αναφέρεται στην προσβολή της πνευματικής ιδιοκτησίας μέσω του διαδικτύου και περιλαμβάνει ένα προτεινόμενο μοντέλο για την καταπολέμηση της, το οποίο είναι επηρεασμένο από τον γαλλικό νόμο HADOPI. Συγκεκριμένα, προτείνει την αποστολή προειδοποιητικών μηνυμάτων στους χρήστες του διαδικτύου που ανταλλάσουν παράνομα προστατευμένο υλικό, την διακοπή της σύνδεσης αυτών οι οποίοι δεν

συμμορφώνονται παρά τις προειδοποιήσεις, αλλά και την επιβολή κυρώσεων, (όπως πρόστιμο και ποινή φυλάκισης) από τα δικαστήρια.

Επιπρόσθετα το νομοσχέδιο αυτό αναφέρει πως εάν αυτά τα μέτρα κριθούν αναποτελεσματικά, οι ISP θα υποχρεωθούν να παρακολουθούν την δραστηριότητα των πελατών τους και σε περίπτωση που ανιχνεύσουν παραβατική συμπεριφορά από μέρους τους, να παραδίδουν όλες τις καταγεγραμμένες πληροφορίες σε οργανώσεις προστασίας πνευματικών δικαιωμάτων.

Η ανακοίνωση του νομοσχεδίου προκάλεσε πολλές αντιδράσεις, κυρίως από οργανώσεις προστασίας προσωπικών δεδομένων. Ταυτόχρονα πολλοί αναλυτές εκφράζουν την ανησυχία τους, αφού όπως υποστηρίζουν το νομοσχέδιο δεν προτείνει, όπως θα έπρεπε, λύσεις για την βελτίωση της ευρυζωνικότητας και την διευκόλυνση της πρόσβασης σε αυτή ακόμα και από οικονομικά ασθενέστερους πολίτες, αλλά αντιθέτως προτείνει μόνο μέτρα για την τιμωρία των χρηστών του διαδικτύου που ανταλλάσουν προστατευόμενο υλικό.

Συμπεράσματα

Το Internet είχε αρχικά σχεδιαστεί να είναι ένα ανοικτό σύστημα όπου ο κάθε υπολογιστής θα μπορούσε να συνδεθεί με άλλον υπολογιστή και να επικοινωνούν. Όμως στη συνέχεια θέματα ασφάλειας καθώς και η υπερανάπτυξη του διαδικτύου, το οδήγησε να έχει τη μορφή πελάτης/ εξυπηρετητής (client/server). Το 1999 όμως το Napster άνοιξε το δρόμο για όλα τα P2P εργαλεία δικτύων ώστε να επιτύχουν την απευθείας σύνδεση δύο υπολογιστών. Αφότου έκλεισε ακολούθησαν μια σειρά από άλλα εργαλεία που πήραν τη θέση του καθώς και πολλές εφαρμογές πλέον με την λογική P2P.

Υπάρχουν δύο μεγάλες κατηγορίες αρχιτεκτονικών για τα P2P δίκτυα. Τα κεντρικοποιημένα και τα μη-κεντρικοποιημένα δίκτυα. Στις κεντρικοποιημένες αρχιτεκτονικές γίνετε χρήση ενός κεντρικού Server, με τον οποίο επικοινωνούν οι κόμβοι για να πάρουν πληροφορίες για το αντικείμενο που αναζητείται. Η αρχιτεκτονική αυτή είναι αρκετά αποδοτική αλλά δεν κάνει καλό scaling και έχει ενιαίο σημείο της αποτυχίας. Από την άλλη πλευρά έχουμε τις μη- κενρικοποιημένες αρχιτεκτονικές οι οποίες μπορεί να έχουν κάποια δομή ή να μην έχουν καμία δομή. Στις δομημένες μη-κεντρικοποιημένες αρχιτεκτονικές υπάρχει έλεγχος στην τοπολογία του δικτύου και καθώς και στη τοποθέτησης των αρχείων. Για τις αναζητήσεις σε αυτές χρησιμοποιείται συνήθως ένας κατανεμημένος πίνακας κατακερματισμού. Προσφέρουν αποδοτικές αναζητήσεις και κλιμακώνονται καλά αλλά δεν υπάρχουν τέτοια ευρέως διαδεδομένα δίκτυα έτσι ώστε να αποδειχθεί ότι μπορούν να δουλέψουν καλά. Στις αρχιτεκτονικές που δεν παρέχουν καμία δομή οι αναζητήσεις γίνονται με επερωτήσεις από τους κόμβους προς τους γείτονες τους, συνήθως χρησιμοποιώντας το πρωτόκολλο πλημμύρας. Η αρχιτεκτονική αυτή είναι εξαιρετικά ανεκτική σε αλλαγές στο δίκτυο αλλά δεν κλιμακώνεται καλά και δημιουργεί μεγάλα φορτία.

Ένα πολύ σημαντικό ζήτημα στα P2P συστήματα, όπως και γενικότερα σε κάθε τεχνολογία, εφαρμογή κλπ που προβλέπει επικοινωνία μεταξύ υπολογιστικών συστημάτων, είναι η ασφάλεια. Η ασφάλεια αφορά τόσο το επίπεδο της επικοινωνίας

μεταξύ των εμπλεκόμενων υπολογιστικών συστημάτων όσο και το επίπεδο των δεδομένων και του χρήστη. Όμως με τα καλύτερα πρωτόκολλα ασφάλειας αυτό θα μπορούσε να αποφευχθεί.

Ένα άλλο σημαντικό ζήτημα που προκύπτει από την χρήση των P2P είναι τα νομικά ζητήματα. Η ανταλλαγή προστατευμένων αρχείων με την χρήση δικτύων P2P, παρουσιάζει συνεχή αύξηση, με αποτέλεσμα οι δικαιούχοι συχνά να κινούνται νομικά, ολοένα και συχνότερα, εναντίων διανομέων προγραμμάτων P2P, διαχειριστών ιστοσελίδων αναζήτησης αρχείων torrent αλλά και απλών χρηστών τέτοιων προγραμμάτων. Η αντικρουόμενες όμως δικαστικές αποφάσεις καθιστούν φανερό πως η οριστική λύση του προβλήματος μπορεί να επέλθει μόνο μέσω της δημιουργίας συγκεκριμένων νομοθετικών ρυθμίσεων σε παγκόσμιο επίπεδο σχετικά με την ανταλλαγή αρχείων μέσω διαδικτύου. Προτάσεις όπως αυτή του Global License αλλά και πρωτοβουλίες όπως η ψήφιση του νόμου HADOPI και η παρουσίαση του νομοσχεδίου Digital Rights Bill θα είναι αυτές που θα καθορίσουν το ζήτημα αυτό, το οποίο όμως θα πρέπει να επιλυθεί με γνώμονα τον σεβασμό και τη μη παραβίαση των θεμελιωδών ανθρωπίνων δικαιωμάτων.

Πηγές

[1] Zhonchong Ou."Structuted P2P, Hierarchical Architrcture And Performance Evaluation". http://herkules.oulu.fi/isbn9789514262487/isbn9789514262487.pdf

[2] H. Balakrishnan, M. Frans Kaashoek, D. Karger, R. Morris, and I. Stoica,"Looking Up Data in P2P Systems".

[3] Ν. Κρεμμύδας, "Επισκόπηση στα Συστήματα Ομότιμων Κόμβων", Ε.Μ.Π., 2005.

[4] Σ.Μαργαρίτη, "Data Management in Peer`to`Peer Systems", Technical report, Πανεπιστήμιο Ιωαννίνων, 2005.

[5]JamesLi."ASurveyofPeertoPeerNetworkSecurityIssues".http://www.cs.wustl.edu/~jain/cse571-07/ftp/p2p.pdf. 2008.

[6] Φώτης Ι. Γώγουλος," Μελέτη και προσομοίωση αλγορίθμων αναζήτησης, μεταφοράς και διαφοροποίησης χρηστών σε εφαρμογές κοινής χρήσης αρχείων". 2007.

[7] Νίκος Σμυρναίος," Πνευματικά δικαιώματα, πολιτιστική βιομηχανία και διαδίκτυο". 2010.

[8] Βεσυρόπουλος Νικόλαος,"Peer to Peer και προστασία της πνευματικής ιδιοκτησίας".

[9] Δρ. Εμμανουήλ Μάγκος, Σημειώσεις Μαθήματος "Ασφάλεια Υπολογιστών και Προστασία Δεδομένων",2006.

[10] http://www.worldlingo.com/ma/enwiki/el/File_sharing#Legal_and_copyright_issues

[11] The World of Peer-to-Peer (P2P), http://en.wikibooks.org/wiki/The_World_of_Peer-to-Peer_(P2P)

[12] Peer-to-peer, http://el.wikipedia.org/wiki/Peer-to-peer

[13] The Pirate Bay, http://en.wikipedia.org/wiki/The_Pirate_Bay_raid

[14] Πνευματική ιδιοκτησία, http://el.wikipedia.org/wiki/ Πνευματική_ιδιοκτησία

[15] File & music sharing (Family Safety)
http://tech.lds.org/wiki/File_%26_music_sharing_(Family_Safety)