**ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ**

**Τμήμα Διδακτικής της Τεχνολογίας και Ψηφιακών Συστημάτων**

**Π.Μ.Σ Ψηφιακά Δίκτυα και Τηλεπικοινωνίες**


Μεταπτυχιακή Διπλωματική Εργασία

# Επιδημιολογικά μοντέλα διάδοσης ιομορφικού λογισμικού

Επιβλέπων καθηγητής: Σ. Κάτσικας

Ανδρικόπουλος Κων*/*νος

Πειραιάς **2009**

## Περιεχόμενα

## Λίστα Πινάκων

## Λίστα Σχημάτων

Η συγγραφή της παρούσας μεταπτυχιακής διπλωματικής εργασίας θα ήταν ανέφικτη χωρίς την αμέριστη υποστήριξη και συμπαράσταση από τους γονείς μου,

στους οποίους και την αφιερώνω.

**Ευχαριστίες**

Θερμές ευχαριστίες εκφράζω στον Καθηγητή κο. Κάτσικα Σωκράτη για την συνεχόμενη επίβλεψη και βοήθεια που μου παρείχε χωρίς την οποία θα ήταν αδύνατη η ολοκλήρωση της διπλωματικής μου εργασίας.

Ιδιαίτερες ευχαριστίες οφείλονται στον Επίκουρο Καθηγητή κο. Στέλιο Ζήμερα, για την καθοδήγηση, το υλικό καθώς και τις πολύτιμες συμβουλές που μου παρείχε, οι οποίες με οδήγησαν στην καλύτερη κατανόηση της επιστήμης της επιδημιολογίας.

Τέλος εκφράζω την ευγνωμοσύνη μου στους γονείς μου για την υποστήριξη και βοήθειά τους σε όλη τη διάρκεια των μεταπτυχιακών σπουδών μου.

# 1 Εισαγωγή

Κατά τη διάρκεια των τελευταίων δεκαετιών ιδίως μετά το **1981** έχει υπάρξει ένα ιδιαίτερο ενδιαφέρον για τους ιούς υπολογιστών. Θεωρείται ότι η κατανόηση των παραγόντων που επηρεάζουν την διάδοση των ιών στα τεχνολογικά δίκτυα (όπως το Διαδίκτυο, το **World Wide Web**, τα τηλεφωνικά δίκτυα, δίκτυα **IP**, κ.λπ....) θα οδηγήσει στην πρόταση χρήσιμων τρόπων για τον έλεγχό τους. Μέχρι τώρα, το πλήθος των μελετών έχει υιοθετήσει απλά επιδημιολογικά μοντέλα για να καταλάβουν τα γενικά χαρακτηριστικά της διάδοσης των ιών. Τα επιδημιολογικά μοντέλα έχουν χρησιμοποιηθεί παραδοσιακά για την κατανόηση αλλά και πρόβλεψη της έκβαση των ξεσπασμάτων των ιών στους ανθρώπινους **[93]** ή ζωικούς πληθυσμούς. Εντούτοις, τα ίδια πρότυπα εφαρμόζονται και στην ανάλυση των επιδημιών των υπολογιστών **[71]**.

Οι ομοιότητες που παρουσιάζουν μεταξύ τους οι βιολογικοί ιοί και οι ιοί υπολογιστών είναι πολλές **[85]** και μας οδηγούν τόσο στην βαθύτερη κατανόηση όσο και στον έλεγχό τους. Και οι δύο, βιολογικοί ιοί (ζωντανοί οργανισμοί φτιαγμένοι από **DNA** ή **RNA** μέσα σε ένα πρωτεϊνικό επίστρωμα) και ιοί υπολογιστών παρασιτούν στον οικοδεσπότη τους και μπορούν να αναπαραχθούν μόνο όταν είναι μέσα σε αυτόν. Οι βιολογικοί ιοί εισέρχονται στον οικοδεσπότη τους παθητικά μέσω ενός "ανοίγματος" μετά από μια εισπνοή, κατάποση ή μέσω άμεσης επαφής. Κατά αντιστοιχία οι ιοί των υπολογιστών εισέρχονται επίσης παθητικά στον οικοδεσπότη τους με την τοποθέτηση ενός μολυσμένου αποθηκευτικού μέσου όπως είναι ένας σκληρός δίσκος ή ένα **usb** ή με το άνοιγμα ενός μολυσμένου μηνύματος ηλεκτρονικού ταχυδρομείου. Άλλη μία κοινή παράμετρος είναι ότι τόσο οι βιολογικό ιοί όσο και οι ιοί υπολογιστών πρέπει να βρεθούν στον κατάλληλο οικοδεσπότη για να δράσουν έτσι όπως ένας ιός για γάτες δεν μπορεί να κάνει έναν άνθρωπο άρρωστο έτσι και ένας ιός για **MAC** δεν μπορεί να μολύνει ένα υπολογιστή που τρέχει **Linux**. Ομοιότητες παρουσιάζονται επίσης και στις συνέπειες που έχουν οι ιοί, όπου οι βιολογικοί ιοί αναπαράγονται σε βάρος του οικοδεσπότη προκαλώντας του αδυναμία, πόνο η ακόμα και θάνατο. Ομοίως οι ιοί υπολογιστών επιβραδύνουν τους υπολογιστές, κάνουν απρόσιτα ή παραλλάσουν τα αρχεία και τις υπηρεσίες τους ή ακόμα και τα/τις καταστρέφουν.

Όσον αφορά την διάδοσή τους και εκεί εμφανίζουν ομοιότητες. Τα δικτυακά σκουλήκια διαδίδονται χωρίς καμία αλληλεπίδραση μεταξύ των χρηστών όπως και οι κοινωνικά διαβιβαζόμενες ασθένειες (παραδείγματος χάρη η γρίπη), οι οποίες έχουν τη δυνατότητα να μολύνουν ευπαθείς ομάδες. Αντίθετα, οι ιοί υπολογιστών είναι όπως τις σεξουαλικά διαβιβασθείσες ασθένειες. Η διάδοσή τους (μέσω της

διανομής αρχείων και προγραμμάτων**)** είναι όπως τα **STDs,** του οποίου η διάδοση σχετίζεται με τις συγκεκριμένες πρακτικές συμπεριφοράς**.** Οι λογικές βόμβες είναι όπως το **HIV,** επειδή ενεργοποιούνται μόνο σε μια μεταγενέστερη ημερομηνία από αυτής της μόλυνσης**.**

Παρατηρώντας κανείς αυτές τις συσχετίσεις οι οποίες σε ένα μεγάλο βαθμό επηρεάζουν την διάδοση των ιών και κατ' επέκταση την μοντελοποίησή της είναι εύκολο να αντιληφθεί κανείς γιατί η επιδημιολογία η οποία αφορά κυρίως βιολογικούς οργανισμούς**,** αποδεικνύεται χρήσιμη για την αντιμετώπιση της εξάπλωσης του κακόβουλου λογισμικού**.**

Οι επιδημίες επηρέασαν και επηρεάζουν διαχρονικά την ανθρωπότητα επιφέροντας από δραστικές αλλαγές έως και ολικές ανατροπές του τρόπου ζωής των ανθρώπων **[128].** Η σοβαρότητα των συνεπειών τους ήταν φυσικό να προκαλέσει τον ενδιαφέρον του ανθρώπου από πολύ νωρίς**.** Τα θεμέλια της επιδημιολογίας σαν αυτόνομο επιστημονικό κλάδο**,** έθεσε το **400** π**.** Χ**.** ο Ιπποκράτης με την πραγματεία του 'Περί επιδημιών' **(**αν και διάφοροι ιστορικοί αμφισβητούν

ότι το σύνολο αυτού του έργου γράφτηκε μόνο από έναν άνθρωπο**).** Η επιδημιολογία γνώρισε καινούργιο ενδιαφέρον και ώθηση από το έργο του **John Graunt,** Φυσικές και Πολιτικές Παρατηρήσεις σχετικά με τους Ρυθμούς Θνησιμότητας **[51].** Στη συνέχεια πολλοί διακεκριμένοι επιστήμονες όπως οι **Daniel Bernoulli, Ronald Ross, Lowell Reed** και ο **Wade Hampton Frost** συνδύασαν την επιδημιολογία με τα μαθηματικά**,** δημιουργώντας ένα καινούργιο επιστημονικό κλάδο την Μαθηματική Επιδημιολογία**.** Η μεγαλύτερη συνεισφορά προήλθε από τους **William Ogilvy Kermack** και **Anderson Gray McKendrick [75],** οι οποίοι παρουσίασαν το Γενικό Επιδημιολογικό Μοντέλο **(General Epidemic Model).** Το βασικό πλεονέκτημα του Γενικού Επιδημιολογικού Μοντέλου είναι ότι μπορεί να περιγράψει ικανοποιητικά την εξέλιξη μιας επιδημίας με τη χρήση διαφορικών εξισώσεων**.**

Τις τελευταίες δεκαετίες η Μαθηματική Επιδημιολογία γνώρισε μεγάλη ανάπτυξη και μπόρεσε να συμπεριλάβει και άλλες πολλές παραμέτρους**,** δημιουργώντας ακριβέστερα μοντέλα για αρκετές ασθένειες που εμφανίζουν ιδιαιτερότητες στους πληθυσμούς που μολύνουν ή στο τρόπο εξάπλωσης τους**.** Οι σημαντικότερες εξελίξεις στο χώρο της Μαθηματικής Επιδημιολογίας αποτυπώνονται αναλυτικά στα συγγράμματα **[3,21,37,57],** ενώ οι βασικότερες αρχές της Επιδημιολογίας παρουσιάζονται επακριβώς στο σύγγραμμα του Τριχόπουλου **[121].** Το Γενικό Επιδημιολογικό Μοντέλο**,** το οποίο είναι γνωστό και ως **S-I-R (Susceptible-Infective-Recovered)** μπορεί με τις κατάλληλες παραδοχές να περιγράψει με μεγάλη ακρίβεια την εξάπλωση του κακόβουλου λογισμικού**.** Ο πρώτος που

χρησιμοποίησε τα επιδημιολογικά μοντέλα του **McKendrick** σε αυτόν το τομέα, υπήρξε ο **Kephart [67,68,70,71]** δημιουργώντας ουσιαστικά τον κλάδο της Επιδημιολογίας Υπολογιστών. Την εποχή την οποία ασχολήθηκε ο **Kephart** οι επιδημίες κακόβουλου λογισμικού δεν αποτελούσαν μεγάλη απειλή, λόγω του πρωτόγονου τρόπου εξάπλωσης των ιών που βασιζόταν στην ανταλλαγή δισκετών χέρι με χέρι. Για το λόγο αυτό η Επιδημιολογία Υπολογιστών δεν γνώρισε σημαντική εξέλιξη μέχρι τις αρχές του **2000**, καθώς οι ερευνητικές προσπάθειες για την αντιμετώπιση του επιβλαβούς λογισμικού είχανε εστιαστεί σε μικροσκοπικό επίπεδο, δηλαδή στην ανάλυση του επιζήμιου κώδικα. Αργότερα, με τα προβλήματα που προέκυψαν από τις επιδημίες κακόβουλου λογισμικού από διάφορα δικτυακά σκουλήκια, όπως τα **Code Redv2**, **Code Red II [45, 90,134,158]** και **Nimda [82,149,165,224]**, έγινε εμφανές ότι οι υπάρχοντες τρόποι προστασίας δεν επαρκούν. Ειδικότερα, ο **Staniford [115]** μελέτησε τις δυναμικές εξάπλωσης του κακόβουλου λογισμικού υπό το πρίσμα της επιδημιολογίας δίνοντας νέα ώθηση σε αυτό το χώρο. Τόσο οι δύο αυτές θεμελιώδεις έρευνες όσο και πολλές άλλες που ακολούθησαν, βασίζονται στο Γενικό Επιδημιολογικό Μοντέλο. Οι αντιστοιχίσεις και οι αναλογίες των βιολογικών μεγεθών που εμφανίστηκαν στο αρχικό μοντέλο σε έννοιες και μεγέθη, τα οποία είναι συμβατά με το κακόβουλο λογισμικό και την επιστήμη των υπολογιστών γενικότερα, είναι ζητήματα τα οποία ο κάθε ερευνητής καλύπτει σε κάποιο βαθμό αυθαίρετα με βάση τη κρίση του και τις παραδοχές που κάνει στα πειράματά του.

## 1.1 Ανάγκη για μοντελοποίηση

Η μοντελοποίηση της εξάπλωσης του κακόβουλου λογισμικού προσφέρει ουσιαστικά πλεονεκτήματα στην υλοποίηση αποτελεσματικών αμυντικών μηχανισμών. Το σημαντικότερο όφελος της μοντελοποίησης είναι ότι επιτρέπει τη δημιουργία μιας γενικότερης εποπτικής εικόνας, σχετικά με την εξάπλωση μορφών κακόβουλου λογισμικού. Επίσης σε αρκετές περιπτώσεις είναι εφικτό, εάν είναι γνωστά κάποια βασικά χαρακτηριστικά κάποιας μορφής κακόβουλου λογισμικού, να εκτιμηθεί η επικινδυνότητα του ή γενικότερα ο αριθμός των ευπαθών στόχων που αναμένεται να πλήξει. Συνήθως, χρησιμοποιείται για την εκ των υστέρων μελέτη διαφόρων επιδημιών κακόβουλου λογισμικού **[115,134]** και την ανασύνθεση

των γεγονότων που οδήγησαν σε αυτή. Επιπρόσθετα, είναι αρκετά συνηθισμένη η χρήση της μοντελοποίησης, για την πρόβλεψη της εξάπλωσης και των συνεπειών που είναι πιθανό να έχουν νέες μορφές κακόβουλου λογισμικού **[114,129]**.

## 1.2 Αντικείμενο

Το θέμα που πραγματεύεται η εν λόγο πτυχιακή εργασία είναι η μελέτη των επιδημιολογικών μοντέλων διάδοσης ιομορφικού λογισμικού η ανάλυσή τους καθώς επίσης και ο συσχετισμός τους με τα αντίστοιχα βιολογικά μοντέλα διάδοσης βιολογικών ιών. Για να μπορέσει να καταστεί κάτι τέτοιο δυνατό είναι αναγκαία η ανάλυση των συνιστωσών που επηρεάζουν την διαδικασία της διάδοσης. Εν γένει οι παράγοντες που επηρεάζουν την διάδοση κακόβουλου λογισμικού είναι:

- το δίκτυο που διαδίδεται δηλαδή ο τύπος, η αρχιτεκτονική και τα χρησιμοποιούμενα πρωτόκολλα
- τα μέτρα ασφαλείας που έχουν ληφθεί δηλαδή χρήση τοίχους προστασίας, αντιβιοτικών προγραμμάτων, συστημάτων ανίχνευσης επιθέσεων κ.τλ
- το ίδιο το κακόβουλο λογισμικό δηλαδή η πύλη εισόδου του, η στρατηγική επιλογής νέων στόχων και η μολυσματικότητα του.

οι οποίοι και αναλύονται σε βάθος στα σχετικά κεφάλαια. Όλοι αυτοί οι παράγοντες συνθέτουν ένα πολύπλοκο περιβάλλον διάδοσης το οποίο μπορεί να μοντελοποιηθεί επαρκώς και να προσομοιωθεί με την χρήση κατάλληλων διαφορικών εξισώσεων οδηγώντας σε ευρέως χρησιμοποιούμενα μοντέλα όπως είναι το **SIS (Susceptible Infected Susceptible)**

## 1.3 Δομή διπλωματικής

Στο πρώτο κεφάλαιο μελετώνται τα τοπικά δίκτυα υπό το πρίσμα της αρχιτεκτονικής, της τοπολογίας καθώς και των χρησιμοποιούμενων πρωτοκόλλων δίνοντας έμφαση το υποεπίπεδο ελέγχου πρόσβασης στο μέσο **(MAC)**.

Στο δεύτερο κεφάλαιο αναλύονται οι τεχνικές ασφάλειας που εφαρμόζονται στα δίκτυα παραθέτοντας μεταξύ των άλλων πιθανά ευπαθή σημεία, πολιτικές ασφαλείας, συστήματα ανίχνευσης εισβολών, την λειτουργία των τοίχων προστασίας, χρησιμοποιούμενα πρωτόκολλα **(IPsec)** και άλλα.

Στο τρίτο κεφάλαιο γίνεται μια εκτενή αναφορά στα κακόβουλα λογισμικά, κατηγοριοποιώντας τα και μελετάμε τις τεχνικές της διάδοσής τους, τον τρόπο λειτουργίας τους καθώς επίσης και τεχνικές ανίχνευσης και καταστολής τους.

Στο τέταρτο κεφάλαιο παρουσιάζονται μερικά από τα επικρατέστερα μοντέλα διάδοσης ιομορφικού λογισμικού καθώς επίσης και τα αντίστοιχα επιδημιολογικά μοντέλα διάδοσης βιολογικών ιών παρουσιάζοντας έτσι τον άμεσο συσχετισμό τους.

Τέλος στο πέμπτο κεφάλαιο παρουσιάζεται αναλυτικά το **SIDR** μοντέλο διάδοσης καθώς επίσης και τα αποτελέσματα που έχουν προκύψει από τις προσομοιώσεις αυτού.

# 2 Τοπικά δίκτυα

## 2.1 Τι είναι Δίκτυο Υπολογιστών

Ένα δίκτυο υπολογιστών είναι ένα σύστημα επικοινωνίας δεδομένων που συνδέει δύο ή περισσότερους αυτόνομους και ανεξάρτητους υπολογιστές ή ανεξάρτητες περιφερειακές συσκευές **[89].** Δύο υπολογιστές θεωρούνται διασυνδεδεμένοι όταν μπορούν να ανταλλάσσουν μεταξύ τους πληροφορίες.

## 2.2 Σκοπός των Δικτύων

Τα δίκτυα δημιουργήθηκαν για να εξυπηρετήσουν τις ανάγκες που προέκυψαν από την εξάπλωση της χρήσης των υπολογιστών. Βασικός σκοπός της ύπαρξης των δικτύων είναι ο διαμερισμός των πόρων του συστήματος και η ανταλλαγή πληροφοριών κάθε μορφής **(**προγράμματα, αρχεία, δεδομένα**).** Πόροι του συστήματος μπορούν να είναι είτε υλικό **(hardware),** π.χ. υπολογιστές, εκτυπωτές, **plotters,** σκληροί δίσκοι, είτε λογισμικό **(software),** π.χ. δεδομένα, προγράμματα εφαρμογών, υπηρεσίες. Τα προγράμματα, τα δεδομένα και οι συσκευές **(**σκληροί δίσκοι, εκτυπωτές, κλπ**)** είναι διαθέσιμα σε οποιονδήποτε είναι συνδεδεμένος στο δίκτυο, ανεξάρτητα από τη φυσική του θέση. Με τον τρόπο αυτό επιτυγχάνεται εξοικονόμηση χρημάτων, αύξηση της απόδοσης του συστήματος, κεντρικός έλεγχος και εύκολη επεκτασιμότητα. Σε ένα δίκτυο μπορούμε να έχουμε ανταλλαγή δεδομένων, προγραμμάτων, χρήση κοινών βάσεων δεδομένων, αρχείων, αποστολή μηνυμάτων **(electronic mail).** Επιπλέον, ανεξάρτητα της τεχνολογίας, ένα δίκτυο είναι ένα πανίσχυρο μέσο επικοινωνίας ανθρώπων που βρίσκονται σε διαφορετικά μέρη.

## 2.3 Είδη Δικτύων

**Ι. Με βάση την γεωγραφική ανάπτυξη διακρίνονται σε:**

**Δίκτυα ευρείας περιοχής (Wide Area Networks, WAN) [101],** που καλύπτουν αποστάσεις μερικών χιλιομέτρων **(**συνήθως άνω των **5 km)** στην ίδια πόλη, μέχρι χιλιάδων χιλιομέτρων σε διαφορετικές πόλεις - κράτη - ηπείρους. Αποτελούνται από υπολογιστές, τηλεπικοινωνιακές συσκευές και γραμμές. Παραδείγματα τέτοιων δικτύων είναι τα δίκτυα των αεροπορικών εταιρειών,. τα τραπεζικά δίκτυα, τα δημόσια δίκτυα δεδομένων κλπ.

**Δίκτυα μικρών αποστάσεων ή τοπικά δίκτυα (Local Area Networks, LAN) [118]** που καλύπτουν μικρές αποστάσεις **(**μερικών εκατοντάδων μέτρων ή λίγων χιλιομέτρων**)** και περιορίζονται στα πλαίσια μιας επιχείρησης. Ο διαχωρισμός τους

από τα δίκτυα ευρείας περιοχής οφείλεται στο ότι χρησιμοποιούν διαφορετικές τεχνικές λειτουργίας.

**Αστικά Δίκτυα (Metropolitan Area Networks,** MAN**) [136],** που καλύπτουν δίκτυα που δεν ξεπερνούν τα σύνορα μιας πόλης. Είναι ταχύτερα από τα τοπικά δίκτυα και μπορούν να μεταδίδουν εικόνα, φωνή και δεδομένα αποδοτικότερα.

**ΙΙ. Με βάση τον τηλεπικοινωνιακό φορέα εξυπηρέτησης διακρίνονται σε:**

**Ιδιωτικά δίκτυα (Private Networks).** Ανήκουν εξ ολοκλήρου σε ιδιωτικούς οργανισμούς και χρησιμοποιούν είτε αποκλειστικές γραμμές επικοινωνίας δημόσιων τηλεπικοινωνιακών φορέων **(leased lines)** χωρίς να τις μοιράζονται με άλλους χρήστες ή ιδιόκτητες γραμμές επικοινωνίας.

**Δημόσια δίκτυα (Public Networks)** που εξυπηρετούν τις διασυνδέσεις μεταξύ απομακρυσμένων σημείων. Χρησιμοποιούνται όταν η απόσταση είναι μεγάλη και καθίσταται απαγορευτική, λόγω κόστους, η χρήση αποκλειστικών γραμμών ή όταν ο φόρτος μεταξύ των σημείων δεν είναι μεγάλος και επιτυγχάνεται έτσι μεγάλη ταχύτητα μεταφοράς.

**ΙΙΙ. Με βάση την τεχνική προώθησης της πληροφορίας διακρίνονται σε:**

**Δίκτυα μεταγωγής και Δίκτυα Ακρόασης**.

## 2.4 Ιστορική αναδρομή

Το σημερινό **Internet** αποτελεί εξέλιξη του **ARPANET [108],** ενός δικτύου που άρχισε να αναπτύσσεται πειραματικά στα τέλη της δεκαετίας του **60** στις ΗΠΑ.

### 2.4.1 Δεκαετία '60: ένα ενδιαφέρον πείραμα ξεκινά

Στα πανεπιστήμια των ΗΠΑ οι ερευνητές ξεκινούν να πειραματίζονται με τη διασύνδεση απομακρυσμένων υπολογιστών μεταξύ τους. Το δίκτυο **ARPANET** γεννιέται το **1969** με πόρους του προγράμματος **ARPA (Advanced Research Project Agency)** του Υπουργείου Άμυνας, με σκοπό να συνδέσει το Υπουργείο με στρατιωτικούς ερευνητικούς οργανισμούς αποτελώντας ένα πείραμα για τη μελέτη της αξιοπιστίας των δικτύων. Στην αρχική του μορφή, το πρόγραμμα απέβλεπε στον πειραματισμό με μια νέα τεχνολογία γνωστή σαν μεταγωγή πακέτων **(packet switching),** σύμφωνα με την οποία τα προς μετάδοση δεδομένα κόβονται σε πακέτα και πολλοί χρήστες μπορούν να μοιραστούν την ίδια επικοινωνιακή γραμμή. Στόχος ήταν η δημιουργία ενός διαδικτύου που θα εξασφάλιζε την επικοινωνία μεταξύ απομακρυσμένων δικτύων, έστω και αν κάποια από τα ενδιάμεσα συστήματα βρίσκονταν προσωρινά εκτός λειτουργίας. Κάθε πακέτο θα είχε την πληροφορία που χρειάζονταν για να φτάσει στον προορισμό του, όπου και θα γινόταν η

ανασύνθεση του σε δεδομένα τα οποία μπορούσε να χρησιμοποιήσει ο τελικός χρήστης. Το παραπάνω σύστημα θα επέτρεπε σε υπολογιστές να μοιράζονται δεδομένα και σε ερευνητές να υλοποιήσουν το ηλεκτρονικό ταχυδρομείο.

### 2.4.2 Δεκαετία '70: οι πρώτες συνδέσεις

Το **1973**, ξεκινά ένα νέο ερευνητικό πρόγραμμα που ονομάζεται **Internetting Project (**Πρόγραμμα Διαδικτύωσης**)** προκειμένου να ξεπεραστούν οι διαφορετικοί τρόποι διακίνησες δεδομένων μέσα από χρήση δικτύων. Στόχος ήταν η διασύνδεση ανόμοιων δικτύων και η ομοιόμορφη διακίνηση δεδομένων από το ένα δίκτυο στο άλλο. Από την έρευνα γεννιέται μια νέα τεχνική, το **Internet Protocol (IP) [63] (**Πρωτόκολλο Διαδικτύωσης**),** από την οποία θα πάρει αργότερα το όνομά του το **Internet.** Διαφορετικά δίκτυα που χρησιμοποιούν το κοινό πρωτόκολλο **IP** μπορούν να συνδέονται και να αποτελούν ένα διαδίκτυο. Σε ένα δίκτυο **IP** όλοι οι υπολογιστές είναι ισοδύναμοι, οπότε οποιοσδήποτε υπολογιστής του διαδικτύου μπορεί να επικοινωνεί με οποιονδήποτε άλλον. Επίσης, σχεδιάζεται μια άλλη τεχνική για τον έλεγχο της μετάδοσης των δεδομένων, το **Transmission Control Protocol (TCP)[63] (**Πρωτόκολλο Ελέγχου Μετάδοσης**).** Ορίζονται προδιαγραφές για τη μεταφορά αρχείων μεταξύ υπολογιστών **(FTP)** και για το ηλεκτρονικό ταχυδρομείο **(E-mail).** Σταδιακά συνδέονται με το **ARPANET** ιδρύματα από άλλες χώρες, με πρώτα το **University College of London (**Αγγλία**)** και το **Royal Radar Establishment (**Νορβηγία**).**

### 2.4.3 Δεκαετία '80: ένα παγκόσμιο δίκτυο για την ακαδημαϊκή κοινότητα

Το **1983**, το πρωτόκολλο **TCP/IP (**δηλ. ο συνδυασμός των **TCP** και **IP)** αναγνωρίζεται ως πρότυπο από το Υπουργείο Άμυνας των ΗΠΑ. Η έκδοση του λειτουργικού συστήματος **Berkeley UNIX** το οποίο περιλαμβάνει το **TCP/IP** συντελεί στη γρήγορη εξάπλωση της δικτύωσης των υπολογιστών μέσω διαδικτύου. Εκατοντάδες Πανεπιστήμια συνδέουν τους υπολογιστές τους στο **ARPANET,** το οποίο επιβαρύνεται πολύ και το **1983,** χωρίζεται σε δύο τμήματα: στο **MILNET (**για στρατιωτικές επικοινωνίες**)** και στο νέο **ARPANET (**για χρήση αποκλειστικά από την πανεπιστημιακή κοινότητα και συνέχιση της έρευνας στη δικτύωση**).** Το **1985,** το **National Science Foundation (NSF)** δημιουργεί ένα δικό του γρήγορο δίκτυο, το **NSFNET** χρησιμοποιώντας το πρωτόκολλο **TCP/IP,** προκειμένου να συνδέσει πέντε κέντρα υπερ-υπολογιστών μεταξύ τους και με την υπόλοιπη επιστημονική κοινότητα. Στα τέλη της δεκαετίας του **'80,** όλο και περισσότερες χώρες συνδέονται στο **NSFNET (**Καναδάς, Γαλλία, Σουηδία, Αυστραλία, Γερμανία, Ιταλία, κ.α.**).** Χιλιάδες πανεπιστήμια και οργανισμοί δημιουργούν τα δικά τους δίκτυα και τα

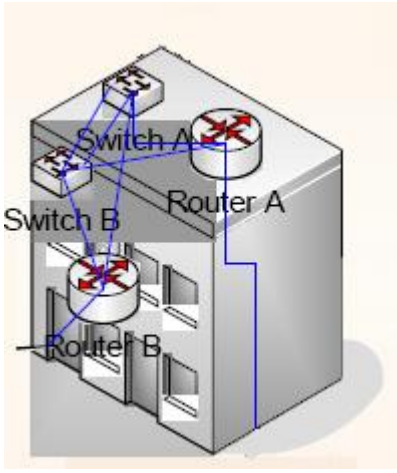
συνδέουν πάνω στο παγκόσμιο αυτό δίκτυο το οποίο αρχίζει να γίνεται γνωστό σαν **INTERNET** και να εξαπλώνεται με τρομερούς ρυθμούς σε ολόκληρο τον κόσμο. Το **1990,** το **ARPANET** πλέον καταργείται.

### 2.4.4 Δεκαετία '90: ένα παγκόσμιο δίκτυο για όλους

Όλο και περισσότερες χώρες συνδέονται στο **NSFNET,** μεταξύ των οποίων και η Ελλάδα τ**ο 1990.** Το **1993,** το εργαστήριο **CERN** στην Ελβετία παρουσιάζει το **World Wide Web (WWW) (**Παγκόσμιο Ιστό**)** που αναπτύχθηκε από τον **Tim Berners-Lee.** Πρόκειται για ένα σύστημα διασύνδεσης πληροφοριών σε μορφή πολυμέσων **(multimedia)** που βρίσκονται αποθηκευμένες σε χιλιάδες υπολογιστές του **Internet** σε ολόκληρο τον κόσμο και παρουσίασής τους σε ηλεκτρονικές σελίδες**,** στις οποίες μπορεί να περιηγηθεί κανείς χρησιμοποιώντας περιφερειακά μέσα**.** Το γραφικό αυτό περιβάλλον έκανε την εξερεύνηση του **Internet** εφικτή από τον απλό χρήστη**.** Παράλληλα**,** εμφανίζονται στο **Internet** διάφορα εμπορικά δίκτυα που ανήκουν σε εταιρίες παροχής υπηρεσιών **Internet (Internet Service Providers - ISP)** και προσφέρουν πρόσβαση σε όλους**.** Οποιοσδήποτε διαθέτει **PC** και **modem** μπορεί να συνδεθεί στο **Internet** σε τιμές που διαρκώς μειώνονται**.** Το **1995,** το **NSFNET** καταργείται πλέον επίσημα και το φορτίο του μεταφέρεται σε εμπορικά δίκτυα**.** Η ανακάλυψη του **WWW** σε συνδυασμό με την ευκολία απόκτησης πρόσβασης στο **Internet** προσέλκυσε έναν μεγάλο αριθμό καινούργιων χρηστών και έφερε την **"**έκρηξη**"** που παρακολουθούμε τα τελευταία χρόνια**.** Παρατηρούμε ότι καθημερινά περιοδικά και εφημερίδες εκδίδονται **"on-line"** και μας παραπέμπουν στις διευθύνσεις τους**,** επιχειρήσεις και ιδιώτες φτιάχνουν τις δικές τους σελίδες στο **WWW,** κλπ**.** Είναι προφανές ότι το **Internet** δεν αποτελεί πλέον ένα δίκτυο των φοιτητών και των ερευνητών**,** αλλά ότι επεκτείνεται και επιδρά στις καθημερινές πρακτικές όλων μας**.** Ήδη μιλάμε για ηλεκτρονικό εμπόριο**,** τηλεεργασία**,** τηλεκπαίδευση**,** τηλεϊατρική**,** κλπ**.** μέσα από το **Internet.**

## 2.5 Τοπικά δίκτυα (LAN)

Τα Τοπικά Δίκτυα Υπολογιστών **(LAN - Local Area Network) [118],** είναι δίκτυα επικοινωνίας σχεδιασμένα να υποστηρίζουν την διασύνδεση διαφόρων υπολογιστών και περιφερειακών συσκευών μέσα σε μια σχετικά μικρή περιοχή **(**π**.**χ**.** από ένα γραφείο μέχρι ένα συγκρότημα κτηρίων**,** Σχήμα **1).**




**Σχήμα 1. Τοπικό δίκτυο (LAN)**

Η εφαρμογή των **LANs** έχει ως στόχο την διευκόλυνση της άμεσης επικοινωνίας **(**σύγχρονη μορφή επικοινωνίας**),** την μεταφορά της πληροφορίας σε ελάχιστο χρόνο **(**ασύγχρονή μορφή επικοινωνίας**),** καθώς και την δυνατότητα χρησιμοποίησης όλων των πόρων που είναι διαθέσιμοι από τους χρήστες. Τα βασικά πλεονεκτήματα που παρουσιάζουν είναι **[89**,**118] :**

α**)** Διαμοιρασμός των ψηφιακών πόρων του συστήματος, δηλαδή προγραμμάτων, φακέλων, αρχείων κ.λπ. Αυτό πρακτικά σημαίνει ότι συγκροτείται ένας εικονικός κοινόχρηστος χώρος, όπου όλοι οι χρήστες, ανάλογα και με τα προνόμια - δικαιώματα που τους έχουν δοθεί από το διαχειριστή του δικτύου, έχουν πρόσβαση από τον υπολογιστή τους και μπορούν να χρησιμοποιούν τα ίδια αρχεία, τους ίδιους φακέλους και τις ίδιες εφαρμογές, ανεξάρτητα από το ποιος έχει δημιουργήσει το αρχείο ή σε ποιον υπολογιστή έχει εγκατασταθεί η εφαρμογή. Η δυνατότητα αυτή εξοικονομεί πολύτιμο χρόνο, καθώς οι χρήστες δεν χρειάζεται να αντιγράφουν σε δισκέτες, **CD**, **DVD** ή φορητές μνήμες τα αρχεία που θέλουν να μεταφέρουν από τον έναν υπολογιστή στον άλλο. Πλέον, αρκεί η είσοδος στον υπολογιστή τους. Στο ίδιο πλαίσιο, προκειμένου ένα πρόγραμμα να χρησιμοποιείται από όλους, αρκεί η εγκατάστασή του μία φορά και μόνο.

β**)** Κοινή χρήση περιφερειακών συσκευών. Αρκεί μία συσκευή από το κάθε είδος, η οποία θα χρησιμοποιείται από όλους. Η δυνατότητα αυτή μεταφράζεται ξεκάθαρα σε εξοικονόμηση κεφαλαίων αλλά και χώρου.

γ**)** Διαμοιρασμός μιας σύνδεσης **Internet** σε όλους τους υπολογιστές του δικτύου. Αυτό σημαίνει ότι η ύπαρξη μιας και μοναδικής σύνδεσης με το Διαδίκτυο αρκεί για να παράσχει πρόσβαση σε όλους τους υπολογιστές του τοπικού δικτύου. Η δυνατότητα αυτή μειώνει σημαντικά το κόστος σύνδεσης και παροχής **Internet**, αυξάνοντας παράλληλα την ασφάλεια.

δ) Αξιοποίηση υπολογιστών περιορισμένων δυνατοτήτων ή παλαιότερης τεχνολογίας. Αυτό σημαίνει ότι υπολογιστές που ως αυτόνομες μονάδες δεν μπορούσαν να χρησιμεύσουν σε κάτι αξιόλογο (λ.χ. επειδή δεν διέθεταν συσκευή ανάγνωσης **CD-ROM** ή επειδή ο σκληρός τους δίσκος είχε περιορισμένο αποθηκευτικό χώρο), μπορούν τώρα να ενταχθούν σε ένα μικρό δίκτυο και να παίξουν κάποιο ρόλο μέσα σ' αυτό.

Συμπερασματικά, η υλοποίηση ενός τοπικού δικτύου αποφέρει υπολογίσιμα οικονομικά, οργανωτικά, λειτουργικά και χωροταξικά οφέλη.

### 2.5.1 Ιστορική αναδρομή

Το **1970** (έως και το **1984**) έκαναν την εμφάνισή τους τα τοπικά δίκτυα υπολογιστών πρώτης γενιάς. Τα δίκτυα αυτά χαρακτηρίζονταν από τη χρησιμοποίηση τεχνολογιών εκπομπής **(broadcasting)** και περιλάμβαναν περισσότερους από έναν σταθμούς οι οποίοι εξέπεμπαν δεδομένα μέσα από ένα και μοναδικό μέσο μετάδοσης, κοινό για όλους τους σταθμούς. Η μέθοδος πρόσβασης των σταθμών στο μέσο μετάδοσης, στηριζόταν στη χρήση πρωτοκόλλων **[118]**, τα οποία λειτουργούσαν είτε με τη μέθοδο του ανταγωνισμού **(contention protocols)** (πρότυπο **802.3**) είτε με τη μέθοδο της διαιτησίας η οποία οδηγεί σε εκπομπή χωρίς συγκρούσεις **(collision free protocols)** (πρότυπα **802.4** και **802.5**) . Τα δίκτυα αυτής της γενιάς ήταν κατάλληλα για μετάδοση μόνο δεδομένων, με ρυθμούς που δεν υπερέβαιναν τα **20Mbps** και για αποστάσεις μικρότερες των **50 Km**. Ένα επιπρόσθετο χαρακτηριστικό αυτών των δικτύων είναι ότι λειτουργούσαν με τη μέθοδο του ανταγωνισμού και έτσι θα έπρεπε να διασφαλίζεται η αρχή της ισομοιρίας **(fair share)** που δίνει τη δυνατότητα σε κάθε κόμβο να έχει τις ίδιες ευκαιρίες με τους υπόλοιπους όσον αφορά τη δέσμευση του καναλιού.

Η δεύτερη γενιά τοπικών δικτύων **(1985-1990)**, χαρακτηρίζεται από την περαιτέρω εξέλιξη της τεχνολογίας μεταγωγής πακέτων **(packet switching)** του προτύπου **IEEE 802.5** καθώς και από την ανάπτυξη νέων τεχνολογιών, προκειμένου να εξασφαλιστεί μεγαλύτερη διαθέσιμη χωρητικότητα στις εφαρμογές. Αυτά τα δίκτυα επιτρέπουν τη μετάδοση μόνο δεδομένων, αλλά με ταχύτητες που φτάνουν τα **155 Mbps**, και χρησιμοποιούνται ως κορμός στη διασύνδεση των τοπικών δικτύων με άλλα τοπικά δίκτυα, και άλλα δίκτυα ευρείας περιοχής. Παραδείγματα προτύπων τοπικών δικτύων δεύτερης γενιάς, είναι τα δίκτυα διεπαφής κατανεμημένων δεδομένων με οπτική ίνα **(FDDI I** και **FDDI II) [62]** που είχαν και τη μεγαλύτερη ζήτηση σε σχέση με άλλες τοπολογίες που αναπτύχθηκαν στο ίδιο χρονικό διάστημα.

Η τρίτη γενιά τοπικών δικτύων χαρακτηρίζεται από την περαιτέρω εξέλιξη της τεχνολογίας μεταγωγής πακέτων του προτύπου **802.3,** καθώς και από την ανάπτυξη νέων τεχνολογιών προκειμένου να εξασφαλιστεί μεγαλύτερη διαθέσιμη χωρητικότητα από αυτή των **150Mbps** των δικτύων της προηγούμενης γενιάς. Παραδείγματα προτύπων τοπικών δικτύων αυτής της γενιάς, είναι **Fast Ethernet,** το **ISO-Ethernet,** το **100Base-VGAnyLAN** και το **Gigabit Ethernet [24,61,118].**

Τέλος, από το **1990** και μετά γίνονται προσπάθειες για την ανάπτυξη δικτύων νέας γενιάς που βασίζονται σε νέες τεχνολογίες, όπως είναι η **ATM (Asynchronous Transfer Mode) [42,79]** καθώς και η τεχνική της εξομοίωσης τοπικών δικτύων **(LAN Emulation).**

### 2.5.2 Χαρακτηριστικά των Τοπικών Δικτύων

Βασικά χαρακτηριστικά των Τοπικών Δικτύων είναι **[89,118,136]:**

- **Ø** Η ύπαρξη ενός κοινού επικοινωνιακού μέσου, μέσω του οποίου όλοι οι σταθμοί εργασίας των χρηστών μπορούν να μοιράζονται πληροφορίες, προγράμματα και συσκευές, ανεξάρτητα από την φυσική θέση των χρηστών ή των συσκευών.

- **Ø** Οι υψηλοί ρυθμοί μεταφοράς δεδομένων **(**της τάξεως των **Mbps** καθώς και των **Gbps).**

- **Ø** Η περιορισμένη γεωγραφική απόσταση που καλύπτουν, που συνήθως δεν υπερβαίνει μερικές εκατοντάδες μέτρα.

- **Ø** Ο χαμηλός ρυθμός σφαλμάτων **($10^{-8}$ - $10^{-11}$).**

- **Ø** Το γεγονός ότι είναι ιδιόκτητα, χαρακτηριστικό που τα διαφοροποιεί από άλλα επικοινωνιακά συστήματα τα οποία είναι δημόσια και υπάγονται σε διαφορετικά κανονιστικά πλαίσια.

### 2.5.3 Τύποι Τοπικών Δικτύων

Τα **LANs** γίνονται πιο εύκολα κατανοητά όταν αναλυθούν στις φυσικές τους συνιστώσες. Συνήθως αυτές οι συνιστώσες κατανέμονται σε διάφορα επίπεδα, σύμφωνα με το Μοντέλο Αναφοράς Διασύνδεσης Ανοικτών Συστημάτων **(OSI RM - Open System Interconnect Reference Model) [63,118].**

Δύο πολύ σημαντικές συνιστώσες που χαρακτηρίζουν τα Τοπικά Δίκτυα αποτελούν:

α**)** το μέσο μετάδοσης που χρησιμοποιούν **(**διάφοροι τύποι καλωδίων, οπτικές ίνες, ασύρματες επικοινωνίες**)** καθώς και

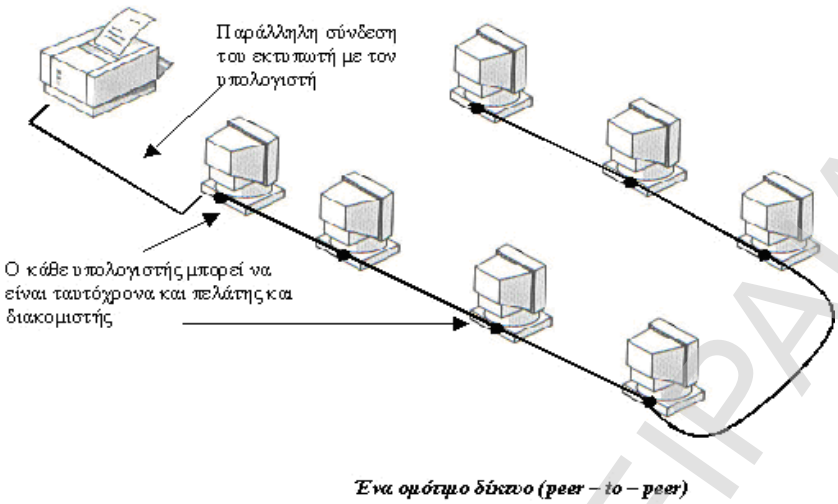
β**)** η τοπολογία του δικτύου.

Η τοπολογία ενός Τοπικού Δικτύου αναφέρεται στην φυσική διάταξη των συσκευών διασύνδεσης και της συνδεσμολογίας τους. Οι δύο πιο σημαντικές οντότητες είναι οι **clients** και οι **servers.** Ένας **server** είναι κάθε συνδεδεμένος υπολογιστής που μπορεί να "φιλοξενήσει" πόρους οι οποίοι διαμοιράζονται από άλλες συσκευές οι οποίες είναι συνδεδεμένες πάνω στο Τοπικό Δίκτυο. Ένας **client** είναι οποιοσδήποτε υπολογιστής που μπορεί να προσπελάσει τους πόρους οι οποίοι αποθηκεύονται στους **servers,** μέσω του **LAN.**

Ο τύπος δικτύου αντιπροσωπεύει την διάταξη με την οποία οι συνδεδεμένες συσκευές σε αυτό μπορούν να προσπελαστούν. Οι πόροι του δικτύου μπορούν να είναι: πελάτες **(clients),** εξυπηρετητές **(servers),** ή κάθε συσκευή, αρχεία κλπ. τα οποία βρίσκονται στους **clients** ή στους **servers.** Αυτοί οι πόροι μπορούν να προσπελαστούν με έναν από τους δύο τρόπους: σημείο-προς-σημείο **(peer-to-peer) [109][110]** ή μέσω κάποιου εξυπηρετητή **(server-based) [118].**

**Σημείο-προς-σημείο δίκτυα (peer-to-peer)**

Ένα δίκτυο υπολογιστών **peer-to-peer (**ή **P2P)** είναι ένα δίκτυο που επιτρέπει σε δύο ή περισσότερους υπολογιστές να μοιράζονται τους πόρους τους ισοδύναμα. Το δίκτυο αυτό χρησιμοποιεί την επεξεργαστική ισχύ, τον αποθηκευτικό χώρο και το εύρος ζώνης **(bandwidth)** των κόμβων ομότιμα. Όλοι οι κόμβοι του δικτύου έχουν ίσα δικαιώματα. Πληροφορίες που βρίσκονται στον ένα κόμβο, ανάλογα με τα δικαιώματα που καθορίζονται, μπορούν να διαβαστούν από όλους τους άλλους και αντίστροφα. Ένα σημείο-προς-σημείο δίκτυο υποστηρίζει μία αδόμητη μορφή προσπέλασης στους συνδεόμενους σε αυτό πόρους. Κάθε συσκευή σε ένα **peer-to-peer** δίκτυο μπορεί να είναι ταυτόχρονα πελάτης και εξυπηρετητής. Όλες οι συσκευές του δικτύου είναι ικανές να προσπελάσουν τα δεδομένα, το λογισμικό και τους άλλους πόρους του δικτύου άμεσα. Επομένως κάθε υπολογιστής στο δίκτυο είναι ισάξιος με κάθε άλλο υπολογιστικό σύστημα στο δίκτυο. Δεν υπάρχει δηλαδή ιεραρχία **(**Σχήμα **2).**




**Σχήμα 2. Αρχιτεκτονική P2P**

Τα **Peer-to-Peer** δίκτυα χωρίζονται σε τρεις κατηγορίες **[109,110]:**

ο Συγκεντρωτικά **P2P** δίκτυα γνωστά και ως **«**πρώτης γενιάς **P2P** δίκτυα**».** Σ' αυτή την αρχιτεκτονική υπάρχει ένας κεντρικός **Index Server** στον οποίο αποθηκεύονται οι πληροφορίες για τα περιεχόμενα των καταλόγων που οι συμμετέχοντες επιθυμούν να μοιράζονται**.** Οι χρήστες μπορούν να αναζητήσουν στους **Index Servers** τα αρχεία που ψάχνουν**,** χρησιμοποιώντας ένα κατάλληλο πρόγραμμα**-**πελάτη**.** Όταν το αρχείο βρεθεί**,** πραγματοποιείται μια σύνδεση μεταξύ των δύο χρηστών για τη μεταφορά του**.** Σ' αυτή τη κατηγορία ανήκουν το **Napster** το **DC++** και το **WinMX.**

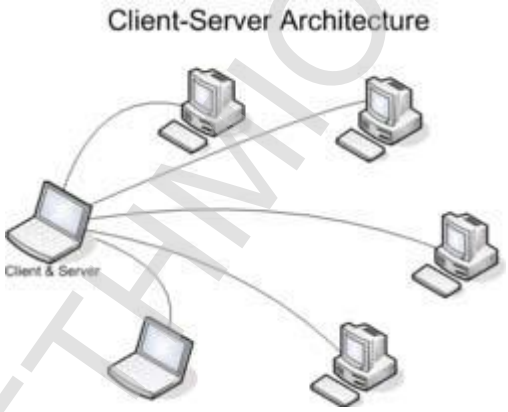
ο Αποκεντρωτικά **P2P** δίκτυα**,** όπου κάθε σύστημα που συμμετέχει αποτελεί ταυτόχρονα **client** και **server (**ή αλλιώς **servent).** Μόλις κάποιος συνδεθεί μέσω ενός ανάλογου προγράμματος**-**πελάτη **P2P,** κάνει γνωστή την παρουσία του σε ένα μικρό αριθμό υπολογιστών ήδη συνδεδεμένων οι οποίοι με τη σειρά τους προωθούν τη δήλωση παρουσίας του σε ένα μεγαλύτερο δίκτυο υπολογιστών κ.λ.π Πλέον ο χρήστης έχει τη δυνατότητα να αναζητήσει οποιαδήποτε πληροφορία μεταξύ των διαμοιραζόμενων αρχείων**.** Τα δίκτυα αυτά λέγονται και δεύτερης γενιάς**.** Η μεταφορά των αρχείων είναι όμοια με αυτή των συγκεντρωτικών **P2P** δικτύων**.** Σε αυτή τη κατηγορία ανήκουν το **Kazaa,** το **Gnutella** και το **BearShare.**

ο **P2P** δίκτυα τρίτης γενιάς**,** είναι αυτά τα οποία διαθέτουν χαρακτηριστικά ανωνυμίας όπως το **Freenet,** το **I2P** και το **Entropy.** Είναι αποκεντρωτικού τύπου και η φιλοσοφία του βασίζεται εκτός από την ανωνυμία**,** στην υψηλή βιωσιμότητα του**,** στο συνεχή διαμοιρασμό των αρχείων και στην κωδικοποίησή τους έτσι ώστε κανείς να μην μπορέσει ποτέ να αποκτήσει κανένα είδος ελέγχου πάνω σε αυτό**.** Τα

δίκτυα αυτού του τύπου είναι υπό ανάπτυξη και έχουν χαρακτηριστεί ως μικρά παγκόσμια δίκτυα.

**Δίκτυα βασισμένα σε εξυπηρετητή (server based)**

Τα βασισμένα σε εξυπηρετητή δίκτυα συνιστούν ιεραρχία η οποία σχεδιάστηκε με σκοπό τη βελτίωση της διαχείρισης των υποστηριζόμενων λειτουργιών του δικτύου καθώς το μέγεθός του αυξάνεται **[65].** Συχνά τα βασισμένα σε εξυπηρετητή δίκτυα αναφέρονται αλλιώς και ως πελάτης**/**εξυπηρετητής **(client/server)** δίκτυα**.** Σε ένα δίκτυο πελάτη**/**εξυπηρετητή**,** συχνά οι διαμοιραζόμενοι πόροι εγκαθίστανται σε μία ξεχωριστή κατηγορία υπολογιστών που είναι γνωστοί ως εξυπηρετητές **(servers).** Οι εξυπηρετητές είναι πολυχρηστικά υπολογιστικά συστήματα τα οποία διαμοιράζουν τους πόρους του δικτύου σε όλους τους συνδεδεμένους σταθμούς εργασίας**.** Σε αυτό τον τύπο δικτύου οι σταθμοί εργασίας μπορούν να λειτουργήσουν οι ίδιοι ως εξυπηρετητές σε άλλα υπολογιστικά συστήματα **(**Σχήμα **3).**




**Σχήμα 3. Αρχιτεκτονική client server**

## 2.5.4 Μέθοδοι μετάδοσης στα LAN

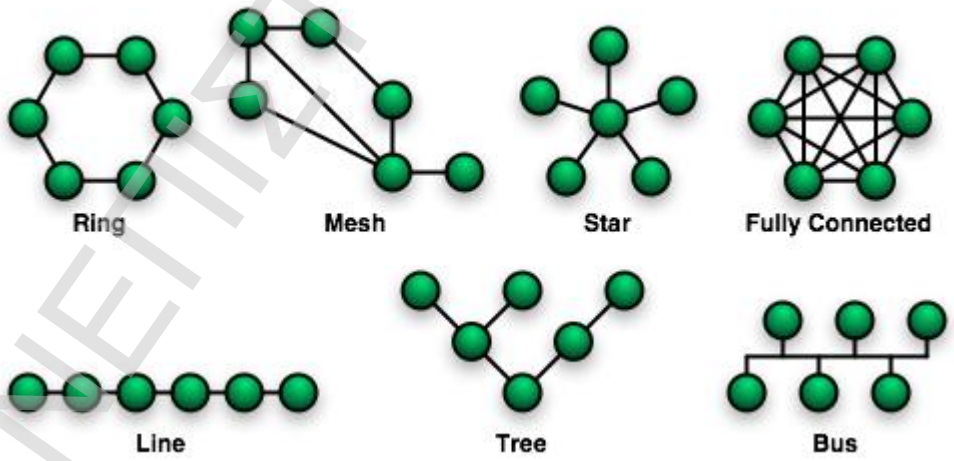
Η μετάδοση δεδομένων στα Τοπικά Δίκτυα ταξινομείται σε τρεις κατηγορίες **[89,118]:** εκπομπή σε συγκεκριμένο κόμβο **(unicast),** εκπομπή σε πολλούς κόμβους **(multicast)** και εκπομπή σε όλους τους κόμβους **(broadcast).** Σε κάθε τύπο μετάδοσης, ένα απλό πακέτο δεδομένων αποστέλλεται σε έναν ή περισσότερους κόμβους. Σε μια μετάδοση **unicast,** ένα απλό πακέτο αποστέλλεται από την πηγή στο δίκτυο προς ένα συγκεκριμένο σταθμό**.** Αρχικά**,** ο πρώτος κόμβος καθορίζει το δρόμο μεταβίβασης του πακέτου χρησιμοποιώντας τη διεύθυνση προορισμού του**.** Στη συνέχεια το πακέτο αποστέλλεται στο δίκτυο όπου και μεταβιβάζεται στον προορισμό του**.** Σε μια **multicast** μετάδοση το πακέτο δεδομένων αντιγράφεται και αποστέλλεται σε ένα συγκεκριμένο υποσύνολο κόμβων του δικτύου**.** Στην κατηγορία αυτή**,** ο πρώτος κόμβος διευθυνσιοδοτεί το πακέτο χρησιμοποιώντας μια

**multicast** διεύθυνση. Το πακέτο τότε αποστέλλεται στο δίκτυο, το οποίο δημιουργεί αντίγραφα του πακέτου και τα στέλνει σε κάθε κόμβο που αποτελεί τμήμα της **multicast** διεύθυνσης. Σε μια **broadcast** μετάδοση το πακέτο δεδομένων αντιγράφεται και αποστέλλεται σε όλους τους κόμβους του δικτύου. Σε αυτόν τον τύπο μετάδοσης, ο πρώτος κόμβος διευθυνσιοδοτεί το πακέτο χρησιμοποιώντας μια **broadcast** διεύθυνση. Κατόπιν, το πακέτο διοχετεύεται στο δίκτυο, το οποίο δημιουργεί αντίγραφα αυτού και τα οποία στέλνονται σε όλους τους κόμβους του δικτύου.

### 2.5.5 Τοπολογίες Δικτύων

Οι τοπολογίες των Τοπικών Δικτύων **(LANs) [118]** ορίζουν τον τρόπο με τον οποίο οι συσκευές έχουν οργανωθεί στο δίκτυο. Υπάρχουν αρκετές διαφορετικές μεταξύ τους τοπολογίες οι οποίες είναι διαθέσιμες για τα Τοπικά Δίκτυα και τα δίκτυα γενικότερα. Μερικές από αυτές είναι **(**Σχήμα **4):**

- Τοπολογία Αρτηρίας **(Bus)**
- Τοπολογία Αστέρα **(Star)**
- Τοπολογία Δακτυλίου **(Ring)**
- Τοπολογία Δένδρου **(Tree)**
- Τοπολογία **Mesh**

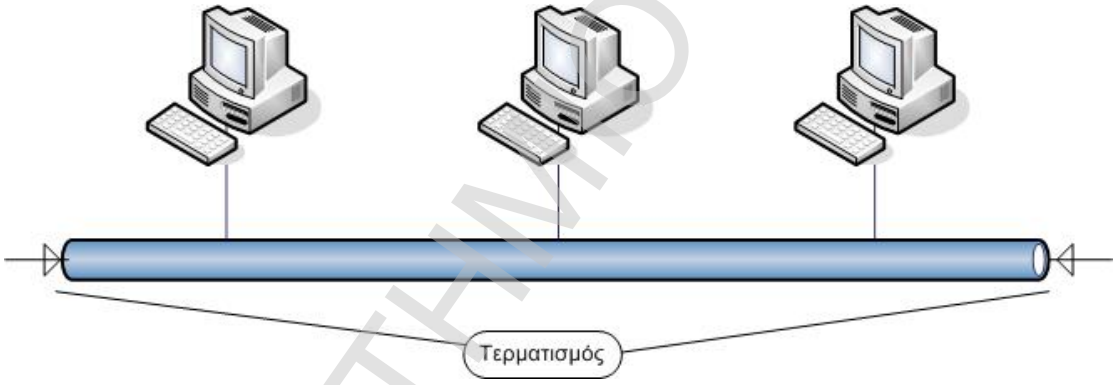



**Σχήμα 4. Τοπολογίες LAN**

Αυτές οι τοπολογίες είναι λογικές διατάξεις μια και στην πραγματικότητα οι συσκευές δεν διατάσσονται αυστηρά με κάποιον από τους παραπάνω πέντε τρόπους. Η τοπολογία **Mesh** συναντάται περισσότερο σε **WAN** δίκτυα όπου οι δρομολογητές **(routers)** παρέχουν πολλαπλά μονοπάτια για έναν συγκεκριμένο προορισμό.

**Τοπολογία Αρτηρίας (Bus)**

Στην τοπολογία αρτηρίας, όλοι οι σταθμοί είναι συνδεδεμένοι σε ένα κοινό διαμοιραζόμενο επικοινωνιακό μέσο, το όποιο διατρέχει όλο το τοπικό δίκτυο. Η σύνδεση επιτυγχάνεται μέσω μονάδων διασύνδεσης και παροχέτευσης καλωδίου **(taps).** Τα μηνύματα διοχετεύονται σε όλο το μέσο. Κάθε υπολογιστής συνδεδεμένος στο μέσο γνωρίζει πλήρως τη διεύθυνσή του ώστε να λαμβάνει τα μηνύματα. Κατά την αποστολή μηνυμάτων οι υπολογιστές πρέπει να συγχρονίζονται και να επιτρέπουν έναν υπολογιστή να μεταδίδει κάθε φορά **(**Σχήμα **5).** Η τοπολογία αρτηρίας υλοποιείται συνήθως με δύο τρόπους: **10Base5** και **10Base2 [54,118].** Ο πρώτος αριθμός **(**το **10)** υποδηλώνει την μέγιστη ταχύτητα μετάδοσης των δεδομένων στο δίκτυο, η λέξη **"Base"** την ζώνη μετάδοσης **(**βασική ζώνη μετάδοσης**)** και ο δεύτερος αριθμός πολλαπλασιασμένος με το **100** την μέγιστη απόσταση που μπορεί να καλύψει το δίκτυο με τις συγκεκριμένες προδιαγραφές.




**Σχήμα 5. Τοπολογία αρτηρίας**

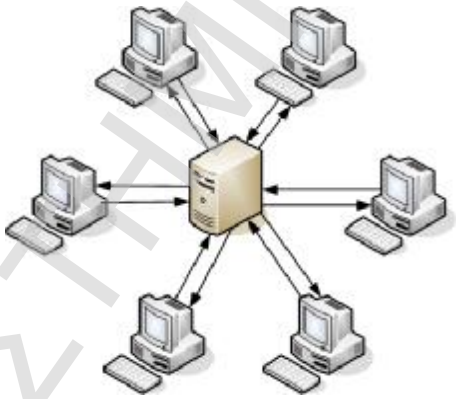
α**) 10Base5:** Έχει ως κύριο μέσο μετάδοσης χοντρό ομοαξονικό καλώδιο **RG-8** το οποίο μπορεί να έχει μήκος έως **500** μέτρα. Λειτουργεί με ταχύτητα **10 Mbps.**

β**) 10Base2:** Έχει ως κύριο μέσο μετάδοσης λεπτό ομοαξονικό καλώδιο το οποίο μπορεί να έχει μήκος έως **200** μέτρα. Λειτουργεί με ταχύτητα **10 Mbps.** Το φυσικό μήκος της τοπολογίας αρτηρίας αυξάνεται με διασύνδεση πολλαπλών τμημάτων ομοαξονικού καλωδίου μέσω ενός επαναλήπτη **(repeater),** ή γέφυρας **(bridge).** Τα δίκτυα τοπολογίας αρτηρίας αποτελούν καλή επιλογή για μικρά δίκτυα και για δίκτυα με χαμηλό φορτίο κίνησης, ενώ παρουσιάζουν σχετικά χαμηλή πολυπλοκότητα και η απόδοση τους είναι πολύ καλή όταν τα φορτία κίνησης είναι μικρά. Σε περίπτωση που το φορτίο αυξηθεί η απόδοσή τους μειώνεται. Η επέκταση και η αναδιάταξη ενός δικτύου αρτηρίας είναι εύκολη. Μια καινούργια ή αναδιατασσόμενη συσκευή μπορεί εύκολα να συνδεθεί στο πλησιέστερο διαθέσιμο σημείο πρόσβασης στο δίκτυο. Τα δίκτυα αυτά προσφέρουν υψηλή αξιοπιστία.

Μειονέκτημα αποτελεί η χαμηλή ασφάλεια που προσφέρουν καθώς και η δύσκολη διάγνωση προβλημάτων.

### Τοπολογία Αστέρα (Star)

Σε μία τοπολογία αστέρα, έχουμε έναν μεταγωγέα **(switch)** στον οποίο συνδέονται όλοι οι υπολογιστές και οι λοιπές συσκευές. Η σύνδεση μπορεί να γίνει μέσω συνεστραμμένων ζευγών **(UTP - Unshielded Twisted Pair).** Η διαδικασία ελέγχου σε μια τοπολογία αστέρα μπορεί να υλοποιηθεί είτε με το να έχει τον έλεγχο η κεντρική μονάδα εξυπηρέτησης, είτε με το να βρίσκεται σε κάποιον από τους περιφερειακούς σταθμούς, είτε τέλος με το να είναι ο έλεγχος ισοκατανεμημένος στους σταθμούς εργασίας **(**Σχήμα **6).** Το **IEEE 802.3 CSMA/CD [24,54]** τοπικό δίκτυο μπορεί να λειτουργήσει σε έναν αστέρα χρησιμοποιώντας καλώδιο **UTP, CAT-3,** ή **CAT-5.** Τα δίκτυα τοπολογίας αστέρα αποτελούν την καλύτερη επιλογή σε περιπτώσεις που απαιτούνται ολοκληρωμένες υπηρεσίες φωνής**/**δεδομένων ή μεγάλες ταχύτητες μεταγωγής. Επίσης διευκολύνουν πολύ την προσθήκη νέων σταθμών εργασίας, την διαχείριση των πόρων του δικτύου, την ασφάλιση, την διάγνωση προβλημάτων καθώς και την κατανομή των προτεραιοτήτων.

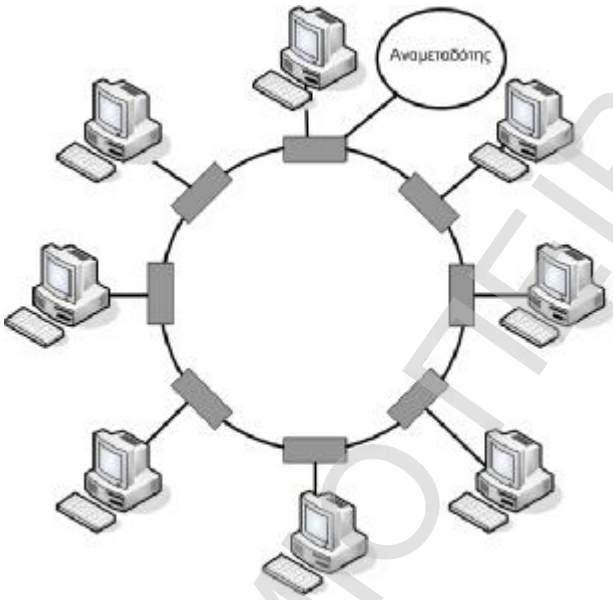


**Σχήμα 6. Τοπολογία αστέρα**

### Τοπολογία Δακτυλίου (Ring)

Στην τοπολογία δακτυλίου οι υπολογιστές καθώς και οι λοιπές συσκευές συνδέονται έτσι ώστε να σχηματίζουν ένα κλειστό βρόχο. Τα μηνύματα μεταδίδονται από υπολογιστή σε υπολογιστή. Έτσι ο πρώτος στέλνει την πληροφορία στον δεύτερο, ο δεύτερος στον τρίτο κλπ. έως ότου φθάσει στον προορισμό της. Η σύνδεση του κάθε σταθμού εργασίας με τον δακτύλιο γίνεται μέσω μιας μονάδας διασύνδεσης η οποία είναι συνδεδεμένη με έναν αναμεταδότη, ο οποίος και αναμεταδίδει τα μηνύματα που κατευθύνονται σε άλλους σταθμούς εργασίας. Το **FDDI (Fiber Distributed Data Interchange) [62]** είναι θεωρητικά ένα τέτοιο δίκτυο αλλά λόγω του ότι είναι ένα σύστημα υψηλών ταχυτήτων **(100Mbps)** χρησιμοποιείται για να διασυνδέει πολλά **LANs** μικρότερης ταχύτητας. Τα δίκτυα δακτυλίου αποτελούν

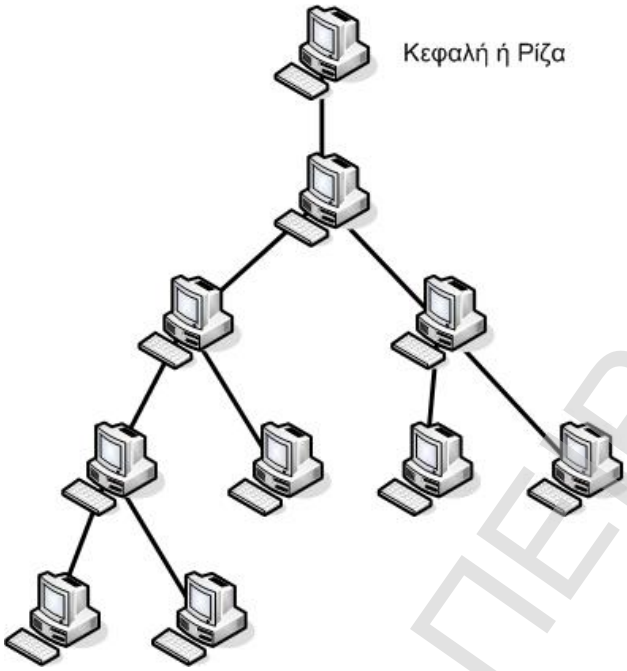
καλή επιλογή σε περιπτώσεις που απαιτείται ισοκατανομή της χωρητικότητας του δικτύου, καθώς επίσης και σε περιπτώσεις που πρέπει να συνδεθούν, σε μικρές αποστάσεις, λίγοι σταθμοί εργασίας οι οποίοι θα λειτουργούν σε υψηλές ταχύτητες. Προσφέρουν υψηλή αξιοπιστία και εύκολη προσθήκη/αφαίρεση σταθμών εργασίας από το δίκτυο (Σχήμα **7**).




**Σχήμα 7. Τοπολογία δακτυλίου**

### Τοπολογία Δένδρου (Tree)

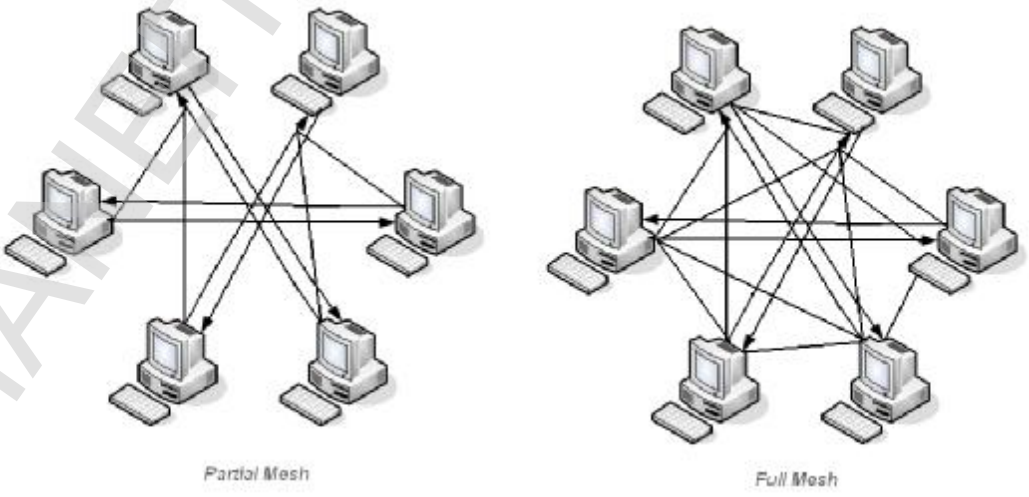
Η τοπολογία δένδρου αποτελεί παραλλαγή της τοπολογίας αρτηρίας. Η μορφή του δικτύου μοιάζει με ένα ανεστραμμένο δένδρο όπου τα "κλαδιά" είναι αρτηρίες. Η αρτηρία αυτή περιλαμβάνει έναν κεντρικό κόμβο που ονομάζεται ρίζα του δένδρου **(root)** και οι υπόλοιποι σταθμοί εργασίας είναι συνδεδεμένοι με αυτή ή σε αυτήν μέσω άλλων σταθμών εργασίας σχηματίζοντας επίπεδα διασύνδεσης. Πλεονεκτήματα αυτής της τοπολογίας θεωρείται η εύκολη προσθήκη αλλά και αφαίρεση σταθμών εργασίας καθώς και η προσωρινή απομόνωση στοιχείων που παρουσιάζουν βλάβη. Ωστόσο όμως, μία πιθανή βλάβη της ρίζας θα έχει ως αποτέλεσμα τη δυσλειτουργία ολόκληρου του δικτύου (Σχήμα **8**).




**Σχήμα 8. Τοπολογία δέντρου**

### Κατανεμημένη τοπολογία ή τοπολογία πλέγματος (Mesh)

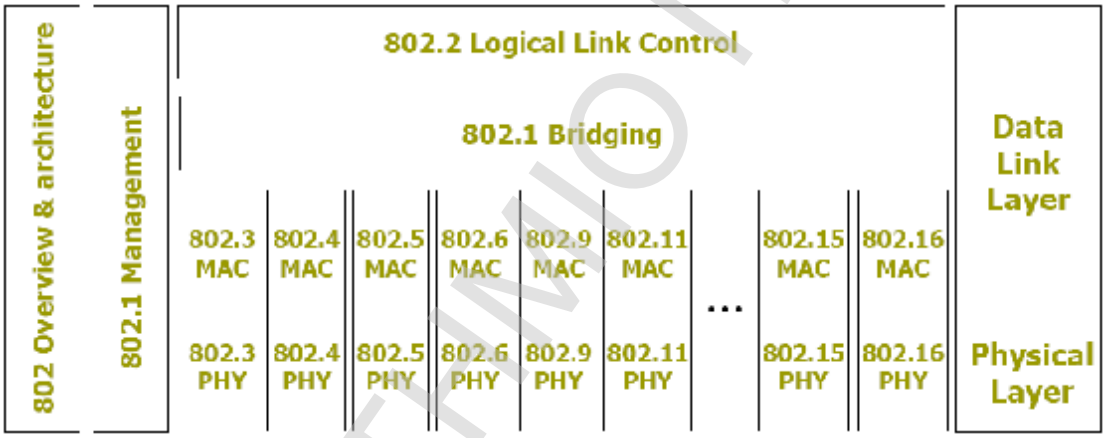
Η κατανεμημένη τοπολογία χωρίζεται στην πλήρως κατανεμημένη **(full mesh)** και μερικώς κατανεμημένη **(partial mesh).** Στην πλήρως κατανεμημένη κάθε σταθμός εργασίας συνδέεται απευθείας με όλους τους υπόλοιπους σταθμούς**,** επικοινωνεί δηλαδή άμεσα με κάθε ένα από αυτούς**.** Στην μερικώς κατανεμημένη κάποιοι σταθμοί επικοινωνούν άμεσα με όλους ή μερικούς από τους υπόλοιπους ενώ κάποιοι άλλοι μόνο με τους γειτονικούς**.** Το πλεονέκτημα εδώ είναι πως ακόμα και σε περίπτωση μερικής καταστροφής του μέσου υπάρχει η δυνατότητα επικοινωνίας δύο σταθμών μέσω εναλλακτικών διαδρομών**.** Το μειονέκτημα είναι η περιττή καλωδίωση και το κόστος στην περίπτωση που το μέσο είναι το καλώδιο **(**Σχήμα **9).**




**Σχήμα 9. Τοπολογία πλέγματος**

### 2.5.6 Πρωτόκολλα Τοπικών Δικτύων

Τα Τοπικά Δίκτυα **(LANs)** όπως έχουμε ήδη αναφέρει είναι ένα σύνολο από υπολογιστές καθώς και άλλες συσκευές οι οποίες συνδέονται σε μια γεωγραφικά μικρή περιοχή με σκοπό να εξυπηρετήσουν τις ανάγκες μιας επιχείρησης ή μιας μικρής κοινωνίας. Ο οργανισμός **IEEE** παρουσίασε διάφορα πρότυπα τοπικών δικτύων. Αυτά τα πρότυπα είναι συνολικά γνωστά ως **IEEE 802 [54,77,118,63]** και περιλαμβάνουν το πρωτόκολλο πρόσβασης στο μέσο "Πολλαπλή Προσπέλαση με Ακρόαση Φέροντος και Ανίχνευση Συγκρούσεων **(CSMA/CD - Carrier Sense Multiple Access with Collision Detection),** την αρτηρία με κουπόνι **(token bus)** και τον δακτύλιο με κουπόνι **(token ring).** Τα διάφορα **IEEE 802** πρότυπα διαφέρουν στο φυσικό επίπεδο και στο υποεπίπεδο προσπέλασης στο μέσο **(MAC - Medium Access Control),** αλλά είναι συμβατά στο επίπεδο σύνδεσης δεδομένων **(**Σχήμα **10).**




**Σχήμα 10. Πρότυπα 802.***

Τα πρότυπα **IEEE 802** έχουν γίνει αποδεκτά από το οργανισμό **ANSI** ως Εθνικά πρότυπα των ΗΠΑ, από το **NBS** ως κυβερνητικά πρότυπα, και από τον **ISO** ως διεθνή πρότυπα **(**γνωστά ως **ISO 8802).** Τα πρότυπα χωρίζονται σε τμήματα. Το πρότυπο **802.1** κάνει μια εισαγωγή στην ομάδα των προτύπων και προσδιορίζει τις πρωτογενείς λειτουργίες της διασύνδεσης. Το πρότυπο **802.2** εξηγεί το άνω μέρος του επιπέδου σύνδεσης δεδομένων, το οποίο χρησιμοποιεί το πρωτόκολλο **LLC (Logical Link Control –** Έλεγχος Λογικής Σύνδεσης**).** Τα τμήματα **802.3** έως **802.5** εξηγούν τα τρία πρότυπα των **LANs,** το **CSMA/CD,** την αρτηρία με κουπόνι **(token bus)** και τον δακτύλιο με κουπόνι **(token ring),** αντίστοιχα. Κάθε πρότυπο καλύπτει τα πρωτόκολλα του φυσικού επιπέδου και του υποεπιπέδου **MAC.**

#### 2.5.6.1 Ιστορία 802.* πρότυπα IEEE

Οι τυποποιήσεις τόσο των τοπικών όσο και των μητροπολιτικών δικτύων **(LAN/MAN)** καθορίζονται από την ομάδα εργασίας **802** της **IEEE (Institute of Electrical and Electronics Engineers),** ενός διεθνούς μη κερδοσκοπικού

επαγγελματικού συλλόγου, που απαριθμεί εκατοντάδες χιλιάδες μέλη (ηλεκτρολόγους και ηλεκτρονικούς μηχανικούς) σε πάνω από **150** χώρες στον κόσμο.

Η ομάδα **IEEE 802** συναντήθηκε για πρώτη φορά στις **27 – 29** Φεβρουαρίου **1980** στο **San Francisco, CA,** χάρη στις επίμονες προσπάθειες των **Maris Graube** και **Robert Rosenthal.** Σ' αυτήν τη συνάντηση συμμετείχαν περίπου **125** άτομα, τα περισσότερα με εμπειρία στην ανάπτυξη τοπικού δικτύου, καθώς εκείνη τη χρονική στιγμή υπήρχαν περίπου **80** τύποι τοπικών δικτύων υπό σχεδίαση ή σε περιορισμένη χρήση. Αποστολή της ομάδας εργασίας ορίστηκε η συγγραφή διεθνών προτύπων για τα τοπικά δίκτυα, τα οποία να αντιστοιχούν στα επίπεδα **1** και **2** του μοντέλου αναφοράς **OSI.**

| Number | Topic |
|---|---|
| 802.1 | Overview and architecture of LANs |
| 802.2 ↓ | Logical link control |
| 802.3 * | Ethernet |
| 802.4 ↓ | Token bus (was briefly used in manufacturing plants) |
| 802.5 | Token ring (IBM's entry into the LAN world) |
| 802.6 ↓ | Dual queue dual bus (early metropolitan area network) |
| 802.7 ↓ | Technical advisory group on broadband technologies |
| 802.8 † | Technical advisory group on fiber optic technologies |
| 802.9 ↓ | Isochronous LANs (for real-time applications) |
| 802.10 ↓ | Virtual LANs and security |
| 802.11 * | Wireless LANs |
| 802.12 ↓ | Demand priority (Hewlett-Packard's AnyLAN) |
| 802.13 | Unlucky number. Nobody wanted it |
| 802.14 ↓ | Cable modems (defunct: an industry consortium got there first) |
| 802.15 * | Personal area networks (Bluetooth) |
| 802.16 * | Broadband wireless |
| 802.17 | Resilient packet ring |

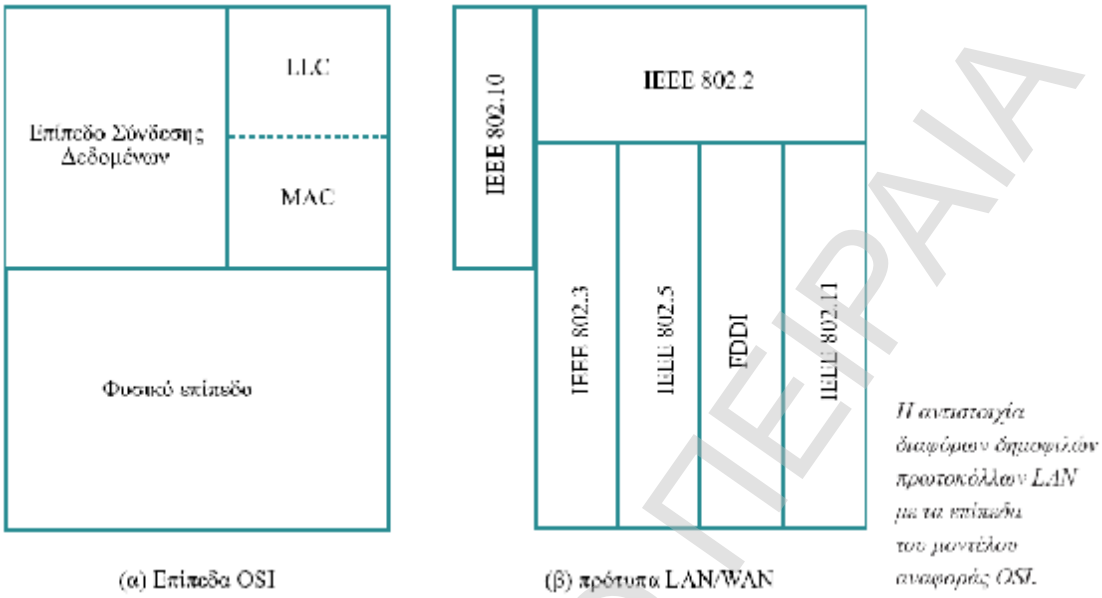
**Πίνακας 1. Πρότυπα 802.***

Μέσα στα πρώτα δύο χρόνια εκδόθηκαν τα πρώτα προσχέδια προτύπων, επί των οποίων διενεργήθηκαν μακροχρόνιες διαβουλεύσεις. Τελικά, τον Ιανουάριο **1985** εκδόθηκε το πρώτο πρότυπο της ομάδας, το οποίο ονομάστηκε **IEEE 802.3.** Από τότε μέχρι σήμερα, έχουν εκδοθεί πάνω από **50** πρότυπα και συμπληρώματα προτύπων, τα οποία καλύπτουν όλο το ευρύ φάσμα της αρχιτεκτονικής των δικτύων **LAN/MAN (**Πίνακας **1).**

### 2.5.6.2 Τα πρωτόκολλα LAN και το μοντέλο αναφοράς OSI

Τα πρωτόκολλα τοπικού δικτύου λειτουργούν στα δύο χαμηλότερα επίπεδα του μοντέλου αναφοράς **OSI,** δηλαδή στο Φυσικό Επίπεδο και στο Επίπεδο Σύνδεσης

Δεδομένων. Στο σχήμα που ακολουθεί δίδεται η αντιστοιχία διαφόρων πρωτοκόλλων **LAN** με τα επίπεδα του **OSI (**Σχήμα **11).**




**Σχήμα 11. Μοντέλο αναφοράς OSI**

Όλα, τα ηλεκτρικά και μηχανικά χαρακτηριστικά του μέσου μετάδοσης καθορίζονται στο Φυσικό Επίπεδο **[54].** Επίσης, το Επίπεδο Σύνδεσης Δεδομένων φροντίζει για την ανταλλαγή πλαισίων μεταξύ των υπολογιστών που διασυνδέονται στο ίδιο τοπικό δίκτυο. Οι υπολογιστές σ' ένα τοπικό δίκτυο επικοινωνούν μεταξύ τους χρησιμοποιώντας έναν κοινό σύνδεσμο πολλαπλής πρόσβασης αντί για συνδέσμους σημείο με σημείο και αυτό το ιδιαίτερο χαρακτηριστικό αποτελεί μία ειδοποιό διαφορά των δικτύων **LAN/MAN** από τα δίκτυα ευρείας περιοχής. Για τον αποδοτικό χειρισμό αυτού του χαρακτηριστικού, το Επίπεδο Σύνδεσης Δεδομένων στα τοπικά δίκτυα χωρίζεται σε δύο υποεπίπεδα: στον Έλεγχο Προσπέλασης στο Μέσο **(Media Access Control – MAC)** και στον Έλεγχο Λογικής Σύνδεσης **(Logical Link Control – LLC).**

Οι λειτουργίες που εκτελούνται στο υποεπίπεδο **MAC** ρυθμίζουν την προσπέλαση στον κοινό σύνδεσμο. Για κάθε συνομιλία μεταξύ δύο κόμβων στο τοπικό δίκτυο, ο Έλεγχος Προσπέλασης Μέσων υλοποιεί έναν ιδεατό σύνδεσμο σημείου με σημείο μεταξύ των ενδιαφερομένων μερών, δίδοντάς τους έτσι την ψευδαίσθηση ότι επικοινωνούν μέσω απευθείας συνδέσμου και όχι μέσω διαμοιραζόμενου συνδέσμου πολλαπλής πρόσβασης.

Ο Έλεγχος Λογικής Σύνδεσης υλοποιεί τις υπηρεσίες μετάδοσης πλαισίων μεταξύ των κόμβων του τοπικού δικτύου. Έτσι, μπορεί να υλοποιήσει μία υπηρεσία αξιόπιστης μετάδοσης πλαισίων, ζητώντας την επανεκπομπή όλων των πλαισίων που αλλοιώθηκαν κατά τη μεταφορά τους. Επίσης, μπορεί να υλοποιήσει μία

υπηρεσία κατά την οποία να απορρίπτει απλώς τα πλαίσια που υπέστησαν σφάλμα μεταφοράς και να προωθεί στο Επίπεδο Δικτύου τα υπόλοιπα πλαίσια.

Όπως παρατηρούμε και στο σχήμα, το πρότυπο **IEEE 802.2** καθορίζει το υποεπίπεδο **LLC [54,118].** Επίσης, υπάρχει ένα πλήθος από πρότυπα **(IEEE 802.3 – 16)** που καλύπτουν τόσο το Φυσικό Επίπεδο όσο και το υποεπίπεδο **MAC** των τοπικών δικτύων, με πιο δημοφιλή τα IEEE **802.3 (**δίκτυα τύπου **Ethernet)[118], IEEE 802.5 (**δίκτυα τύπου Δακτυλίου με Κουπόνι**)[62]** και **IEEE 802.11 [35,39] (**ασύρματα τοπικά δίκτυα**)(**Πίνακας **2).**

Η ύπαρξη του υποεπιπέδου **LLC** δίδει ευελιξία στην προσθήκη μελλοντικών προτύπων **LAN,** καθώς απαλλάσσει το Επίπεδο Δικτύου από την υποχρέωση προσαρμογής σ' αυτό το νέο πρότυπο. Τα πρότυπα που εξελίσσονται στο χρόνο, τηρούν μία αρίθμηση συμβατή με αυτή του αρχικού προτύπου. Για παράδειγμα, τα πρότυπα για τα προηγμένα δίκτυα τύπου **Ethernet,** τα οποία εμφανίζουν ρυθμό μετάδοσης πολλαπλάσιο του αρχικού, έχουν αριθμηθεί ως **IEEE 802.3u (Fast Ethernet), IEEE 802.3z (Gigabit Ethernet)** και **IEEE 802.3ae (10 Gigabit Ethernet) [24,61].** Επίσης, το πρότυπο **IEEE 802.10** ασχολείται με την ασφάλεια στα τοπικά δίκτυα και εντάσσεται αποκλειστικά στο Επίπεδο Σύνδεσης Δεδομένων.

### 2.5.6.3 Πρότυπο IEEE 802.3 (CSMA/CD)

Τα δίκτυα τύπου **Ethernet (IEEE 802.3** βασικής ζώνης, Πινάκας **2) ,** αποτελούν την πλέον δημοφιλή δικτυακή λύση σε τοπικό επίπεδο. Το πρότυπο **IEEE 802.3** ορίζει το πρωτόκολλο Ελέγχου Πρόσβασης στο Μέσο για τοπικό δίκτυο υπολογιστών τοπολογίας αρτηρίας, που χρησιμοποιεί ως μέθοδο πρόσβασης στο μέσο την Πολλαπλή Προσπέλαση με Ακρόαση Φέροντος και Ανίχνευση Συγκρούσεων **(CSMA/CD - Carrier Sense Multiple Access with Collision Detection) (**Σχήμα **12).**

| Ethernet Standard | Date | Description |
|---|---|---|
| **Experimental Ethernet** | **1972** | **2.94 Mbit/s (367 kB/s)** με χρήση ομοαξονικού καλωδίου **(coax)** καλώδιο διαύλου |
| **Ethernet II (DIX v2.0)** | **1982** | **10 Mbit/s (1.25 MB/s)** με χρήση λεπτού ομοαξονικού καλωδίου **(thinnet)** Τα **Frames** έχουν ένα πεδίο **Type.** Η μορφοποίηση αυτού του πλαισίου αυτό χρησιμοποιείται σε όλες τις μορφές **Ethernet** από τα πρωτόκολλα στην στοίβα πρωτοκόλλων του **Internet.** |
| **IEEE 802.3** | **1983** | **10BASE5 10 Mbit/s (1.25 MB/s)** με χρήση λεπτού ομοαξονικού καλωδίου είναι το ίδιο με το **DIX** μόνο που το πεδίο **Type** έχει αντικατασταθεί με το πεδίο **Length,** και μία επικεφαλίδα **802.2 LLC** ακολουθεί την επικεφαλίδα |

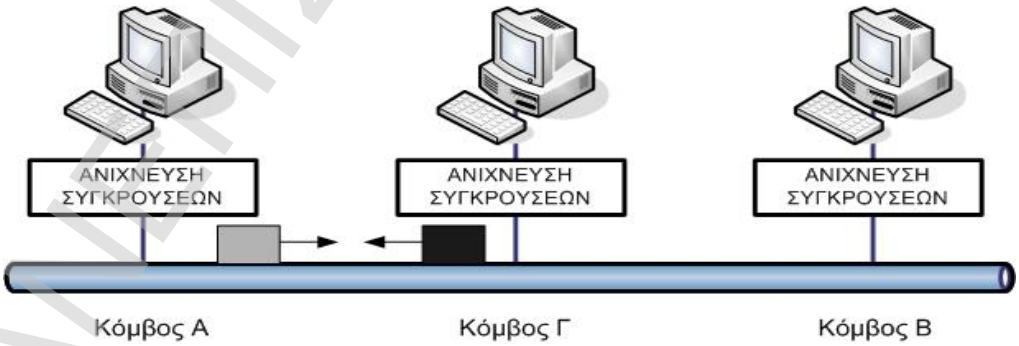
| | | |
|---|---|---|
| | | του **802.3** |
| **802.3a** | **1985** | **10BASE2 10 Mbit/s (1.25 MB/s)** με χρήση λεπτού ομοαξονικού καλωδίου **(thinnet or cheapernet)** |
| **802.3b** | **1985** | **10BROAD36** |
| **802.3c** | **1985** | **10 Mbit/s (1.25 MB/s)** με προδιαγραφές για τους επαναλήπτες |
| **802.3d** | **1987** | **FOIRL (Fiber-Optic Inter-Repeater Link)** |
| **802.3e** | **1987** | **1BASE5** ή **StarLAN** |
| **802.3i** | **1990** | **10BASE-T 10 Mbit/s (1.25 MB/s)** με χρήση συνεστραμμένων ζεύγων |
| **802.3j** | **1993** | **10BASE-F 10 Mbit/s (1.25 MB/s)** με χρήση οπτικών ινών |
| **802.3u** | **1995** | **100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet at 100 Mbit/s (12.5 MB/s) w/autonegotiation** |
| **802.3x** | **1997** | Με πλήρη αμφίδρομη επικοινωνία και έλεγχο ροής επίσης ενσωματώνει το **DIX framing,** δεν είναι πλέον απαραίτητος ο διαχωρισμός **DIX/802.3** |
| **802.3y** | **1998** | **100BASE-T2 100 Mbit/s (12.5 MB/s)** με χρήση συνεστραμμένων ζευγών χαμηλής ποιότητας |
| **802.3z** | **1998** | **1000BASE-X Gbit/s Ethernet** με χρήση οπτικών ινών στα **1 Gbit/s (125 MB/s)** |
| **802.3-1998** | **1998** | Μια αναθεωρημένη έκδοση του αρχικού προτύπου ενσωματώνοντας τις τροποποιήσεις που προέκυψαν από τις λίστες σφαλμάτων |
| **802.3ab** | **1999** | **1000BASE-T Gbit/s Ethernet** με χρήση συνεστραμμένων ζευγών στα **1 Gbit/s (125 MB/s)** |
| **802.3ac** | **1998** | Το μέγιστο μέγεθος του πακέτου γίνετε **1522 bytes (**για να επιτρέψει το **"Q-tag")** το οποίο **(Q-tag)** περιέχει πληροφορίες για το **802.1Q VLAN** και την πληροφορία για την προτεραιότητα στο **802.1p.** |
| **802.3ad** | **2000** | Συνάθροιση συνδέσεων για παράλληλες συνδέσεις |
| **802.3-2002** | **2002** | Η αναθεώρηση του προτύπου με βάση τις τρεις προγενέστερες τροπολογίες και την λίστα σφαλμάτων |
| **802.3ae** | **2003** | **10 Gbit/s (1,250 MB/s) Ethernet** με χρήση οπτικών ινών **10GBASE-SR,** |

| | | |
|---|---|---|
| | | **10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW, 10GBASE-EW** |
| **802.3af** | **2003** | **Power over Ethernet** |
| **802.3ah** | **2004** | **Ethernet** στο πρώτο μίλι |
| **802.3ak** | **2004** | **10GBASE-CX4 10 Gbit/s (1,250 MB/s) Ethernet** με χρήση διπλού αξονικού καλωδίου |
| **802.3-2005** | **2005** | Μια αναθεώρηση των προτύπων που ενσωματώνει τις τέσσερις προγενέστερες τροποποιήσεις και τα τυπογραφικά λάθη**.** |
| **802.3an** | **2006** | **10GBASE-T 10 Gbit/s (1,250 MB/s) Ethernet** με χρήση αθωράκιστου συνεστραμμένου ζεύγους **(UTP)** |
| **802.3aq** | **2006** | **10GBASE-LRM 10 Gbit/s (1,250 MB/s) Ethernet** με χρήση πολυτροπικών οπτικών ινών |
| **802.3as** | **2006** | Επέκταση πλαισίου |
| **802.3au** | **2006** | Απομονωμένες **for Power Over Ethernet (802.3-2005/Cor 1)** |
| **802.3ap** | **2007** | **Backplane Ethernet (1 and 10 Gbit/s (125 and 1,250 MB/s)** με χρήση πλακετών κυκλωμάτων **printed circuit boards)** |
| **802.3aw** | **2007** | Επιδιόρθωσε μία συνιστώσα του **10GBASE-T (released as 802.3-2005/Cor 2)** |
| **802.3ar** | Σε αναμονή | Διαχείριση Συμφόρησης |
| **802.3at** | Σε αναμονή το **2008** | **Power over Ethernet** Εξελιγμένη |
| **802.3ax** | Σε αναμονή το **2008** | Μεταφορά του συνδυασμού των συνδέσεων από το **802.3** στο **IEEE 802.1** |
| **802.3ay** | Σε αναμονή το **2008** | Συντήρηση του αρχικού προτύπου |
| **802.3av** | Αναμένεται το **2009** | **10 Gbit/s EPON** |

| | | |
|---|---|---|
| **802.3ba** | Αναμένεται το **2009.** | **Higher Speed Study Group. 40 Gbit/s over 1m backplane, 10m Cu cable assembly (4x25 Gbit or 10x10 Gbit lanes) and 100 m of MMF and 100 Gbit/s up to 10 m or Cu cable assembly, 100 m of MMF or 40 km of SMF respectively** |

**Πίνακας 2. Πρότυπα 802.3xx**

Η μέθοδος **CSMA/CD [118]** είναι η συνήθης μέθοδος ελέγχου πρόσβασης στο μέσο, των τοπικών δικτύων τοπολογίας αρτηρίας / δένδρου. Με τη μέθοδο αυτή όταν ένας σταθμός θέλει να μεταδώσει, "ακούει" το μέσω (καλώδιο). Εάν το καλώδιο είναι απασχολημένο ο σταθμός περιμένει έως ότου ελευθερωθεί (**idle**), διαφορετικά μεταδίδει αμέσως. Εάν δύο ή περισσότεροι σταθμοί αρχίσουν να μεταδίδουν συγχρόνως σε ένα ελεύθερο καλώδιο, θα συγκρουστούν. Όλοι οι συγκρουόμενοι σταθμοί τότε τερματίζουν τη μετάδοσή τους, περιμένουν ένα χρονικό διάστημα και επαναλαμβάνουν ολόκληρη τη διαδικασία ξανά από την αρχή. Μια κρίσιμη παράμετρος που επηρεάζει την απόδοση της μεθόδου, είναι ο χρόνος που απαιτείται για την ανίχνευση μιας σύγκρουσης. Γενικά, σε ένα δίκτυο εκπομπής βασικής ζώνης, ο χρόνος αυτός είναι διπλάσιος της καθυστέρησης μετάδοσης, όπου η καθυστέρηση μετάδοσης ισούται με το χρόνο που χρειάζεται το σήμα να μεταδοθεί από το ένα άκρο του δικτύου στο άλλο. Στην περίπτωση ευρυζωνικών δικτύων, ο αντίστοιχος χρόνος ισούται με το τετραπλάσιο της καθυστέρησης μετάδοσης, διότι για δύο σταθμούς που βρίσκονται κοντά, το σήμα θα πρέπει να μεταδοθεί από τον έναν σταθμό μέχρι το άκρο (**headend**) του καλωδίου και μετά να επιστρέψει διανύοντας ίση απόσταση. Κατά συνέπεια το μήκος των πλαισίων θα πρέπει να είναι τέτοιο, που να επιτρέπει την ανίχνευση των συγκρούσεων πριν από το τέλος της μετάδοσης.




**Σχήμα 12. Πρότυπο 802.3**

Όπως έχει ήδη λεχθεί, η μέθοδος **CSMA/CD** δεν παρέχει επιβεβαιώσεις λήψης. Επειδή η απουσία των συγκρούσεων σίγουρα δεν εγγυάται την αποφυγή αλλοίωσης των **bits**, από ριπές θορύβου στο καλώδιο. Για να επιτευχθεί αξιόπιστη επικοινωνία πρέπει ο σταθμός προορισμού να επαληθεύει το άθροισμα ελέγχου και αν είναι

σωστό, να στέλνει πίσω στην πηγή ένα πλαίσιο επιβεβαίωσης λήψης. Τα δίκτυα τύπου **Ethernet (IEEE 802.3)** υποστηρίζουν ρυθμούς μεταφοράς μέχρι **10 Mbps.** Το μειονέκτημα της μεθόδου **CSMA-CD** είναι η μη ντετερμινιστική του συμπεριφορά. Έτσι χρησιμοποιείται γενικά σε ελεγχόμενα και προστατευόμενα περιβάλλοντα. Λόγω έλλειψης εγγυήσεων καθυστέρησης, τα δίκτυα τύπου **Ethernet** δεν συνίσταται για μετάδοση πολυμεσικών εφαρμογών. Το πρόβλημα των ανεπαρκών κριτηρίων απόδοσης των κλασσικών δικτύων **Ethernet** όταν αυτά καλούνται να υποστηρίξουν ευρυζωνικές εφαρμογές, αντιμετωπίζεται με τους ακόλουθους δύο τρόπους **[118]:**

1. Τη χρήση τμηματοποίησης **(segmentation)**
2. Τη μετανάστευση σε δίκτυα **Ethernet** υψηλού εύρους ζώνης.

Η τμηματοποίηση σημαίνει πρακτικά τη σύνδεση ενός πολύ μικρού αριθμού υπολογιστών ανά τμήμα **Ethernet.** Η δεύτερη προσέγγιση αναφέρεται στα πρότυπα των λεγόμενων δικτύων **Ethernet** υψηλών ταχυτήτων και περιλαμβάνει τις ακόλουθες τεχνολογίες:

- **IEEE 802.9** Ισόγχρονο **Ethernet**
- **IEEE 802.3u (Fast Ethernet)**
- **100Base-Tx (UTP-CAT 5)**
- **100Base-Fx (**Οπτικές ίνες**)**
- **100Base-T4 (UTP-CAT 3)**
- **IEEE 802.12 Demand Priority LAN (Fast Ethernet)**
- **IEEE 802.3z (Gigabit Ethernet)**
- **1000Base-Sx**
- **1000Base-Lx**
- **1000Base-Cx**

Το πρότυπο **IEEE 802.3** είναι αναμφίβολα το πιο διαδεδομένο καθώς και το πιο ώριμο από τα υπάρχοντα πρότυπα **(**Πίνακας **3).** Δίνει τη δυνατότητα προσθήκης σταθμών εργασίας χωρίς την "κατάρρευση" του δικτύου. Επιπρόσθετα, η καθυστέρηση σε χαμηλή φόρτωση είναι σχεδόν μηδενική. Ένα μειονέκτημα αυτών των δικτύων αποτελεί το γεγονός ότι οι συνδεδεμένοι στο δίκτυο υπολογιστές θα πρέπει να είναι ικανοί διαρκώς να ανιχνεύουν την ύπαρξη σήματος των άλλων υπολογιστών, ακόμη και την ώρα που μεταφέρουν δεδομένα στο δίκτυο. Επιπρόσθετα, το **802.3** είναι μη προσδιοριστικό **(non deterministic)** πρότυπο και

συνεπώς ακατάλληλο για εργασία σε πραγματικό χρόνο. Επίσης δεν θέτει προτεραιότητες. Ακόμη, καθώς η ταχύτητα μετάδοσης των πλαισίων αυξάνεται, η αποτελεσματικότητα πέφτει εξαιτίας της αργής μεταφοράς αυτών. Τα πλαίσια έχουν μέγεθος **64 bytes,** ακόμη και όταν μεταφέρουν έναν απλό χαρακτήρα. Τέλος αξίζει να επισημάνουμε ότι σε μεγάλη φόρτωση του δικτύου, η εμφάνιση συγκρούσεων αποτελεί σοβαρό πρόβλημα

*Τα χαρακτηριστικά των πιο συχνά χρησιμοποιούμενων τοπικών δικτύων 802.3.*

| Χαρακτηριστικό | 10Base – T | 100Base – TX | 100Base – FX | 1000Base – T | 1000Base – SX | 1000Base – LX |
|---|---|---|---|---|---|---|
| Ρυθμός μετάδοσης | 10 Mbps | 100 Mbps | 100 Mbps | 1 Gbps | 1 Gbps | 1 Gbps |
| Μέγιστο μήκος τμήματος (m) | 100 | 100 | 2000 | 100 | 275 | 5000 |
| Φυσικό μέσο | 2 ζεύγη από UTP cat – 3 ή καλύτερο | 2 ζεύγη από UTP cat – 5 ή καλύτερο | 2 πολυτροπικές ίνες 62,5/125 | 4 ζεύγη από UTP cat – 5e ή καλύτερο | 2 πολυτροπικές ίνες 62,5/125 | 2 μονοτροπικές ίνες |
| Κωδικοποίηση σήματος | Manchester | 4B/5B | 4B/5B | 4B/5B | 8B/10B | 8B/10B |
| Τοπολογία υλοποίησης | Αστέρας | Αστέρας | Σημείου με σημείο | Αστέρας | Σημείου με σημείο | Σημείου με σημείο |

**Πίνακας 3. Πινάκας με χαρακτηριστικά 802.3**

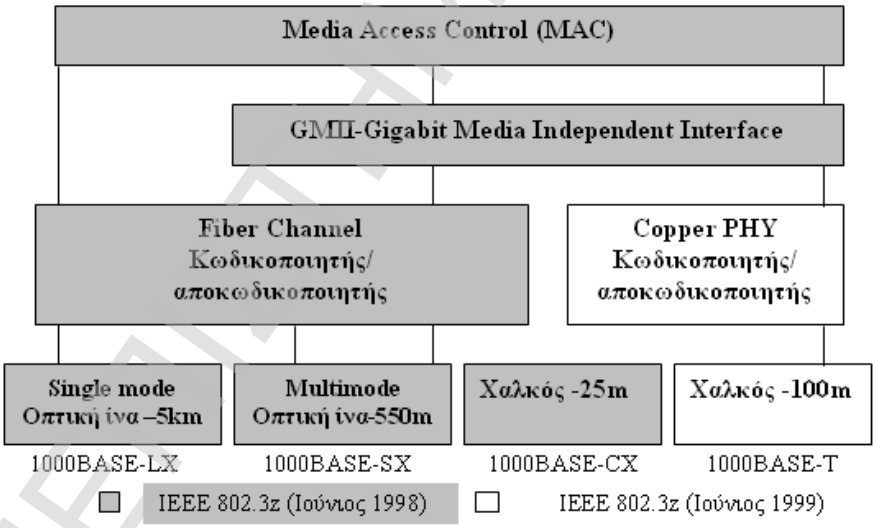
### Fast Ethernet 100Base-T (IEEE 802.3u)

Το **1990** συγκροτήθηκε μια ομάδα εργασίας με σκοπό την δημιουργία προδιαγραφών για ένα δίκτυο **Ethernet** με εύρος ζώνης τα **100Mbps [24].** Το **Fast Ethernet 802.3u** αποτελεί φυσική εξέλιξη των προτύπων **IEEE 802.3** και χρησιμοποιεί το ίδιο πρωτόκολλο **CSMA/CD.** έτσι, το δίκτυο **100Base-T** έχει τους ίδιους περιορισμούς σε ότι αφορά στα χαρακτηριστικά καθυστέρησης πρόσβασης. Επίσης, όπως και στο κλασσικό **Ethernet,** η χρήση δεν υπερβαίνει συνήθως το **50%** του μεγίστου εύρους ζώνης που στην προκείμενη περίπτωση είναι **100 Mbps.** Το δίκτυο **100Base-T** μπορεί να χρησιμοποιηθεί όπου ισχυροί σταθμοί εργασίας αποτελούν μια ομάδα με αυξημένες απαιτήσεις εύρους ζώνης. Εκτός από την αύξηση του εύρους ζώνης ιδιαίτερη προσοχή δόθηκε στο να μην διαταραχθεί η υπάρχουσα καλωδιακή υποδομή. Για αυτό δημιουργήθηκαν διάφορα επιμέρους πρότυπα ανάλογα με το χρησιμοποιούμενο φυσικό μέσο. Ένα επιπλέον θετικό στοιχείο, είναι το γεγονός ότι δίκτυα **100Base-T** και **10Base-T** μπορούν να

συνυπάρξουν σε κάποιο βαθμό. Δεν επιτρέπεται όμως ανάμειξη των δύο τεχνολογιών στο ίδιο τμήμα δικτύου. Το **Fast Ethernet 802.3u** είναι πολύ αξιόπιστο. Παρέχει αρκετό εύρος για μεγάλο αριθμό πολυμεσικών εφαρμογών καθώς και πολυδιανομή. Αλλά δεν μπορεί να δώσει εγγυήσεις για καθυστέρηση. Είναι καλή λύση για μικρές ή μεσαίες δομές αλλά όχι για πολυμεσικές εφαρμογές μεγάλων απαιτήσεων.

**Gb Ethernet**

Στα τέλη του **1995** η επιτροπή **IEEE 802.3** συγκρότησε μια ομάδα μελέτης υψηλών ταχυτήτων δικτύων με σκοπό να ανακαλύψει μεθόδους για μεταβίβαση πακέτων στα δίκτυα **Ethernet** σε ταχύτητες των **Gigabits** ανά δευτερόλεπτο **[24,61,118].** Η στρατηγική του **Gb Ethernet** είναι ίδια με αυτή του **Fast Ethernet.** Αν και ορίστηκε ένα νέο μέσο μετάδοσης και προδιαγραφές μεταβίβασης, το **Gb Ethernet** διατήρησε το πρωτόκολλο **CSMA/CD** και τη μορφή του **Ethernet** των **10 Mbps** και **100 Mbps.** Το δίκτυο αυτό είναι συμβατό με το **100Base-T** και **10Base-T,** διατηρώντας ένα απλό μονοπάτι μετανάστευσης. Καθώς περισσότερες επιχειρήσεις μετακινούνται στα **100Base-T** τοποθετώντας ένα τεράστιο φορτίο κυκλοφορίας στα κεντρικά δίκτυα, δημιουργήθηκε η ανάγκη για να επεκταθούμε στα **Gb Ethernet (**Σχήμα **13).**



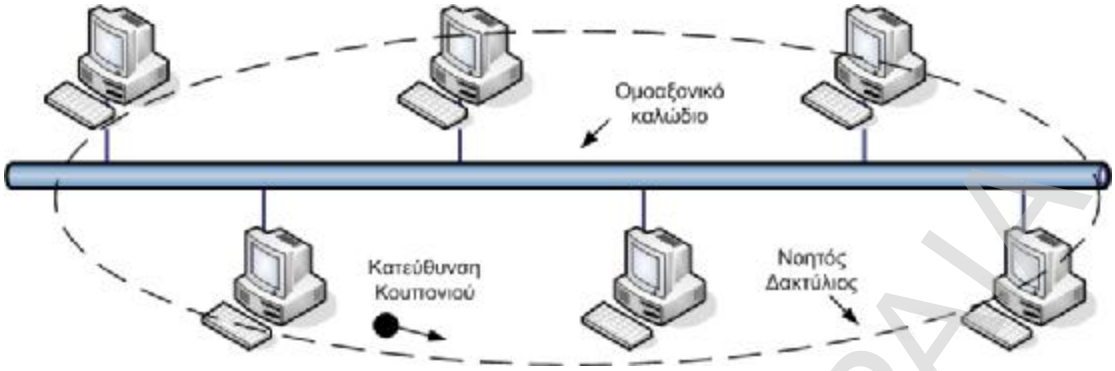

**Σχήμα 13. Πρότυπο Gigabit Ethernet**

Το μέσο μετάδοσης στα δίκτυα αυτά είναι η οπτική ίνα για μικρές αποστάσεις, αν και τα **UTP, STP** καθώς και το ομοαξονικό καλώδιο επιτρέπονται να χρησιμοποιηθούν. Η τεχνολογία **Gb Ethernet** αποτελεί το επόμενο λογικό βήμα στα ευρυζωνικά δίκτυα. Τα δίκτυα αυτά είναι **100** φορές πιο γρήγορα από τα δίκτυα **Ethernet,** ωστόσο όμως, διατηρούν την απλότητα των τελευταίων. Η μεταφορά των πακέτων βασίζεται στη μέθοδο "χωρίς σύνδεση". Το δε μήκος αυτών είναι μεταβλητό από **64** έως **1526 byte.** Τα δίκτυα αυτά έχουν σχεδιαστεί για να

μεταφέρουν συνεχή κίνηση δεδομένων. Η αποδοτικότητα του ωφέλιμου φορτίου φτάνει στο **98%**. Ο ρυθμός των δεδομένων στο δίκτυο είναι τις τάξεως των **980Mb/s** σε αντίθεση με το **Fast Ethernet** που είναι της τάξεως των **98Mb/s**. Το κόστος για αυτή την τεχνολογία είναι αρκετά χαμηλό, ενώ η υλοποίησή της αρκετά εύκολη όπως και η διαχείρισή της.

#### 2.5.6.4 Πρότυπο IEEE 802.4 (Token Passing Bus)

Το πρότυπο **IEEE 802.4 [118]**, ορίζει το πρωτόκολλο Ελέγχου Πρόσβασης στο Μέσο **(MAC)** "περάσματος κουπονιού" **(token passing)** για ένα τοπικό δίκτυο τοπολογίας αρτηρίας. Το πρότυπο αυτό προτάθηκε κυρίως για την επικοινωνιακή υποστήριξη ολοκλήρωσης εργασιών που αφορούν τον βιομηχανικό αυτοματισμό. Η αρτηρία με κουπόνι **(token passing bus)** είναι ένα γραμμικό ή μορφής δέντρου καλώδιο, στο οποίο συνδέονται οι σταθμοί **(**Σχήμα **14)**. Οι σταθμοί του δικτύου σχηματίζουν έναν λογικό δακτύλιο και κάθε σταθμός γνωρίζει τη διεύθυνση των σταθμών που βρίσκονται "αριστερά του" και "δεξιά του". Όταν πρωτοδημιουργείται **(initialized)** ο λογικός δακτύλιος, ο σταθμός με την υψηλότερη αρίθμηση μπορεί να στείλει το πρώτο πλαίσιο. Αφού γίνει αυτό, δίνει την άδεια στον αμέσως διπλανό του, στέλνοντας ένα ειδικό πλαίσιο ελέγχου, που ονομάζεται κουπόνι **(token)**. Το κουπόνι διαδίδεται πάνω στο λογικό δακτύλιο και μόνο αυτός που κατέχει το κουπόνι επιτρέπεται να μεταδίδει πλαίσια. Επειδή ένας μόνο σταθμός κάθε φορά κατέχει το κουπόνι, δεν γίνονται συγκρούσεις. Ένα σημαντικό σημείο είναι ότι η φυσική σειρά που συνδέονται οι σταθμοί με το καλώδιο, δεν είναι σημαντική. Επειδή το καλώδιο είναι ένα μέσο εκπομπής, κάθε σταθμός λαμβάνει κάθε πλαίσιο απορρίπτοντας αυτά τα οποία δεν απευθύνονται σε αυτόν. Όταν ένας σταθμός μεταβιβάζει το κουπόνι, στέλνει ένα πλαίσιο κουπονιού ειδικά κατευθυνόμενο στον λογικά βρισκόμενο δίπλα του στον δακτύλιο, ανεξάρτητα από το που είναι η φυσική θέση αυτού του σταθμού στο καλώδιο. Η αρτηρία με κουπόνι ορίζει τέσσερα είδη προτεραιότητας, **0**, **2**, **4** και **6** για την κυκλοφορία, με την **0** να είναι η χαμηλότερη και με τη **6** να είναι υψηλότερη προτεραιότητα. Είναι εύκολο να θεωρηθεί κάθε σταθμός εσωτερικά χωρισμένος σε τέσσερις υποσταθμούς, έναν για κάθε επίπεδο προτεραιότητας. Καθώς τα δεδομένα εισόδου έρχονται στο υποεπίπεδο **MAC**, ελέγχεται η προτεραιότητα αυτών και προωθούνται σε έναν από τους τέσσερις υποσταθμούς. Έτσι κάθε υποσταθμός τηρεί τη δική του ουρά πλαισίων που πρόκειται να μεταδοθούν. Όταν το κουπόνι εισέρχεται στο σταθμό μέσω του καλωδίου, διέρχεται εσωτερικά από τον υποσταθμό προτεραιότητας **6**, ο οποίος μπορεί να αρχίσει να μεταδίδει πλαίσια, εάν έχει κάποιο.




**Σχήμα 14. Πρότυπο 802.4**

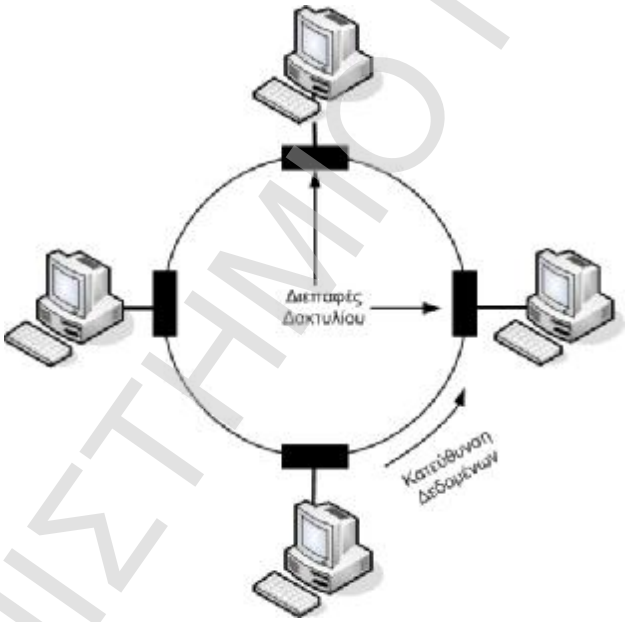
Όταν γίνει αυτό **(**ή όταν τελειώσει ο χρόνος του**),** το κουπόνι διέρχεται εσωτερικά από τον υποσταθμό προτεραιότητας **4,** ο οποίος μπορεί τότε να μεταδίδει πλαίσια έως ότου τελειώσει ο χρόνος του και στο σημείο αυτό το κουπόνι εισέρχεται στον υποσταθμό με προτεραιότητα **2.** Η διαδικασία αυτή επαναλαμβάνεται έως ότου ο υποσταθμός προτεραιότητας **0** έχει στείλει όλα του τα πλαίσια ή έχει τελειώσει ο χρόνος του**.** Στο σημείο αυτό το κουπόνι στέλνεται στον επόμενο σταθμό του δακτυλίου**.** Τα δίκτυα αρτηρίας που υποστηρίζουν το πρότυπο **IEEE 802.4** χρησιμοποιούν ένα πολύ αξιόπιστο καλώδιο όπως αυτό της τηλεόρασης**.** Επίσης είναι πιο προσδιοριστικά **(deterministic)** από ότι τα δίκτυα με το πρότυπο **IEEE 802.3,** αν και επαναλαμβανόμενες απώλειες του κουπονιού σε κρίσιμες στιγμές**,** δημιουργούν ένα κλίμα αστάθειας**.** Μπορεί ωστόσο να διαχειριστεί πολύ μικρά πλαίσια**.** Τα δίκτυα αυτά υποστηρίζουν τις προτεραιότητες**.** Ακόμη μπορούν να υποδιαιρέσουν την συχνότητα για να εξυπηρετήσουν υψηλής προτεραιότητας κυκλοφορία**,** όπως η ψηφιοποιημένη φωνή**.** Τέλος**,** συμπεριφέρονται πολύ καλά σε καταστάσεις υπερφόρτωσης**.**

### 2.5.6.5 Πρότυπο IEEE 802.5 (Token Passing Ring)

**Το Token Passing Ring (IEEE 802.5) [118]** πρωτόκολλο πρόσβασης ταιριάζει καλύτερα από το **Ethernet** για την υποστήριξη πολυμεσικών εφαρμογών**.** Ένας λόγος είναι το διαθέσιμο εύρος των **16 Mbps** σε αντίθεση με τα **10 Mbps.** Πιο σημαντικό όμως είναι η ύπαρξη πρωτοκόλλου προτεραιοτήτων τύπου **MAC.** Αυτό χρησιμοποιείται για να διαχωρίσει τα υψηλής προτεραιότητας δεδομένα από τα χαμηλής προτεραιότητας συνήθη δεδομένα**.** Τα δίκτυα δακτυλίου έχουν χρησιμοποιηθεί πάρα πολύ σε τοπικά και ευρείας περιοχής δίκτυα εδώ και πολλά χρόνια**.** Ανάμεσα στις πολλές και ελκυστικές δυνατότητες τους είναι και το γεγονός ότι ένας δακτύλιος στην πραγματικότητα δεν είναι ένα μέσο εκπομπής αλλά ένα σύνολο από ανεξάρτητες συνδέσεις από σημείο σε σημείο **(point-to-point)** που σχηματίζουν ένα κύκλο**.** Σε έναν δακτύλιο με κουπόνι μια ειδική ακολουθία από **bits,** που ονομάζονται κουπόνι **(token),** περιστρέφεται γύρω**-**γύρω στο δακτύλιο

όταν όλοι οι σταθμοί είναι αδρανείς. Όταν ένας σταθμός θέλει να μεταδώσει ένα πλαίσιο, πρέπει να συλλάβει το κουπόνι και να το απομακρύνει από το δακτύλιο πριν να μεταδώσει. Επειδή υπάρχει μόνο έναν κουπόνι, μόνο ένας σταθμός μπορεί να μεταδίδει σε μια δεδομένη στιγμή, έτσι λύνεται το πρόβλημα προσπέλασης στο κανάλι, με τον ίδιο τρόπο που λύνεται και στην αρτηρία με κουπόνι **(**Σχήμα **15).** Ένα επακόλουθο της σχεδίασης του δακτυλίου με κουπόνι είναι ότι ο ίδιος ο δακτύλιος πρέπει να έχει μια ικανοποιητική καθυστέρηση για να περιέχει ένα πλήρες κουπόνι που θα το περιστρέφει, όταν όλοι οι σταθμοί είναι αδρανείς. Η καθυστέρηση έχει δύο συνιστώσες:

- την καθυστέρηση **1-bit** που δημιουργείται από κάθε σταθμό και
- την καθυστέρηση διάδοσης του σήματος.




**Σχήμα 15. Πρότυπο 802.5**

Οι διασυνδέσεις του δακτυλίου έχουν δύο φάσεις λειτουργίας, τη φάση της ακρόασης και τη φάση της μετάδοσης. Στη φάση της ακρόασης τα **bits** εισόδου απλώς αντιγράφονται στην έξοδο, με χρονική καθυστέρηση ενός **bit.** Στη φάση της μετάδοσης, στην οποία ο σταθμός εισέρχεται μετά τη σύλληψη του κουπονιού, η διασύνδεση σπάει τη σύνδεση μεταξύ εισόδου και εξόδου, εισάγοντας τα δικά της δεδομένα στο δακτύλιο. Για να μπορεί να περνά από τη φάση της ακρόασης στη φάση της μετάδοσης σε χρόνο **1 bit,** η διασύνδεση συνήθως χρειάζεται να αποθηκεύει στην ενδιάμεση μνήμη ένα ή περισσότερα πλαίσια, παρά να τα φέρνει από το σταθμό μέσα σε τόσο σύντομο χρόνο. Καθώς τα **bits** που έχουν διαδοθεί γύρω από τον δακτύλιο επανέρχονται, απομακρύνονται εκτός δακτυλίου από τον πομπό. Ο σταθμός εκπομπής μπορεί είτε να τα αποθηκεύει για να τα συγκρίνει με

τα αρχικά δεδομένα, και να παρακολουθεί έτσι την αξιοπιστία του δακτυλίου, είτε να τα απορρίπτει. Αυτή η αρχιτεκτονική δακτυλίου δεν θέτει κανένα όριο στο μέγεθος του πλαισίου, επειδή το πλαίσιο ολόκληρο δεν εμφανίζεται ποτέ στον δακτύλιο σε μια δεδομένη χρονική στιγμή. Αφότου ένας σταθμός τελειώσει τη μετάδοση του τελευταίου **bit** του πλαισίου του πρέπει να ξαναδημιουργήσει το κουπόνι. Όταν το τελευταίο **bit** του πλαισίου έχει κάνει το γύρο και επιστρέφει, πρέπει να απομακρυνθεί, και η διασύνδεση πρέπει να επανέλθει αμέσως στη φάση της ακρόασης, για να αποφευχθεί η απομάκρυνση του κουπονιού το οποίο μπορεί να ακολουθεί, εάν κανείς άλλος σταθμός δεν το έχει απομακρύνει. Όσον αφορά την αξιοπιστία, παρέχει αρκετό εύρος για ένα περιορισμένο αριθμό πολυμεσικών εφαρμογών. Μπορεί να δώσει εγγυήσεις καθυστέρησης αν χρησιμοποιηθούν οι μηχανισμοί προτεραιότητας πρόσβασης και ο διαχειριστής του εύρους φάσματος. Επίσης το γεγονός ότι προσφέρει πολυδιανομή το **Token Ring** των **16 Mbps** το καθιστά κατάλληλη λύση για επικοινωνία με πολυμέσα. Τέλος η αποτελεσματικότητα αυτού του δικτύου σε καταστάσεις υπερφόρτωσης είναι πολύ αξιόλογη.

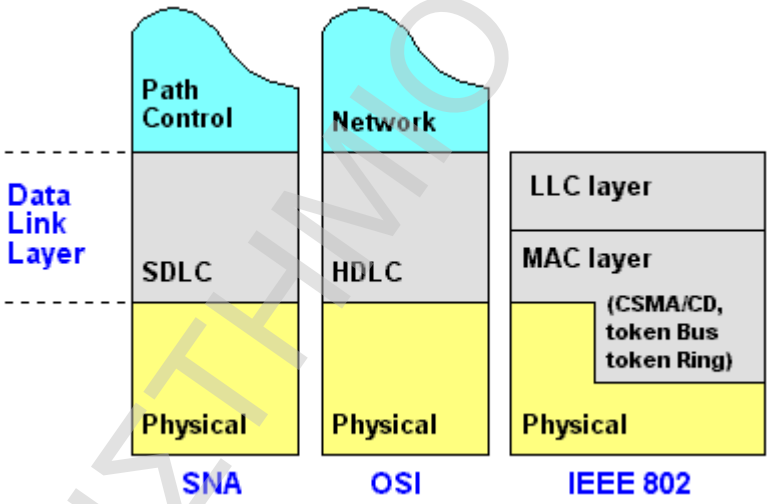
#### 2.5.6.6 Ισόχρονο Ethernet IEEE 802.9

Το Ισόχρονο **Ethernet** αποτελεί παραλλαγή του κλασσικού **Ethernet,** η οποία προτάθηκε από την επιτροπή **IEEE 802.9 [118],** στα πλαίσια των Τοπικών Δικτύων με ολοκλήρωση φωνής/δεδομένων **(IVD LAN-Integrated Voice Data LAN).** Αντικειμενικό στόχο της υποεπιτροπής **802.9,** αποτέλεσε η συνδυασμένη παροχή υπηρεσιών τοπικών δικτύων υπολογιστών και ισόγχρονων καναλιών όπως αυτά των ψηφιακών δικτύων ενοποιημένων υπηρεσιών **(ISDN)** χρησιμοποιώντας αθωράκιστο καλώδιο συνεστραμμένων ζευγών **(UTP).** Αποτελεί μια πιο έξυπνη τεχνική δίνοντας άλλα **6 Mbps** και παρέχοντας **64** ισόχρονα Β- κανάλια στο ίδιο καλώδιο με το στάνταρ **10 Mbps** σήμα **Ethernet.** Τα επιπλέον **6 Mbps** χρησιμοποιούνται σε ένα τύπο διαύλου- ένα σύγχρονο πλαίσιο στα **8 Khz** το οποίο είναι το φέρον των Β-καναλιών. Αυτή η λύση έχει το πλεονέκτημα να διατηρεί τα **10 Mbps** τεχνολογίας **Ethernet,** το οποίο σημαίνει ότι οι συσκευές πολυμέσων **ISDN** μπορούν να χρησιμοποιηθούν για τα Β- κανάλια. Το **Iso-Ethernet** έχει σχετικά περιορισμένο εύρος και δεν υποστηρίζει πολυδιανομή **(multicasting).** Παρέχει πραγματική ισόχρονη κίνηση και η παρόμοια δομή του με το **ISDN** κανάλι σχεδιάστηκε για ήχο ή **H.261** κωδικοποιημένη μετάδοση εικόνας, αλλά του λείπει απαραίτητο εύρος για **IVD, Motion JPEG** ή κωδικοποιημένο **MPEG (**Σχήμα **16).**

#### 2.5.6.7 Fast Ethernet - Demand Priority LAN (IEEE 802.12)

Μια άλλη τεχνική **LAN** των **100 Mbps** τυποποιείται από την **802.12 [24,118]** ομάδα εργασίας. Είναι μια εξέλιξη του κλασικού **Ethernet** και του **Token Passing Ring** των

**100 Mbps.** Τα δίκτυα αυτά πέρα του ότι υποστηρίζουν πλαίσια **Ethernet,** βασίζονται σε μια νέα μέθοδο ελέγχου πρόσβασης στο μέσο**.** Η μέθοδος περιγράφεται από το Πρωτόκολλο Ζήτησης Προτεραιότητας **(DPP - Demand Priority Protocol)** και μοιάζει πολύ με τον έλεγχο πρόσβασης που στηρίζεται στα κουπόνια**.** Αποτελεί μια πιο έξυπνη κωδικοποίηση χρησιμοποιώντας **4** ζεύγη καλωδίων αντί για ένα ζεύγος επιτυγχάνοντας μια δεκαπλάσια αύξηση της ταχύτητας με μέτρια αύξηση του εύρους και με κόστος παρόμοιο με αυτό της τεχνικής **10Base-**T**.** Το πρωτόκολλο αυτό**,** σχεδιάστηκε για να αντιμετωπίσει τους περιορισμούς στις αποστάσεις και στον μέγιστο αριθμό επαναληπτικών που εισάγει η μέθοδος **CSMA/CD,** καθώς και τους περιορισμούς που επιβάλλει στην υποστήριξη χρονικά κρίσιμων εφαρμογών**.** Σύμφωνα με το Πρωτόκολλο Ζήτησης Προτεραιότητας **(DPP),** ένας σταθμός όταν έχει δεδομένα προς μετάδοση υποβάλλει μια αίτηση στο τοπικό του κομβικό σημείο **(hub).** Κάθε **hub** έχει ένα συγκεκριμένο αριθμό θυρών και σε κάθε θύρα μπορεί να συνδεθεί ένας σταθμός**.** Αρχικά το δίκτυο είναι χωρίς δραστηριότητα**.**




**Σχήμα 16. Αρχιτεκτονική 802**

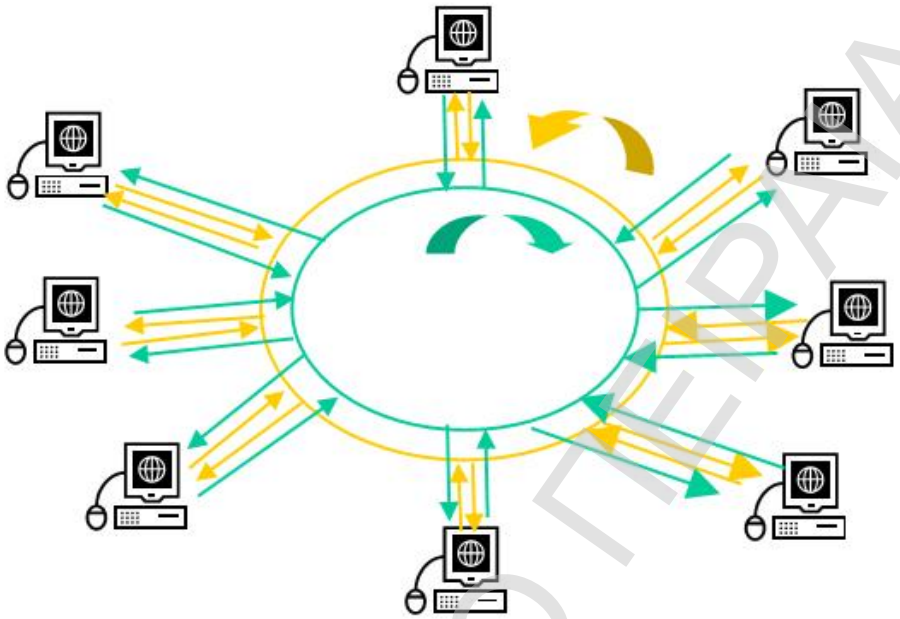
Οι σταθμοί αποστέλλουν το σήμα και το **Hub** τους απαντά με το ίδιο σήμα **(idle).** Όταν ένας σταθμός θελήσει να στείλει ένα πλαίσιο ζητάει την άδεια κάνοντας μία **"**αίτηση**".** Η επιλογή του ποιος σταθμός θα στείλει και με ποια σειρά γίνεται στο κομβικό σημείο **hub.** Η άδεια αποστολής ακολουθεί τη διαδικασία **"**εξυπηρέτηση εκ περιτροπής**".** Εάν για παράδειγμα κατά τη μετάδοση ενός πλαισίου από τον σταθμό **1,** υποβληθούν αιτήσεις κατά σειρά από τους σταθμούς **5, 3** και **2,** η σειρά εξυπηρέτησης θα είναι **2, 3** και **5.** Στη συνέχεια το **Hub** γνωστοποιεί στον σταθμό που έχει επιλέξει ότι μπορεί να μεταδώσει και αποστέλλει στους σταθμούς σήμα ελέγχου ότι ενδέχεται να λάβουν ένα πλαίσιο**.** Με την λήψη του σήματος οι σταθμοί κλείνουν τους σταθμούς τους και ο σταθμός αποστολής μεταδίδει το πλαίσιο στο **hub.** Το **hub** λαμβάνοντας το απαραίτητο τμήμα του πλαισίου αναγνωρίζει τον

σταθμό προορισμού και του μεταδίδει το πλαίσιο ενώ στους υπόλοιπους μεταδίδει το σήμα ελέγχου **idle**. Το **hub** με την ολοκλήρωση της μετάδοσης επιλέγει τον επόμενο σταθμό. Μια αίτηση στέλνεται στο κέντρο το οποίο παρέχει πρόσβαση βασισμένη σε μια διαδικασία επαναλαμβανόμενου ελέγχου αίτησης. Μέσω αυτής της διαδικασίας μπορεί να υπολογιστεί και να εγγυηθεί κάθε όριο καθυστέρησης. Για παράδειγμα ο χρόνος μετάδοσης **4 Kb** είναι **0.3 ms**. Ακόμα και όταν όλοι οι **30** σταθμοί στέλνουν αιτήσεις ταυτόχρονα η καθυστέρηση πρόσβασης είναι κάτω από **10 ms**. Μια διαδικασία διπλού επιπέδου προτεραιότητας θα μπορούσε να μειώσει ακόμα περισσότερο την καθυστέρηση. Σχετικά με το εύρος του, εξυπηρετεί περισσότερο από το **100Base-T** τις πολυμεσικές εφαρμογές, μη έχοντας περιορισμό όσον αφορά την καθυστέρηση πρόσβασης. Αν ένας διαχειριστής εύρους περιορίζει τον αριθμό της ροής των πολυμέσων χρησιμοποιώντας υψηλής προτεραιότητας πρόσβαση τότε μπορεί να εγγυηθεί την καθυστέρηση κάτω από τα **10 ms**. Η πολυδιανομή είναι δυνατή καθώς και η επικοινωνία με πολυμέσα για τοπολογίες μικρότερες από **30** σταθμούς.

#### 2.5.6.8 FDDI

Το **FDDI - Fiber Distributed Data Interface [62,118]** βασίζεται στο πρότυπο **802.5** είναι ένα υψηλής απόδοσης τοπικό δίκτυο δακτυλίου με κουπόνι χρησιμοποιώντας ως μέσο μετάδοσης οπτικές ίνες. Το μήκος του δακτυλίου μπορεί να φτάσει μέχρι και τα **100** χιλιόμετρα. Η ταχύτητά του φθάνει τα **100 Mbps** ενώ το πλήθος των σταθμών που μπορούν να συνδεθούν τους **500**. Η καλωδίωση του αποτελείται από δύο δακτυλίους ινών, ο ένας μεταδίδει με τη φορά των δεικτών του ρολογιού και ο άλλος μεταδίδει αντίθετα προς αυτή. Οι δύο δακτύλιοι αποκαλούνται: πρωτεύοντας και δευτερεύοντας. Ο δεύτερος δακτύλιος είναι εφεδρικός προσδίδοντας μεγαλύτερη αξιοπιστία στο δίκτυο. Αν σπάσουν και οι δύο δακτύλιοι στο ίδιο σημείο τότε οι δύο δακτύλιοι μπορούν να ενωθούν συγκροτώντας έναν μεγαλύτερο δακτύλιο διπλάσιο περίπου σε μήκος. Κάθε σταθμός διαθέτει διακόπτες που επιτρέπουν την ένωση των δύο δακτυλίων σε περίπτωση ζημιάς ή την παράκαμψη του σταθμού σε περίπτωση που ζητηθεί ή θεωρηθεί απαραίτητο για την αποφυγή τυχόν προβλημάτων που μπορεί να δημιουργηθούν κατά την συμμετοχή του στο δακτύλιο. Το **FDDI** καθορίζει δύο κατηγορίες σταθμών: τους σταθμούς Α και τους σταθμούς Β. Οι σταθμοί της πρώτης κατηγορίας συνδέονται και με τους δύο δακτυλίους, ενώ οι σταθμοί κατηγορίας Β συνδέονται μόνο με τον ένα δακτύλιο. Ανάλογα με το πόσο σημαντική είναι η ανοχή σφαλμάτων, μια εγκατάσταση μπορεί να επιλέξει μία από τις δύο κατηγορίες ή ακόμη και συνδυασμών σταθμών από τις δύο κατηγορίες. Στην διαδικασία της μετάδοσης βάση προτεραιότητας, το **FDDI**

υποστηρίζει σύγχρονο τρόπο κίνησης με το όριο καθυστέρησης να έχει τη δυνατότητα τροποποίησης κατά τη στιγμή εκκίνησης στο δακτύλιο **(**Σχήμα **17).**



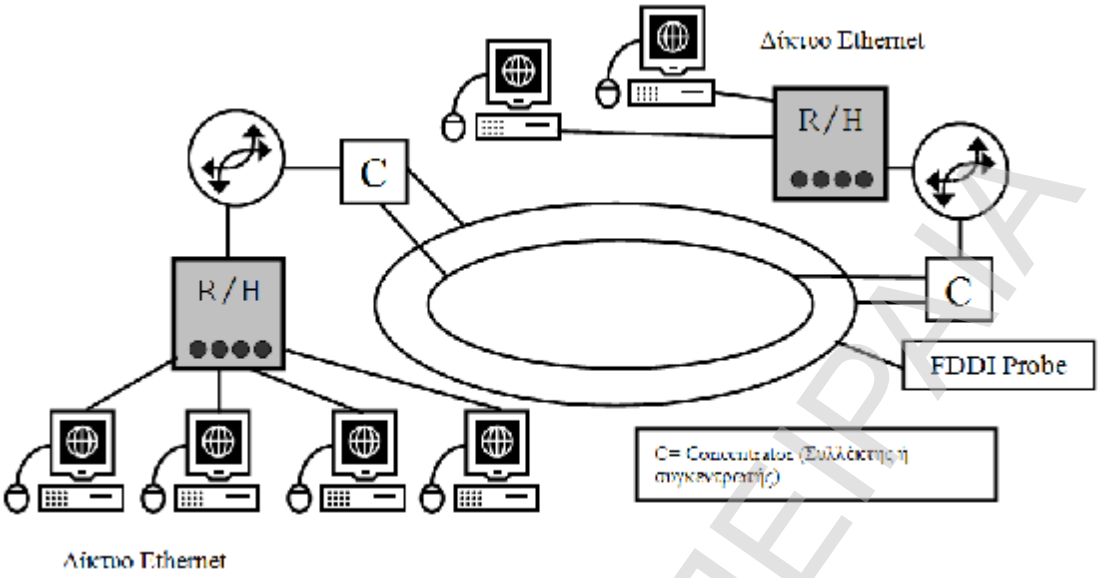
**Σχήμα 17. Δακτύλιος FDDI**

Μειώνοντας ωστόσο το όριο καθυστέρησης οδηγούμαστε σε αντίστοιχη μείωση της εκμετάλλευση του εύρους**.** Λόγω του μεγάλου εύρους στο **FDDI,** η καθυστέρηση μετάδοσης εξαρτάται από την καθυστέρηση πρόσβασης**.** Το **FDDI** χρησιμοποιεί πολύτροπες ίνες και η μετάδοση γίνεται με ακτίνες φωτός και όχι με **laser,** για λόγους ασφάλειας**.** Τα χαρακτηριστικά σχεδίασης του **FDDI** απαιτούν όχι περισσότερα από **1** σφάλμα ανά **2,5 x $10^{10}$ bits.** Το φυσικό επίπεδο του **FDDI** υλοποιείται με χρήση πολύτροπης οπτικής ίνας**,** συνήθως **62,5/125** μ**m** και **laser** στα **1300 nm.** Η απόσταση μεταξύ διαδοχικών σταθμών δεν μπορεί να ξεπερνά τα **2 km.** Το πλαίσιο του **FDDI** περιέχει μέχρι **4500 bytes.** Χρησιμοποιείται η κωδικοποίηση **4**B**/5**B**.** Η δομή του πλαισίου είναι παρόμοια με εκείνη του **token ring.** Το **FDDI** χρησιμοποιείται κυρίως ως η σπονδυλική στήλη πάνω στην οποία θα συνδεθούν τα διαφόρων τύπων τοπικά δίκτυα με χάλκινα καλώδια**.** Όσον αφορά την αξιοπιστία του **FDDI** υποστηρίζει επικοινωνία με πολυμέσα λόγω του μεγάλου του εύρους**,** σύγχρονο τύπο κίνησης και πολυδιανομή**.** Για την χρησιμοποίηση του **FDDI** σε εφαρμογές πολυμέσων**,** απαιτείται είτε ένας πρόσθετος διαχειριστής εύρους ή η διαθεσιμότητα του σύγχρονου τύπου κίνησης του **FDDI.** Τα πρωτόκολλα **FDDI** είναι βασισμένα στα πρωτόκολλα **802.5.** Για τη μετάδοση των δεδομένων**,** ένας σταθμός πρέπει πρώτα να πιάσει το κουπόνι**.** Κατόπιν μεταδίδει ένα πλαίσιο και το απομακρύνει όταν έρχεται ξανά πίσω**.** Μια διαφορά ανάμεσα στο **FDDI** και το **802.5** είναι ότι στο **802.5,** ένας σταθμός μπορεί να μη δημιουργήσει ένα νέο κουπόνι**,** έως ότου το πλαίσιό του έχει κάνει όλο το γύρο και επιστρέψει**.** Στο **FDDI** με **500**

σταθμούς και **100 km** από οπτικές ίνες, ο χρόνος που χάνεται περιμένοντας το πλαίσιο να κάνει το γύρο του δακτυλίου είναι σημαντικός. Για το λόγο αυτό επιτρέπεται σε έναν σταθμό να βάλει ένα νέο κουπόνι ξανά επάνω στον δακτύλιο μόλις μεταδώσει τα πλαίσιά του. Σ' έναν μεγάλο δακτύλιο μπορούν να υπάρχουν πολλά πλαίσια ταυτόχρονα.

### 2.5.6.9 FDDI II

Το **FDDI-II [62,118]** σχεδιάστηκε για καλύτερη υποστήριξη κίνησης σε πραγματικό χρόνο. Η ισόχρονη δυνατότητά του παρέχεται χρησιμοποιώντας χρονοθυρίδες σε ρυθμό **8 Khz** ανά δευτερόλεπτο. Όπως και το **FDDI**, το **FDDI-II** φθάνει σε ταχύτητα τα **100 Mbps**. Ένα σύνθετο σήμα και μια δυναμική διαδικασία διαχειρίζεται το εύρος ανάμεσα σε ασύγχρονα, σύγχρονα και ισόχρονα δεδομένα. Η τεχνική αυτή επιτρέπει την υποστήριξη κίνησης σταθερού ρυθμού δυαδικών ψηφίων, παρέχοντας ισόχρονα κανάλια καθυστέρησης. Το **FDDI-II** σχεδιάστηκε να υποστηρίζει κίνηση σταθερού ρυθμού. Παρέχει πραγματικά ισόχρονα κανάλια με καθυστέρηση της τάξεως μερικών μ**s**. Για να εξυπηρετήσει περιοδικές ισόχρονες αιτήσεις, το **FDDI-II** χρησιμοποιεί μία πολιτική περιοδικής μετάδοσης στην οποία οι ευκαιρίες μετάδοσης επαναλαμβάνονται κάθε **125** μ**s**. Αυτό το διάστημα έχει επιλεχθεί εξαιτίας του ότι αντιστοιχίζεται στο βασικό σύστημα αναφοράς της συχνότητας του ρολογιού που χρησιμοποιείται στα περισσότερα δημόσια δίκτυα τηλεπικοινωνιών παγκοσμίως. Σε αυτό το διάστημα, ένα ειδικό πλαίσιο που καλείται κύκλος **(cycle)**, δημιουργείται. Στα **100 Mbps, 1562,5 bytes** μπορούν να μεταδοθούν στα **125** μ**s**. Από αυτά, **1560 bytes** χρησιμοποιούνται για τα δεδομένα και **2,5 bytes** χρησιμοποιούνται για τα εσωτερικά κενά του πλαισίου. Τα **bytes** του πλαισίου μεταδίδονται μέσα από διαφορετικά κανάλια (για επικοινωνία μεταξύ δύο ή περισσότερων σταθμών), στον δακτύλιο (Σχήμα **18**). Για παράδειγμα, ένα κανάλι μπορεί να έχει το δικαίωμα να χρησιμοποιεί το **26**$^{o}$ και **122**$^{o}$ **byte** κάθε πλαισίου.




**Σχήμα 18. Δακτύλιος FDDI II**

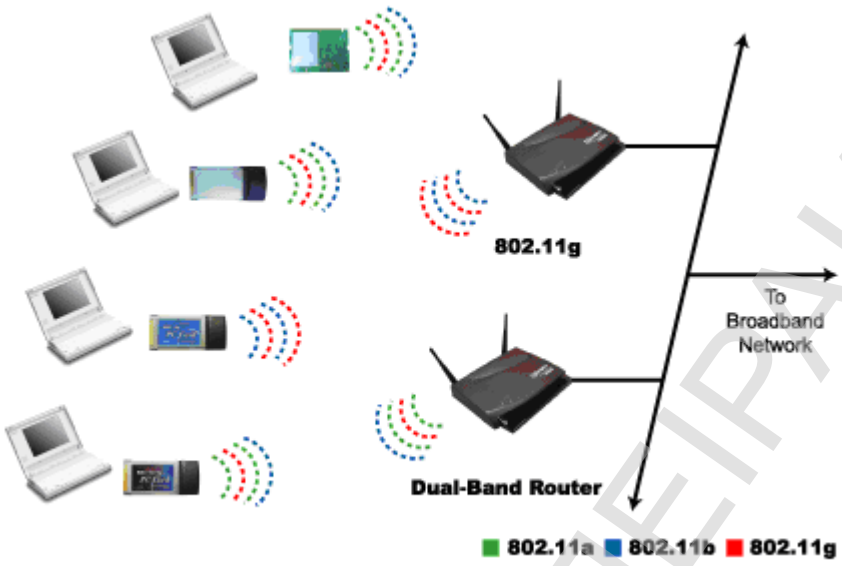
Αυτά τα **bytes** δεσμεύονται για το κανάλι με την έννοια ότι εάν κάποιος σταθμός που του ανήκει αυτό το κανάλι δεν το χρησιμοποιεί**,** οι υπόλοιποι σταθμοί δεν μπορούν να το χρησιμοποιήσουν και τα **bytes** θα παραμείνουν αχρησιμοποίητα**.** Τα **1560 bytes** του πλαισίου διαιρούνται σε **16** ευρυζωνικά κανάλια **(WBC – WideBand Channels)** των **96 bytes** έκαστο**.** Κάθε **WBC** παρέχει μία ζώνη συχνοτήτων για τα **96 bytes** για κάθε **125** μ**s** ή **6,144 Mbps.** Αυτό είναι ικανοποιητικό για να υποστηρίξουμε μία εκπομπή τηλεόρασης**, 4** υψηλής ποιότητας προγράμματα **stereo** ή **96** τηλεφωνικές συνδιαλέξεις**.** Μερικά από τα **16** ευρυζωνικά κανάλια μπορούν να διατεθούν για τη μεταφορά πακέτων και τα άλλα για ισόχρονες μορφές μεταφορές**.** Η κατανομή αυτή γίνεται σύμφωνα με τα πρωτόκολλα διαχείρισης των σταθμών**.** Έτσι για παράδειγμα**,** τα ευρυζωνικά κανάλια **1,5** και **7** μπορούν να χρησιμοποιηθούν για μεταφορά **(**μεταγωγή**)** πακέτων και τα κανάλια **2,3,4,6** και **8** μέχρι **15** να χρησιμοποιηθούν για ισόχρονη μορφή μεταφοράς ή μεταγωγή κυκλώματος**.** Μπορούμε επίσης να δεσμεύσουμε όλα τα κανάλια εξ ολοκλήρου για μεταγωγή κυκλώματος ή μεταγωγή πακέτου**.** Τα **16 WBC** χρησιμοποιούν **1536 bytes** από τα συνολικά **1560 bytes** του πλαισίου**.** Από τα εναπομείναντα **24 bytes, 12 bytes** χρησιμοποιούνται για την επικεφαλίδα του πλαισίου **(header)** και τα υπόλοιπα **12 bytes** δεσμεύονται προσωρινά για πιθανή μεταγωγή πακέτου**.** Αυτά τα **bytes** καλούνται **Dedicated Packet Group (DRG)** και διασφαλίζουν ότι τουλάχιστον **0,768 Mbps** από το εύρος ζώνης θα είναι διαθέσιμο για μεταγωγή πακέτων σε περίπτωση όπου όλα τα ευρυζωνικά κανάλια έχουν διατεθεί για μεταγωγή κυκλώματος**.**

| | Token Ring Passing | FDDI |
|---|---|---|
| **(+)** | **-**Μεγαλύτερη ικανότητα υπό αυξημένο φόρτο σε σχέση με το **Ethernet**<br>**-**Πολύ καλή δυνατότητα για **monitoring** της απόδοσης του δικτύου<br>-Χαμηλός ο λόγος **overhead/payload**<br>**- -Υ**ψηλά **deterministic** απόδοση | **-**Υψηλό εύρος ζώνης<br>**-**Δυνατότητες υποστήριξης σύγχρονης κίνησης και πολλαπλής εκπομπής |
| **(-)** | **-**Χαμηλή πυκνότητα πληθυσμού σε σχέση με το **Ethernet** που μπορεί να υποστηρίξει **1024** συσκευές ενώ το **Token Ring** περιορίζεται στις **260** | **-**Ο ορισμός ενός χαμηλού ορίου καθυστέρησης οδηγεί σε μείωση της χρήσης του εύρους ζώνης<br>**-**Ελάχιστες υλοποιήσεις **FDDI** υποστηρίζουν σύγχρονη κίνηση παρά το γεγονός οτι αυτή υποστηρίζεται σε επίπεδο προδιαγραφών πρωτοκόλλου**.** Ετσι**,** η χρήση του για πολυμεσικές εφαρμογές και επικοινωνίες απαιτεί την ύπαρξη ενός μηχανισμού υποστήριξης σύγχρονης κίνησης ή ενός επιπρόσθετου σχήματος διαχείρισης εύρους ζώνης**.** |

**Πίνακας 4.Πλεονεκτήματα και μειονεκτήματα Token Ring Passing και FDDI**

### 2.5.6.10 Πρότυπο 802.11

Το **1997** η IEEE υιοθέτησε το πρώτο πρότυπο ασύρματων τοπικών δικτύων **(WLAN) [35,39,118],** το IEEE **802.11**, Το πρότυπο αυτό καθορίζει τον έλεγχο πρόσβασης μέσου **(MAC)** και τα φυσικά στρώματα **(PHY)** για ένα **LAN** με ασύρματη σύνδεση**.** Το πρότυπο αυτό εξετάζει την τοπική δικτύωση όπου οι συνδεδεμένες συσκευές επικοινωνούν μέσω του αέρα με άλλες συσκευές που βρίσκονται κοντά η μια στην άλλη **(**Σχήμα **19)**.




**Σχήμα 19. Πρωτόκολλο 802.11**

Από την αρχική καθιέρωση της ομάδας εργασίας **802.11,** αυτή έχει επεκταθεί σε πολυάριθμες στοιχειώδεις ομάδες**,** που καθορίζονται από τα γράμματα **a** μέχρι το **i.** Οι ομάδες **a, b,** και **c** έχουν ολοκληρώσει την εργασία τους**,** και τα αποτελέσματα προστέθηκαν στα αρχικά πρότυπα**.** Οι λεπτομέρειες κάθε στοιχειώδους ομάδας εργασίας παρατίθενται κατωτέρω.

Οι στοιχειώδεις ομάδες εργασίας του προτύπου **802.11** είναι**:**

- Το πρωτόκολλο **802.11a**

Το επικυρωμένο πρότυπο **802.11a** εγκαθιδρύει ένα νέο εύρος συχνοτήτων για τα ασύρματα δίκτυα και αυξάνει τη ρυθμαπόδοση **(throughput)** για τα δίκτυα στα **54 Mbps.** Μεγάλο μέρος της αύξησης οφείλεται από τη χρήση της Ορθογώνιας Πολυπλεξίας με Διαίρεση Συχνότητας **(OFDM).**Το πρότυπο χρησιμοποιεί την περιοχή συχνοτήτων **UNII.** Αυτή η περιοχή συχνοτήτων διαχωρίζεται σε τρία μη συνεχόμενα τμήματα συχνότητας**:**

**Το UNII-1,** που είναι στη συχνότητα των **5.2 GHz.**

**Το UNII-2,** που είναι στη συχνότητα των **5.7 GHz**

**Το UNII-3** είναι στη συχνότητα των **5.8 GHz**

Μία συνηθισμένη παρανόηση είναι ότι το πρότυπο **802.11a** ήρθε πρώτο**.** Το **802.11b** αντιπροσωπεύει τη δεύτερη γενιά των ασύρματων δικτύων**,** αλλά βασικά το **802.11a** αντιπροσωπεύει την Τρίτη γενιά**.** Το πρότυπο **802.11a** δεν μπορεί**,** όπως μερικοί δηλώνουν**,** να αντικαταστήσει το **802.11b** ένα προς ένα διότι η

ρυθμαπόδοση και η εμβέλεια είναι πολύ διαφορετικές μεταξύ τους. Το **802.11b** έχει περίπου επτά φορές την εμβέλεια του **802.11a.**

- Το πρωτόκολλο **802.11b**

Το πρότυπο **802.11b,** είναι μία διόρθωση της **IEEE 802.11** προδιαγραφής, το οποίο αύξησε το **throughput** στα **11 Mbps** χρησιμοποιώντας το ίδιο εύρος συχνοτήτων**(2.4 GHz).**Το **802.11b** έχει ένα μέγιστο ρυθμό δεδομένων των **11 Mbps** και χρησιμοποιεί την ίδια μέθοδο **CSMA/CA** με το αρχικό πρωτόκολλο. Εξαιτίας της επιβάρυνσης του πρωτοκόλλου **CSMA/CA,** στην πράξη το μέγιστο **throughput** που μία εφαρμογή μπορεί να πετύχει είναι περίπου **5.9 Mbps** χρησιμοποιώντας **TCP** και **7.1** χρησιμοποιώντας **UDP.** Τα προϊόντα του **802.11 b** εμφανίστηκαν στην αγορά στις αρχές του **2000,** μιας και το **802.11b** είναι μία άμεση προέκταση της **DSSS** τεχνικής διαμόρφωσης που ορίζεται στο αρχικό πρότυπο. Τεχνικά, το πρότυπο **802.11b** χρησιμοποιεί το Συμπληρωματικό Κώδικα Διαμόρφωσης**(CCK)** ως τεχνική διαμόρφωσής του. Η δραματική αύξηση στη ρυθμαπόδοσης του **802.11b (**έναντι των αρχικών προτύπων**)** μαζί με τις ταυτόχρονες ουσιαστικές μειώσεις τιμών οδήγησε στη γρήγορη αποδοχή **802.11b** ως οριστική ασύρματη τεχνολογία του τοπικού **LAN.** Οι **802.11b** συσκευές πάσχουν από την παρέμβαση άλλων προϊόντων που λειτουργούν στη ζώνη των **2,4 GHz**. Στις συσκευές που λειτουργούν στη ζώνη αυτή συμπεριλαμβάνονται: φούρνοι μικροκυμάτων, **Bluetooth** συσκευές, συσκευές για την παρακολούθηση των βρεφών και ασύρματα τηλέφωνα. Τα ζητήματα παρέμβασης, και τα προβλήματα πυκνότητας χρηστών μέσα στη ζώνη **2,4 GHz** έχουν γίνει μια από τις σημαντικές ανησυχίες και έχει απογοητεύσει τους χρήστες. Στο **802.11b** χρησιμοποιείται μία **point-to-multipoint** διαμόρφωση, όπου ένα σημείο πρόσβασης επικοινωνεί μέσω μιας πανκατευθυντικής κεραίας με έναν ή περισσότερους νομαδικούς ή κινητούς πελάτες που βρίσκονται σε μια περιοχή κάλυψης γύρω από το σημείο πρόσβασης. Η εμβέλεια είναι **30** μ στα **11 Mbits/s** και **90** μ στα **1 Mbits/s.** Το συνολικό εύρος ζώνης διανέμεται δυναμικά κατ' απαίτηση σε όλους τους χρήστες σε ένα κανάλι. Με τις εξωτερικές κεραίες υψηλού κέρδους, το πρωτόκολλο μπορεί επίσης να χρησιμοποιηθεί στη σταθερή από σημείο σε σημείο επικοινωνία. Αυτό γίνεται συνήθως προκειμένου να αποφευχθούν δαπανηρές μισθωμένες γραμμές ή ο πολύ δυσκίνητος εξοπλισμός μικροκυματικών επικοινωνιών.

- Το πρωτόκολλο **802.11e**

Το πρωτόκολλο **802.11e-2005** ή **802.11e** είναι μια εγκεκριμένη τροποποίηση του **IEEE 802.11** που καθορίζει, επιπρόσθετα, ένα σύνολο ποιότητας υπηρεσιών**(QoS)** για το ασύρματο **LAN** που αφορά τις διαμορφώσεις του **MAC** επιπέδου. Το πρότυπο θεωρείται κρίσιμης σημασίας για τις εφαρμογές που παρουσιάζουν ευαισθησία στις

καθυστερήσεις, όπως η Μετάδοση Φωνής μέσω Διαδικτύου **IP(VoIP).** Η τροποποίηση αυτή έχει ενσωματωθεί δημοσιευμένο IEEE **802.11-2007** πρότυπο.

Το **802.11** είναι ένα **IEEE** πρότυπο που επιτρέπει συσκευές όπως φορητοί υπολογιστές ή κινητά τηλέφωνα για να δημιουργήσει ένα ασύρματο τοπικό **LAN** ευρέως χρησιμοποιημένο στο σπίτι, το γραφείο και μερικά εμπορικά κέντρα.

Το **802.11e** ενισχύει τις δύο καταστάσεις λειτουργίας **DCF** και **PCF** που χρησιμοποιούνται στο **IEEE 802.11,** μέσω μιας νέας λειτουργίας συντονισμού: Υβριδική Λειτουργία Συντονισμού **(HCF).** Στο **HCF,** υπάρχουν δύο μέθοδοι πρόσβασης καναλιών, παρόμοιες με εκείνες που καθορίζονται στο **MAC** του **802.11: HCF** Ελεγχόμενης Πρόσβασης Καναλιού **(HCCA)** και Ενισχυμένη Κατανεμημένη Πρόσβαση Καναλιού **(EDCA).** Και το **EDCA** και το **HCCA** καθορίζουν τις κατηγορίες κυκλοφορίας **(TC).** Παραδείγματος χάριν, το ηλεκτρονικό ταχυδρομείο θα μπορούσε να καταταχτεί σε μια κατηγορία χαμηλής προτεραιότητας, και η μετάδοση φωνής πάνω από τα ασύρματα τοπικά δίκτυα **(VoWLAN)** θα μπορούσε να καταταχτεί σε μια κατηγορία υψηλής προτεραιότητας.

**EDCA**

Με Ενισχυμένη Κατανεμημένη Πρόσβαση Καναλιού **(EDCA),** η κυκλοφορία υψηλής προτεραιότητας έχει υψηλότερη πιθανότητα αποστολής από την κυκλοφορία χαμηλής προτεραιότητας: ένας σταθμός με κυκλοφορία υψηλής προτεραιότητας περιμένει λίγο λιγότερο προτού να στείλει το πακέτο του, κατά μέσον όρο, από έναν σταθμό με τη κυκλοφορία χαμηλής προτεραιότητας. Επιπλέον, σε κάθε επίπεδο προτεραιότητας ορίζεται μια Ευκαιρία Μετάδοσης **(TXOP).** Μία **TXOP** είναι ένα περιορισμένο χρονικό διάστημα κατά τη διάρκεια του οποίου ένας σταθμός μπορεί να στείλει όσο το δυνατόν περισσότερα πλαίσια μπορεί **(**εφ' όσον δεν επεκτείνεται η διάρκεια των μεταδόσεων πέρα από τη μέγιστη διάρκεια του **TXOP).** Εάν ένα πλαίσιο είναι πάρα πολύ μεγάλο για να διαβιβαστεί σε ένα ενιαίο **TXOP,** πρέπει να τεμαχιστεί σε μικρότερα πλαίσια

**HCCA**

Η λειτουργία της **HCCA** είναι παρόμοια με αυτή της **PCF.** Εντούτοις, σε αντίθεση με τη **PCF,** στην οποία το διάστημα μεταξύ δύο πλαισίων ελέγχου διαιρείται σε δύο περιόδους: **CFP** και **CP,** η **HCCA** επιτρέπει στα **CFPs** να ξεκινούν σχεδόν οποτεδήποτε κατά τη διάρκεια μιας **CP.** Αυτό το είδος του **CFP** καλείται Φάση Ελεγχόμενης Πρόσβασης **(CAP)** στο **802.11e.** Μια **CAP** αρχικοποιείται από το σημείο πρόσβασης, όποτε αυτό θέλει να στείλει ένα πλαίσιο σε έναν σταθμό, ή να λάβει ένα πλαίσιο από έναν σταθμό, κατά τρόπο ελεύθερου ανταγωνισμού. Στην πραγματικότητα, το **CFP** είναι μια **CAP** επίσης. Κατά τη διάρκεια μιας **CAP,** ο

υβριδικός συντονιστής **(HC)** που είναι επίσης το σημείο πρόσβασης έλεγχει η πρόσβαση στο μέσο**.** Κατά τη διάρκεια του **CP,** όλη η λειτουργία σταθμών είναι σε **EDCA.** Η άλλη διαφορά με το **PCF** είναι ότι η κατηγορία κυκλοφορίας **(TC)** και τα ρεύματα **(TS)** κυκλοφορίας καθορίζονται**.** Αυτό σημαίνει ότι το **HC** δεν περιορίζεται στον ανά**-**σταθμό σειρά και μπορεί να παρέχει ένα είδος υπηρεσίας ανά**-**σύνοδο**.** Επίσης**,** το **HC** μπορεί να συντονίσει αυτά τα ρεύματα ή τις συνόδους σε οποιονδήποτε αλγόριθμο προτεραιότητας επιλέγει **(**όχι μόνο **round-robin).** Επιπλέον**,** οι σταθμοί δίνουν τις πληροφορίες για τα μήκη των ουρών αναμονής τους για κάθε κατηγορία κυκλοφορίας **(TC).** Το **HC** μπορεί να χρησιμοποιήσει αυτές τις πληροφορίες για να δώσει προτεραιότητα σε έναν σταθμό έναντι κάποιου άλλου**,** ή να ρυθμίσει καλύτερα το μηχανισμό σχεδιασμού του**.** Μια άλλη διαφορά είναι ότι στους σταθμούς που δίνεται ένα **TXOP:** μπορούν να στείλουν τα πολλαπλά πακέτα σε μια σειρά**,** για ένα δεδομένο χρονικό διάστημα που επιλέγεται από το **HC.** Κατά τη διάρκεια του **CP,** το **HC** επιτρέπει στους σταθμούς για να στείλει τα στοιχεία με την αποστολή των πλαισίων **CF-Poll.**

Η **HCCA** θεωρείται γενικά η πιο προηγμένη **(**και σύνθετη**)** λειτουργία συντονισμού**.** Με την **HCCA,** η **QoS** μπορεί να διαμορφωθεί με τη μεγάλη ακρίβεια**.** Οι σταθμοί που υποστηρίζουν **QoS** έχουν τη δυνατότητα να ζητήσουν συγκεκριμένες παραμέτρους μετάδοσης **(**ρυθμό δεδομένων**,** κ**.**λ**.**π**.)** γεγονός που επιτρέπει τις προηγμένες εφαρμογές όπως **VoIP** και το βίντεο να λειτουργούν αποτελεσματικότερα σε ένα δίκτυο **Wi-Fi** δίκτυο**.**

- Το πρωτόκολλο **802.11g**

Το **IEEE 802.11g-2003** ή **802.11g,** είναι μια τροποποίηση της προδιαγραφής **IEEE 802.11** που επέκτεινε τη ρυθμαπόδοση σε μέχρι **54** M**bps** χρησιμοποιώντας την ίδια περιοχή συχνοτήτων των **2,4 GHz** όπως και το **802.11b.** Αυτή η προδιαγραφή με το εμπορικό όνομα **Wi-Fi** έχει εφαρμοστεί σε όλο τον κόσμο**.** Το πρωτόκολλο **802.11g** βρίσκεται στο άρθρο **19** του δημοσιευμένου **IEEE 802.11-2007** προτύπου**.**

Το **802.11g** ήταν το τρίτο πρότυπο διαμόρφωσης για το ασύρματο τοπικό **LAN.** Λειτουργεί στη ζώνη των **2,4 GHz (**όπως και το **802.11b)** αλλά λειτουργεί σε ένα ρυθμό δεδομένων των **54 Mbps. Το** υλικό του **802.11g** είναι πλήρως συμβατό με το υλικό του προτύπου **802.11b** ωστόσο για να επιτευχθεί η συνεργασία τους χρειάστηκε αρκετή τεχνική προσπάθεια**.** Σε ένα **11g** δίκτυο**,** εντούτοις**,** η παρουσία ενός **802.11b** θα μειώσει σημαντικά την ταχύτητα του γενικού δικτύου **802.11g.**

Το σχήμα διαμόρφωσης που χρησιμοποιείται στο πρωτόκολλο **802.11g** είναι ορθογώνια πολυπλεξία με διαίρεση συχνότητας **(OFDM)** αντιγραμμένο από **802.11a** με ρυθμούς δεδομένων **6, 9, 12, 18, 24, 36, 48,** και **54 Mbps,** και επανέρχεται **CCK**

**(**όπως τ**ο** πρότυπ**ο 802.11b)** για **5,5** και **11 Mbps** και **DBPSK+DSSS** για **1** και **2 Mbps.** Ακόμα κι αν το **802.11g** λειτουργεί στην ίδια ζώνη συχνότητας με το **802.11b,** μπορεί να επιτύχει υψηλότερα ρυθμούς δεδομένων λόγω της κληρονομιάς του από το **802.11a.**

Τα προτεινόμενα πρότυπα του **802.11g,** που ακολούθησαν υιοθετήθηκαν γρήγορα από τους καταναλωτές**,** κάνοντας αρχή από τον Ιανουάριο του **2003,** πολύ πριν από την επικύρωση**,** λόγω της επιθυμίας για υψηλότερες ταχύτητες**,** και τη μείωση του κόστους παραγωγής**.** Μέχρι το καλοκαίρι του **2003,** τα περισσότερα προϊόντα που υποστήριζαν τα πρότυπα **802.11a** και **802.11b** υποστήριζαν πλέον και το πρότυπο **802.11g.**

Παρά τη σημαντική αποδοχή του**,** το πρωτόκολλο **802.11g** πάσχει από την ίδια παρεμβολή με **802.11b** στην ήδη βεβαρυμμένη ζώνη των **2,4 GHz.** Οι συσκευές που λειτουργούν σε αυτήν την ζώνη περιλαμβάνουν**:** φούρνους μικροκυμάτων**,** **Bluetooth** συσκευές**,** συσκευές για την παρακολούθηση βρεφών και **(**στις ΗΠΑ**)** ψηφιακά ασύρματα τηλέφωνα που διαχειριστούν τα προβλήματα που προκύπτουν από τις παρεμβολές**.** Επιπλέον η επιτυχία των προτύπων έχει προκαλέσει τα προβλήματα **«**συχνοτικής πυκνότητας**»** που οφείλεται στη συσσώρευση πληθυσμού στις αστικές περιοχές**.** Αυτή η συσσώρευση μπορεί να προκαλέσει μια δυσάρεστη εμπειρία χρηστών δεδομένου ότι ο αριθμός μη**-**επικαλυπτόμενων χρησιμοποιήσιμων καναλιών είναι μόνο **3** στα έθνη της **FCC (CH 1, 6, 11)** ή **4** στα ευρωπαϊκά έθνη **(CH 1, 5, 9, 13).**

- Το πρωτόκολλο **802.11h**

**Το IEEE 802.11h-2003**, ή **802.11h,** αναφέρεται στην τροποποίηση που προστίθεται στο πρότυπο IEEE **802.11** για επεκτάσεις διαχείρισης του φάσματος και της μεταφερσιμότητας**.** Λύνει τα προβλήματα όπως την παρεμβολή με τους δορυφόρους και τα ραντάρ χρησιμοποιώντας την ίδια ζώνη συχνότητας **5 GHz.** Αρχικά**,** είχε ως σκοπό να απευθύνεται στις ευρωπαϊκές διατάξεις αλλά τώρα ισχύει σε πολλές άλλες χώρες**.** Το πρότυπο παρέχει Δυναμική Επιλογή Συχνότητας **(DFS)** και **TPC** στο **802.11a MAC.** Έχει ενσωματωθεί πλήρες **802.11-2007** πρότυπο**.**

Το **DFS** εξασφαλίζει ότι τα κανάλια που περιέχουν ραντάρ αποφεύγονται από ένα σημείο πρόσβασης **(AP)** και η ενέργεια διαδίδεται πέρα από τη ζώνη για να μειώσει την παρέμβαση στους δορυφόρους**.** Το **TPC** εξασφαλίζει ότι η μέση δύναμη είναι λιγότερη από το καθορισμένο μέγιστο να μειωθεί την παρεμβολή στους δορυφόρους**.**

- Το πρωτόκολλο **802.11n**

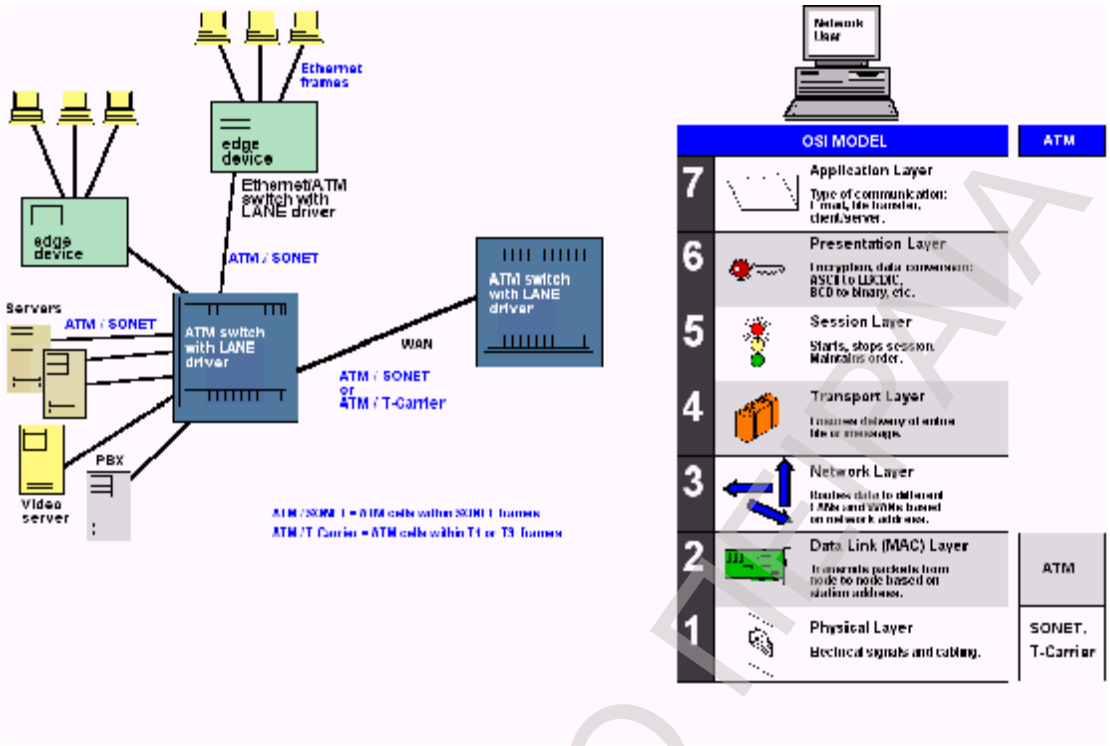
Το πρότυπο **802.11n** είναι μια προτεινόμενη τροποποίηση του IEEE **802.11-2007** για να βελτιώσει την απόδοση συστημάτων. Το **802.11** είναι ένα IEEE πρωτόκολλο που επιτρέπει σε συσκευές όπως οι φορητοί υπολογιστές ή τα κινητά τηλέφωνα να δημιουργήσουν έναν ασύρματο τοπικό **LAN** ευρέως χρησιμοποιημένος στο σπίτι, το γραφείο και σε μερικά εμπορικά κέντρα. Αν και το πρότυπο **802.11n** είναι ακόμα στο στάδιο «σχεδίων» σύμφωνα με το IEEE, πολλοί προμηθευτές υλικού πωλούν ήδη το μη ολοκληρωμένο υλικό ,το οποίο είναι βασισμένο στο πιο πρόσφατο σχέδιο. Αυτοί οι προμηθευτές προσδοκούν ότι η τελική έκδοση δεν θα είναι σημαντικά διαφορετική από το σχέδιο. Μια λογισμική αναπροσαρμογή πρέπει να είναι σε θέση να καταστήσει το τρέχον μη ολοκληρωμένο υλικό (αυτό που βρίσκεται ακόμη στη φάση του σχεδίου) συμβατό με την τελική έκδοση.

Το πρότυπο **802.11n** αναμένεται να είναι σημαντικά γρηγορότερο από τα προηγούμενα πρότυπα, όπως το **802.11b** και το **802.11g**, με πολλούς εμπειρογνώμονες να πιστοποιούν ότι αυτή η ασύρματη τεχνολογία θα επιτρέψει τελικά στους καταναλωτές να κινηθούν πέρα από παραδοσιακό **10/100** ενσύρματο τοπικό **LAN**.

Το **802.11n** στηρίζεται στα προηγούμενα **802.11** πρότυπα με την προσθήκη της τεχνολογίας **MIMO** στο φυσικό στρώμα. Η τεχνολογία **MIMO** χρησιμοποιεί πολλαπλές κεραίες πομπού και δέκτη για να βελτιώσει την απόδοση συστημάτων.

### 2.5.7 Ασύγχρονος Τρόπος Μεταφοράς στα Τοπικά Δίκτυα

Η εξομοίωση Τοπικών Δικτύων είναι μια δικτυακή ικανότητα που επιτρέπει σε δίκτυα τύπου **Ethernet/**Περάσματος κουπονιού να επικοινωνούν απευθείας με σταθμούς **ATM [42,79]** (και αντιστρόφως) σαν να χρησιμοποιούν το ίδιο πρωτόκολλο. Τα τοπικά δίκτυα υπολογιστών προσφέρουν υπηρεσίες "χωρίς σύνδεση" με βάση την αρχή της "καλύτερης προσπάθειας", δηλαδή δεν επανεκπέμπουν πακέτα τα οποία έχουν χαθεί ή δεν είναι έγκυρα, μεταφέροντας πακέτα δεδομένων μεταβλητού μήκους. Επίσης, υποστηρίζουν μεταφορά από σημείο σε σημείο, πολλαπλή εκπομπή **(multicast)** και εκπομπή **(broadcast)**. Πολλά από τα υπάρχοντα πρωτόκολλα στηρίζονται στη δυνατότητα εκπομπής. Από τους χρήστες δε ζητείται η εγκατάσταση σύνδεσης πριν την υποβολή δεδομένων για μετάδοση, ούτε και απαιτείται η περιγραφή των χαρακτηριστικών της κίνησης πριν από τη μετάδοση. Οι χρήστες απλά υποβάλουν το φορτίο τους στο τοπικό δίκτυο, το οποίο και δυναμικά διαμοιράζει το διαθέσιμο εύρος ζώνης μεταξύ των ενεργών χρηστών (Σχήμα **20**).




**Σχήμα 20. Αρχιτεκτονική ATM**

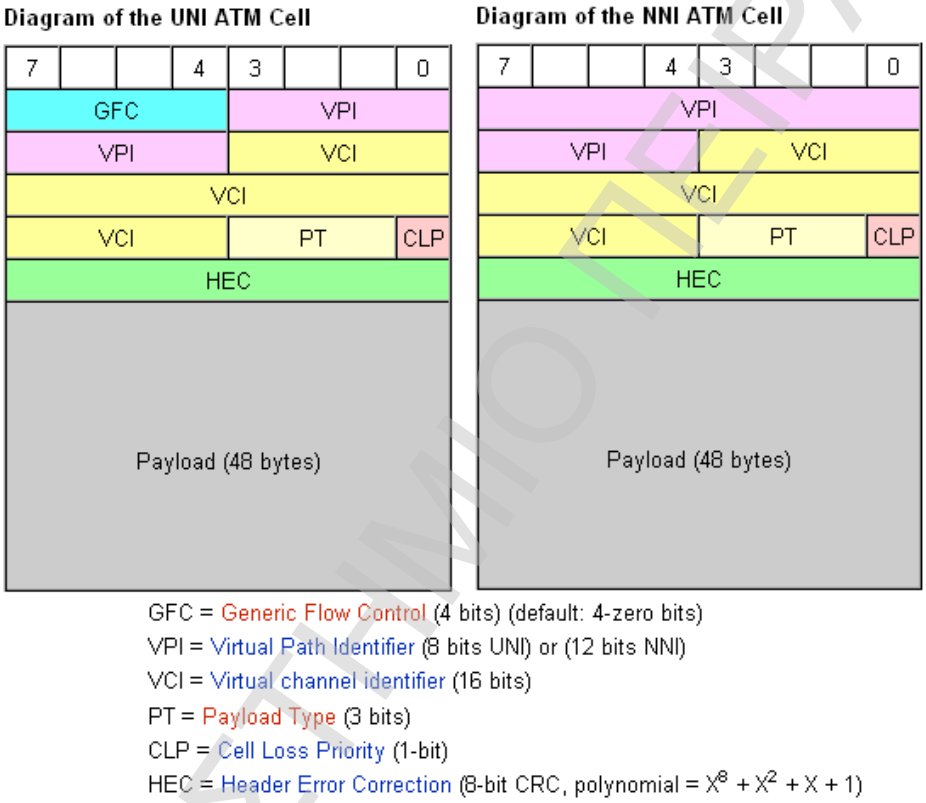
Ο πλέον βασικός παράγοντας εισαγωγής της τεχνολογίας ATM σε περιβάλλοντα τοπικών δικτύων, είναι η λεγόμενη "εξομοίωση Τοπικού Δικτύου" **(LAN emulation).** Ο όρος αναφέρεται στην τεχνική εξομοίωσης δικτύων **IEEE 802 (Ethernet** και **Token Ring)** πάνω από υποδομή ATM, δηλαδή προσπάθειας "μίμησης" από ένα **ATM LAN** της συμπεριφοράς ενός δικτύου **IEEE 802.3** ή **802.5.** Για να γίνει εύκολα αντιληπτή η διαδικασία εξομοίωσης τοπικών δικτύων, θα πρέπει αρχικά να "καταγραφούν" εκείνα τα χαρακτηριστικά τους, που δεν μπορούν να παρασχεθούν απευθείας από ένα δίκτυο ATM και επομένως πρέπει να εξομοιωθούν. Οι διαφορές των τοπικών δικτύων με τα ATM δίκτυα και οι οποίες πρέπει να επιλυθούν αφορούν τα εξής θέματα:

- Κατάτμηση και επανασύσταση των πλαισίων των τοπικών δικτύων
- Καθορισμός μεθόδων που θα παρέχουν υπηρεσίες χωρίς σύνδεση σε ένα περιβάλλον ATM
- Καθορισμός μεθόδων που θα παρέχουν υπηρεσίες **broadcast/multicast**
- Ανάγκη προσφοράς παρόμοιας με αυτή της "καλύτερης προσπάθειας", είτε μέσω της δημιουργίας "αποθέματος" εύρους ζώνης στο επίπεδο ATM, είτε απευθείας παροχή της δυνατότητας από το ATM (χρησιμοποιώντας την υπηρεσία **ABR).** Συνοδευτικά δημιουργείται η ανάγκη μιας μεθόδου ελέγχου συμφόρησης, μέσω

ενός μηχανισμού που θα στηρίζεται είτε στον ρυθμό **(rate-based)** είτε στην παρεχόμενη **"**πίστωση**" (credit based).**

Η μεθοδολογία εξομοίωσης αφορά**:**

- Τα δομικά στοιχεία εξομοίωσης ενός **LAN** από ATM και τις απαιτούμενες μεταξύ τους συνδέσεις
- Το μηχανισμό εξομοίωσης τοπικού δικτύου σύμφωνα με το ATM **Forum.**




**Σχήμα 21. Δομή ATM πλαισίου**

Γενικά η εξομοίωση ενός τοπικού δικτύου χρησιμοποιώντας ATM**,** απαιτεί τόσο τη συνεργασία των σταθμών εργασίας όσο και την υλοποίηση υπηρεσιών που θα παρέχονται κεντρικά**.** Συγκεκριμένα **[79]:**

α**)** Σε κάθε σταθμό του τοπικού δικτύου εγκαθίσταται ο λεγόμενος **"**πελάτης εξομοίωσης τοπικού δικτύου**" (LEC - LAN Emulation Client).**

β**)** Στο δίκτυο εισάγονται τρία νέα δομικά στοιχεία

- Ο διαθέτης εξυπηρέτησης πλαισίων εκπομπής και **"**αγνώστων**"** πλαισίων σε όλους τους άμεσα συνδεδεμένους πελάτες εξομοίωσης **LANs.**
- Ο διαθέτης εξομοίωσης τοπικού δικτύου **(LES - LAN Emulation Server),** με αντικείμενο την υποστήριξη του **"**πρωτοκόλλου ανάλυσης διεύθυνσης για εξομοίωση τοπικού δικτύου**".** Το πρωτόκολλο αυτό απαιτείται προκειμένου ο **LEC**

αποστολής να βρει την ATM διεύθυνση του **LEC** προορισμού**,** που είναι υπεύθυνος για μια συγκεκριμένη **MAC** διεύθυνση προορισμού**.**

- Ο διαθέτης σύνθεσης της εξομοίωσης Τοπικού Δικτύου**.** Στο διαθέτη αυτό συνδέεται ένας πελάτης **(LEC)** προκειμένου να πληροφορηθεί την ATM διεύθυνση του υπεύθυνου **LES.**

Σε ένα περιβάλλον χρήστη **/** εξυπηρετητή **(client/server),** η εξομοίωση των τοπικών δικτύων **(LAN - Local Area Networks)** μπορεί να συνοψιστεί στα ακόλουθα **(**Σχήμα **21):**

- Η εξομοίωση **LAN** παρέχει μηχανισμούς για υπάρχουσες **client/server** εφαρμογές στα **LAN** να **"**τρέξουν**"** πάνω σε **ATM** δίκτυα χωρίς τροποποίηση**.**
- Η εξομοίωση των **LAN** χρησιμοποιεί τα **ATM** ως **"**σκελετό**"** για την αλληλοσύνδεση των υπαρχόντων **LANs** προκειμένου να επιτευχθεί υψηλότερο πλάτος συχνότητας**.**
- Η εξομοίωση **LAN** επιτρέπει ποικίλες ακολουθίες **LANs** ή **Virtual LANs (VLANs)** να μοιράζονται από κοινού τα ίδια **ATM** δίκτυα**.** Η ιδιότητα αυτή επιτρέπει ένα φυσικό δίκτυο να εμφανίζεται σαν διαφορετικά λογικά δίκτυα**.**
- Η εξομοίωση **LAN** πρέπει να εφαρμόζεται απευθείας στα **ATM** δίκτυα**.**

# 3 Ασφάλεια δικτύων

## 3.1 Εισαγωγή

Το Διαδίκτυο άρχισε πειραματικά στα τέλη της δεκαετίας του **'60** από την **Advanced Research Projects Agency (ARPA) [108]** του Αμερικανικού Υπουργείου Αμύνης**.** Το Δεκέμβριο του **1969** το πειραματικό δίκτυο είχε **4 online** κόμβους συνδεδεμένους με κυκλώματα των **56 kbps.** Η τεχνολογία αυτή αποδείχθηκε αξιόπιστη και οδήγησε σε δύο παρόμοια στρατιωτικά δίκτυα**,** το **MILNET** στις ΗΠΑ και το **MINET** στην Ευρώπη**.** Ακολούθησαν αρκετές ακόμη προσπάθειες πειραματικών δικτύων μέχρι την εγκαθίδρυση του Διαδικτύου**,** όπως το γνωρίζουμε στην εποχή μας**.** Το Διαδίκτυο είναι ένα παγκόσμιας κλίμακας δίκτυο **(World Wide Web)[105],** το οποίο συνδέει ετερογενή**,** ως προς τεχνολογία υλοποίησης και πρωτόκολλα επικοινωνίας**,** δίκτυα**.** Στη συνήθη περίπτωση**,** συνδέονται Τοπικά Δίκτυα **(Local Area Networks)** που επικοινωνούν μεταξύ τους με το γνωστό πρωτόκολλο **TCP/IP.** Το **IP** πρωτόκολλο αναλαμβάνει τη διασύνδεση ετερογενών δικτύων και τη διευθυνσιοδότηση των κόμβων διασύνδεσης **(Network Layer** στο μοντέλο **ISO/OSI),** ενώ το **TCP** πρωτόκολλο αφορά στη αξιόπιστη μεταφορά της πληροφορίας μεταξύ των κόμβων **(Transport Layer** στο μοντέλο **ISO/OSI) [54].**

Κατά το σχεδιασμό του **IP (Internet Protocol –** Διαδικτυακό Πρωτόκολλο**),** στόχος ήταν η δημιουργία ενός πρωτοκόλλου που θα διασύνδεε ετερογενή δίκτυα**,** με τέτοιο τρόπο ώστε οι υπολογιστές να είναι μοναδικά προσδιορισμένοι**,** να μπορούν να ανταλλάσσουν δεδομένα με κοινή μορφοποίηση και να μεταδίδουν δεδομένα χωρίς να γνωρίζουν στοιχεία για τη δομή και τη μορφή των δικτύων που ανήκουν οι παραλήπτες**.** Αρχικά τα δίκτυα που διασυνδέθηκαν αφορούσαν πανεπιστήμια ή ερευνητικά κέντρα και για αυτό το λόγο ουδέποτε τέθηκε θέμα ασφάλειας στο σχεδιασμό του πρωτοκόλλου**.** Μοιραία**,** λοιπόν**,** σε επίπεδο δικτύου απουσιάζουν οι ασφαλιστικές δικλείδες**,** ενώ θα έπρεπε σαφέστατα να ήταν ενσωματωμένες σε αυτό**.** Με τη τεράστια εξάπλωση του διαδικτύου ανά τον κόσμο εμφανίστηκε το κρίσιμο ζήτημα της ασφάλειας και προφανώς η αντιμετώπισή του εντοπιζόταν πλέον στα υψηλότερα επίπεδα**,** όπως αυτό των Εφαρμογών **[63,118] (Application Layer)** ή σπανιότερα στο επίπεδο Μεταφοράς **(Transportation Layer).** Παραδείγματα της παραπάνω διαπίστωσης είναι το πρωτόκολλο **Secure Sockets Layer (SSL) [119],** που λειτουργεί στο επίπεδο μεταφοράς και το πρωτόκολλο **Secure HTTP (SHTTP)[118],** που λειτουργεί στο επίπεδο εφαρμογής**.** Μία ακόμη μέθοδος ενίσχυσης της ασφάλειας που εμφανίστηκε τα τελευταία χρόνια και έχει εξαπλωθεί είναι αυτή της δημιουργίας Ιδεατών Ιδιωτικών Δικτύων **(Virtual Private Networks - VPN) [50,118].** Βασική φιλοσοφία της εν λόγω μεθόδου είναι η κωδικοποίηση του

μεταδιδόμενου πακέτου και η εν συνεχεία ενσωμάτωσή του σε ένα νέο πακέτο που μεταδίδεται στον παραλήπτη. Ουσιαστικά μετατρέπεται το αρχικό **IP** πακέτο σε δεδομένα ενός άλλου **IP** πακέτου, του οποίου τα πεδία που αφορούν τις διευθύνσεις αποστολέα και παραλήπτη είναι διαφορετικά από ότι στο αρχικό **(tunneling).**

Παρά τις όποιες επιτυχημένες προσπάθειες το πρόβλημα παραμένει και αυτό γιατί, ακόμη και αν χρησιμοποιείται προστασία στο επίπεδο εφαρμογής, υπάρχει αρκετή πληροφορία στην επικεφαλίδα του πακέτου, στο οποίο ενσωματώνονται τα δεδομένα **(**ακόμη και στα **VPN** δίκτυα**)** και για αυτό παραμένουν ευάλωτα σε επιθέσεις. Με χρήση προγραμμάτων ανάλυσης της δικτυακής κυκλοφορίας **(sniffers)** είναι δυνατό να αποκαλυφθούν οι διεργασίες και τα συστήματα που ανταλλάσσουν πληροφορίες. Θα πρέπει να προστεθεί, επίσης, ότι το κόστος προστασίας από κάθε εφαρμογή ξεχωριστά είναι υψηλότερο σε σχέση με την παροχή ασφάλειας σε επίπεδο δικτύου. Στο επίπεδο μεταφοράς, θα πρέπει οι εφαρμογές που θα εμφωλεύουν κάποιο είδος προστασίας να ξαναεγγραφούν, προκειμένου τόσο ο χρήστης όσο και ο εξυπηρετητής να κάνουν χρήση αυτής της ασφάλειας. Τέλος, τα πρωτόκολλα **tunnelling [55,120]** έχουν μέτρια απόδοση και πάσχουν από την έλλειψη ενός κοινού προτύπου που να είναι κοινώς αποδεκτό και κατ' επέκταση να ακολουθείται από όλους.

Οι περισσότεροι οργανισμοί ή ιδιώτες που συμμετέχουν στο Διαδίκτυο, παρόλα αυτά, φαίνονται να έχουν ένα ατεκμηρίωτο αίσθημα ασφάλειας, αγνοώντας τους ανυπολόγιστους κινδύνους που παραμονεύουν. Πιστεύουν πως η εκάστοτε ιστοσελίδα δεν αποτελεί στόχο και ότι έχουν ληφθεί τα απαραίτητα μέτρα. Η τεχνολογία, όμως, μεταβάλλεται με την πάροδο του χρόνου και τα εργαλεία των εισβολέων προσαρμόζονται ανάλογα. Επιπροσθέτως, η εμπιστευτικότητα και η ακεραιότητα των πληροφοριών δεν είναι εφικτή, καθώς το μεγαλύτερο μέρος της πληροφορίας που διακινείται δεν είναι κρυπτ**ο**γραφημένο. Έτσι, μία ιστοσελίδα μπορεί να δεχθεί επίθεση συλλέγοντας πληροφορίες για αυτή με διάφορα εργαλεία, όπως ένα **packet sniffer.**

Επιπλέον παράγοντας που πρέπει να ληφθεί υπόψη στην επιδείνωση του προβλήματος είναι η ραγδαία ανάπτυξη των υπηρεσιών πάνω από το Διαδίκτυο. Με χρήση πολύπλοκων εφαρμογών που δε σχεδιάζονται, εγκαθίστανται και συντηρούνται με προσοχή μένουν τρωτά σημεία στον κώδικα των προγραμμάτων και των λειτουργικών. Ακόμη, η επιλογή λειτουργικού συστήματος του εκάστοτε εξοπλισμού θα πρέπει να γίνεται με γνώμονα την ενίσχυση της ασφάλειας και όχι μόνο την ταχύτητα, τις επιδόσεις, την τιμή, την ευκολία χρήσης, τη διαχείριση ή την υποστήριξη. Συνήθως, η αρχική διαμόρφωση του λειτουργικού που προσφέρει

ο κατασκευαστής είναι ακατάλληλη για τη διασφάλιση της ασφάλειας, πόσο μάλλον για την ενίσχυσή της. Γίνεται, τέλος, σαφής η ανάγκη τόσο για εξειδικευμένα δικτυακά πρωτόκολλα ασφάλειας, όσο και για εξειδικευμένο προσωπικό που θα αναλύουν, θα σχεδιάζουν και θα συντηρούν την ασφάλεια ενός διαδικτυακού τόπου.

### 3.1.1 Βασικές διαστάσεις της ασφάλειας

Οι βασικές διαστάσεις της ασφάλειας μπορούν να χωριστούν σε πέντε κύριους άξονες **[137]**:

- Εμπιστευτικότητα: οι πληροφορίες είναι προσπελάσιμες μόνο από εξουσιοδοτημένους χρήστες
- Ακεραιότητα: τα δεδομένα και τα προγράμματα τροποποιούνται και καταστρέφονται μόνο με καλά καθορισμένους τρόπους και με κατάλληλη εξουσιοδότηση
- Διαθεσιμότητα: Οι εξουσιοδοτημένοι χρήστες θα μπορούν να χρησιμοποιήσουν δεδομένα, προγράμματα και υπηρεσίες όταν το επιθυμήσουν
- Αυθεντικότητα: εξασφάλιση ότι τα δεδομένα είναι απαλλαγμένα ατελειών και ανακριβειών κατά τις εξουσιοδοτημένες τροποποιήσεις
- Εγκυρότητα: εξασφάλιση ότι τα δεδομένα είναι ακριβή και πλήρη

### 3.1.2 Συνηθισμένες απειλές κατά της ασφάλειας

- Αποκάλυψη συνθηματικών

Τα συνθηματικά είναι ένας από τους πιο διαδεδομένους τρόπους για να «αναγνωρίζεται» ένας χρήστης από το σύστημα. Παρά την ευρεία τους διάδοση και πολύχρονη χρήση, υπάρχει μία σειρά από ζητήματα που σχετίζονται με τη χρήση και την αποτελεσματικότητά τους. Τα συνθηματικά μπορεί να αποκαλυφθούν **[123]** είτε μέσω εξαντλητικής αναζήτησης (δοκιμή όλων των δυνατών συνθηματικών), είτε με χρήση λιστών με συχνά χρησιμοποιούμενα συνθηματικά, είτε με αξιοποίηση προκαθορισμένων συνθηματικών, καθώς και με πληθώρα άλλων μεθόδων. Οι επιθέσεις που αφορούν αποκάλυψη συνθηματικών διευκολύνονται από τους γρήγορους υπολογιστές (δυνατότητα εξέτασης περισσότερων συνθηματικών στη μονάδα του χρόνου) και τα γρήγορα δίκτυα.

- Πλοήγηση

Ένας «νόμιμος» χρήστης ενός συστήματος (ή ένας εισβολέας που έχει αποκτήσει περιορισμένη πρόσβαση) ψάχνει στο σύστημα για να βρει πληροφορίες που θα του

δώσουν περισσότερα προνόμια. Η αναζήτηση μπορεί να γίνεται σε μπλοκ δίσκου, σε σελίδες μνήμης, σε απροστάτευτα αρχεία κ.λπ.

- Ø Αντιποίηση ή μεταμφίεση

Στην περίπτωση αυτή ο χρήστης πιστεύει ότι αλληλεπιδρά με μία οντότητα **[40]** (πρόγραμμα, υπηρεσία, χρήστη) ενώ στην πραγματικότητα αλληλεπιδρά με κάποια άλλη που προσποιείται ότι είναι η πραγματική. Από τις πρώτες (ιδιαίτερα επιτυχημένες) προσπάθειες αντιποίησης ήταν η συγγραφή προγραμμάτων που προσομοίωναν τη λειτουργικότητα του προγράμματος σύνδεσης **(login)** του συστήματος. Οι χρήστες ανυποψίαστοι εισήγαγαν τους κωδικούς της σύνδεσής τους στο πρόγραμμα αυτό, το οποίο αντί να τους παρέχει σύνδεση με το σύστημα τα καταχωρούσε για να τα βρει ο συγγραφέας του. Στο περιβάλλον του διαδικτύου είναι δυνατόν να αντιποιηθούν ιστοχώροι, π.χ. είναι δυνατόν να δημιουργηθεί ο ιστοχώρος **www.amason.com** ο οποίος θα μοιάζει καθ' όλα με τον «κανονικό» ιστοχώρο **www.amazon.com**, εκτός από το ότι τα στοιχεία της πιστωτικής κάρτας που θα εισάγει ένας «πελάτης» δεν θα χρησιμοποιηθούν για την πληρωμή των βιβλίων.

Τέλος, σε περιβάλλον δικτύου η αντιποίηση εμφανίζεται με την αποστολή δικτυακών πακέτων που φαίνονται να προέρχονται από διαφορετικούς υπολογιστές από αυτούς όπου πραγματικά εκπέμφθηκαν.

- Ø Αξιοποίηση προγραμματιστικών σφαλμάτων

Σε πολλές περιπτώσεις, προγραμματιστικά σφάλματα σε εφαρμογές ή σε λειτουργικά συστήματα επιτρέπουν σε επίδοξους εισβολείς να υποβαθμίσουν την ασφάλεια των υπολογιστικών συστημάτων.

- Ø Καταπακτή **(trapdoors)**

Πρόκειται για τροποποιήσεις συστημάτων που παρέχουν πρόσβαση στα συστήματα, χωρίς ιδιαίτερες διατυπώσεις. Μολονότι συνήθως εγκαθίστανται από τους εισβολείς μετά από μία επιτυχημένη επίθεση και για μελλοντική χρήση, δεν είναι σπάνια η περίπτωση να εγκατασταθούν από τους κατασκευαστές ως «δίοδοι ταχείας πρόσβασης» για την περίπτωση που «κάτι πάει στραβά». Διάσημα προγράμματα αυτής της κατηγορίας είναι οι τροποποιημένες εκδόσεις του **login** που επιτρέπουν είσοδο με δικαιώματα υπερχρήστη σε συγκεκριμένα **usernames** και το **Back Office** σε περιβάλλον **PC** που δίνει σε απομακρυσμένους χρήστες δικαιώματα διαχείρισης στον δικό μας υπολογιστή.

- Διαρροή δεδομένων

Διεργασίες που είναι εξουσιοδοτημένες να προσπελαύνουν δεδομένα τα αποκαλύπτουν σε χρήστες που δεν είναι εξουσιοδοτημένοι. Για παράδειγμα, το πρόγραμμα διακίνησης ηλεκτρονικής αλληλογραφίας **sendmail** ήταν δυνατόν να κληθεί με την ένδειξη **–bp** με αποτέλεσμα να αναφέρει τα μηνύματα των οποίων η παράδοση εκκρεμούσε κατά τη στιγμή της εκτέλεσης, αναφέροντας μάλιστα και τον αποστολέα και τον παραλήπτη. Με συνεχή χρήση αυτής της εντολής ήταν δυνατόν να πληροφορηθεί κανείς ποιος επικοινωνεί με ποιον.

- Συμπερασμός πληροφοριών

Ο συμπερασμός πληροφοριών αναφέρεται στη συσχέτιση φαινομενικά άσχετων δεδομένων για εξαγωγή χρήσιμων πληροφοριών. Πολλά τέτοια προβλήματα εμφανίζονται στις στατιστικές βάσεις δεδομένων, οι οποίες οφείλουν να δίνουν πληροφορίες για ομάδες πληθυσμού, αλλά όχι για μεμονωμένα άτομα. Με κατάλληλες ωστόσο ερωτήσεις και ελλείψει μηχανισμών ασφαλείας είναι δυνατόν να εξαχθούν ατομικές πληροφορίες: Για παράδειγμα, έστω η ερώτηση «ποιο είναι το πλήθος και μέσος μισθός των ανδρών με ηλικία μικρότερη των **35** ετών» η οποία απαντάται με τα στοιχεία **(10, 2000)**. Αν η ερώτηση «ποιο είναι το πλήθος και μέσος μισθός των ανδρών με ηλικία μικρότερη των **34** ετών» απαντάται με τα στοιχεία **(9,1800)** τότε συνάγεται ότι ο μοναδικός άνδρας ηλικίας **34** ετών έχει μισθό **3800**.

- Πλαστογράφηση

Πρόκειται για τη μη εξουσιοδοτημένη τροποποίηση δεδομένων με αποτέλεσμα τη δημιουργία πλαστογραφημένων εκδόσεών τους. Η τροποποίηση μπορεί να γίνει είτε στα αποθηκευμένα δεδομένα (με αποτέλεσμα τη μόνιμη παραποίησή τους), είτε στα δεδομένα όταν αυτά μεταδίδονται μέσω δικτύου.

- Κανάλια διαρροής

Τα κανάλια διαρροής είναι ένας μηχανισμός σύμφωνα με τον οποίο μία διεργασία που έχει δικαίωμα να προσπελάσει κάποια δεδομένα τα μεταδίδει σε μία διεργασία που δεν θα είχε κανονικά δικαίωμα να τα προσπελάσει, χρησιμοποιώντας όχι τυποποιημένους μηχανισμούς διαδιεργασιακής επικοινωνίας αλλά τεχνικές φαινομενικά άσχετες προς τη μετάδοση δεδομένων. Για παράδειγμα μία διεργασία μπορεί να αυξάνει ή να μειώνει τη μνήμη που έχει δεσμεύσει, μεταδίδοντας έτσι τα **bits 1** και **0** αντίστοιχα. Μία άλλη διεργασία μπορεί παρακολουθώντας το μέγεθος της μνήμης που καταλαμβάνει η πρώτη (που συνήθως είναι αδιαβάθμητη και προσπελάσιμη σε όλους πληροφορία) να «λάβει» τα δεδομένα που «μεταδίδει» η πρώτη. Το ίδιο μπορεί να επιτευχθεί με άλλους τρόπους π.χ. κλείδωμα και

ξεκλείδωμα πόρων, τον χρόνο διεκπεραίωσης μιας εργασίας, την αυξομείωση μεγέθους αρχείων, τη χρήση της ΚΜΕ κ.λπ.

Ø Παρεμπόδιση παροχής υπηρεσιών

Η υποβάθμιση της αξίας ενός υπολογιστικού συστήματος μπορεί να επέλθει χωρίς κάποια φυσική καταστροφή ή φθορά δεδομένων, αλλά επίσης και με την ανάθεση σ' αυτό ενός ιδιαίτερα επαχθούς έργου που να εξαντλεί τους πόρους του καθιστώντας το ανίκανο να προσφέρει το έργο που του έχει ανατεθεί. Έτσι ένας εξυπηρέτης ηλεκτρονικού ταχυδρομείου μπορεί να καταστεί «άχρηστος» αν του ανατεθεί να διακινήσει **50000** μηνύματα των **200 Mbytes** έκαστο, καθώς σίγουρα θα εξαντληθεί ο αποθηκευτικός του χώρος. Επίσης ένας εξυπηρέτης **WWW** θα είναι επίσης «άχρηστος» αν «βομβαρδισθεί» με δυσανάλογο προς τις προδιαγραφές του αριθμό αιτήσεων. Η παρεμπόδιση παροχής υπηρεσιών συνίσταται, συνήθως, στην υποβολή πολλών αιτήσεων που η κάθε μία είναι μεμονωμένα «νομότυπη», αλλά συνδυαστικά έχουν άσχημα αποτελέσματα. Η παρεμπόδιση παροχής υπηρεσιών αποσκοπεί στη στέρηση από τους νόμιμους χρήστες της δυνατότητάς τους να εξυπηρετηθούν από το υπολογιστικό σύστημα.

Ø Μη ηθελημένη καταστροφή

Ένας χρήστης μπορεί να πραγματοποιήσει ατυχείς ενέργειες π.χ. να διαγράψει ένα (χρήσιμο) αρχείο ή να σβήσει ένα σύνολο εγγραφών από μια βάση δεδομένων. Ως ενέργειες που υποβαθμίζουν την αξία του συστήματος τα περιστατικά αυτά πρέπει να καλύπτονται από τους μηχανισμούς ασφάλειας. Μολονότι προφανώς δεν είναι δυνατόν να στερήσουμε από τους χρήστες τα βασικά τους προνόμια για να αποτραπούν οι ατυχείς ενέργειες, θα πρέπει στο σχέδιο ασφάλειας να μεριμνούμε για μεθόδους αντιμετώπισης των περιστατικών αυτών.

Παρά την πληθώρα δυνατών επιθέσεων στην ασφάλεια και τις σημαντικές συνέπειες που μπορεί αυτές να έχουν, πολλές φορές οι επιθέσεις αυτές δεν αναφέρονται στους υπεύθυνους, στη διοίκηση ή σε κατάλληλους φορείς στο **Internet**. Οι λόγοι μη αναφοράς είναι κυρίως οι ακόλουθοι **[137]**:

- Η αναφορά ενός προβλήματος δίνει ιδέες σε άλλους επίδοξους εισβολείς. Έτσι αν διαρρεύσει μία πληροφορία ότι «ο τάδε υπολογιστής έχει μία αδυναμία σ' αυτή την υπηρεσία», αρκετοί εισβολείς μπορεί να προσπαθήσουν να εκμεταλλευτούν το συγκεκριμένο κενό ή να εντοπίσουν και άλλα.
- Η αρνητική δημοσιότητα διώχνει πελάτες και δυσαρεστεί τους μετόχους. Για παράδειγμα, αν μία τράπεζα ανακοινώσει ότι κάποιος «έσπασε» το διαδυκτιακό σύστημα εξυπηρέτησης πελατών, οι καταθέτες της τράπεζας θα είναι

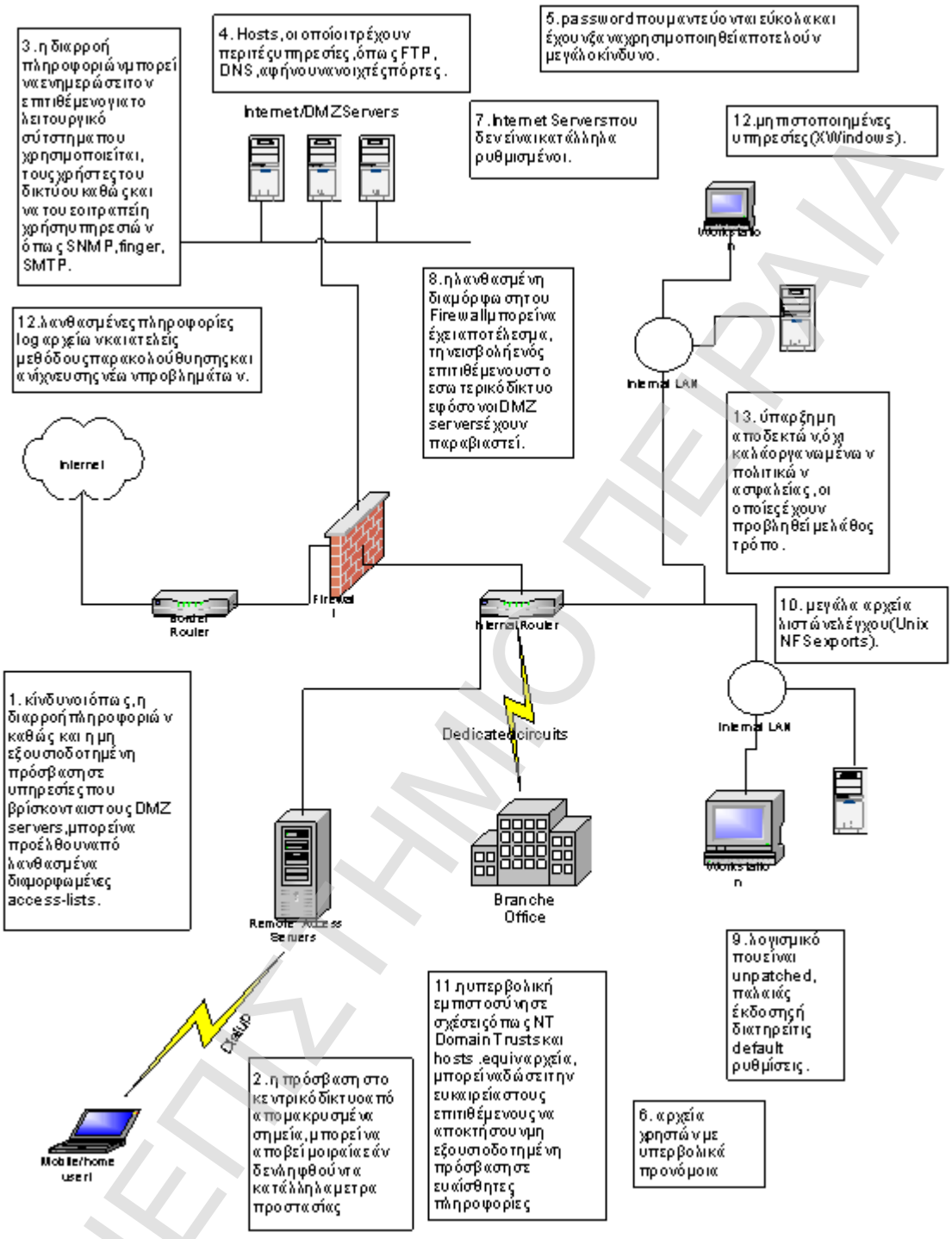
πολύ διστακτικοί στο να αξιοποιήσουν την υπηρεσία αυτή, ενώ και η μετοχή στη Σοφοκλέους πιθανόν να μπει στην κόκκινη ζώνη.

- Πολλές φορές η σημασία ενός συμβάντος υποβαθμίζεται και δεν τίθεται στις πραγματικές της διαστάσεις, πιθανώς λόγω άγνοιας των ενδεχόμενων συνεπειών.Η μη αναφορά των περιστατικών πάντως δίνει την ψευδαίσθηση ότι «όλα πάνε καλά» και έτσι δεν βοηθά στην δημιουργία (ή αναμόρφωση) και εφαρμογή ενός καλύτερου σχεδίου ασφάλειας.

- Κακόβουλο λογισμικό

Η κατηγορία αυτή αναλύεται λεπτομερέστερα στο **4**ο κεφάλαιο.

Στο (Σχήμα **22)** μπορούμε να δούμε συγκεντρωτικά συνήθεις απειλές κατά τις ασφάλειας (σημεία ευπάθειας) σε ένα εταιρικό δίκτυο




**Σχήμα 22. Σημεία ευπάθειας**

## 3.2 Ασφάλεια σε δικτυακό περιβάλλον

Οι χρήστες σε ένα δικτυακό περιβάλλον προσπελαύνουν υπηρεσίες και ανταλλάσσουν ή και αποθηκεύουν πληροφορίες δημιουργώντας έτσι τις απαιτήσεις

από πλευράς ασφάλειας να εξασφαλιστούν, η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα δεδομένων και υπηρεσιών.

Για να είναι δυνατή η επίτευξη αυτών των στόχων, είναι απαραίτητο να εξασφαλισθούν οι κάτωθι συνιστώσες **[2,137]:**

**Ø** Ισχυρή διακρίβωση ταυτότητας των ενεχόμενων μερών **(**χρηστών-συστημάτων**),** έτσι ώστε αφ' ενός το σύστημα να είναι βέβαιο για την ταυτότητα του χρήστη με το οποίο συνδιαλλάσσεται, αφ' ετέρου δε ο χρήστης να είναι βέβαιος ότι έχει συνδεθεί με το σύστημα που επιθυμεί.

**Ø** Αξιόπιστοι μηχανισμοί ελέγχου εξουσιοδότησης**/**προσπέλασης, έτσι ώστε να εξασφαλίζεται ότι τα κατάλληλα δικαιώματα έχουν αποδοθεί στους κατάλληλους χρήστες και ότι οι κανένας χρήστης δεν μπορεί να υπερβεί τα προνόμιά του.

**Ø** Αποτελεσματικοί έλεγχοι κατάχρησης δικαιωμάτων, προκειμένου να εντοπίζονται οι περιπτώσεις όπου δικαιώματα που έχουν παραχωρηθεί για συγκεκριμένους λόγους χρησιμοποιούνται για άλλους σκοπούς.

**Ø** Τέλειες πολιτικές και απαράβατη εφαρμογή τους, δηλαδή επακριβής ορισμός των δικαιοδοσιών του κάθε χρήστη και επιβολή αυτών των περιορισμών και στην πράξη.

**Ø** Άψογα πρωτόκολλα, λειτουργικά συστήματα και εφαρμογές, τα οποία είναι τα εργαλεία που θα επιτρέψουν την εφαρμογή των πολιτικών.

**Ø** Κάθε χρήστης να είναι ειδικός στην ασφάλεια, έτσι ώστε να είναι σε θέση να αξιολογήσει τους κινδύνους που μπορεί να επιφέρει οποιαδήποτε ενέργειά του και να πράττει αναλόγως.

**Ø** Ωστόσο όπως και γίνετε εύκολα αντιληπτό επειδή δεν είναι δυνατή η εξασφάλιση των προαναφερθέντων συνιστωσών μια πιο ρεαλιστική λίστα έχει ως ακολούθως:

**Ø** Δεν εφαρμόζονται αποτελεσματικοί μέθοδοι προστασίας.

**Ø** Δεν εγκαθίστανται οι επιδιορθώσεις που παρέχονται από τους κατασκευαστές λογισμικού, προκειμένου να αντιμετωπισθούν προβλήματα ασφάλειας στα λειτουργικά συστήματα, στα πρωτόκολλα ή τις εφαρμογές.

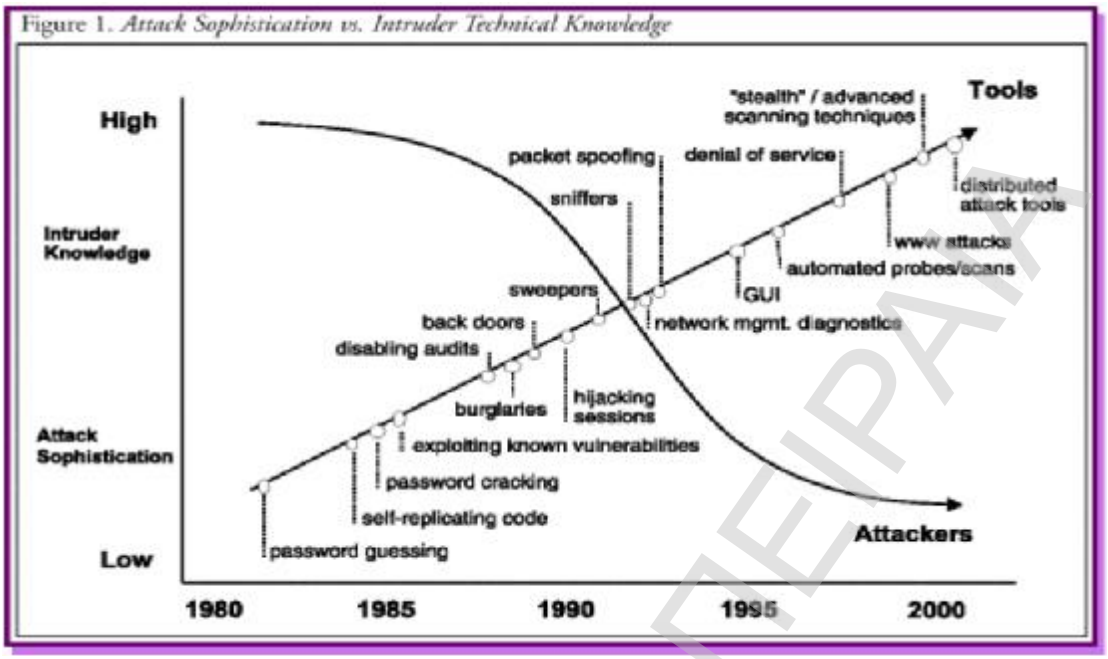
**Ø** Η δικτυακή πρόσβαση δεν απαιτεί επαρκή πιστοποίηση, η πρόσβαση στους **«**εσωτερικούς**»** υπολογιστές **(**τους υπολογιστές δηλαδή ενός εταιρικού δικτύου, σε αντιδιαστολή με τους υπολογιστές εκτός αυτού**)** δεν παρακολουθείται και δεν ελέγχεται.

**Ø** Δεν διατίθεται προσωπικό για ζητήματα ασφάλειας. Τα ζητήματα αυτά επαφίενται στους διαχειριστές, οι οποίοι δεν είναι κατ' ανάγκην ειδικοί ή καλά καταρτισμένοι στα ζητήματα ασφάλειας, και σε κάθε περίπτωση έχουν και άλλα καθήκοντα να επιτελέσουν.

**Ø** Δεν εφαρμόζονται πολιτικές, δεν συντάσσεται δηλαδή μία γενική «χάρτα» δικαιωμάτων και υποχρεώσεων των χρηστών, αναφορικά με την ασφάλεια.

**Ø** Σε πολλές περιπτώσεις η πεποίθηση ότι το σύστημα είναι ασφαλές στηρίζεται στην άποψη ότι «δεν είναι γνωστό τι υπηρεσίες παρέχω, άρα δεν είναι δυνατόν να επιτεθεί κανείς σ' αυτές». Η πεποίθηση αυτή είναι απόλυτα εσφαλμένη, καθώς οι επιθέσεις δεν γίνονται πλέον χειρωνακτικά από τους χρήστες αλλά με αυτοματοποιημένα εργαλεία που μπορούν να αναλύσουν σε λίγα δευτερόλεπτα όλες τις υπηρεσίες που προσφέρει ένας μη επαρκώς προστατευμένος υπολογιστής, υποδεικνύοντας έτσι τις πιθανές κερκόπορτες στην ασφάλεια του συστήματος.

Από το **1990** και μετά, υπάρχει μία μεταστροφή σε επιθέσεις με αυτοματοποιημένα εργαλεία, τα οποία είναι διαθέσιμα ευρέως στην κοινότητα του διαδικτύου. Η χρήση τέτοιων εργαλείων έχει δύο παρεπόμενα: πρώτον, μία επίθεση είναι ιδιαίτερα εξαντλητική, εξετάζοντας ένα ιδιαίτερα μεγάλο πλήθος μεθόδους παραβίασης της ασφάλειας, άρα και πιο αποτελεσματική σε σχέση με μία χειρονακτική επίθεση. Δεύτερον, δεν χρειάζεται να είναι πια κανείς ειδικός σε θέματα παραβίασης ασφάλειας για να ξεπεράσει τις όποιες προστασίες έχει ένα υπολογιστικό σύστημα: οποιοσδήποτε χρήστης του **Internet** μπορεί να εγκαταστήσει στον υπολογιστή του ένα τέτοιο εργαλείο, να διαλέξει τον στόχο του και να ξεκινήσει την επίθεση **(**Σχήμα **23)**.




**Σχήμα 23. Χρονική εξέλιξη των διάφορων τύπων επιθέσεων**

## 3.3 Προσεγγίσεις στην επίτευξη ασφάλειας

Προκειμένου να επιτευχθεί υψηλό επίπεδο ασφάλειας σε κάποιο σύστημα μπορούν να ακολουθηθούν οι εξής κατευθύνσεις **[81,137]**.

- Ορισμός ασφαλών διαδικασιών. Η κατεύθυνση αυτή αφορά περισσότερο εξωσυστημικά ζητήματα, όπως π.χ. ποιος θα κάνει κάποια εργασία, αν η εργασία θα πρέπει να γίνεται παρουσία άνω του ενός ατόμων, ζητήματα καταγραφής κ.λπ.
- Εφαρμογή μηχανισμών για την επιβολή μέτρων ασφάλειας.
- Διασφάλιση μέσω ανάλυσης-επαλήθευσης.

### 3.3.1 Μηχανισμοί προστασίας

Οι δύο βασικοί μηχανισμοί προστασίας στα συστήματα είναι ο έλεγχος ταυτότητας, προκειμένου να εξασφαλίζεται ότι η οντότητα που παρουσιάζεται με κάποια ταυτότητα όντως είναι αυτή που ισχυρίζεται, και ο έλεγχος προσπέλασης που χρησιμοποιείται για να επιτρέψει σε κάποια διακριβωμένη πια οντότητα να προσπελάσει μόνο τα αντικείμενα και τις υπηρεσίες για τα οποία είναι εξουσιοδοτημένη**[88]**.

#### 3.3.1.1 Διακρίβωση ταυτότητας

Η διακρίβωση ταυτότητας είναι ένα βασικό δομικό στοιχείο της ασφάλειας συστημάτων**[52]**, καθώς αποτελεί τη βάση για τους περισσότερους τύπους ελέγχου πρόσβασης και καταλογισμού ευθυνών. Το σύστημα θα πρέπει να έχει τη

δυνατότητα να ταυτοποιεί τους χρήστες και να μπορεί να τους ξεχωρίζει, για παράδειγμα ο έλεγχος πρόσβασης συχνά βασίζεται στην αρχή των ελάχιστων προνομίων, δίνοντας στους χρήστες μόνο τα δικαιώματα που τους είναι απολύτως απαραίτητα για την επιτέλεση των εργασιών τους. Ο καταλογισμός ευθυνών απαιτεί τη σύνδεση των δραστηριοτήτων σε ένα υπολογιστικό σύστημα με συγκεκριμένα άτομα, συνεπώς το σύστημα πρέπει να γνωρίζει την ταυτότητα των χρηστών. Κατά τη διακρίβωση ταυτότητας, η οντότητα αρχικά παρουσιάζει στο σύστημα έναν ισχυρισμό περί της ταυτότητας της και ακολούθως το σύστημα εξετάζει αν αυτός ο ισχυρισμός είναι αληθής. Στη διαδικασία αυτή υπάρχουν τα εξής βήματα: η συλλογή των πληροφοριών που δίνει ο χρήστης, η ασφαλής μετάδοσή τους και ο προσδιορισμός του αν ο χρήστης που αρχικά διακριβώθηκε εξακολουθεί να είναι ο ίδιος που τώρα χρησιμοποιεί το σύστημα. Για παράδειγμα, αν ένας χρήστης συνδεθεί σε κάποιο τερματικό και στη συνέχεια το εγκαταλείψει προσωρινά, είναι δυνατόν κάποιος άλλος χρήστης να το χρησιμοποιήσει υπό την ταυτότητα του πρώτου. Υπάρχουν τρεις βασικοί τρόποι διακρίβωσης της ταυτότητας, που μπορούν να χρησιμοποιηθούν μεμονωμένα ή συνδυαστικά:

**1.** να ζητείται κάτι που ο χρήστης γνωρίζει **(**π.χ. ένα συνθηματικό, ένας προσωπικός αριθμός αναγνώρισης ή ένα κρυπτογραφικό κλειδί**)**

**2.** να ζητείται κάτι που βρίσκεται υπό την κατοχή του χρήστη, όπως μία έξυπνη κάρτα, μία κάρτα αυτόματων ταμειακών συναλλαγών κ.λπ.

**3.** να εξετάζεται κάποιο βιομετρικό χαρακτηριστικό του χρήστη, όπως π.χ. δακτυλικά αποτυπώματα, σχήμα ίριδας, τρόπος γραφής κ.τ.λ.

Μολονότι φαίνεται ότι οποιοδήποτε από αυτά τα μέσα μπορεί να παρέχει ισχυρή διακρίβωση ταυτότητας, υπάρχουν προβλήματα μ' αυτές: τα συνθηματικά μπορεί να διαρρεύσουν ή να μαντευθούν, οι έξυπνες κάρτες μπορεί να κλαπούν ή να κατασκευαστούν πλαστές. ακόμη και τα βιομετρικά συστήματα μπορούν να ξεγελασθούν. Κάθε μέθοδος έχει επίσης μειονεκτήματα για τους διαχειριστές και τους «νόμιμους» χρήστες: οι χρήστες ξεχνάνε τα συνθηματικά ή χάνουν τις έξυπνες κάρτες, και η διαχειριστική επιβάρυνση για την αντιμετώπιση αυτών των ζητημάτων μπορεί να είναι σημαντική. Επίσης, τα βιομετρικά συστήματα συναντούν προβλήματα αποδοχής από πλευράς χρηστών, έχουν υψηλό κόστος και τεχνικές δυσκολίες.

**a)** Τεχνικές όπου ζητείται κάτι που ο χρήστης γνωρίζει

Η πιο συνηθισμένη τεχνική διακρίβωσης ταυτότητας **[137]** συσχετίζει κάθε ταυτότητα χρήστη με ένα συνθηματικό. Η τεχνική αυτή βασίζεται αποκλειστικά σε

κάτι που ο χρήστης γνωρίζει. Υπάρχουν και άλλες τεχνικές που ζητούν κάτι που γνωρίζει ο χρήστης, όπως π.χ. ένα κρυπτογραφικό κλειδί.

Συνθηματικά

Γενικώς, τα συστήματα συνθηματικών λειτουργούν απαιτώντας από τον χρήστη να εισάγει την ταυτότητά του μαζί με ένα συνθηματικό (ή συνθηματική φράση ή προσωπικό αριθμό ταυτότητας κ.λπ.). Το σύστημα συγκρίνει το συνθηματικό με αυτό που είναι αποθηκευμένο στο αρχείο συνθηματικών για τον συγκεκριμένο χρήστη. Αν είναι ίδια, η ταυτότητα έχει διακριβωθεί επιτυχώς. Η χρήση συνθηματικών έχει παράσχει ασφάλεια σε υπολογιστικά συστήματα για μεγάλο χρονικό διάστημα. Οι σχετικοί μηχανισμοί είναι ενσωματωμένοι στα λειτουργικά συστήματα και οι χρήστες, αλλά και οι διαχειριστές συστημάτων είναι εξοικειωμένοι με αυτά. Με κατάλληλη διαχείριση σε ένα ελεγχόμενο περιβάλλον μπορούν να αποτελέσουν αποτελεσματικό μηχανισμό διακρίβωσης ταυτότητας.

Από την άλλη πλευρά, η λειτουργία του όλου σχήματος βασίζεται στο ότι δεν θα διαρρεύσουν τα συνθηματικά. Δυστυχώς υπάρχουν πολλοί τρόποι με τους οποίους είναι δυνατόν να αποκαλυφθούν **[137]**:

**1.** «Μάντεμα» ή εύρεση συνθηματικών. Αν οι χρήστες διαλέγουν μόνοι τους τα συνθηματικά, τείνουν να επιλέγουν κάποια εύκολα για απομνημόνευση. Αυτό συνήθως συνεπάγεται και ευκολία στο μάντεμα, καθώς οι συνήθεις επιλογές είναι ονόματα συζύγων, παιδιών, ομάδων ή κατοικίδιων, τηλέφωνα κ.λπ., τα οποία όμως είναι γνωστά και σε άλλους. Από την άλλη πλευρά, αν τα συνθηματικά δεν είναι εύκολο να απομνημονευθούν, οι χρήστες πιθανότατα θα τα σημειώσουν, ενδεχομένως σε σημεία που και άλλοι έχουν πρόσβαση.

Πολλά συστήματα με προεγκατεστημένα λειτουργικά έχουν τυποποιημένα συνθηματικά για τους διαχειριστές ή άλλους χρήστες, που συχνά κανείς δεν μεριμνά να τροποποιήσει. Μολονότι οι ειδικοί συνεχώς ειδοποιούν για τα ζητήματα αυτά για πολλά χρόνια τώρα, οι χρήστες και οι διαχειριστές δεν έχουν συμμορφωθεί. Ένας εναλλακτικός τρόπος να μάθει κανείς το συνθηματικό κάποιου άλλου είναι να τον παρατηρεί κατά την ώρα που ο τελευταίος εισάγει το συνθηματικό.

**2.** «Διαμοιρασμός» των συνθηματικών. Σε πολλές περιπτώσεις οι χρήστες κοινοποιούν τα συνθηματικά τους και σε τρίτους, πιθανώς σε συναδέλφους προκειμένου για διαμοιρασμό αρχείων. Σε μερικές περιπτώσεις οι χρήστες δίνουν τα συνθηματικά τους σε άτομα που δηλώνουν «διαχειριστές» ή «υπεύθυνοι ασφάλειας» ή ακόμη και σε προγράμματα που προσομοιάζουν τη λειτουργία σύνδεσης.

**3.** Ηλεκτρονική παρακολούθηση. Κατά τη μετάδοση των συνθηματικών προς ένα υπολογιστικό σύστημα **(**κυρίως σε κατανεμημένα περιβάλλοντα**)** είναι δυνατόν αυτά να υποκλαπούν. Η κρυπτογράφηση εδώ δεν λύνει το πρόβλημα, καθώς η επανακρυπτογράφηση του ίδιου συνθηματικού θα δώσει το ίδιο κρυπτογραφημένο κείμενο. Συνεπώς, σε ό,τι αφορά το σύστημα που λαμβάνει το συνθηματικό, αν του σταλεί ξανά το κρυπτογραφημένο κείμενο που υπεκλάπη θα το θεωρήσει ως σωστό συνθηματικό.

**4.** Πρόσβαση στο αρχείο συνθηματικών. Αν το αρχείο συνθηματικών δεν είναι επαρκώς προστατευμένο με μηχανισμούς ελέγχου πρόσβασης, μπορεί να προσπελασθεί από οποιονδήποτε χρήστη. Τα περισσότερα αρχεία συνθηματικών συνήθως προστατεύονται με μονόδρομη κρυπτογράφηση **(**δηλαδή κωδικοποίηση της οποίας το αποτέλεσμα δεν μπορεί να χρησιμοποιηθεί για να βρεθεί το αρχικό κείμενο με υπολογιστικά εφικτό τρόπο**)**, έτσι ώστε τα συνθηματικά να μην είναι διαθέσιμα στους διαχειριστές ή τους εισβολείς. Ακόμη και σ' αυτήν την περίπτωση όμως, είναι δυνατή η προσπάθεια εύρεσης των συνθηματικών με εξαντλητική αναζήτηση, δεδομένης μάλιστα της αυξημένης υπολογιστικής ισχύος των σύγχρονων υπολογιστών.

Πολλές φορές τα συνθηματικά χρησιμοποιούνται από τα λειτουργικά συστήματα και για έλεγχο πρόσβασης σε πόρους. Η πολλαπλή αυτή χρήση των συνθηματικών δεν είναι καλή ιδέα, καθώς μειώνει τη συνολική ασφάλεια του συστήματος. Προκειμένου να αντιμετωπισθούν τα ανωτέρω ζητήματα σχετικά με την ασφάλεια των συνθηματικών, είναι δυνατόν να ληφθούν τα κάτωθι μέτρα**[46]**:

**1.** Γεννήτριες συνθηματικών. Αν δεν επιτρέπεται στους χρήστες να δώσουν τα συνθηματικά που οι ίδιοι επιθυμούν, προφανώς είναι αδύνατη η επιλογή από μέρους τους συνθηματικών που μπορούν να μαντευθούν εύκολα. Μερικές γεννήτριες παράγουν συνθηματικά που είναι εύκολο να προφερθούν, προκειμένου να μειωθεί η πιθανότητα να τα σημειώσει ο χρήστης σε κάποιο ευπρόσιτο σε άλλους μέρος.

**2.** Περιορισμός στις αποτυχημένες προσπάθειες σύνδεσης. Πολλά λειτουργικά συστήματα παρέχουν τη δυνατότητα κλειδώματος ενός κωδικού μετά από ένα συγκεκριμένο πλήθος διαδοχικών αποτυχημένων προσπαθειών σύνδεσης, αποτρέποντας έτσι την αποκάλυψη συνθηματικών με τη μέθοδο **«**δοκιμή και λάθος**»**.

**3.** Χαρακτηριστικά συνθηματικών. Το σύστημα μπορεί να επιβάλλει στους χρήστες να επιλέγουν συνθηματικά που

**(**α**)** έχουν ένα ελάχιστο μήκος

**(**β**)**περιέχουν ειδικούς χαρακτήρες

**(**γ**)** δεν **«**μοιάζουν**»** με την ταυτότητα χρήστη

**(**δ**)** δεν περιέχονται σε κάποιο λεξικό**.** Έτσι τα συνθηματικά γίνονται δύσκολο να μαντευθούν **(**αν και αυξάνεται η πιθανότητα να τα σημειώσει ο χρήστης σε κάποιο χαρτί**).**

**4.** Αλλαγή συνθηματικών**.** Η περιοδική αλλαγή των συνθηματικών μπορεί να μειώσει τις επιπτώσεις από μία ενδεχόμενη διαρροή του αρχείου κρυπτογραφημένων συνθηματικών και να καταστήσει δυσχερέστερες τις επιθέσεις που βασίζονται σε εξαντλητική δοκιμή όλων των δυνατών συνθηματικών**.** Οι πολύ συχνές αλλαγές ωστόσο δεν γίνονται ευμενώς δεκτές από τους χρήστες**.**

**5.** Προστασία του αρχείου συνθηματικών**.** Τα συνθηματικά πρέπει να αποθηκεύονται μετά από τη μονόδρομη κρυπτογράφησή τους**,** ενώ το ίδιο το αρχείο που περιέχει τα συνθηματικά πρέπει κανονικά να είναι απροσπέλαστο για τους κοινούς χρήστες**.**

**6.** Χρήση πλήκτρων ενεργοποίησης της διαδικασίας σύνδεσης**.** Μια σημαντική απειλή για την αποκάλυψη συνθηματικών σε τρίτους είναι η χρήση προγραμμάτων που προσομοιώνουν τη διαδικασία σύνδεσης και προτρέπουν τους χρήστες να εισάγουν τα διαπιστευτήρια σύνδεσής τους**,** τα οποία αποστέλλονται στον συγγραφέα του προγράμματος**.** Το πρόβλημα αυτό αντιμετωπίζεται με την εισαγωγή ενός επιπλέον βήματος στη διαδικασία σύνδεσης**,** στο οποίο ο χρήστης πατάει έναν συγκεκριμένο συνδυασμό πλήκτρων**,** για τον οποίο το λειτουργικό σύστημα εγγυάται ότι δεν είναι δυνατόν να παγιδευτεί ή να χρησιμοποιηθεί για άλλο σκοπό **(**π**.**χ**.** **CTRL-ALT-DEL** στα **Windows)**. Μετά το πάτημα του συγκεκριμένου συνδυασμού πλήκτρων**,** ο χρήστης είναι βέβαιος ότι η οθόνη που του παρουσιάζεται είναι η κανονική οθόνη σύνδεσης του συστήματος**.**

Κρυπτογραφικά κλειδιά

Αν και η δυνατότητα διακρίβωσης της ταυτότητας μέσω κρυπτογραφικού κλειδιού βασίζεται σε κάτι που γνωρίζει ο χρήστης**,** αυτός πρέπει συνήθως να έχει στη διάθεσή του κάποια συσκευή **(**π**.**χ**.** έξυπνη κάρτα ή **PC)**, η οποία θα εκτελέσει τους κρυπτογραφικούς υπολογισμούς**.** Για τον λόγο αυτό**,** η συγκεκριμένη προσέγγιση περιγράφεται στην συνέχεια όπου πραγματεύεται η διακρίβωση ταυτότητας βάσει αντικειμένων που έχει στην κατοχή του ο χρήστης**.**

#### 3.3.1.2 b) Τεχνικές όπου ζητάται κάτι που ο χρήστης κατέχει

Αν και αρκετές τεχνικές βασίζονται αποκλειστικά σε κάτι που ο χρήστης κατέχει**,** συνήθως ζητάται παράλληλα και κάτι που ο χρήστης γνωρίζει**[137].** Ο συνδυασμός

αυτός συνήθως αποφέρει υψηλότερα επίπεδα ασφάλειας από προσεγγίσεις όπου απαιτείται μόνον κάτι που γνωρίζει ο χρήστης ή μόνον κάτι που κατέχει. Τα αντικείμενα που κατέχει ο χρήστης για σκοπούς διακρίβωσης ταυτότητας καλούνται διακριτικά **(tokens)**, τα οποία διαχωρίζονται σε διακριτικά μνήμης και σε έξυπνα διακριτικά.

Διακριτικά μνήμης

Τα διακριτικά μνήμης αποθηκεύουν αλλά δεν επεξεργάζονται πληροφορίες. Η εγγραφή και η ανάγνωση δεδομένων σε ή από αυτά διενεργείται μέσω ειδικών συσκευών. Ο πιο διαδεδομένος τύπος διακριτικών μνήμης είναι οι κάρτες που είναι εφοδιασμένες με μία μαγνητική ταινία **(**π.χ. κάρτες τραπεζών για ανάληψη μετρητών**)**, οι οποίες διαβάζονται από ειδικούς αναγνώστες **(**αυτόματες ταμειακές μηχανές – ΑΤΜ**)**. Οι χρήστες απαιτείται, πέρα από το ίδιο το διακριτικό **(**την κάρτα**)**, να εισάγουν και έναν προσωπικό αριθμό αναγνώρισης. Σε μερικά συστήματα η διακρίβωση ταυτότητας γίνεται αποκλειστικά μέσω ενός διακριτικού, χωρίς να ζητάται κάτι που ο χρήστης γνωρίζει. Τα συστήματα αυτά είναι σχετικά λίγα και κυρίως αφορούν τον έλεγχο φυσικής πρόσβασης σε χώρους. Τα διακριτικά μνήμης που συνδυάζονται με προσωπικούς αριθμούς αναγνώρισης είναι πολύ πιο ασφαλή από τα συνθηματικά. Επιπρόσθετα, τα διακριτικά μνήμης είναι ιδιαίτερα φθηνά, ενώ για καταφέρει ένας μη εξουσιοδοτημένος χρήστης να αποκτήσει πρόσβαση πρέπει και να έχει στην κατοχή του το διακριτικό και να γνωρίζει και τον αριθμό. Ο συνδυασμός αυτός είναι πιο δύσκολο να αποκτηθεί απ' ό,τι ένα ζεύγος **(**ταυτότητα χρήστη, συνθηματικό**)**, ειδικότερα αν λάβουμε υπόψη ότι οι ταυτότητες χρήστη δεν είναι μυστικές. Ένα περαιτέρω πλεονέκτημα των διακριτικών είναι ότι μπορούν να χρησιμοποιηθούν για παραγωγή αρχείων καταγραφής, χωρίς να είναι απαραίτητο να εισάγει ο χρήστης την ταυτότητά του για κάθε δοσοληψία ή συμβάν που πρέπει να καταγραφεί, καθώς το σύστημα αντλεί τη σχετική πληροφορία από το διακριτικό. Αν το διακριτικό χρησιμοποιείται –εκτός από την διακρίβωση ταυτότητας στον υπολογιστή– και για είσοδο και έξοδο από τον φυσικό χώρο, τότε οι χρήστες αναγκαστικά το αφαιρούν από τον υπολογιστή όταν απομακρύνονται από τον χώρο. Με τον τρόπο αυτό μηδενίζεται η πιθανότητα να χρησιμοποιήσει κανείς κάποιο τερματικό που άφησε ανεπιτήρητο ένας χρήστης.

Η χρήση διακριτικών μνήμης όμως έχει και κάποια μειονεκτήματα. Αν και είναι τελικά δυνατή η πραγματοποίηση πολύ καλά προετοιμασμένων επιθέσεων ενάντια σε συστήματα που χρησιμοποιούν αυτή τη μέθοδο, τα περισσότερα προβλήματα ανάγονται στο κόστος, τη διαχείριση, την απώλεια των διακριτικών, τη δυσαρέσκεια των χρηστών και τη διαρροή των προσωπικών αριθμών αναγνώρισης. Ενδεικτικά αναφέρονται μερικά από τα προβλήματα **[118]**

**1.** Απαίτηση για εξειδικευμένες συσκευές ανάγνωσης. Για να είναι δυνατόν να χρησιμοποιηθεί το διακριτικό μνήμης σε ένα σύστημα, απαιτείται μία διάταξη που θα διαβάζει το διακριτικό και τον προσωπικό αριθμό του χρήστη. Κατόπιν η συσκευή είτε θα στέλνει τα δεδομένα στο σύστημα προς διακρίβωση της ορθότητας, είτε θα διενεργεί η ίδια τη διακρίβωση. Στην πρώτη περίπτωση απαιτείται η χρήση κρυπτογραφίας κατά τη μετάδοση για να μην είναι δυνατόν να υποκλαπούν τα δεδομένα.

**2.** Απώλεια διακριτικού. Αν ένας χρήστης χάσει το διακριτικό του, δεν θα μπορεί να συνδεθεί στο σύστημα μέχρι να αντικατασταθεί το διακριτικό. Με τον τρόπο αυτό αυξάνεται το διαχειριστικό κόστος και η επιβάρυνση. Το απολεσθέν διακριτικό μπορεί να έχει κλαπεί ή μπορεί να βρεθεί από κάποιον και ο νέος κάτοχός του μπορεί να επιχειρήσει να εισέλθει στο σύστημα με την ταυτότητα του χρήστη στον οποίο κανονικά ανήκει το διακριτικό. Αν το σύστημα απαιτεί πέραν του διακριτικού και κάποιον προσωπικό αριθμό αναγνώρισης, οποιαδήποτε μέθοδος από αυτές που περιγράφηκαν ανωτέρω για την κλοπή συνθηματικών είναι δυνατόν να χρησιμοποιηθεί για κλοπή του προσωπικού αριθμού.

**3.** Δυσαρέσκεια χρηστών. Γενικά, οι χρήστες επιθυμούν υπολογιστές εύκολους στη χρήση. Πολλοί χρήστες το βρίσκουν άβολο να κουβαλάνε και να χρησιμοποιούν ένα διακριτικό. Οι αντιδράσεις ωστόσο περιορίζονται αν είναι προφανής η αναγκαιότητα για αυξημένη ασφάλεια.

Έξυπνα διακριτικά

Ένα έξυπνο διακριτικό επεκτείνει τη λειτουργικότητα ενός διακριτικού μνήμης, ενσωματώνοντας ένα ή περισσότερα ολοκληρωμένα κυκλώματα. Όταν χρησιμοποιείται για διακρίβωση ταυτότητας, ένα έξυπνο διακριτικό εμπίπτει στην κατηγορία τεχνικών όπου ζητάται κάτι που ο χρήστης κατέχει, ενώ είναι δυνατόν παράλληλα να ζητάται και κάτι που ο χρήστης γνωρίζει (όπως π.χ. ένας προσωπικός αριθμός αναγνώρισης).

Υπάρχουν πολλά διαφορετικά είδη έξυπνων διακριτικών. Γενικά, τα έξυπνα διακριτικά μπορούν να καταταχθούν σε κατηγορίες βάσει των φυσικών χαρακτηριστικών τους, της διεπαφής τους και των πρωτοκόλλων που χρησιμοποιούν. Οι κατηγοριοποιήσεις αυτές δεν είναι αμοιβαία αποκλειόμενες**[103]**.

1. Φυσικά χαρακτηριστικά. Τα έξυπνα διακριτικά μπορεί να είναι «έξυπνες κάρτες», οι οποίες μοιάζουν με πιστωτικές κάρτες αλλά περιλαμβάνουν επίσης και κάποιον μικροεπεξεργαστή. Οι έξυπνες κάρτες περιγράφονται από ένα πρότυπο του διεθνούς οργανισμού προτύπων **(ISO)**. Τα έξυπνα διακριτικά που δεν είναι «έξυπνες κάρτες» μοιάζουν συνήθως με μικρές αριθμομηχανές.

**2.** Διεπαφή**.** Τα έξυπνα διακριτικά έχουν μία διεπαφή που μπορεί να τους επιτρέπει να επικοινωνούν είτε με ανθρώπους είτε με ηλεκτρονικά συστήματα**.** Τα διακριτικά που έχουν διεπαφή για επικοινωνία με ανθρώπους ενσωματώνουν οθόνες ή**/**και πληκτρολόγια για να επιτρέπουν την εισαγωγή και την προβολή στοιχείων**.** Τα διακριτικά με διεπαφές για επικοινωνία με ηλεκτρονικά συστήματα ανταλλάσσουν δεδομένα με ειδικές διατάξεις ανάγνωσης**/**εγγραφής**.** Τα διακριτικά που έχουν τη μορφή αριθμομηχανών συνήθως διαθέτουν διεπαφή για επικοινωνία με ανθρώπους**.**

**3.** Πρωτόκολλο**.** Υπάρχουν πολλά πρωτόκολλα που ένα έξυπνο διακριτικό μπορεί να χρησιμοποιήσει για διακρίβωση ταυτότητας**.** Γενικά μπορούν να διακριθούν σε τρεις κατηγορίες**:**

**a.** Στατική ανταλλαγή συνθηματικών**.** Βάσει του πρωτοκόλλου αυτού οι χρήστες εισάγουν το συνθηματικό τους στο έξυπνο διακριτικό**,** το οποίο κατόπιν συνεργάζεται με τον υπολογιστή για τη διακρίβωση της ταυτότητας του χρήστη**.**

**b.** Δυναμική γέννηση συνθηματικών**.** Βάσει του πρωτοκόλλου αυτού**,** το έξυπνο διακριτικό δημιουργεί μία μοναδική τιμή**,** π**.**χ**.** έναν οκταψήφιο αριθμό**,** ο οποίος αλλάζει περιοδικά **(**π**.**χ**.** κάθε λεπτό**).** Αν το διακριτικό έχει διεπαφή προσανατολισμένη σε επικοινωνία με ανθρώπους**,** ο χρήστης απλά διαβάζει τον αριθμό από την οθόνη του διακριτικού και το εισάγει στον υπολογιστή για διακρίβωση της ταυτότητάς του**.** Αν το διακριτικό έχει διεπαφή προσανατολισμένη σε επικοινωνία με ηλεκτρονικές διατάξεις**,** ο αριθμός αποστέλλεται αυτομάτως**.** Αν η εισαχθείσα τιμή είναι σωστή **(**δηλαδή είναι ανάμεσα στις παραδεκτές τιμές που ο υπολογιστής γνωρίζει ότι μπορεί να παράγει το συγκεκριμένο διακριτικό για τη δεδομένη χρονική περίοδο**),** θεωρείται ότι η ταυτότητα του χρήστη έχει διακριβωθεί**.**

**c.** Πρωτόκολλα ερωταποκρίσεων**.** Βάσει του πρωτοκόλλου αυτού ο υπολογιστής δημιουργεί μία ερώτηση π**.**χ**.** μία τυχαία ακολουθία από αριθμούς**.** Το έξυπνο διακριτικό παράγει μία απάντηση**,** ως συνάρτηση της ερώτησης**,** η οποία αποστέλλεται στον υπολογιστή**,** και ο υπολογιστής διακριβώνει την ταυτότητα του χρήστη βάσει της απάντησης**.** Οι αλγόριθμοι υπολογισμού της απάντησης από την ερώτηση στηρίζονται σε κρυπτογραφικές μεθόδους**.** Τα πρωτόκολλα ερωταποκρίσεων μπορούν να χρησιμοποιηθούν είτε με διεπαφές προσανατολισμένες σε επικοινωνία με ανθρώπους είτε με διεπαφές για επικοινωνία με ηλεκτρονικές διατάξεις**.**

Τα έξυπνα διακριτικά παρέχουν μεγάλη ευελιξία και μπορούν να λύσουν πολλά προβλήματα διακρίβωσης ταυτότητας**.** Τα πλεονεκτήματα που αποκομίζουμε από τη χρήση τους ποικίλλουν**,** ανάλογα με το είδος των διακριτικών που

χρησιμοποιούνται, στη γενική περίπτωση πάντως προσφέρουν μεγαλύτερη ασφάλεια από τα διακριτικά μνήμης. Τα έξυπνα διακριτικά μπορούν να λύσουν και το πρόβλημα της υποκλοπής των συνθηματικών κατά τη δικτυακή επικοινωνία, ακόμη και αν αυτή πραγματοποιείται μέσα από ανοικτά δημόσια δίκτυα, καθώς μπορούν να εφαρμόσουν τεχνικές συνθηματικών μίας χρήσης (π.χ. στην περίπτωση του πρωτοκόλλου ερωταποκρίσεων).

**1.** Συνθηματικά μιας χρήσης. Τα έξυπνα διακριτικά μπορούν να χρησιμοποιούν είτε δυναμική γέννηση συνθηματικών είτε πρωτόκολλα ερωταποκρίσεων για να παράξουν συνθηματικά μίας χρήσης. Η υποκλοπή του συνθηματικού σε αυτή την περίπτωση δεν συνεπάγεται κάποιο πρόβλημα στην ασφάλεια, καθώς σε κάθε διαδικασία διακρίβωσης ταυτότητας χρησιμοποιείται διαφορετικό συνθηματικό.

**2.** Ελαττωμένος κίνδυνος παραχάραξης. Γενικά, η μνήμη ενός έξυπνου διακριτικού δεν είναι αναγνώσιμη αν δεν εισαχθεί ο προσωπικός αριθμός αναγνώρισης. Επιπρόσθετα, τα έξυπνα διακριτικά είναι πιο πολύπλοκα και πιο δύσκολο να δημιουργηθούν παραχαραγμένα αντίγραφά τους.

**3.** Χρήση με πολλές εφαρμογές. Τα έξυπνα διακριτικά με διασύνδεση επικοινωνίας με ηλεκτρονικές συσκευές επιτρέπουν στους χρήστες τους να προσπελαύνουν πολλούς υπολογιστές και υπηρεσίες με μία μόνο διαδικασία σύνδεσης. Οι χρήστες πιστοποιούν τον εαυτό τους στο διακριτικό και στη συνέχεια αυτό μπορεί να εμπεριέχει όλη την απαραίτητη πληροφορία για να πιστοποιήσει τον χρήστη στις υπηρεσίες ή υπολογιστές που αυτός προσπελαύνει.

Η χρήση των έξυπνων διακριτικών έχει όμως και προβλήματα. Όπως και με τα διακριτικά μνήμης, αυτά εντοπίζονται στο κόστος, τη διαχείριση, την απώλεια των διακριτικών και τη δυσαρέσκεια των χρηστών. Η πιθανότητα διαρροής των προσωπικών αριθμών αναγνώρισης είναι ελαττωμένη, καθώς αυτοί δεν μεταδίδονται προς τους υπολογιστές αλλά ελέγχονται από το ίδιο το διακριτικό. Από την άλλη πλευρά βέβαια, τα έξυπνα διακριτικά κοστίζουν περισσότερο από τα διακριτικά μνήμης. Υπάρχει βέβαια και πάλι η αναγκαιότητα για διατάξεις ανάγνωσης-εγγραφής, ενώ όταν χρησιμοποιούνται διακριτικά με διεπαφές για επικοινωνία με ανθρώπους, οι χρήστες πρέπει να πληκτρολογούν μακροσκελείς συμβολοσειρές, κάτι που αυξάνει τη δυσαρέσκειά τους. Τέλος, υπάρχει υψηλό διαχειριστικό κόστος, ειδικότερα όταν χρησιμοποιούνται τεχνικές κρυπτογραφίας.

**c)** Πιστοποίηση βασισμένη σε βιομετρικά χαρακτηριστικά

Τα συστήματα διακρίβωσης ταυτότητας βάσει βιομετρικών χαρακτηριστικών αξιοποιούν τη μοναδικότητα ορισμένων χαρακτηριστικών των ανθρώπων για να τους αναγνωρίσουν. Μπορεί να εξετάζουν φυσικά χαρακτηριστικά (π.χ. δακτυλικά

αποτυπώματα, γεωμετρία χειρός κ.τ.λ.) ή χαρακτηριστικά συμπεριφοράς (π.χ. τρόπος υπογραφής ή χροιά φωνής). Υπάρχουν ήδη υλοποιημένες τεχνικές διακρίβωσης ταυτότητας που βασίζονται σε βιομετρικά μεγέθη και που έχουν ολοκληρωθεί σε υπολογιστικά συστήματα. Η διακρίβωση ταυτότητας βάσει βιομετρικών μεγεθών είναι δαπανηρή και τεχνικά περίπλοκη, ενώ οι χρήστες είναι δυνατόν να μην την αποδεχθούν εύκολα. Μπορούν να παράσχουν υψηλά επίπεδα ασφάλειας, αλλά η τεχνολογία τους δεν είναι ακόμη το ίδιο ώριμη όπως αυτή των διακριτικών. Σ' αυτά πρέπει να συνυπολογίσουμε ότι μερικά βιομετρικά χαρακτηριστικά μπορεί να μεταβάλλονται, π.χ. η χροιά της φωνής κάποιου μπορεί να αλλάξει σε συνθήκες υπερβολικής έντασης ή ενός κρυολογήματος.

Ο γενικός τρόπος λειτουργίας των συστημάτων διακρίβωσης ταυτότητας βάσει βιομετρικών χαρακτηριστικών είναι ο ακόλουθος: πριν από οποιαδήποτε προσπάθεια διακρίβωσης ταυτότητας για έναν συγκεκριμένο χρήστη μετρώνται τα σχετικά βιομετρικά μεγέθη του και οι μετρήσεις αυτές συσχετίζονται με το συγκεκριμένο φυσικό πρόσωπο. Κατόπιν, όταν ένας χρήστης επιχειρεί να συνδεθεί με το σύστημα, μετρώνται τα ίδια βιομετρικά χαρακτηριστικά του και συγκρίνονται με αυτά που έχουν αποθηκευθεί. Τα αποτελέσματα της σύγκρισης καθορίζουν αν η σύνδεση του χρήστη θα γίνει αποδεκτή ή όχι.

#### 3.3.1.3 Έλεγχος προσπέλασης

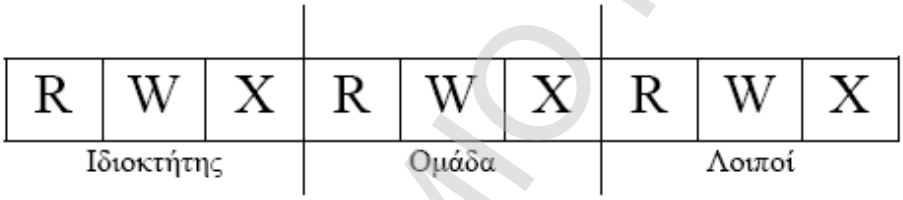
Από τη στιγμή που έχει διακριβωθεί η ταυτότητα ενός χρήστη (ή, γενικότερα, μιας οντότητας), το σύστημα θα πρέπει να φροντίζει έτσι ώστε η οντότητα αυτή να μπορεί να ενεργήσει μόνο στα πλαίσια των κανόνων που καθορίζονται από την πολιτική ασφάλειας. Αυτό μπορεί να επιτευχθεί εφαρμόζοντας ελέγχους προσπέλασης. Σχετικά με τους ελέγχους προσπέλασης ισχύουν οι ακόλουθες έννοιες[7]:

• Υποκείμενα. Πρόκειται για τις ενεργές οντότητες στο σύστημα (χρήστες, διεργασίες, υπηρεσίες)

• Αντικείμενα. Με τον όρο αυτό περιγράφονται οι πόροι ή οι παθητικές οντότητες στο σύστημα (αρχεία, συσκευές, προγράμματα)

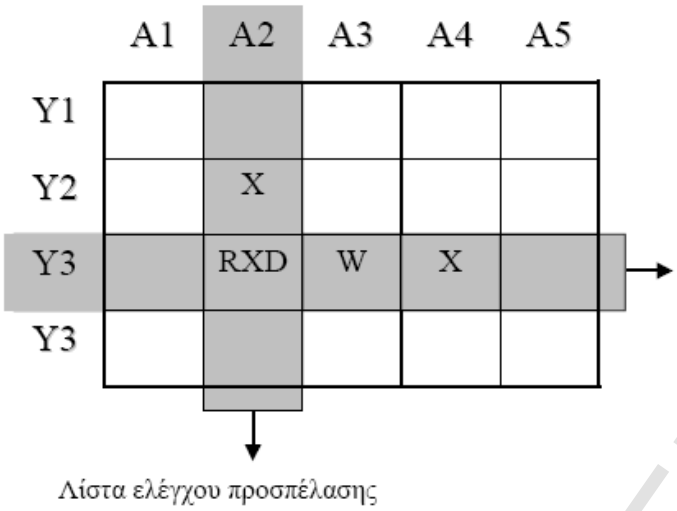
• Τρόπος προσπέλασης. Ο όρος αυτός αναφέρεται στην ενέργεια που πραγματοποιεί ένα υποκείμενο σε ένα αντικείμενο π.χ. ανάγνωση, εγγραφή, εκτέλεση, αναφορά ιδιοχαρακτηριστικών. Ο έλεγχος προσπέλασης συνίσταται στην εξέταση αν το υποκείμενο έχει δικαίωμα για τον συγκεκριμένο τρόπο προσπέλασης στο αντικείμενο, και στην απαγόρευση της ενέργειας, αν τελικά δεν υπάρχει το σχετικό δικαίωμα. Υπάρχουν δύο γενικές κατηγορίες σχημάτων προσπέλασης, τα κατ' επιλογήν και τα υποχρεωτικά. Στα κατ' επιλογήν σχήματα, ο ιδιοκτήτης του

αντικειμένου αποφασίζει τα δικαιώματα που θα εκχωρήσει σε διάφορες οντότητες πάνω στο αντικείμενο. Στα κατ΄ επιλογήν σχήματα ελέγχου προσπέλασης μπορούμε να κατατάξουμε τα **bits RWX** του **UNIX,** καθώς και τους πίνακες ελέγχου προσπέλασης που λαμβάνουν τη μορφή λιστών ελέγχου προσπέλασης ή λιστών προσδιοριστών δικαιωμάτων. Βάσει του σχήματος των **bits RWX** του **UNIX**, σε κάθε αντικείμενο αντιστοιχίζονται εννέα **bits,** οργανωμένα σε τρεις τριάδες. Η πρώτη από αυτές αφορά τον ιδιοκτήτη του αρχείου, η δεύτερη την ομάδα στην οποία ανήκει το αρχείο και η τρίτη όλους τους υπόλοιπους χρήστες. Εντός κάθε τριάδας **bits,** το πρώτο από αυτά προσδιορίζει το δικαίωμα ανάγνωσης, το δεύτερο το δικαίωμα εγγραφής και το τρίτο το δικαίωμα εκτέλεσης πάνω στο αρχείο, για την οντότητα **(**ή τις οντότητες**)** που αφορά η ομάδα **bits.** Το σχήμα των **bits RWX** απεικονίζεται στο Σχήμα **24.**




**Σχήμα 24. Σχήμα δικαιωμάτων χρηστών**

Το σχήμα των **bits RWX** είναι εύκολο στην υλοποίησή του, είναι σχετικά κατανοητό από τους χρήστες, αλλά είναι ιδιαίτερα δύσκαμπτο στη λεπτομερή ανάθεση προνομίων. Στους πίνακες ελέγχου προσπέλασης, ουσιαστικά καταρτίζεται ένας πίνακας του οποίου οι γραμμές αντιστοιχούν στα υποκείμενα, οι στήλες στα αντικείμενα, ενώ οι τιμές των κελιών του πίνακα προσδιορίζουν τα δικαιώματα που το υποκείμενο που αντιστοιχεί στη συγκεκριμένη γραμμή έχει πάνω στο αντικείμενο που αντιστοιχεί στη συγκεκριμένη στήλη, όπως φαίνεται στο σχήμα που ακολουθεί. Διαβάζοντας τον πίνακα ελέγχου προσπέλασης κατά στήλες έχουμε διανύσματα που καθορίζουν όλες τις δυνατές προσβάσεις σε κάθε ένα αντικείμενο ή αλλιώς λίστες ελέγχου προσπέλασης. Διαβάζοντας τον πίνακα ελέγχου κατά γραμμές έχουμε διανύσματα που καθορίζουν όλες τις δυνατές προσβάσεις για κάθε υποκείμενο, ή αλλιώς λίστες προσδιοριστών δικαιωμάτων **(**Σχήμα **25).**




**Σχήμα 25. Λίστες προσδιοριστών δικαιωμάτων και ελέγχου προσπέλασης**

Στα υποχρεωτικά σχήματα το σύστημα είναι αυτό που αποφασίζει ποιο υποκείμενο μπορεί να προσπελάσει κάθε αντικείμενο και τους επιτρεπτούς τρόπους. Η απόφαση βασίζεται στα ιδιοχαρακτηριστικά του υποκειμένου που ζητά πρόσβαση, και του αντικειμένου που επιχειρείται να προσπελασθεί.

Σε ένα υποχρεωτικό σχήμα ελέγχου προσπέλασης, κάθε υποκείμενο και κάθε αντικείμενο έχει ένα επίπεδο ασφάλειας, με κάθε επίπεδο ασφάλειας να αποτελείται από μια διαβάθμιση και ένα σύνολο κατηγοριών. Όταν ένα υποκείμενο επιχειρεί πρόσβαση σε ένα αντικείμενο, τα επίπεδα ασφαλείας τους συγκρίνονται, και η σύγκριση δίνει ένα από τα αποτελέσματα ίσο, μεγαλύτερο, μικρότερο και μη συγκρίσιμο. Για να γίνει πιο κατανοητό το σχήμα αυτό, αναφέρουμε το εξής παράδειγμα:

- Τρία επίπεδα ασφάλειας, αδιαβάθμητο, εμπιστευτικό, απόρρητο
- Τρεις κατηγορίες ασφάλειας, προμήθειες, λογιστήριο, διοίκηση
- Συγκρίσεις:

  εμπιστευτικό**/(**προμήθειες**) =** εμπιστευτικό**/(**προμήθειες**)**

  απόρρητο**/(**προμήθειες**) >** εμπιστευτικό**/(**προμήθειες**)**

  εμπιστευτικό**/(**προμήθειες**) <** εμπιστευτικό**(**προμήθειες, λογιστήριο**)**

  απόρρητο**(**προμήθειες**)** μη συγκρίσιμο απόρρητο**(**λογιστήριο**)**

Έχοντας πραγματοποιήσει τη σύγκριση, η πρόσβαση επιτρέπεται ή απαγορεύεται βάσει των εξής κανόνων:

- Η ανάγνωση επιτρέπεται αν το υποκείμενο έχει μεγαλύτερο ή ίσο επίπεδο ασφάλειας από το αντικείμενο **(no read-up)**

**Ø** Η εγγραφή επιτρέπεται αν το υποκείμενο έχει μικρότερο ή ίσο επίπεδο ασφάλειας από το αντικείμενο **(no write-down)**

Η χρησιμότητα του πρώτου κανόνα είναι προφανής. ο δεύτερος κανόνας αποτρέπει την μεταφορά πληροφορίας από ανώτερο επίπεδο σε κατώτερο, απ' όπου μπορεί να διαβαστεί από υποκείμενα κατώτερης εξουσιοδότησης. Προκειμένου να εφαρμόζονται οι κανόνες που ορίζονται για τον έλεγχο πρόσβασης, είναι απαραίτητο να εξετάζονται όλες οι απόπειρες προσπέλασης αντικειμένων και ανάλογα να επιτρέπονται ή να απαγορεύονται. Ένας τρόπος εφαρμογής των κανόνων αυτών είναι η εισαγωγή μιας ενότητας λογισμικού στο λειτουργικό σύστημα που ονομάζεται επόπτης αναφορών, δια μέσω του οποίου διέρχονται όλες οι αιτήσεις προσπέλασης σε αντικείμενα. Για κάθε πρόσβαση, ο επόπτης αναφορών συμβουλεύεται τα στοιχεία εξουσιοδοτήσεων, ταυτοτήτων και δικαιωμάτων και αποφασίζει ανάλογα. Ο επόπτης αναφορών πρέπει να μην είναι δυνατόν να παρακαμφθεί (δηλαδή κάποιες αιτήσεις προσπέλασης να μην διέλθουν μέσω αυτού), να μην είναι δυνατόν να ξεγελασθεί (δηλαδή να αποφασίζει πάντα χρησιμοποιώντας τις σωστές ταυτότητες αντικειμένων και υποκειμένων και τα σωστά στοιχεία εξουσιοδότησης), να έχει τη δυνατότητα καταγραφής και θα πρέπει να είναι δυνατόν να ελεγχθεί η ορθότητά του.

Μια εναλλακτική προσέγγιση είναι η συγκέντρωση όλων των ελέγχων και μηχανισμών που σχετίζονται με την ασφάλεια σε μία ειδική ενότητα του λειτουργικού συστήματος, τον πυρήνα ασφάλειας. Ο πυρήνας ασφάλειας είναι υπεύθυνος για την υλοποίηση όλων των μηχανισμών ασφάλειας του Λ.Σ. και σε όλα τα επίπεδα (υλικό, εφαρμογές, χρήστες κ.λπ.), ενώ τα υπόλοιπα τμήματα του Λ.Σ. απλά καλούν λειτουργίες που παρέχονται από τον πυρήνα ασφάλειας. Στα υπέρ της προσέγγισης αυτής είναι ο διαχωρισμός των λειτουργιών ασφάλειας από τις λοιπές λειτουργίες του Λ.Σ., η ενοποίησή τους σε ένα ξεχωριστό τμήμα, το οποίο μπορεί να συντηρηθεί και να επαληθευτεί ξεχωριστά από το υπόλοιπο Λ.Σ. Από την άλλη πλευρά, ένας διαχωρισμός τέτοιου είδους καταργεί πολλές βελτιστοποιήσεις οδηγώντας σε υποβάθμιση της απόδοσης, αυξάνει το μέγεθος του συστήματος, ενώ είναι πρακτικά αδύνατο να ενσωματωθεί σε υπάρχοντα λειτουργικά συστήματα, καθ' όσον απαιτεί αλλαγή της δομής τους.

### 3.3.2 Τεχνικές διασφάλισης

Οι τεχνικές διασφάλισης **[46]** αποσκοπούν στο να εξασφαλίσουν ότι ένα σύστημα είναι ασφαλές ή/και στην ανάδειξη και έγκαιρη διόρθωση των τρωτών σημείων του συστήματος, πριν αυτά γίνουν αντικείμενο εκμετάλλευσης από εισβολείς. Η πρώτη προσέγγιση, η οποία συνίσταται από τους μηχανικούς λογισμικού, είναι η υιοθέτηση

καλών προγραμματιστικών τεχνικών και πρακτικών, καθώς και εκτεταμένες δοκιμές του προϊόντος λογισμικού. Μολονότι ακούγεται πολύ δελεαστική προσέγγιση, στην πράξη δεν δίνει αποτελέσματα καθώς τα προϊόντα λογισμικού που κυκλοφορούν στην αγορά θεωρητικά τουλάχιστον έχουν αναπτυχθεί σωστά και ελεγχθεί διεξοδικά, χωρίς αυτό να αποτρέπει την ύπαρξη προβλημάτων ασφάλειας.

Μία δεύτερη προσέγγιση είναι η ανάλυση του συστήματος για εντοπισμό πιθανών αδυναμιών. Σύμφωνα με την πρακτική αυτή δημιουργείται μία «ομάδα τίγρης» **(tiger team)**, η οποία συλλέγει γνωστές αδυναμίες και τεχνικές εκμετάλλευσής τους, επιχειρεί μία γενίκευση και κατόπιν τις εφαρμόζει στο υπό διερεύνηση σύστημα. Το σκεπτικό της διενέργειας μίας τέτοιας ελεγχόμενης επίθεσης είναι να εντοπισθούν έγκαιρα και να διορθωθούν οι αδυναμίες από το προσωπικό ασφάλειας πριν τις εντοπίσουν και τις εκμεταλλευτούν οι –λιγότερο φιλικοί– εισβολείς. Μία τέτοια δοκιμή ωστόσο θα καταδείξει ενδεχομένως την ύπαρξη αδυναμιών, δεν εγγυάται όμως την απουσία τους.

Η τρίτη προσέγγιση είναι η προσπάθεια πρόληψης ή ανίχνευσης των προσπαθειών για εκμετάλλευση των αδυναμιών των συστημάτων. Συνολικά, η ασφάλεια των συστημάτων διακυβεύεται από **[52]:**

- Προγραμματιστικά σφάλματα σε μεμονωμένες διεργασίες, όπως π.χ. υπερχείλιση ενδιάμεσης μνήμης, συνθήκες ανταγωνισμού, δούρειοι ίπποι κ.λπ.
- Απρόσμενες αλληλεπιδράσεις μεταξύ προγραμμάτων, όπως εσφαλμένη ανάθεση δικαιωμάτων σε αρχεία, σφάλματα στη δομή και το περιεχόμενο αρχείων διαμόρφωσης κ.ά.

Προκειμένου να αντιμετωπισθούν τα ζητήματα αυτά είναι δυνατόν να υιοθετηθούν στατικές ή δυναμικές μέθοδοι, όπως συνοψίζεται στον πίνακα **5:**

| | **Ανάλυση (στατική μέθοδος)** | **Ανίχνευση επιβολή πολιτικών (δυναμική μέθοδος)** |
|---|---|---|
| **Προγραμματιστικά σφάλματα** | Ανάλυση πρωτογενούς κώδικα για ανίχνευση σφαλμάτων | Παρακολούθηση συμπεριφοράς και επιβολή ασφαλών προτύπων για τα προγράμματα |
| **Σφάλματα ολοκλήρωσης** | Ανάλυση διαμόρφωσης συστήματος για εντοπισμό αδυναμιών | Ανίχνευση προσπαθειών για εκμετάλλευση αδυναμιών |

**Πίνακας 5. Στατικές και δυναμικές μέθοδοι**

Η ανάλυση του πρωτογενούς κώδικα για ανίχνευση σφαλμάτων **(security audit)** είναι μία διαδικασία όπου ειδικοί περί την ασφάλεια αναλύουν γραμμή προς γραμμή τον πρωτογενή κώδικα των συστημάτων για εντοπισμό πιθανών ευπαθειών.

Δεδομένου όμως ότι η ανάλυση γίνεται από ανθρώπους πάντα ενυπάρχει ο κίνδυνος σφάλματα να **«**ξεφύγουν**»** και έτσι προϊόντα που έχουν περάσει από πολλαπλές αναλύσεις ασφάλειας κώδικα διαπιστώθηκε στο τέλος ότι έχουν προβλήματα ασφάλειας. Σχετικά με τις δυναμικές μεθόδους, υπάρχουν οι ακόλουθες διαστάσεις**[137]:**

**Ø** Ανίχνευση αδόκιμων τρόπων χρήσης. Με την προσέγγιση αυτή κωδικοποιούνται οι αδόκιμοι τρόποι χρήσης του συστήματος και επιχειρείται η ανίχνευση εμφανίσεών των. Κάθε τέτοια εμφάνιση είναι και μία πιθανή επίθεση.

**Ø** Ανίχνευση μη φυσιολογικών συμπεριφορών. Βάσει αυτής της τεχνικής, το σύστημα έχει κάποια **«**φυσιολογική συμπεριφορά**»**, ποσοτικοποιημένη από κάποια μεγέθη. Απόκλιση από αυτά τα μεγέθη σηματοδοτεί κάποια ενδεχόμενη επίθεση.

**Ø** Ανίχνευση βάσει προδιαγραφών. Με βάση την προσέγγιση αυτή καθορίζεται η προτιθέμενη συμπεριφορά των προγραμμάτων έναντι της κωδικοποίησης των αδόκιμων τρόπων χρήσης. Για παράδειγμα, μπορεί να κωδικοποιηθεί ότι η προτιθέμενη συμπεριφορά ενός κειμενογράφου είναι το άνοιγμα ενός αρχείου ακολουθούμενο από την εγγραφή του. Αν ένας κειμενογράφος διαπιστωθεί ότι προσπαθεί να τροποποιήσει ένα αρχείο συστήματος που δεν έχει ανοιχθεί προηγουμένως ρητώς από τον χρήστη, τότε μάλλον υφίσταται πρόβλημα στην ασφάλεια.

## 3.4 Υπάρχουν καλοί ιοί;

Ένα θέμα που έχει τεθεί σχετικά με τους ιούς εισάγει τον προβληματισμό του αν κάποιο πρόγραμμα που έχει όλα τα χαρακτηριστικά του ιού μπορεί να χρησιμοποιηθεί για καλό σκοπό **[31],** περιλαμβάνοντας στο κομμάτι που ονομάζεται πρόκληση ζημιάς κώδικα ο οποίος θα απέβαινε έπ' ωφελεία του χρήστη. Ως συγκεκριμένα παραδείγματα **«**καλών ιών**»** έχουν προβληθεί τα κάτωθι:

**Ø** Ο **«**αντιβιοτικός**»** ιός, ο οποίος εντοπίζει και **«**σκοτώνει**»** τους κακούς ιούς.

**Ø** Ο ιός **«**συμπιεστής**»**, που εντοπίζει τα αρχεία με σπάνια χρήση και τα συμπιέζει, επισυνάπτοντας στο συμπιεσμένο αρχείο και μία παραλλαγή του εαυτού του που στοχεύει στην αποσυμπίεση του αρχείου.

**Ø** Ο ιός **«**κρυπτογράφος**»**, ο οποίος εγκαθίσταται στο σκληρό δίσκο και τον κρυπτογραφεί βάσει ενός συνθηματικού που δίνει ο χρήστης, προκειμένου να κρατήσει τα περιεχόμενά του αθέατα για τα αδιάκριτα βλέμματα.

**Ø** Ο ιός **«**συντηρητής**»** που πραγματοποιεί κάποιες λειτουργίες συντήρησης π.χ. διαγραφή προσωρινών αρχείων.

Σε κάθε περίπτωση, η τοποθέτησή μας πάνω στο ζήτημα ύπαρξης «καλών ιών» πρέπει να είναι κατηγορηματικά αρνητική. Σ' αυτή την κατεύθυνση συντρέχουν τόσο τεχνικοί λόγοι, όσο και ηθικά, νομικά και ψυχολογικά ζητήματα **[31,103,137]**.

**1)** Τεχνικοί λόγοι

**i)** Αδυναμία ελέγχου. Οι ιοί εκ κατασκευής δεν έχουν δικλείδες ελέγχου: η δράση τους υπαγορεύεται από το σχήμα «μόλυνση-επίθεση» (εδώ η επίθεση θα πρέπει να είναι μια δέσμη θετικών ενεργειών) και δεν υπάρχει άμεσος τρόπος να υπαγορεύσουμε σε κάποιον ιό να κάνει ή να μην κάνει κάποια πράγματα, μέσω π.χ. ενός συνόλου ρυθμίσεων, όπως θα συνέβαινε με ένα «κανονικό» πρόγραμμα.

**ii)** Δυσκολία διάκρισης. Προκειμένου να αντιμετωπισθεί ένας «κακός» ιός που έχει εισέλθει σε ένα σύστημα πρέπει πρώτα να εντοπισθεί η ύπαρξή του, είτε από τον χρήστη είτε από κάποιο αυτοματοποιημένο σύστημα. Ο εντοπισμός του ιού, η διάκρισή του δηλαδή από τα «κανονικά» προγράμματα που υπάρχουν στον υπολογιστή είναι μία ήδη πολύ δύσκολη υπόθεση, η οποία θα δυσχερανθεί σε πολύ μεγάλο βαθμό αν εισάγουμε και μία διάκριση μεταξύ «καλών» και «κακών» ιών.

**iii)** Σπατάλη πόρων. Αν χρησιμοποιούμε κάποιο «κανονικό» πρόγραμμα για ένα συγκεκριμένο σκοπό, προφανώς θα έχουμε μόνο ένα αντίγραφό του. Αντίθετα αν σκοποί του συστήματός μας εξυπηρετούνται από ιούς, το πλήθος των αντιγράφων θα ισούται με το πλήθος των αρχείων που έχει μολύνει ο ιός. Επίσης, τίποτε δεν αποκλείει την πιθανότητα να εισέλθουν στο σύστημα πάνω από ένα είδη ιών που ασχολούνται με το ίδιο ζήτημα (π.χ. διαγραφή προσωρινών αρχείων), μεγαλώνοντας έτσι ακόμη περισσότερο τη σπατάλη πόρων.

**iv)** Πιθανότητα ύπαρξης σφαλμάτων. Κανείς δεν μας εγγυάται την ορθότητα των αλγορίθμων ή της υλοποίησης των ιών, ενώ δεν μπορεί να αναμένει κανείς ότι όλοι οι συγγραφείς τους θα επιδείξουν την ίδια υπευθυνότητα που επιδεικνύουν οι κατασκευαστές λογισμικού.

**v)** Ζητήματα συμβατότητας. Υπάρχει μία κατηγορία προγραμμάτων που περιέχουν κώδικα αυτοεπαλήθευσης, είτε για λόγους προστασίας από αντιγραφή είτε για λόγους εγγυημένης καλής λειτουργίας. Αν ένας «καλός ιός» μολύνει ένα τέτοιο αρχείο θα προκαλέσει μοιραία και την διακοπή της ομαλής λειτουργίας του, καθιστώντας το άχρηστο.

**2)** Ηθικά, νομικά και ψυχολογικά ζητήματα

**i)** Μη εξουσιοδοτημένη τροποποίηση δεδομένων. Ο «καλός ιός» εισέρχεται στο σύστημα χωρίς τη γνώση και τη ρητή συγκατάθεση του χρήστη και ξεκινά να τροποποιεί προγράμματα και δεδομένα χωρίς και πάλι ο χρήστης (ή ο ιδιοκτήτης) να γνωρίζει κάτι σχετικά. Αυτό αντιβαίνει, εκτός των άλλων, σε έναν από τους

βασικούς κανόνες της ασφάλειας όπου επιθυμούμε όλες οι ενέργειες να γίνονται κατόπιν κατάλληλης εξουσιοδότησης.

**ii)** Ζητήματα ιδιοκτησίας και πνευματικής ιδιοκτησίας. Οι κατασκευαστές των **«**κανονικών προγραμμάτων**»** μπορεί να εγείρουν τέτοιου είδους ζητήματα, καθώς η άδεια χρήσης ενός προγράμματος συνήθως δεν περιλαμβάνει την παροχή δυνατότητας στον χρήστη να τροποποιήσει το πρόγραμμα καθ' οιονδήποτε τρόπο.

**iii)** Πιθανή κακή χρήση. Καμία εγγύηση δεν παρέχεται από τους –πιθανότατα άγνωστους συνολικά– κατασκευαστές **«**καλών ιών**»** ότι θα έχουν μόνο θετικές επιπτώσεις για το σύστημα και δεν θα προβαίνουν και σε ύποπτες ή επιζήμιες ενέργειες.

**iv)** Υπευθυνότητα και καταλογισμός ευθυνών. Δεν υπάρχει η δυνατότητα καταλογισμού ευθυνών για αρνητικές συνέπειες που θα έχει ένας **«**καλός ιός**»**, καθώς ο κατασκευαστής του είναι συνήθως άγνωστος. Ακόμη και αν τυχόν προβλήματα προέρχονται από προγραμματιστικά σφάλματα παρά από κακή πρόθεση, δεν είναι βέβαιο ότι οι κατασκευαστές των ιών θα φροντίσουν να τα διορθώσουν και αν ακόμη το κάνουν, δεν είναι σαφές πώς οι επιδιορθωμένες εκδόσεις θα φτάσουν στους υπολογιστές των τελικών χρηστών, μια και οι ίδιοι οι χρήστες δεν γνωρίζουν ότι ο ιός είναι εγκατεστημένος στο σύστημά τους, συνεπώς δεν θα σπεύσουν να προμηθευτούν την τελευταία έκδοση.

**v)** Αντίληψη του όρου **«**ιός**»**. Τόσο από τον χώρο της βιολογίας και της ιατρικής, όσο και από τον χώρο της πληροφορικής, ο όρος **«**ιός**»** είναι αρνητικά φορτισμένος και έτσι ελάχιστοι χρήστες θα δεχόταν θετικά την ύπαρξη ενός τέτοιου λογισμικού στον υπολογιστή τους.

**vi)** Ζητήματα εμπιστοσύνης και αισθήματος ασφάλειας. Οι χρήστες αισθάνονται καλύτερα έχοντας την ψευδαίσθηση ότι γνωρίζουν τι συμβαίνει στον υπολογιστή τους, ή τουλάχιστον γνωρίζοντας ότι έχουν επιλέξει το λογισμικό που χρησιμοποιούν. Η πιθανότητα για ανεξέλεγκτη είσοδο και λειτουργία λογισμικού στον υπολογιστή ελαττώνει την ασφάλεια που νοιώθει ο μέσος χρήστης και τον κάνει να μην εμπιστεύεται ιδιαίτερα τη χρήση του υπολογιστή.

## 3.5 Αντιμετώπιση κακόβουλου λογισμικού

Με δεδομένο ότι το κακόβουλο λογισμικό είναι ένας εν δυνάμει ιδιαίτερα καταστροφικός εχθρός της ασφάλειας οποιουδήποτε πληροφοριακού συστήματος, είναι απαραίτητο να υπάρχει μία στρατηγική πρόληψης και αντιμετώπισής του. Η στρατηγική αυτή έχει δύο σκέλη, το διαδικαστικό σκέλος που συνίσταται σε ενέργειες που πρέπει ή δεν πρέπει να γίνονται από τους χρήστες και τους

διαχειριστές, ενώ το τεχνικό σκέλος περιλαμβάνει κυρίως λογισμικό και ρυθμίσεις. Το διαδικαστικό σκέλος της αντιμετώπισης **malware** περιέχει τα ακόλουθα βήματα**[46]**:

**1.** Η επεξεργασία των δεδομένων γίνεται μόνο με συγκεκριμένα και ελεγμένα προγράμματα. Από τη στιγμή που σε έναν υπολογιστή εκτελούνται μόνο προγράμματα που δεν περιέχουν κακόβουλο λογισμικό, ο υπολογιστής είναι βέβαιο ότι δεν θα μολυνθεί. Νέα προγράμματα που υπόσχονται περισσότερη λειτουργικότητα ή ευχρηστία μπορούν κάλλιστα να είναι δούρειοι ίπποι που θα εναποθέσουν ιούς στο σύστημά μας. Ως ακραίο μέτρο για την αποφυγή εισόδου νέων ανέλεγκτων προγραμμάτων στα συστήματά τους, πολλές εταιρίες έχουν αφαιρέσει βασικές μονάδες εισόδου **(**οδηγούς **cd-dvd-**δισκέτας**)** από τους υπολογιστές τους.

**2.** Αποφυγή λήψης και εκτέλεσης αρχείων που έχουν επισυναφθεί σε ύποπτα μηνύματα ή από αμφιβόλου αξιοπιστίας ιστοχώρους ή από **newsgroups**. Τα προγράμματα αυτά είναι το κυριότερο μέσο διάδοσης ιών και οι χρήστες πρέπει συνειδητά να αποφεύγουν την εκτέλεσή τους.

**3.** Συχνή λήψη εφεδρικών αντιγράφων και τήρησή τους επί μακρόν. Ανεξαρτήτως των μέτρων που θα ληφθούν για πρόληψη, είναι τελικά πιθανό το σύστημα να μολυνθεί. Στην περίπτωση αυτή θα πρέπει να είμαστε σε θέση να αποκαταστήσουμε την προ της μολύνσεως εικόνα του συστήματος. Καθώς η αποκάλυψη του **Malware** μπορεί να μην είναι άμεση, θα πρέπει να τηρούμε τα εφεδρικά αντίγραφα για πολύ καιρό ώστε η αντικατάσταση των μολυσμένων αρχείων με τα αντίστοιχα **«**καθαρά**»** να είναι εφικτή.

Στο τεχνικό σκέλος μπορούμε να διακρίνουμε τις κάτωθι συνιστώσες**[103]**:

**1.** Απαγόρευση της εκκίνησης από μονάδες δισκέτας**-cd-dvd.** Οι περισσότεροι ιοί τομέων εκκίνησης μολύνουν τους υπολογιστές κατά την εκκίνηση από μολυσμένη δισκέτα. Οι χρήστες δεν πρέπει να ξεκινούν τους υπολογιστές με δισκέτες μέσα στη μονάδα, ενώ το **BIOS** των υπολογιστών πρέπει να ρυθμίζεται κατάλληλα ώστε να μην προσπαθεί να εκκινήσει τον υπολογιστή από τη δισκέτα.

**2**. Ρύθμιση του υπολογιστή στο μέγιστο επίπεδο ασφάλειας. Η οδηγία αυτή ισχύει κατά μείζονα λόγο για προγράμματα πλοήγησης και ανάγνωσης ηλεκτρονικού ταχυδρομείου, καθώς αυτά είναι εν δυνάμει πύλες εισόδου κακόβουλου λογισμικού στο σύστημα.

**3.** Χρήση ειδικού λογισμικού για αντιμετώπιση κακόβουλου λογισμικού. Το λογισμικό αντιμετώπισης **Malware** είναι ένα ζήτημα που αναλύεται εκτενώς στις παραγράφους που ακολουθούν.

### 3.5.1 Λογισμικό αντιμετώπισης Malware

Το λογισμικό αντιμετώπισης **Malware** είναι μία πολυσύνθετη κατηγορία λογισμικού που περιλαμβάνει εργαλεία με στόχο**[137]:**

**1.** την ανίχνευση. Τα εργαλεία ανίχνευσης προσδιορίζουν και αναφέρουν αν το σύστημά μας έχει μολυνθεί. Η ανίχνευση μπορεί να γίνεται είτε με ανάλυση των αντικειμένων του συστήματος σε περιοδική βάση ή κατά τη χρησιμοποίησή τους, με παρεμπόδιση των παράνομων ενεργειών ή με ανίχνευση των αναιτιολόγητων αλλαγών.

**2.** τον προσδιορισμό της ταυτότητας του κακόβουλου λογισμικού. Αν το σύστημά μας έχει μολυνθεί από ιό, ένα εργαλείο προσδιορισμού ταυτότητας θα μας πληροφορήσει για το ποιος συγκεκριμένος ιός έχει προκαλέσει τη μόλυνση. Ο προσδιορισμός ταυτότητας είναι χρήσιμος αφ' ενός για να μπορέσουμε να αποτιμήσουμε το μέγεθος της ζημιάς και τον πιθανό κίνδυνο που διατρέχουμε, αφ' ετέρου δε για να χαράξουμε τη βέλτιστη στρατηγική επανόρθωσης.

**3.** τον καθαρισμό του κακόβουλου λογισμικού. Σε πολλές περιπτώσεις οι αλλαγές που έχουν επιφέρει τα **Malware** στο σύστημα είναι αντιστρέψιμες με αυτοματοποιημένο τρόπο. Τα εργαλεία καθαρισμού φροντίζουν για την αναίρεση των αλλαγών που έχουν προκληθεί.

### 3.5.2 Κριτήρια επιλογής εργαλείων

Για να επιλέξουμε ποια κατηγορία εργαλείων αντιμετώπισης **Malware** είναι πιο κατάλληλη για το σύστημά μας, ή ακόμη και για επιλογή μεταξύ εργαλείων της ίδιας κατηγορίας θα χρησιμοποιήσουμε τέσσερις άξονες κριτηρίων: την ακρίβεια, την ευχρηστία, τη διαχειριστική επιβάρυνση και την επιβάρυνση του συστήματος**[137]**.

#### 3.5.2.1 Ακρίβεια

Ένα ακριβές εργαλείο πρέπει να επιτελεί τον σκοπό του σωστά σε όλες τις περιπτώσεις. Η ακρίβεια λαμβάνει διαφορετική σημασία για κάθε μία από τις κατηγορίες εργαλείων ως εξής:

**1**. για τα εργαλεία ανίχνευσης **Malware**, ως ακριβή ορίζονται τα εργαλεία που ανιχνεύουν όλα τα **Malware** και μόνον αυτά. Η ακρίβεια χάνεται όταν έχουμε αναφορά ανύπαρκτων **Malware (false positives)** ή αδυναμία εντοπισμού υπαρκτών **(false negatives)**. Η αδυναμία εντοπισμού υπαρκτών **Malware** είναι σαφώς πιο επικίνδυνη καθώς δεν λαμβάνονται μέτρα για το λογισμικό που έχει ήδη μολύνει το σύστημα, αλλά από την άλλη πλευρά η συχνή αναφορά ανύπαρκτων **Malware**

μειώνει την αξιοπιστία του συστήματος και ενδεχομένως η χρήστες να μην λάβουν υπόψη τους μία ορθή αναφορά ύπαρξης **Malware.**

**2.** για τα εργαλεία προσδιορισμού ταυτότητας, ως ακριβή ορίζονται τα εργαλεία που προσδιορίζουν επακριβώς το λογισμικό που έχει μολύνει το σύστημα. Η ακρίβεια εδώ χάνεται όταν δεν είναι δυνατόν να προσδιοριστεί συγκεκριμένο **Malware** ή προσδιορίζεται διαφορετικό από αυτό που πραγματικά έχει μολύνει το σύστημα. Ως κριτήρια διαφορετικότητας των **Malware** θα χρησιμοποιείται **(**α**)** η διαφορά στη ζημιά που μπορούν να προκαλέσουν και **(**β**)** η διαφορά στη στρατηγική ή τα εργαλεία αντιμετώπισής τους.

**3.** για τα εργαλεία καθαρισμού, ως ακριβή ορίζονται τα εργαλεία εκείνα που καταφέρνουν να φέρουν το κάθε μολυσμένο αντικείμενο στην κατάσταση που βρισκόταν πριν μολυνθεί. Η ακρίβεια εδώ μειώνεται όταν η επάνοδος αυτή δεν επιτυγχάνεται πλήρως, αλλά στην απώλεια ακρίβειας μπορούμε να έχουμε δύο υποπεριπτώσεις. Η πρώτη είναι η συνολική αποτυχία, όπου παράγεται αντικείμενο που δεν λειτουργεί **(**εκτελέσιμο πρόγραμμα που δεν **«**τρέχει**»** ή τομέας εκκίνησης που δεν εκκινεί το σύστημα**)** ή όταν η απομάκρυνση του **Malware** είναι συνολικά αδύνατη. Η δεύτερη είναι η μερική αποτυχία, όπου παράγεται μεν ένα αντικείμενο που λειτουργεί, αλλά είναι διαφορετικό από το αρχικό.

#### 3.5.2.2 Ευχρηστία

Τα ζητήματα ευχρηστίας αξιολογούν το κατά πόσο είναι εύκολο για τον χρήστη να χρησιμοποιήσει το λογισμικό, δηλαδή να το ενεργοποιήσει και να ανταποκριθεί σωστά στα μηνύματα που τυχόν του εμφανίζεται. Επιπρόσθετα, αξιολογείται το κατά πόσο τροποποιείται η συνήθης λειτουργία του συστήματος αναφορικά με τους χρήστες, δηλαδή αν αυτοί αναγκάζονται να κάνουν πρόσθετες ενέργειες ή να εκτελούν κάποιες διαδικασίες με πιο δύσκολο τρόπο.

#### 3.5.2.3 Διαχειριστική επιβάρυνση

Κάθε λογισμικό που σε ένα υπολογιστικό σύστημα έχει ένα διαχειριστικό κόστος που αντανακλά το πόσο πρέπει να απασχοληθεί η ομάδα διαχείρισης του συστήματος με το συγκεκριμένο λογισμικό. Το διαχειριστικό κόστος είναι το άθροισμα του κόστους εγκατάστασης, του κόστους ρύθμισης, του κόστους συντήρησης και του κόστους υποστήριξης των τελικών χρηστών.

#### 3.5.2.4 Επιβάρυνση συστήματος

Τα εργαλεία αντιμετώπισης **Malware**, όταν εγκατασταθούν σε κάποιο σύστημα καταναλώνουν πόρους του συστήματος, όπως χώρος στον δίσκο, μνήμη και χρόνο εκτέλεσης της κεντρικής μονάδας επεξεργασίας. Όλα αυτά θα προκαλέσουν μία

επιβράδυνση της λειτουργίας του συστήματος, η οποία οφείλει να είναι όσο το δυνατόν μικρότερη. Στην ιδεώδη περίπτωση, οι πόροι (κυρίως η μνήμη και η ΚΜΕ) θα καταναλώνονται σε χρόνο που δεν θα επικαλύπτεται με τις ώρες «κανονικής» χρήσης του μηχανήματος από τους χρήστες, αν και αυτό δεν είναι πάντα εφικτό.

### 3.5.3 Εργαλεία και τεχνικές

Στην συνέχεια θα παρουσιασθούν οι κυριότερες κατηγορίες εργαλείων λογισμικού και τεχνικών για την αντιμετώπιση των **Malware[31,46].**

#### 3.5.3.1 Εντοπισμός υπογραφών

Η μέθοδος αυτή χρησιμοποιείται κυρίως από εργαλεία εντοπισμού ιών, τα οποία δρουν παράλληλα και ως εργαλεία προσδιορισμού ταυτότητας των ιών, και τα οποία επιχειρούν να ανιχνεύσουν αν υπάρχει ιός προσκολλημένος σε αντικείμενα του δίσκου ή εγκατεστημένος στη μνήμη. Τα εργαλεία αυτά είναι δυνατόν να ελέγχουν τα αντικείμενα σε κάθε πρόσβαση που γίνεται σε αυτά, ή σε περιοδική βάση, π.χ. μία φορά κάθε εβδομάδα. Με τον όρο «υπογραφή ιού» περιγράφεται μία ακολουθία από **bytes** τα οποία είναι γνωστό ότι ανήκουν σε ιούς ή οικογένειες ιών. Για παράδειγμα, αν ο κώδικας ενός συγκεκριμένου ιού για προσωπικούς υπολογιστές περιλαμβάνει τις εντολές συμβολικής γλώσσας:

```
push ax
mov ax, 2032
push bx
mov bx, 6782
call 8776
pop bx
pop ax
```

αυτό σημαίνει ότι το αντικείμενο στο οποίο ο ιός έχει προσκολληθεί θα περιλαμβάνει την ακολουθία **bytes 50 B8 32 20 53 BB 82 67 E8 6B 86 5B 58**

Μία ακολουθία από **bytes** που θα χρησιμοποιηθεί ως υπογραφή ενός ιού θα πρέπει να έχει τα εξής δύο χαρακτηριστικά:

**1.** να υπάρχει σε όλα τα αρχεία που έχουν μολυνθεί από το ιό.

**2.** να είναι αδύνατον (ή τουλάχιστον σχετικά απίθανο) να εμφανιστεί η συγκεκριμένη ακολουθία σε αρχεία που δεν έχουν μολυνθεί από τον ιό.

Οι υπογραφές συλλέγονται από μολυσμένα αντικείμενα, μετά από ανάλυσή τους. Μία υπογραφή μπορεί να περιέχει μεταχαρακτήρες, προκειμένου να αντιμετωπίζονται περιπτώσεις όπου συγκεκριμένα **bytes** μπορούν να αλλάζουν ανάμεσα σε διαφορετικά αντικείμενα που έχουν μολυνθεί από τον ίδιο ιό. Για παράδειγμα, στον κώδικα που παρατίθεται ανωτέρω, η διεύθυνση που καλείται μέσω εντολή **call** της πέμπτης γραμμής θα μπορούσε να είναι διαφορετική για δύο μολυσμένα αρχεία, ανάλογα με το σημείο του αρχείου όπου έχει προσκολληθεί ο ιός. Στην περίπτωση αυτή η υπογραφή του ιού θα μπορούσε να διαμορφωθεί σε **50 B8 32 20 53 BB ? ? E8 6B 86 5B 58** όπου κάθε χαρακτήρας **?** έχει την έννοια **«**ένα, οποιοδήποτε **byte»**. Παρομοίως θα μπορούσαν να χρησιμοποιηθούν και άλλοι μεταχαρακτήρες, όπως το *** (**οσαδήποτε, οποιαδήποτε **bytes –** αν και η εμφάνισή του είναι σχετικά ασυνήθιστη**)** ή ειδικές γραφές για την αναπαράσταση ενός **byte** που μπορεί να λάβει μία τιμή από ένα καθορισμένο σύνολο **(**π.χ. **{02, 2A, C0, DF})** κ.λπ.

Η υπογραφή μπορεί επίσης να συμπληρώνεται από κάποια ένδειξη θέσης εντός του αντικειμένου, π.χ. **«**τα πρώτα **bytes** του αντικειμένου**» (**περίπτωση που θα κάλυπτε τους ιούς που επικαλύπτουν τον εκτελέσιμο κώδικα**), «**τα τελευταία **bytes** του αντικειμένου**» (**π.χ. ιοί που προσκολλώνται στο τέλος και τοποθετούν εντολές άλματος στην αρχή των αντικειμένων**)** ή **«**μέσα στα **300** πρώτα **bytes** του αντικειμένου**»**. Η παράθεση της ένδειξης θέσης είναι χρήσιμη αφ' ενός διότι μειώνει το πλήθος των **bytes** που πρέπει να ελεγχθούν για ύπαρξη της υπογραφής, αφ' ετέρου δε διότι μειώνει την πιθανότητα να ανιχνευθεί η υπογραφή σε κάποιο σημείο όπου η παρουσία της δεν υποδηλώνει ύπαρξη ιού. Οι πολυμορφικοί ιοί είναι δύσκολο να ανιχνευθούν μέσω υπογραφών καθώς μεταλλάσσονται τόσο πολύ μεταξύ δύο μολύνσεων που δεν έχουν κάποια σταθερή **«**υπογραφή**»**. Για τους ιούς αυτούς απαιτείται αλγοριθμική ανίχνευση.

Ακρίβεια

Η μέθοδος του εντοπισμού υπογραφών είναι απόλυτα ακριβής αν έχουν ελεγχθεί από τον κατασκευαστή του σχετικού λογισμικού όλοι τα **Malware** και όλα τα **«**κανονικά**»** εκτελέσιμα, κάτι που προφανώς είναι αδύνατον. Έτσι είναι πιθανόν να υπάρξουν ψευδείς αναφορές για ύπαρξη αυτών, όταν κάποια **«**υπογραφή**»** συμβεί να υπάρχει σε κάποιο **«**κανονικό**»** πρόγραμμα, ή να μην αναφερθεί η ύπαρξη κάποιου υπαρκτού ιού, είτε διότι αυτός χρησιμοποιεί τεχνικές απόκρυψης **(stealth techniques)[46]** είτε διότι το **«**πακέτο υπογραφών**»** που χρησιμοποιεί το λογισμικό είναι ελλιπές ή παρωχημένο και δεν περιλαμβάνει την **«**υπογραφή**»** του κακόβουλου λογισμικού. Με δεδομένο ότι τα εργαλεία που βασίζονται στον εντοπισμό υπογραφών λειτουργούν και ως εργαλεία προσδιορισμού ταυτότητας, η

διάσταση της ακρίβειας περιλαμβάνει και τον ορθό προσδιορισμό της ταυτότητας του λογισμικού, και πιθανά προβλήματα σ' αυτή τη διάσταση περιλαμβάνουν την αναφορά λανθασμένης ταυτότητας ιού ή εσφαλμένης παραλλαγής του ίδιου ιού, κάτι που μπορεί να συμβεί αν οι ιοί «μοιάζουν» πολύ και αν δεν έχουν διαμορφωθεί με αρκετή ακρίβεια τα «πακέτα υπογραφών».

Ευχρηστία

Τα εργαλεία που βασίζονται στον εντοπισμό υπογραφών είναι ιδιαίτερα εύχρηστα για τους τελικούς χρήστες, καθώς απαιτούν πολύ λίγες γνώσεις. Ουσιαστικά οι χρήστες πρέπει μόνο να ζητούν την εκτέλεσή τους και να ανταποκρίνονται σε μηνύματα του τύπου «το τάδε αρχείο είναι μολυσμένο από ιό», μήνυμα που είναι καταληπτό ακόμη και από μη ειδικούς στην πληροφορική.

Διαχειριστική επιβάρυνση

Δεδομένου ότι κάθε μέρα εμφανίζονται νέα **Malware**, ένα «πακέτο υπογραφών» που φτιάχνεται σήμερα σε μία εβδομάδα θα υπολείπεται σημαντικά σε γνώση για τα νέα **Malware**. Η διαρκής ενημέρωση που απαιτείται μπορεί να αποτελέσει πρόβλημα σε μεγάλους οργανισμούς, ειδικά αν δεν υπάρχει η δυνατότητα αυτοματοποίησής της. Η εγκατάσταση των σχετικών εργαλείων είναι εύκολη, ακόμη και για απλούς χρήστες και, στον βαθμό που οι διαγνώσεις είναι σωστές, δεν απαιτείται υποστήριξη των χρηστών. Αν, ωστόσο, το πρόγραμμα αναφέρει κάποιο **Malware** που δεν υπάρχει στην πραγματικότητα **(false positive)**, η συνδρομή του διαχειριστή είναι απαραίτητη.

Επιβάρυνση συστήματος

Τα εργαλεία που βασίζονται σε εντοπισμό υπογραφών είναι αρκετά αποδοτικά, καθώς χρησιμοποιούνται για πολύ καιρό και οι σχετικοί αλγόριθμοι έχουν βελτιστοποιηθεί σε μεγάλο βαθμό. Ειδικότερα, αν λειτουργούν σε περιοδική βάση (σε αντιδιαστολή με τη διαρκή παρακολούθηση), η επιβάρυνση του συστήματος είναι αμελητέα, καθώς μάλιστα μπορούν να διενεργούν τους ελέγχους σε περιόδους που το σύστημα δεν χρησιμοποιείται παραγωγικά (π.χ. βραδινές ώρες, Σαββατοκύριακα).

Εντοπισμός υπογραφών – Σύνοψη

Τα θετικά σημεία της τεχνικής εντοπισμού υπογραφών καθώς και των εργαλείων που βασίζονται σ' αυτή είναι τα εξής (Πίνακας **6**):

- Τα καλά συντηρούμενα συστήματα εντοπίζουν άνω του **95%** των ιών
- Δρούν και ως εργαλεία προσδιορισμού ταυτότητας, μειώνοντας τον χρόνο ανάκαμψης.

- Δοκιμασμένη τεχνολογία με βελτιστοποιημένους αλγόριθμους
- Απαιτείται ελάχιστη γνώση

Ενώ τα αρνητικά είναι ότι:

- Βρίσκουν μόνο ιούς που ήταν γνωστοι κατά την ανάπτυξη του «πακέτου υπογραφών»
- Πρέπει να συντηρούνται διαρκώς
- Είναι επιρρεπή σε εσφαλμένους προσδιορισμούς ταυτότητας
- Οι χρήστες παρανοούν το «δεν ανιχνεύθηκε ιός» πιστεύοντας ότι σημαίνει ότι «δεν υπάρχει ιός»

| *Υπέρ* | *Κατά* |
|---|---|
| Τα καλά συντηρούμενα συστήματα εντοπίζουν άνω του 95% των ιών | Βρίσκουν μόνο τους ιούς που ήταν γνωστοί κατά την ανάπτυξη του «πακέτου υπογραφών» |
| Δρουν και ως εργαλεία προσδιορισμού ταυτότητας, μειώνοντας τον χρόνο ανάκαμψης | Πρέπει να συντηρούνται διαρκώς |
| Δοκιμασμένη τεχνολογία με βελτιστοποιημένους αλγόριθμους | Είναι επιρρεπή σε εσφαλμένους προσδιορισμούς ταυτότητας |
| Απαιτείται ελάχιστη γνώση | Οι χρήστες παρανοούν το «δεν ανιχνεύθηκε ιός» πιστεύοντας ότι σημαίνει «δεν υπάρχει ιός» |

**Πίνακας 6. Θετικά και αρνητικά σημεία της τεχνικής εντοπισμού υπογραφών**

### 3.5.3.2 Έλεγχος ακεραιότητας

Ο έλεγχος ακεραιότητας είναι μία τεχνική που χρησιμοποιείται για την ανίχνευση μόνο των **Malware,** χωρίς να δίνει τη δυνατότητα προσδιορισμού της ταυτότητάς τους. Η τεχνική αυτή έχει δύο στάδια**[137]:**

**1.** Στο πρώτο στάδιο δημιουργείται μία βάση δεδομένων με αθροίσματα ελέγχου**,** για κάθε αντικείμενο του συστήματος που είναι πιθανό θύμα επίθεσης**.** Τα αθροίσματα ελέγχου μπορούν να δημιουργούνται με χρήση κυκλικών πλεοναστικών κωδίκων **(CRC)** ή με κρυπτογραφικές μεθόδους**.** Καθώς η χρήση κρυπτογραφικών μεθόδων είναι ιδιαίτερα δαπανηρή υπολογιστικά**,** μία τρίτη επιλογή είναι να δημιουργείται πρώτα μία συνάρτηση κερματισμού **(hash function)** στο αντικείμενο και στη συνέχεια να εφαρμόζεται στο αποτέλεσμά της κάποια κρυπτογραφική

μέθοδος. Η δημιουργία της βάσης δεδομένων πρέπει να γίνει σε «καθαρό» σύστημα, δηλαδή σε σύστημα που είναι βέβαιο πως δεν έχει μολυνθεί από ιό.

**2.** Στο δεύτερο στάδιο για κάθε αντικείμενο του συστήματος επανυπολογίζεται το άθροισμα ελέγχου και συγκρίνεται με το αντίστοιχο άθροισμα ελέγχου που έχει αποθηκευθεί στη βάση δεδομένων. Αν τα αθροίσματα ελέγχου είναι διαφορετικά, τότε το αντικείμενο έχει τροποποιηθεί, πιθανότατα λόγω δράσης κάποιου **Malware**.

Ακρίβεια

Η τεχνική του ελέγχου ακεραιότητας εντοπίζει όλα τα **Malware**, αρκεί ο αρχικός υπολογισμός να έχει γίνει σε καθαρό σύστημα, συνεπώς δεν υπάρχει πιθανότητα να μην αναφερθεί κάποιο υπάρχων **Malware (false negative)**. Υπάρχει όμως σημαντική πιθανότητα για ψευδείς αναφορές ύπαρξης **Malware**, καθώς δεν είναι σπάνιες οι περιπτώσεις προγραμμάτων που τροποποιούν τον εαυτό τους, π.χ. για να αποθηκεύσουν ρυθμίσεις, στατιστικά στοιχεία ή οποιαδήποτε άλλη πληροφορία. Επίσης, η τεχνική αυτή δεν μπορεί να αντιμετωπίσει καθόλου τους ιούς μακροεντολών, καθώς αυτοί μολύνουν τα αρχεία δεδομένων, τα οποία είναι φυσιολογικό να αλλάζουν ως αποτέλεσμα της επεξεργασίας τους.

Ευχρηστία

Για να είναι αποτελεσματική η τεχνική αυτή, θα πρέπει η βάση δεδομένων των αθροισμάτων ελέγχου πρέπει να αποθηκεύεται σε μη προσβάσιμη περιοχή, καθώς αν η περιοχή είναι προσβάσιμη ένα πιο «έξυπνο» **Malware** θα μπορούσε εκτός από το αντικείμενο να τροποποιήσει και το σχετικό άθροισμα ελέγχου στη βάση δεδομένων. Η απαίτηση αυτή εισάγει διαδικασίες που δεν είναι αρεστές στους μέσους χρήστες. Πέραν αυτού, ο μέσος χρήστης δεν γνωρίζει αν ένα πρόγραμμα αυτοτροποποιείται ή όχι, και τέτοιου είδους ψευδείς αναφορές δημιουργούν μεγάλα προβλήματα στους χρήστες. Αν δε, το πλήθος των ψευδών αναφορών γίνει μεγάλο, οι χρήστες θα γίνουν ιδιαίτερα επιφυλακτικοί στις προειδοποιήσεις.

Διαχειριστική επιβάρυνση

Η εγκατάσταση των εργαλείων ελέγχου ακεραιότητας είναι ιδιαίτερα εύκολη, και στη φάση της εγκατάστασης υπάρχει η δυνατότητα να ολοκληρωθεί και ο αρχικός υπολογισμός των αθροισμάτων ελέγχου. Είναι ωστόσο απαραίτητο η διαδικασία του υπολογισμού αθροισμάτων να επαναλαμβάνεται σε κάθε εγκατάσταση ή αναβάθμιση λογισμικού ή εγκατάσταση επιδιορθωτικών προγραμμάτων. Υπάρχει τέλος αναγκαιότητα για την διαρκή υποστήριξη των χρηστών, καθώς αυτοί δεν έχουν συνήθως τις ικανότητες να αντιμετωπίσουν μηνύματα του τύπου «το τάδε αρχείο έχει αλλάξει».

Επιβάρυνση συστήματος

Η τεχνική του ελέγχου ακεραιότητας δεν επηρεάζει τη συνήθη λειτουργία του συστήματος, καθώς η όλη διαδικασία μπορεί να λαμβάνει χώρα σε περιόδους όπου οι υπολογιστές δεν χρησιμοποιούνται παραγωγικά. Ο χρόνος υπολογισμού των αθροισμάτων ελέγχου μπορεί ωστόσο να είναι σημαντικός, ιδιαίτερα αν χρησιμοποιούνται αμιγώς κρυπτογραφικές μέθοδοι για την παραγωγή τους.

Έλεγχος ακεραιότητας – Σύνοψη

Στα θετικά σημεία (Πίνακας 7) της τεχνικής ελέγχου ακεραιότητας καθώς και των εργαλείων που βασίζονται σ' αυτή είναι ότι δεν χρειάζονται ενημέρωση.

Στα αρνητικά περιλαμβάνονται τα εξής:

- Πρέπει να υπολογίζονται αθροίσματα ελέγχου σε κάθε εγκατάσταση – αναβάθμιση προγράμματος.
- Δεν βρίσκουν τους ιούς, αλλά μόνο τις αλλαγές και επομένως είναι αναγκαία συμπληρωματικά εργαλεία προσδιορισμού ταυτότητας
- Εσφαλμένες αναφορές κυρίως θετικές
- Δεν είναι καθόλου αποτελεσματικοί για ιους μακροεντολών

| *Υπέρ* | *Κατά* |
|---|---|
| Δεν χρειάζονται ενημέρωση | Πρέπει να υπολογίζονται αθροίσματα ελέγχου σε κάθε εγκατάσταση-αναβάθμιση προγράμματος |
| | Δεν βρίσκουν τους ιούς – μόνο τις αλλαγές, συνεπώς απαιτούνται συμπληρωματικά εργαλεία προσδιορισμού ταυτότητας |
| | Εσφαλμένες αναφορές, κυρίως θετικές |
| | Δεν είναι καθόλου αποτελεσματικοί για ιούς μακροεντολών |

**Πίνακας 7.Θετικά και αρνητικά σημεία της τεχνικής ελέγχου ακεραιότητας**

### 3.5.3.3 Επόπτες γενικού σκοπού

Οι επόπτες γενικού σκοπού **[137,103]** προστατεύουν το σύστημα από τη διάδοση ιών ή τη δράση των Δούρειων Ίππων αναχαιτίζοντας κακόβουλες ενέργειες. Προκειμένου να αναχαιτισθεί μία κακόβουλη ενέργεια θα πρέπει πρώτα να είναι δυνατόν να διαχωριστούν οι ενέργειες που λαμβάνουν χώρα σε ένα σύστημα σε «φυσιολογικές» και «κακόβουλες». Οι κατασκευαστές των σχετικών εργαλείων μοντελοποιούν τη συμπεριφορά των ιών και των δούρειων ίππων και δημιουργούν κώδικα που προσπαθεί να ανιχνεύσει και να παρεμποδίσει τις ενέργειες αυτές. Ως

παραδείγματα μοντέλων κακόβουλων συμπεριφορών μπορούμε να παραθέσουμε τα κάτωθι**[103]:**

- Ø ένα πρόγραμμα ζητά μνήμη που **«**αυτονομείται**»**
- Ø ένα πρόγραμμα ανοίγει αρχεία συστήματος **(**π.χ**. command.com)**
- Ø ένα πρόγραμμα ανοίγει εκτελέσιμα σε άλλους καταλόγους
- Ø μακροεντολή σε ένα έγγραφο **Word** διαγράφει αρχεία **MP3**

Οι ενέργειες αυτές δεν είναι **«**φυσιολογικές**»** και δεν είναι πολύ πιθανό να γίνονται από **«**κανονικά**»** προγράμματα**.** Κατά συνέπεια**,** η εμφάνιση μιας τέτοιας ενέργειας είναι πολύ πιθανό να σηματοδοτεί τη δράση ενός **Malware.**

Ακρίβεια

Για να είναι δυνατή η ανίχνευση των κακόβουλων ενεργειών πρέπει τα **Malware** να συμπεριφερθούν βάσει των μοντέλων που έχουν καθορισθεί από τους κατασκευαστές των εργαλείων**.** Κάτι τέτοιο δεν συμβαίνει πάντα**,** καθώς νέες τεχνικές **Malware** μπορεί να ενεργούν με εντελώς διαφορετικό ή απρόσμενο τρόπο**,** με αποτέλεσμα να έχουμε **Malware** που δεν αναφέρονται **(false negatives).** Τα **Malware** επίσης μπορεί να προσπαθήσουν να απενεργοποιήσουν τον επόπτη**,** ακυρώνοντας τη δράση του**.** Αν τα καταφέρουν**,** το σύστημα θα είναι ανυπεράσπιστο**,** και έτσι θα πρέπει ο επόπτης να είναι προετοιμασμένος να **«**αμυνθεί**»** σε τέτοια ενδεχόμενα. Υπάρχει επίσης η περίπτωση μερικά **«**κανονικά προγράμματα**»** να προβαίνουν σε ενέργειες που εντάσσονται στα μοντέλα **Malware,** προκαλώντας έτσι ψευδείς αναφορές ύπαρξης **Malware (false positives).**

Ευχρηστία

Ο μέσος χρήστης δεν έχει τις γνώσεις να χειρισθεί εργαλεία που βασίζονται στην τεχνική των εποπτών γενικού σκοπού**,** καθώς η λειτουργία τους απαιτεί λεπτομερειακή διαμόρφωση και ρύθμιση**.** Επίσης**,** τα μηνύματα με τα οποία θα έλθουν αντιμέτωποι οι χρήστες δεν είναι πάντα κατανοητά **(**το πρόγραμμα ζητά την αυτονόμηση ενός μπλοκ μνήμης μεγέθους **32**K στη διεύθυνση **8023:**AB**56** και ο κώδικας σ' αυτό έχει παγιδεύσει το διάνυσμα διακοπής **19).**

Διαχειριστική επιβάρυνση

Δεδομένου ότι οι επόπτες γενικού σκοπού απαιτούν ρύθμιση**,** η διαχειριστική επιβάρυνση κατά την εγκατάσταση είναι σημαντική**,** ειδικά αν υπάρχουν ετερογενή συστήματα ή συστήματα με διαφορετικές απαιτήσεις**.** Οι απαιτήσεις για υποστήριξη των χρηστών είναι επίσης αυξημένες**,** εξαρτωμένου βέβαια και από το προφίλ των χρηστών **(**τεχνικές γνώσεις**,** πλήθος προγραμμάτων που χρησιμοποιούν**,** ειδικά

χαρακτηριστικά των ενεργειών τους κ.τ.λ.). Από την άλλη πλευρά, ένα καλά διαμορφωμένο σύστημα επόπτη γενικού σκοπού απαιτείται να ενημερωθεί μόνο όταν εμφανίζονται νέοι τρόποι δράσης **Malware**, ενώ η εμφάνιση απλά νέων κακόβουλων λογισμικών που χρησιμοποιούν «γνωστές» στο σύστημα πρακτικές δεν εγείρει ζητήματα ενημέρωσης.

Επιβάρυνση συστήματος

Η χρήση εργαλείων που βασίζονται στην τεχνική των εποπτών γενικού σκοπού εισάγει κάποια επιβάρυνση στο σύστημα, η οποία οφείλεται στην παρακολούθηση και ανάλυση των ενεργειών που λαμβάνουν χώρα στο σύστημα, προκειμένου να εντοπισθούν και να αναχαιτισθούν οι κακόβουλες πράξεις. Συνολικά, η επιβάρυνση δεν είναι ιδιαίτερα σημαντική.

Επόπτες γενικού σκοπού – Σύνοψη

Τα θετικά σημεία (Πίνακας 8) της τεχνικής των εποπτών γενικού σκοπού καθώς και των εργαλείων που βασίζονται σ' αυτή είναι τα εξής:

- Αρκετά γενική τεχνική
- Κανονικά λειτουργεί και για άγνωστους ιούς
- Μικρή συχνότητα ενημερώσεων

Ενώ στα αρνητικά περιλαμβάνονται τα ακόλουθα:

- Είναι δύσχρηστο για τον μέσο χρήστη
- Παρουσιάζει αρκετές ψευδείς αναφορές ύπαρξης ιών
- Έχει μεγάλο διαχειριστικό κόστος
- Είναι ευάλωτο σε νέες τεχνικές ιών
- Μπορεί να απενεργοποιηθεί από τους ιούς

| *Υπέρ* | *Κατά* |
|---|---|
| Αρκετά γενική τεχνική | Δύσχρηστο για τον μέσο χρήστη |
| Κανονικά λειτουργεί και για άγνωστους ιούς | Αρκετές ψευδείς αναφορές ύπαρξης ιών |
| Μικρή συχνότητα ενημερώσεων | Μεγάλο διαχειριστικό κόστος |
| | Ευάλωτο σε νέες τεχνικές ιών |
| | Μπορεί να απενεργοποιηθεί από τους ιούς |

**Πίνακας 8. Θετικά και αρνητικά σημεία της τεχνικής των εποπτών γενικού σκοπού**

### 3.5.3.4 Κελύφη ελέγχου πρόσβασης

Τα εργαλεία που βασίζονται στην τεχνική των κελυφών ελέγχου πρόσβασης **[103,137]** ενσωματώνονται στο λειτουργικό σύστημα και έχουν ως στόχο να επιβάλλουν πολιτικές που ορίζουν ποιος χρήστης μπορεί να χρησιμοποιήσει ποιο πρόγραμμα για να πραγματοποιήσει συγκεκριμένους τύπους ενεργειών σε ορισμένους τύπους αρχείων. Με δεδομένο ότι μερικά λειτουργικά συστήματα δεν περιλαμβάνουν ισχυρούς μηχανισμούς διακρίβωσης της ταυτότητας των χρηστών ή περιορισμού της πρόσβασης σε αρχεία, μερικά κελύφη ελέγχου πρόσβασης μπορούν να εισάγουν τους δικούς τους μηχανισμούς διακρίβωσης ταυτότητας ή εργαλεία κρυπτογράφησης. Τα εργαλεία κρυπτογράφησης δεν αποτρέπουν την πρόσβαση στα αρχεία, αλλά καθιστούν την πρόσβαση από μη εξουσιοδοτημένους χρήστες ουσιαστικά άχρηστη, καθώς το αρχείο θα είναι σε ακατάληπτη μορφή. Ως παραδείγματα κανόνων πρόσβασης που μπορεί να χρησιμοποιεί ένα κέλυφος ελέγχου πρόσβασης μπορούμε να παραθέσουμε τα εξής:

---

**+ (*, winword, “*.doc”, rw)**

**+ (admin, winword, “*.dot”, rw)**

**+ (*, winword, “*.dot”, r)**

**+ (admin, windowsUpdate, “c:\windows*”, “rw”)**

**- (*, *, “c:\windows\system*”, “w”)**

---

Η πρώτη γραμμή ορίζει ότι όλοι οι χρήστες μπορούν να χρησιμοποιήσουν την εφαρμογή **Winword (Word** για **Windows)** για να διαβάσουν ή να τροποποιήσουν αρχεία με επέκταση **«.doc».** Οι δύο επόμενες γραμμές δίνουν τη δυνατότητα στον διαχειριστή να διαβάζει και να τροποποιεί πρότυπα εγγράφων και στους υπόλοιπους χρήστες να τα διαβάζουν, πάντα μέσω της εφαρμογής **Winword.** Η τέταρτη γραμμή επιτρέπει στον διαχειριστή να ενημερώνει αρχεία στον κατάλογο **c:\windows** μέσω της εφαρμογής **WindowsUpdate,** ενώ η τελευταία γραμμή απαγορεύει όλες τις υπόλοιπες ενημερώσεις στον κατάλογο **c:\windows\system** από οποιονδήποτε χρήστη και με οποιαδήποτε εφαρμογή.

Ακρίβεια

Τα κελύφη ελέγχου πρόσβασης ανιχνεύουν όλα τα **Malware** που συμπεριφέρονται βάσει των κωδικοποιημένων προτύπων. **Malware** που δεν συμπεριφέρονται σύμφωνα με τα κωδικοποιημένα πρότυπα δεν είναι δυνατόν να ανιχνευθούν. Αν ένα **Malware** εισέλθει στο σύστημα και μολύνει κάποιο εκτελέσιμο, τότε μπορεί να μολύνει κατ’ επέκταση όλα τα αρχεία που επιτρέπεται στον ξενιστή του να τροποποιήσει. Αυτό σημαίνει ότι οι ιοί μακροεντολών διαδίδονται ελεύθερα, καθώς ο ιός εκτελείται πάντα μέσα από το πρόγραμμα που έχει το δικαίωμα να

τροποποιήσει τα σχετικά αρχεία δεδομένων. Επίσης, απαιτείται καλή ρύθμιση για να αποφευχθούν εσφαλμένες αναφορές ύπαρξης **Malware**: για παράδειγμα, αν για το πρόγραμμα **Winword** δεν περιληφθεί η ρύθμιση για τα αρχεία τύπου **".dot"**, ένα κέλυφος ελέγχου πρόσβασης θα ανέφερε **(**εσφαλμένα**)** την ύπαρξη **Malware**.

Ευχρηστία

Σε ένα περιβάλλον όπου οι χρήστες υποστηρίζονται από διαχειριστές, οι οποίοι αναλαμβάνουν την εγκατάσταση και τη ρύθμιση, οι χρήστες απλά δουλεύουν όπως πριν, ζητώντας επιπλέον προνόμια όταν το σύστημα τους αρνείται λειτουργίες. Για περιβάλλον **«**οικιακής χρήσης**»**, η τεχνική αυτή είναι ακατάλληλη διότι οι τεχνικές γνώσεις που απαιτούνται υπερβαίνουν κατά πολύ αυτές του μέσου χρήστη.

Διαχειριστική επιβάρυνση

Οι τεχνικές που βασίζονται στα κελύφη ελέγχου πρόσβασης απαιτούν σημαντική προσπάθεια από πλευράς διαχειριστών κατά την αρχική εγκατάσταση, καθώς απαιτείται να τεθούν όλοι οι κανόνες των επιτρεπτών ενεργειών. Υπολογίσιμο είναι επίσης το διαχειριστικό κόστος όταν αλλάζει το λογισμικό **(**εγκαθίσταται νέο ή τροποποιείται το υπάρχον**)** ή ακόμη και όταν αλλάζουν οι ρόλοι στο εταιρικό περιβάλλον **(**π.χ. αν ένας εργαζόμενος μεταπηδήσει από το λογιστήριο στη διοίκηση, οι επιτρεπτές γι' αυτόν ενέργειες θα είναι διαφορετικές, συνεπώς οι κανόνες πρέπει να αλλάξουν. Από την άλλη πλευρά, η ενημέρωση του ίδιου του λογισμικού είναι σπάνια απαραίτητη.

Επιβάρυνση συστήματος

Η επιβάρυνση που εισάγεται από τα κελύφη ελέγχου πρόσβασης είναι μικρή, προκειμένου για την επιβολή των πολιτικών. Αν, ωστόσο, είναι απαραίτητη η χρήση μηχανισμών κρυπτογράφησης, η επιβάρυνση είναι αρκετά μεγαλύτερη.

#### 3.5.3.5 Ευρεστική ανάλυση κώδικα

Η ευρεστική ανάλυση κώδικα **[103,137]** έχει ως στόχο να εντοπίζει την ύπαρξη **Malware** σε αντικείμενα του συστήματος μέσω στατικής ανάλυσης του περιεχομένου τους. Σε αντίθεση με την τεχνική εντοπισμού υπογραφών, η ευρεστική ανάλυση κώδικα δεν προσπαθεί να εντοπίσει συγκεκριμένες ακολουθίες από **bytes**, αλλά κώδικα που μοιάζει με **Malware**. Για παράδειγμα, ένα πρόγραμμα που έχει ως πρώτη εντολή του μία εντολή άλματος στο τέλος του αρχείου, όπου υπάρχει αυτοτροποποιούμενος κώδικας που καταλήγει με μία εντολή άλματος στην αρχή, είναι πιθανότατα μολυσμένο από **Malware**. Η τεχνικές αυτές καταλήγουν σε εντοπισμό πιθανώς μολυσμένων αρχείων, και για περαιτέρω ενδυνάμωση των συμπερασμάτων πολλές φορές συνδυάζονται με τεχνικές εντοπισμού υπογραφών.

Τα εργαλεία που βασίζονται στην ευρεστική ανάλυση κώδικα είναι συνήθως εύκολα στη χρήση, καθώς δεν απαιτούν ιδιαίτερες ρυθμίσεις, πλην της αρχικής εγκατάστασής τους. Έχουν τη δυνατότητα να ανιχνεύουν άγνωστους ή πολυμορφικούς ιούς, οι οποίοι εμπίπτουν στους ευρεστικούς κανόνες. Από την άλλη πλευρά μπορεί να μην εντοπίσουν όλα τα **Malware**, αν δεν περιγράφονται από τον κατάλληλο ευρεστικό κανόνα, ενδέχεται να αναφέρουν ανύπαρκτα **Malware (false positives)** αν κάποιο «νομότυπο» πρόγραμμα ταιριάζει με κάποιον από τους ευρεστικούς κανόνες του εργαλείου. Τέλος, η λειτουργία τους απαιτεί πολύ επεξεργαστική ισχύ, καθώς η ανάλυση του κώδικα είναι πιο επαχθής υπολογιστικά από την αναζήτηση ακολουθιών **bytes**.

#### 3.5.3.6 Εργαλεία καθαρισμού Malware

Τα εργαλεία καθαρισμού **Malware** έχουν ως στόχο να απομακρύνουν τα **Malware** από το σύστημα, πραγματοποιώντας τις αντίστροφες αλλαγές από αυτές που επέφερε αυτό. Για τη δημιουργία των εργαλείων καθαρισμού, οι κατασκευαστές λογισμικού αναλύουν τη δράση του **Malware** και αναπτύσσουν κατάλληλους αλγόριθμους αναίρεσης. Οι αλγόριθμοι αναίρεσης ενσωματώνονται ακολούθως στα εργαλεία, είτε μεμονωμένα, καταλήγοντας σε εργαλεία που καθαρίζουν έναν μόνο συγκεκριμένο **Malware** (κάτι που συνήθως συμβαίνει μετά από «επιδημίες» συγκεκριμένου **Malware**), είτε κατά ομάδες, οδηγώντας σε εργαλεία καθαρισμού πλειάδων **Malware**.

Βασικές προϋποθέσεις για να λειτουργήσει σωστά ένα εργαλείο καθαρισμού είναι οι ακόλουθες**[46]**:

**1.** οι αλλαγές πρέπει να είναι αντιστρέψιμες. Αν ένα **Malware** καταστρέφει αντικείμενα, επικαλύπτοντας το περιεχόμενό τους με άλλες ακολουθίες **bytes** χωρίς να αποθηκεύει κάπου το αρχικό περιεχόμενο, η αποκατάσταση της αρχικής μορφής του αντικειμένου δεν είναι εφικτή.

**2.** να προσδιορισθεί σωστά το **Malware** που έχει μολύνει το αντικείμενο, έτσι ώστε να εφαρμοσθεί ο σωστός αλγόριθμος αναίρεσης. Προβλήματα εδώ δημιουργούνται πολλές φορές όταν παραλλαγές του ίδιου **Malware** μοιάζουν μεν πολύ, αναφορικά με την αναγνώρισή τους, αλλά ο τρόπος που μολύνουν είναι αρκετά διαφορετικός ώστε να απαιτεί διαφορετικό πρόγραμμα αναίρεσης. Για παράδειγμα, οι παραλλαγές ιών **Jerusalem-DC** και **Jerusalem-E2** απαιτούσαν διαφορετικό πρόγραμμα καθαρισμού, αν και οι υπογραφές τους έμοιαζαν αρκετά για να «μπερδέψουν» τα περισσότερα προγράμματα προσδιορισμού ταυτότητας. Ο καθαρισμός των **Malware** είναι δύσκολος ή αδύνατος για πολλαπλές μολύνσεις, δηλαδή για περιπτώσεις όπου το ίδιο αντικείμενο έχει μολυνθεί διαδοχικά από περισσότερους του ενός **Malware**.

Επίσης, σε κάθε περίπτωση είναι προτιμότερη η αντικατάσταση του μολυσμένου αντικειμένου με ένα καθαρό, π.χ. από το **CD** διανομής του σχετικού λογισμικού.

## 3.6 Συστήματα Ανίχνευσης Εισβολών (Intrusion Detection Systems, IDSs)

Τα **IDS [6,38,76]** είναι **software** ή **hardware** συστήματα τα οποία αυτοματοποιούν τη διαδικασία παρακολούθησης όλων των **events** που συμβαίνουν σε ένα υπολογιστικό σύστημα ή σε ένα δίκτυο αναλύοντας τα σε βάθος για την ανακάλυψη τυχών προβλημάτων ασφαλείας. Εισβολές **(intrusions)**, προέρχονται είτε από επιτιθέμενους που έχουν πρόσβαση σε εσωτερικά συστήματα μέσω **internet**, είτε από εσωτερικούς χρήστες των συστημάτων που προσπαθούν να αποκτήσουν παραπάνω προνόμια από όσα έχουν, είτε από εσωτερικούς χρήστες που χρησιμοποιούν με λανθασμένο τρόπο τα προνόμια που τους έχουν δοθεί.

### 3.6.1 Λόγοι χρησιμοποίησης των IDS

Τα **IDS**, θεωρούνται πλέον απολύτως απαραίτητα στη δομή ασφαλείας ενός οργανισμού. Τέτοια συστήματα είναι αναγκαίο να υπάρχουν για τους παρακάτω λόγους**[6]**:

- Πρόληψη προβλημάτων. Τα συστήματα ανίχνευσης εισβολών συνεισφέρουν στην πρόληψη προβλημάτων κατά δύο τρόπους: αφ' ενός είναι πιθανόν να επισημάνουν τις προσπάθειες εισβολής σε ένα πρώιμο στάδιο, οπότε και θα ληφθούν τα κατάλληλα μέτρα για την αντιμετώπισή τους πριν γίνει κάποια σημαντική ζημιά. Αφ' ετέρου, γνωρίζοντας οι επίδοξοι εισβολείς ότι υφίσταται κάποιο τέτοιο σύστημα, ξέρουν ότι η πιθανότητα αποκάλυψης και τιμωρίας τους είναι σαφώς μεγαλύτερη, και κατά συνέπεια ενδέχεται να μην εκδηλώσουν συνολικά την επίθεσή τους.

- Ανίχνευση επιθέσεων και παραβιάσεων που δεν ανιχνεύονται με άλλα μέσα. Επί παραδείγματι, οι καταχρήσεις δικαιωμάτων από εσωτερικούς χρήστες δεν είναι δυνατόν να αντιμετωπισθούν με σχήματα διακρίβωσης ταυτότητας και ελέγχου πρόσβασης, διότι τα σχήματα αυτά δεν είναι σχεδιασμένα για να αντιμετωπίζουν τέτοιου είδους ζητήματα.

- Εντοπισμός και αντιμετώπιση προσπαθειών ανίχνευσης. Ένα τυπικό σχήμα επίθεσης σε πληροφοριακά συστήματα χωρίζεται σε τρεις φάσεις: αρχικά ανιχνεύεται το πληροφοριακό σύστημα για να διαπιστωθεί η διαμόρφωσή του και οι προσφερόμενες από αυτό υπηρεσίες. Στη συνέχεια, ανασύρονται από «βιβλιοθήκες» οι τεχνικές που είναι δυνατόν να χρησιμοποιηθούν για να παραβιαστεί η ασφάλεια του συστήματος και, τέλος, οι τεχνικές αυτές

χρησιμοποιούνται. Ενώ τα υπόλοιπα μέτρα ασφάλειας **(firewalls,** προγράμματα επιδιόρθωσης, έλεγχος πρόσβασης κ.ά.**)** εστιάζονται στην αντιμετώπιση της τελευταίας φάσης, τα συστήματα ανίχνευσης εισβολών μπορούν να ανιχνεύσουν τις προσπάθειες ανίχνευσης και να τις αναχαιτίσουν ή να ενημερώσουν σχετικά τους διαχειριστές για λήψη μέτρων. Η άμεση αντίδραση σε τέτοια ενδεχόμενα θωρακίζει το σύστημα και αποθαρρύνει τους επίδοξους εισβολείς.

- Τεκμηρίωση υπαρκτών απειλών. Τα συστήματα ανίχνευσης εισβολών μπορούν να αποδείξουν το γεγονός ότι ένα πληροφοριακό σύστημα αντιμετωπίζει απειλές, πριν κάποια από αυτές δημιουργήσει σημαντικές ζημιές. Μία τέτοια τεκμηρίωση είναι πολλαπλώς χρήσιμη, καθώς πείθει τη διοίκηση του οργανισμού-εταιρίας για κατανομή πόρων στα συστήματα ασφάλειας, βοηθά στον προσδιορισμό των μέτρων ασφάλειας που είναι πιο κατάλληλα για το σύστημα, καθώς η φύση των απειλών προσδιορίζει σε μεγάλο βαθμό και τα αντίμετρα που πρέπει να εφαρμοσθούν και βοηθά στην πιο αποτελεσματική κατανομή των πόρων ασφάλειας στα διάφορα τμήματα του πληροφοριακού συστήματος, ανάλογα με τις απειλές που το καθένα αντιμετωπίζει και την αξία του για τον οργανισμό.

- Έλεγχος ποιότητας για το σχεδιασμό ασφάλειας και τη διαχείριση. Τόσο το σχέδιο ασφάλειας του οργανισμού όσο και η υλοποίησή του από τους διαχειριστές ασφάλειας και συστημάτων είναι πιθανόν να παρουσιάζουν ατέλειες. Τα συστήματα ανίχνευσης εισβολών μπορούν να καταδείξουν τις ατέλειες, βοηθώντας έτσι στη διόρθωσή τους, πριν αυτές γίνουν αντικείμενο εκμετάλλευσης.

- Τα συστήματα ανίχνευσης εισβολών μπορούν να παράσχουν πληροφορίες για επιτυχείς επιθέσεις, συνεισφέροντας στην αποτίμηση του μεγέθους της ζημιάς, στη διαμόρφωση της λίστας ενεργειών για την ανάκαμψη και στον σχεδιασμό και εφαρμογή προληπτικών μέτρων για μελλοντική αποφυγή αντίστοιχων περιστατικών.

- Θωράκιση παλαιών συστημάτων. Σε αρκετές περιπτώσεις είναι απαραίτητη η διατήρηση σε λειτουργία παλαιών συστημάτων τα οποία δεν υποστηρίζονται πια από τους κατασκευαστές τους και που, ως εκ τούτου, είναι πιο ευάλωτα σε επιθέσεις. Τα πεπαλαιωμένα συστήματα μπορούν να προστατευθούν με τη χρήση συστημάτων ανίχνευσης εισβολών.

- Συμπλήρωση των διαδικασιών εγκατάστασης επιδιορθωτικών προγραμμάτων. Ακόμη και στην περίπτωση που τα συστήματα του οργανισμού υποστηρίζονται από τους κατασκευαστές και έτσι υπάρχουν τα σχετικά επιδιορθωτικά προγράμματα, η διαθεσιμότητα των προγραμμάτων αυτών δεν είναι

πάντα άμεση, ενώ για πολύπλοκα περιβάλλοντα η εγκατάστασή τους μπορεί να καθυστερεί για διάφορους λόγους.

- Αναγκαιότητα ύπαρξης ευπαθών υπηρεσιών. Μολονότι για μερικές υπηρεσίες είναι γνωστό ότι είναι επισφαλείς από την πλευρά της ασφάλειας, οι χρήστες ή η διοίκηση οργανισμών απαιτούν μερικές φορές τη διατήρησή τους διότι θεωρούνται πιο εύχρηστες και άρα πιο παραγωγικές. Τυπικό παράδειγμα είναι η υπηρεσία **FTP** που σαφώς είναι προβληματική καθώς διακινεί μη κρυπτογραφημένα συνθηματικά, ωστόσο το ασφαλέστερο αντίστοιχο, το ασφαλές πρωτόκολλο μεταφοράς αρχείων, είναι σημαντικά πιο δύσχρηστο. Τα συστήματα ανίχνευσης εισβολών μπορούν να ελέγχουν τις επισφαλείς υπηρεσίες, εντοπίζοντας περιστατικά όπου αυτές προξενούν αυξημένους κινδύνους.

- Αξιολόγηση των ενεργειών των χρηστών ή των διαχειριστών. Οι μηχανισμοί ασφάλειας που παρέχονται από το σύστημα είναι δυνατόν να μην χρησιμοποιούνται σωστά ή αποτελεσματικά από τους χρήστες και τους διαχειριστές. Το σύστημα ανίχνευσης εισβολών μπορεί να επισημαίνει τις σχετικές δυνατότητες βελτίωσης.

- Έλεγχος συνέπειας μεταξύ πολιτικής ασφάλειας και κανόνων πρόσβασης. Η πολιτική ασφάλειας που ισχύει στα πλαίσια του οργανισμού είναι δυνατόν να μην απεικονίζεται πιστά στους κανόνες πρόσβασης που έχουν θεσπίσει οι διαχειριστές . Μέσω αρχείων καταγραφών που τηρούνται από τα συστήματα ανίχνευσης εισβολών είναι δυνατόν να εντοπισθούν οι ασυνέπειες και να διορθωθούν.

### 3.6.2 Βασικοί τύποι IDS

Υπάρχουν διαφορετικοί τύποι **intrusion detection** συστημάτων, οι οποίοι χαρακτηρίζονται από διαφορετικούς τρόπους παρακολούθησης και ανάλυσης των **events**. Τα περισσότερα **IDS** περιγράφονται με βάση τα τρία θεμελιώδη λειτουργικά τμήματα, που είναι τα εξής**[6,76]**:

**Τμήμα παρακολούθησης της πληροφορίας**. Οι διαφορετικές πηγές πληροφορίας χρησιμοποιούνται για το αν τελικά έχει συμβεί μια επίθεση. Οι πηγές αυτές μπορεί να είναι είτε το δίκτυο, είτε ένας κόμβος είτε ακόμη μια εφαρμογή που τρέχει σε ένα σύστημα.

**Τμήμα ανάλυσης**. Το τμήμα αυτό ουσιαστικά συγκεντρώνει και οργανώνει τις πληροφορίες που προέρχονται από το προηγούμενο τμήμα, αποφασίζοντας αν οι επιθέσεις έχουν ήδη συμβεί ή αν δεν έχουν ολοκληρωθεί ακόμα.

**Τμήμα απάντησης**. Εδώ παίρνονται αποφάσεις σχετικά με τα μέτρα που θα πρέπει να ληφθούν σε περίπτωση παραβίασης του δικτύου. Τα μέτρα αυτά διαχωρίζονται

σε ενεργά και παθητικά μέτρα με τα πρώτα να συμπεριλαμβάνουν αυτοματοποιημένες αντιδράσεις εκ μέρους του συστήματος και τα δεύτερα να συμπεριλαμβάνουν κάποιες αναφορές έτσι ώστε ο υπεύθυνος ασφαλείας να έχει την δυνατότητα να ενεργήσει με βάση αυτές.

### 3.6.3 Αρχιτεκτονική των IDS

Το βασικά τμήματα που αποτελούν το **IDS** είναι πρώτον ο **Host,** δηλαδή το σύστημα όπου τρέχει το λογισμικό του **IDS** και δεύτερον ο **Target,** δηλαδή το σύστημα που το **IDS** παρακολουθεί για την ανακάλυψη προβλημάτων. Υπάρχουν δύο διαφορετικές προσεγγίσεις όσο αφορά τις αρχιτεκτονικές των **IDS.** Αυτές είναι οι εξής**[38]:**

- **Host-Target Co-location**

Παλαιότερα, τα περισσότερα συστήματα **intrusion detection** έτρεχαν στα ίδια τα υπό προστασία συστήματα. Η αρχιτεκτονική αυτή θεωρείται κάπως προβληματική από πλευράς ασφάλειας, αφού σε περίπτωση που ο επιτιθέμενος καταφέρει να εισβάλει στο **Target** σύστημα, αυτομάτως αποκτά τη δυνατότητα επέμβασης και στο ίδιο το **IDS.**

- **Host-Target Separation**

Η αρχιτεκτονική αυτή είναι πλέον διαδεδομένη στα συστήματα **intrusion detection.** Βασικό της χαρακτηριστικό είναι η τοποθέτηση σε διαφορετικά συστήματα του **Host** και του **Target** έτσι ώστε να παραμείνει κρυφό το **IDS** από τους επιτιθέμενους.

### 3.6.4 Σκοπός των IDS

Δύο είναι οι βασικοί σκοποί των συστημάτων **intrusion detection[38,76]:**

**1)** Ανακάλυψη των στοιχείων του επιτιθέμενου **(Accountability)**

Η φράση που χαρακτηρίζει το σκοπό αυτόν είναι: **"**Θεωρούμαι ικανός να αντιμετωπίσω περιστατικά παραβίασης της ασφάλειας του δικτύου όσο γνωρίζω ποιος είναι ο υπεύθυνος για τα περιστατικά αυτά**".** Η ανακάλυψη των στοιχείων του επιτιθέμενου είναι αρκετά δύσκολη υπόθεση στις περιπτώσεις των δικτύων **TCP/IP,** όπου οι επιτιθέμενοι μπορούν να τροποποιήσουν την πραγματική διεύθυνση προέλευσης των πακέτων που στέλνουν στο δίκτυο. Γενικά θεωρείται δύσκολο να επιτευχθεί αυτός ο σκοπός όταν δεν υπάρχουν μηχανισμοί πιστοποίησης και αναγνώρισης των χρηστών.

**2) Response**

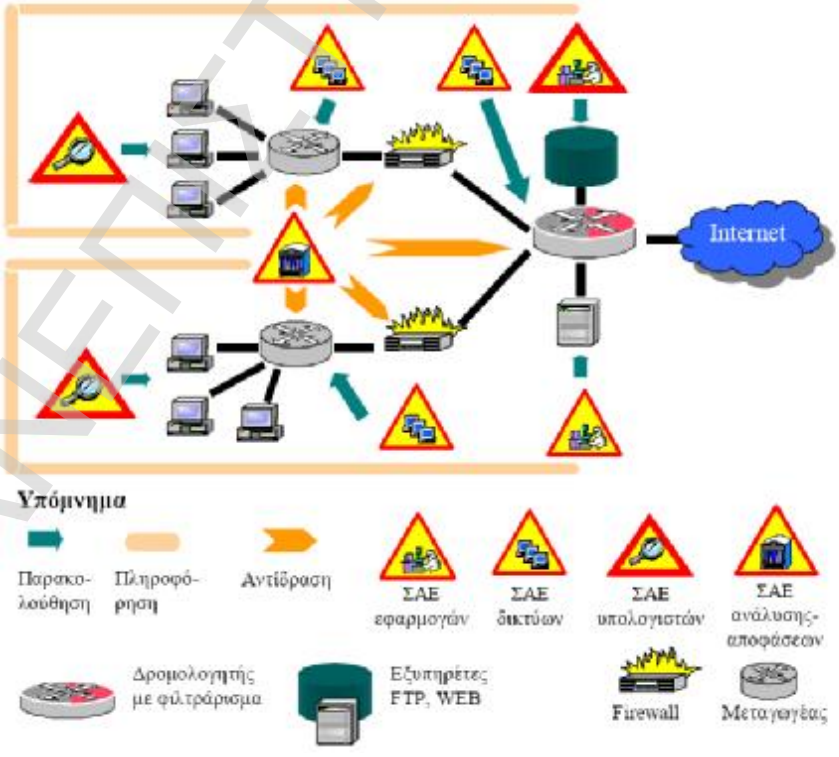
Με την έννοια **response** εννοούμε την ικανότητα αναγνώρισης ενός **event** ως δείγμα επίθεσης προς το εσωτερικό δίκτυο και την άμεση αντίδραση των συστημάτων έτσι ώστε να ελαχιστοποιηθεί ο κίνδυνος εμφάνισης νέων προβλημάτων. Η χαρακτηριστική φράση που συνδέεται με αυτόν τον σκοπό είναι η εξής: **"** Δεν μας ενδιαφέρει η προέλευση της επίθεσης από την στιγμή που υπάρχει η δυνατότητα αναγνώρισης και μπλοκαρίσματος της**."**

### 3.6.5 Στρατηγικές ελέγχου

Οι στρατηγικές που ακολουθούν περιγράφουν τον τρόπο διαχείρισης των τμημάτων του **IDS** καθώς επίσης και τον τρόπο διαχείρισης της πληροφορίας που παράγεται. Οι στρατηγικές αυτές είναι**[76]:**

- Ø Συγκεντρωτική
- Ø Εν μέρη κατανεμημένη
- Ø Πλήρως κατανεμημένη
- Ø Συγκεντρωτική

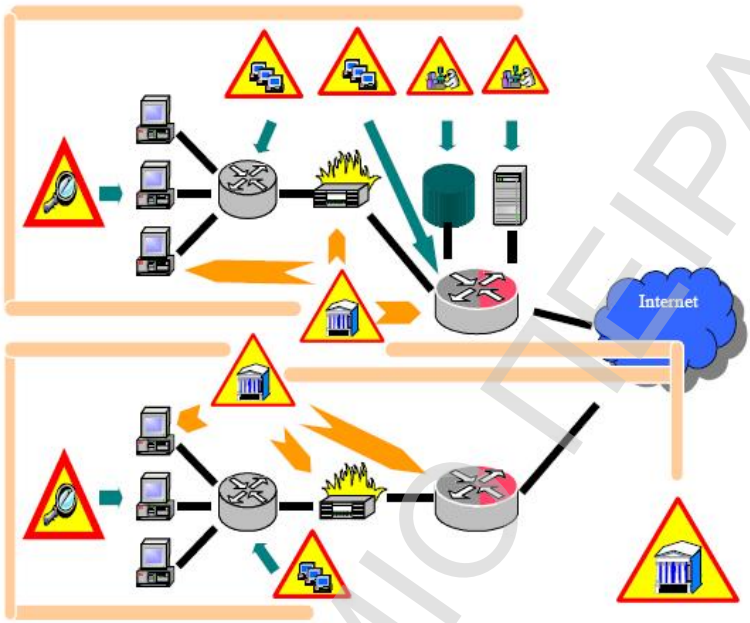
Σύμφωνα με τη στρατηγική αυτή, όλα τα τμήματα παρακολούθησης, ανακάλυψης και αναφοράς της κατάστασης ελέγχονται από μια κεντρική τοποθεσία. Παρακάτω φαίνεται σχηματικά η στρατηγική αυτή **(**Σχήμα **26).**




**Σχήμα 26. Συγκεντρωτική Στρατηγική Ελέγχου**

Ø Εν μέρη κατανεμημένη

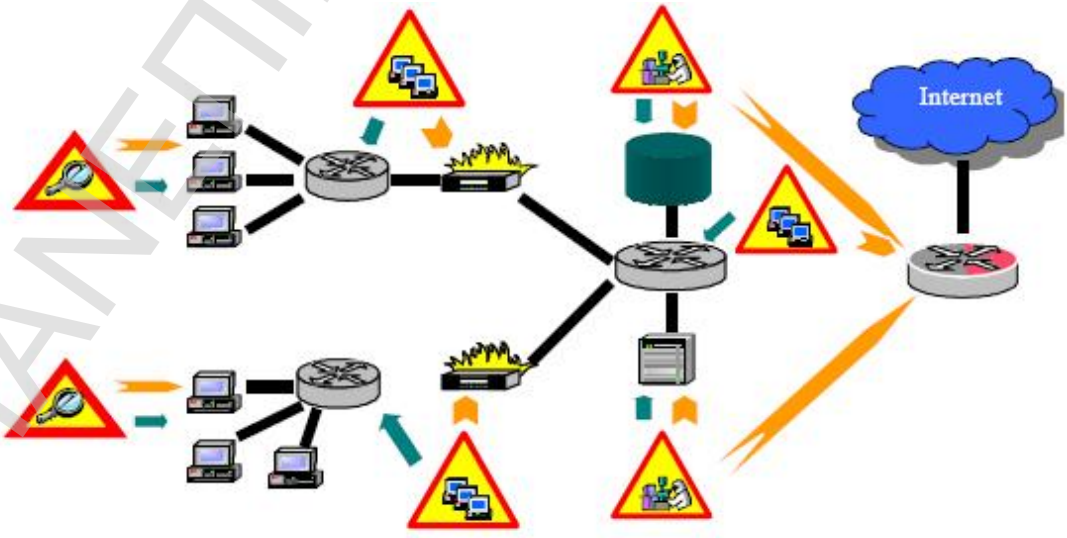
Εδώ, οι διαδικασίες της παρακολούθησης και της ανίχνευσης προβλημάτων γίνεται από ένα τοπικό κόμβο ελέγχου, με ιεραρχικές αναφορές σε μία ή περισσότερες κεντρικές τοποθεσίες (Σχήμα **27**).




**Σχήμα 27. Εν Μέρη Κατανεμημένη Στρατηγική Ελέγχου**

Ø Πλήρως κατανεμημένη

Σε αυτήν την περίπτωση οι διαδικασίες παρακολούθησης και ανίχνευσης προβλημάτων πραγματοποιούνται μέσω αντιπροσώπων **(agents),** όπου οι αποφάσεις για τις νέες κινήσεις που θα γίνουν παίρνονται στο σημείο όπου έγινε και η ανάλυση. Σχηματικά φαίνεται παρακάτω η στρατηγική αυτή (Σχήμα **28**):




**Σχήμα 28. Πλήρως Κατανεμημένη Στρατηγική Ελέγχου**

### 3.6.5.1 Ανάλυση των τμημάτων ενός IDS

**1)** Τμήμα παρακολούθησης της πληροφορίας

Κάποια **IDS** έχουν την ικανότητα ανάλυσης των πακέτων που μετακινούνται από και προς το εσωτερικό δίκτυο ενός οργανισμού ενώ κάποια άλλα έχουν τη δυνατότητα ανάλυσης πληροφοριών που προέρχονται από λειτουργικά συστήματα ή από εφαρμογές που τρέχουν σε αυτά.

Έτσι τα **IDSs** διακρίνονται σε**[38,76]:**

- **Network-Based IDSs**
- **Host-Based IDSs**
- **Application-Based IDSs**

**Network-Based IDSs**

Αυτού του είδους τα **IDSs** αποτελούν και την πλειοψηφία αυτών των συστημάτων. Βασική τους λειτουργία είναι η σύλληψη και ανάλυση πακέτων που κινούνται σε ένα δίκτυο με σκοπό την ανίχνευση επιθέσεων. Τα **Network-Based IDSs [38]** συχνά αποτελούνται από **«**αισθητήρες**»** που είναι τοποθετημένοι σε διάφορα σημεία του δικτύου. Οι αισθητήρες αυτοί παρακολουθούν την κίνηση στο δίκτυο, πραγματοποιούν ανάλυση αυτής και τέλος στέλνουν σε μια κεντρική κονσόλα αναφορές για τυχών επιθέσεις.

Τα πλεονεκτήματα των **Network-Based IDSs** είναι ότι αρκούν λίγα, κατάλληλα τοποθετημένα, για την παρακολούθησης ενός αρκετά μεγάλου δικτύου. Επίσης η χρήση των **Network-Based IDSs** δεν επιβαρύνει τη λειτουργία του δικτύου αφού συνήθως οι συσκευές αυτές έχουν παθητικό ρόλο στο δίκτυο, ενώ επιπρόσθετα εχουν την ικανότητα να αποκρύψουν την ταυτότητα τους, και να μην γίνονται αντιληπτά στους επιτιθέμενους.

Στα μειονεκτήματα των **Network-Based IDSs** συγκαταλέγονται ότι εμφανίζουν προβλήματα σε περιόδους υψηλή δικτυακής κίνησης καθώς επίσης ότι δεν έχουν τη δυνατότητα ανάλυσης κρυπτογραφημένης πληροφορίας. Το πρόβλημα αυτό γίνεται ακόμη πιο έντονο σε οργανισμούς που κάνουν χρήση των ιδεατών ιδιωτικών δικτύων. Ένα ακόμα μειονέκτημα είναι ότι τα περισσότερα **Network-Based IDSs** δεν είναι σε θέση να πουν εάν μια επίθεση ήταν επιτυχημένη. Έχουν τη δυνατότητα να διακρίνουν μόνο εάν μια επίθεση έχει αρχικοποιηθεί. Στη συνέχεια είναι εργασία του υπεύθυνου ασφαλείας να ερευνήσει εάν με την επίθεση αυτή έχουν παραβιαστεί τα εσωτερικά συστήματα.

- **Host-Based IDSs**

Η λειτουργία των **Host-Based IDS** στηρίζεται στη συλλογή πληροφοριών μέσα από κάθε υπολογιστικό σύστημα. Η ικανότητα αυτή επιτρέπει την ακριβέστερη ανάλυση πληροφοριών καθώς προσδιορίζονται ακριβώς ποιες διαδικασίες και ποιοι χρήστες συμμετέχουν σε μια επίθεση. Επιπλέον τα **Host-Based IDSs** μπορούν να διακρίνουν και το αποτέλεσμα μιας επίθεσης και ακόμη μπορούν να έχουν άμεση εικόνα των **data files** και των διαδικασιών του συστήματος που έχουν **«**χτυπηθεί**»**. Συνήθως τα **Host-Based IDSs [76]** κάνουν χρήση των **audit trails** του λειτουργικού συστήματος καθώς και των **systems logs.** Τα **audit trails** του λειτουργικού συστήματος γεννιούνται στο εσωτερικό τμήμα **(**τον πυρήνα**)** του λειτουργικού συστήματος και είναι αναλυτικότερα από τα **logs** αρχεία. Που θεωρούνται ευκολότερα στη κατανόηση τους.

Το πλεονεκτήματα των **Host-Based IDSs** είναι ότι από τη στιγμή που έχουν τη δυνατότητα παρακολούθησης των **events** σε κάθε **host,** μπορούν και ανιχνεύουν επιθέσεις που δεν ανακαλύπτονται από τα **network-based IDSs.** Επίσης μπορούν και λειτουργούν σε περιβάλλοντα όπου συμβαίνει κρυπτογράφηση της δικτυακής κίνησης**,** αφού συλλέγουν πληροφορίες είτε πριν την κρυπτογράφηση είτε μετά τη αποκρυπτογράφηση. Τέλος εχουν τη δυνατότητα ανίχνευσης **trojan horses** καθώς επίσης και επιθέσεων που αφορούν σφάλματα λογισμικού.

Στα μειονεκτήματά τους συγκαταλέγονται**,** ο δυσκολότερος τρόπος διαχείρισης αφού κάθε σύστημα απαιτεί διαφορετικό τρόπο ρύθμισης**,** ότι σε περίπτωση που ο επιτιθέμενος αποκτήσει πρόσβαση σε σύστημα που τρέχει ένα **Host-Based IDS,** αυτομάτως μπορεί και να το εξουδετερώσει. Επίσης ότι δυσκολεύονται στην ανίχνευση επιθέσεων που αφορούν ολόκληρο το δίκτυο όπως **networks scans,** ενώ τέλος ότι είναι ευάλωτα σε **DoS** επιθέσεις αφού η χρήση **Host-Based IDSs** έχει ως αποτέλεσμα την μείωση της απόδοσης του συστήματος.

- **Application-Based IDSs**

Τα **Application-Based IDSs** αποτελούν υποσύνολο των **host-based IDSs** και έργο τους είναι η ανάλυση των πληροφοριών και των **events** που παράγονται από εφαρμογές λογισμικού. Η πιο συνηθισμένες πηγές που χρησιμοποιούν τα **Application-Based IDSs [76]** είναι τα **logs** αρχεία. Η ικανότητα της σε βάθος ανάλυσης των εφαρμογών επιτρέπει στην ανίχνευση ύποπτων συμπεριφορών που αφορούν χρήστες που επιζητούν περισσότερα προνόμια από όσα τους έχουν δοθεί.

Στα πλεονεκτήματα των **Application-Based IDSs** συγκαταλέγεται η δυνατότητα παρακολούθησης αλληλεπίδρασης του χρήστη με μια συγκεκριμένη εφαρμογή

καθώς και ότι έχουν και αυτά την ικανότητα να λειτουργούν σε περιβάλλοντα όπου γίνεται χρήση κρυπτογραφημένης πληροφορίας.

Στα μειονεκτήματα τους συγκαταλέγεται ότι τα συστήματα αυτά είναι περισσότερο ευάλωτα από τα **host-based IDS** αφού τα **logs** αρχεία που χρησιμοποιούν εκτίθενται σε μεγαλύτερο βαθμό από τα **audit trails.** Επειδή τα **Application-Based IDSs** συχνά παρακολουθούν και συλλέγουν πληροφορίες σε επίπεδο χρήστη, δεν έχουν τη δυνατότητα να ανιχνεύσουν για παράδειγμα επιθέσεις που αφορούν προβλήματα σε λογισμικό. Για το λόγο αυτό συνίσταται να χρησιμοποιούνται παράλληλα με **host-bases IDS** και τα **network-based IDS.**

**2)** Τμήμα Ανάλυσης

Υπάρχουν δύο βασικές τεχνικές ανάλυσης της πληροφορίας και των **events** που παράγονται από το τμήμα παρακολούθησης. Αυτές είναι οι εξής:

- **Misuse Detection**
- **Anomaly Detection**

o **Misuse Detection.**

Σύμφωνα με αυτήν την τεχνική **[38],** ένα σύστημα **intrusion detection** έχει αποθηκεύσει ένα σύνολο από **events** που συνθέτουν διαφορετικούς τύπους επιθέσεων και ψάχνει για **events** τα οποία ταιριάζουν με την αποθηκευμένη πληροφορία. Η ανίχνευση τέτοιων **events** αποδεικνύει και την ύπαρξη κάποιας επίθεσης.

Πλεονεκτήματα

**Ø** Οι ανιχνευτές αυτού του είδους είναι ικανοί να ανιχνεύουν πραγματικές επιθέσεις χωρίς να παράγουν λανθασμένες εκτιμήσεις και προειδοποιήσεις.

**Ø** Υπάρχει δυνατότητα διάγνωσης των λεπτομερειών της επίθεσης καθώς επίσης και της τεχνικής που χρησιμοποίησε ο επιτιθέμενος.

**Ø** Επιτρέπουν σε κάποιον που δεν είναι ειδικός σε θέματα ασφαλείας να αναγνωρίσει μια επίθεση.

Μειονεκτήματα

**Ø** Δυνατότητα ανίχνευσης μόνο εκείνων των επιθέσεων που έχουν δηλωθεί αρχικά στο **IDS.** Για το λόγο αυτό είναι απαραίτητη συνεχή ενημέρωση αυτών με τις υπογραφές των καινούριων επιθέσεων.

Ø Συχνά τέτοιου τύπου **IDS** έχουν σχεδιαστεί έτσι ώστε να μπορούν να ανιχνεύσουν αρκετά σύνθετες επιθέσεις, και δεν είναι σε θέση να ανιχνεύσουν πολύ απλές επιθέσεις.

- **Anomaly Detection**

Η τεχνική αυτή στηρίζεται σε ανιχνευτές που αναγνωρίζουν συμπεριφορές και καταστάσεις διαφορετικές των συνηθισμένων σε ένα **host** ή μέσα σε ένα δίκτυο. Οι ανιχνευτές αυτοί **(anomaly detectors) [6]** δημιουργούν ένα προφίλ των χρηστών, των εσωτερικών συστημάτων και των δικτυακών συνδέσεων και δρουν σύμφωνα με αυτό. Τα προφίλ συνθέτονται από δεδομένα που έχουν συγκεντρωθεί σε καταστάσεις ομαλής και κανονικής λειτουργίας ανά τακτά χρονικά διαστήματα.

Τα μέτρα και οι τεχνικές που χρησιμοποιούνται συμπεριλαμβάνουν:

Ø Ανίχνευση του κατωφλιού **(Threshold)**, όπου υπάρχει ένα όριο που η τιμή του καθορίζεται από κάποια χαρακτηριστικά των χρηστών και συστημάτων σε ομαλές καταστάσεις. Εάν αυτό το όριο ξεπεραστεί τότε θεωρείται πως έχει προκύψει πρόβλημα. Για παράδειγμα το ποσοστό της **CPU** που καταναλώνει μια διαδικασία, ο αριθμός των εσφαλμένων προσπαθειών **login** ενός χρήστη στο σύστημα ή ακόμη και ο αριθμός των αρχείων που ένας χρήστης επισκέπτεται σε ένα χρονικό διάστημα, διαμορφώνουν το όριο αυτό.

Ø Μέτρα βασισμένα σε κανόνες, όπου διαμορφώνονται κανόνες οι οποίοι καθορίζουν και τη συμπεριφορά των χρηστών αλλά και τη δικτυακή κατάσταση.

Δυστυχώς οι **anomaly** ανιχνευτές παράγουν ένα μεγάλο αριθμό προειδοποιήσεων που δεν αντιστοιχούν σε πραγματικές επιθέσεις.

Πλεονεκτήματα

Ø Δυνατότητα ανίχνευσης ακόμη και νέων, άγνωστων επιθέσεων αφού αρκεί να καταγράψουν μια μη φυσιολογική συμπεριφορά για να παράγουν μηνύματα κινδύνου.

Ø Οι **anomaly** ανιχνευτές μπορούν να παράγουν πληροφορίες που να χρησιμοποιηθούν για τον προσδιορισμό νέων υπογραφών επιθέσεων από τους **misuse** ανιχνευτές. Για παράδειγμα, η τιμή ενός ορίου μπορεί να χρησιμοποιηθεί από έναν **misuse** ανιχνευτή για την δημιουργία ενός ακόμη περιστατικού επίθεσης με τον ακόλουθο τρόπο: "εάν ο αριθμός των αρχείων που μπορεί να επισκεφθεί ένας χρήστης αυξηθεί **10%** σε σχέση με την τιμή του ορίου, τότε στείλε σήμα κινδύνου".

Μειονεκτήματα

**Ø** Συχνά παράγονται μηνύματα κινδύνου χωρίς να υπάρχει πραγματικός κίνδυνος ασφαλείας.

**Ø** Δυσκολία στον καθορισμό της φυσιολογικής συμπεριφοράς των συστημάτων και του δικτύου και συνεπώς των τιμών των ορίων.

**3)** Τμήμα Απάντησης

Μετά την συλλογή πληροφοριών και την ανάλυση τους για την ανίχνευση τυχών επιθέσεων, ένα σύστημα **intrusion detection** σχεδιάζει τα μέτρα που θα λάβει και ειδικότερα την απάντηση που θα δώσει στις διαφαινόμενες επιθέσεις. Τα εμπορικά **IDS** υποστηρίζουν πολλούς τρόπους απάντησης όπως ενεργές απαντήσεις, παθητικές απαντήσεις αλλά και συνδυασμούς των παραπάνω δύο τρόπων.

Ενεργές Απαντήσεις **(Active Responses)**

Οι ενεργές απαντήσεις αποτελούν αυτοματοποιημένες δράσεις των **IDSs** σε περίπτωση ανίχνευσης επίθεσης. Υπάρχουν τρεις κατηγορίες ενεργών απαντήσεων από τη πλευρά των **IDSs [6].**

**a)** Συγκέντρωση επιπλέον πληροφοριών

Η πιο παραγωγική αντίδραση σε περίπτωση επίθεσης είναι η συλλογή επιπλέον πληροφοριών για την ίδια την επίθεση. Αυτό μπορεί να σημαίνει για παράδειγμα, αύξηση του επιπέδου της παρακολούθησης**(**παρακολούθηση μεγαλύτερου αριθμού **events**, ανάλυση όλων των πακέτων που μετακινούνται στο δίκτυο**)**, έτσι ώστε να συγκεντρωθούν όλα τα στοιχεία που μπορεί να οδηγήσουν στα ίχνη του επιτιθέμενου και των χαρακτηριστικών της επίθεσης.

**b)** Αλλαγή περιβάλλοντος

Ένας άλλος τρόπος ενεργής αντίδρασης του **IDS** είναι ο τερματισμός της επίθεσης και το **«**μπλοκάρισμα**»** του επιτιθέμενου απαγορεύοντας του την πρόσβαση στο σύστημα ή στην διαδικασία. Γενικά είναι αρκετά δύσκολο να **«**μπλοκάρεις**»** τον επιτιθέμενο, αλλά τα **IDSs** έχουν τη δυνατότητα να αποτρέψουν κάποιον εισβολέα λαμβάνοντας τα απαραίτητα μέτρα.

**c)** Κινήσεις αντιμετώπισης του εισβολέα

Ο τρόπος αυτός συμπεριλαμβάνει ενέργειες όπως επιθέσεις στο **site** του επιτιθέμενου, που στοχεύουν στην ανακάλυψη του. Οι αντιδράσεις αυτές πρέπει να είναι πολύ προσεχτικές διότι δεν είναι γνωστό αν ο επιτιθέμενος χρησιμοποιεί ως βάση του ένα άλλο νόμιμο **site.** Υπάρχουν περιπτώσεις που έχουν κατηγορηθεί οργανισμοί για τέτοιες ενέργειες.

Παθητικές Απαντήσεις **(Passive Responses)**

Παθητικές απαντήσεις των συστημάτων **intrusion detection** θεωρούνται όλες εκείνες οι πληροφορίες που παρέχουν στους διαχειριστές συστημάτων και στους χρήστες έτσι ώστε οι τελευταίοι να δράσουν στηριζόμενοι σε αυτές τις πληροφορίες. Τα είδη των πληροφορικών που παράγοντα φαίνονται παρακάτω **[6]:**

**a) Alarms and Notifications**

**Alarms** και **Notification** παράγονται από τα **IDSs** για να ενημερώσουν τους χρήστες για τυχών επιθέσεις που έχουν ανιχνευτεί. Οι πληροφορίες αυτές στέλνονται στην κονσόλα του **IDS** καθώς επίσης και σε όποια μηχανήματα έχουν ρυθμιστεί να δέχονται τέτοιου είδους πληροφορίες. Γενικά οι πληροφορίες δίνουν στοιχεία για τα χαρακτηριστικά μιας εισβολής, συμπεριλαμβανομένων των διευθύνσεων προέλευσης του επιτιθέμενου και του στόχου του, των εργαλείων που χρησιμοποιήθηκαν και τέλος των αποτελεσμάτων αυτής της επίθεσης.

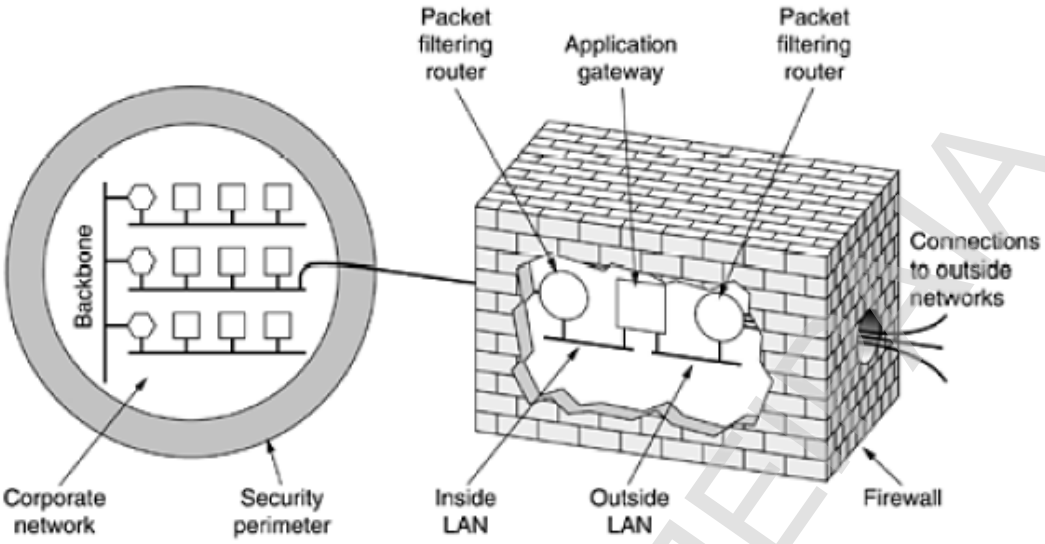
**b) SNMP Traps** και **Plug-ins**

Κάποια **IDSs** έχουν σχεδιαστεί με τέτοιο τρόπο ώστε να αναφέρουν πληροφορίες όπως οι παραπάνω σε συστήματα διαχείρισης στέλνοντας **SNMP Traps.** Η δυνατότητα αυτή έχει αρκετά πλεονεκτήματα αφού παρέχει μια συνολική εικόνα του δικτύου, και επιτρέπει τις άμεσες ρυθμίσεις όποτε χρειαστεί.

## 3.7 Firewalls

Όπως είναι γνωστό η σύνδεση ενός συστήματος στο διαδίκτυο δίνει την δυνατότητα πλήρους αμφίδρομης επικοινωνίας με αυτό. Η δυνατότητα αυτή δεν είναι πάντα επιθυμητή αφού εμπιστευτικές λεπτομέρειες που βρίσκονται στα συστήματα ενός οργανισμού μπορούν να διαρρεύσουν.

Για να υπάρξει ένα είδος διαχωρισμού ανάμεσα στο **Intranet** του οργανισμού και το **Internet,** υπάρχει μια ομάδα συστημάτων που δημιουργεί έναν τοίχο ασφαλείας ανάμεσα στα **2** δίκτυα. Η χρήση τους βέβαια βοηθά την ενίσχυση της ασφάλειας **,** αλλά δεν την εγγυάται. Ο σωστός σχεδιασμός της περιμέτρου και της διαμόρφωσης των συστημάτων είναι απαραίτητος για την σωστή λειτουργία τους **(**Σχήμα **29).**




**Σχήμα 29. Δομή ένα firewall**

Ένα **firewall [18,49,86]** μπορεί να μας προσφέρει **:**

- Ένα σημείο εφαρμογής των αποφάσεων που αφορούν την ασφάλεια
- Ένα μέσο για την εφαρμογή της πολιτικής ασφάλειας
- Ένα τρόπο καταγραφής της δικτυακής κίνησης
- Ένα φράγμα σε ανεπιθύμητες επιθέσεις

Αντίθετα ένα **firewall** δεν μπορεί να μας προστατέψει από **:**

- Εσωτερικούς χρήστες που σκοπεύουν να επιτεθούν
- Συνδέσεις που δεν περνούν από αυτό
- Εντελώς νέους τύπους απειλών-επιθέσεων
- Ιούς,αποδοτικά
- Λάθη στην διαμόρφωση

Παρόλα αυτά μπορούμε να έχουμε μεγαλύτερη απόλυτη ασφάλεια στο δίκτυο με τη χρήση **firewalls .** Όταν μιλάμε για ασφάλεια θα πρέπει να λάβουμε υπόψη μας το κόστος που απαιτείται για την προστασία **,** το βαθμό πολυπλοκότητας του συστήματος μας καθώς και την ευκολία στην χρήση**.** Το **firewall** αλληλεπιδρά με το **internet** και χρειάζεται ιδιαίτερη προσοχή στην εγκατάσταση του και στην σωστή διαμορφωσή του**.**

**Firewall** λοιπόν είναι ένας μηχανισμός **[28]** που χρησιμοποιείται για να ελέγχει την πρόσβαση από και προς το δίκτυο με απώτερο σκοπό την προστασία του δικτύου**.** Ένα **firewall** λειτουργεί σαν μια πύλη από την οποία περνάει όλη η κίνηση από και

προς το εξωτερικό δίκτυο . Με την χρήση ενός **Firewall** περιορίζεται η επικοινωνία ανάμεσα στο προστατευόμενο δίκτυο και ένα οποιοδήποτε άλλο δίκτυο.

Γενικά ένα **firewall** θα μπορούσαμε να το παρομοιάσουμε με έναν τοίχο ανάμεσα στο εσωτερικό δίκτυο και ένα εξωτερικό δίκτυο **(**πχ Διαδίκτυο**).**Το βασικό χαρακτηριστικό αυτού του τοίχου είναι να βρεθούν οι δρόμοι – πύλες από τους οποίους θα μπορεί να περάσει συγκεκριμένη πληροφορία. Το πιο δύσκολο κομμάτι στην υλοποίηση του **firewall** είναι η εύρεση των κριτηρίων που θα προσδιορίζουν ποια πακέτα επιτρέπεται και ποια όχι να περάσουν στο εσωτερικό δίκτυο.

Ένα **firewall** μπορεί να είναι ένας συνδυασμός δρομολογητών **(routers),** Υποδικτύων **(network segments)** και υπολογιστών που έχουν ρόλο **host .**

### 3.7.1 Τρόπος λειτουργίας

Η λειτουργία των **firewall** μπορεί να είναι ένα ή περισσότερα από τα ακόλουθα **[28]: Packet-filtering router , Application-level gateway**

- Δρομολογητές φιλτραρίσματος πακέτων **( Packet-Filtering Routers)**

Ένας δρομολογητής κινεί δεδομένα από και προς ένα ή περισσότερα δίκτυα**,** παίρνοντας ένα πακέτο από ένα δίκτυο «Α» και δρομολογώντας το προς ένα δίκτυο **«**Β**» .** Ένας δρομολογητής φιλτραρίσματος κάνει ακριβώς το ίδιο με ένα απλό δρομολογητή **,** επιπλέον όμως αποφασίζει για το αν θα δρομολογήσει ή όχι το πακέτο αυτό. Αυτό επιτυγχάνεται με την εγκατάσταση κάποιων φίλτρων βάση των οποίων ο δρομολογητής αποφασίζει για το τι θα κάνει με οποιοδήποτε πακέτο φτάνει σε αυτόν.

Σημαντικό είναι ακόμη το αν ο δρομολογητής επαναπροσδιορίζει τις εντολές φιλτραρίσματος και αν είναι δυνατή η εφαρμογή φίλτρων για εισερχόμενα ή εξερχόμενα πακέτα σε κάθε διεπαφή. Ένα άλλο σημαντικό θέμα είναι η ικανότητα ανάπτυξης φίλτρων που βασίζονται σε επιλογές του **IP header** και στον τεμαχισμό των πακέτων. Η κατασκευή ενός καλού φίλτρου είναι πολύ δύσκολη και απαιτείται η πλήρης κατανόηση των πρωτοκόλλων που θέλουμε να φιλτράρουμε. Ο δρομολογητής εξετάζει κάθε **datagram** για να αποφασίσει αν ταιριάζει με κάποιον από τους κανόνες φιλτραρίσματος των πακέτων. Οι πληροφορίες είναι η IP αποστολέα **,** η IP παραλήπτη **,** το πρωτόκολλο **( TCP, UDP,ICMP,** ή **IPTunnel) ,** το **TCP/UDP port** προέλευσης **,** το **TCP/UDP port** προορισμού κ.ά.

Τα πλεονεκτήματα του τύπου αυτού είναι το μικρό κόστος υλοποίησης και είναι διάφανο στους χρήστες και στις εφαρμογές. Στα μειονεκτήματα πρέπει να υπολογίσουμε την δυσκολία εξακρίβωσης της ορθότητας των κανόνων φιλτραρίσματος. Για πολύπλοκες εγκαταστάσεις η απόδοση του συστήματος πέφτει

όσο αυξάνουν οι κανόνες φιλτραρίσματος. Τέλος η εγκατάσταση αυτού του είδους δεν είναι σε θέση να πάρει αποφάσεις σε σχέση με την εφαρμογή ή το περιεχόμενο των δεδομένων.

- Πύλες Εφαρμογών **(Application-level gateways)**

Οι πύλες εφαρμογών επιτρέπουν στον διαχειριστή , να υλοποιήσει μια αυστηρότερη πολιτική ασφαλείας . Στο σύστημα εγκαθίστανται **proxies** των εφαρμογών που επιτρέπουν την προσπέλαση σε εξωτερικούς χρήστες μόνο μέσα από αυτές , ενώ κάθε άλλη χρήση αποτρέπεται από το **firewall** . Οι χρήστες επιτρέπεται να προσπελαύνουν τις υπηρεσίες του **gateway** αλλά δεν επιτρέπεται να κάνουν **Login** σε αυτόν . Για να φτάσει κάποιο πακέτο στο δευτερεύον δίκτυο θα πρέπει να περάσει από το **bastion host [14] (** υπολογιστής γενικου σκοπού**).** Έτσι περιορίζεται ο αριθμός των άμεσα προσπελάσιμων κόμβων των δικτύων με αποτέλεσμα να επιτυγχάνεται περισσότερη ασφάλεια.

Οι **proxy servers** χρησιμοποιούνται προκειμένου να έχουμε πρόσβαση στα δεδομένα με ασφαλή τρόπο. Με την χρήση τους είναι δυνατή η προσθήκη μιας λίστας ελέγχου προσπέλασης **( access control list )** για τις διάφορες υπηρεσίες , απαιτώντας από τους χρήστες και τα συστήματα κάποια μορφή πιστοποίησης προτού τους επιτραπεί πρόσβαση σε κάποια από τις υπηρεσίες. Επίσης , οι **proxy servers** μπορούν να διαμορφωθούν με τέτοιο τρόπο ώστε να κωδικοποιούνται οι ροές των δεδομένων με βάση διάφορες παραμέτρους. Τέτοιες δυνατότητες μπορούν να χρησιμοποιηθούν από οργανισμούς για να πετύχουν ασφαλή διασύνδεση των **sites** τους μέσω του Διαδικτύου.

Τα πλεονεκτήματα αυτού του τρόπου είναι η μεγαλύτερη ασφάλεια αφού αυτά τα συστήματα «τρέχουν» μειωμένο σετ εφαρμογών και ένα ασφαλές λειτουργικό σύστημα .Η προσπέλαση στα εσωτερικά συστήματα γίνεται μόνο απο τον **proxy** εμποδίζοντας έτσι την απευθείας σύνδεση . Οι κανόνες φιλτραρίσματος είναι αρκετά πιο εύκολοι να υλοποιηθούν και να εξακριβωθούν για την ορθότητα τους . Το μεγαλύτερο μειονέκτημα είναι πως πρέπει οι χρήστες να αλλάξουν την συμπεριφορά τους ή να στηθεί εξειδικευμένο λογισμικό που θα δίνει ευελιξία στους εσωτερικούς χρήστες χωρίς να μειώνεται η προσφερόμενη ασφάλεια.

- Υβριδικά συστήματα

Ο συνδυασμός των δυο **[28]** παραπάνω περιπτώσεων οδηγεί σε καλύτερα αποτελέσματα και συνήθως η υλοποίηση περιλαμβάνει και **packet filtering** και **proxy applications.** Το καλύτερο **firewall** σε ένα δίκτυο επιτυγχάνεται με το συνδυασμό **2 screening routers** με ένα ή περισσότερους **proxy servers** που τοποθετούνται ανάμεσα στους **2 routers** . Ο εξωτερικός **router** εμποδίζει την μη

εξουσιοδοτημένη πρόσβαση σε επίπεδο IP ενώ επιτρέπει στον **proxy server** να παρέχει ασφάλεια στα πρωτόκολλα υψηλότερων επιπέδων**.** Ο σκοπός του εσωτερικού **router** είναι να μπλοκάρει όλη την κίνηση εκτός από αυτή του **proxy server .**

### 3.7.2 Αρχιτεκτονικές

- Αρχιτεκτονικές με χρήση μιας συσκευής

Η απλούστερη περίπτωση εγκατάστασης **firewall** είναι με μία μοναδική συσκευή που αναλαμβάνει την λειτουργία του **firewall[14].** Το πλεονέκτημά της είναι πως υπάρχει ένα σημείο στο οποίο πρέπει κάποιος να επικεντρωθεί ώστε να κάνει σωστή διαμόρφωση **,** ενώ σαν μειονέκτημα μπορεί να θεωρηθεί ακριβώς το ότι η ασφάλεια εξαρτάται μόνο από μία συσκευή**.** Στην πράξη το πλεονέκτημα των αρχιτεκτονικών αυτών με μία συσκευή δεν είναι στην ασφάλεια **,** που δεν είναι σε πολλαπλά επίπεδα **,** αλλά σε πρακτικά θέματα**.** Η λύση αυτή είναι φτηνότερη **,** ευκολότερη στην υλοποίηση και στη συντήρηση κάνοντάς την κατάλληλη για μικρά **sites .** Ενδεικτικά παραδείγματα αυτού του τύπου αρχιτεκτονικής **firewall** είναι ο δρομολογητής ελέγχου κίνησης **(screening router)** και ο **dual-homed host.**

- Αρχιτεκτονικές με διαχωρισμό υπηρεσιών

Σε αυτήν την περίπτωση για ορισμένες υπηρεσίες η σύνδεση του διαδικτύου με το εσωτερικό δίκτυο γίνεται μέσω ενός εσωτερικού κόμβου **,** τον ενδιάμεσο **(proxy) [17],** που παίζει το ρόλο της αντίστασης σε επιθέσεις**.** Η χρήση αυτής της αρχιτεκτονικής συνίσταται όταν υπάρχουν λίγες εισερχόμενες συνδέσεις και όταν το δίκτυο που προστατεύεται έχει σχετικά μεγάλο επίπεδο ασφάλειας στους κόμβους**.**

- Αρχιτεκτονικές με διαχωρισμό υποδικτύων

Η αρχιτεκτονική του διαχωρισμού των υποδικτύων προσθέτει ένα επιπλέον επίπεδο ασφάλειας**.** Με την υλοποίηση ενός περιμετρικού δικτύου **( DeMilitary Zone-DMZ )[28]** απομονώνεται ακόμα περισσότερο το εσωτερικό δίκτυο από τους χρήστες του διαδικτύου**.**Το περιμετρικό δίκτυο είναι ένα ακόμα επίπεδο ασφάλειας ανάμεσα στο διαδίκτυο και το εσωτερικό δίκτυο**.**Η αρχιτεκτονική αυτή είναι η καταλληλότερη για τις περισσότερες περιπτώσεις δικτύων και **firewalls.**

- Αρχιτεκτονικές με διαχωρισμό πολλαπλών υποδικτύων

Υπάρχουν περιπτώσεις που χρειάζεται κάτι παραπάνω από αυτά που προσφέρει η αρχιτεκτονική του διαχωρισμού υποδικτύων**[28].**Στις περιπτώσεις αυτές προσφέρονται πιο σύνθετες αρχιτεκτονικές διπλού διαχωρισμού δικτύων**.**Σε αυτόν τον τύπο υπάρχουν ο εξωτερικός και ο εσωτερικός δρομολογητής αλλά υπάρχουν **2** περιμετρικά υποδίκτυα που συνδέονται μεταξύ τους**.** Χαρακτηριστικά παραδείγματα

αυτής της αρχιτεκτονικής είναι η περίπτωση του Διπλού διαχωρισμού υποδικτύων με χρήση υπολογιστή διπλής κάρτας δικτύου και η περίπτωση του Διπλού διαχωρισμού σε ανεξάρτητα υποδίκτυα. Η χρήση αυτών των αρχιτεκτονικών ενδείκνυται σε περιπτώσεις που έχει μεγάλη σημασία η εναλλακτική όδευση της επικοινωνίας , ή απαιτήσεις για υψηλή ασφάλεια και διαφορετικές ανεξάρτητες χρήσεις του διαδικτύου.

### 3.7.3 Σχεδιασμός

Παραθέτουμε παρακάτω βήματα σχεδιασμού **firewalls [28,86]:**

1. **Σχεδιασμός**
   - **1.1.** Τεκμηρίωση του περιβάλλοντος. Όταν σχεδιάζεται ένα **firewall** χρειάζεται να γνωρίζουμε τα όρια ανάμεσα στα διαφορετικά τμήματα ασφάλειας σε ένα **site**
   - **1.2.** Επιλογή των λειτουργιών του **firewall** ανάμεσα σε **packet filtering, application proxies, dynamic packet filtering .**
   - **1.3.** Επιλογή της αρχιτεκτονικής **firewall**
   - **1.4.** Ανάλυση των υπέρ και κατά της αρχιτεκτονικής
   - **1.5.** Προστασία του συστήματος από μη εξουσιοδοτημένη προσπέλαση
2. **Επιλογή λογισμικού και υλικού για firewall**
   - **2.1.** Προσδιορισμός των απαραίτητων τμημάτων υλικού **(** υπολογιστές**,** δρομολογητές**,** επεξεργαστές**,** μνήμη, δίσκος**,** κάρτες κλπ**)**
   - **2.2.** Προσδιορισμός των απαραίτητων τμημάτων λογισμικού **(** λειτουργικά συστήματα**, patches, device drivers** κλπ**)**
   - **2.3.** Προσδιορισμός των εργαλείων ελέγχου
3. **Επιλογή του υλικού τεκμηρίωσης , της εκπαίδευσης και της υποστήριξης**
   - **3.1.** Προσδιορισμός των απαιτήσεων εκπαίδευσης**,** όπως πρωτόκολλα**,** αρχιτεκτονική δικτύων**,** λογισμικό **firewall,** ασφάλεια δικτύων και υπολογιστών**,** παρακολούθηση λειτουργίας δικτύων**, system management.** Επιλογή μαθημάτων**,** βιβλίων**,** περιοδικών**,** συνεδρίων και ιστοσελίδων**.**
   - **3.2.** Προσδιορισμός των αναγκών σε υποστήριξη. Η υποστήριξη από τον κατασκευαστή μπορεί να είναι κρίσιμη σε περιπτώσεις που το σύστημα είναι ειδικού σκοπού.
4. **Εγκατάσταση του υλικού και του λογισμικού του firewall**
   - **4.1.** Εγκατάσταση του απαραίτητου ελάχιστου περιβάλλοντος του λειτουργικού συστήματος
   - **4.2.** Εγκατάσταση όλων των διαθέσιμων **patches**
   - **4.3.** Περιορισμός της προσπέλασης στο σύστημα ανάλογα με τον χρήστη και τον κόμβο
   - **4.4.** Απενεργοποίηση της δυνατότητας IP **forwarding**
   - **4.5. Backup** στο σύστημα
5. **Διαμόρφωση της δρομολόγησης IP**
   - **5.1.** Εξασφάλιση των IP διευθύνσεων
   - **5.2.** Εγκατάσταση της διαμόρφωσης δρομολόγησης
6. **Διαμόρφωση του φιλτραρίσματος πακέτων στο firewall**
   - **6.1.** Σχεδιασμός των κανόνων φιλτραρίσματος των πακέτων **,** με κριτήρια στοιχεία από την επικεφαλίδα του πακέτου**.** Σαν αρχή για την δημιουργία κανόνων για φορά έχουμε τα ακόλουθα **:**
     - **6.1.1.** Γενικά ο κανόνας είναι **deny all packets**
     - **6.1.2.** Σχεδιάζουμε κανόνες **anti-spoofing** και τους τοποθετούμε στην αρχή της λίστας των κανόνων
     - **6.1.3.** Δημιουργούμε ένα πίνακα με τους αποστολείς και παραλήπτες πακέτων με τα πρωτόκολλα και τις θύρες που χρησιμοποιούνται στην

συνήθη λειτουργία τους **,** ώστε να διαπιστώσουμε πως δεν έχουμε αποκλείσει την επικοινωνία κάποιου χρήστη με άλλον ή με υπηρεσία

**6.1.4.** Ταξινομούμε τον πίνακα ως προς το πρωτόκολλο και μετά την θύρα

**6.1.5.** Συγκεντρώνουμε τα ίδια πρωτόκολλα σε μια γραμμή και στις επόμενες συνεχόμενα τις θύρες

**6.1.6.** Μετατρέπουμε τον πίνακα σε σετ από κανόνες και τις τοποθετούμε ανάμεσα στους κανόνες **anti-spoofing** και στον κανόνα **deny all**

**6.2.** Προσοχή χρειάζεται στις ακόλουθες περιπτώσεις **:**

**6.2.1.** Σε ορισμένα συστήματα κενή λίστα κανόνων σημαίνει πως δεν επιτρέπεται να περάσει κυκλοφορία

**6.2.2.** Μερικά συστήματα έχουν προκαθορισμένους κανόνες

**6.2.3.** Μερικά συστήματα έχουν ξεχωριστούς κανόνες για εισερχόμενα και εξερχόμενα πακέτα

**6.2.4.** Για να λειτουργήσουν οι κανόνες **anti-spoofing** πρέπει το **firewall** να αντιλαμβάνεται την εισερχόμενη και εξερχόμενη κίνηση σε κάθε **interface.** Χρειάζεται να τεθούν οι κανόνες ανάλογα με την φορά

**6.2.5.** Το φιλτράρισμα πακέτων πρέπει να βασίζεται σε IP διευθύνσεις και όχι σε ονόματα κόμβων

**6.2.6.** Αν το σύστημα επιτρέπει την αναφορά σε εγκαθιδρυμένες συνδέσεις **TCP ( established TCP connections )** από το εσωτερικό μας δίκτυο τότε μπορεί να επιτραπεί η προώθηση των πακέτων που προέρχονται από εξωτερικό κόμβο και αφορά αυτή τη σύνδεση **.** Αυτό είναι επικίνδυνο αφού δεν είναι όλες οι υλοποιήσεις του **TCP** ασφαλείς

**6.2.7.** Αν χρειάζεται έλεγχος στα πακέτα **UDP ,** τότε ορισμένες υπηρεσίες πρέπει να τρέχουν σε **proxies** , αλλιώς αν δεν επιτρέψουμε **UDP** κάποιες υπηρεσίες δεν θα λειτουργούν **(** π.χ**.** το **DNS «**τρέχει**»** στο **port UDP 53)**

**6.2.8.** Το **ICMP** είναι **connectionless** πρωτόκολλο και έχει τους ίδιους κινδύνους με το **UDP ,** όμως έχει **13** διαφορετικές παραλλαγές και μπορούμε να αποφασίσουμε ποια θα επιτρέψουμε

**6.2.9.** Προσοχή στην απενεργοποίηση του **source routing feature** και την απόρριψη όλων των πακέτων που έχουν αυτό το **flag**

**6.2.10.** Τεκμηρίωση των κανόνων φιλτραρίσματος πακέτων

**6.2.11.** Εγκατάσταση των κανόνων

**7. Εγκατάσταση των μηχανισμών καταγραφής και συναγερμού**

**7.1.** Σχεδιασμός του περιβάλλοντος καταγραφών

**7.2.** Επιλογή των περιπτώσεων φιλτραρίσματος πακέτων που θα καταγράφονται

**7.3.** Σχεδιασμός του συστήματος συναγερμού

**7.4.** Προμήθεια ή δημιουργία των εργαλείων υποστήριξης

**8. Έλεγχος στο σύστημα firewall**

**8.1.** Δημιουργία πλάνου ελέγχων για πρωτόκολλα**,** θύρες**,** υπηρεσίες και χρήστες

**8.2.** Προμήθεια εργαλείων ελέγχου

**8.3.** Έλεγχος των λειτουργιών του **firewall** στο περιβάλλον εργαστηρίου

**8.3.1.** Απενεργοποίηση του φιλτραρίσματος πακέτων

**8.3.2.** Εισαγωγή πακέτων που θα εξετάσουν όλους τους κανόνες δρομολόγησης και να σταλούν μέσα από το **firewall**

**8.3.3.** Επιβεβαίωση πως τα πακέτα στάλθηκαν σωστά αντιπαραβάλλοντας τα στοιχεία των καταγραφών του **firewall** και τα ευρήματα του **scanner**

**8.3.4.** Ενεργοποίηση του **packet filtering**

**8.3.5.** Εισαγωγή πακέτων που περιέχουν δείγμα από όλες τις πιθανές διευθύνσεις αποστολέων **,**παραληπτών για όλα τα πρωτόκολλα_ και όλες τις θύρες

**8.3.6.** Επιβεβαίωση πως τα πακέτα που έπρεπε να αποκλειστούν αποκλείστηκαν και όλα όσα έπρεπε να περάσουν πέρασαν **.** Εξετάζουμε τις καταγραφές του **firewall** και συγκρίνουμε τα αποτελέσματα

**8.3.7.** Διενέργεια ανίχνευσης για ανοιχτά και μπλοκαρισμένα **ports ,** για να διαπιστώσουμε πως το **firewall** λειτουργεί όπως το σχεδιάσαμε

**8.3.8.** Αντιπαραβάλλουμε όλη την κίνηση που καταγράφηκε σαν συναγερμός αντιστοιχεί με αυτή που έπρεπε να έχει καταγραφεί από τους κανόνες

**8.3.9.** Εξετάζουμε αν όλοι οι κανόνες πουν ενεργοποιούν συναγερμούς αποστέλλονται

**8.4.** Έλεγχος του **firewall** στο παραγωγικό περιβάλλον

**8.5.** Επιλογή και εξέταση λειτουργιών που σχετίζονται με την καταγραφή

**8.6.** Ανίχνευση για τρωτά σημεία

**8.7.** Επιλογή επαναλαμβανόμενων τεστ για την επιβεβαίωση της ορθής λειτουργίας σε τακτά χρονικά διαστήματα

**8.8.** Προετοιμασία για παραγωγική χρήση

**8.9.** Προετοιμασία για παρακολούθηση της λειτουργίας

**9. Εγκατάσταση του firewall**

**9.1.** Εγκατάσταση της νέας συνδεσμολογίας

**9.2.** Εγκατάσταση της συνδεσμολογίας αντικατάστασης των συστημάτων

**10. Φάση ενεργοποίησης λειτουργίας του συστήματος**

**10.1.** Προετοιμασία μεταγωγής στο νέο σύστημα

**10.2.** Ενημέρωση χρηστών

**10.3.** Ενεργοποίηση της ιδιωτικής κίνησης πάνω από το **firewall**

**10.4.** Εγκατάσταση των συνδέσεων του διαδικτύου και του ιδιωτικού δικτύου στο **firewall**

**10.5.** Αλλαγή των **default gateways**

**10.6.** Ενημέρωση των πινάκων δρομολόγησης **( Update routing table )**

## 3.8 IPsec

Η **IETF** γνώριζε για χρόνια ότι η ασφάλεια στο Διαδίκτυο ήταν ανεπαρκής. Μετά την τεράστια εξάπλωση που γνώρισε το Διαδίκτυο και τη σημασία που απέκτησε στον τομέα των επιχειρήσεων και του ηλεκτρονικού εμπορίου η ασφάλεια έγινε μία από τις πιο απαιτητικές ανάγκες στο Διαδίκτυο. Για να καλύψει τις ανάγκες αυτές η **IETF** δημιούργησε το IP **Security Working Group[43]** με στόχο να σχεδιάσει μια αρχιτεκτονική ασφαλείας και τα αντίστοιχα πρωτόκολλα. Η προσθήκη της ασφάλειας δεν ήταν εύκολη υπόθεση επειδή ένας πόλεμος ξέσπασε σχετικά με το σημείο που έπρεπε να τοποθετηθεί. Οι περισσότεροι ειδικοί στην ασφάλεια θεωρούν ότι για να υπάρχει πραγματικά ασφάλεια, οι κρυπτογράφηση και οι έλεγχοι ακεραιότητας πρέπει να γίνονται απ' άκρο εις άκρο. Δηλαδή η διεργασία προέλευσης θα κρυπτογραφεί ή και θα προστατεύει την ακεραιότητα των δεδομένων, και μετά θα τα στέλνει στη διεργασία προορισμού όπου θα αποκρυπτογραφούνται ή και θα επαληθεύονται. Οποιεσδήποτε τροποποιήσεις γίνουν ανάμεσα σε αυτές τις δύο διεργασίες θα μπορούν να εντοπιστούν. Το πρόβλημα με αυτήν την προσέγγιση είναι ότι απαιτεί την αλλαγή όλων των εφαρμογών , ώστε να ασχολούνται με την ασφάλεια. Κατά αυτήν την άποψη, η επόμενη καλύτερη προσέγγιση είναι να τοποθετηθεί η κρυπτογράφηση στο επίπεδο μεταφοράς ή σε ένα νέο επίπεδο μεταξύ του επιπέδου εφαρμογών και το επίπεδο μεταφοράς.

Η αντίθετη άποψη είναι ότι οι χρήστες δεν κατανοούν την ασφάλεια και δεν θα είναι σε θέση να την χρησιμοποιούν σωστά , και ότι κανείς δε θέλει να τροποποιήσει τα υπάρχοντα προγράμματα με κανένα τρόπο , έτσι το επίπεδο δικτύου θα πρέπει να πιστοποιεί την ταυτότητα ή/και να κρυπτογραφεί τα πακέτα χωρίς να αναμιγνύεται ο χρήστης . Μετά από χρόνια έντονων μαχών, αυτή η προσέγγιση απέκτησε αρκετή υποστήριξη ώστε να οριστεί ένα πρότυπο ασφαλείας επιπέδου δικτύου. Το επιχείρημα ήταν εν μέρει ότι η ύπαρξη κρυπτογράφησης σε επίπεδο δικτύου δεν αποτρέπει τους χρήστες που είναι ενήμεροι για την ασφάλεια να κάνουν το σωστό , ενώ βοηθά σε κάποιο βαθμό τους χρήστες που δεν είναι ενήμεροι για την ασφάλεια .

Το αποτέλεσμα αυτού του πολέμου ήταν μια σχεδίαση που ονομάζεται ασφάλεια IP ή **Ipsec[19],[43] (IP security),** η οποία περιγράφεται κυρίως στα **RFC 2401,2402,** και **2406.** Σε γενικές γραμμές , δεν θέλουν όλοι οι χρήστες κρυπτογράφηση **(** επειδή είναι υπολογιστικά δαπανηρή**).** Αντί να γίνει προαιρετική η κρυπτογράφηση , αποφασίστηκε να απαιτείται πάντοτε αλλά να επιτρέπεται η χρήση ενός κενού αλγόριθμου. Ο κενός αλγόριθμος περιγράφεται και εγκωμιάζεται για την απλότητά του, ευκολία της υλοποίησης του, και τη μεγάλη του ταχύτητα στο **RFC 2410.**

Το πλήρες σχέδιο **IPsec** είναι ένα πλαίσιο εργασίας για περισσότερες από μία υπηρεσίες, αλγορίθμους και επίπεδα λεπτομέριας . Ο λόγος της ύπαρξης πολλαπλών υπηρεσιών είναι ότι δεν θέλουν όλοι να να πληρώνουν το κόστος για να έχουν όλες τις υπηρεσίες ανά πάσα στιγμή. Οι σημαντικότερες υπηρεσίες είναι η μυστικότητα, ακεραιότητα δεδομένων, και προστασία από τις επιθέσεις αναπαραγωγείς. Όλες οι υπηρεσίες είναι βασισμένες στην κρυπτογραφία συμμετρικού κλειδιού, επειδή είναι κρίσιμο το θέμα της υψηλής απόδοσης .

Οι υπηρεσίες που μπορούν να θεωρηθούν μερος του **IPsec** περιλαμβάνουν **[43] (**Σχήμα **30):**

**Έλεγχο πρόσβασης .** Η πρόσβαση σε οποιαδήποτε υπηρεσία ή σύστημα απαιτεί κωδικό.Υπάρχουν διάφορα πρωτόκολλα ασφαλείας που μπορούν να χρησιμοποιηθούν για να ορίσουν μία ασφαλή ανταλλαγή κλειδιών

**Ακεραιότητα δεδομένων .** Είναι δυνατή η πιστοποίηση ακεραιότητας ενός οποιουδήποτε IP πακέτου χωρίς την ανάγκη να ελεγθεί άλλο πακέτο πριν ή μετά το πακέτο που πρέπει να ελεχθεί.

**Πιστοποίηση του αποστολέα .** Είναι δυνατή η πιστοποίηση του αποστολέα με χρήση των κατάλληλων αλγορίθμων ψηφιακών κλειδιών

**Προστασία εναντίων επιθέσεων τύπου packet replay .** Παρέχονται μηχανισμοί προστασίας του κόμβου αποστολέα από επιθέσεις όπου ο επιτιθέμενος προσπαθεί να

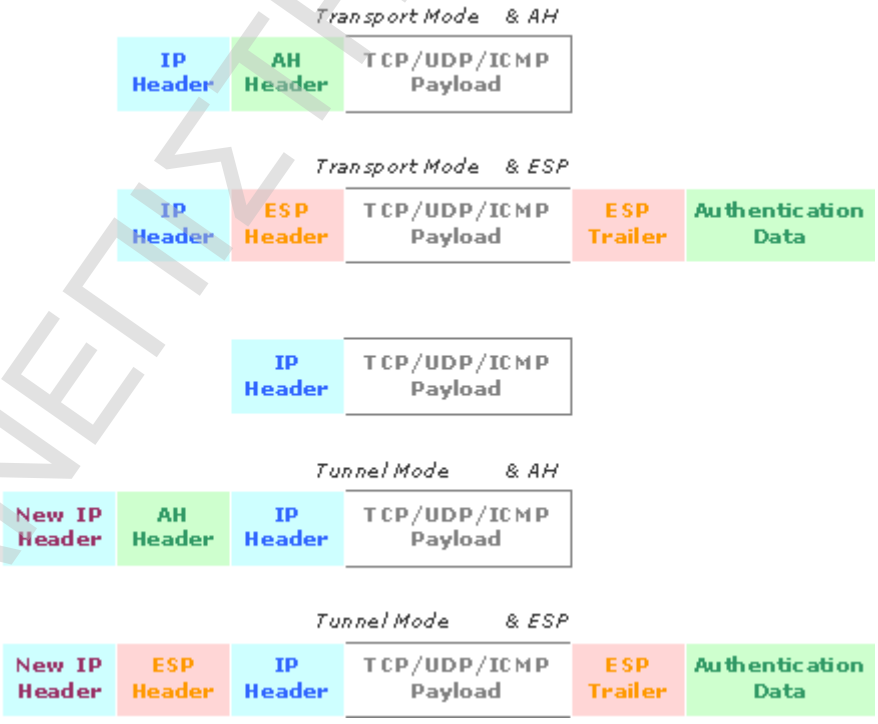
βλάψει την διαθεσιμότητα του συστήματος, υποκλέπτοντας ένα πακέτο και στέλνοντας το πολλές φορές στον αποστολέα.

**Κωδικοποίηση των δεδομένων.** Παρέχονται μηχανισμοί κωδικοποίησης για να εξασφαλιστεί το απόρρητο των δεδομένων.

**Εξασφάλιση απόρρητου της ροής των δεδομένων.** Παρέχονται μηχανισμοί προστασίας της ροής των πακέτων ώστε ο επιτιθέμενος να μην μπορεί να βγάλει συμπεράσματα παρακολουθώντας ένα προς ένα τα πακέτα.

Ο λόγος ύπαρξης πολλών αλγορίθμων είναι ότι ένας αλγόριθμος που θεωρείται τώρα ασφαλής μπορεί να σπάσει στο μέλλον. Αν το **IPsec** είναι ανεξάρτητο από τους αλγόριθμους , το γενικό πλαίσιο θα μπορεί να επιβιώσει ακόμα και αν κάποιος συγκεκριμένος αλγόριθμος σπάσει στο μέλλον . Ο λόγος για την ύπαρξη πολλών επιπέδων λεπτομέρειας είναι να καταστεί εφικτή η προστασία είτε μόνο μιας σύνδεσης **TCP** , είτε όλης της κίνησης ανάμεσα σε ένα ζεύγος υπολογιστών υπηρεσίας , ή όλης της κίνησης ανάμεσα σε ένα ζεύγος ασφαλών δρομολογητών.

Το **IPsec** μπορεί να χρησιμοποιηθεί σε μία από **2** πιθανές καταστάσεις λειτουργίας . Στην κατάσταση μεταφοράς **( transport mode )** η κεφαλίδα **IPsec** εισάγεται αμέσως μετά την από την κεφαλίδα IP . Στην κατάσταση σήραγγας **( tunnel mode )** ολόκληρο το πακέτο IP , κεφαλίδα και ωφέλιμο φορτίο , ενθυλακώνεται στο σώμα ενός νέου πακέτου IP με μια νέα εντελώς κεφαλίδα IP.




**Σχήμα 30. IPsec modes**

Τεχνικά, **IPsec** έχει δύο κύρια μέρη**[43].** Το πρώτο μέρος περιγράφει δύο νέες κεφαλίδες που μπορούν να προστεθούν στα πακέτα για να μεταφέρουν το αναγνωριστικό μέρος της ασφάλειας , τα δεδομένα ελέγχου ακεραιότητας και άλλες πληροφορίες. Το άλλο μέρος , το Πρωτόκολλο Συσχετίσεων Ασφαλείας και Διαχείρισης Κλειδιών **Internet** ή **ISAKMP ( Internet Security Association and Key Management Protocol)** ασχολείται με την εγκαθίδρυση των κλειδιών.

Η πρώτη νέα κεφαλίδα είναι η Κεφαλιδα Πιστοποίησης ταυτότητας ή ΑΗ **(Authentication Header ).** Η κεφαλίδα αυτή παρέχει έλεγχο ακεραιότητας και ασφάλεια έναντι στις επιθέσεις αναπαραγωγής , αλλά δεν παρέχει μυστικότητα**(** δηλαδή δεν παρέχει κρυπτογράφηση δεδομένων**).**Η χρήση της ΑΗ γίνεται **(**κυρίως **)** στην κατάσταση μεταφοράς .

Η εναλλακτική κεφαλίδα του **IPsec** είναι η κεφαλίδα Ενθυλακωμένου Ασφαλούς Ωφέλιμου Φορτίου ή **ESP ( Encapsulating Security Payload) .** Η κεφαλίδα αυτή χρησιμοποιείται τόσο στην κατάσταση μεταφοράς όσο και στην κατάσταση σήραγγας . Στην κεφαλίδα αυτή πέρα όλων των άλλων καλύπτεται και η ανάγκη της μυστικότητας **(** πράγμα που δεν παρέχει η κεφαλίδα ΑΗ**).**

## 3.9 Ψηφιακές Υπογραφές

Η αυθεντικότητα πολλών νομικών, οικονομικών, και άλλων εγγράφων καθορίζεται από την παρουσία ή την απουσία μιας εξουσιοδοτημένης χειρόγραφης υπογραφής. Τα φωτοαντίγραφα δεν μετρούν. Για να μπορέσουν τα υπολογιστικά συστήματα μεταφοράς μηνυμάτων να αντικαταστήσουν τη φυσική μεταφορά εγγράφων που είναι γραμμένα με χαρτί και μελάνι, μια μέθοδος πρέπει να βρεθεί που να επιτρέπει την υπογραφή των εγγράφων με τρόπο που να μην επιτρέπει την πλαστογραφία.

Το πρόβλημα της επινόησης ενός αντικαταστάτη για τις χειρόγραφες υπογραφές είναι δύσκολο. Βασικά, αυτό που απαιτείται είναι ένα σύστημα στο οποίο το ένα μέρος να μπορεί να στέλνει ένα υπογεγραμένο μύνημα σε ένα άλλο μέρος , με τέτοιον τρόπο ώστε να ισχύουν οι ακόλουθες συνθήκες **[137] (**Σχήμα **31):**

**1.**Ο παραλήπτης να μπορεί να επαληθεύσει την υποτιθέμενη ταυτότητα του αποστολέα.

**2.**Ο αποστολέας να μην μπορεί αργότερα να αποκηρύξει το περιεχόμενο του μηνύματος.

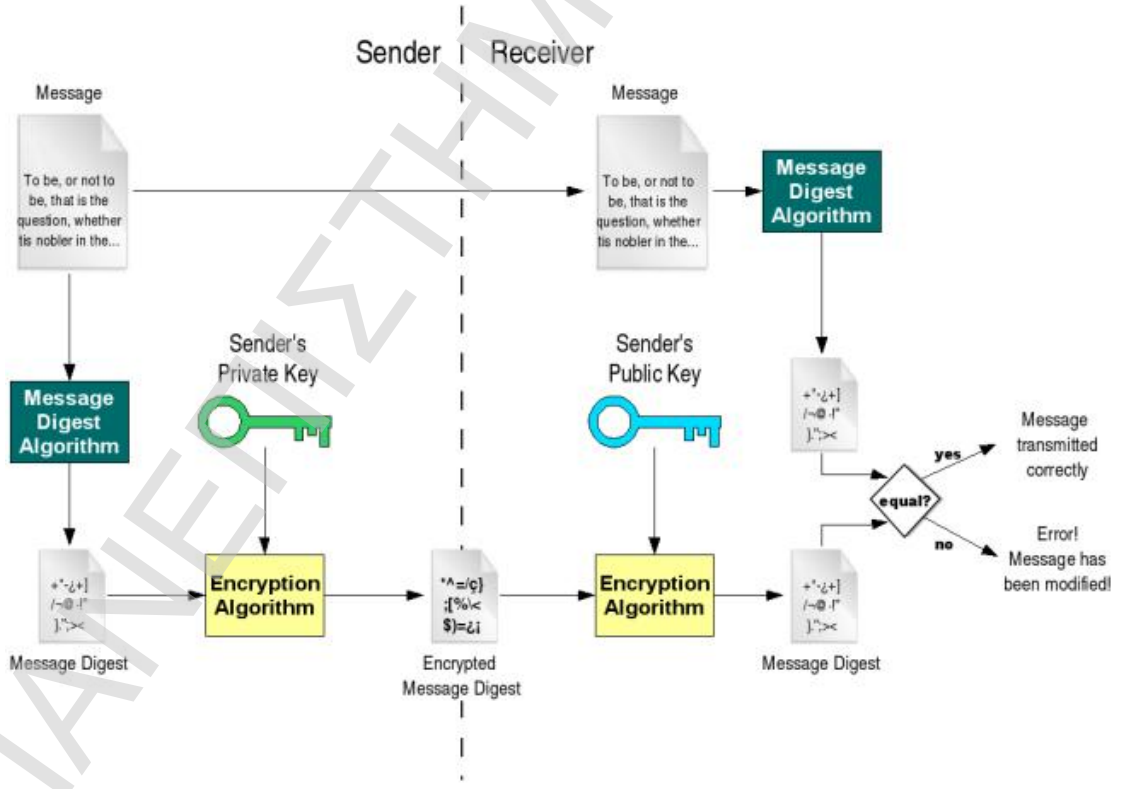
**3.**Ο παραλήπτης να μην μπορεί να έχει κατασκευάσει το μήνυμα ο ίδιος.

Η πρώτη απαίτηση χρειάζεται, παραδείγματος χάριν, στα οικονομικά συστήματα. Όταν ο υπολογιστής ενός πελάτη διατάζει τον υπολογιστή μιας τράπεζας για να αγοράσει έναν τόνο χρυσού, ο υπολογιστής της τράπεζας πρέπει να είναι σε θέση

να σιγουρευτεί ότι ο υπολογιστής που δίνει τη διαταγή ανήκει πραγματικά στην επιχείρηση της οποίας θα πιστωθεί ο λογαριασμός. Με άλλα λόγια, η τράπεζα πρέπει να πιστοποιήσει την ταυτότητα του πελάτη (και ο πελάτης πρέπει να πιστοποιήσει την ταυτότητα της τράπεζας).

Η δεύτερη απαίτηση απαιτείται για να προστατεύσει την τράπεζα από τις απάτες. Υποθέστε ότι η τράπεζα αγοράζει τον τόνο του χρυσού, και αμέσως η τιμή του χρυσού πέφτει απότομα. Ένας ανέντιμος πελάτης μπορεί να μηνύσει την τράπεζα, υποστηρίζοντας ότι δεν εξέδωσε ποτέ οποιαδήποτε εντολή να αγοράσει το χρυσό. Όταν η τράπεζα εμφανίσει το μήνυμα στο δικαστήριο, ο πελάτης αρνείται ότι το έστειλε. Η ιδιότητα ότι κανένα από τα συμβαλλόμενα μέρη σε ένα συμβόλαιο δεν μπορεί αργότερα να αρνηθεί ότι το έχει υπογράψει ονομάζεται μη αποκύρηξη **(nonrepudiation).**Οι μέθοδοι ψηφιακής υπογραφής παρέχουν αυτή την ιδιότητα.

Η τρίτη απαίτηση απαιτείται για να προστατεύσει τον πελάτη σε περίπτωση που η τιμή του χρυσού αυξηθεί και η τράπεζα προσπαθήσει να κατασκευάσει ένα υπογεγραμμένο μήνυμα στο οποίο ο πελάτης ζήτησε μια ράβδο χρυσού αντί ενός τόνου. Σε αυτό το σενάριο απάτης, η τράπεζα θα κρατούσε τον υπόλοιπο χρυσό για τον εαυτό της.




**Σχήμα 31. Ψηφιακή υπογραφή**

### 3.9.1 Υπογραφές συμμετρικού κλειδιού

Μια προσέγγιση στις ψηφιακές υπογραφές είναι να υπάρξει μια κεντρική αρχή που ξέρει τα πάντα **[118]** και που να εμπιστεύονται οι πάντες, για παράδειγμα Μεγάλος Αδελφός ή **BB (Big Brother) (**Σχήμα **32).** Κατά συνέπεια, μόνο η **Alice** και ο **BB** ξέρουν το μυστικό κλειδί της **Alice, KA,** και ούτω καθεξής.

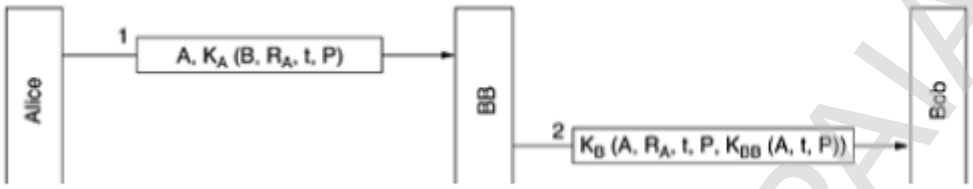
Όταν η **Alice** θέλει να στείλει ένα υπογεγραμμένο μήνυμα απλού κειμένου, P, στον τραπεζίτη της,τον **Bob,** παράγει **KA(B, RA, t,** P**),** όπου το **B** είναι η ταυτότητα του **Bob, RA** είναι ένας τυχαίος αριθμός που επιλέγεται από την **Alice,** το **t** είναι μια χρονοσφραγίδα που εγγυάται την φρεσκάδα του μυνήματος, και **KA(B, RA, t,** P**)** είναι το μήνυμα που κρυπτογραφείται με το κλειδί της, KA.Κατόπιν στέλνει το μύνημα όπως απεικονίζεται στην εικόνα .Ο **BB** βλέπει ότι το μήνυμα είναι από την **Alice,** το αποκρυπτογραφεί, και στέλνει ένα μήνυμα στο **Bob** όπως φαίνεται στην εικόνα.Το μήνυμα προς τον **Bob** περιέχει το απλό κείμενο του μηνύματος και επίσης το υπογεγραμμένο μήνυμα **KBB (A, t, P) .** Ο **Bob** στη συνέχεια εκτελεί την αίτηση της **Alice.**

Τι συμβαίνει εάν η **Alice** αρνηθεί αργότερα ότι έστειλε το μήνυμα; Το πρώτο βήμα είναι ότι όλοι μυνήουν όλους τους υπολοίπους. Τελικά,όταν η υπόθεση έρχεται στο δικαστήριο και η **Alice** αρνείται επίμονα στον **Bob** ότι του έστειλε το αμφισβητούμενο μήνυμα, ο δικαστής θα ρωτήσει τον **Bob** πώς μπορεί να είναι βέβαιος ότι το συζητημένο μήνυμα προήλθε από την **Alice** και όχι από την **Trudy. Ο** Bo**b** αρχικά επισημαίνει ότι ο **BB** δεν θα δεχτόταν κανένα μήνυμα από την **Alice** εκτός αν αυτό δεν ήταν κρυπτογραφημένο με το KA, έτσι δεν υπάρχει καμία πιθανότητα η **Trudy** να έστειλε στον **BB** ένα ψεύτικο μήνυμα από την **Alice** χωρίς ο **BB** να το εντοπίσει άμεσα.

**Ο Bob** έπειτα θα εμφανίσει το Πειστήριο Α: το **KBB (** A**, t, P). Ο Bob** λέει ότι αυτό είναι ένα μήνυμα υπογεγραμμένο από τον **BB** που αποδεικνύει ότι η **Alice** έστειλε το P στον **Bob** .Ο δικαστής έπειτα θα ζητήσει από τον **BB (**που όλοι εμπιστεύονται**)** να αποκρυπτογραφήσει το Πειστήριο Α.Όταν ο **BB** καταθέσει ότι ο **Bob** λέει την αλήθεια, ο δικαστής αποφασίζει υπέρ του **Bob.** Η υπόθεση έκλεισε.

Ένα πιθανό πρόβλημα με το πρωτόκολλο υπογραφών της εικόνας είναι ότι η **Trudy** μπορεί να αναπαραγάγει κάποιο από τα μυνήματα. Για να ελαχιστοποιηθεί αυτό το πρόβλημα, χρησιμοποιούνται παντού χρονοσφραγίδες. Επιπλέον, ο **Bob** μπορεί να εξετάσει όλα τα πρόσφατα μηνύματα για να δει εάν το **RA** χρησιμοποιήθηκε σε οποιαδήποτε από αυτά. Σε αυτή την περίπτωση, το μήνυμα απορρίπτεται ως αναπαραγωγή.Έτσι ο **Bob** απορρίπτει τα πολύ παλαιά μηνύματα. Για να εξασφαλιστεί από τις άμεσες επιθέσεις αναπαραγωγής , ο **Bob** απλώς ελέγχει το **RA**

κάθε εισερχόμενου μυνήματος , για να δει αν έχει λάβει ένα τέτοιο μήνυμα από την **Alice** την τελευταία μία ώρα.Αν δεν συμβεί αυτό , ο **Bob** μπορεί να υποθέσει με ασφάλεια ότι πρόκειται για νέα αίτηση.




**Σχήμα 32. Ψηφιακές υπογραφές από τον Μεγάλο Αδερφό**

### 3.9.2 Υπογραφές δημόσιου κλειδιού

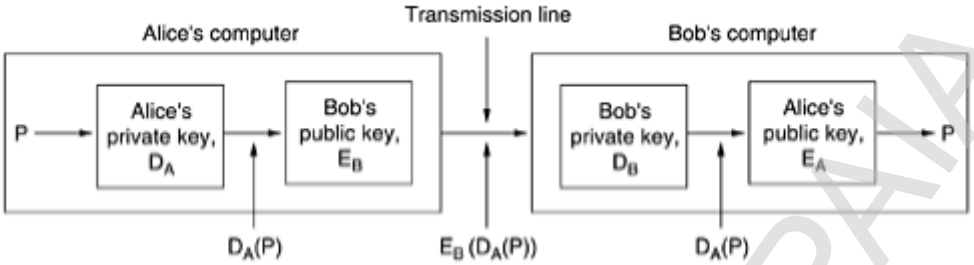
Ένα δομικό πρόβλημα με τη χρήση κρυπτογραφίας του συμμετρικού κλειδιού για τις ψηφιακές υπογραφές είναι ότι όλοι πρέπει να συμφωνήσουν ότι εμπιστεύονται τον Μεγάλο Αδελφό. Επιπλέον, ο μεγάλος αδελφός παίρνει να διαβάσει όλα τα υπογεγραμμένα μηνύματα. Οι πλέον λογικοί υποψήφιοι για τη διαχείριση του διακομιστή του Μεγάλου Αδερφού είναι η κυβέρνηση, οι τράπεζες, οι λογιστές,και οι δικηγόροι. Δυστυχώς, κανένας από τους οργανισμούς αυτούς δεν εμπνέει απόλυτη εμπιστοσύνη σε όλους τους πολίτες. Ως εκ τούτου, θα ήταν καλό να μην απαιτεί η υπογραφή εγγράφων μια έμπιστη αρχή.

Ευτυχώς, η κρυπτογραφία δημόσιου κλειδιού **[118,137]** μπορεί να έχει μια σημαντική συνεισφορά σε αυτόν τον τομέα.Ας υποθέσουμε ότι οι αλγόριθμοι κρυπτογράφησης και αποκρυπτογράφησης δημοσίου κλειδιού έχουν την ιδιότητα ότι **D(E(P)) = P.**Υποθέτωντας ότι αυτό συμβαίνει, η **Alice** μπορεί να στείλει ένα υπογεγραμμένο μήνυμα απλού κειμένου, P, στον **Bob** μεταδίδοντας το **EB(DA(P)).** Παρατηρούμε ότι η **Alice** ξέρει το δικό της **(**ιδιωτικό**)** κλειδί, **DA** , καθώς επίσης και το δημόσιο κλειδί του **Bob,EB** , έτσι η κατασκευή του μυνήματος αυτού είναι κάτι που η **Alice** μπορεί κάνει **(**Σχήμα **33).**

Όταν ο **Bob** λάβει το μήνυμα, το μετασχηματίζει χρησιμοποιώντας το ιδιωτικό κλειδί του, όπως συνήθως, παράγοντας τη **DA (P),** όπως φαίνεται στην εικόνα. Αποθηκεύει αυτό το κείμενο σε ένα ασφαλές μέρος και εφαρμόζει έπειτα EA για να πάρει το αρχικό απλό κείμενο.

Υποθέτουμε ότι η **Alice** αρνείται στη συνέχεια ότι έχει στείλει το μήνυμα P στον **Bob.** Όταν η περίπτωση φτάσει στο δικαστήριο, ο **Bob** μπορεί να εμφανίσει και το P και τη **DA (P).** Ο δικαστής μπορεί εύκολα να επιβεβαιώσει ότι ο **Bob** έχει πράγματι ένα έγκυρο μήνυμα κρυπτογραφημένο με το **DA,**απλά εφαρμόζοντας το EA σε αυτό. Δεδομένου ότι ο **Bob** δεν ξέρει το ιδιωτικό κλειδί της **Alice,** ο μόνος τρόπος για να

λάβει ο **Bob** ένα μήνυμα κρυπτογραφημένο με το κλειδί αυτό είναι να το έστειλε πραγματικά η **Alice.**




**Σχήμα 33. Ψηφιακές υπογραφές με χρήση κρυπτογραφίας δημόσιου κλειδιού**

## 3.10 Πιστοποίηση (Authentication)

Για πολλά χρόνια η μέθοδος της πιστοποίησης των χρηστών εφαρμοζόταν με την χρήση γνωστών, συχνά χρησιμοποιούμενων συνθηματικών **(passwords).** Αυτά τα συνθηματικά χρησιμοποιούνταν αρχικά από χρήστες τερματικών που ήθελαν να έχουν πρόσβαση σε κάποιο κεντρικό υπολογιστή. Την εποχή εκείνη δεν υπήρχαν ούτε τοπικά δίκτυα ούτε και δίκτυα ευρείας περιοχής και έτσι δεν υπήρχε κίνδυνος για την ανακάλυψη ενός συνθηματικού. Σήμερα με την εκτεταμένη χρήση των δικτύων , η αποστολή επαναχρησιμοποιούμενων **password** σε μορφή απλού κειμένου **( clear text)** δίνει την δυνατότητα σε οποιονδήποτε να τα βρίσκει με σχετικά εύκολο τρόπο. Στοιχεία που προέρχονται από τον οργανισμό **CERT** δείχνουν ότι μεγάλος αριθμός από **clear text password** εντοπίζονται εύκολα από **sniffers** πακέτων.

Οι τελευταίες τεχνολογικές τάσεις στο χώρο της πιστοποίησης είναι η χρήση **on-line passwords (S/key)**, **PGP** και η πιστοποίηση συσκευών να βασίζεται στην χρήση **«**κουπονιών**» ( token) .** Οι χρήστες χρησιμοποιούν αλφαριθμητικά συνθηματικά σαν κρυφά **token** και **pins.** Τα **token** αυτά συνήθως δεν επιλέγονται προσεκτικά ούτε προστατεύονται . Έτσι μπορεί εύκολα να υπονομευθεί η πιστοποίηση.

## 3.11 Εμπιστευτικότητα (Confidentiality)

Σε κάποια **site** τις περισσότερες φορές υπάρχουν πληροφορίες οι οποίες δε θα πρέπει να προσπελαστούν από μη εξουσιοδοτημένους χρήστες . Τα λειτουργικά συστήματα διαθέτουν συνήθως ενσωματωμένους μηχανισμούς για την προστασία των αρχείων . Οι μηχανισμοί αυτοί δίνουν τη δυνατότητα σε ένα διαχειριστή να ελέγχει ποιος θα έχει πρόσβαση στα περιεχόμενα των αρχείων αυτών.

Η εμπιστευτικότητα μπορεί να επιτευχθεί και με την κρυπτογράφηση. Η κρυπτογράφηση επιτυγχάνεται με την παρεμβολή χαρακτήρων στα δεδομένα, έτσι

ώστε να είναι δύσκολη και χρονοβόρα η εύρεση της αρχικής πληροφορίας για οποιονδήποτε άλλο εκτός από τους εξουσιοδοτημένος παραλήπτες. Οι εξουσιοδοτημένοι παραλήπτες και οι ιδιοκτήτες της πληροφορίας κατέχουν κλειδιά για την αποκρυπτογράφηση της πληροφορίας.

## 3.12 Ακεραιότητα (Integrity)

Ένας χρήστης πρέπει να εξασφαλίσει την ακεραιότητα της πληροφορίας που υπάρχει στο σύστημα του. Ένας τρόπος για να επιτευχθεί ο έλεγχος της ακεραιότητας των δεδομένων είναι να παράγουμε το **checksum** του αναλλοίωτου αρχείου και να το αποθηκεύουμε **off-line ,** και περιοδικά να συγκρίνουμε το **checksum** που αποθηκεύτηκε **off-line** με αυτό το αρχείο που χρησιμοποιείται **on-line.**

Υπάρχουν λειτουργικά συστήματα τα οποία έχουν ενσωματωμένα **checksumming** προγράμματα όπως το **unix sum .** Παρόλα αυτά είναι καλύτερο να χρησιμοποιούνται ισχυρές μέθοδοι και προγράμματα κρυπτογράφησης όπως το **message digest-MD5 .** Υπάρχουν επίσης προγράμματα τα οποία χρησιμοποιούνται για να ελέγχουν την ακεραιότητα των δεδομένων που ανταλλάσονται μεταξύ διαφόρων εφαρμογών όπως το **e-mail ,** όπου θέλουμε ένα μύνημα να φτάσει αναλλοίωτο από τον αποστολέα στον παραλήπτη.

# 4 Κακόβουλο λογισμικό (Malware)

## 4.1 Εισαγωγή

Ένας στους πέντε υπολογιστές έχει **rootkits**

Η επίθεση των **rootkits** συνεχίζεται με εντατικούς ρυθμούς, σύμφωνα με στοιχεία που αποκαλύπτονται από μια νέα έρευνα της εταιρείας **Prevx [138] (www.prevx.com/)**. Σε διάστημα δύο μηνών ελέγχθηκαν με τη βοήθεια του λογισμικού **Prevx CSI** της εταιρείας περισσότερα από **725.000 PC.** Κι ενώ το ποσοστό των υπολογιστών που είχαν εγκατεστημένο κάποιο **rootkit [4]** ήταν στο **15,6%** σε αντίστοιχη μέτρηση τον Οκτώβριο **(2008),** αυξήθηκε στο **22%** στις αρχές του Δεκεμβρίου.

Τα κακόβουλα **rootkits** μπορούν να επιτρέψουν σε έναν επιτιθέμενο να παρακολουθεί, να καταγράφει και να μεταφέρει πληροφορίες από έναν υπολογιστή εξ αποστάσεως. Παρ' όλο που δεν πρόκειται για μια καινούργια απειλή, η **Prevx** ισχυρίζεται ότι "η άνοδος των **rootkits** έχει ξεκινήσει", καθώς χρησιμοποιούνται ολοένα και πιο συχνά από όσους δημιουργούν κακόβουλο κώδικα, για να έχουν πρόσβαση σε άλλους υπολογιστές χωρίς να εντοπίζονται.

Ακόμη, η **Prevx** τονίζει ότι ο εντοπισμός και η απομάκρυνση των **rootkits** είναι κάτι που ξεπερνά κατά πολύ τις δυνατότητες των παραδοσιακών προγραμμάτων **anti-virus** και **anti-spyware** που αποκαλούνται **security suites.**

**Επίθεση phishing "χτυπά" τη Citibank**

Στο στόχαστρο των κακογραμμένων **phishing e-mail** βρέθηκε αυτήν τη φορά η **Citibank [139].** Το πλαστό **e-mail** ζητά τον αριθμό **PIN** αλλά και τον αριθμό της πιστωτικής κάρτας του χρήστη. Η ψεύτικη ιστοσελίδα, στην οποία οδηγούνται οι χρήστες, φιλοξενείται σε **domain** με κατάληξη **.hu (**Ουγγαρία**)** και σε μηχάνημα **(server)** με έδρα τη Βουδαπέστη.

Ενδιαφέρον παρουσιάζει το γεγονός ότι η κεντρική ιστοσελίδα φαίνεται να είναι **portal** τουριστικού ενδιαφέροντος. Ενδεχομένως το **phishing URL,** που είναι τμήμα της προαναφερθείσας ιστοσελίδας, να είναι το αποτέλεσμα παραβίασης της ασφάλειας του **TravelPort.hu.** Το κείμενο του πλαστού **e-mail** φαίνεται να προέρχεται από λογαριασμό που ανήκει στην τράπεζα.

Είναι σημαντικό να τονίσουμε ότι καμία τράπεζα δεν πρόκειται ποτέ να σας ζητήσει να της στείλετε το **PIN** ή τον αριθμό της πιστωτικής σας κάρτας, μέσω **e-mail.** Ακόμα, δε θα πρέπει ποτέ να ακολουθείτε **link** που βρίσκετε σε **e-mail,** για την

είσοδο σας σε **e-banking site,** αλλά να πληκτρολογείτε οι ίδιοι το **URL** στην **address bar** του **browser** σας.

Αυτά είναι ενδεικτικά κάποια από τα αναρίθμητα περιστατικά παραβίασης ασφαλείας που υποδεικνύουν ότι παρόλο την χρήση δικλίδων ασφαλείας όπως αυτές περιγράφηκαν στο προηγούμενο κεφάλαιο, υπάρχει πάντα το ενδεχόμενο παραβίασης της ασφάλειας. Σκοπός αυτού του κεφαλαίου είναι να αναλύσουμε μία από τις βασικές συνιστώσες παραβίασης της ασφάλειας, αυτή των κακόβουλων λογισμικών. Ξεκινώντας καταγράφουμε τα τρωτά σημεία που έρχονται να εκμεταλλευτούν και συνεχίζουμε με την ανάλυση των βασικών κατηγοριών τους, τον τρόπο δράσης τους αλλά και τους μηχανισμούς καταστολής και αφαίρεσής τους.

## 4.2 Τα Τρωτά Σημεία

Τα τρωτά σημεία των δικτύων μπορούν να ταξινομηθούν σε τρεις ευρείες κατηγορίες **[6, 52,125, 137]:**

**1)** Ελαττώματα στο λογισμικό ή το σχεδιασμό πρωτοκόλλων

Μέσω των πρωτοκόλλων προσδιορίζονται οι κανόνες και οι μέθοδοι, με τις οποίες μπορούν να επικοινωνούν μεταξύ τους οι υπολογιστές. Αν υπάρχει σχεδιαστικό σφάλμα στο πρωτόκολλο, υπάρχει μεγάλη πιθανότητα να εξελιχθεί σε τρωτό σημείο, ασχέτως με την ποιότητα υλοποίησης του πρωτοκόλλου. Αντίστοιχο παράδειγμα αποτελεί το **Network File System (NFS –** Δικτυακό Σύστημα Αρχείων**),** το οποίο αναλαμβάνει το διαμοιρασμό αρχείων μεταξύ συστημάτων, δίχως, όμως, να περιλαμβάνει κάποιο τρόπο πιστοποίησης, έτσι ώστε ο χρήστης που συνδέεται να πιστοποιείται για το αν είναι αυτός που διατείνεται. Προφανώς, το **NFS** αποτελεί προσφιλή στόχο της κοινότητας των εισβολέων.

Όταν σχεδιάζεται λογισμικό χωρίς να περιλαμβάνεται η ασφάλεια στις αρχικές του προδιαγραφές, ενδέχεται το τμήμα που προστίθεται εκ των υστέρων για την προστασία των χρηστών, να μην έχει την αναμενόμενη αλληλεπίδραση και να προκύπτουν νέα ευάλωτα σημεία.

**2)** Αδυναμίες στην υλοποίηση του λογισμικού ή πρωτοκόλλου

Σε περίπτωση που το πρωτόκολλο έχει σχεδιαστεί σωστά, υπάρχει πιθανότητα να προκύπτουν τρωτά σημεία από τον τρόπο υλοποίησής του. Παραδείγματος χάριν, ένα πρωτόκολλο για ηλεκτρονικό ταχυδρομείο μπορεί να υλοποιηθεί με τέτοιο τρόπο που να επιτρέπει τη σύνδεση στο **mail port** του συστήματος που θα γίνει επίθεση και να ζητήσει να εκτελέσει συγκεκριμένες εντολές. Ο εισβολέας μπορεί να γράψει στο πεδίο **«**To:**»**, αντί τη σωστή διεύθυνση, συγκεκριμένες εντολές και να

ζητήσει το **password file** του συστήματος, δίχως να χρειάζεται καν λογαριασμός σε αυτό.

Όσον αφορά το λογισμικό, αυτό μπορεί να περιέχει ευάλωτα σημεία, επειδή δε βρέθηκαν πριν την τελική του έκδοση. Οι εισβολείς αναζητούν ελαττώματα με ειδικά εργαλεία σε περιπτώσεις όπως:

- Ø Ανυπαρξία ελέγχων για το περιεχόμενο και το μέγεθος των δεδομένων
- Ø Ανυπαρξία ελέγχων για την αντιμετώπιση εσωτερικών λαθών
- Ø Ελλιπής έλεγχος του λειτουργικού περιβάλλοντος
- Ø Ανάρμοστη χρήση κλήσεων του συστήματος
- Ø Αδυναμία προσαρμογής σε εξάντληση πόρων
- Ø Ανταγωνιστικές καταστάσεις στην προσπέλαση αρχείων
- Ø Χρήση τμημάτων του λογισμικού για άλλο σκοπό από αυτό, για τον οποίο σχεδιάστηκαν

Εκμεταλλευόμενοι αδυναμίες του λογισμικού, οι εισβολείς μπορούν να αποκτήσουν πρόσβαση στο σύστημα, χωρίς την απαραίτητη εξουσιοδότηση.

**3)** Αδυναμίες στη διαμόρφωση των συστημάτων και των δικτύων

Τα προβλήματα, σε αυτή την περίπτωση προέρχονται από τον τρόπο εγκατάστασης και χρήσης των δομικών στοιχείων. Οι παράμετροι εγκατάστασης του συστήματος είναι προκαθορισμένες, γεγονός που οι εισβολείς γνωρίζουν και εκμεταλλεύονται. Ένα παράδειγμα αυτής της κατηγορίας είναι το γνωστό **File Transfer Protocol (FTP – Πρωτόκολλο Μεταφοράς Αρχείων)[18],** στο οποίο οι εισβολείς συχνά εκμεταλλεύονται την ανώνυμη χρήση του. Η ασφαλής διαμόρφωση της συγκεκριμένης υπηρεσίας υπαγορεύει τη χρήση **password file,** τα βοηθητικά προγράμματα και τα αρχεία δεδομένων να βρίσκονται σε διαφορετική θέση στο σύστημα από το υπόλοιπο λειτουργικό και αυτό να μην μπορεί να προσπελαστεί από το χώρο αποθήκευσης του **FTP.** Αν κάποιος δικτυακός τόπος δεν προσέξει τη διαμόρφωση του **ftp server**¸ μη εξουσιοδοτημένοι χρήστες μπορούν να βρουν πληροφορίες πιστοποίησης και να αποκτήσουν κατά αυτό τον τρόπο πρόσβαση.

Τα τρωτά αυτά σημεία των συστημάτων έρχονται να εκμεταλλευτούν τα διαφορά είδη του κακόβουλου λογισμικού που θα εξετάσουμε σε αυτό το κεφάλαιο.

## 4.3 Malware

Ένας ενδεδειγμένος τρόπος για την προσβολή ενός συστήματος είναι η χρήση του λεγόμενου κακόβουλου κώδικα **(malicious code)[46,137].** Ο **Malicious code** είναι

οποιοσδήποτε κώδικας που προστίθεται, αλλάζεται, ή αφαιρείται από ένα σύστημα λογισμικού προκειμένου να προκληθεί σκόπιμα ζημιά ή να υπονομεύθει η προοριζόμενη λειτουργία του συστήματος χωρίς την συγκατάθεση του ιδιοκτήτη. Πρόκειται για μια σύνθεση των λέξεων κακόβουλου και λογισμικού και είναι ένας γενικός όρος που χρησιμοποιείται για τον προσδιορισμό ποικίλων μορφών εχθρικού, παρεισφρητικού, ή ενοχλητικού κώδικα λογισμικού ή προγράμματος. Αν και το πρόβλημα του **malicious code** έχει μια μακροχρόνια ιστορία, διάφορες πρόσφατες, ευρέως κοινοποιημένες επιθέσεις και ορισμένες οικονομικές τάσεις υποδεικνύουν ότι ο **malicious code** γίνεται γρήγορα ένα κρίσιμο πρόβλημα για τη βιομηχανία, την κυβέρνηση και για τους ιδιώτες.

Το **Malware** περιλαμβάνει τους ιούς υπολογιστών, τα σκουλήκια, τα τρωικά άλογα **(Trojan horses) [47],** τα περισσότερα **rootkits, spyware[44], adware [112],** καθώς και κάθε άλλο κακόβουλο και ανεπιθύμητο λογισμικό.

Μερικά παραδείγματα **malicious code** παρουσιάζονται στην συνέχεια. Θα πρέπει να σημειωθεί ότι οι πρόσφατες εκδόσεις του **malicious code** είναι πραγματικά συγχωνεύσεις των διάφορων κατηγοριών.

Ø **Love Bug (2000).** Ο ιός αυτός κατατάσεται στην κατηγορία **Mobile Code virus** και ήταν ο γρηγορότερος ιός όλων των εποχών, χρησιμοποίησε το **VB script** και το ταχυδρομείο της **Microsoft Outlook** για να διαδοθεί. Προκάλεσε, κατ' εκτίμηση, **10**δις δολλάρια ζημία.

Ø **Melissa (1999).** Και αυτός ο ιός αυτός κατατάσεται στην κατηγορία **Mobile Code virus** και ήταν ο δεύτερος γρηγορότερος ιός ο οπόιος χρησιμοποίησε το ηλεκτρονικό ταχυδρομείο. Μπόρεσε να μολύνει πάνω από **1,2** εκατομμύριο μηχανές σε μερικές ώρες.

Ø **Explore.Zip (1999).** Πρόκειται για ένα **worm (Mobile Code worm)** σε ηλεκτρονικό ταχυδρομείο που εκμεταλλεύτηκε τα προβλήματα στα **Windows** της **Microsoft** για να διαδοθεί.

Ø **Happy99 (1999).** Αποτέλεσε ένα ευρέως διαδεδομένο ιό που μόλυνε **Microsoft PCs.**

Ø **CIH (1998).** Ήταν ένας ιδιαίτερα επικίνδυνος ιός που επιτίθετο στο **BIOS** των **PCs.** Μόλυνε κυρίως Ασιατικές χώρες.

Ø **Back orifice (1998).** Πρόκειται για κακόβουλο λογισμικό τύπου **(Offensive code)** και αποτελούσε πρόγραμμα τηλεχειρισμού εγκατεστημένο στις μηχανές των **Windows** από **crackers.** Διαβρωτικός.

Ø **Attack scripts (1997).** Πρόκειται για κακόβουλο λογισμικό τύπου **(Offensive code)** τον οποίο οι αποκαλούμενοι **"script kiddies"** κατεβάζουν τον **malicious code** από το **Internet** και τον τρέχουν εναντίον οποιουδήποτε στόχου. Κάποιος **crackers** πρέπει να δημιουργήσει και να διαδώσει το **script** για να γίνει η αρχή. Πιο κοινή επίθεση **:** υπερχείλιση καταχωρητών.

Ø **ActiveX (1997).** Επικριθέν από τους επαγγελματίες ασφάλειας, το σύστημα **ActiveX** της **Microsoft** εισάγει σοβαρούς κινδύνους ασφάλειας με τη στήριξη του χρήστη.

Ø **Java attack Applets (1996-1999).** Τα **applets** επίθεσης που τοποθετούνται στους ιστότοπους εκμεταλλεύονται τις 'ρωγμές' **(**κενά ασφαλείας**)** στο πρότυπο ασφάλειας της **Java** για να πραγματοποιήσουν τις επιθέσεις**. 17** γνωστές επιθέσεις.

Ø **Morris worm (1998).** Απελευθερώθηκε το **1988** από **Robert Morris,** και συνέτριψε περίπου **6000** υπολογιστές **(**περίπου **10%** του **Internet** της εποχής**).**

Ø **Thompson's compiler trick (1984).** Το **Ken Thompson** εισήγαγε έναν Δούρειο ίππο σε έναν **C** μεταγλωττιστή που **«**έτρεχε**»** τον εαυτό του σε μελλοντικά προγράμματα.

### 4.3.1 Ιοί

Θέλοντας να δώσουμε έναν γενικό ορισμό για το τι είναι ένας ιός, θα λέγαμε πως είναι ένα είδος προγράμματος **(**κώδικας**)** που είναι ικανό να δημιουργεί αντίγραφα του εαυτού του **(**πιθανώς τροποποιημένα**)** και εισάγεται σκοπίμως σε κάποιο πρόγραμμα ηλεκτρονικού υπολογιστή ή σε κάποιο σύστημα. Είναι σημαντικό να αναφέρουμε ότι κάθε ιός έχει μία ταυτότητα**/**υπογραφή **(signature)** η οποία δεν είναι τίποτα άλλο από μία σειρά **(string)** από **bytes.**

Ο **Fred Cohen [30,32, 33]** ήταν ο πρώτος που μελέτησε τη συμπεριφορά των ιών συστηματικά. Απέδειξε ότι μόλυνση είναι δυνατόν να υπάρξει όποτε υπάρχει διαμοιράσιμη πληροφορία ή μη ελεγχόμενη ροή πληροφορίας. Αν ένα πρόγραμμα Π που ανήκει στο χρήστη Α είναι μολυσμένο και ένας χρήστης Β το εκτελέσει, τα αρχεία του Β μπορεί να μολυνθούν. Επιπλέον, αν υπάρχει διαδρομή επικοινωνίας από το χρήστη Α στο χρήστη Β και άλλη διαδρομή από το χρήστη Β στο χρήστη Γ, τότε υπάρχει διαδρομή επικοινωνίας από τον Α στον Γ, ακόμη και αν ο Β δεν το γνωρίζει.

Τα βασικά πορίσματα της θεωρητικής ανάλυσης του **Cohen [33]**είναι τα ακόλουθα**:**

Ø Η ένωση οποιουδήποτε συνόλου ιομορφών είναι επίσης ιομορφή.

Ø Το πλήθος των διαφορετικών ιών μιας υπολογιστικής μηχανής είναι άπειρο.

Ø Το πλήθος των προγραμμάτων που δεν είναι ιοί, για μια συγκεκριμένη υπολογιστική μηχανή, είναι άπειρο.

Ø Δεν είναι δυνατόν να σχεδιαστεί υπολογιστική μηχανή ικανή να αποφανθεί αν μια ακολουθία συμβόλων είναι ιός ή όχι απαριθμώντας όλα τα προγράμματα που είναι ιοί ή αποκλείοντας όλα εκείνα που δεν είναι.

Ø Κάθε πρόγραμμα που αντιγράφει τον εαυτό του είναι ιός.

Ø Δεν είναι δυνατή η σχεδίαση ενός προγράμματος το οποίο να αποφαίνεται, σε πεπερασμένο χρόνο, αν μια δεδομένη ακολουθία συμβόλων που αποτελούν ένα πρόγραμμα για μια συγκεκριμένη μηχανή είναι ιός ή όχι.

Ø Η διαπίστωση αν μια δεδομένη ακολουθία συμβόλων που είναι ιός μπορεί να παραχθεί από μια άλλη δεδομένη ακολουθία συμβόλων που επίσης είναι ιός είναι μη επιλύσιμο **(undecidable)** πρόβλημα.

Ø Δεν υπάρχει πρόγραμμα το οποίο να μπορεί να ανιχνεύσει όλους τους ιούς μιας συγκεκριμένης υπολογιστικής μηχανής.

Ø Δεν υπάρχει πρόγραμμα το οποίο να μπορεί να εντοπίσει από ποιο πρόγραμμα–φορέα προκλήθηκε η προσβολή ενός αρχικά απρόσβλητου προγράμματος.

Σύμφωνα με τη θεωρητική ανάλυση του **Cohen[112],** ο μόνος σίγουρος τρόπος για να εμποδίσουμε τη διάδοση μιας μόλυνσης που οφείλεται σε ιό είναι να απαγορεύσουμε την ύπαρξη διαμοιράσιμων πόρων και τη ροή πληροφορίας στο σύστημά μας. Τότε, όμως, στην ουσία θα καταλήξουμε να έχουμε ένα σύστημα που δε λειτουργεί.

Κατά τη διάρκεια της ζωής του ένας ιός περνάει τις εξής τέσσερις φάσεις:

**1**. Φάση ύπνωσης. Κατά τη φάση αυτή ο ιός είναι ανενεργός και αναμένει την πυροδότηση κάποιας λειτουργίας **(**συνθήκης**)** για να ξεκινήσει την διάδοσή του **.** Η ενεργοποίηση αυτή μπορεί να προέλθει από κάποιο γεγονός, όπως την έλευση μιας ημερομηνίας, την παρουσία ενός άλλου προγράμματος ή αρχείου ή την υπέρβαση κάποιου αποθηκευτικού ορίου στο δίσκο. Η φάση αυτή δεν είναι απαραίτητο να υπάρχει σε όλους τους ιούς.

**2**. Φάση διάδοσης. Κατά τη φάση αυτή ο ιός τοποθετεί ένα ακριβές αντίγραφο του εαυτού του σε άλλα προγράμματα ή σε συγκεκριμένες περιοχές του δίσκου. Κάθε μολυσμένο πρόγραμμα θα περιέχει τώρα έναν κλώνο του ιού, ο οποίος με τη σειρά του θα μπει σε φάση διάδοσης.

**3.** Φάση ενεργοποίησης. Ο ιός ενεργοποιείται για να επιτελέσει τη λειτουργία για την οποία έχει σχεδιαστεί. Όπως και με τη φάση διάδοσης, η φάση ενεργοποίησης μπορεί να πυροδοτηθεί από την εμφάνιση κάποιου γεγονότος σχετικού με το σύστημα. Αν και η ποικιλία τέτοιων γεγονότων είναι πολύ μεγάλη, ένα συνηθισμένο τέτοιο γεγονός είναι η δημιουργία συγκεκριμένου αριθμού αντιγράφων του ιού ή η έλευση μιας συγκεκριμένης ημερομηνίας.

**4.** Φάση εκτέλεσης. Η λειτουργία που προβλέπεται στον κώδικα του ιού επιτελείται. Η λειτουργία μπορεί να είναι ουσιαστικά αβλαβής, όπως η απλή εμφάνιση ενός μηνύματος στην οθόνη, ή επιβλαβής, όπως η καταστροφή προγραμμάτων και αρχείων δεδομένων.

#### 4.3.1.1 Ιστορική αναδρομή – οι πρώτοι ιοί

Υπάρχουν πολλές και διαφορετικές απόψεις για το πότε ακριβώς δημιουργήθηκε καθώς και για το ποιος ήταν ο πρώτος ιός. Είναι ωστόσο γνωστό ότι οι **Univac 1108** και **IBM 360/370[32]** είχαν δεχθεί ιούς **(**συγκεκριμένα τους **"Pervading Animal"** και **"Christmas tree")** οπότε μπορούμε να πούμε σχεδόν σίγουρα πως ο πρώτος ιός δημιουργήθηκε κάπου στις αρχές του **1970 (**παρόλο που ο όρος **«**ιός**»** ήρθε πολύ αργότερα **–**πιθανόν το **1983** από τον **Fred Cohen (University of Southern California)- ).** Την περίοδο εκείνη **(**τέλη του **1960** με αρχές του **1970)** έκαναν περιοδικά την εμφάνισή τους διάφορα προγράμματα με την ονομασία **the Rabbit,** τα οποία κλωνοποιούσαν τον εαυτό τους, και καταλάμβαναν πόρους του συστήματος μειώνοντας κατά συνέπεια την παραγωγικότητα του. Αυτά πιθανότατα δεν αντιγράφονταν από σύστημα σε σύστημα και ήταν αυστηρά τοπικά φαινόμενα **(**λάθη ή φάρσες από τους προγραμματιστές συστημάτων που συντηρούσαν αυτούς τους υπολογιστές**).** Το πρώτο περιστατικό που θα μπορούσε να ονομαστεί **«**επιδημία ενός ιού υπολογιστών**»** συνέβη στον **Univac 1108** και ήταν ο **"Pervading Animal"** ο οποίος συγχωνευόταν στο τέλος εκτελέσιμων αρχείων.

Το πρώτο πρόγραμμα καταπολέμησης ιών **(anti-virus)** ήρθε στις αρχές της δεκαετίας του **'70** όταν μετά την εμφάνιση του ιού **Creeper (**τα συστήματα στα οποία είχε εισχωρήσει τύπωναν το μήνυμα**: 'I'M THE CREEPER : CATCH ME IF YOU CAN.')** στο **Arpanet** δημιουργήθηκε ο **Reaper** ο οποίος ήταν ουσιαστικά ένας νέος ιός ο οποίος διαδιδόταν μέσα από το δίκτυο και όταν έβρισκε κάποιον υπολογιστή μολυσμένο από τον **Creeper** έσβηνε τον ιό. Το **1981** κάνει την εμφάνισή του ο **elk-cloner (**ο οποίος δημιουργήθηκε από έναν **15**χρονο μαθητή**)** που δρούσε στους **Apple II** υπολογιστές**,** ενώ ο πρώτος ιός για **IBM-PC** ήρθε το **1986,** ο λεγόμενος **Brain virus [32]** που προκάλεσε πανδημία. Ο τελευταίος ο οποίος σύμφωνα με τα λεγόμενα των δημιουργών του **(**δύο αδέλφια από το Πακιστάν**)** είχε σαν σκοπό την

μέτρηση της «πειρατείας» στην χώρα τους, εξαπλώθηκε στιγμιαία σε ολόκληρο τον κόσμο και ήταν ο πρώτος που είχε **stealth** ικανότητες.

| Χρονολογίες | Εξέλιξη |
|---|---|
| 1987-1990 | Εμφάνιση των πρώτων ιών που μεταδίδονταν με τη βοήθεια των δισκετών (μέσω της περιοχής εκκίνησης των δισκετών) |
| 1990-1995 | Άρχισαν να μεταδίδονται οι ιοί με τη βοήθεια των αρχείων. |
| 1995-1998 | Εμφάνιση των πρώτων ιών μακρο-εντολών που μεταδίδονταν με τα έγγραφα κειμένου. |
| 1998-2001 | Εμφάνιση των πρώτων ιών τύπου worm που μεταδίδονταν με τα μηνύματα του ηλεκτρονικού ταχυδρομείου. |
| 2001 - ... | Κατακόρυφη αύξηση των ιών που μεταδίδονταν μέσω του διαδικτύου |

**Πίνακας 9. Η εξέλιξη των ιών**

#### 4.3.1.2 Κατηγορίες ιών

Σε γενικές γραμμές υπάρχουν ποικίλοι τρόποι για να κατηγοριοποιήσει κανείς τους ιούς. Ενδεικτικά βλέπουμε μερικές κατηγορίες ιών παρακάτω **[112]:**

- **Boot sector infectors**
- **Macro Viruses**
- **Polymorphic Viruses**

**parasitic (**Παρασιτικοί**).** Ο παραδοσιακός αλλά και πιο διαδεδομένος τύπος ιού. Οι ιοί αυτοί προσαρτώνται σε εκτελέσιμα αρχεία και αναπαράγονται, όταν εκτελεστεί το μολυσμένο πρόγραμμα, βρίσκοντας και άλλα εκτελέσιμα αρχεία για να μολύνουν.

**memory–resident (**Παραμένοντες στη μνήμη**).** Οι ιοί αυτοί εγκαθίστανται στην κύρια μνήμη ως τμήματα προγραμμάτων που παραμένουν στη μνήμη. Από τη στιγμή της εγκατάστασής τους, οι ιοί αυτοί μολύνουν κάθε πρόγραμμα που εκτελείται.

**1. Boot Sector** ιοί

Γενικά χαρακτηριστικά

Οι **boot sector** ιοί **[32,84]** μπορούν να μολύνουν ή να αντικαθιστούν με τον δικό τους κώδικα, τόσο το **DOS boot sector** όσο και το **Master Boot Record (MBR).** Το **MBR** είναι ένα μικρό πρόγραμμα που τρέχει κάθε φορά που ανοίγει ο υπολογιστής, το οποίο έχει στον έλεγχό του το **boot sequence** και καθορίζει από ποιο **partition** θα κάνει εκκίνηση **(boot)** ο υπολογιστής. Γενικά το **MBR** βρίσκεται στο πρώτο τομέα **(sector)** του σκληρού δίσκου. Γίνεται εύκολα αντιληπτό ότι από τη στιγμή που το **MBR** εκτελείται κάθε φορά που ανοίγει ο υπολογιστής, η μόλυνσή του από έναν ιό είναι άκρως επικίνδυνη. Από τη στιγμή που θα μολυνθεί ο κώδικας εκκίνησης του

δίσκου, ο ιός θα φορτώνεται στη μνήμη σε κάθε άνοιγμα του υπολογιστή. Από τη μνήμη ο **boot sector** ιός μπορεί να μολύνει κάθε δίσκο **(local** ή **removable)** που διαβάζεται από το σύστημα. Οι ιοί αυτοί μπορούν να προκαλέσουν μία ποικιλία προβλημάτων ανάκτησης δεδομένων ή και στοιχείων εκκίνησης. Σε κάποιες περιπτώσεις μάλιστα είναι δυνατόν να προκληθεί απώλεια δεδομένων – και μάλιστα από ολόκληρα κομμάτια του δίσκου. Επίσης πολύ συχνά ο υπολογιστής γίνεται ξαφνικά ασταθής, αποτυγχάνει να ξεκινήσει, ή δεν μπορεί να εντοπίσει τον σκληρό δίσκο. Σε τέτοιες περιπτώσεις μηνύματα λάθους όπως: **"invalid system disk"** είναι συχνό φαινόμενο. Η μετάδοση αυτού του είδους ιομορφικού λογισμικού γινόταν συνήθως από μολυσμένα **floppy disks**. Σήμερα η μετάδοσή τους γίνεται κατά βάση μέσω δικτύων **(**και του Διαδικτύου φυσικά**)** από **downloads** αρχείων ή και από μολυσμένα **emails**. Στις περισσότερες των περιπτώσεων όλοι οι δίσκοι **(**με ενεργοποιημένη την εγγραφή στη μνήμη**)** σε έναν μολυσμένο υπολογιστή θα "κωλύσουν" τον ιό.

Μερικοί γνωστοί **boot sector** ιοί είναι **[32]:**

- **Brain**
- **Monkey**
- **NYB (**γνωστός και ως **B1)**
- **Stoned**
- **Form**
- **Michelangelo**

Τρόποι αντιμετώπισης – αντίμετρα

Ένα μεγάλο πρόβλημα με τους ιούς αυτούς είναι η απομάκρυνσή τους, και αυτό γιατί συχνά είναι δύσκολο για ένα **antivirus** πρόγραμμα να καθαρίσει το **MBR** την ώρα που εκτελείται το λειτουργικό σύστημα. Γενικά η πρόληψη είναι θέμα επαγρύπνησης και αποφυγής επαφής με άγνωστους δίσκους. Πέρα από τα γενικά αντίμετρα που θα αναλυθούν στη συνέχεια υπάρχουν κάποιοι τρόποι για να μειώσουμε την πιθανότητα μόλυνσης από έναν **boot sector** ιό **[84].** Καταρχάς είναι δυνατόν να γίνουν κάποιες ρυθμίσεις στο **CMOS (complementary metal oxide semiconductor)** ώστε να μην είναι δυνατή η εγγραφή στον **boot** τομέα του σκληρού δίσκου. Αυτό αν και μπορεί να βοηθήσει κάπως, είναι πιθανόν να δημιουργήσει προβλήματα **(**πχ όταν θελήσουμε να ξανά εγκαταστήσουμε το λειτουργικό μας σύστημα**).** Ακόμη είναι καλό οι διάφοροι **removable** δίσκοι που χρησιμοποιούμε να είναι κλειδωμένοι **(write protected)** και να τους χρησιμοποιούμε μόνο σε υπολογιστές που έχουμε βεβαιωθεί ότι είναι ασφαλείς.

Παραδείγματα **boot sector** ιών

Ο ιός **monkey**

Ο ιός **monkey** είναι ένας **boot sector** ιός που προσβάλλει το **Master Boot Record (MBR)** του σκληρού δίσκου **(**αλλά και το **boot sector** των δισκετών**),** εμφανίστηκε το **1991** στο **Edmonton** του Καναδά**,** και γρήγορα διαδόθηκε στις ΗΠΑ, στην Αυστραλία και την Μεγάλη Βρετανία**. Ο monkey** είναι εκτός των άλλων **stealth** ιός**[111],** από τη στιγμή που καταφέρει να εξαπλωθεί στη μνήμη δεν μπορεί να εντοπιστεί στον σκληρό δίσκο ή σε κάποια δισκέτα**.** Η απομάκρυνσή του παρακωλύεται περαιτέρω από το γεγονός ότι δεν υπάρχει πρόσβαση στον σκληρό δίσκο αν προσπαθήσουμε να επανεκκινήσουμε το σύστημα χρησιμοποιώντας κάποια δισκέτα εκκίνησης αφού λαμβάνουμε μηνύματα του τύπου**: "Invalid drive specification".** Ο τρόπος διάδοσης του είναι να προσπαθήσουμε να κάνουμε **boot** το σύστημα με μία δισκέτα που είναι μολυσμένη**.** Σε αυτή τη περίπτωση αυτό που θα συμβεί είναι ότι θα προσπαθήσει το σύστημα να ξεκινήσει**,** διαβάζοντας την δισκέτα **(**για να δει εάν είναι **boot** δισκέτα**)** και θα τυπώσει το κλασικό μήνυμα**: "Non-system disk or disk error".** Από τη στιγμή αυτή ο ιός έχει εισβάλει στον υπολογιστή πρώτα στο **MBR** και έπειτα στη μνήμη**.** Αυτό που συμβαίνει σε ένα σύστημα που έχει μολυνθεί από τον ιό πρακτικά είναι ότι όλο το σύστημα και η διαθέσιμη μνήμη μειώνεται κατά **1,024 bytes.** Η εκκαθάριση τελικά του ιού μπορεί να γίνει είτε με την χρήση κάποιου **antivirus** προγράμματος **(**αναγκαστικά μέσω κάποιας δισκέτας εκκίνησης**)** είτε με τη χρήση εργαλείων **FDISK (**όπως πχ το **Norton Disk Doctor)** που μπορούν να ξαναφτιάξουν **(**να κάνουν**"rebuild")** το **Master Boot Sector.** Επίσης είναι δυνατόν να επαναφέρουμε τις αρχικές ρυθμίσεις του πρωτότυπου **Master Boot Record** και του **partition table** εάν έχει γίνει **backup** πριν την μόλυνση**.**

Ο ιός **NYB (** ή B**1 )**

Ο ιός **NYB (New York boot)** είναι ένας τυπικός **Boot Sector (**εμφανίστηκε κάπου στα τέλη του **1994),** ο οποίος μολύνει όπως και ο **monkey** μόνο αν προσπαθήσουμε να κάνουμε εκκίνηση ενός συστήματος με μία μολυσμένη δισκέτα**.** Εκείνη τη στιγμή ο ιός περνάει στο **Main Boot Record** και στη συνέχεια **"**κατοικεί**"** στην **high dos** μνήμη σε κάθε επανεκκίνηση του υπολογιστή**.** Ο **NYB** είναι και αυτός ένας **stealth** ιός οπότε οι διάφορες

αλλαγές στο **MBR** δεν είναι ορατές**.** Κάθε φορά που έχουμε πρόσβαση στη δισκέτα υπάρχει **1/512** πιθανότητα να ενεργοποιηθεί ο ιός**.** Τότε υπάρχει η περίπτωση να καταστραφεί η κεφαλή της δισκέτας **(**και επομένως και η ίδια η δισκέτα**).** Τέλος ενδιαφέρον έχει ότι από τους περισσότερους μελετητές των ιών **"**ξέφυγε**",** ένας άλλος τρόπος ενεργοποίησης του**.** Έτσι το σύστημα μπορεί συντριβή εάν επιχειρηθεί

εγγραφή όταν το ρολόι του υπολογιστή έχει όλα τα πεδία μηδέν **(**όταν δηλαδή είναι μεσάνυχτα**).**

**2.** Πολυμορφικοί **(Polymorphic)** ιοί

Γενικά χαρακτηριστικά

Πολυμορφικός ιός είναι αυτός που παράγει μία μεγάλη ποικιλία από διαφορετικά αντίγραφα του εαυτού του **[116] (**τα οποία είναι λειτουργικά**).** Η στρατηγική υποθέτει ότι το αντιικό πρόγραμμα δεν θα μπορέσει να εντοπίσει όλα τα διαφορετικά στιγμιότυπα του ιού**.** Ένας τρόπος για την αποφυγή ανίχνευσης είναι η κρυπτογράφηση του εαυτού τους **(selfencryption)** με ένα μεταβλητό κλειδί**.** Κάποιοι πιο εξελιγμένοι πολυμορφικοί ιοί **(**πχ **V2p6)** ωστόσο αλλάζουν τις ακολουθίες οδηγιών μέσα στις μεταβλητές τους με το να παραβάλουν τις οδηγίες κρυπτογράφησης με **"**θορυβώδη**" (noise)** οδηγίες, με το να εναλλάσσουν αμοιβαία ανεξάρτητες οδηγίες**,** ή ακόμα και με τη χρησιμοποίηση ποικίλων συχνοτήτων οδηγιών με πανομοιότυπα **net effects.** Μία από τις πιο εξελιγμένες μορφές πολυμορφισμού που χρησιμοποιείται είναι η **Dark Angel's Multiple Encryptor(DAME),** που εμφανίζεται με μία μορφή **object module (**άλλες γεννήτριες πολυμορφικότητας είναι οι**: MTE, TPE, NED** κα**).** Με τη βοήθειά της**,** οποιοσδήποτε ιός μπορεί να γίνει πολυμορφικός με το να προσθέσει συγκεκριμένες κλήσεις στον **assembly** κώδικά του και συνδέοντας τον με την **DAME** και γεννήτριες τυχαίων αριθμών**.** Η εμφάνιση των πολυμορφικών ιών μετέτρεψε την επιστήμη της ανίχνευσης των ιών σε ένα εξαιρετικά δύσκολο και ακριβό εγχείρημα**.** Αυτό δεν σημαίνει απαραίτητα ότι οι πολυμορφικοί ιοί είναι οι πιο καταστροφικοί **(**υπάρχουν απλοί ιοί που μπορούν να σβήσουν όλα τα δεδομένα από τον σκληρό δίσκο **(format)** ή να δημιουργήσουν μεγάλα προβλήματα στο **BIOS).** Το μεγάλο πλεονέκτημά τους είναι η δυσκολία εντοπισμού τους**.** Η απλή πρόσθεση όλο και περισσότερων συμβολοσειρών **(strings)** αναζήτησης σε απλούς ανιχνευτές είναι προφανές ότι δεν μπορεί πάντα να επιλύσει επαρκώς το πρόβλημα**,** αφού πλέον είναι δυνατόν να μην υπάρχει ένα συγκεκριμένο **string** από **bytes** που να ταυτοποιεί τον ιό**.**

Μερικοί πολυμορφικοί ιοί είναι **[116]:**

- **Chameleon (**από τους πρώτους πολυμορφικούς**)**
- **Bootache**
- **CivilWar**
- **Uruguay**
- **MVF**

- **Moctezuma**
- **PcFly**

Τρόποι αντιμετώπισης – αντίμετρα

Οι τρόποι που χρησιμοποιούνται από τα διάφορα **antivirus** προγράμματα για την ανίχνευση πολυμορφικών ιών ποικίλουν. Οι συνηθέστεροι είναι **[116]:**

- **Scan Strings**
- **Variable Scan Strings**
- **Cryptanalysis**
- **Generic Decryptor**
- **Heuristic analysis**

Το απλό **Scan String (**αναζήτηση συμβολοσειράς**)** είναι η ανίχνευση για συγκεκριμένες ακολουθίες από **bytes.** Πχ.το **scan string** που είναι της μορφής**: aa ?? bb ?? cc** μπορεί να εντοπίσει ιούς μόνο της μορφής**: aa xx bb xx cc.** Το **Variable Scan String (**μεταβλητή αναζήτηση συμβολοσειράς**)** είναι μία βελτίωση του παραπάνω που λειτουργεί με δυναμικό τρόπο. Πχ. το **scan string** που είναι της μορφής**: aa * bb * cc** Μπορεί να εντοπίζει ιούς των μορφών**: aa xx xx bb xx xx xx xx cc** ή **aa bb xx xx xx cc** κτλ.

Η κρυπτανάλυση **(Cryptanalysis)** λειτουργεί με το να εντοπίζει ένα μέρος από το σώμα του ιού**,** να εκτελεί μία βασική κρυπτανάλυση πάνω σε αυτό και τελικά εάν είναι επιτυχής να τον εντοπίζει**.**

Το **Generic Decryptor (**Γενικός Αποκρυπτογράφος**)** λειτουργεί με το να προσομοιώνει οδηγίες σε έναν πολυμορφικό αποκρυπτογράφο με σκοπό να αναγκάσει τον ιό να αποκρυπτογραφηθεί μόνος του και στην συνέχεια τον εντοπίζει με μία απλή αναζήτηση συμβολοσειράς**.**

Η **Heuristic analysis –**ευριστική ανάλυση**- (**από τα πιο δυνατά όπλα των **antivirus** προγραμμάτων**)** αναζητούν αντιφατικότητες μεταξύ του κώδικα που αναλύεται και του κώδικα που πρέπει να έχει κανονικά ένα πρόγραμμα**.**

Παραδείγματα πολυμορφικών ιών

Ο **MVF** ιός

Ο **MVF (**ή και **Arkanoid)** είναι ένας πολυμορφικός ιός που εμφανίστηκε το **1992** στη Ρωσία**,** και έχει σαν στόχο τα **.COM** αρχεία **(**συμπεριλαμβανομένου του **COMMAND.COM).** Από τη στιγμή που ένα μολυσμένο πρόγραμμα εκτελεστεί ο **MVF** εγκαθίσταται στην μνήμη ως **TSR (terminate and stay resident).** Από τη στιγμή που

βρίσκεται ο ιός στη μνήμη θα μολύνει κάθε **.COM** πρόγραμμα που εκτελείται. Προγράμματα μολυσμένα με τον ιό θα έχουν μία αύξηση μεγέθους της τάξης των **1,898** με **1,909 bytes** με τον **MVF** να βρίσκεται στο τέλος του αρχείου. Αξιοσημείωτο είναι ότι μέσα στον κώδικα του ιού βρίσκεται κρυπτογραφημένο το παρακάτω κείμενο **(**το οποίο δεν εμφανίζεται στα μολυσμένα αρχεία**):**

---

**"????????COM"**

**"THE MVF-FILEVIRUS"**

**"Programmed 1991 by the MVF"**

**"MAD Virus Factory"**

**"No.0001"**

**"*.COM"**

---

Στα συστήματα στα οποία έχει εισχωρήσει ο **MVF** είναι πιθανόν να παρατηρούνται καθυστερήσεις στην εκτέλεση **.COM** αρχείων **(**αυτό συμβαίνει πολύ συχνά όταν έχει μολυνθεί το **COMMAND.COM).**

**3.** Οι **Macro** ιοί

Γενικά χαρακτηριστικά

Γενικά**,** οι μακροεντολές **[46]**μπορούν να χρησιμοποιηθούν σε προγράμματα όπως το **Word** και το **Excel,** για να αυτοματοποιήσουν σύνθετους ή επαναλαμβανόμενους στόχους**.** Μόλις γραφτούν, ορίζεται σε αυτές ένας συνδυασμός πλήκτρων**,** ή κάποιο κουμπί από μία εργαλειοθήκη που θα ενεργοποιεί την μακροεντολή**.** Οι μακροεντολές αποθηκεύονται σαν μία σειρά οδηγιών σε μία γλώσσα όπως η **visual basic.** Από τη στιγμή που καταγραφεί μια μακροεντολή ο χρήστης μπορεί να την επεξεργαστεί ή ακόμα και να προσθέσει πιο περίπλοκες εντολές που δεν είναι κανονικά εγγράψιμες**.** Αυτό δίνει στον έμπειρο χρήστη τη δυνατότητα όχι μόνο να αυτοματοποιήσει λειτουργίες μέσα στο πρόγραμμα αλλά και να εκτελεί βασικές εντολές του συστήματος όπως διαγραφή**,** μετονομασία**,** ή αλλαγή των ιδιοτήτων αρχείων**.** Ένας μακροιός χρησιμοποιεί την δύναμη και την λειτουργικότητα των μακροεντολών για να δημιουργήσει αντίγραφα του εαυτού του και για να διαδοθεί**.** Όταν ένας χρήστης λαμβάνει και ανοίγει ένα αρχείο που περιέχει έναν μακροϊό**,** αυτός **(**ο ιός**)** είτε θα εκτελεστεί αυτόματα είτε από τον συνδυασμό κάποιων πλήκτρων**,** την εκτέλεση κάποιας εντολής από το **menu** επιλογών**,** το πάτημα κάποιου κουμπιού μιας εργαλειοθήκης κτλ**.** Στη συνέχεια ο ιός θα αντιγραφτεί στο σύστημα **(**ο τρόπος μπορεί να ποικίλει ανάλογα με τις λεπτομέρειες του ιού**).** Ο **macro** ιός θα είναι παρών πλέον στα αρχεία που ανοίγει ο χρήστης και μπορεί να μεταδοθεί με πολλούς διαφορετικούς τρόπους**.** Μερικά πολύ επικίνδυνα πράγματα

που μπορεί να κάνει ένας τέτοιος ιός είναι να διαγράψει/τροποποιήσει τα περιεχόμενα ενός κειμένου, να αλλάξει τις ρυθμίσεις του **Word,** να τοποθετήσει κωδικό πρόσβασης, να αντιγράψει έναν **DOS** ιό στο σύστημα ή και να παρεμβάλει επιβλαβής γραμμές κώδικα στα αρχεία **config.sys** και **autoexec.bat.** Θεωρητικά ένας μακροϊός μπορεί να γραφτεί για οποιοδήποτε πρόγραμμα που αποθηκεύει μακροεντολές σε μορφή που μπορεί να ανοιχτεί και να επεξεργαστεί χρησιμοποιώντας μία γλώσσα όπως **Word Basic** και **Visual Basic.** Στην πράξη ωστόσο οι περισσότεροι που έχουν βρεθεί αφορούν κυρίως το **Word** και το **Excel.**

Μία άλλη ενδιαφέρουσα ιδιότητα των μακροϊών είναι ότι μπορούν ενδεχομένως να διαδίδονται σε διαφορετικές πλατφόρμες, όπως από **Mac** σε **PC** κα. Οι **macro** ιοί υφίστανται και μεταδίδονται μέσα στο περιβάλλον κάθε εφαρμογής το οποίο για τις μακρο εντολές είναι κοινό στις διαφορετικές πλατφόρμες. Οι διάφοροι ιοί που προσπαθούν να προκαλέσουν ζημιά σε ένα μέρος του συστήματος του χρήστη έξω από το **word** δεν θα είναι σε θέση να κάνουν το ίδιο πράγμα σε μία διαφορετική πλατφόρμα **(**Πχ. ένας μακροϊός που προσπαθεί να επεξεργαστεί το αρχείο **config.sys** του χρήστη σε ένα **pc** θα δυσκολευτεί να κάνει το ίδιο πράγμα σε έναν **Mac,** ο οποίος δεν έχει κανένα αρχείο **Config.sys.).** Συνοψίζοντας δηλαδή ένας μακροϊός που διαδίδεται και μπορεί να προκαλεί βλάβες σε ένα σύστημα, μπορεί να διαδίδεται σε κάποιο άλλο, αλλά να μην προκαλεί κάποια βλάβη. Υπάρχει η δυνατότητα βέβαια ένας **macro** ιός να βρίσκει-εντοπίζει σε ποιο σύστημα τρέχει **(**αν είναι **pc,mac** ή κάτι άλλο**)** και να αλλάζει την συμπεριφορά του ανάλογα, όμως κάτι τέτοιο δεν είναι σύνηθες.

Παραδείγματα μακρο ιών αποτελούν **[46]:**

- **Concept (**από τους πρώτους που εμφανίστηκαν **-1995)**
- **Melissa**
- **DMV**
- **Nuclear**
- **NiceDay**
- **Groov**

Τρόποι αντιμετώπισης – αντίμετρα

Όταν τον Αύγουστο του **1995** έκανε την εμφάνιση του ο πρώτος μακροϊός στην πραγματικότητα δεν ήταν ο πρώτος, αφού κάποιες εταιρίες αντιβιοτικών είχαν πειραματικά δημιουργήσει ιούς που μεταδίδονταν από ένα κείμενο στο άλλο, ωστόσο σχεδόν κανείς δεν ενδιαφέρθηκε για αυτό το μάλλον αποτυχημένο πείραμα- η αντιική κοινότητα βρέθηκε απροετοίμαστη. Αξιοσημείωτο μάλιστα είναι

ότι αν παρατηρούσε κανείς την τότε βιβλιογραφία σε σχέση με τους ιούς θα έβλεπε ότι στην ερώτηση, αν μπορεί ένα κείμενο να περιέχει κάποιον ιό, η απάντηση ήταν απλή: ΟΧΙ. Έτσι η πρώτη βιαστική αντιμετώπιση της επιδημίας μακροϊών που προέκυψε ήταν η δημιουργία άλλων ιών που μεταδίδονταν από κείμενο σε κείμενο και έσβηναν τις κακόβουλες μακροεντολές. Οι τρόποι για την ανίχνευση των μακροϊών πλέον ποικίλουν. Ένας πολύ απλός είναι με την ανίχνευση του ονόματος του ιού. Επίσης επειδή ένα μεγάλο μέρος των νέων ιών που κυκλοφορούν είναι ουσιαστικά "αλλαγμένες" εκδόσεις παλιών, είναι δυνατόν να γίνεται η ανίχνευση με βάση το βασικό σώμα ενός ιού. Τέλος χρησιμοποιείται και η ευριστική ανάλυση που είδαμε παραπάνω.

Παραδείγματα μακρο ιών

Ο ιός **Concept**

**Ο** ιός **concept [137,46]** εμφανίστηκε για πρώτη φορά το **1995** και είχε σαν στόχους το **Microsoft word (windows) 6.x** και **7.x,** το **word for macintosh 6.x** καθώς και τα ίδια τα λειτουργικά συστήματα **windows 95** και **windows nt. Ο** ιός εκτελείται κάθε φορά που ανοίγει ένα μολυσμένο έγγραφο και προσπαθεί να μολύνει το **NORMAL.DOT.** Αν εντοπίσει κάποια από τις μακρο εντολές **"payload"** ή **"filesaveas"** υποθέτει ότι ο ιός υπάρχει ήδη οπότε σταματάει την λειτουργία του. Αν όμως δεν βρει τις παραπάνω εντολές τότε αρχίζει να γράφει τις κακόβουλες εντολές και εμφανίζει ένα μικρό μήνυμα στην οθόνη: Το μήνυμα αυτό εμφανίζεται μόνο κατά την αρχική μόλυνση του **NORMAL.DOT.** Από τη στιγμή αυτή ο ιός περνάει σε κάθε κείμενο που δημιουργήθηκε με την **"Save As"** εντολή. Ο **concept** αποτελείται από τις ακόλουθες μακρο εντολές:

```
AAAZAO

AAAZFS

AutoOpen

FileSaveAs

PayLoad
```

Να παρατηρήσουμε εδώ ότι η **AutoOpen** και η **FileSaveAs** είναι ονόματα που υπάρχουν και υπό φυσιολογικές συνθήκες στο **word. Το PayLoad** που βλέπουμε παραπάνω περιέχει το εξής κείμενο:

```
Sub MAIN

REM That's enough to prove my point

End Sub
```

Το οποίο δεν εκτελείται ποτέ.

Ο ιός **Melissa**

Ο ιός **Melissa [46]** έκανε την εμφάνισή του την Παρασκευή **26** Μαρτίου **1999** και μπόρεσε να διαδοθεί σε ολόκληρο τον κόσμο μέσα σε μερικές ώρες –κάτι που δεν είχε ξανασυμβεί μέχρι τότε. Εξαπλώθηκε με το να στέλνει αυτόματα σε **email** τον εαυτό του από τον ένα χρήστη στον άλλο. Όταν ο ιός ενεργοποιηθεί τροποποιεί τα έγγραφα του χρήστη παρεμβάλλοντας κάποια σχόλια από μία γνωστή τηλεοπτική σειρά **("The Simpsons").** Ανησυχητικό είναι το γεγονός ότι μπορεί να στείλει και εμπιστευτικές πληροφορίες ενός χρήστη σε έναν άλλο. Ο ιός "χτύπησε" μεγάλους οργανισμούς όπως η **Microsoft** και η **Intel,** η **Microsoft** μάλιστα αναγκάστηκε να κλείσει τελείως το σύστημα ηλεκτρονικού ταχυδρομείου της για να σταματήσει την περεταίρω εξάπλωση του ιού. Ο **Melissa** αρχικά μεταδόθηκε σε φόρουμ συζητήσεων **(alt.sex).** Ο ιός εστάλη στους χρήστες με το όνομα **LIST.DOC** που περιείχε κωδικούς πρόσβασης από ιστοσελίδες που είχαν χαρακτηριστεί **X-rated (**σεξουαλικού περιεχομένου**).** Όταν κάποιος άνοιγε το αρχείο**,** ο μακρο ιός εκτελείτο και έστελνε το **LIST.DOC** με **email** σε **50** άτομα από το **address book** του χρήστη. Το **email** είχε την μορφή**:**

---

**From: (name of infected user)**

**Subject: Important Message From (name of infected user)**

**To: (50 names from alias list)**

**Here is that document you asked for ... don't show anyone else ;-)**

**(Attachment: LIST.DOC)**

---

Ο **Melissa** ενεργοποιείται αν εκτελεστεί τα λεπτά από το ρολόι του συστήματος συμπίπτουν με την ημερομηνία **(**πχ **18:27** στις **27** κάποιου μήνα**).**Σε αυτή τη περίπτωση ο ιός παρέμβαλλε στα κείμενα του μολυσμένου υπολογιστή το παρακάτω κείμενο**:**

**"Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here". This text, as well as the alias name of the author of the virus, "Kwyjibo", are all references to the popular cartoon TV series called "The Simpsons".**

Γενικά αντίμετρα

Υπάρχουν μερικοί τρόποι για να μειώσουμε την πιθανότητα να "κολλήσει" το σύστημά μας έναν ιό και να αυξήσουμε το ενδεχόμενο να καθαρίσει "σωστά" εάν προσβληθεί**.**

Ø Εγκατάσταση ενός **antivirus** προγράμματος, τακτική ενημέρωσή του και ένας τουλάχιστον έλεγχος του συστήματος κάθε εβδομάδα.

Ø Δημιουργία **backup** αρχείων. Πολύ σημαντικό αφού μας εγγυάται την ασφάλεια των δεδομένων μας και για άλλα εκτός των ιών ενδεχόμενα όπως για παράδειγμα πρόβλημα με τον σκληρό δίσκο.

Ø Χρήση κάποιου **Firewall**

Ø Ενημέρωση των χρηστών ενός συστήματος για τον κίνδυνο των ιών και το πώς μπορούν να προφυλαχθούν.

Ø Χρήση πιο ασφαλών λειτουργικών συστημάτων

Είναι γεγονός ότι οι περισσότεροι δημιουργοί ιών στοχεύουν κατά του λογισμικού της **Microsoft.**

### 4.3.2 WORMS

Ένα **worm [8,10,11]** είναι ένα αυτοαναπαραγώμενο πρόγραμμα ηλεκτρονικού υπολογιστή το οποίο χρησιμοποιεί το δίκτυο για να στείλει αντίγραφα του εαυτού του σε άλλους κόμβους **(**υπολογιστές στο δίκτυο**)** χωρίς να είναι αναγκαία κάποια παρέμβαση από το χρήστη. Σε αντίθεση με τους ιούς, δεν χρειάζεται να προσκολλάται σε ένα υπάρχων πρόγραμμα. Τα **Worms** σχεδόν πάντα προκαλούν βλάβες στο δίκτυο, έστω και μόνο από την κατανάλωση εύρους ζώνης, σε αντιδιαστολή με τους ιούς που σχεδόν πάντα καταστρέφουν ή τροποποιούν τα αρχεία στον υπολογιστή που έχουν στοχεύσει.

Η ονομασία των **worm** προέρχεται από ένα επιστημονικής φαντασίας μυθιστόρημα με τίτλο **The Shockwave Rider** το οποίο δημοσιεύτηκε το **1975** από τον **John Brunner.** Οι ερευνητές **John F Shock** και **John Hupp [111]** της **Xerox PARC** ήταν οι πρώτοι που χρησιμοποίησαν αυτό το όνομα σε ένα έγγραφο που δημοσίευσαν το **1982, (The Worm Programs, Comm ACM, 25(3):172-180, 1982)** και έκτοτε έχει υιοθετηθεί ευρέως. Επίσης ήταν και οι δύο πρώτοι ερευνητές που υλοποίησαν ένα **worm** το **1978**. Οι **Shoch** και **Hupp** κατασκεύασαν αρχικά ένα **worm** με σκοπό να εντοπίζει τους αδρανής επεξεργαστές στο δίκτυο και να τους αναθέτει εργασίες, ισοκατανέμοντας κατ' αυτό τον τρόπο το φορτίο επεξεργασίας, οδηγώντας στη βελτίωση της κατανομής της χρησιμοποίησης των **CPU** του δικτύου. Ένα άλλο στοιχείο που διέθετε το εν λόγο λογισμικό, ήταν ότι ήταν αυτοπεριοριζόμενο, έτσι ώστε να μην είναι δυνατή η περαιτέρω εξάπλωσή του στο διαδίκτυο.

#### 4.3.2.1 Payload

Πολλά σκουλήκια έχουν δημιουργηθεί με σκοπό μόνο την εξάπλωσή τους χωρίς να προσπαθούν να τροποποιήσουν τα συστήματα που διέρχονται. Ωστόσο, όπως έδειξαν τα σκουλήκια **Morris** και **Mydoom [46,113]** η διαδικτυακή κίνηση και άλλες ακούσιες συνέπειες μπορεί συχνά να προκαλέσουν σημαντικές διαταραχές. Αυτό οφείλεται στο **payload (**φορτίο**)** που φέρουν τα **worms** το οποίο είναι ένας κώδικας σχεδιασμένος να κάνει κάτι περισσότερο από το να εξαπλώνεται, όπως είναι η διαγραφή αρχείων σε ένα υπολογιστή **(**π.χ., το **ExploreZip worm),** η κρυπτογράφηση αρχείων σε **cryptoviral extortion** επίθεση, ή η αποστολή εγγράφων μέσω **e-mail.** Ένα πολύ συνηθισμένο **payload** για σκουλήκια είναι η εγκατάσταση μιας κερκόπορτας **(trapdoor)** στον μολυσμένο υπολογιστή για να επιτρέψει τη δημιουργία ενός **"zombie"** υπολογιστή, ο οποίος βρίσκεται υπό τον έλεγχο του σχεδιαστή του **worm.** Δίκτυα με τέτοιους υπολογιστές **'zombie'** συχνά αναφέρονται ως **botnets** και χρησιμοποιούνται από τους σχεδιαστές των λογισμικών για την αποστολή **email junk** ή για την παραλλαγή της διεύθυνσης του δικτυακού τους τόπου. Γι' αυτό το λόγο οι **Spammers [102]** θεωρούνται ως μια πηγή "χρηματοδότησης" για τη δημιουργία τέτοιων **worms,** ενώ αρκετοί δημιουργοί τους, έχουν συλληφθεί για την πώληση καταλόγων με διευθύνσεις **IP** μολυσμένων μηχανημάτων, ενώ άλλοι προσπαθούν να εκβιάσουν εταιρείες υπό την απειλή **DoS** επιθέσεων.

Οι κερκόπορτες μπορούν να αξιοποιηθούν και από άλλα κακόβουλα προγράμματα, συμπεριλαμβανομένων και των σκουληκιών. Χαρακτηριστικό παράδειγμα αυτού αποτελεί το **Doomjuice**, το οποίο εξαπλώθηκε χρησιμοποιώντας την κερκόπορτα που είχε ανοίξει το **Mydoom.**

#### 4.3.2.2 Worms με καλή πρόθεση

Αρχίζοντας με την πρώτη έρευνα για τα **worms** στο **Xerox PARC,** υπήρξαν προσπάθειες να δημιουργηθούν χρήσιμα σκουλήκια. Η οικογένεια των σκουληκιών **Nachi,** για παράδειγμα, προσπάθησε να κατεβάσει και να εγκαταστήσει **patches** από το δικτυακό τόπο της **Microsoft** με σκοπό την επιδιόρθωση των τρωτών σημείων του συστήματος, μέσα από την αξιοποίηση των ίδιων των τρωτών σημείων. Στην πράξη, παρόλο που μπορούν να κάνουν τα συστήματα αυτά πιο ασφαλή, καθώς και να σκοτώνουν ορισμένους ιούς της ίδιας ημέρας **[5],** σαν αντιστάθμισμα δημιουργούν σημαντική κίνηση δικτύου, προκαλούν την επανεκκίνηση του υπολογιστή κατά τη διάρκεια της ενημέρωσης του κώδικα, και όλα αυτά γίνονται χωρίς τη συγκατάθεση του ιδιοκτήτη του υπολογιστή ή του χρήστη. Η πλειονότητα των ειδικών σε θέματα ασφάλειας θεωρούν όλα τα σκουλήκια ως κακόβουλα

προγράμματα, ανεξαρτήτως του φορτίου ή των ενδεχομένως καλών προθέσεων των δημιουργών τους.

#### 4.3.2.3 Προστασία από επικίνδυνα σκουλήκια

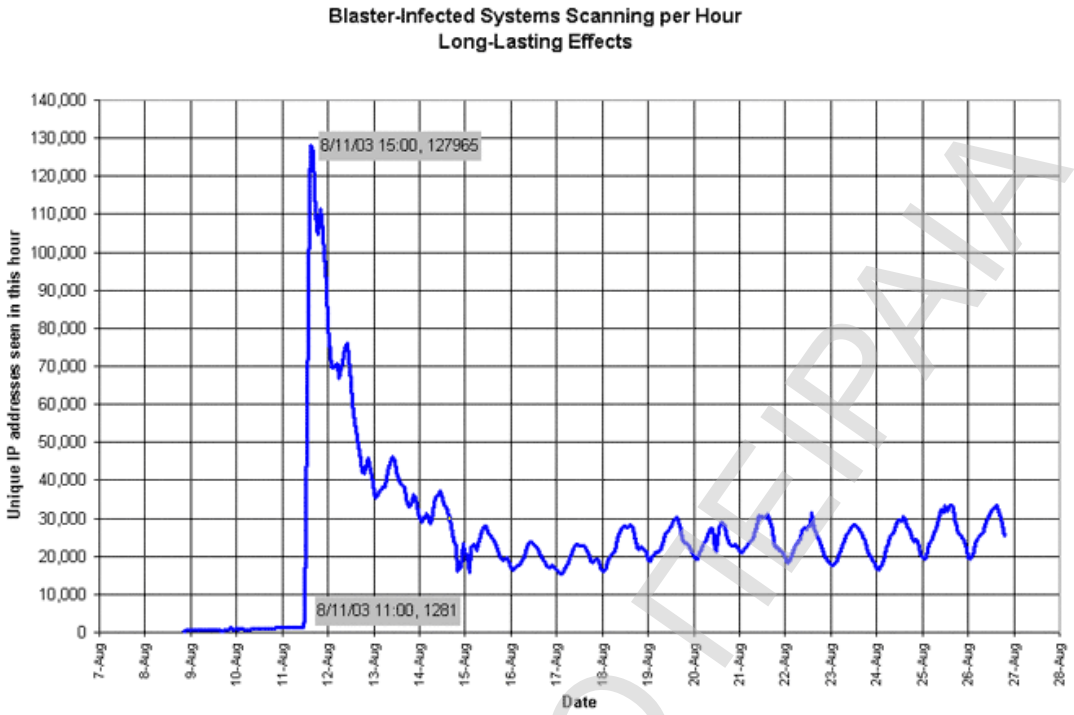
Τα **worms** εξαπλώνονται εκμεταλλευόμενα τα τρωτά σημεία των λειτουργικών συστημάτων. Όλες οι κατασκευάστριες αντιβιοτικών παρέχουν τακτικές ενημερώσεις ασφαλείας και εφόσον αυτές έχουν εγκατασταθεί σε ένα υπολογιστή, τότε η πλειοψηφία των σκουληκιών δεν είναι σε θέση να εξαπλωθούν από αυτόν. Εάν μία κατασκευάστρια είναι ενημερωμένη για ένα θέμα ευπάθειας αλλά δεν έχει ακόμα κυκλοφορήσει ένα **patch** για την ενημερωμένη έκδοση ασφαλείας, είναι πιθανή μια έκθεση μηδενικής ημέρας.

Εν γένει θα πρέπει να είμαστε δύσπιστοι όσον αφορά το άνοιγμα απρόσμενης ηλεκτρονικής αλληλογραφίας και δεν θα πρέπει να τρέχουμε συνημμένα αρχεία ή προγράμματα, ή να επισκεπτόμαστε δικτυακούς τόπους που συνδέονται με τέτοιου είδους μηνύματα. Όπως και με το **ILOVEYOU [46]** τύπο **worm**, αλλά και με την παράλληλη ανάπτυξη και αυξημένη αποδοτικότητα των επιθέσεων τύπου **phishing**, εξακολουθεί να είναι δυνατόν να παραπλανηθεί ο τελικός χρήστης θέτοντας σε λειτουργία ένα κακόβουλο κώδικα.

Ως μέτρο πρόληψης για αυτού του είδους τις απειλές συνιστάται η χρήση **Anti-virus** και **anti-spyware** λογισμικών, τα οποία θα πρέπει να ενημερώνονται σε καθημερινή βάση, ενώ θα πρέπει να εκτελείται μία πλήρης σάρωση του τερματικού τουλάχιστον μια φορά την εβδομάδα. Φυσικά τα αποτελέσματα αυτά μπορούν να βελτιωθούν σημαντικά με την παράλληλη χρήση ενός τείχους προστασίας.

**Blaster** και **Sobig**

Δύο από τα ποιο δημοφιλή σκουλήκια ήταν ο **Blaster** και ο **Sobig [11].** Η έκρηξη του **Blaster** έγινε την **11**η Αυγούστου **2003.** Το μεσημέρι της ίδιας μέρας είχαν μολυνθεί **7.000** υπολογιστές και το βράδυ **330.000.** Το λογισμικό ήταν προγραμματισμένο να επιτεθεί στο δικτυακό τόπο της **Microsoft** στις **16** Αυγούστου. Οι τεχνικοί της **Microsoft** πρόλαβαν και άλλαξαν τις διευθύνσεις των διακομιστών της εταιρίας και η επίθεση απέτυχε. Ακολουθεί ένα ενδεικτικό διαγράμματα εξάπλωσης του **Blaster (**Σχήμα **34):**




**Σχήμα 34. Εξάπλωση του Blaster**

Μια εβδομάδα αργότερα έκανε την εμφάνισή του η έκτη έκδοση ενός ακόμα σκουληκιού του **Sobig.** Το **malware** αυτό μεταδιδόταν μέσω ηλεκτρονικού ταχυδρομείου και επιβάρυνε τα συστήματα ηλεκτρονικής αλληλογραφίας**. Ο Sobig** ήταν παράλληλα ένας πολυμορφικός ιός**.** Όταν οι χρήστες άνοιγαν το μολυσμένο μήνυμα ο κώδικας του ιού ξεκινούσε την αναπαραγωγή του**.** Έβρισκε τις διευθύνσεις αλληλογραφίας του χρήστη και έστελνε μολυσμένα μηνύματα**.** Οι μολυσμένοι υπολογιστές θα επιχειρούσαν να συνδεθούν στο διαδίκτυο και Παρασκευή και Κυριακή από τις **0:00** έως τις **3:00.** Τότε επικοινωνούσαν με **20** διακομιστές και θα κατέβαζαν επιπλέον λογισμικό**.**

Η εξάπλωση του λογισμικού ήταν τεράστια**.** Οι διακομιστές αλληλογραφίας κατακλύστηκαν από μηνύματα που μετέφεραν τον ιό**.** Η **America On Line (**παροχέας διαδικτύου στις ΗΠΑ**)** έλαβε σε μία μέρα **31** εκατομμύρια μηνύματα **(**τρεις φορές περισσότερα από το κανονικό**).** Τα **11,5** εκατομμύρια ήταν μολυσμένα μηνύματα με τον **Sobig.** Μέσα σε μία εβδομάδα στάλθηκαν **200** εκατομμύρια μολυσμένα μηνύματα**.** Η όλη δραστηριότητα του ιού σταμάτησε στις **10** Σεπτεμβρίου καθώς έτσι είχε προγραμματιστεί ο ιός**.**

### 4.3.3 Δούρειος Ίππος (trojan horse)

Οι Δούρειοι Ίπποι **(Trojan Horses)** δανείστηκαν το όνομά τους από το διάσημο μυθικό τέχνασμα των Ελλήνων στην Τροία**,** καθώς εισβάλλουν με **«**αθώο**»** τρόπο

στο εκάστοτε σύστημα και μόλις ενεργοποιηθούν τα αποτελέσματα τις εκτέλεσής τους μπορεί να είναι καταστροφικά. Συνήθεις «κρυψώνες» ενός Δούρειου Ίππου **[112]** είναι κάποιο νέο, δωρεάν παιχνίδι στο Διαδίκτυο, κάποιο τραγούδι σε μορφή **MP3**, κάποιο εξειδικευμένο πρόγραμμα θέασης πορνογραφικού υλικού ή κάποιο πρόγραμμα αρκετά δελεαστικό ώστε να το κατεβάσουν οι χρήστες.

Όταν εκτελεστεί το εν λόγω «ύποπτο» πρόγραμμα, καλείται η διαδικασία του Δούρειου Ίππου, η οποία επιτελεί ανεπιθύμητες λειτουργίες, όπως η τροποποίηση, η διαγραφή, η κρυπτογράφηση, η αντιγραφή αρχείων χρηστών σε σημείο όπου ο σχεδιαστής του λογισμικού μπορεί να τις ανακτήσει αργότερα ή να τις αποστείλει στον εαυτό του ή σε κάποια ασφαλή κρυψώνα μέσω ηλεκτρονικού ταχυδρομείου ή **FTP**.

Ένας συχνός τρόπος λειτουργίας των Δούρειων Ίππων είναι η απενεργοποίηση του ήχου του μόντεμ και η εν συνεχεία κλήση κάποιου διεθνούς αριθμού με ιδιαίτερα υψηλό κόστος. Συνήθως επιλέγονται μακρινές χώρες της πρώην Σοβιετικής Ένωσης (π.χ. Μολδαβία κ.λπ.) ή χώρες του Ειρηνικού, όπου επιλέγεται κάποιος πολύ ακριβός παροχέας Διαδικτύου, ώστε ο χρήστης να μην αντιληφθεί τίποτα ύποπτο και να συνεχίζει να δουλεύει ώρες. Τέτοιες περιπτώσεις Δούρειων Ίππων είναι γνωστές με το όνομα **dialers** από το ρήμα **dial** που σημαίνει καλώ. Αξίζει να αναφερθεί μία ανάλογη περίπτωση, στην οποία οι θύτες ξόδεψαν περίπου **800.000** λεπτά χρόνου σύνδεσης πριν η Ομοσπονδιακή Επιτροπή Εμπορικών Αδικημάτων των ΗΠΑ κατορθώσει να ανακαλύψει τους τρεις υπευθύνους στο **Long Island** και να τους μηνύσει. Η ποινή που επιβλήθηκε στους δράστες ήταν η επιστροφή **2,74** εκατομμυρίων δολαρίων σε **38.000** θύματα.

Σε **Unix-Linux** συστήματα ένας Δούρειος Ίππος θα μπορούσε να τοποθετηθεί σε κάποιο συχνά χρησιμοποιούμενο φάκελο, όπως το **/bin** ή το **/usr/bin** και να του δοθεί κάποιο όνομα παραπλήσιο με κάποιο υπάρχον αρχείο. Για παράδειγμα στον κατάλογο **/usr/bin/X11** υπάρχει ένα αρχείο **ls** και ο εισβολέας αποθηκεύει ένα αρχείο με το όνομα **la**. Αν κάποιος χρήστης πληκτρολογήσει κατά λάθος τη **la**, τότε ο Δούρειος Ίππος θα εκτελεστεί και στη συνέχεια θα εμφανιστεί μήνυμα λάθους, ώστε ο χρήστης να μην υποψιαστεί το αθώο σφάλμα του. Είναι πιθανό, ακόμη και αν ο Δούρειος Ίππος τοποθετηθεί σε πολύπλοκους καταλόγους, που δε χρησιμοποιούνται συχνά, να υπάρξουν λάθη πληκτρολόγησης που θα οδηγήσουν στην εκτέλεση καταστροφικού κώδικα. Μπορεί, επίσης, ο επικίνδυνος κώδικας να έχει τοποθετηθεί σε φάκελο υπερχρήστη, όπως για παράδειγμα ο **/bin** και κάποιο λάθος να οδηγήσει πάλι σε απρόσμενα αποτελέσματα.

Μία ακόμη πιθανή εισβολή μπορεί να πραγματοποιηθεί από τον χρήστη, ο οποίος θα εκτελέσει μία παραλλαγμένη έκδοση της κλήσης συστήματος **ls** στον προσωπικό

του κατάλογο οδηγώντας σε αυξημένη υπολογιστική δραστηριότητα στο σύστημα, παρόμοια με την εκκίνηση **100** υπολογιστικών διαδικασιών, με στόχο το να τραβήξουν την προσοχή του υπερχρήστη. Είναι πιθανό ότι ο υπερχρήστης να προσπαθήσει να δει τι γίνεται πληκτρολογώντας

---

**cd /usr/**όνομα_χρήστη

**ls –i**

---

για να δει τι περιέχεται στον κατάλογο του χρήστη. Καθώς μερικά **shells** δοκιμάζουν τον τοπικό κατάλογο πριν από τον κατάλογο εργασίας που βρίσκεται στη μεταβλητή περιβάλλοντος **$PATH (**χρησιμοποιείται για έλεγχο καταλόγων στους οποίους γίνεται αναζήτηση**),** ο υπερχρήστης μπορεί να εκτελέσει το Δούρειο Ίππο με προνόμια υπερχρήστη. Ο Δούρειος Ίππος μπορεί να μετατρέψει το **SETUID** του **/usr/**όνομα_χρηστη**/bin/sh** σε **root.** Το μόνο που χρειάζεται είναι να εκτελεστούν δύο κλήσεις συστήματος**:**

**chown:**

Για να αλλάξει τον ιδιοκτήτη του **/usr/**όνομα_χρηστη**/bin/sh** σε **root.**

**chmod:**

Για να ορίσει το **bit SETUID** αυτού του **shell.**

Από αυτή τη στιγμή και μετά ο χρήστης έχει δικαιώματα υπερχρήστη εκτελώντας απλά αυτό το **shell.**

#### 4.3.3.1 Ιστορία

Ο όρος "δούρειος ίππος" χρησιμοποιήθηκε για πρώτη φορά από τον Κεν Τόμσον στην ομιλία του το **1983** κατά την τελετή απονομής των βραβείων **Turing.** Ο Τόμσον παρατήρησε ότι είναι δυνατόν να προστεθεί κακόβουλος κώδικας στην εντολή **login** του **Unix** για την υποκλοπή των κωδικών πρόσβασης. Αυτή του την ανακάλυψη την ονόμασε "δούρειο ίππο". Επιπρόσθετα υποστήριξε ότι οποιοσδήποτε μεταγλωττιστής **C** μπορεί να μετατραπεί κατάλληλα ούτως ώστε να προσθέτει αυτόματα κακόβουλο κώδικα στα προγράμματα που δημιουργεί κάνοντας έτσι ακόμα πιο δύσκολη την διαδικασία εντοπισμού του.

#### 4.3.3.2 Τύποι δούρειων ίππων

Εν γένη υπάρχουν δύο είδη δούρειων ίππων**:**

**Ø** Το πρώτο είδος αποτελείται από κανονικά προγράμματα, τα οποία κακόβουλοι προγραμματιστές **(**χάκερς**)** μεταβάλλουν προσθέτοντάς τους κακόβουλο κώδικα. Στην κατηγορία αυτή ανήκουν διάφορα ομότιμα προγράμματα ανταλλαγής αρχείων **(peer-to-peer)** καθώς και προγράμματα ανακοίνωσης καιρικών συνθηκών.

- Το δεύτερο είδος περιλαμβάνει μεμονωμένα προγράμματα που ξεγελούν τον χρήστη και τον κάνουν να νομίζει ότι πρόκειται για κάποιο παιχνίδι ή εικόνα. Με τον τρόπο αυτό τον παρασύρουν να εκτελέσει το αρχείο, μολύνοντας έτσι τον υπολογιστή του.

Οι τύποι δούρειων ίππων μπορούν να διαχωριστούν περαιτέρω ανάλογα με τις συνέπειες που έχουν στον μολυσμένο υπολογιστή στις εξής κατηγορίες:

- Απομακρυσμένης πρόσβασης.
- Αποστολής **e-mail**.
- Καταστροφής αρχείων.
- Κατεβάσματος αρχείων.
- **Proxy Trojan**.
- **FTP Trojan** (προσθήκη, διαγραφή ή μεταφορά αρχείων από τον μολυσμένο υπολογιστή).
- Απενεργοποίησης λογισμικού ασφαλείας (**firewall**, αντιϊκά κλπ).
- **Denial of Service (DoS)**.
- **URL Trojan** (επιτρέπουν στον υπολογιστή να συνδεθεί στο διαδίκτυο μόνο μέσω μίας πολύ ακριβής σε κόστος σύνδεσης).

#### 4.3.3.3 Μέθοδοι ανίχνευσης – εξουδετέρωσης

Εξαιτίας του μεγάλου πλήθους των μορφών των **Trojan [46] [47]** δεν υπάρχει ένας μονοσήμαντος τρόπος για να προβούμε στην ανίχνευση και εξόντωσή τους. Οι απλούστεροι πρακτικές που μπορούν να ακολουθηθούν είναι ο καθαρισμός των προσωρινών αρχείων του διαδικτύου του υπολογιστή ή η ανίχνευση του αρχείου και η χειροκίνητη διαγραφή του. Στην πράξη τα προγράμματα προστασίας (εφόσον είναι ενημερωμένα) είναι ικανά να ανιχνεύσουν και να αφαιρέσουν αυτού του είδους το κακόβουλο λογισμικό αυτόματα, αν όμως παρόλα αυτά δεν είναι δυνατή η ανίχνευση του λογισμικού μια καλή λύση είναι να χρησιμοποιήσουμε ένα δεύτερο υπολογιστή στον οποίο και θα τρέχει το πρόγραμμα προστασίας και να θεωρήσουμε ως πόρο αυτού τον σκληρό δίσκο του υπό εξέταση υπολογιστή.

#### 4.3.3.4 Γνωστοί δούρειοι ίπποι

- **Downloader-EV**
- **Dropper-EV**
- **Pest Trap**
- **NetBus**

- **flooder**
- **Vundo trojan**
- **Gromozon Trojan**
- **Sub-7**

### 4.3.4 Rootkit

Τα **rootkit [4,58,125]** είναι προγράμματα ή συνδυασμός διαφόρων προγραμμάτων σχεδιασμένα με σκοπό να λάβουν τον πλήρη έλεγχο της λειτουργίας των υπολογιστών, χωρίς την άδεια από τους χειριστές, τους ιδιοκτήτες ή τους νόμιμους διαχειριστές. Αυτό είναι δυνατό χωρίς κατ' ανάγκη να υπάρχει πρόσβαση στο υλικό καθώς στοχεύουν στην λήψη έλεγχου του λειτουργικού συστήματος που εκτελείται στο υλικό. Συνήθως, τα **rootkits** επισκιάζουν την παρουσία τους μέσα από την υπεκφυγή ή καταστροφή των πρότυπων μηχανισμών ασφαλείας των λειτουργικών συστημάτων, ενώ συχνά είναι και **trojan** καταφέρνοντας έτσι να ξεγελάσουν τους χρήστες κάνοντάς τους να πιστέψουν ότι είναι ασφαλής η εκτέλεσή τους στο σύστημα. Τεχνικές που χρησιμοποιούνται για να επιτευχθεί αυτό περιλαμβάνουν, την απόκρυψη εκτελούμενων προγραμμάτων από προγράμματα παρακολούθησης, ή την απόκρυψη αρχείων ή δεδομένων του συστήματος από το λειτουργικό σύστημα.

Τα **Rootkits** αρχικά έβρισκαν εφαρμογή σε έκτακτες καταστάσεις όπου έθεταν υπό έλεγχο συστήματα που δεν αποκρίνονταν, αλλά τα τελευταία χρόνια έχουν χρησιμοποιηθεί σε μεγάλο βαθμό ως κακόβουλα προγράμματα τα οποία και χρησιμοποιούνται για να βοηθήσουν τους εισβολείς να αποκτήσουν πρόσβαση σε συστήματα, αποφεύγοντας παράλληλα την ανίχνευση τους. **Rootkits** υπάρχουν για μια σειρά από λειτουργικά συστήματα, όπως τα **Microsoft Windows, Mac OS X , Linux** και **Solaris** και δρουν συνήθως δρουν τροποποιώντας συνιστώσες των λειτουργικών συστημάτων ή εγκαθίστανται ως οδηγοί ή λειτουργίες του πυρήνα ανάλογα με τις εσωτερικές λεπτομέρειες των μηχανισμών του εκάστοτε λειτουργικού συστήματος.

#### 4.3.4.1 Ιστορια

Ο όρος **rootkit** χρησιμοποιήθηκε αρχικά για τον προσδιορισμό της κακόβουλης τροποποίησης των εργαλείων διαχείρισης για ένα **Unix-like** λειτουργικό σύστημα. Έτσι αν ένας εισβολέας μπορούσε να αντικαταστήσει τα πρότυπα εργαλεία διαχείρισης σε ένα σύστημα με ένα **rootkit**, τα τροποποιημένα εργαλεία θα έδιναν τον έλεγχο του συστήματος σε αυτόν, ενώ παράλληλα θα του πρόσφεραν την απόκρυψη των δραστηριοτήτων του από το νόμιμο διαχειριστή του συστήματος.

Η παλαιότερη γνωστή μορφή **rootkit [4]** είχε γραφεί το **1990** από τους **Lane Davis** και **Riley Dake** για το λειτουργικό σύστημα **SunOS 4.1.1.** Ωστόσο υπήρξε μια προηγούμενη, αρκετά γνωστή έκθεση παρόμοια με **rootkit ,** που είχε διαπραχθεί από τον **Ken Thompson,** εργαζόμενο στα εργαστήρια της **Bell** εναντίον του **Naval Laboratory** στην Καλιφόρνια με σκοπό να κερδίσει ένα στοίχημα. Αυτό που έκανε ήταν η τροποποίηση του **C compiler** σε μία διανομή του **Unix** στο εργαστήριο.

Τα **rootkits** έλαβαν αρχικά την ονομασία τους από την ιδιότητά τους να επιτρέπουν στον εισβολέα να αποκτήσει δικαιώματα διαχειριστή **(root user)** σε ένα **Unix** σύστημα. Έκτοτε, παρόμοιου τύπου λογισμικό έχει αναπτυχθεί και για άλλα λειτουργικά συστήματα, και ο όρος έχει διευρυνθεί ώστε να συμπεριλαμβάνει οποιοδήποτε λογισμικό το οποίο εν κρυπτό μεταβάλλει το λειτουργικό σύστημα έτσι ώστε ένας μη εξουσιοδοτημένος χρήστης να μπορεί να λάβει τον έλεγχο αυτού.

Τα **rootkits** έγιναν ευρέως γνωστά το **2005,** όταν η **Sony BMG,** προκάλεσε σκάνδαλο με τη συμπερίληψη **rootkit** λογισμικού σε μουσικά **CD** το οποίο τροποποιούσε τα λειτουργικά συστήματα **Windows** για να επιτρέψει την πρόσβαση σε οποιονδήποτε γνώριζε αυτή την εγκατάσταση. Ο λόγος για τον οποίο έγινε αυτό, ήταν για να επιβάλει την προστασία από την αντιγραφή του εν λόγο **CD.** Το σκάνδαλο αυτό ήταν που οδήγησε στην ανακάλυψη και την επακόλουθη δημόσια ανακοίνωση της χρήσης **malware** από την εταιρία, προκαλώντας έτσι την ανησυχία πολλών μη εξοικειωμένων χρηστών.

#### 4.3.4.2 Τρόπος λειτουργίας

Μια επιτυχής εγκατάσταση ενός **rootkit** επιτρέπει σε μη εξουσιοδοτημένους χρήστες να ενεργούν ως διαχειριστές του συστήματος και, συνεπώς, να έχουν τον πλήρη έλεγχο αυτού. Επιπρόσθετα είναι δυνατό να αποκρύπτουν, αρχεία, συνδέσεις δικτύου, μπλοκ μνήμης ή και καταχωρήσεις μητρώου **(registry),** από άλλα προγράμματα που χρησιμοποιούν οι διαχειριστές για την ανίχνευση λογισμικού πρόσβασης με ειδικά προνόμια στους πόρους του υπολογιστή . Ωστόσο δεν είναι αναγκαίο τα **rootkits** να είναι κατ' ανάγκη κακόβουλο λογισμικό, καθώς μπορούν να χρησιμοποιηθούν τόσο για παραγωγικούς όσο και για καταστροφικούς σκοπούς.

Ένα **rootkit** το οποίο αποκρύπτει βοηθητικά προγράμματα, συνήθως το πράττει για να καταχραστεί εκτεθειμένα σύστημα, και συχνά χρησιμοποιεί τις λεγόμενες **"backdoors"** για να βοηθήσει τον εισβολέα στη συνέχεια να αποκτήσει πρόσβαση κατά βούληση. Ένα απλό παράδειγμα θα μπορούσε να είναι ένα **rootkit** το οποίο αποκρύπτει μια εφαρμογή που παράγει ένα κέλυφος επεξεργασίας εντολών όταν ο εισβολέας συνδέεται σε μία συγκεκριμένη πόρτα δικτύου στο σύστημα. **Η backdoor** μπορεί επίσης να επιτρέψει σε διεργασίες που εκτελούνται από μη προνομιούχους

χρήστες να τρέχουν σαν να έχουν εκτελεστεί από προνομιούχους **(**συμπεριλαμβανομένου και του διαχειριστή**)** και να εκτελούν καθήκοντα που κανονικά προορίζονται για **superuser.**

Άλλο ένα στοιχείο των **rootkits** είναι ότι μπορεί να περιλαμβάνουν εργαλεία για επιθέσεις κατά συστημάτων των υπολογιστών**,** όπως είναι οι **sniffers** και τα **keyloggers.** Μια επίσης πιθανή κατάχρηση είναι η χρήση ενός μολυσμένου υπολογιστή για περαιτέρω εξάπλωση όπως δηλαδή και στην περίπτωση των ζόμπι υπολογιστών**,** δίνοντας το πλεονέκτημα ότι αποκρύπτεται ο πραγματικός εισβολέας αφού η επίθεση φαίνεται ότι ξεκινάει από τον μολυσμένο υπολογιστή**.** Λογισμικό για τέτοιες επιθέσεις μπορεί να περιλαμβάνει εργαλεία για επιθέσεις τύπου άρνησης υπηρεσίας**,** εργαλεία για την αναμετάδοση συνομιλιών **chat,** και την αποστολή **e-mail spam.**

Μια επίσης πολύ σημαντική χρήση των **rootkits** είναι να επιτρέψουν στον δημιουργό τους να δει και να έχει πρόσβαση στα ονόματα χρηστών και στην λίστα των **log-in** των συστημάτων**,** με σχετικά μεγάλη ευκολία και για μεγάλο πλήθος υπολογιστών **(**μερικές χιλιάδες**).** Η δυνατότητα αυτή τα καθιστά ακόμα πιο επικίνδυνα**,** καθώς είναι εφικτός ο συνδυασμός τους με **trojan** επιτρέποντας την πρόσβαση τους σε αυτά τα συστήματα την ώρα που τα **rootkit** τους παρέχουν την αναγκαία κάλυψη**.** Αυτός είναι και ο λόγος για τον οποίο οι συγγραφείς κακόβουλου λογισμικού κάνουν ευρεία χρήση αυτών**,** καθώς καθιστούν δυνατή την απόκρυψη του κακόβουλου λογισμικού τόσο από τους χρήστες των **PC** όσο και από τα προγράμματα εντοπισμού ιών.

#### 4.3.4.3 Είδη

Υπάρχουν τουλάχιστον πέντε είδη **rootkit: firmware , virtualized , kernel , library** και **application level [125].**

- **Firmware**

Ένα **rootkit** τύπου **firmware** χρησιμοποίει τις συσκευές ή την πλατφόρμα του **firmware** για την απόκρυψή του**.** Το **rootkit** μπορεί με επιτυχία να κρυφτεί στο **firmware,** διότι αυτό δεν υπόκειται συχνά σε έλεγχο ακεραιότητας του κώδικα**.** Ο **John Heasman** κατάφερε να αποδείξει έμπρακτα τη βιωσιμότητα των **firmware rootkits** τόσο στις **ACPI firmware** ρουτίνες όσο και σε μια **PCI** κάρτα επέκτασης **ROM.**

- **Virtualized**

Αυτά τα **rootkits** λειτουργούν τροποποιώντας την ακολουθία της εκκίνησης του υπολογιστή με στόχο να φορτώνονται τα ίδια αντί του αρχικού λειτουργικού

συστήματος. Μόλις φορτωθεί στη μνήμη, ένα **virtualized rootkit**, φορτώνει το αρχικό λειτουργικό σύστημα ως ιδεατή μηχανή, επιτρέποντας έτσι σε αυτό να εμποδίζει όλες τις κλήσεις που πραγματοποιούνται από το πραγματικό λειτουργικό σύστημα.

- **Kernel level**

Τα **rootkits** επιπέδου πυρήνα προσθέτουν επιπλέον κώδικα ή αντικαθιστούν τμήματα του λειτουργικού συστήματος, συμπεριλαμβανομένων τόσο του πυρήνα όσο και των συσχετιζόμενων οδηγών των συσκευών. Τα περισσότερα λειτουργικά συστήματα δεν επιβάλλουν καμία διάκριση ασφάλειας μεταξύ του πυρήνα και των οδηγών των συσκευών έχοντας ως συνέπεια, πολλά **rootkits** επιπέδου πυρήνα να έχουν σχεδιαστεί ως οδηγοί συσκευών ή συνιστώσες **(loadable modules)**, όπως είναι οι διεργασίες πυρήνα στο **Linux** ή τα προγράμματα οδήγησης συσκευών στα **Microsoft Windows.** Έτσι κάθε κώδικας που λειτουργεί σε επίπεδο πυρήνα μπορεί να έχει σοβαρές επιπτώσεις στη σταθερότητα του συστήματος αν υπάρχουν λάθη σε αυτόν.

Αυτή η κατηγορία είναι ιδιαίτερα επικίνδυνη διότι είναι πολύ δύσκολο να ανιχνευτούν και ο λόγος για τον οποίο αυτό συμβαίνει είναι επειδή λειτουργούν στο ίδιο επίπεδο με το λειτουργικό σύστημα και έτσι μπορούν να τροποποιήσουν ή να εμποδίσουν οποιαδήποτε λειτουργία του συστήματος και των εφαρμογών. Σε μια τέτοια κατάσταση, το ίδιο το σύστημα δεν μπορεί να θεωρηθεί αξιόπιστο και ένας τρόπος για να το επαναφέρουμε στην αρχική του κατάσταση είναι να εκτελέσουμε μια ανάλυση του συστήματος χωρίς σύνδεση δικτύου, χρησιμοποιώντας ένα δεύτερο έμπιστο σύστημα, στο οποίο θα θεωρήσουμε ως πόρο τον σκληρό δίσκο του πρώτου.

- **Library level**

Τα **rootkit** επιπέδου βιβλιοθήκης παραλλάσουν ή αντικαθιστούν τις κλήσεις του συστήματος με άλλες εκδόσεις οι οποίες αποκρύπτουν πληροφορίες για τον εισβολέα. Τα **rootkit** αυτής της κατηγορίας μπορούν να ανιχνευθούν, τουλάχιστον θεωρητικά, με την εξέταση του κώδικα των βιβλιοθηκών **(**υπό τον όρο των **Windows** είναι συνήθως **DLL)** για αλλαγές. Παρόλα αυτά στην πράξη, η ποικιλία των τροποποιημένων βιβλιοθηκών από τις διάφορες εκδόσεις με εφαρμογές και **ServicePacks** καθιστούν αυτή την διαδικασία εξαιρετικά δύσκολη.

- **Application level**

Τα **rootkit** επιπέδου εφαρμογής μπορούν να αντικαταστήσουν ψηφία συνηθισμένων εφαρμογών με δυαδικά αρχεία κακόβουλου λογισμικού, ή μπορούν να

τροποποιήσουν τη συμπεριφορά των υπαρχουσών εφαρμογών χρησιμοποιώντας διάφορες τεχνικές όπως **hooks, patches,** εμβόλιμο κώδικα ή άλλα μέσα**.**

#### 4.3.4.4 Τρόποι Ανίχνευσης.

Τα **Rootkit** είναι δυνατό να ανιχνευθούν διαμέσου της ψηφιακής υπογραφής τους από αντιβιοτικά προγράμματα ωστόσο υπάρχουν εγγενείς περιορισμοί για κάθε πρόγραμμα που επιχειρεί να τα εντοπίσει καθώς τα ίδια τα προγράμματα ανίχνευσης εκτελούνται από το ίδιο το υπό εξέταση σύστημα**.** Με άλλα λόγια, ενέργειες όπως η παροχή της λίστας με τις διεργασίες που εκτελούνται**,** ή μια λίστα όλων των αρχείων σε έναν κατάλογο**,** δεν μπορεί να θεωρούνται αξιόπιστες αναμένοντας ότι θα λειτουργήσουν όπως προβλέπετε από τα πρότυπα**.**

Η καλύτερη και πιο αξιόπιστη**,** μέθοδος ανίχνευσης **rootkit** είναι να κλείσουμε τον υπό εξέταση υπολογιστή και στη συνέχεια να ελέγξουμε τα αποθηκευτικά του μέσα εκκινώντας από ένα εναλλακτικό μέσο όπως είναι το **CD-ROM** ή ο οδηγός **USB.** Ένα **rootkit** δεν μπορεί να κρύψει εξολοκλήρου την παρουσία του**,** και το γεγονός αυτό εκμεταλλεύονται τα αντιβιοτικά προγράμματα για να τα εντοπίσουν**,** εφοδιασμένα με πρότυπες εντολές συστήματος και ερωτήματα χαμηλού επιπέδου τα οποία πρέπει να παραμένουν αξιόπιστα **(**αναλλοίωτα**).** Έτσι αν υπάρξει κάποια διαφορά**,** θα πρέπει να υποθέσουμε την ύπαρξη ενός **rootkit.** Τα εκτελούμενα **rootkits** είναι σε θέση να αποκρύψουν την παρουσία τους από τις διεργασίες παρακολούθησης**-**σάρωσης αναστέλλοντας την λειτουργία τους μέχρι την ολοκλήρωση της σάρωσης**.**

Οι προμηθευτές λογισμικού ασφαλείας επιχείρουν να δώσουν μία λύση ενσωματώνοντας την ανίχνευση των **rootkit** στα παραδοσιακά αντιβιοτικά προϊόντα**.** Αν λοιπόν ένα **rootkit** επιχειρήσει να αποκρύψει την παρουσία του κατά τη διάρκεια της σάρωσης**,** θα εντοπίζονται με την χρήση ενός **stealth** ανιχνευτή**.** Εάν δοκιμάσει να ξεφορτωθεί προσωρινά από το σύστημα**,** τα παραδοσιακά **antivirus** προγράμματα είναι σε θέση να ανιχνεύσουν την ύπαρξή του με την χρήση της ανίχνευσης των αποτυπωμάτων. Ωστόσο οι επιτιθέμενοι μπορούν ενσωματώνοντας μηχανισμούς αντιμετώπισης επιθέσεων **(**επονομαζόμενες και ως **retro** ρουτίνες**)** στον κώδικα των **rootkit** κατορθώνοντας έτσι να αφαιρέσουν τις διεργασίες των αντιβιοτικών προγραμμάτων από την μνήμη**,** αναστέλλοντας κατ' αυτό τον τρόπο την λειτουργία τους.

Υπάρχουν διαθέσιμα στην αγορά πολλά προγράμματα για την ανίχνευση των **rootkits.** Στα βασισμένα στο **Unix** συστήματα**,** τρία από τα πιο δημοφιλή είναι τα **chkrootkit, rkhunter** και **OSSEC.** Για τα **Windows,** υπάρχουν πολλά δωρεάν εργαλεία ανίχνευσης όπως το **Sophos Anti-Rootkit, F-Secure Blacklight, Hypersight Rootkit Detector** ή το **Radix Anti-Rootkit.** Ένας άλλος ανιχνευτής για **Windows** είναι

ο **RootkitRevealer** από τη **Microsoft (**πρώην **Sysinternals)** ο οποίος ανιχνεύει τα τρέχων **rootkits** από τη σύγκριση των αποτελεσμάτων από το λειτουργικό σύστημα με την πραγματική καταγραφή διαβάζοντας από τον ίδιο το δίσκο **(cross checking).** Ωστόσο, ορισμένα **rootkit** άρχισαν να προσθέτουν **RootkitRevealer** και έτσι στην ουσία εξαλείφουν τις διαφορές μεταξύ των δύο λιστών, και ο ανιχνευτής δεν είναι σε θέση να τα ανιχνεύσει. Μια άλλη μέθοδος είναι η σύγκριση του περιεχομένου των δυαδικών αρχείων στο δίσκο με τους αντίγραφα τους στην μνήμη του λειτουργικού **(**κάποιες διαφορές μπορούν να παρουσιαστούν από τους νόμιμους μηχανισμούς του λειτουργικού συστήματος**).**

Όπως πάντα όμως επειδή η πρόληψη είναι καλύτερη από τη θεραπεία, και ως εκ τούτου για να ήμαστε βέβαιοι ότι έχουμε απομακρύνει ένα **rootkit,** αυτό συνήθως συνεπάγεται εκ νέου εγκατάσταση του συνόλου του λογισμικού. Εάν όμως η ακεραιότητα της εγκατάστασης των δίσκων του συστήματος θεωρείται αξιόπιστη, μπορεί να γίνει χρήση της κρυπτογραφίας για την παρακολούθηση της ακεραιότητας του συστήματος. Με την αποτύπωση των αρχείων του συστήματος, αμέσως μετά από μια νέα εγκατάσταση του συστήματος και στη συνέχεια μετά από κάθε μεταγενέστερη μεταβολή του συστήματος **(**π.χ., εγκατάσταση νέου λογισμικού**),** ο χρήστης ή ο διαχειριστής του συστήματος θα ειδοποιείται για οποιεσδήποτε τυχόν επικίνδυνες αλλαγές των αρχείων του συστήματος. Στη διαδικασία λήψης αποτυπωμάτων ένα πρότυπο μήνυμα χρησιμοποιείται για να δημιουργήσει μια σταθερού μήκους ακολουθία η οποία εξαρτάται από κάθε **bit** του αρχείου που υπόκειται στην διαδικασία αυτή. Με τον υπολογισμό και τη σύγκριση έτσι αυτών των μηνυμάτων σε τακτά χρονικά διαστήματα είναι δυνατή η ανίχνευση των μη εξουσιοδοτημένων αλλαγών στο σύστημα.

### 4.3.5 Spyware

Το **spyware [44,46,47,59,106]** είναι λογισμικό υπολογιστή το οποίο εγκαθίσταται ένα αγνοία του χρήστη με στόχο να σταματήσει ή να λάβει το μερικό έλεγχο της αλληλεπίδρασης του χρήστη με τον υπολογιστή. Μία συνηθισμένη λειτουργία τους είναι να κατακλύζουν τους προσβεβλημένους υπολογιστές με **pop-up** διαφημίσεις **(**παρόλο που κάτι τέτοιο είναι δυνατόν να υλοποιηθεί και από τις ίδιες τις ιστοσελίδες χρησιμοποιώντας **JavaScript).** Η λειτουργικότητα τους παρόλα αυτά ξεπερνά κατά πολύ την απλή παρακολούθηση της συμπεριφοράς των χρηστών, καθώς είναι ικανά να συλλέξουν διάφορα είδη προσωπικών πληροφοριών, όπως είναι οι συνήθειες που έχουν οι χρήστες κατά την πλοήγησή τους στο διαδίκτυο, τους δικτυακούς τόπους που επισκέπτονται αλλά και να παρέμβουν στον έλεγχο του χρήστη εγκαθιστώντας επιπρόσθετο λογισμικό, ανακατευθύνοντας την λειτουργία των φυλλομετρητών και προσπελαύνοντας ιστοσελίδες που μπορούν να

προσβάλουν τον υπολογιστή με πολύ πιο επικίνδυνους ιούς. Επιπρόσθετα είναι ικανά ακόμα και να αλλάξουν της ρυθμίσεις του υπολογιστή προκαλώντας έτσι μείωση της ταχύτητας των συνδέσεων, διαφορετικές **homepages** στους περιηγητές καθώς και απώλεια των συνδέσεων αλλά και των προγραμμάτων.

#### 4.3.5.1 Ιστορία και εξέλιξη

**Η** πρώτη καταγεγραμμένη χρήση του όρου **spyware** ήταν στις **16** Οκτωβρίου **1995** σε μια δημοσίευση η οποία γελοιοποιούσε το επιχειρησιακό μοντέλο της **Microsoft.** Ενώ αρχικά ο όρος αυτός παρέπεμπε σε υλικό το οποίο χρησιμοποιούταν για κατασκοπευτικούς σκοπούς, στις αρχές του **2000** ο ιδρυτής των **Zone Labs , Gregor Freund,** έκανε χρήση αυτού του όρου σε μία συνέντευξη τύπου για το τοίχος προστασίας του **ZoneAlarm.** Έκτοτε ο όρος **"spyware"** χρησιμοποιείται με την σημερινή του έννοια. Σύμφωνα με μία έρευνα του **2005** από την **AOL** και την Εθνική συμμαχία κυβερνοασφάλειας το **61%** των ερωτηθέντων χρηστών είχε προσβληθεί ο υπολογιστής τους από μία μορφή **spyware,** εκ των οποίον το **92%** ανέφερε ότι δεν γνώριζε καν την παρουσία του και ότι δεν είχαν δώσει την συγκατάθεσή τους για την εγκατάσταση αυτού του λογισμικού. Ένα δεύτερο σημαντικό στοιχείο είναι η διαπίστωση ότι ιδιαίτερα ευπαθείς εμφανίζονται να είναι οι υπολογιστές που έχουν ως πρωτεύων περιηγητή τον **Internet Explorer (IE)** και αυτό δεν αποτελεί μόνο απόρροια της ευρείας διάδοσης του **IE,** αλλά και εξαιτίας της στενής του ενοποίησης με τα **Windows** γεγονός που εκμεταλλεύονται τα **spyware** για να έχουν πρόσβαση σε κρίσιμα τμήματα του λειτουργικού συστήματος. Πριν από την έκδοση του **Internet Explorer 7** ο **IE** εμφάνιζε αυτόματα ένα παράθυρο εγκατάστασης για κάθε συστατικό **ActiveX** που μια ιστοσελίδα ήθελε να εγκατασταθεί και το γεγονός αυτό σε συνδυασμό με την ελλιπή ενημέρωση και γνώση των χρηστών σχετικά με τα **malware** ήταν που οδήγησαν στην μαζική εξάπλωση αυτών.

Άλλο ένα στοιχείο που τα **Spyware** εκμεταλλεύονται είναι μητρώο των **Windows** το οποίο περιέχει πολλαπλές ενότητες όπου με κατάλληλη τροποποίηση των τιμών των αντίστοιχων κλειδιών επιτρέπουν στο λογισμικό να εκτελείται αυτόματα κατά την εκκίνηση του λειτουργικού συστήματος. Έτσι καθίσταται δυνατό αφενός να παρακάμψουν τυχών προσπάθειες αφαίρεσής τους, αφετέρου να συνδεθούν με τις αντίστοιχες τοποθεσίες του μητρώου που επιτρέπουν την εκτέλεσή τους. Όσον αφορά τον τρόπο λειτουργίας τους, κατά την διάρκεια εκτέλεσης τους, τα **spyware** ελέγχουν περιοδικά αν κάποιος από αυτούς τους δεσμούς με το μητρώο έχει διαγραφεί και αν κάτι τέτοιο ισχύει απλά επαναφέρουν αυτό το δεσμό. Η διαδικασία αυτή διασφαλίζει ότι το κατασκοπευτικό λογισμικό θα συνεχίσει να εκτελείται ακόμα

και όταν το λειτουργικό σύστημα εκκινεί έχοντας αφαιρέσει κάποιους ή ακόμα και τους περισσότερους συνδέσμους του μητρώου.

#### 4.3.5.2 Μέσα έννομης προστασίας και πρόληψης

Δεδομένου της ραγδαίας εξάπλωσης των **spyware,** μια σειρά από τεχνικές έχουν αναπτυχθεί, για να μετριάσουν αυτό το πρόβλημα. Αυτές περιλαμβάνουν τόσο προγράμματα σχεδιασμένα για την αφαίρεση ή το μπλοκάρισμα αυτών, όσο και διάφορες πρακτικές που πρέπει να υιοθετήσουν οι χρήστες για να μειώσουν την πιθανότητα να προσβληθεί ο υπολογιστής τους από **spyware.**

Στην πράξη παρόλο την δεδομένη ανάπτυξη μηχανισμών και διαδικασιών αφαίρεσής τους τα **spyware** εξακολουθούν να αποτελούν ένα σημαντικό πρόβλημα. Όταν ένας μεγάλος αριθμός από **spyware** έχει προσβάλει έναν υπολογιστή, η μόνη δυνατή λύση είναι η δημιουργία αντιγράφων ασφαλείας των δεδομένων του χρήστη και ακολούθως η επανεγκατάσταση του λειτουργικού συστήματος.

Εν γένη δύο είναι οι βασικοί τρόποι με τους οποίους τα **anti-spyware** προγράμματα είναι σε θέση να καταπολεμήσουν τα **spyware [106]:**

- Μπορούν να παρέχουν προστασία σε πραγματικό χρόνο αποτρέποντας έτσι την εγκατάσταση κατασκοπευτικού λογισμικού στους υπολογιστές. Αυτού του είδους η προστασία κατά των **spyware** λειτουργεί με τον ίδιο ακριβώς τρόπο που λειτουργούν και τα **antivirus** προγράμματα δηλαδή ανιχνεύει όλη την εισερχόμενη κίνηση του δικτύου για τυχόν ύπαρξη κατασκοπευτικού λογισμικό και μπλοκάρει όλες τις πιθανές απειλές που εντοπίζει.

- Ένας δεύτερος τρόπος λειτουργίας για τα **anti-spyware** προγράμματα είναι να χρησιμοποιούνται αποκλειστικά για τον εντοπισμό και την απομάκρυνση **spyware** λογισμικού που έχει ήδη εγκατασταθεί στον υπολογιστή. Αυτό του είδος η προστασία είναι συνήθως πολύ πιο εύκολη στη χρήση και αρκετά πιο δημοφιλής, ενώ παράλληλα παρέχει στους χρήστες την δυνατότητα να προγραμματίζουν σε καθημερινό, εβδομαδιαίο ή και σε μηνιαίο επίπεδο, περιοδικές σαρώσεις του υπολογιστή με σκοπό την ανίχνευση και εξόντωση **spyware** λογισμικού που τυχών να έχει εγκατασταθεί σε αυτόν. Ο τρόπος λειτουργίας αυτού του λογισμικού είναι η σάρωση των περιεχομένων του μητρώου των **Windows,** των αρχείων του λειτουργικού συστήματος καθώς και των εγκατεστημένων προγραμμάτων παρέχοντας κατ' αυτό τον τρόπο έναν κατάλογο με τις πιθανές απειλές που βρέθηκαν, επιτρέποντας στους χρήστες να επιλέξουν τι θα διαγράψουν και τι θα διατηρήσουν.

Όπως σε όλα τα λογισμικά προστασίας από **malware** έτσι και στα **anti-spyware** είναι επιτακτική η συχνή ενημέρωση της βάσης δεδομένων με τις νέες απειλές. Έτσι όταν

υπάρξουν νέες απειλές οι προγραμματιστές τις εξετάζουν και τις αναλύουν δημιουργώντας στην συνέχεια υπογραφές ή ορισμούς που επιτρέπουν στο λογισμικό να τις ανιχνεύει και να τις εξαλείφει. Ωστόσο δεν στηρίζονται όλα τα προγράμματα στην ενημέρωση της βάσης. Κάποια προγράμματα στηρίζονται εν μέρη **(Windows Defender Spynet, TeaTimer, Spysweeper)** και άλλα εξολοκλήρου **(WinPatrol)**στην παρατήρηση του ιστορικού. Ουσιαστικά αυτό που κάνουν είναι να παρατηρούν τις ρυθμίσεις των παραμέτρων όπως είναι οι ρυθμίσεις του περιηγητή ή ορισμένα τμήματα του μητρώου των **Windows** και αναφέρουν οποιαδήποτε αλλαγή στον χρήστη χωρίς να παρέχουν κρίση ή κάποια προτροπή. Η έλλειψη αυτή οφείλεται στο γεγονός ότι δεν στηρίζονται στην ενημέρωση της βάσης με τα **spyware** όπου και θα τους επέτρεπε να εντοπίσουν νέες απειλές και άρα δεν είναι εφικτή η παροχή κάποιας σύστασης. Έτσι ο χρήστης μένει να αποφασίσει "τι ήταν αυτό που μόλις έκανε, και ποια είναι η κατάλληλη αλλαγή της ρύθμισης"

Το **Spynet** προσπαθεί να δώσει λύση σε αυτό το πρόβλημα μέσω της δημιουργίας μιας κοινότητας που διαμοιράζεται πληροφορίες βοηθώντας τόσο τους χρήστες που μπορούν να κοιτάξουν αποφάσεις που έχουν ήδη ληφθεί από άλλους, όσο και τους αναλυτές που μπορούν να εντοπίσουν **spyware** τα οποία εξαπλώνεται γοργά. Ένα άλλο δημοφιλές εργαλείο κατάργησης κατασκοπευτικού λογισμικού που χρησιμοποιείται από χρήστες με κάποιο βαθμό εμπειρίας είναι το **HijackThis,** το οποίο σαρώνει ορισμένες περιοχές του λειτουργικού συστήματος των **Windows** που συχνά εντοπίζονται **spyware** και παρουσιάζει μια λίστα με αντικείμενα τα οποία θα πρέπει να διαγραφούν χειροκίνητα

Συνήθως μια καλή πρακτική για να αυξηθούν οι πιθανότητες αφαίρεσης επίμονων **spyware** είναι η εκκίνηση του μολυσμένου υπολογιστή σε ασφαλή λειτουργία . Ωστόσο μία νέα γενιά **spyware (Look2Me** από την **NicTechNetworks)** έχει αρχίσει να κρύβεται στο εσωτερικό των κρίσιμων διεργασιών του συστήματος εκκινώντας έτσι ακόμα και σε **safe mode.** Καθώς δεν υπάρχει καμία διαδικασία για να τερματιστεί είναι δυσκολότερο να εντοπιστούν και να καταργηθούν και μερικές φορές δεν αφήνουν κανένα ίχνος υπογραφής στον δίσκο. Ένα άλλο εξίσου ανησυχητικό στοιχείο είναι ότι παρουσιάζουν συγκεκριμένα αντίμετρα κατά γνωστών αντικατασκοπευτικών λογισμικών εμποδίζοντάς τα να τρέχουν ή ακόμη και αποκαθιστώντας τα. Ένα χαρακτηριστικό παράδειγμα ενός **spyware** που χρησιμοποιεί αυτές τις μεθόδους είναι το **Gromozon** το οποίο χρησιμοποιεί εναλλακτικές ροές δεδομένων για να κρυφτεί.

Προκειμένου να αποτραπεί ή τουλάχιστον να περιοριστεί η πιθανή προσβολή από **spyware,** έχουν αναπτυχθεί αρκετές χρήσιμες πρακτικές πέρα από την εγκατάσταση **anti-spyware** προγραμμάτων. Ξεκινώντας, μια καλή πρακτική είναι η εγκατάσταση

ενός διαφορετικού περιηγητή από τον IE όπως είναι ο **Mozilla Firefox** η ο **Opera.** Αν και στην πράξη κανένας περιηγητής δεν είναι απόλυτα ασφαλής**,** για λόγους που έχουμε ήδη αναφέρει**,** ένας υπολογιστής ο οποίος έχει τον IE έχει τις περισσότερες πιθανότητες να προσβληθεί από **spyware.** Μια διαφορετική προσέγγιση έχει υιοθετηθεί από διάφορα κολέγια και πανεπιστήμια όπου κάνοντας χρήση των τοίχων προστασίας του δικτύου τους αλλά και των **web proxies** μπλοκάρουν την πρόσβαση σε δικτυακούς τόπους που είναι γνωστό ότι κάνουν εγκατάσταση κατασκοπευτικού λογισμικού**.** Στις **31** Μαρτίου **2005,** με έναυσμα που έδωσε το τμήμα της πληροφορικής του πανεπιστημίου **Cornell** το οποίο εξέδωσε μια αναφορά με λεπτομερή ανάλυση της συμπεριφοράς ενός συγκεκριμένου **spyware (Marketscore),** και τα μέτρα που έλαβε το ίδιο το πανεπιστήμιο για να το αναχαιτίσει οδήγησε στην υιοθέτηση αυτής της συμπεριφοράς και από πολλά άλλα εκπαιδευτικά ιδρύματα**.** Άλλη μία εξίσου διαδεδομένη πρακτική είναι η εγκατάσταση μεγάλων αρχείων με **hosts** τα οποία και χρησιμοποιούνται για την αποτροπή της σύνδεσης του υπολογιστή με ιστοσελίδες οι οποίες είναι συσχετισμένες με την χρήση **spyware.** Ωστόσο**,** κάνοντας σύνδεση με την διεύθυνση **IP,** αντί με το όνομα του τομέα τα **spyware** είναι σε θέση να παρακάμψουν αυτό το είδος προστασίας**.** Κλείνοντας μια άλλη πρακτική είναι να κατεβάζουμε προγράμματα μόνο από αξιόπιστες τοποθεσίες και αυτό διότι είναι συχνή η προσβολή από **spyware** μέσω της εγκατάστασης προγραμμάτων τύπου **shareware (**πρόσφατα η **CNet** ανανέωσε τον κατάλογο κατεβάσματος ανακοινώνοντας ότι θα διατηρεί μόνο αρχεία που περνούν τον έλεγχο από τα το **Ad-Aware** και το **Spyware Doctor).**

#### 4.3.5.3 Αξιοσημείωτα προγράμματα που διανέμονται - διανέμονταν μαζί με κατασκοπευτικό λογισμικό

- **Grokster**
- **Kazaa**
- **LimeWire (**εγκαθιστά το **Mirar Toolbar** μεταξύ άλλων εφαρμογών που διαταράσσουν σοβαρά τη χρήση του υπολογιστή**)**
- **Morpheus**
- **EDonkey2000**
- **Sony 's Extended Copy Protection**
- **AOL Instant Messenger**
- **DivX (**εκτός από την έκδοση επί πληρωμής**,** και από την **"**πρότυπη**"** έκδοση χωρίς τον κωδικοποιητή**).** Η **DivX** ανακοίνωσε την απομάκρυνση αυτού του λογισμικού από την έκδοση **5.2**

- **FlashGet (**η δοκιμαστική έκδοση πριν το πρόγραμμα γίνει **freeware)**

#### 4.3.5.4 Ψεύτικα anti-spyware προγράμματα

Κακόβουλοι προγραμματιστές έχουν κυκλοφορήσει ένα μεγάλο αριθμό απομιμήσεων προγραμμάτων **anti-spyware,** και διένειμαν ευρέως διαφημιστικά **banners** προειδοποιώντας τους χρήστες των οποίων οι υπολογιστές έχουν προσβληθεί με **spyware,** να αγοράσουν τα προγράμματα τα οποία στην πραγματικότητα όχι μόνο δεν αφαιρούσαν τα **spyware** αλλά προσθέταν ακόμα περισσότερα**.** Χαρακτηριστικά παραδείγματα αυτής της κατηγορίας είναι τα εξής**:**

- **AntiVirus Gold**
- **Errorsafe (AKA system doctor)**
- **MacSweeper**
- **PSGuard**
- **Spy Sheriff**
- **UltimateCleaner**
- **WinAntiVirus Pro 2006**

### 4.3.6 Adware

Λογισμικό **adware** ή λογισμικό υποστήριξης διαφημίσεων είναι οποιοδήποτε πακέτο λογισμικού που αυτόματα, παίζει, εμφανίζει**,** ή κατεβάζει διαφημιστικό υλικό σε έναν υπολογιστή**,** αφού έχει γίνει εγκατάσταση αυτού ή κατά την διάρκεια της εκτέλεσής του**.** Ορισμένα είδη **adware** είναι επίσης και **spyware** και μπορούν να θεωρηθούν ως λογισμικό παραβίασης της ιδιωτικότητας**.**

#### 4.3.6.1 Εφαρμογή

Το **adware [46]** είναι λογισμικό με λειτουργίες διαφήμισης οι οποίες ενσωματώνονται ή ομαδοποιούνται μαζί με ένα πρόγραμμα**.** Όπως εύκολα γίνετε αντιληπτό αυτού του είδους το λογισμικό έχει σαν απώτερο σκοπό την αποφορά χρημάτων στους συγγραφείς τους **(**λόγω των διαφημίσεων**)** παρακινώντας τους έτσι κατά αυτό τον τρόπο να συνεχίσουν να αναβαθμίζουν και να αναπτύσσουν νέο λογισμικό. Μία άλλη δυνατότητα των **adware** είναι ότι μπορούν να κατεβάζουν και να εγκαθιστούν στον υπολογιστή **PUPs (Potentially unwanted programs,** ένας όρος που αναφέρεται σε λογισμικό που πιθανόν δεν θέλουμε να εγκατασταθεί χωρίς ωστόσο να είναι τόσο ενοχλητικό όσο είναι τα **spyware).**

#### 4.3.6.2 Γνωστά adware προγράμματα / προγράμματα που διανέμονται μαζί με adware:

- **123 Messenger**
- **Yahoo Messenger**
- **Cursor Mania**
- **Daemon Tools – (**Το λογισμικό είναι ενσωματωμένο με το **"Daemon Tools WhenUSave Toolbar"** αλλά δεν είναι δυνατό να μην επιλεχθεί κατά την διάρκεια της εγκατάστασης **)**
- **Kazaa**
- **Messenger Plus! Live (**Είναι προαιρετική η εγκατάσταση χορηγών**)**
- **RealPlayer**
- **Sweet IM**
- **VirusProtectPro**

Το λογισμικό διαχείρισης **e-mail Eudora** αποτελεί ένα δημοφιλές παράδειγμα μίας **adware** εφαρμογής σε ένα πρόγραμμα. Μετά το πέρας της δοκιμαστικής περίοδου κατά την οποία όλα τα χαρακτηριστικά του προγράμματος είναι διαθέσιμα, ο χρήστης καλείται να επιλέξει μεταξύ των εξής εκδόσεων: μίας δωρεάν αλλά περιορισμένης λειτουργικότητας, μιας έκδοσης με όλα τα χαρακτηριστικά ενεργοποιημένα αλλά με επιπρόσθετες λειτουργίες **(**διαφημιστικά**)** ή μιας έκδοσης επί πληρωμή με πλήρη λειτουργικότητα και χωρίς διαφημίσεις.

#### 4.3.6.3 Πρόληψη και εντοπισμός

Καθώς υπάρχουν πολλά παραδείγματα **adware** λογισμικού που είναι επίσης **spyware** ή γενικότερα **malware**, έχουν αναπτυχθεί πολλά προγράμματα προστασίας για την ανίχνευση, την απομόνωση, και την αφαίρεση των **adware.** Μεταξύ των πιο διακεκριμένων προγραμμάτων αυτού του είδους είναι το **Ad-Aware** και το **Spybot - Search & Destroy** τα οποία έχουν αναπτυχθεί ειδικά για την ανίχνευση **spyware** και δεν ανιχνεύουν ιούς, παρόλο που μερικά διαφημιστικά προγράμματα προστασίας παρέχουν αυτή την δυνατότητα.

### 4.3.7 Λογικές βόμβες

Οι Λογικές Βόμβες **[112]** τυπικά είναι μικρά προγράμματα, τα οποία προστίθενται σε κάποιο υπάρχον πρόγραμμα, ή ακόμη και τροποποιήσεις σε υπάρχοντα κώδικα. Καλούνται έτσι, διότι είναι προγραμματισμένες να «εκραγούν» υπό συγκεκριμένες προϋποθέσεις. Η Λογική Βόμβα πρέπει να προστεθεί στο πρόγραμμα που θα

προσβάλει από κάποιον που έχει πρόσβαση στο σύστημα και την κατάλληλη γνώση προκειμένου να το τροποποιήσει. Η πρόσβαση μπορεί να αποκτηθεί με κάποιο από τους γνωστούς τρόπους υποκλοπής κωδικών, π.χ. **login spoofing**. Οι Λογικές Βόμβες δεν τείνουν να προσβάλλουν **PCs** όσο συγκεκριμένο λογισμικό που τρέχει σε συγκεκριμένες πλατφόρμες ή πιο γενικευμένα εταιρείες. Ένα παράδειγμα που θα μπορούσε να δοθεί είναι ένα τμήμα κώδικα που έχει προστεθεί από προγραμματιστή εταιρείας στο λειτουργικό σύστημα που χρησιμοποιείται. Για όσο ο προγραμματιστής τροφοδοτεί τον υπολογιστή με τον κωδικό πρόσβασής του δε συμβαίνει τίποτε. Σε περίπτωση απόλυσής του, η βόμβα, μετρώντας κάποιο χρονικό διάστημα που δεν έχει δεχτεί κωδικό πρόσβασης, θα «εκραγεί» με αποτελέσματα, όπως καθαρισμό δίσκων, διαγραφή τυχαίων αρχείων ή κρυπτογράφηση βασικών αρχείων. Σε ένα άλλο σενάριο, η Λογική Βόμβα κάνει έλεγχο στην κατάσταση μισθοδοσίας του προγραμματιστή και αν ο προσωπικός αριθμός του δεν εμφανιζόταν σε δύο συνεχόμενες περιόδους μισθοδοσίας, τότε η βόμβα «εκρήγνυτο».

Αρκετά είδη κακόβουλου λογισμικού όπως οι ιοί και τα σκουλήκια, συχνά περιέχουν λογικές βόμβες που ενεργοποιούνται αυτόματα μετά από ένα προκαθορισμένο χρονικό διάστημα ή όταν κάποιες άλλες λογικές συνθήκες γίνουν αληθείς. Η τεχνική αυτή χρησιμοποιείται για να αποκτήσει προβάδισμα το κακόβουλο λογισμικό και να εξαπλωθεί πριν γίνει αντιληπτό. Πολλοί ιοί που περιέχουν λογικές βόμβες επιτίθενται στα συστήματα σε συγκεκριμένες ημερομηνίες όπως είναι Παρασκευή και **13** ή Πρωταπριλιά. Τα **trojans** που ενεργοποιούνται στις ορισμένες ημερομηνίες συχνά αποκαλούνται "ωρολογιακές βόμβες".

Για να θεωρηθεί ένα πρόγραμμα ως λογική βόμβα πρέπει το ωφέλιμο φορτίο που περιέχει να είναι ανεπιθύμητο και άγνωστο στο χρήστη του λογισμικού, δηλαδή τα δοκιμαστικά προγράμματα, με κωδικό που απενεργοποιεί ορισμένες λειτουργίες τους μετά από ένα χρονικό διάστημα, δεν θεωρούνται λογικές βόμβες.

#### 4.3.7.1 Ιστορική αναδρομή

- Ο Μιχαήλ Άγγελος ήταν μια λογική βόμβα σχεδιασμένη να ενεργοποιείται κάθε χρόνο (από τις αρχές της δεκαετίας του **1990**), στην επέτειο των γενεθλίων του ομωνύμου ζωγράφου (**6** Μαρτίου). Το **1992 20.000** υπολογιστές επηρεάστηκαν από αυτή την λογική βόμβα και μόνο δύο κατά το **1998**.

- Τον Ιούνιο του **1992** συνελήφθη ένας υπάλληλος της **General Dynamics**, ο **Michael Lauffenburger**, για την εισαγωγή μιας λογικής βόμβας που θα διέγραφε ζωτικής σημασίας στοιχεία για τον σχεδιασμό ενός πυραύλου. Ο ίδιος ισχυρίστηκε ότι το σχέδιό του ήταν να επιστρέψει ως σύμβουλος της εταιρίας για να λύσει το πρόβλημα μόλις αυτή ενεργοποιόταν. Ο **Lauffenburger** κατηγορήθηκε για απάτη και

απόπειρα παραποίησης αντιμετωπίζοντας πρόστιμο ύψους **500.000** δολαρίων και φυλάκιση**.**

**Ø** Τον Φεβρουάριο του **2000,** ο **Tony Xiaotong,** κατηγορήθηκε από μια ανώτερη επιτροπή για την τοποθέτηση μιας λογικής βόμβας κατά τη διάρκεια της απασχόλησής του ως προγραμματιστής και έμπορος της **Deutsche Morgan Grenfell.** Η βόμβα**,** που είχε εγκατασταθεί το **1996,** είχε ως ημερομηνία ενεργοποίησης τις **20** Ιουλίου του **2000,** αλλά ανακαλύφθηκε από άλλους προγραμματιστές της εταιρείας όπου και χρειάστηκαν αρκετούς μήνες για να μπορέσουν να την αποκαταστήσουν και να καθαρίσουν το σύστημα**.**

**Ø** Στις **2** Οκτωβρίου του **2003** η **Yung-Hsun Lin,** γνωστή επίσης και ως **Andy Lin,** άλλαξε τον κώδικα σε ένα **server** στην **Medco Health Solutions** Α**.**Ε**.** δημιουργώντας μια λογική βόμβα που ενεργοποιούταν στα γενέθλιά της το **2004.** Ωστόσο εξαιτίας ενός προγραμματιστικού σφάλματος απέτυχε να ενεργοποιηθεί**,** και έτσι η **Lin** διόρθωσε το σφάλμα και έθεσε ως νέα ημερομηνία ενεργοποίησης τα επόμενα γενέθλιά της**,** αλλά ανακαλύφθηκε και από ένα διαχειριστή της **Medco** σε λίγους μήνες πριν από την ημερομηνία ενεργοποίησης**.** Η **Lin** ομολόγησε την ενοχή της και καταδικάστηκε σε **30** μήνες φυλάκιση σε ομοσπονδιακή φυλακή και σε πρόστιμο ύψους **81.200$** μειώνοντας έτσι την ποινή από **10** χρόνια φυλάκιση και πρόστιμο ύψους **250000$.**

**Ø** Τον Ιούνιο του **2006** ο **Roger Duronio,** ένας διαχειριστής συστήματος της **UBS** είχε κατηγορηθεί για απάτη και για την χρησιμοποίηση μιας λογικής βόμβας με σκοπό την πρόκληση ζημιών στο δίκτυο υπολογιστών της εταιρείας με στόχο την κατακόρυφη μείωση του μετοχικού της κεφαλαίου**.** Ο **Duronio** δικάτικε αργότερα και καταδικάστηκε με **8** έτη και **1** μήνα φυλάκιση καθώς και με πρόστιμο ύψους **3.1** εκατομμύριων δολαρίων**.**

## 4.4 Ιστορικές Επιθέσεις- παραδείγματα δράσης κακόβουλου λογισμικού

### 4.4.1 Το Σκουλήκι του Διαδικτύου

Πρόκειται για μία από τις πρώτες μεγάλες επιθέσεις που δέχθηκε το **Internet** από σκουλήκι**.** Το Σκουλήκι του Διαδικτύου εμφανίστηκε το βράδυ της **2**ας Νοεμβρίου **1988** και μέσα σε ελάχιστες ώρες προσέβαλε μηχανήματα **VAX** και **Sun-3** που έτρεχαν λειτουργικό **Berkeley UNIX** ή παρόμοια **(**π**.**χ**. SunOS)** σε ολόκληρη την έκταση των Ηνωμένων Πολιτειών**.** Η επόμενη μέρα **(**που χαρακτηριστικά ονομάστηκε Μαύρη Πέμπτη**)** βρήκε τους διαχειριστές των συστημάτων να

προσπαθούν μάταια να επανεκκινήσουν τους υπολογιστές τους**,** ενώ ένα κλίμα πανικού επεκτάθηκε όπου είχε προηγουμένως περάσει το Σκουλήκι **(**Πίνακας **10).**

| Ιστορικό Επίθεσης | | |
|---|---|---|
| Ημερομηνία | Ώρα | Γεγονότα |
| 2/11/1988 | 18:00 | Η ακριβής ώρα δράσης δεν έγινε ποτέ γνωστή, αλλά αυτή αναφέρεται ως η επικρατέστερη. Το VAX11/750 του MIT Artificial Intelligence Lab, με όνομα prep.ai.mit.edu, γίνεται ο πρώτος στόχος. Στο μηχάνημα αυτό δεν υπήρχε τακτική μέθοδος backup, ούτε μηχανισμός accounting, γι'αυτό τα ίχνη του Σκουληκιού δεν εντοπίστηκαν. Το Σκουλήκι μπήκε στο σύστημα χρησιμοποιώντας κάποιους από τους πολλούς δημόσιους λογαριασμούς του συστήματος. |
| | 18:24 | Πρώτος επίσημος στόχος: rand.org (Rand Corp., Santa Monica) |
| | 19:04 | Προσβάλλεται το csgw.berkeley.edu. Το μηχάνημα αυτό είναι και το gateway του Πανεπιστημίου του Berkeley. Γίνεται άμεσα αντιληπτό από τους διαχειριστές. |
| | 19:54 | Χτυπάει το finger server του mimsy.umd.edu στο τμήμα Υπολογιστικών Υπηρεσιών του Πανεπιστημίου του Maryland. |
| | 20:00 | 'Εχουν χτυπηθεί τα Sun του MIT AI Lab. |
| | 20:40 | Το Berkeley ανακαλύπτει επιθέσεις από το sendmail και το rsh. Περίεργη συμπεριφορά των finger και telnet. Αναγκάζονται να κλείσουν συστήματα. |
| | 20:49 | Προσβάλλεται ο cs.utah.edu, ο κεντρικός εξυπηρετητής του τμήματος Υπολογιστικών Υπηρεσιών του Πανεπιστημίου της Utah. (Τα γεγονότα παρακάτω είναι καταγεγραμμένα από την Utah και είναι παρόμοια και σύγχρονα με άλλα αμερικάνικα Πανεπιστήμια). |
| | 21:09 | Επίθεση από sendmail στον cs.utah.edu. |
| | 21:21 | Ο μέσος φόρτος (διεργασίες στην ουρά το λεπτό) του cs.utah.edu φθάνει το 5. Πριν τις 21:00 ήταν 0.2-2, ενώ μία τιμή 20 μπορούσε να φορτώσει τόσο πολύ το σύστημα που θα ήταν άχρηστο για οτιδήποτε άλλο. |
| | 21:41 | Ο μέσος φόρτος στο cs.utah.edu φθάνει το 7. |
| | 22:01 | Ο μέσος φόρτος στο cs.utah.edu φθάνει το 16. |
| | 22:06 | Το cs.utah.edu τρέχει ταυτόχρονα 100 διαδικασίες (το μέγιστό του). Πλέον καθίσταται άχρηστο. |
| | 22:20 | Καταφέρνουν να καθαρίσουν το Σκουλήκι στο cs.utah.edu. Ωστόσο έχουν προσβληθεί όλα τα υπόλοιπα μηχανήματα Sun του Utah. |
| | 22:41 | Προσβάλλεται πάλι το cs.utah.edu. Ο μέσος φόρτος φθάνει το 27. |
| | 22:49 | Οι διαχειριστές του cs.utah.edu αναγκάζονται να κλείσουν προσωρινά το σύστημα μέχρι να βρεθεί αιτία. |
| | 23:21 | Στην επανεκκίνηση ο μέσος φόρτος φθάνει το 37. |
| | 23:28 | Ο Peter Yee από τη NASA στέλνει το ακόλουθο μήνυμα στη λίστα TCP/IP:<br><br>«Δεχόμαστε επίθεση από έναν ιό του διαδικτύου. Έχει |

| | | |
|---|---|---|
| | | προσβάλει ήδη τα UC Berkeley, UC San Diego, Lawrence Livermore, Stanford και NASA Ames».<br><br>Συμβουλεύει την απενεργοποίηση των telnet, ftp, finger, rsh, SNMP αλλά δεν αναφέρει το rexec |
| 3/11/88 | 00:34 | Ο Andy Sudduth του Harvard στέλνει ανώνυμα mail στη λίστα TCP/IP περιγράφοντας για πρώτη φορά πώς γίνεται η επίθεση από το finger, πώς να αποτραπεί η επίθεση από το sendmail, ενώ αναφέρει για πρώτη φορά επιθέσεις από το rexec. Δυστυχώς το μήνυμα δεν παραδίδεται στη λίστα παρά 2 μέρες αργότερα, επειδή ο relay.cs.net έχει βγει εκτός λειτουργίας, προσβεβλημένος από το Σκουλήκι. |
| | 02:54 | Στέλνεται στη λίστα TCP/IP καθώς και στο newsgroup comp.bugs.4bsd.ucb-fixes ένα fix για το sendmail. |
| | Νωρίς το πρωί | Το wtmp session log χάνεται μυστηριωδώς από το prep.ai.mit.edu. |
| | 05:07 | Από το Berkeley στέλνεται αναφορά για την επίθεση από το finger, αλλά το μήνυμα δε γίνεται αντιληπτό για τις επόμενες 12 ώρες. |
| | 09:00 | Αρχίζει το ετήσιο Berkeley Unix Workshop στο Πανεπιστήμιο του Berkeley. Παραπάνω από 40 διαχειριστές σημαντικών συστημάτων βρίσκονταν στην California την ώρα που ξεσπούσε η κρίση. |
| | 15:00 | Μια ομάδα από το MIT ανακαλύπτει το bug του finger. |
| | 16:26 | Απομονώνεται το Σκουλήκι και αρχίζει η προσπάθεια για το disassemble και decompile στο Berkeley. |
| | 18:00 | Παράλληλη δουλειά και στο MIT. |
| 4/11/1988 | 06:00 | Η ομάδα του Berkeley καταφέρνει να αποκωδικοποιήσει το Σκουλήκι. |
| | 12:36 | Ανακοίνωση από το MIT ότι οι ομάδες Berkeley και MIT κατάφεραν να αποκωδικοποιήσουν το Σκουλήκι. |
| | 17:00 | Γίνεται μικρή παρουσίαση του Σκουληκιού στο τέλος του Berkeley Unix Workshop. |
| 8/11/1988 | | Το National Computer Security Center των ΗΠΑ συναντάται για να συζητήσει για το Σκουλήκι. |
| 11/11/1988 | | Παρουσιάζεται η πλήρως αποκωδικοποιημένη έκδοση του Σκουληκιού με σχολιασμένο κώδικα. |

**Πίνακας 10.Το ιστορικό της επίθεσης**

Είναι προφανής ο πανικός που δημιούργησε η επίθεση του Σκουληκιού, ενός καλογραμμένου προγράμματος, για το οποίο αρχικά δεν υπήρχε καμία ένδειξη της λειτουργίας του. Όπως φάνηκε αργότερα, αποτελείτο από **99** γραμμές κώδικα αρχικοποίησης **(bootstrap)** σε **C** και έναν επιπλέον μεγάλο **object code** που κυκλοφορούσε σε διάφορες εκδόσεις **(**ανάλογα αν ο στόχος ήταν **VAX** ή **Sun-3).** Η αποκωδικοποίηση αυτού του κώδικα έδωσε **3200** γραμμές προγράμματος **C.**

Η δράση του Σκουληκιού μπορεί να κατηγοριοποιηθεί σε επίθεση και άμυνα**:**

Ø Επίθεση

Αρχικά προσπαθούσε να εισέλθει στο σύστημα χρησιμοποιώντας τρύπες γνωστών δικτυακών προγραμμάτων και στη συνέχεια χρησιμοποιώντας διάφορα συνηθισμένα αρχεία συστήματος **(/etc/hosts.equiv, ~/.rhosts,** κλπ.**)** προσπαθούσε να εντοπίσει νέους πιθανούς στόχους. Ακόμη αναζητούσε λογαριασμούς χρηστών, ώστε να μπορέσει να χρησιμοποιήσει την κοινή πρόσβαση μέσω **rsh** και **rexec** για να προχωρήσει και σε άλλα συστήματα.

Ø Άμυνα

Αρχικά άλλαζε την ταυτότητά του σε **sh,** το πιο συνηθισμένο μεταγλωτιστή εντολών στο **Unix,** ώστε να μην εντοπίζεται εύκολα. Επίσης, άλλαζε συνέχεια τα **PIDs,** ώστε να μην μπορεί να τερματιστεί με κάποια **kill.** Τα αρχεία του παρέμεναν για ελάχιστο χρονικό διάστημα στο δίσκο και ακόμα και αν εντοπίζονταν, τα ονόματά τους ήταν δυσνόητα, ώστε να μην είναι άμεσα ορατή η λειτουργία τους.

Ο πραγματικός σκοπός του, ωστόσο, δεν ήταν η καταστροφή των συστημάτων που προσέβαλε. Αυτό προκύπτει από συγκεκριμένα στοιχεία της δράσης του, όπως:

- Δεν έσβηνε αρχεία συστήματος ούτε τροποποιούσε υπάρχοντα αρχεία με κανένα τρόπο και για κανένα σκοπό.
- Δεν κρατούσε για μελλοντική χρήση του κωδικούς του προσβληθέντος εκάστοτε συστήματος.
- Για τη μεταφορά του χρησιμοποιούσε το **TCP/IP** και δεν προσπαθούσε εισβολή μέσω **UUCP (Unix-to-Unix CoPy)** ή των **X.25** και **BITNET.**
- Δεν προσπαθούσε να αποκτήσει πρόσβαση διαχειριστή, αφού μπορούσε να πετύχει τους στόχους του και ως χρήστης.

Το Σκουλήκι του Διαδικτύου πέτυχε επίθεση τύπου **DoS (Denial of Service – Άρνηση Υπηρεσίας),** αφού το σύστημα δεν μπορούσε να εξυπηρετήσει τις υπηρεσίες που ζητούσαν οι χρήστες, μιας και τα Σκουλήκια απασχολούσαν αποκλειστικά τη **CPU.** Ένα ακόμη παράξενο είδος **DoS** που εμφανίστηκε ήταν το γεγονός ότι οι διαχειριστές των συστημάτων, κυριευμένοι από τον πανικό μόλυνσης, δε δίσταζαν να βγάλουν τα συστήματα εκτός λειτουργίας. Με αυτό τον τρόπο, όμως, αποκόπτονταν από τις συντονισμένες προσπάθειες όλων των άλλων να θέσουν σε έλεγχο την κατάσταση, ενώ απόκοπταν και την επικοινωνία σε άλλους ενδιαφερόμενους **(**Πίνακας **10).**

Πολλά ειπώθηκαν για τους στόχους του Σκουληκιού του Διαδικτύου. Το σίγουρο είναι πως η καταστροφή δεν ήταν ο σκοπός του. Υπήρξε μια εκδοχή ότι ήταν ένα καλοσχεδιασμένο πείραμα που ξέφυγε από τον έλεγχο των ιθυνόντων. Πάντως, οι

διαχειριστές και οι λοιποί χρήστες διδάχτηκαν πως θα πρέπει να είναι πιο έτοιμοι στο μέλλον. Τέλος, αξιοσημείωτο είναι το γεγονός ότι εξαιτίας του Σκουληκιού του Διαδικτύου θεμελιώθηκε το **CERT©CC** το **1988.**

### 4.4.2 Pakistani-Brain Virus

Ένας από τους πιο γνωστούς ιούς στον κόσμο των **IBM-PCs** υπήρξε ο **Pakistani (**Πακιστανός**)** ή **Brain (**Εγκέφαλος**)** ιός **[32].** Θεωρείται ο πρώτος ιός που προσέβαλε Η/Υ εκτός εργαστηρίου. Σύμφωνα με την **Ann Webster** του Ακαδημαϊκού Υπολογιστικού Κέντρου του Πανεπιστημίου του **Delaware, Newark** η πρώτη αναφορά χρονολογείται στις **22** Οκτώβρη του **1987.** Είχε εντοπιστεί και σε άλλες τοποθεσίες στο χώρο του Πανεπιστημίου μία ή δύο μέρες νωρίτερα.

Ονομάστηκε **Brain (**Εγκέφαλος**),** διότι ονόμαζε έτσι όποια δισκέτα προσέβαλε. Μετά την αρχική ανάλυση του ιού βρέθηκαν δύο ονόματα, **Basit** και **Amjad,** και η διεύθυνση τους στο **Lehore,** Πακιστάν. Έτσι, ο **Brain** απέκτησε το όνομα **Pakistani (**Πακιστανός**).**

Όταν, λοιπόν μία **«**μολυσμένη**»** δισκέτα εισερχόταν σε κάποιον υπολογιστή, ο ιός έφτιαχνε αντέγραφε τον εαυτό του στις υψηλότερες θέσεις μνήμης και άλλαζε το μέγεθος της μνήμης που έβλεπε το σύστημα τροποποιώντας το **interrupt vector (**διάνυσμα διακοπής**)** Α**2**Η με σκοπό να προστατέψει το αντίγραφο που είχε φτιάξει. Επίσης τροποποιούσε και το **interrupt vector 13**Η ώστε να δείχνει στον κώδικα του στις υψηλές θέσεις μνήμης και το **6**Η **(**αχρησιμοποίητο από τις υπάρχουσες εκδόσεις του **DOS)** ώστε να δείχνει στο **interrupt vector 13**Η. Μετά από αυτά τα γεγονότα, η κανονική διαδικασία εκκίνησης συνεχιζόταν φορτώνοντας τα **IBMBIO.COM** και **IBMDOS.COM** σε **PC-DOC** ή **IO.SYS** και **MSDOS.SYS** σε **MS-DOS.**

Η **«**μολυσμένη δισκέτα περιλάμβανε ένα μήνυμα και μέρος του κώδικα του ιού στον τομέα **(sector)** εκκίνησης. Ο υπόλοιπος κώδικας και ένα αντίγραφο του αρχικού τομέα εκκίνησης **(boot sector)** της δισκέτας περιλαμβανόταν σε τρείς ομάδες **(clusters)** (ή έξι τομείς **– sectors),** τις οποίες ο ιός ονόμαζε **«**χαλασμένες**»** στο **FAT.**

Με τον ιό στις υψηλές θέσεις μνήμης ήταν αδύνατο να διαβαστεί ο μολυσμένος τομέας εκκίνησης. Αν γινόταν κάποια προσπάθεια να διαβαστεί ο τομέας εκκίνησης, τότε ο Πακιστανός κατεύθυνε την αίτηση ανάγνωσης στον αρχικό τομέα εκκίνησης που αποθήκευε σε κάποια από τις **«**χαλασμένες**»** ομάδες. Ο μόνος τρόπος να αναγνωστεί το μήνυμα του Εγκεφάλου που βρισκόταν στον τομέα εκκίνησης ήταν να εκκινήσεις το σύστημα με μία μη **«**μολυσμένη**»** δισκέτα και να τοποθετήσεις τη **«**μολυσμένη**»** δισκέτα στην κεφαλή **(drive)** Β. Το μήνυμα ήταν το εξής:

**“Welcome to the Dungeon…Beware of this Virus…Contact us for Vaccination……”**

Επίσης δινόταν η ακριβής διεύθυνση μίας εταιρείας υπολογιστών στο Πακιστάν και συγκεκριμένα:

**©1986 Basit & Amjad (pvt) Ltd. BRAIN COMPUTER SERVICES, 730 NIZAM BLOCK ALLAMA IQBAL TOWN, LAHOR, PAKISTAN**

Ο ιός διέκοπτε κάθε αίτηση ανάγνωσης στη δισκέτα. Αν αυτή η αίτηση δεν ήταν για τον τομέα εκκίνησης ή για οποιαδήποτε άλλη πηγή εκτός από τη δισκέτα, τότε ο ιός διάβαζε τον τομέα εκκίνησης της δισκέτας και εξέταζε το τέταρτο και το πέμπτο **byte** για **"1234,"** και τα αποθήκευε ως **34 12,** την υπογραφή του Εγκέφαλου. Αν αυτή η υπογραφή δεν υπήρχε στη δισκέτα, ο ιός τη **«**μόλυνε**»** και συνέχιζε με την αίτηση ανάγνωσης με την προϋπόθεση ότι η δισκέτα δεν είχε προστασία εγγραφής. Κανονικά, στην προσπάθειά του να **«**μολύνει**»** τη δισκέτα ο Εγκέφαλος θα έψαχνε τρεις ομάδες για να τις μαρκάρει ως χαλασμένες. Αν δεν υπήρχαν κενές, ο ιός δε θα μόλυνε τη δισκέτα. Παρόλα αυτά, αν υπήρχε μόνο μία κενή ομάδα και δεν ήταν καμία από τις δύο τελευταίες στο δίσκο, ο ιός θα επέλεγε αυτή την ομάδα, θα αντικαθιστούσε τις επόμενες δύο ομάδες και μετά θα τις μάρκαρε ως **«**χαλασμένες**»**. Αν το υλικό που αντικαταστάθηκε ήταν μέρος κάποιου αρχείου, το αρχείο θα εξαφανιζόταν και αυτός ήταν ένας τρόπος να εντοπιστεί ο ιός.

### 4.4.3 Παρασκευή και 13-Ισραήλ

Το Υπολογιστικό Κέντρο του Εβραϊκού Πανεπιστημίου της Ιερουσαλήμ μολύνθηκε από έναν ιό που προσέβαλε **IBM-PCs**. Ο ιός αντέγραφε τον εαυτό του σε όλα τα προγράμματα που έτρεχαν στο μολυσμένο υπολογιστή. Παρόλα αυτά, υπήρχε ένα προφανές λάθος ή **bug** στον ιό, καθώς ένα ήδη μολυσμένο πρόγραμμα θα μπορούσε να ξαναμολυνθεί από τον ιό. Σταδιακά, αυτό προκαλούσε την ανεξέλεγκτη αύξηση μεγέθους των προγραμμάτων, με αποτέλεσμα να μη χωρούν στη μνήμη του υπολογιστή.

Όταν τελικά απομονώθηκε ο ιός, ανακαλύφθηκε ότι ήταν προγραμματισμένος να ενεργοποιηθεί Παρασκευή και **13**. Πολλοί πιστεύουν ότι στόχος ήταν η Παρασκευή, **13** Μαΐου **1988**- η **40**η επέτειος του Ισραήλ. Αν ο ιός είχε ενεργοποιηθεί, όλα τα μολυσμένα προγράμματα θα είχαν διαγραφεί από το δίσκο. Υπάρχουν μερικές ακόμα παραλλαγές αυτού του ιού με διαφορετικές ημερομηνίες ενεργοποίησης.

### 4.4.4 Η Χριστουγεννιάτικη Κάρτα της IBM

**Ο «**ιός**»** Χριστουγεννιάτικη Κάρτα της **IBM** δεν ήταν ακριβώς ένας ιός και δε μόλυνε μεμονωμένα υπολογιστικά συστήματα. Είχε, όμως τρομακτικά αποτελέσματα στο ηλεκτρονικό ταχυδρομείο της **IBM** κατά τη διάρκεια του Δεκεμβρίου του **1987**. Το πρόγραμμα του **«**ιού**»** ήταν ένα ηλεκτρονικό μήνυμα **(email)**, το οποίο

δημιουργήθηκε στην Ευρώπη. Το μήνυμα εμφάνιζε μια Χριστουγεννιάτικη Κάρτα στην οθόνη του αποδέκτη, ενώ έστελνε αντίγραφα του εαυτού του σε όλες τις διευθύνσεις **email** του «βιβλίου διευθύνσεων» του. Το μήνυμα σύντομα διέσχισε τον Ατλαντικό Ωκεανό και διείσδυσε σε άλλα δίκτυα **email** συμπεριλαμβανομένου και του παγκοσμίου δικτύου της **IBM**. Κατόπιν, τα δίκτυα **email** γέμισαν από αντίγραφα της Χριστουγεννιάτικης Κάρτας μπαίνοντας τελικά σε κατάσταση αναμονής **(halt)**. Χρειάστηκαν από μία μέχρι τρεις μέρες για να «καθαρίσουν» τα δίκτυα από το μήνυμα της Χριστουγεννιάτικης Κάρτας.

### 4.4.5 Η επίθεση των Ολλανδών Hackers

Την **1**η Απριλίου **1990** ξεκίνησε η προσπάθεια εισβολής στο **domain .mil (**Αμερικανικός Στρατός**)** και διήρκεσε σχεδόν δύο χρόνια. Στο **CERT ® /CC** αναφέρεται ως το πιο μακροχρόνιο περιστατικό και είχε προσβάλει **383 sites,** ένα εκ των οποίων ήταν ελληνικό. Η εν λόγω επίθεση εκτυλίσσεται κατά τη διάρκεια του Περσικού Πολέμου και ορισμένες από τις προεκτάσεις της θα μπορούσαν να είχαν επιπτώσεις στην αποστολή.Οι **hackers** εισέβαλαν σε **34** αμερικάνικα στρατιωτικά **sites** στο **Internet,** συμπεριλαμβανομένων και **sites** που συμμετείχαν στην επιχείρηση **"Desert Storm/Shield".** Αναζήτησαν λέξεις, όπως **"desert shield", "desert storm", «**πυρηνικά**», «**όπλα**», «**πύραυλοι**»** και βρήκαν πληροφορίες για την ακριβή θέση των αμερικανικών στρατευμάτων, τον τύπο των όπλων τους, τις δυνατότητες των πυραύλων **Patriot** και τις κινήσεις των αμερικάνικων πλοίων. Ο **Jim Christy,** ένας από τους υπεύθυνους του προγράμματος για την ανακάλυψη εγκλημάτων σε θέματα πολέμου των πληροφοριών, του γραφείου της αμερικάνικης αεροπορίας **(Air Force Office of Special Investigations)** αναφέρει ότι οι επιθέσεις αφορούσαν και συστήματα τροφοδοσίας των στρατευμάτων στον Κόλπο. Χαρακτηριστικά έχει δηλώσει στο **ABCNews : «**Θα μπορούσαν αντί για πυρομαχικά να είχαν στείλει οδοντόβουρτσες**».**

Οι **hackers** συγκέντρωσαν μέρος της πληροφορίας τους σε χώρο των υπολογιστικών συστημάτων στο **Bowling Green University** και στο **University of Chicago.** Οι εισβολείς επιχείρησαν ακόμη και να πουλήσουν πληροφορίες στους Ιρακινούς κατά τη διάρκεια του πολέμου. Η πληροφορία μεταδόθηκε μέσω του **BBC**, που πήρε την πληροφορία από κυβερνητικούς αξιωματούχους του Ιράκ, αλλά ο Σαντάμ Χουσεΐν αρνήθηκε την προσφορά των **hackers,** γιατί θεώρησε ότι ήταν παγίδα.

Οι εισβολείς ακόμα και όταν εντοπίστηκαν δεν ήταν δυνατό να συλληφθούν, καθώς εκείνο τον καιρό οι επιθέσεις σε υπολογιστές δεν ήταν παράνομες. Το **FBI** προσπάθησε να παγιδεύσει τον εμπνευστή της ομάδας των **hackers,** φέρνοντας τον

στην Αμερική με πρόφαση μια συνέντευξη για δουλειά από μεγάλη αεροναυπηγική εταιρεία στη **Florida,** μα εκείνος αθέλητα ειδοποιήθηκε και το αντιλήφθηκε**.** Εν τέλει δύο από τους Ολλανδούς **Hackers** συλλαμβάνονται και οδηγούνται στη φυλακή για παραποίηση στοιχείων και χρήση πιστωτικής κάρτας**! (**Πίνακας **11)**

| Ιστορικό Επίθεσης | |
|---|---|
| Ημερομηνίες | Γεγονότα |
| 1/4/1990 | Απόπειρα εισβολής σε .mil site από .edu site. Αποδείχθηκε ότι η επίθεση ξεκίνησε από 4 νεαρούς Ολλανδούς σε μια επαρχιακή πόλη της Ολλανδίας. |
| 5/1990 | Τρόπος δράσης των εισβολέων:<br><br>Επιλέγουν site, αποκτούν πλήρη πρόσβαση διαχειριστή και χτυπούν. Εντοπίζονται από το FBI και ειδοποιούνται οι τοπικές αρχές, οι οποίες ελλείψει σχετικού νόμου περί hacking δεν μπορούν να τους συλλάβουν. Ανακαλύπτεται ότι άφηναν backdoor στα συστήματα μέσω εξυπηρετητή στο port 87. |
| 5/1990 | Οι hackers επιδεικνύουν τις δυνάμεις τους εισβάλλοντας σε sites σε Γαλλία και Αμερική, χρησιμοποιώντας μάλιστα τεχνάσματα ώστε να επιτύχουν δωρεάν τηλεφωνήματα για τις κλήσεις τους (in-band signaling). Εμφανίζονται στα newsgroups χρησιμοποιώντας το κωδικό όνομα rchack. |
| 8/1990 | Εξαφανίζονται όλα τα αρχεία σε Υπολογιστικό Κέντρο Πανεπιστημίου της Ολλανδίας. |
| 30/12/1990 | Στέλνονται μηνύματα σε πολλά sites, μεταξύ των οποίων και στο CERT®/CC, ζητώντας λογαριασμό για πρόσβαση. Το CERT®/CC ξεκινά έρευνα και ανακαλύπτει το login name του hacker από κάποιο σύστημα στις ΗΠΑ, όπου βρίσκει και το πραγματικό του όνομα. |
| 1-4/1991 | Έντονη περίοδος δραστηριότητας των hackers, ενώ στην Ολλανδία συνεχίζει να είναι ανύπαρκτη η νομοθεσία για computer crimes. |
| 2/1991 | Επίθεση σε site που τους παρακολουθούσε και προς την ομάδα που προσπαθούσε να τους εντοπίσει και προς άλλες κατευθύνσεις. |
| 21/4/1991 | Αναφέρονται για πρώτη φορά σε άρθρο στους NY Times οι Ολλανδοί Hackers. |
| 5-7/1991 | Ύφεση της δράσης τους. |
| 10/1992-αρχές 1992 | Επανάληψη επιθέσεων. Προσπάθεια θωράκισης των μηχανημάτων που δούλευαν οι hackers. |
| 27/1/1992 | Στις 10.30 η Ολλανδική Αστυνομία εισβάλλει στα σπίτια δύο εκ των Ολλανδών Hackers και συγκεκριμένα στα πατρικά σπίτια του 21χρονου φοιτητή H.W. στην πόλη Roermond και του 25χρονου R.N., μηχανικού Η/Υ, στην πόλη Nuenen, τους συλλαμβάνει και τους μεταφέρει στο Άμστερνταμ. Οι επίσημες κατηγορίες είναι:<br><br>πλαστογραφία (παραποίηση πληροφοριών με σκοπό απόκτηση πρόσβασης διαχειριστή)<br><br>βανδαλισμός (τα συστήματα που δέχθηκαν επίθεση έπρεπε να |

| | |
|---|---|
| | αποσυρθούν από το δίκτυο για αρκετό καιρό προκειμένου να εκτιμηθεί το μέγεθος των ζημιών)<br><br>λοιπές απάτες, όπως χρήση κλεμμένων κωδικών και πιστωτικών καρτών. Η αστυνομία ισχυρίζεται πως οι hackers προσποιούνταν ότι ήταν κανονικοί χρήστες για να κάνουν τη «δουλειά» τους. |
| 17/2/1992 | Το CERT®/CC εκδίδει οδηγία με τίτλο "Internet Intruder Activity", δηλαδή "Η Δραστηριότητα των εισβολέων του Internet», περιγράφοντας τις λεπτομέρειες δράσης των Ολλανδών Hackers. |
| 3/1992 | Το CERT®/CC δημοσιοποιεί το αποτέλεσμα της ανάκρισης των δύο συλληφθέντων, οι οποίοι υποδεικνύουν την ύπαρξη άλλων δύο. Έτσι, κλείνει τυπικά η υπόθεση των Ολλανδών Hackers. |

**Πίνακας 11.Ιστορικό της επίθεσης**

Οι μέθοδοι που χρησιμοποίησαν οι Ολλανδοί **Hackers** μπορούν να συνοψιστούν στις εξής**: weak passwords, no passwords, password files, password tracking, Trojan login, FTP, deleted files, open servers, social engineering, user accounts, system accounts, login attempts, hosts.equiv, .rhosts, sendmail attack, debug, chsh/chfn, mail spoofing, rm –rf/, 87 socket, software privacy.** Όλα αυτά τα κατάφεραν χρησιμοποιώντας είτε απλές εντολές που έδιναν με το χέρι**,** είτε με **scripts.**

### 4.4.6 Το σκουλήκι ILOVEYOU

Στις **4** Μαΐου του **2000** εμφανίστηκε το σκουλήκι των ερωτικών γραμμάτων**,** το λεγόμενο **ILOVEYOU [46].** Το σκουλήκι αυτό ήταν ένα πρόγραμμα σε **VBScript,** το οποίο εξαπλωνόταν με διάφορους τρόπους**.** Στις **5**μ.μ**.** της **8**ης Μαΐου **2000,** το Συντονιστικό Κέντρο του **CERT** είχε λάβει αναφορές από **650** και πλέον ιστοσελίδες για περισσότερα από **500.000 «**μολυσμένα**»** συστήματα**.** Επιπλέον**,** υπήρξαν αρκετές αναφορές από ιστοσελίδες που είχαν υποστεί σοβαρές ζημιές στο δίκτυο τους λόγω αυξημένης κίνησης τόσο στο ηλεκτρονικό ταχυδρομείο**,** όσο και σε διαδικτυακά αρχεία που προερχόταν από το **ILOVEYOU.**

Το σκουλήκι εισέβαλε στο εκάστοτε σύστημα τόσο από το ηλεκτρονικό ταχυδρομείο**,** όσο και από άλλες διαδικτυακές δραστηριότητες**,** όπως **Windows File Sharing, IRC, USENET news** και πιθανόν από ιστοσελίδες**.** Όταν εκτελείτο ο κώδικας του **ILOVEYOU** προσπαθούσε να στείλει αντίγραφα του εαυτού του σε όλες τις ηλεκτρονικές διευθύνσεις που ήταν καταχωρημένες στο **Microsoft Outlook.** Το μήνυμα που στελνόταν είχε τα εξής χαρακτηριστικά**:**

---

Ένα συνημμένο αρχείο με όνομα **"LOVE-LETTER-FOR-YOU.TXT.VBS"**

Θέμα **: ILOVEYOU**

Το περιεχόμενο του μηνύματος ήταν**: «**Παρακαλώ κοιτάξτε το συνημμένο ΕΡΩΤΙΚΟ ΜΗΝΥΜΑ που σας στέλνω**».**

---

Ο **ILOVEYOU** είχε τις εξής επιπτώσεις στο σύστημα που μόλυνε:

**1)** Αντικαθιστούσε αρχεία που υπήρχαν ανάλογα με τις καταλήξεις τους:

- Αν ήταν **.vbs** ή **.vbe** τα αντικαθιστούσε με ένα αντίγραφο του εαυτού του.
- Αν ήταν **.js, .jse, .css, wsh, sct** ή **.hta** τα αντικαθιστούσε με ένα αντίγραφο του εαυτού του και άλλαζε την κατάληξή τους σε **.vbs.**
- Αν ήταν **.jpg** ή **.jpeg** τα αντικαθιστούσε με ένα αντίγραφο του εαυτού του και πρόσθετε μία κατάληξη **.vbs.**
- Αν ήταν **.mp3** ή **.mp2** εκτελούσε ακριβώς την ίδια διαδικασία που ακολουθούσε με τα **.jpg** αρχεία.

Αφού τα αρχεία αντικαθίσταντο από τον κώδικα του σκουληκιού, ήταν αρκετά δύσκολο εώς αδύνατο να ανακτηθούν τα προϋπάρχοντα αρχεία. Οι χρήστες που εκτελούσαν τα τροποποιημένα αρχεία θα προκαλούσαν την εκτέλεση του **ILOVEYOU.** Αν αυτά τα αρχεία συμπεριλαμβάνονταν σε κάποιο σύστημα αρχείων ενός τοπικού δικτύου, πιθανόν να μολύνονταν και άλλα συστήματα.

**2)** Δημιουργούσε ένα **mIRC script.** Πιο συγκεκριμένα, αν εντόπιζε κάποιο αρχείο με όνομα **mirc32.exe, mlink32.exe, mirc.ini, script.ini, script.ini** ή **mirc.hlp** το σκουλήκι δημιουργούσε ένα αρχείο με όνομα **script.ini** στον ίδιο φάκελο. Το αρχείο αυτό περιείχε τον κώδικα:

```
[script]
n0=on 1:JOIN:#:{
n1= /if ( $nick == $me ) { halt }
n2= /.dcc send $nick DIRSYSTEM\LOVE-LETTER-FOR-YOU.HTM
n3=}
```

όπου το **DIRSYSTEM** ποικίλει ανάλογα με την πλατφόρμα, στην οποία εκτελείται το σκουλήκι. Αν υπήρχε αρχείο **script.ini** , τότε δε συνέβαιναν αλλαγές. Αυτό το **script,** λοιπόν, έστελνε αντίγραφα του **ILOVEYOU** σε κάθε νέο χρήστη που εισερχόταν σε κάποιο **IRC** κανάλι, στο οποίο προηγουμένως είχε εισελθεί ο **«**μολυσμένος**»** χρήστης.

**3)** Τροποποιούσε την αρχική σελίδα του **Explorer:**

Αν το αρχείο **<DIRSYSTEM>\WinFAT32.exe** δεν υπήρχε, το σκουλήκι έθετε ως αρχική σελίδα του **Explorer** μία από τέσσερις τυχαία **URLs.** Αυτά τα **URLs** αναφέρονταν σε κάποιο αρχείο **WIN-BUGSFIX.exe,** το οποίο περιείχε επικίνδυνο κώδικα. Το σκουλήκι έλεγχε αυτό το αρχείο στο φάκελο των **downloads** του

**Internet Explorer** και αν το έβρισκε, το αρχείο προστίθετο στη λίστα των προγραμμάτων που έτρεχαν στην εκκίνηση. Κατόπιν έθετε ως αρχική σελίδα του **Explorer** την **"about:blank".**

**4)n**Επίσης τροποποιούσε κάποια κλειδιά στο ευρετήριο **(Registry)** του συστήματος και πιο συγκεκριμένα τα:

---

**HKLM\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32**

**HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\Win32DLL**

**HKLM\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX**

**HKLM\Software\Microsoft\WindowsScriptingHost\Settings\Timeout**

**HKLM\Software\Microsoft\InternetExplorer\Main\StartPage**

**HKLM\Software\Microsoft\WAB***

---

Αξιοσημείωτο είναι ακόμη το γεγονός ότι, όταν το σκουλήκι αυτό έστελνε μηνύματα, ανανέωνε κάθε φορά την τελευταία εγγραφή. Αν στελνόταν ένας μεγάλος αριθμός μηνυμάτων, τότε το μέγεθος της **registry** αυξανόταν σημαντικά προκαλώντας επιπλέον προβλήματα.

### 4.4.7 Εισβολή στη Microsoft

Το φθινόπωρο του **2000** έγινε ένα σοβαρό περιστατικό εισβολής στο δίκτυο της **Microsoft.** Χωρίς να έχουν γνωστοποιηθεί πολλά για την υπόθεση και το είδος της προσπέλασης που είχαν αποκτήσει οι εισβολείς είναι σίγουρο πως η φήμη της εταιρείας είχε δεχτεί καίριο πλήγμα.

Η επίθεση φαίνεται πως ξεκίνησε από τον υπολογιστή στο σπίτι ενός υπαλλήλου που συνδεόταν με το δίκτυο της εταιρείας. Από εκεί, λοιπόν, ένας Δούρειος Ίππος με όνομα **QAZ** μεταφέρθηκε στο εσωτερικό του δικτύου και μεταδόθηκε μέσω του ηλεκτρονικού ταχυδρομείου και αυτόματης αντιγραφής του μέσω διαμοιρασμένων φακέλων, αλλάζοντας τη γνωστή εφαρμογή **Notepad** με τον εαυτό του.

Με την ενεργοποίησή του ο **QUAZ.trojan (W32.HLLW.QUAZ.A)** ψάχνει για την εφαρμογή **Notepad.exe** και αντιγράφει τον εαυτό του στη θέση του μετονομάζοντας το αυθεντικό σε **note.exe.** Κάθε φορά κάποιος που τρέχει το μεταλλαγμένο **Notepad.exe** εκτελείται και το **note.exe,** ώστε ο χρήστης να μην διαπιστώνει κάποιο πρόβλημα. Κατόπιν ψάχνει στο δίκτυο για να μολύνει και άλλα αντίγραφα του **Notepad.exe.** Από τη στιγμή που μολύνει ένα σταθμό, στέλνει με **email** στο **hacker** την **IP** διεύθυνσή του, ενεργοποιεί το **Winsock** για την επικοινωνία του και περιμένει σύνδεση στο **port 7597.** Απλά ο **hacker** ελέγχει το ηλεκτρονικό ταχυδρομείο του μέσω **web (**που προφανώς έχει ανοιχτεί σε μία

δωρεάν υπηρεσία με λάθος στοιχεία) και κάνει **telnet** από έναν άλλο κόμβο κρύβοντας με τους γνωστούς τρόπους την πραγματική του **IP.**

Χωρίς να έχουν δοθεί στη δημοσιότητα αρκετά στοιχεία για τη δράση των εισβολέων και με αντικρουόμενες πληροφορίες για το χρονικό διάστημα που είχαν προσπέλαση στο δίκτυο (λέχθηκε για ένα μήνα ή στην καλύτερη περίπτωση για **9** μέρες), συνηθίζεται από τους **hackers,** τις πρώτες μέρες , να αντιγράφεται ή να αποστέλλεται με **email** ότι φαίνεται χρήσιμο, από το φόβο να γίνουν αντιληπτοί (χωρίς βέβαια να μπορεί κανείς να πει πως έγινε έτσι σε αυτή την περίπτωση).

Έχει ενδιαφέρον να αναλογιστούμε πως κατάφερε ο ιός και πέρασε τα συστήματα ελέγχου της εταιρείας. Εδώ μάλλον η απάντηση βρίσκεται στον τρόπο που τα προγράμματα προστασίας ελέγχουν για ιούς. Στην πλειοψηφία τους τα προγράμματα αυτά έχουν αρχεία με τις υπογραφές των ιών που έχουν βρεθεί σε κανονική και συμπιεσμένη μορφή. Έτσι, αν για παράδειγμα συμπιεστεί ένα αρχείο που περιέχει ιό με ένα πρόγραμμα συμπίεσης, όχι ευρέως γνωστό (π.χ. **NeoLite)** σε αυτοσυμπιεζόμενο αρχείο, τότε τα συστήματα προστασίας δεν το αντιλαμβανόνται αφού το αρχείο είναι εκτελέσιμο **(.exe)** και η υπογραφή του δεν υπάρχει μέσα σε αυτό.

Είναι, λοιπόν, εύκολο για οποιονδήποτε χωρίς ιδιαίτερες γνώσεις να συλλέξει πληροφορίες που χρειάζονται και να προσπαθήσει να κάνει μία επιτυχή επίθεση σε ένα **site.** Για να μπορέσει όμως να παραμείνει άγνωστη η ταυτότητά του, χρειάζεται εμπειρία και χρόνος.

Την επόμενη χρονιά η **Microsoft** ήταν πάλι στόχος των **hackers.** Αυτή τη φορά η επίθεση αφορούσε τα στοιχεία για το **DNS** της εταιρείας. Για λίγες ώρες τα στοιχεία για το **DNS** είχαν αλλάξει και εκατομμύρια χρήστες για δύο μέρες δεν μπορούσαν να προσπελάσουν τους **web servers** της.

### 4.4.8 SirCam

Φτάνει στον υπολογιστή μέσα σε μήνυμα **e-mail** και φυσικά έχει ένα **attached** αρχείο. Ο τίτλος του μηνύματος είναι διαφορετικός κάθε φορά, ίδιος με το όνομα του τυχαίου μολυσμένου αρχείου που συνοδεύει το μήνυμα. Στην πρώτη γραμμή μπορούμε να δούμε τη φράση **Hi! How are you?** ή **Hola como estas ?** ανάλογα με τη γλώσσα. Μετά θα βρούμε κάποια πρόταση από τις παρακάτω **: I send you this file in order to have your advice / I hope you can help me with this file that I send / I hope you like the file that I sendo you / This is the file with the information that you ask for,** ή **Te mando este archivo para que me des tu punto de vista / Espero me puedas ayudar con el archivo que te mando / Espero te guste este archivo que**

**te mando / Este es el archivo con la informacion que me pediste.** Στην τελευταία γραμμή θα λέει **: See you later. Thanks** ή **Nos vemos pronto, gracias.**

Αφού μολύνει τον **«**ξενιστή**»** υπολογιστή**,** ψάχνει συγκεκριμένους φακέλους του σκληρού δίσκου του για οποιαδήποτε **e-mail** διεύθυνση περιέχεται στα αρχεία **sho*., get*., hot*.** και ***.htm,** τις οποίες και καταγράφει στα δικά του αρχεία με όνομα **scy1.dll, sch1.dll, sci1.dll** και **sct1.dll.** Ακόμη και με κλειστό το πρόγραμμα αποστολής μηνυμάτων**,** εκείνο έχει δικό του **SMTP server,** δηλαδή δεν είναι απόλυτα εξαρτημένο από το **PC,** και θα καταφέρει να στείλει τον εαυτό του **8000** φορές σε όσες διευθύνσεις μαζέψει**.**

Έχει κάνει καταχωρήσεις στο **Registry** των **Windows** και έχει σκορπίσει διάφορα αρχεία του στο **Recycled,** το **Temp,** το **System** και άλλους φακέλους**.** Επίσης μέσω δικτύου **(**αν έχετε κάτι τέτοιο**)** διαδίδεται σε όσους περισσότερους σκληρούς δίσκους μπορεί**,** στους οποίους κάνει ακριβώς την ίδια ζημιά**.** Φυσικά δε μολύνει μόνο τον δίσκο **C:** αλλά οποιοδήποτε εκτελέσιμο **«**τρέξει**»** σε οποιονδήποτε σκληρό δίσκο του υπολογιστή**.**

Αφού μολύνει όσα **.exe** αρχεία εκτελείτε **(.exe = executable)** και διαλέξει στην τύχη ένα **(**το οποίο πρέπει να είναι τουλάχιστον **134 kilobyte)** και το στείλει **8000** φορές σε όσους ξέρετε και δεν ξέρετε **(**αντί για **.exe** τα στέλνει με κατάληξη **.bat, .com, .lnk** ή **.pif** για να μην τραβήξουν αμέσως την προσοχή**),** τότε **«**υποκρίνεται**»** πως σταματάει να λειτουργεί**.**

### 4.4.9 BadTrans

Ο **Badtrans** εμφανίστηκε στις **24** Νοεμβρίου του **2001,** έρχεται ως μήνυμα ηλεκτρονικού ταχυδρομείου με διάφορα ονόματα επισυναπτόμενου αρχείου και συνδυασμό δύο καταλήξεων**.** Οι επιχειρήσεις που διαθέτουν δίκτυο δεν πρέπει να ανησυχούν ιδιαίτερα διότι οι εταιρείες ανάπτυξης αντι**-**ιικών προγραμμάτων αναφέρουν ότι ο ιός αποτυγχάνει στις περισσότερες περιπτώσεις που επιχειρεί να εισβάλει σε υπολογιστές επιχειρήσεων**,** καθώς συνήθως χρησιμοποιούνται προγράμματα που φιλτράρουν ύποπτα μηνύματα με κατάληξη **.scr** ή **.pif.** Το μεγαλύτερο πρόβλημα εντοπίζεται στους **Home Users** που αν δεν έχουν ενημερώσει το **Antivirus** που χρησιμοποιούνε με τη τελευταία **version** είναι πολύ πιθανό ο ιός να μεταδοθεί στο **pc** τους**.**

Αυτό που μέχρι στιγμής είναι γνωστό ο **Badtrans** δημιουργεί μεγάλο πρόβλημα ασφάλειας διότι εκτός του ότι διαδίδει τον εαυτό του αυτόματα**,** εγκαθιστά ένα **Trojan** το οποίο μεταδίδει στον κατασκευαστή του ίου το **IP address** του **infected** Η**/**Υ καθώς και **passwords** που πληκτρολόγησε ο χρήστης ή αριθμούς πιστωτικών καρτών που χρησιμοποίησε ο υπολογιστής κατά τη διάρκεια που είναι **infected.**

Το θέμα **(Subject)** του μηνύματος είτε είναι κενό, είτε περιλαμβάνει το **"Re:"** είτε το **"Re:"** ακολουθούμενο από το πραγματικό θέμα ενός από τα μηνύματα που το **worm** θα βρει στο **Inbox.** Το κυρίως μήνυμα είναι πάντα κενό ενώ υπάρχει πάντα και ένα συνημμένο αρχείο το οποίο απαρτίζεται από τρία μέρη: το όνομα του αρχείου και δύο επιθέματα **(FILENAME + EXT1 + EXT2). Ο** ιός λοιπόν είναι ενσωματωμένος στο κυρίως σώμα του **e-mail** και εκτελείται αυτόματα εν αγνοία του χρήστη, όταν αυτός κάνει κλικ πάνω στο συγκεκριμένο μήνυμα. Όταν το **worm** ενεργοποιηθεί εγκαθιστά το αρχείο **KERNEL32.EXE** στο **directory system (**π.χ. **\windows\system)** και τροποποιεί την **Registry** τοποθετώντας το κλειδί **"KERNEL=KERNEL32.EXE"** στο πεδίο

**"HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce''.**

Ο **W32.Badtrans.B@mm,** για να μην αποστείλει τον εαυτό του σε κάποιον παραλήπτη πάνω από μία φορά, ώστε αυτός να υποψιαστεί, αποθηκεύει όλες τις διευθύνσεις, στις οποίες έχει μεταδοθεί στο αρχείο, **PROTOCOL.DLL,** στο **directory** των **Windows** και κάθε φορά κάνει ένα σχετικό έλεγχο.

Το πιο σημαντικό όμως κομμάτι είναι πως ο ιός αυτός εγκαθιστά ένα πρόγραμμα με την ονομασία **"KDLL.DLL",** μέσω του οποίου καταγράφεται κάθε πλήκτρο που θα πατηθεί. Οι πληροφορίες αυτές αποθηκεύονται στο αρχείο **CP_25389.NLS** στο **directory** των **Windows** και αποστέλλονται, σε ανύποπτο χρόνο, σε μία από τις διευθύνσεις **uckyjw@hotmail.com** ή **ld8dl1@mailandnews.com,** μαζί με τη **IP address** του **infected** Η/Υ.

### 4.4.10 SoBig

Ο ιός με την κωδική ονομασία **"Sobig"** προκάλεσε πολύ μεγάλα προβλήματα στους χρήστες υπολογιστών ανά τον κόσμο. Ο ιός χτυπά τους υπολογιστές και διαδίδεται μέσω του ηλεκτρονικού ταχυδρομείου.

Ενεργοποιείται με το άνοιγμα ενός αρχείου που έρχεται συνημμένο σε ένα **e-mail,** το οποίο αναφέρει ότι πρόκειται για ένα αρχείο προστασίας οθόνης ή ρυθμίσεων.

Η εταιρεία ασφαλείας υπολογιστών **MessageLabs** ανακοίνωσε ότι μέσα σε μία μόνο ημέρα εντόπισε ένα εκατομμύριο αντίγραφα του **Sobig** που μεταδίδεται μέσω του ηλεκτρονικού ταχυδρομείου **(e-mail)** και έχει ήδη **"**μολύνει**"** χιλιάδες υπολογιστές σε **150** περίπου χώρες.

Ο ιός αλλάζει τακτικά την περιγραφή στο θέμα του ηλεκτρονικού μηνύματος και το όνομα του συνημμένου αρχείου και όσοι μολύνονται από τον ιό, λαμβάνουν αρκετά αντίγραφά του, με μηνύματα που μοιάζουν μεταξύ τους.

# 5 Επιδημιολογικά μοντέλα

## 5.1 Ιστορική αναδρομή

Σε αυτό το κεφάλαιο θα εξετάσουμε, τεχνικές χρήσης επιδημιολογικών μοντέλων με σκοπό την μοντελοποίηση διάδοσης κακόβουλου λογισμικού. Είναι αναμενόμενο, ότι οι περισσότερες απόπειρες μοντελοποίησης του κακόβουλου λογισμικού, βασίζονται σε ανάλογες τεχνικές.

Η πρώτη ολοκληρωμένη απόπειρα μοντελοποίησης της εξάπλωσης του κακόβουλου λογισμικού πραγματοποιήθηκε από τον **Kephart [68]** στις αρχές της δεκαετίας του **90.** Ο **Kephart** ήταν ο πρώτος που χρησιμοποίησε επιδημιολογικά μοντέλα για να μελετήσει την διάδοση των ιών. Η προσέγγιση του ήταν καινοτόμα και ουσιαστικά οδήγησε στη δημιουργία του κλάδου της Επιδημιολογίας των υπολογιστών. Τα αποτελέσματα της δουλειάς του έχουν επηρεάσει το έργο σχεδόν όλων των ερευνητών που ασχολούνται με το αντικείμενο αυτό. Το σημαντικότερο πρόβλημα που αντιμετώπισε ο **Kephart** ήταν ότι την εποχή που δημοσίευσε τα ερευνητικά του αποτελέσματα, οι ιοί υπολογιστών αποτελούσαν περισσότερο αντικείμενο επιστημονικής φαντασίας, παρά υπαρκτό πρόβλημα για τους περισσότερους χρήστες και έτσι τα Μέσα Μαζικής Ενημέρωσης αδυνατώντας να κατανοήσουν το τρόπο λειτουργίας των ιών και των δικτυακών σκουληκιών, σε αρκετές περιπτώσεις προκαλούσαν πανικό με τις εκτιμήσεις τους για επικείμενες καταστροφές **(**όπως για παράδειγμα με τον ιό **Michaelangelo [71]).** Η διάψευση των προαναγγελλόμενων καταστροφών προκάλεσε την συνολική αμφισβήτηση του προβλήματος του κακόβουλου λογισμικού και αποθάρρυνε την επιστημονική κοινότητα από το να ασχοληθεί επισταμένα με το αντικείμενο. Μετά το **2000** οι μεθοδολογίες των **Code Red** και **Nimda** προκάλεσαν το ενδιαφέρον των ερευνητών για να ασχοληθούν και πάλι με την μαθηματική μοντελοποίηση της εξάπλωσης του κακόβουλου λογισμικού. Οι **Staniford, Weaver** και **Paxson** παρουσίασαν πλήθος σχετικών εργασιών **[115]** και έδωσαν το έναυσμα για να ξεκινήσει ένας νέος κύκλος έρευνας βασισμένος σε επιδημιολογικά μοντέλα, ο οποίος οδήγησε σε δεύτερη φάση στην υλοποίηση κάποιων αλγορίθμων και συστημάτων περιορισμού της διάδοσης του κακόβουλου λογισμικού. Οι παραπάνω ερευνητές, ήταν οι πρώτοι που προέβλεψαν την δραστική μείωση του χρόνου δράσης των σύγχρονων δικτυακών σκουληκιών πριν καν αυτά εμφανιστούν, ενώ μελέτησαν και ανέλυσαν την εξάπλωση διαφόρων ειδών κακόβουλου λογισμικού μέσω επιδημιολογικών μοντέλων, προσομοιώσεων και ιστογραμμάτων.

Οι **Zou** και **Gong [134]** επινόησαν ένα επιδημιολογικό μοντέλο δύο παραγόντων που περιλαμβάνει πιο σύνθετα χαρακτηριστικά από ότι το βασικό επιδημιολογικό

μοντέλο ευπαθούς – μολυσμένου πληθυσμού, το οποίο είναι ευρύτερα γνωστό ως **s-i (Susceptible-Infected).** Συγκεκριμένα, το μοντέλο περιλαμβάνει την αλλαγή της κατάστασης ενός συστήματος από ευπαθές ή μολυσμένο σε άνοσο, κατά την πορεία της εξέλιξης του φαινομένου. Η εισαγωγή της επιπλέον κατάστασης που περιγράφει την ανοσία ενός συστήματος στις εξαπολυμένες απειλές είναι ιδιαίτερα χρήσιμη, καθώς πολλοί διαχειριστές φροντίζουν να καλύψουν τα εκμεταλλευόμενα κενά ασφαλείας μόλις ενημερωθούν για αυτά και ενώ η επιδημία βρίσκεται σε εξέλιξη.

Το μοντέλο αυτό αποτελεί μια παραλλαγή του γνωστού μοντέλου **s-i-r (Susceptible-Infected-Removed)** και αναμφίβολα, το γεγονός ότι υποστηρίζει τη δυναμική αλλαγή κατάστασης κατά την διάρκεια εξέλιξης του φαινομένου είναι θετικό, καθώς περιγράφει ικανοποιητικά την διαδικασία της αναβάθμισης του λογισμικού που συμβαίνει πάντα σε καταστάσεις αυξημένης κακόβουλης δραστηριότητας. Οι **Zou** και **Gong** έχουν επίσης πραγματοποιήσει έρευνα για την μετάδοση κακόβουλου λογισμικού μέσω του ηλεκτρονικού ταχυδρομείου και έχουν διατυπώσει τα σχετικά μαθηματικά μοντέλα για να περιγράψουν την παραπάνω διαδικασία **[135].**

Μια πιο ολοκληρωμένη και πλήρης μελέτη για την εξάπλωση του κακόβουλου λογισμικού έχει γίνει από τον **Leveille [83].** Ο **Leveille** προτείνει τροποποιήσεις στο υπάρχον Γενικό Επιδημιολογικό Μοντέλο, ούτως ώστε να περιλαμβάνει δύο διακριτές περιόδους. Η πρώτη αφορά τα αρχικά στάδια μιας επιδημίας κακόβουλου λογισμικού, όπου ο ιός ή το δικτυακό σκουλήκι εξαπλώνεται ανεμπόδιστα, είτε γιατί δεν έχει γίνει ακόμα αντιληπτός, είτε γιατί δεν υπάρχουν τα κατάλληλα αντίμετρα. Στη δεύτερη περίοδο, όπου πλέον είναι γνωστή η κακόβουλη δραστηριότητα, υπεισέρχονται και τα περιοριστικά, μέτρα ανακόπτοντας την περαιτέρω εξάπλωση της. Το μοντέλο αυτό ονομάζεται **ps-i-d-r (Progressive-Susceptible-Infected-Removed)** και λειτουργεί αρκετά αποτελεσματικά, όπως τεκμηριώνεται από τα πειραματικά αποτελέσματα του **Leveille.** Αναλύοντας προσεκτικότερα τη προσέγγιση του **Leveille** προκύπτει το συμπέρασμα, ότι θα μπορούσε να θεωρηθεί σαν ένας συνδυασμός των επιδημιολογικών μοντέλων **s-i** και **s-i-r.** Συγκεκριμένα το διάστημα που ο ιός δρα λάθρα, κατά τον **Leveille** η εξάπλωση του υπολογίζεται από το **s-i** επιδημιολογικό μοντέλο και στη συνέχεια όταν πλέον έχει γίνει αντιληπτός ακολουθείται το **s-i-r** πρότυπο.

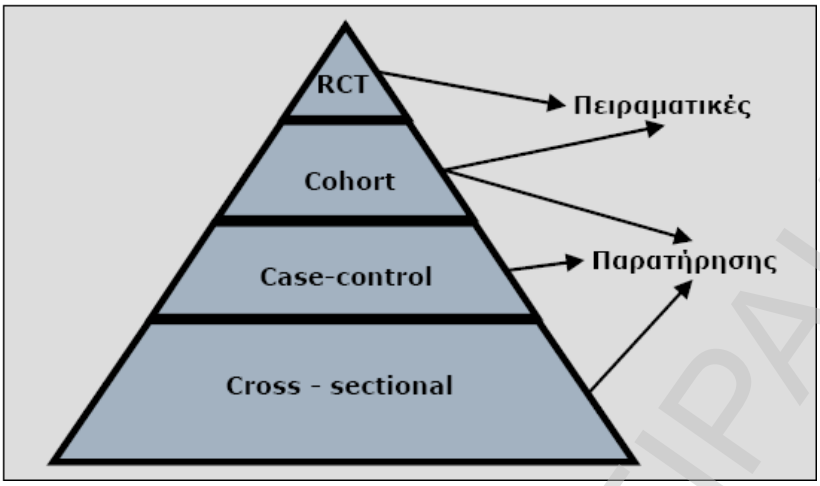
Οι **Boguna** και **Pastor-Satorras [21]** στην έρευνα τους κατάφεραν να αναδείξουν την σημασία που έχει η χρησιμοποίηση γράφων ελεύθερης κλίμακας στην μελέτη επιδημικών εξάρσεων. Ειδικότερα, εστιάστηκαν στις επιπτώσεις που έχει η δομή ενός γράφου στην ύπαρξη ή μη επιδημικού ορίου, πέρα από το οποίο είναι αναπόφευκτη η εκδήλωση κάποιας επιδημίας. Στα πειράματα τους χρησιμοποίησαν

το επιδημιολογικό μοντέλο **s-i-s (Susceptible-Infected- Susceptible).** Η δουλεία τους αποτελεί συνέχεια της προγενέστερης προσπάθεια του **Pastor-Satorras** με τον **Vespignani [99],** όπου και πάλι είχαν χρησιμοποιήσει το επιδημικό μοντέλο **s-i-s** σε γράφους ελεύθερης κλίμακας**.** Οι δυσκολίες αυτού του εγχειρήματος επιβεβαιώνονται και από τον **Volchenkov** και άλλους **[126],** οι οποίοι χρησιμοποιούν και αυτοί στην έρευνα τους το μοντέλο **s-i-s.**

Σε εντελώς θεωρητικό επίπεδο**,** σχετικά με την εμφάνιση επιδημιών σε γράφους ελεύθερης κλίμακας**,** επικεντρώνεται η δουλειά των **Barthelemy** και άλλων **[15],** η οποία στηρίζεται στα μοντέλα **s-i** και **s-i-s.**

## 5.2 Είδη επιδημιολογικών μελετών

Στο Σχήμα **35** φαίνονται τα **4** βασικά είδη των επιδημιολογικών διαβαθμισμένα σε μια ιεραρχική πυραμίδα η οποία υποδεικνύει κατά κάποιον τρόπο την ερευνητική δυναμική τους δηλαδή την αποδεικτική δύναμη των αποτελεσμάτων τους**.** Στη βάση της πυραμίδας του σχήματος υπάρχουν οι μελέτες συγχρονικού τύπου **(cross-sectional)** και η μελέτες ασθενών**-**μαρτύρων **(Case-control) [29]** που ανήκουν στις μελέτες παρατήρησης διότι σε αυτές οι ερευνητές δεν καθορίζουν τις συνθήκες της μελέτης **(**παράγοντες κινδύνου**,** χρονικές συνθήκες κλπ**.)** αλλά απλά παρατηρούν και προσμετρούν τα βιοϊατρικά φαινόμενα που επισυμβαίνουν**.** Οι μελέτες **cross sectional** επειδή ασχολούνται με προσμέτρηση επιπολασμού λέγονται και μελέτες επιπολασμού**.** Οι μελέτες κοορτών **(cohorts) [104]** ακολουθούν στην ιεραρχική πυραμίδα**.** Επειδή ασχολούνται με προσμέτρηση της επίπτωσης λέγονται επίσης μελέτες επίπτωσης**.** Οι μελέτες κοορτών μπορεί να είναι μελέτες παρατήρησης ή και πειραματικές υπό την έννοια ότι οι ερευνητές μπορούν απλά να παρατηρήσουν αλλά και να καθορίσουν επακριβώς τις συνθήκες της μελέτης άρα να κάνουν μια πειραματική μελέτη**.** Στην κορυφή της πυραμίδας βρίσκονται οι τυχαιοποιημένες κλινικές μελέτες ή δοκιμές **(Randomized Clincal Trials –RCT) [104,80]** οι οποίες πραγματοποιούνται από τους γιατρούς για να δοκιμάσουν την αποτελεσματικότητα των θεραπευτικών παρεμβάσεων**.** Οι συνθήκες στις κλινικές δοκιμές **(**ομάδες ασθενών**,** θεραπεία**,** είδος παρακολούθησης**)** καθορίζονται απολύτως από τους ερευνητές και γι' αυτό ανήκουν στις λεγόμενες πειραματικές μελέτες**.**

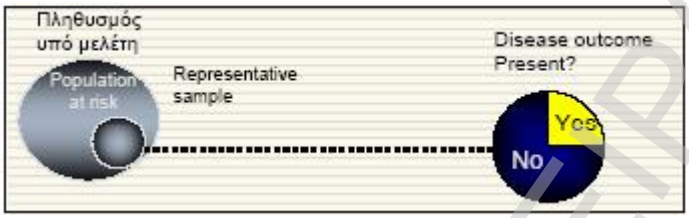



**Σχήμα 35. Τα είδη των επιδημιολογικών μελετών**

### 5.2.1 Cross-sectional studies (Επιπολασμού)

Στις μελέτες επιπολασμού **(crosssectional)** απλώς καταγράφεται κατά την διάρκεια μιας εξέτασης **(**τα άτομα εξετάζονται σε ένα χρονικό σημείο**)** το βιοϊατρικό φαινόμενο που μας ενδιαφέρει. Η εξέταση σε μια μοναδική χρονικά φορά, δεν σημαίνει ότι όλοι οι ασθενείς εξετάζονται μεμιάς αλλά καθένας μπορεί να εξεταστεί σε διαφορετικό χρόνο όμως μια φορά. Η μέτρηση των βιοϊατρικών φαινόμενων υπό αυτή την έννοια αποδίδει μια στιγμιαία εικόνα ενός πληθυσμού η οποία μπορεί να αλλάξει όμως στην πορεία του χρόνου. Έτσι οι μελέτες **cross-sectional** έχουν περιορισμένη χρησιμότητα στην απόδοση αιτιολογικών συσχετίσεων μεταξύ αιτίων και νόσου. Η γνώση όμως των μέτρων επιπολασμού είναι θεμελιώδης στην κλινική ιατρική καθώς δίδει στον κλινικό γιατρό τις γνώσεις για να ξεκινήσει μετά τη λήψη του ιατρικού ιστορικού **&** την κλινική εξέταση την λογική διεργασία που λέγεται διαφορική διαγνωστική. Η διαφορική διαγνωστική ξεκινά με ένα κατάλογο δυνητικών διαγνώσεων οι οποίες έχουν μια πιθανότητα να επαληθευθούν με τις κατάλληλες διαγνωστικές εξετάσεις. Οι πιθανότητες αυτές των υπό εξέταση διαγνώσεων, αριθμητικώς παριστάνονται από τον επιπολασμό. Έτσι οι διαγνώσεις με την υψηλότερη πιθανότητα, άρα με τον ψηλότερο επιπολασμό, να επαληθευθούν στον συγκεκριμένο άρρωστο εξετάζονται πρώτες. Ο επιπολασμός στην περίπτωση αυτή καλείται **pre-test probability (**πριν να σταλούν διαγνωστικές εξετάσεις πιθανότητα**)**. Ο επιπολασμός συμβάλλει σημαντικά στην διερεύνηση των διαγνωστικών δυνατοτήτων των διαφόρων εξετάσεων, δοκιμασιών και **tests** που προγραμματίζουμε για έναν ασθενή. Ο επιπολασμός καθορίζει την τιμή της θετικής και αρνητικής διαγνωστικής αξίας **(positive & negative predictive value)** και επομένως όχι μόνο συμβάλλει στην επιλογή και στην σειρά με την οποία θα παραγγελθούν οι διαγνωστικές εξετάσεις, υπό την έννοια της **pre-test probability,** αλλά και στο κατά πόσο μια θετική ή αρνητική απάντηση μιας διαγνωστικής

εξέτασης θα σημάνει και το τέλος της διαδικασίας διαφορικής διαγνωστικής υπό την έννοια της θετικής ή αρνητικής διαγνωστικής αξίας. Σε αντίθεση με τον επιπολασμό που λέγεται **pre-test probability,** η θετική διαγνωστική αξία λέγεται **post-test probability,** γιατί καθορίζει την πιθανότητα μια θετική διαγνωστική εξέταση να είναι όντως αληθινή **(**δηλ. ο ασθενής να πάσχει πράγματι από την συγκεκριμένη νόσο σχήμα **36).**




**Σχήμα 36. Cross-sectional study**

Παρά την δεδομένη αδυναμία των μελετών επιπολασμού να τεκμηριώσουν σχέσεις αιτίας αποτελέσματος**,** η παρατήρηση αυξημένου επιπολασμού ενός νοσήματος σε μια ομάδα του πληθυσμού μπορεί να πυροδοτήσει αιτιολογικές σκέψεις και συσχετίσεις οι οποίες να επαληθευθούν με μετέπειτα αρτιότερες μελέτες και συσχετίσεις. Μια αύξηση ή ελάττωση του επιπολασμού ενός νοσήματος οδηγεί στην εφαρμογή προληπτικών μέτρων ή στην μείωση προϋπαρχόντων.

Οι μελέτες **Cross-sectional [29]:**

**Ø** Μελετούν πληθυσμούς σε μία καθορισμένη χρονική στιγμή. Όπως μια πολιτική δημοσκόπηση.

**Ø** Δίνουν στοιχεία για τον αριθμό των ανθρώπων που έχουν μια συγκεκριμένη ασθένεια σε μια συγκεκριμένη χρονική στιγμή **(**επιπολασμός**).**

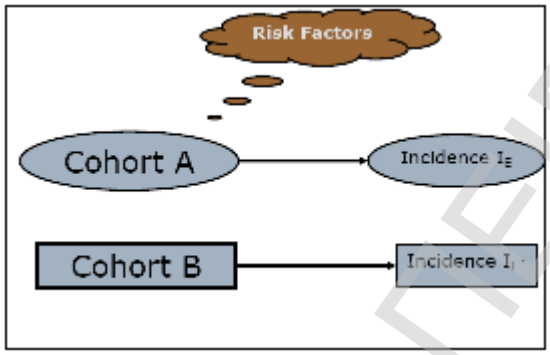
**Ø** Χρήσιμες για τον καθορισμό της επιβάρυνσης μιας πληθυσμιακής ομάδας από μία ασθένεια

**Ø** Μπορούν να διερευνήσουν συσχετίσεις με την ασθένεια αλλά δεν έχουν επαρκή σχεδιασμό για την τεκμηρίωση της αιτιολογίας της ασθένειας

### 5.2.2 Μελέτες Κοορτών – Cohorts Studies

Στην επιδημιολογία ο όρος **cohort –**κοόρτη ορίζεται ως την διαδικασία όπου κάθε ομάδα ατόμων σχεδιάζεται να παρακολουθηθεί για μια χρονική περίοδο. Έχει λάβει το όνομα της αλλά και την συνολική φιλοσοφία **cohort –** κοόρτη από την ονομασία του στρατιωτικού σχηματισμού της αρχαίας Ρωμαϊκής λεγεώνας**,** κάτι σαν τον δικό μας λόχο. Τα μέλη της κοορτής της Λεγεώνας ήταν άνδρες**,** ίδιας ηλικίας που παρέμεναν μαζί στον στρατό έως τα **65** χρόνια τους. Ήταν συνεπώς άτομα περίπου με ίδια χαρακτηριστικά που εκτίθεντο στις ίδιες δυσκολίες και κινδύνους. Στις

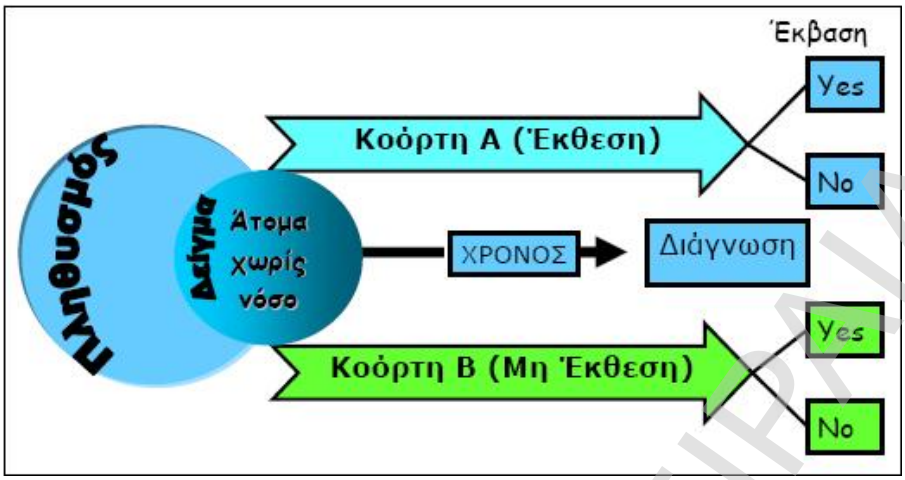
επιδημιολογικές μελέτες, τυπικά η κοόρτη αποτελείται από άτομα με όμοια χαρακτηριστικά τα οποία επιπλέον έχουν κάτι κοινό το οποίο θέλουμε να εκτιμήσουμε πόσο επιδρά στην εμφάνιση (συχνότητα) ενός νοσήματος. Μετρούμε δηλαδή την επίπτωση ενός νοσήματος ή ενός βιοϊατρικού χαρακτηριστικού γι' αυτό και λέγονται μελέτες επίπτωσης. Συνήθως οι μελέτες κοορτών σχεδιάζονται σύμφωνα με το Σχήμα **37.**




**Σχήμα 37. Cohort Study**

Επιλέγονται **2** κοόρτεις με άτομα υγιή και πανομοιότυπα σε όλα τα υπόλοιπα χαρακτηριστικά πλην του γεγονότος, του παράγοντα κινδύνου στον οποίο εκτίθεται μόνο η πρώτη κοόρτη. Έτσι μετρώντας την επίπτωση του νοσήματος που μας ενδιαφέρει στις δύο ομάδες μετά πάροδο του κατάλληλου χρονικού διαστήματος και συγκρίνοντας τις μπορούμε με ασφάλεια να συμπεράνουμε κατά πόσο ο παράγοντας κινδύνου επιδρά στην συχνότητα ενός νοσήματος (Σχήμα **38).** Η έννοια και ο σχεδιασμός των μελετών κοορτών έτσι όπως εκτέθηκε παραπάνω φαίνεται να είναι απλή και ευνόητη. Αλλά δεν είναι τόσο απλά τα πράγματα καθώς υπάρχουν προβλήματα τα οποία πρέπει να αναλυθούν. Τα πιο σημαντικά από αυτά είναι: Πως προσμετρούνται οι περιπτώσεις νόσησης; Ποιος είναι ο πληθυσμός σε κίνδυνο; Πως καθορίζεται η έκθεση στον παράγοντα κινδύνου;

Για να αντιληφθούμε αυτές τις δυσκολίες ας δούμε το ακόλουθο παράδειγμα. Ο **John Snow** προσπάθησε να αναλύσει την επιδημία χολέρας το **1854** στο Λονδίνο. Στο Λονδίνο εκείνη την εποχή υπήρχαν διάφορες εταιρείας ύδρευσης. Ο **Snow** χώρισε τον πληθυσμό σε κίνδυνο, δηλ. τους κάτοικους του Λονδίνου, σε **2** ομάδες (κοόρτεις). Σε αυτούς που υδρεύονταν από νερό του Τάμεση που ήταν μολυσμένο με λύματα με εμπλεκόμενες εταιρείες την **Sauthwark** και την **Vauxhall (cohort A).** Η δεύτερη ομάδα υδρεύονταν με νερό της εταιρείας **Lambeth** που αντλούσε νερό από καθαρό μέρος του Τάμεση χωρίς επιμόλυνση με λύματα **(cohort B).** Ο **Snow** εν συνεχεία μέτρησε τους θανάτους από χολέρα μεταξύ των δύο πληθυσμιακών ομάδων.




**Σχήμα 38. Μελέτη κοορτών**

Στον Πίνακα **12** φαίνονται τα αποτελέσματα του εξαιρετικά έξυπνου επιδημιολογικού σχεδιασμού του **Snow.** Από τον πίνακα είναι εμφανές ότι αυτοί που υδρεύονταν από τις εταιρείες **Southwark & Vauxhall** πέθαιναν **14** φορές περισσότερο από ότι αυτοί που υδρεύονταν από την **Lambeth.**

| Εταιρείες ύδρευσης | | |
|---|---|---|
| | **Southwark & Vauxhall** | **Lambert** |
| Θάνατοι από χολέρα | **4093** | **461** |
| Πληθυσμός | **266516** | **173748** |
| Θνησιμότητα | **0.0154** | **0.0027** |

**Πίνακας 12. Στατιστικά δεδομένα**

Σε μια εποχή λοιπόν που ούτε τα μικρόβια είχαν ανακαλυφθεί**,** ούτε η επιδημιολογία σαν επιστήμη είχε υπόσταση ο γιατρός **John Snow** πραγματοποίησε μια εξαιρετική μελέτη κοορτών με αποτέλεσμα τα συμπεράσματα του να δώσουν αφορμή να παρθούν μέτρα και να ανακοπεί η επιδημία χολέρας του Λονδίνου το **1854.** Δικαίως λοιπόν ο **John Snow** θεωρείται ο πατέρας της Επιδημιολογίας**.** Εν προκειμένω ο **Snow** επιθυμούσε να αναλύσει την σχέση της επιδημίας χολέρας με τις υδρευτικές ανάγκες του πληθυσμού του Λονδίνου**.** Άρα χρειαζόταν άτομα που να μην είναι άρρωστα με χολέρα**,** να μην έχουν πεθάνει αλλά να βρίσκονται υπό κίνδυνο να νοσήσουν σε εύλογο χρονικό διάστημα**.** Αυτός ο κατάλληλος για μελέτη πληθυσμός λέγεται πληθυσμός σε κίνδυνο **(population at risk).** Το να είναι τα άτομα υγιή από την υπό μελέτη νόσο και εν ζωή μοιάζουν να είναι οι δύο πιο βασικές προϋποθέσεις αυτού που ορίσαμε **population at risk.** Διάφορα λοιπόν κριτήρια πρέπει να

θεσπίζονται ώστε να επιλέγονται ποια άτομα μπορούν να είναι υποψήφια να συμπεριληφθούν στις μελέτες κοορτών και είναι τα άτομα που ονομάζονται πληθυσμός σε κίνδυνο **(population at risk).** Τέτοια κριτήρια μπορεί να είναι δημογραφικά**,** σωματομετρικά**,** γεωγραφικά κλπ**.** Αν και ο πληθυσμός υπό παρακολούθηση στις μελέτες κοορτών **(Cohorts)** ορίζεται σαν πληθυσμός ελεύθερος νόσου **(disease free)** αυτό δεν σημαίνει ότι τα άτομα είναι απολύτως υγιή**!** Ο όρος ελεύθερος νόσου απλώς είναι δηλωτικός του ότι τα άτομα δεν πάσχουν από την νόσο ή την έκβαση της νόσου που μας ενδιαφέρει να εκτιμήσουμε**.** Αυτό άλλωστε είναι ιδιαίτερα εμφαντικό στις μελέτες κοορτών προγνωστικών παραγόντων **(**μελέτες επιβίωσης**)** όπου άτομα με συγκεκριμένη νόσο παρακολουθούνται για να εκτιμηθεί η επίδραση διαφόρων προγνωστικών παραγόντων**.**

#### 5.2.2.1 Συνώνυμα & προσδιορισμοί των μελετών κοορτών.

Τέσσερις διαφορετικοί προσδιορισμοί χρησιμοποιούνται στις μελέτες κοορτών**,** όπως μελέτες **[104]:**

- Κοορτών **(Cohort)**
- Επίπτωσης **(Incidence)**
- Προοπτικές **(Prospective)**
- Μακροχρόνιες **(Longitudinal)**

Οι **4** αυτοί επιθετικοί προσδιορισμοί**,** αυτού του τύπου των μελετών δίνουν έμφαση σε διαφορετικές πλευρές του σχεδιασμού τους**.** Ο όρος κοόρτη αναφέρεται περισσότερο στις ιδιότητες της ομάδος των ατόμων που θα μελετηθούν και τα χαρακτηριστικά τους τα οποία έχουν αναλυθεί παραπάνω**.** Μελέτες επίπτωσης επίσης μπορεί να λέγονται διότι προσδιορίζουν και εκτιμούν την επίπτωση**.** Ο όρος προοπτικές αναφέρεται στο γεγονός ότι οι υπό μελέτη ομάδες παρακολουθούνται στην πορεία ενός μελλοντικού χρονικού διαστήματος**.** Ενώ ο όρος μακροχρόνιες **(longitudinal)** προσδιορίζει την μελλοντική σχετικώς μακροχρόνια παρακολούθηση που υφίστανται τα άτομα των μελετών κοορτών**.**

### 5.2.3 Μελέτες ασθενών-μαρτύρων (case-control studies)

Οι μελέτες κοορτών ως εκ της σχεδίασης τους παρουσιάζουν βασικά πλεονεκτήματα όπως **[29]:**

- Είναι ο μόνος τρόπος να μετρηθεί απευθείας η επίπτωση
- Το μοντέλο της ακολουθεί την κλινική λογική **(**έκθεση στον κίνδυνο**-**εκδήλωση νόσου**)**

Ø Δεν υφίσταται το λάθος προκατάληψης **(bias)** να είναι γνωστή η έκβαση

Ø Είναι δυνατή η διερεύνηση της σχέσης του παράγοντα κινδύνου με περισσότερα από ένα νοσήματα

Έχουν όμως και βασικά μειονεκτήματα τα οποία πολλές φορές κάνουν ανέφικτη την εφαρμογή τους. Αυτά είναι:

Ø Αναποτελεσματική σε σπάνια νοσήματα **(**πρέπει να παρακολουθηθούν χιλιάδες άτομα**)**

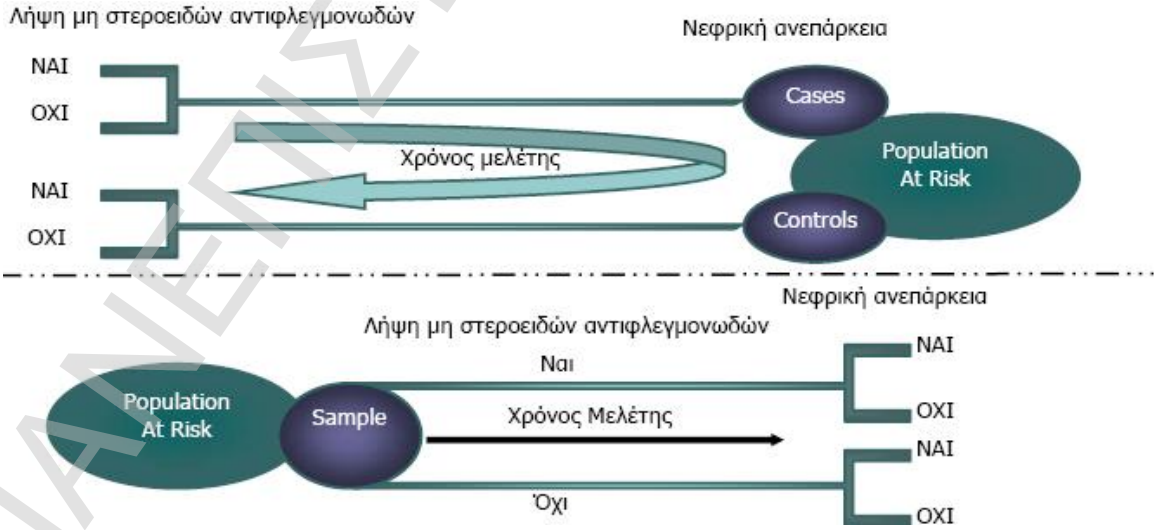
Ø Οικονομικά πολύ δαπανηρή

Ø Τα αποτελέσματα της δεν είναι γνωστά για πολύ μεγάλο χρονικό διάστημα

Ø Δύσκολη η καταγραφή πολλών παραγόντων μαζί

Ø Πολλές φορές λόγοι ηθικής δεν επιτρέπουν την διεξαγωγή τους **(**πχ. δεν είναι ηθικό να εκθέσεις ανθρώπους σε κάποιο βλαπτικό παράγοντα προκειμένου να επιβεβαιωθεί μια επίδραση**).**

Οι μελέτες ασθενών-μαρτύρων αποσκοπούν να εξυπηρετήσουν τους ίδιους σκοπούς με τις μελέτες κοορτών αλλά πιο γρήγορα και αποτελεσματικά και με πολύ χαμηλότερο κόστος. Στο ακόλουθο σχήμα συνοψίζεται ο σχεδιασμός των μελετών ασθενών-μαρτύρων σε αντιπαραβολή με τον σχεδιασμό μελέτης κοορτών. Και στις δύο μελέτες επιχειρείται να διερευνηθεί τυχόν αιτιολογική σχέση μεταξύ παράγοντα κινδύνου **(**π.χ τη λήψη μη στεροειδών αντιφλεγονοδών φαρμάκων **–** ΜΣΑ**)** και νεφρικής ανεπάρκειας **(**Σχήμα **39).**




**Σχήμα 39. Μελέτη κοορτών επάνω και μελέτη ασθενών-μαρτύρων κάτω για την διερεύνηση της**

Στο σχήμα **39** βλέπουμε ότι από ένα πληθυσμό σε κίνδυνο αντλούνται **2** κοόρτεις η μια εκτίθεται στον παράγοντα κινδύνου **(**λήψη ΜΣΑ**)** και η άλλη όχι**.** Μετά πάροδο

αρκετών ετών επιχειρείται να μετρηθεί η επίπτωση της νεφρικής ανεπάρκειας στις δύο ομάδες. Όμως η νεφρική ανεπάρκεια οφειλόμενη στην λήψη ΜΣΑ είναι σπάνια νόσος, έτσι θα πρέπει να παρακολουθηθούν χιλιάδες άτομα σε κάθε κοόρτη για να γίνει εφικτό να εκδηλωθούν μερικά περιστατικά νεφρικής ανεπάρκειας. Αντί αυτού όμως μπορεί να εφαρμοστεί σχεδιασμός μελέτης ασθενών-μαρτύρων. Επομένως ασθενείς με νεφρική ανεπάρκεια (ομάδα ασθενών) συγκρίνετε με μια ομάδα υγιών (μάρτυρες) καθ' όλα τα υπόλοιπα παρόμοια. Στην κάθε ομάδα μετράτε η συχνότητα λήψης ΜΣΑ (έκθεσης στον παράγοντα κινδύνου) και συγκρίνετε. Όπως βλέπουμε από το σχήμα η μελέτη κοορτών εξελίσσεται προοπτικά **(prospective)** ενώ η μελέτη ασθενών-μαρτύρων αντλεί πληροφορίες από το παρελθόν δηλ. αναδρομικά **(retrospective)**. Οι μελέτες ασθενών – μαρτύρων σε αντίθεση με τις μελέτες κοορτών (προδρομικές) καλούνται και αναδρομικές μελέτες.

Οι μελέτες ασθενών-μαρτύρων έχουν βασικά πλεονεκτήματα όπως:

Ø Χρήσιμες για να μελετηθούν αιτιολογικοί και προγνωστικοί ή κλινικοί παράγοντες νοσημάτων

Ø Η ανεύρεση των νοσούντων **(cases)** είναι σχετικά εύκολη ειδικά σε σπάνια νοσήματα κάτι που είναι αδύνατο να γίνει σε **cohort design**

Ø Δεν χρειάζεται να περιμένουμε πολύ χρόνο για να απαντήσουμε σε τυχόν ερευνητικά κλινικά ερωτήματα όπως συμβαίνει π.χ σε μελέτη κοορτών.

Ø Πολύ συχνή η χρήση τους λόγω της ευκολίας, της ταχύτητας και της μικρής οικονομικής δαπάνης με την οποία μπορεί να μελετηθούν διάφορα κλινικά ερωτήματα.

Ø Απαιτούν όμως και βασικές προϋποθέσεις για να γίνει εφικτή η διενέργεια τους όπως:

Ø Ύπαρξη ικανού αριθμού ασθενών έτσι ώστε τα όποια συμπεράσματα να μην οφείλονται σε τυχαία πιθανότητα

Ø Υπάρχει ομάδα ελέγχου (μάρτυρες) που δεν έχει τη νόσο

Ø Οι δύο ομάδες πρέπει να μοιάζουν σε όλα πλην της νόσου και του παράγοντα κινδύνου ή πρόγνωσης που μελετάται

### 5.2.4 Περιγραφή περίπτωσης (case-report) – Περιγραφή σειράς περιστατικών (caseseries)

Η περιγραφή ενός κλινικού περιστατικού η λεπτομερής παρουσίαση μιας περίπτωσης νοσήματος η μικρής ομάδας ομοειδών περιπτώσεων **(3-5).** Παρουσιάζονται λόγω κάποιου κλινικού χαρακτηριστικού (διαφοροδιαγνωστικού,

σπανιότητας, θεραπευτικής ανταπόκρισης) που κατά τους συγγραφείς πρέπει να τύχει προσοχής. Περίπου το **20-30%** των άρθρων παγκοσμίως αφορά **case reports [124].** Η περιγραφή ενδιαφέρουσας περίπτωσης είναι χρήσιμη γιατί είναι:

- Πηγή ερευνητικών υποθέσεων για κάποιο σχετικά σπάνιο ή ιδιάζον περιστατικό σχετικώς με τα παρακάτω
- Ενδιαφέρουσα και σχετικώς σπάνε κλινική παρουσίαση νοσήματος
- Σχέση με πρωτοεμφανιζόμενους παράγοντες κινδύνου
- Ιδιόμορφη εξέλιξη και πρόγνωση (προγνωστικοί παράγοντες)
- Ενδιαφέρουσα ανταπόκριση ή αποτυχία θεραπευτικών μεθόδων

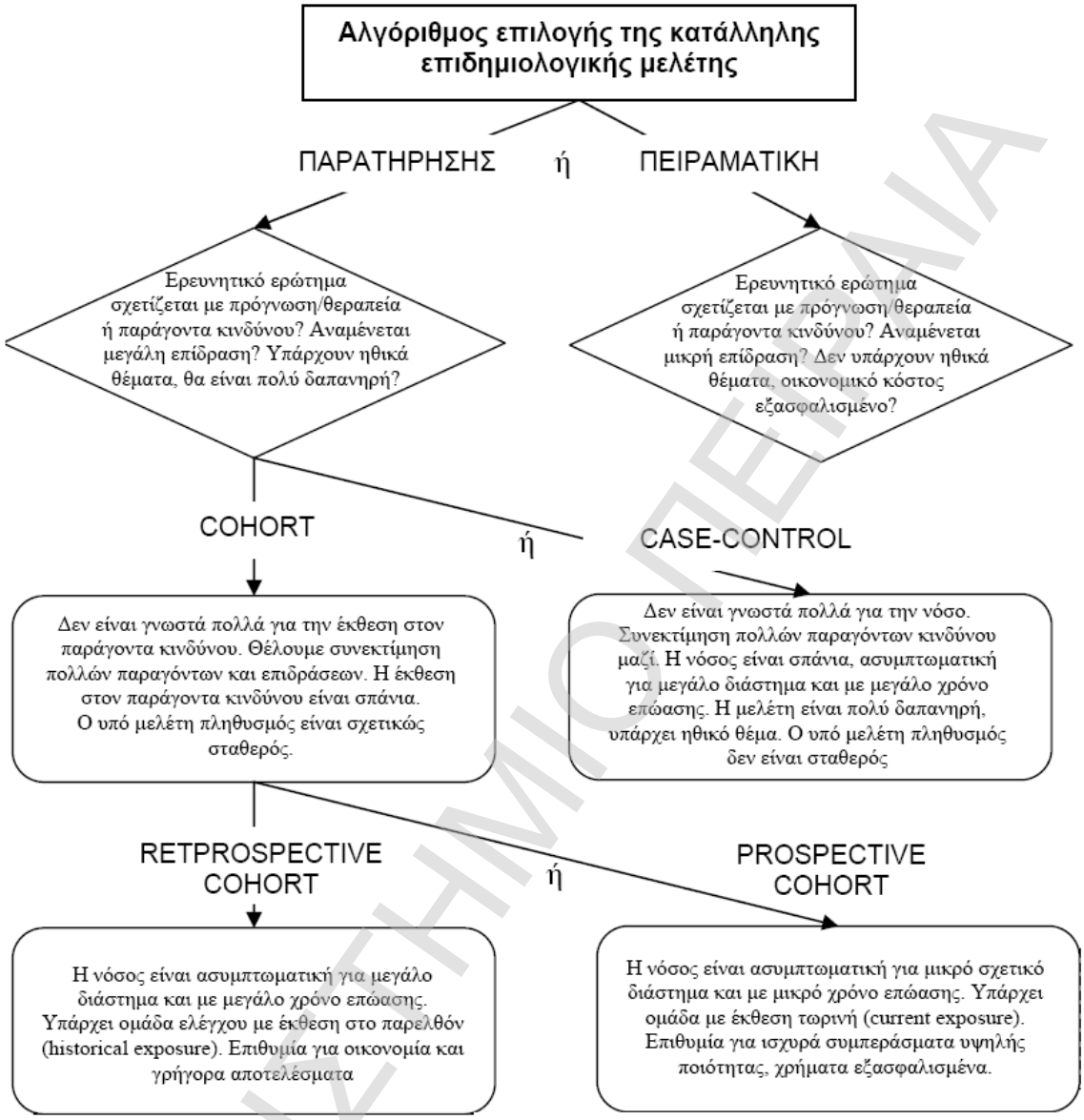
Τα **case reports** όμως:

- Δεν χρησιμεύουν στην επαλήθευση διαφόρων αιτιολογικών υποθέσεων
- Δίνουν την αφορμή για πιο εκτενείς μελέτες ελέγχου των υποθέσεων που τίθενται όπως παθοφυσιολογικοί μηχανισμοί πρόκλησης βλάβης

Η παρουσίαση σειράς περιστατικών **(case-series study)** προσδιορίζεται από το γεγονός ότι είναι μελέτη περιγραφής ομάδος ασθενών **(10** ή περισσοτέρων**)** προσβληθέντων από συγκεκριμένη νόσο. Ο σχετικά μεγαλύτερος αριθμός περιστατικών επιτρέπει στατιστική επεξεργασία και παρουσίαση. Σημαντικό μειονέκτημα η έλλειψη ομάδας ελέγχου για σύγκριση η οποία μπορεί να οδηγήσει σε λάθος συμπεράσματα.

Οι επιδημιολογικές μελέτες έχουν διαφορετικούς στόχους ανάλογα με τους διάφορους παράγοντες που εμπλέκονται. Οι μελέτες κλειδιά είναι οι:

Συγχρονικές **(prevalence)**, Μελέτες ασθενών-μαρτύρων, Προοπτικές **(Cohorts),** Τυχαιοποιημένες μελέτες κλινικής παρέμβασης (Πειραματικές). Κάποιοι σχεδιασμοί μελετών είναι 'καλύτεροι' από κάποιους άλλους για τις ανάγκες του ερευνητικού αντικειμένου και τις συνθήκες που εξασφαλίζονται (οικονομικές κλπ.). Στο σχήμα **40** συνοψίζεται ένας βοηθητικός αλγόριθμος ενδεικτικός των κριτηρίων που υπεισέρχονται στην επιλογή τους είδους της μελέτης που θα εξασφαλίσει τα καλλίτερα αποτελέσματα υπό τις συγκεκριμένες ερευνητικές συνθήκες.




**Σχήμα 40. Αλγόριθμος επιλογής της κατάλληλης επιδημιολογικής μελέτης**

## 5.3 Επιδημιολογικά μοντέλα.

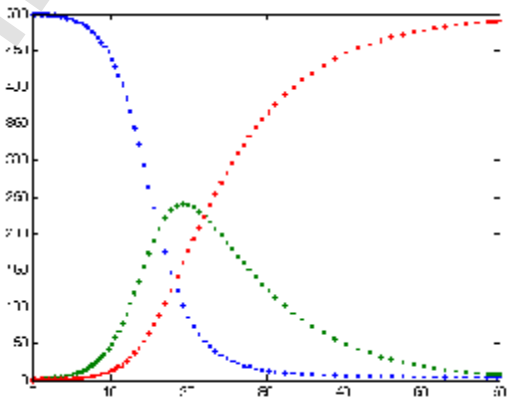
Προκειμένου να μοντελοποιηθεί η πρόοδος μιας επιδημίας σε ένα μεγάλο πληθυσμό που περιλαμβάνει πολλά διαφορετικά άτομα σε διάφορους τομείς, πρέπει (μια τέτοια ποικιλομορφία πληθυσμών) να μειωθεί σε μερικά βασικά χαρακτηριστικά που είναι σχετικά με την υπό εξέταση μόλυνση. Παραδείγματος χάριν, στις περισσότερες κοινές ασθένειες παιδικής ηλικίας που παρέχουν μακράς διαρκείας ανοσία έχει νόημα για να διαιρεθεί ο πληθυσμός σε εκείνους που είναι επιρρεπείς στην ασθένεια, σε εκείνους που είναι μολυσμένοι και εκείνους που έχουν ανακτήσει και είναι άνοσοι. Αυτές οι υποδιαιρέσεις του πληθυσμού καλούνται διαμερίσματα **(compartments).**

### 5.3.1 Το SIR μοντέλο

Με βάση το μοντέλο αυτό ορίζονται τρία διαμερίσματα, **S** (για επιρρεπείς), I (για μολυσμένους) και **R** (για αυτούς που έχουν αναρρώσει) **[78]**. Τα αρχικά αυτά αντιπροσωπεύουν επίσης τον αριθμό των ανθρώπων σε κάθε διαμέρισμα σε μία συγκεκριμένη χρονική στιγμή. Για να δειχθεί ότι το πλήθος μπορεί να ποικίλει κατά την διάρκεια του χρόνου (ακόμα κι αν ο συνολικός πληθυσμός παραμένει σταθερός), μετατρέπουμε τους ακριβείς αριθμούς σε συναρτήσεις του **t** (χρόνου): **S(t)**, **I(t)** και **R(t)**. Για μια συγκεκριμένη ασθένεια σε έναν συγκεκριμένο πληθυσμό, αυτές οι συναρτήσεις μπορούν να επιλυθούν προκειμένου να προβλεφθούν τα πιθανά ξεσπάσματα και να τεθούν υπό έλεγχο.

#### 5.3.1.1 Ο SIR πρότυπο είναι δυναμικό υπό τρεις έννοιες

Όπως υποδεικνύεται από τη μεταβλητή συνάρτηση του **t**, το μοντέλο είναι δυναμικό δεδομένου ότι οι αριθμοί σε κάθε διαμέρισμα μπορούν να κυμαίνονται κατά τη διάρκεια του χρόνου (Σχήμα **41**). Η σημασία αυτής της δυναμικής πτυχής είναι προφανέστερη σε μια ενδημική ασθένεια με μια μικρή μολυσματική χρονική περίοδο (όπως ήταν η ιλαρά στο Ηνωμένο Βασίλειο πριν από την εισαγωγή ενός εμβολίου το **1968**). Τέτοιες ασθένειες τείνουν να εμφανίζουν κυκλικά ξεσπάσματα λόγω της μεταβολής του αριθμού των ευπαθών ατόμων **(S(t))** κατά τη διάρκεια του χρόνου. Κατά τη διάρκεια μιας επιδημίας, ο αριθμός των ευπαθών ατόμων μειώνεται γρήγορα δεδομένου ότι περισσότεροι τους μολύνονται και εισάγονται έτσι στα μολυσματικά και κατόπιν στα αναρρωμένα διαμερίσματα. Μια σημαντική παρατήρηση αποτελεί το γεγονός ότι η ασθένεια δεν μπορεί να ξεσπάσει πάλι μέχρι ο αριθμός των ευπαθών ατόμων να επανέλθει (ως αποτέλεσμα των μωρών που γεννιούνται στο διαμέρισμα των ευπαθών).



**Σχήμα 41. Η επιδημία σταματά όταν ο αριθμός των ευπαθών ατόμων μειώνεται. Με μπλε συμβολίζουμε τους ευπαθείς με πράσινο τους μολυσμένους και με κόκκινο αυτούς που έχουν αναρρώσει**

Το **SIR** είναι επίσης δυναμικό υπό την έννοια ότι τα άτομα γεννιούνται ευπαθή**,** κατόπιν μπορούν να μολυνθούν **(**μετακίνηση στο μολυσματικό διαμέρισμα**)** και τελικά να αναρρώσουν **(**μετακίνηση στο διαμέρισμα αναρρωμένων**).** Κατά συνέπεια κάθε μέλος του πληθυσμού τυπικά κινείται από ευπαθείς σε μολυσμένος και μετά αναρρωμένος**.** Αυτό μπορεί να παρουσιαστεί ως διάγραμμα ροής στο οποίο τα πλαίσια αντιπροσωπεύουν τα διαφορετικά διαμερίσματα και τα βέλη την μετάβαση μεταξύ των διαμερισμάτων **[95].**


**Σχήμα 42. Διάγραμμα ροής SIR**

### 5.3.1.2 Ρυθμοί μετάβασης

Για την πλήρη προδιαγραφή του προτύπου**,** τα βέλη πρέπει να ονομαστούν με τους ρυθμούς μετάβασης μεταξύ των διαμερισμάτων**.** Μεταξύ του **S** και του I**,** το ποσοστό μετάβασης είναι β**,** όπου β είναι ο ρυθμός επαφών**,** ο οποίος χοντρικά συνυπολογίζει την πιθανότητα να μεταφερθεί η ασθένεια με μια επαφή μεταξύ ενός ευπαθή και ενός μολυσματικού ατόμου**.** Μεταξύ του **I** και του **R,** ο ρυθμός μετάβασης είναι ν **(**ο ρυθμός ανάρρωσης**).** Εάν η διάρκεια της μόλυνσης είναι **D,** τότε ν**= 1/D,** δεδομένου ότι ένα άτομο αναρρώνει μία και μοναδική φορά σε **D** χρονικές στιγμές**.** Είναι σημαντικό να τονιστεί εδώ ότι υποθέτουμε ότι η μονιμότητα κάθε ατόμου στις επιδημικές καταστάσεις είναι μια τυχαία μεταβλητή με εκθετική κατανομή**.** Ποιο σύνθετες και ρεαλιστικές κατανομές **(**όπως κατανομές **Erlang)** μπορούν να χρησιμοποιηθούν εξίσου με μερικές τροποποιήσεις**.**

### 5.3.1.3 Βιο-μαθηματική, αιτιοκρατική συμπεριφορά του SIR πρότυπου

**1)** Το **SIR** πρότυπο χωρίς ζωτική δυναμική **(**διαδικασίες γέννησης-θανάτου**)**

Ένα επιδημικό ξέσπασμα είναι συνήθως πολύ γρηγορότερο από τη ζωτική δυναμική ενός πληθυσμού**,** επομένως**,** εάν ο στόχος είναι να μελετηθούν οι άμεσες συνέπειες μιας επιδημίας**,** μπορεί κανείς να παραμελήσει τις διαδικασίες γέννησης-θανάτου**.** Σε αυτήν την περίπτωση το **SIR [78]** σύστημα που περιγράφεται ανωτέρω μπορεί να εκφραστεί από το ακόλουθο σύνολο διαφορικών εξισώσεων **[12,27, 74]**

$$\frac{dS}{dt} = -\beta IS \qquad \textbf{(1)}$$

$$\frac{dI}{dt} = \beta IS - vI \qquad \textbf{(2)}$$

$$\frac{dR}{dt} = \nu I \qquad (3)$$

Αυτό το πρότυπο προτάθηκε για πρώτη φορά από τους Ο. **Kermack** και **Anderson Gray McKendrick [74],** οι οποίοι συνεργάστηκαν με τον βραβευμένο με Νόμπελ και πατέρα της μαθηματικής επιδημιολογίας**, Ronald Ross.**

Αυτό το σύστημα είναι μη γραμμικό**,** και έτσι δεν παρέχει μια γενική αναλυτική λύση**.** Παρόλα αυτά**,** σημαντικά αποτελέσματα μπορούν να παραχθούν αναλυτικά**.**

Βασιζόμενη στην υπόθεση ότι δεν έχουμε θανάτους και άρα ο συνολικός πληθυσμός μας παραμένει σταθερός προκύπτει ότι**:**

$$S(t) + I(t) + R(t) = \text{Constant} = N <=> \frac{dS}{dt} + \frac{dI}{dt} + \frac{dR}{dt} = 0$$

εκφράζοντας με μαθηματικούς όρους τη σταθερότητα του πληθυσμού Ν**.** Σημειωτέων ότι η δυναμική των μολυσματικών κατηγοριών εξαρτάται από την ακόλουθη αναλογία**:**

$$R_0 = \frac{\beta}{\nu}$$

τον αποκαλούμενο βασικό αριθμό αναπαραγωγής**.** Κατόπιν με τη διαίρεση της πρώτης διαφορικής εξίσωσης με την τρίτη**,** το διαχωρισμό των μεταβλητών και την ενσωμάτωση παίρνουμε

$$S(t) = S(0)e^{-R_0(R(t)-R(0))}$$

**(**όπου το **S(0)** και το **R(0)** είναι οι αρχικοί αριθμοί**,** αντίστοιχα**,** των ευπαθών και αναρρωμένων ατόμων**).** Κατά συνέπεια**,** στο όριο**,** το ποσοστό των αναρρωμένων ατόμων υπακούει την υπερβατική **(transcendental)** εξίσωση

$$R_\infty = 1 - S(0)e^{-R_0(R\infty - R(0))}$$

Η εκτίμηση αυτής της εξίσωσης δείχνει ότι γενικά**,** στο τέλος μιας επιδημίας**,** δεν έχουν αναρρώσει όλα τα άτομα**,** έτσι μερικά πρέπει να παραμείνουν ευάλωτα**.** Αυτό σημαίνει ότι το τέλος μιας επιδημίας προκαλείται από την πτώση του αριθμού των μολυσμένων ατόμων και όχι από την παντελή έλλειψη ευπαθών ατόμων**.** Ο ρόλος του βασικού αριθμού αναπαραγωγής είναι εξαιρετικά σημαντικός**.** Στην συνέχεια**,** γράφουμε την εξίσωση για τα μολυσμένα άτομα ως εξής**:**

$$\frac{dI}{dt} = (\beta S - \nu) I$$

είναι σαφές ότι εάν

$\mathbf{R_0 > \frac{1}{S(0)}}$

τότε

$$\frac{dI}{dt}(0) > 0$$

θα υπάρξει ένα κατάλληλο επιδημικό ξέσπασμα με μια αύξηση του πλήθους των μολυσμένων **(**που μπορεί να φθάσει ένα αξιόλογο μέρος του πληθυσμού**).** Κατά συνέπεια**,** είναι σαφές ότι η αναλογία β*/*ν είναι εξαιρετικά σημαντική**.**

Σημειώστε ότι στο ανωτέρω πρότυπο η συνάρτηση**:**

**F=**βI**,**

μοντελοποιεί το ρυθμό μετάβασης από το διαμέρισμα των ευπαθών ατόμων στο διαμέρισμα των μολυσματικών ατόμων και γι' αυτό το λόγω καλείται δύναμη της μόλυνσης**.** Ωστόσο**,** για τις μεγάλες κατηγορίες μεταδοτικών ασθενειών είναι ρεαλιστικότερο να εξεταστεί μια δύναμη μόλυνσης που δεν εξαρτάται από τον απόλυτο αριθμό των μολυσμένων ατόμων, αλλά από ένα μέρος τους **(**όσον αφορά το συνολικό σταθερό πληθυσμό Ν**):**

Ο **Capasso** και**,** κατόπιν**,** άλλοι συγγραφείς έχουν προτείνει μη γραμμικές δυνάμεις μόλυνσης για να μοντελοποιήσουν πιο ρεαλιστικά τη διαδικασία μετάδοσης της ασθένειας**.**

**2)** Το **SIR** πρότυπο με ζωτική δυναμική και σταθερό πληθυσμό

Εξετάζοντας έναν πληθυσμό που χαρακτηρίζεται από ένα ρυθμό θανάτων μ και ρυθμό γεννήσεων ίσο με το ρυθμό θανάτου**,** όπου μια μεταδοτική ασθένεια εξαπλώνεται το μοντέλο **[27]** είναι**:**

$$\frac{dS}{dt} = m\mathrm{N} - mS - b\frac{I}{\mathrm{N}}S$$

$$\frac{dI}{dt} = b\frac{I}{\mathrm{N}}S - (m+v)I$$

$$\frac{dR}{dt} = vI - mR$$

Στο οποίο ισχύει ότι **S+I+R=N**

Επίσης σε περίπτωση που εισάγουμε ένα ρυθμό αναπαραγωγής αυτός ισούται με

$$R_0 = \frac{b}{m+v}$$

και έχει ιδιότητες κατωφλίου. Στην πραγματικότητα, ανεξάρτητα από τις βιολογικά σημαντικές αρχικές τιμές:

$$(S(0), I(0), R(0) \in \{(S, I, R) \in [0, N]^3 : S \geq 0, I \geq 0, R \geq 0, S + I + R = N\}$$

Μπορούμε να δείξουμε ότι

$$R_0 \leq 1 \Rightarrow \lim_{t \to \infty}(S(t), I(t), R(t)) = DFE = (N, 0, 0)$$

$$R_0 > 1, I(0) > 0 \Rightarrow \lim_{t \to \infty}(S(t), I(t), R(t)) = EE = (\frac{N}{R_0}, \frac{m}{b}(R_0 - 1), \frac{n}{b}(R_0 - 1))$$

Το σημείο **DFE (disease free equilibrium)** καλείται ισορροπία ελεύθερης ασθένειας, ενώ το σημείο **EE (Endemic Equilibrium)** καλείται ενδημική ισορροπία. Επιπρόσθετα το $\mathbf{R_0}$ εκφράζει τον μέσο αριθμό μολύνσεων που προκαλούνται από ένα μολυσμένο άτομο σε ένα πλήρως ευπαθή πληθυσμό. Η ανωτέρω σχέση βιολογικά σημαίνει ότι εάν αυτός ο αριθμός είναι μικρότερος ή ίσος της μονάδας η ασθένεια εξαλείφεται, ενώ εάν αυτός ο αριθμός είναι μεγαλύτερος της μονάδας η ασθένεια θα παραμείνει μόνιμα ενδημική στον πληθυσμό.

#### 5.3.1.4 Μεταβλητοί ρυθμοί επαφών και πολυετείς ή χαοτικές επιδημίες

Είναι ευρέως γνωστό ότι η πιθανότητα να ασθενήσει κανείς δεν είναι σταθερή στην πάροδο του χρόνου. Ακόμα και από την προσωπική μας εμπειρία γνωρίζουμε ότι μερικές ασθένειες είναι συχνότερα παρούσες το χειμώνα, ενώ άλλες το καλοκαίρι. Επιπλέον, όσον αφορά τις ασθένειες της παιδικής ηλικίας, υπάρχει μια ισχυρή επιρροή του σχολικού ημερολογίου σε αυτές, τέτοια ώστε κατά τη διάρκεια των σχολικών διακοπών η πιθανότητα να προσβληθεί κανείς από μια τέτοια ασθένεια να μειώνεται εντυπωσιακά.

Κατά συνέπεια, για πολλές κατηγορίες ασθενειών θα πρέπει να ληφθεί υπόψη μια δύναμη μόλυνσης με περιοδικό **("**εποχιακό**")** κυμαινόμενο ρυθμό επαφών

$$F = b(t)\frac{I}{N}, b(t+T) = b(t)$$

με περίοδο ίση με ένα χρόνο.

Έτσι το μοντέλο μετασχηματίζεται ως εξής

$$\frac{dI}{dt} = b(t)\frac{I}{\mathrm{N}}S - (m+v)I$$

**(**η δυναμική της εύκολης ανάρρωσης προκύπτει από την ισότητα **R=N-S-I)**, οδηγώντας σε ένα μη γραμμικό σύνολο διαφορικών εξισώσεων με περιοδικά μεταβαλλόμενες παραμέτρους. Είναι γνωστό ότι αυτή η κατηγορία δυναμικών

συστημάτων μπορεί να υποβληθεί στα πολύ ενδιαφέροντα και σύνθετα φαινόμενα της μη γραμμικής παραμετρικής ενίσχυσης. Είναι εύκολο να φανεί ότι εάν:

$$\frac{1}{T}\int_0^T \frac{b(t)}{m+v}dt < 1 \Rightarrow \lim_{t\to\infty}(S(t), I(t)) = DFE = (N, 0)$$

το ολοκλήρωμα είναι μεγαλύτερο από το ένα η ασθένεια δεν θα εξαλειφτεί και μπορούν να υπάρξουν τέτοιες ενισχύσεις. Παραδείγματος χάριν, θέτοντας τον περιοδικά μεταβαλλόμενο ρυθμό επαφών ως "είσοδο" του συστήματος παίρνουμε ως αποτέλεσμα μια περιοδική συνάρτηση της οποίας η περίοδος είναι ένα πολλαπλάσιο της περιόδου της εισόδου. Αυτό αποτέλεσε μια συμβολή για να εξηγήσει τα πολύχρονα (τυπικά διετή) επιδημικά ξεσπάσματα μερικών μολυσματικών ασθενειών ως αλληλεπίδραση μεταξύ της περιόδου της μεταβολής του ρυθμού επαφών και της ψευδό περιόδου των μετριασμένων ταλαντώσεων κοντά στην ενδημική ισορροπία. Είναι αξιοσημείωτο ότι, σε μερικές περιπτώσεις η συμπεριφορά μπορεί επίσης να είναι ημι-περιοδική ή ακόμα και χαοτική.

**5.3.1.5 Μοντελοποίηση προγραμμάτων μαζικού εμβολιασμού.**

**1)** Εμβολιασμός των νεογνών

Με την παρουσία μεταδοτικών ασθενειών, ένας από τους κύριους στόχους είναι η απάλειψή τους μέσω των μέτρων πρόληψης και, εάν είναι δυνατόν, μέσω της καθιέρωσης ενός προγράμματος μαζικού εμβολιασμού. Ας εξετάσουμε μια ασθένεια για την οποία είναι αναγκαίος ο εμβολιασμός των νεογέννητων **[96](**με ένα εμβόλιο που προσφέρει ισόβια ανοσία**)** με ένα ρυθμό : $P \in (0,1)$ :

$$\frac{dS}{dt} = m\mathrm{N}(1-P) - mS - b\frac{I}{\mathrm{N}}S$$

$$\frac{dI}{dt} = b\frac{I}{\mathrm{N}}S - (m+v)I$$

$$\frac{dV}{dt} = mNP - mV$$

όπου το **V** είναι η κατηγορία των εμβολιασμένων.

$$\lim_{t\to\infty}(V(t)) = NP$$

κατά συνέπεια θα εξετάσουμε τη μακροπρόθεσμη συμπεριφορά του **S** και του I, για την οποία ισχύει ότι **[1]**:

$$R_0(1-P) \le 1 \Rightarrow \lim_{t\to\infty}(S(t), I(t)) = DFE = (N(1-P), 0)$$

$$R_0(1-R)>1, I(0)>0 \Rightarrow \lim_{t\to\infty}(S(t),I(t)) = EE = (\frac{N}{R_0(1-P)}, \frac{m}{b}(R_0(1-P)-1))$$

Ή αλλιώς αν

$$P \geq P^* = 1-\frac{1}{R_0}$$

το πρόγραμμα εμβολιασμού θα αφαιρέσει την ασθένεια, ενώ σε αντίθετη περίπτωση θα παραμείνει ενδημικό παρόλο που θα βρίσκεται σε χαμηλότερα επίπεδα σε σύγκριση με τις ομάδες που δεν έχουν εμβολιαστεί. Αυτό σημαίνει ότι το μαθηματικό μοντέλο προτείνει ότι για μια ασθένεια της οποίας ο βασικός αριθμός αναπαραγωγής μπορεί να είναι τόσο υψηλός όπως **18**, θα πρέπει κανείς να εμβολιάσει το **94,4%** των νεογνών προκειμένου να εξαλειφτεί η ασθένεια.

**2)** Εμβολιασμός και πληροφόρηση

Οι σύγχρονες κοινωνίες αντιμετωπίζουν την πρόκληση της "ορθολογικής" εξαίρεσης, δηλ. η οικογενειακή απόφαση να μην εμβολιαστούν τα παιδιά ως συνεπεία μιας "ορθολογικής" σύγκρισης μεταξύ του αντιληπτού κινδύνου που διατρέχουν από τη μόλυνση και αυτού του να έχουν παρενέργειες από το εμβόλιο. Προκειμένου να αξιολογηθεί εάν αυτή η συμπεριφορά είναι πραγματικά λογική, δηλαδή εάν μπορεί εξίσου να οδηγήσει στην εξόντωση της ασθένειας, κάποιος μπορεί απλά να υποθέσει ότι ο ρυθμός εμβολιασμού είναι μια αυξανόμενη συνάρτηση των μολυσμένων ανθρώπων **[1]:**

**P=P(I), P'(I)>0**

Σε αυτή την περίπτωση η συνθήκη εξόντωσης μετασχηματίζεται

$$P(0) \geq P^*$$

Δηλαδή ο βασικός ρυθμός εμβολιασμού πρέπει να είναι μεγαλύτερος από το κατώτατο όριο του "υποχρεωτικού" εμβολιασμού. Κατά συνέπεια, η "ορθολογική" απαλλαγή μπορεί να είναι μυωπική δεδομένου ότι είναι βασισμένη μόνο στο τρέχων χαμηλό αριθμό συμβάντων λόγω του υψηλού αριθμού εμβολιασμών.

**3)** Εμβολιασμός των μη νεογνών

Σε περίπτωση που υπάρχουν επίσης εμβολιασμοί μη νεογέννητων σε ένα ποσοστό ρ η εξίσωση για τους ευπαθείς και εμβολιασμένων ατόμων πρέπει να τροποποιηθεί ως εξής **[96]:**

$$\frac{dS}{dt} = m\mathrm{N}(1-P) - mS - rS - b\frac{I}{\mathrm{N}}S$$

$$\frac{dV}{dt} = mNP + rS - mV$$

Οδηγώντας στο ακόλουθο κριτήριο εξάλειψης

$$P \geq 1 - (1 + \frac{r}{m})\frac{1}{R_0}$$

**4)** Στρατηγική εμβολιασμού σφυγμού

Η στρατηγική εμβολιασμού σφυγμού είναι μια πολιτική εμβολιασμού που αποτελείται από περιοδικές επαναλήψεις "ενστικτωδών" εμβολιασμών διάφορων ηλικιακών-ομάδων εντός ενός πληθυσμού, δηλαδή κάθε Τ χρονικές στιγμές ένα σταθερό πλήθος π ευπαθών ατόμων εμβολιάζεται σε σχετικά σύντομο (σε σχέση με την δυναμική της ασθένειας) χρονικό διάστημα. Αυτό οδηγεί στις ακόλουθες διαφορικές εξισώσεις για τα ευπαθή και εμβολιασμένα άτομα **[96]:**

$$\frac{dS}{dt} = m\mathrm{N} - mS - b\frac{I}{\mathrm{N}}S,$$

$$S(nT^+) = (1-p)S(nT^-) \quad \textbf{n=0,1,2,....}$$

$$\frac{dV}{dt} = -mV, V(nT^+) = V(nT^-) + pS(nT^-) \quad \textbf{n=0,1,2,....}$$

Είναι εύκολο να φανεί ότι ρυθμίζοντας το **I=0** η δυναμική των ευπαθών ατόμων δίνεται από**:**

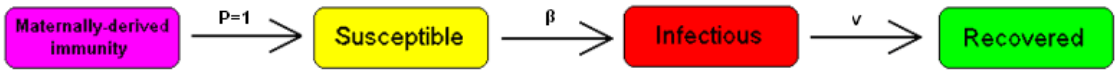
$$S^*(t) = 1 - \frac{p}{1-(1-p)E^{-mT}}E^{-mMOD(t,T)}$$

Και το κριτήριο εξάλειψης είναι

$$R_0\int_0^T S^*(t)dt < 1$$

### 5.3.2 Τροποποιήσεις στο βασικό SIR μοντέλο. Το MSIR μοντέλο

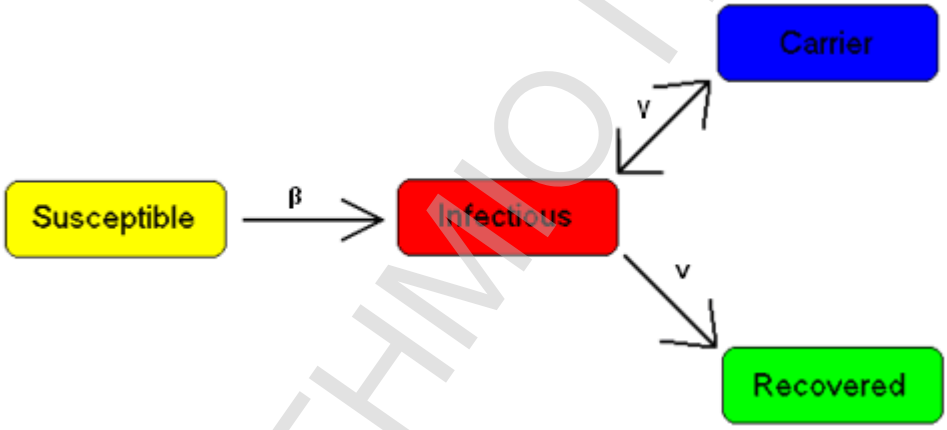
Για πολλές μολύνσεις, συμπεριλαμβανομένης της ιλαράς, τα μωρά δεν γεννιούνται στο διαμέρισμα των ευπαθών αλλά είναι άνοσα στην ασθένεια για τους πρώτους μήνες της ζωής τους λόγω της προστασίας από τα μητρικά αντισώματα. Αυτή η επιπρόσθετη λεπτομέρεια μπορεί να παρουσιαστεί με τη συμπερίληψη μιας κατηγορίας Μ (για την μητρική παραγόμενη ανοσία) στην αρχή του προτύπου (Σχήμα **43**).




**Σχήμα 43. Διάγραμμα ροής MSIR προτύπου**

#### 5.3.2.1 Κατάσταση φορέων

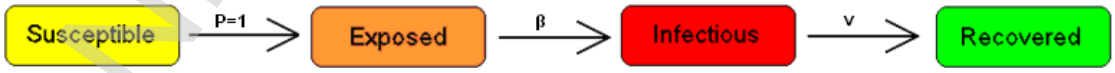
Μερικοί άνθρωποι που είχαν μια μολυσματική ασθένεια όπως η φυματίωση δεν αναρρώνουν ποτέ εντελώς και συνεχίζουν να φέρνουν τη μόλυνση, χωρίς να επηρεάζονται από την ασθένεια οι ίδιοι. Έπειτα μπορεί να μετακινηθούν ξανά στο μολυσματικό διαμέρισμα και να υποστούν τα συμπτώματα (όπως στη φυματίωση) ή μπορούν να συνεχίσουν να μολύνουν άλλα άτομα χωρίς ωστόσο να υποφέρουν και οι ίδιοι από τα συμπτώματα. Το διασημότερο παράδειγμα αυτού είναι πιθανώς η **Mary Mallon**, η οποία μόλυνε **22** ανθρώπους με τον τυφοειδή πυρετό. Το διαμέρισμα των φορέων ονομάζεται **C** (Σχήμα **44**).




**Σχήμα 44. Διάγραμμα ροής SICR μοντέλου**

### 5.3.3 Το μοντέλο SEIR

Για πολλές σημαντικές μολύνσεις υπάρχει μια σημαντική χρονική περίοδος κατά τη διάρκεια της οποίας ενώ το άτομο έχει μολυνθεί δεν είναι ακόμα ο ίδιος μολυσμένος. Κατά τη διάρκεια αυτής της λανθάνουσας περιόδου το άτομο είναι στο διαμέρισμα E (για εκθεμένος Σχήμα **45**).




**Σχήμα 45. Διάγραμμα ροής για το SEIR μοντέλο**

Υποθέτοντας ότι η περίοδος παραμονής στο λανθάνον διαμέρισμα είναι μια τυχαία μεταβλητή με εκθετική κατανομή με παράμετρο **a** (δηλ. η μέση λανθάνουσα περίοδος είναι ένα **a** − **1**), και υποθέτοντας επίσης την παρουσία ζωτικής δυναμικής με ρυθμό γεννήσεων ίσο με το ρυθμό θανάτων, έχουμε το μοντέλο **[78]**:

$$\frac{dS}{dt} = m\mathrm{N} - mS - b\frac{I}{\mathrm{N}}S$$

$$\frac{dE}{dt} = b\frac{I}{\mathrm{N}}S - (m+a)\mathrm{E}$$

$$\frac{dI}{dt} = a\mathrm{E} - (m+v)I$$

$$\frac{dR}{dt} = v\mathrm{I} - mR$$

Επίσης υποθέτουμε ότι **S + E + I + R = N**

Γι' αυτό το μοντέλο ο βασικός ρυθμός αναπαραγωγής είναι

$$R_0 = \frac{a}{m+a}\frac{b}{m+n}$$

Ομοίως με το **SIR** πρότυπο**,** και σε αυτήν την περίπτωση έχουμε μια ισορροπία ελεύθερης ασθένειας **(**N**, 0, 0, 0)** και μια ενδημική ισορροπία **EE,** και εύκολα μπορεί να δειχθεί ότι**,** ανεξάρτητα από τις βιολογικά σημαντικές αρχικές προϋποθέσεις

$$(S(0), E(0), I(0), R(0) \in \{(S, E, I, R) \in [0, N]^4 : S \geq 0, E \geq 0, I \geq 0, R \geq 0, S + E + I + R = N\}$$

$$R_0 \leq 1 \Rightarrow \lim_{t\to\infty}(S(t), E(t), I(t), R(t)) = DFE = (N, 0, 0, 0)$$

$$R_0 > 1, I(0) > 0 \Rightarrow \lim_{t\to\infty}(S(t), E(t), I(t), R(t)) = EE$$

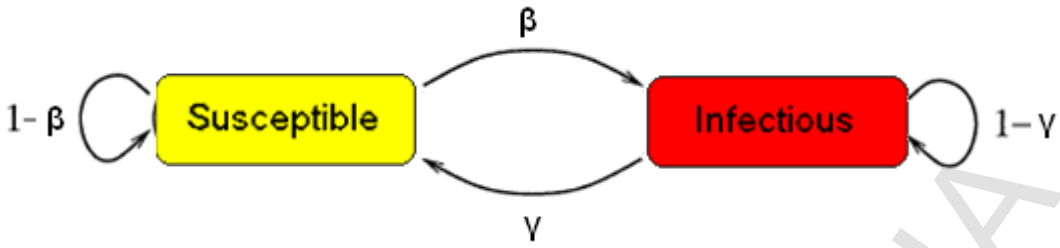
Σε περίπτωση περιοδικά μεταβαλλόμενου ρυθμού επαφών β**(t)** προκύπτει το ακόλουθο γραμμικό σύστημα με τους περιοδικούς συντελεστές**:**

$$\frac{dE_1}{dt} = b(t)I_1 - (v+a)\mathrm{E}_1$$

$$\frac{dI_1}{dt} = a\mathrm{E}_1 - (m+v)I_1$$

### 5.3.4 Το SIS μοντέλο

Μερικές μολύνσεις**,** παραδείγματος χάρην μια ομάδα ατόμων για το κοινό κρυολόγημα**,** δεν βιώνουν οποιαδήποτε μακράς διαρκείας ανοσία**.** Τέτοιες μολύνσεις δεν έχουν κάποια κατάσταση ανάρρωσης και τα άτομα γίνονται ευπαθή πάλι μετά από τη μόλυνση **[78](**Σχήμα **46).**




**Σχήμα 46. Διάγραμμα ροής του SIS μοντέλου**

Έχουμε το ακόλουθο μοντέλο:

$$\frac{dS}{dt} = g\,I - b\,IS$$

$$\frac{dI}{dt} = b\,SI - g\,I$$

$$\frac{dI}{dt} + \frac{dS}{dt} = 0 \Rightarrow S(t) + I(t) = N$$

$$\frac{dI}{dt} = (b\mathrm{N} - g)\mathrm{I} - b\mathrm{I}^2$$

Δηλαδή η δυναμική της μόλυνσης ελέγχεται από μια λογιστική εξίσωση, έτσι ώστε : $\forall \mathrm{I}(0) > 0$ :

$$\frac{b\mathrm{N}}{g} \le 1 \Rightarrow \lim_{t\to\infty} I(t) = 0$$

$$\frac{b\mathrm{N}}{g} > 1 \Rightarrow \lim_{t\to\infty} I(t) = \frac{b\mathrm{N} - g}{b}$$

### 5.3.5 Η επιρροή της ηλικίας: μοντέλα ηλικία δομημένα

Ίσως "η πιο συγκεκριμένη παράμετρος του βιολογικού συστήματος είναι η ηλικία" **(**M. **Iannelli)**, και, ειδικά για μερικές μολυσματικές ασθένειες, έχει μια βαθιά επιρροή στη δυναμική της διάδοσής της σε έναν πληθυσμό. Πολλές από τις παραμέτρους που έχουμε δει μπορούν να εξαρτώνται από την ηλικία, και ειδικά ο ρυθμός επαφών, ο οποίος συνοψίζει τη "μολυσματική αποτελεσματικότητα" των επαφών μεταξύ των ευπαθών και μολυσμένων ατόμων. Αυτή η αποτελεσματικότητα πρέπει, επομένως, να λάβει υπόψη τόσο την ηλικία των μολυσμένων όσο και την ηλικία των ευπαθών ατόμων **[60]**. Τα επιδημικά πρότυπα που μοντελοποιούν τη δομή της ηλικίας ενός πληθυσμού είναι πολύ σύνθετα. Στην πραγματικότητα, είναι άπειρο διαστασιακό μοντέλο δεδομένου ότι πρέπει να εξετάσουμε την πυκνότητα μέσω των

ηλικιών των επιδημικών κατηγοριών **s(t,a),i(t,a),r(t,a) (**για να περιοριστούμε στο ευπαθής-μολυσμένος-αναρρωμένος σχήμα**)** έτσι

ώστε**:**

$$S(t) = \int_0^{a_M} s(t,a)da$$

$$I(t) = \int_0^{a_M} r(t,a)da$$

$$R(t) = \int_0^{a_M} r(t,a)da$$

**(**όπου $\mathbf{a_M \leq +\infty}$ είναι η μέγιστη αποδεκτή ηλικία**)** και η δυναμική που τους δεν περιγράφεται**,** από τις μερικές **"**απλές**"** διαφορικές εξισώσεις**,** αλλά από τις **(integr**ο**)** διαφορικές εξισώσεις**:**

$$\partial_t s(t,a) + \partial_a s(t,a) = -m(a)s(a,t) - s(a,t)\int_0^{a_M} k(a,a_1;t)i(a_1,t)da_1$$

$$\partial_t i(t,a) + \partial_a i(t,a) = s(a,t)\int_0^{a_M} k(a,a_1;t)i(a_1,t)da_1 - m(a)i(a,t) - v(a)i(a,t)$$

$$\partial_t r(t,a) + \partial_a r(t,a) = -m(a)r(a,t) + v(a)i(a,t)$$

Όπου

$$F(a,t,i(.,.)) = \int_0^{a_M} k(a,a_1;t)i(a_1,t)da_1$$

είναι η δύναμη της μόλυνσης**,** που**,** φυσικά**,** θα εξαρτηθεί**,** από τον πυρήνα **k(a,a1;t)** επαφών στις αλληλεπιδράσεις μεταξύ των ηλικιών**.**

Η πολυπλοκότητα προστίθεται από τους αρχικούς όρους για τα νεογνά **(**δηλ**.** για **a=0),** τα οποία είναι μονόδρομα για μολυσμένους και αναρρωμένους**:**

**i(t,0) = r(t,0) = 0**

αλλά αυτοί είναι μη τοπικοί για την πυκνότητα των ευαίσθητων νεογνών**:**

$$s(t,0) = \int_0^{a_M} f_s(a), s(a,t) + f_i(a), i(a,t) + f_r(a), r(a,t))da$$

Όπου φ**j(a), j=s,I,r** είναι οι γονιμότητες των ενηλίκων**.**

Επιπλέον, καθορίζοντας τώρα την πυκνότητα του συνολικού πληθυσμού **n(t,a) = s(t,a) + i(t,a) + r(t,a):**

$$\partial_t n(t,a) + \partial_a s(t,a) = -m(a)n(a,t)$$

Στην απλούστερη περίπτωση ίσων γονιμοτήτων στις τρεις επιδημικές κατηγορίες, για να έχουμε δημογραφική ισορροπία είναι απαραίτητος ο ακόλουθος και ικανοποιητικός όρος που συνδέει τη γονιμότητα φ**(.)** με τη θνησιμότητα μ**(**α**)** πρέπει να ικανοποιεί**:**

$$1 = \int_0^{a_M} f(a)Exp(-\int_o^a m(q)dq))da$$

και η δημογραφική ισορροπία είναι

$$n^*(a) = CExp(-\int_o^a m(q)dq)$$

εξασφαλίζοντας αυτόματα την ύπαρξη της υγιούς λύσης**:**

$$DFS(a) = (n^*(a), 0, 0)$$

Ένας βασικός ρυθμός αναπαραγωγής μπορεί να υπολογιστεί ως η φασματική ακτίνα ενός αρμόδιου συναρτησιακού χειριστή.

## 5.4 Επιδημιολογία υπολογιστών

Παρότι η επιδημιολογία αφορά κυρίως βιολογικούς οργανισμούς, η εμπειρία από τις σχετικές έρευνες, αποδεικνύεται χρήσιμη για την αντιμετώπιση της εξάπλωσης του κακόβουλου λογισμικού. Οι επιδημίες επηρέασαν και επηρεάζουν διαχρονικά την ανθρωπότητα επιφέροντας από δραστικές αλλαγές έως και ολικές ανατροπές του εκάστοτε **status quo [247].**Η σοβαρότητα των συνεπειών τους ήταν φυσικό να προκαλέσει το ενδιαφέρον του ανθρώπου από πολύ νωρίς. Έτσι τα θεμέλια της επιδημιολογίας σαν αυτόνομο επιστημονικό κλάδο, τα έθεσε το **400** π. Χ. ο Ιπποκράτης με την πραγματεία του **'**Περί επιδημιών**'.** Ωστόσο η επιδημιολογία γνώρισε καινούργιο ενδιαφέρον και ώθηση από το έργο του **John Graunt,** Φυσικές και Πολιτικές Παρατηρήσεις σχετικά με τους Ρυθμούς Θνησιμότητας **[103].** Στη συνέχεια πολλοί διακεκριμένοι επιστήμονες όπως οι **Daniel Bernoulli, Ronald Ross, Lowell Reed** και ο **Wade Hampton Frost** συνδύασαν την επιδημιολογία με τα μαθηματικά, δημιουργώντας ένα καινούργιο επιστημονικό κλάδο την Μαθηματική Επιδημιολογία. Η μεγαλύτερη συνεισφορά προήλθε από τους **William Ogilvy Kermack** και **Anderson Gray McKendrick [131],** οι οποίοι παρουσίασαν το Γενικό Επιδημιολογικό Μοντέλο **(General Epidemic Model).** Το βασικό πλεονέκτημα του

Γενικού Επιδημιολογικού Μοντέλου είναι ότι μπορεί να περιγράψει ικανοποιητικά την εξέλιξη μιας επιδημίας με τη χρήση των ακόλουθων διαφορικών εξισώσεων:

$$\frac{dS}{dt} = -\beta SI \quad (1)$$

$$\frac{dI}{dt} = \beta SI - \gamma I \quad (2)$$

$$\frac{dR}{dt} = \gamma I \quad (3)$$

Όπου **S** είναι ο αριθμός των ευπαθών οργανισμών, **I** ο αριθμός των μολυσμένων μελών ενός πληθυσμού, **R** είναι ο αριθμός των μελών που έχουν αναρρώσει ή βρίσκονται σε καραντίνα ή έχουν αποδημήσει, β είναι ο ρυθμός μόλυνσης ανά επαφή **(pairwise rate of infection)** και γ ο ρυθμός απομάκρυνσης μολυσμένων μελών

Οι παραπάνω διαφορικές εξισώσεις για να ισχύουν προϋποθέτουν την ομογενή ανάμιξη του πληθυσμού και ότι ο πληθυσμός είναι σταθερός βάση του τύπου :

**N=S(t) +I(t) +R(t) (4)**

Τις τελευταίες δεκαετίες η Μαθηματική Επιδημιολογία γνώρισε μεγάλη ανάπτυξη και μπόρεσε να συμπεριλάβει και άλλες παραμέτρους, δημιουργώντας ακριβέστερα μοντέλα για αρκετές ασθένειες που εμφανίζουν ιδιαιτερότητες στους πληθυσμούς που μολύνουν ή στο τρόπο εξάπλωσης τους. Οι σημαντικότερες εξελίξεις στο χώρο της Μαθηματικής Επιδημιολογίας αποτυπώνονται αναλυτικά στα εξής συγγράμματα **[22, 67, 99, 108]** ενώ οι βασικότερες αρχές της Επιδημιολογίας παρουσιάζονται επακριβώς στο σύγγραμμα του Τριχόπουλου **[232].** Το Γενικό Επιδημιολογικό Μοντέλο, το οποίο είναι γνωστό και ως **S-I-R (Susceptible-Infective-Recovered)** μπορεί με τις κατάλληλες παραδοχές να περιγράψει με μεγάλη ακρίβεια την εξάπλωση του κακόβουλου λογισμικού. Ας δούμε όμως κάποιες από τις παραμέτρους που λαμβάνουν χώρα στα επιδημιολογικά μοντέλα:

- **N** : ο συνολικός πληθυσμός. Στην επιδημιολογία υπολογιστών και ειδικότερα στην μελέτη διάδοσης κακόβουλου λογισμικού είναι ο αριθμός των συστημάτων που είναι συνδεδεμένα στο διαδίκτυο.

- **S**: ο αριθμός των ευπαθών συστημάτων. Στην προκειμένη περίπτωση ο αριθμός των υπολογιστών που εκτελούν το λειτουργικό σύστημα ή την εφαρμογή που εμφανίζει το κενό ασφαλείας που εκμεταλλεύεται το εξεταζόμενο είδος κακόβουλου λογισμικού. Όσο πιο διαδεδομένο είναι ένα λειτουργικό σύστημα ή μια εφαρμογή τόσο πιθανότερο είναι να προσβληθεί από κάποια μορφή κακόβουλου

λογισμικού αν εμφανίσει κάποιο κενό ασφαλείας. Παράλληλα, κατ' αυτόν το τρόπο ο ευπαθής πληθυσμός καθίσταται γρηγορότερα μολυσμένος, αποδεικνύοντας ότι η ποικιλομορφία στα πληροφοριακά συστήματα δεν αποτελεί μια περιττή πολυτέλεια, αλλά μια απαραίτητη προφύλαξη.

Ø **I**: ο αριθμός των μολυσμένων συστημάτων. Στόχος όλων των ερευνητικών προσπαθειών είναι η ελαχιστοποίηση αυτού του συνόλου.

Ø **R**: ο αριθμός των ανανήψαντων, αποδημήσαντων ή απομονωμένων **(**σε καραντίνα**)** μελών. Στην επιδημιολογία των υπολογιστών το **R** περιλαμβάνει όλα τα συστήματα που είναι επαρκώς προστατευμένα και δεν παρουσιάζουν τα κενά ασφάλειας που αποτελούν τις πύλες εισόδου για το εξεταζόμενο κακόβουλο λογισμικό. Η μεγιστοποίηση του **R** είναι σίγουρα προς το κοινό συμφέρον, αλλά αυτό καθίσταται όλο και δυσκολότερο όσο το χρονικό διάστημα από την κοινοποίηση του κενού ασφαλείας μειώνεται. Επιπρόσθετα, αν κάποιο δικτυακό σκουλήκι εκμεταλλεύεται κάποιο άγνωστο **(zero day)** κενό ασφάλειας, το **R** μπορεί να αυξηθεί μόνο με την χρήση εξωτερικών μηχανισμών ασφαλείας, όπως τα fi**rewall**, τα οποία θα μπορούσαν πιθανώς να ανακόψουν κάποια είδη επιθέσεων. Από την άλλη πλευρά, υπάρχει και μια δεύτερη όψη του **R**, καθώς περιλαμβάνει και τα συστήματα τα οποία καταστρέφονται από το κακόβουλο λογισμικό, κατά αναλογία με τους θανάτους που προκαλούν διάφορα ιογενή νοσήματα στο πρωτότυπο ιολογικό μοντέλο. Για το λόγο αυτό ένα υπερμολυσματικό δικτυακό σκουλήκι είναι αμφίβολο αν θα μπορούσε να διαδοθεί σημαντικά.

Ø β: ο ρυθμός μόλυνσης ανά επαφή. Όσο μεγαλύτερο είναι το β τόσο γρηγορότερα ένα δικτυακό σκουλήκι εξαπλώνεται. Οι συγγραφείς κακόβουλου λογισμικού στην προσπάθεια τους να αυξήσουν το β, χρησιμοποιούν διαισθητικά διάφορες τεχνικές. Χαρακτηριστικά παραδείγματα είναι ανίχνευση πολλών στόχων ταυτόχρονα με την χρήση νημάτων **(threads)** όπως στην περίπτωση του δικτυακού σκουληκιού **Code Red [271]** ή η ενσωμάτωση ολόκληρου του κώδικα του κακόβουλου λογισμικού σε ένα μόνο πακέτο **udp**, προκειμένου να αποφευχθούν οι καθυστερήσεις στην δημιουργία των συνδέσεων που εμπεριέχονται στο πρωτόκολλο **tcp [155]**.

Ø γ: ο ρυθμός απομάκρυνσης μολυσμένων κόμβων λόγω ανάρρωσης, απομόνωσης ή θανάτου σε βιολογικούς οργανισμούς. Κατά την διάρκεια μιας επιδημίας κακόβουλου λογισμικού, αν το γ λάβει μεγάλη τιμή οι προοπτικές για το περιορισμό του λογισμικού που την προκάλεσε είναι ευοίωνες. Αυτό μπορεί να γίνει, είτε με την έγκυρη μεταφόρτωση και εγκατάσταση διορθωτικού κώδικα, είτε αν το φορτίο του κακόβουλου λογισμικού είναι πολύ καταστροφικό. Αντίθετα με

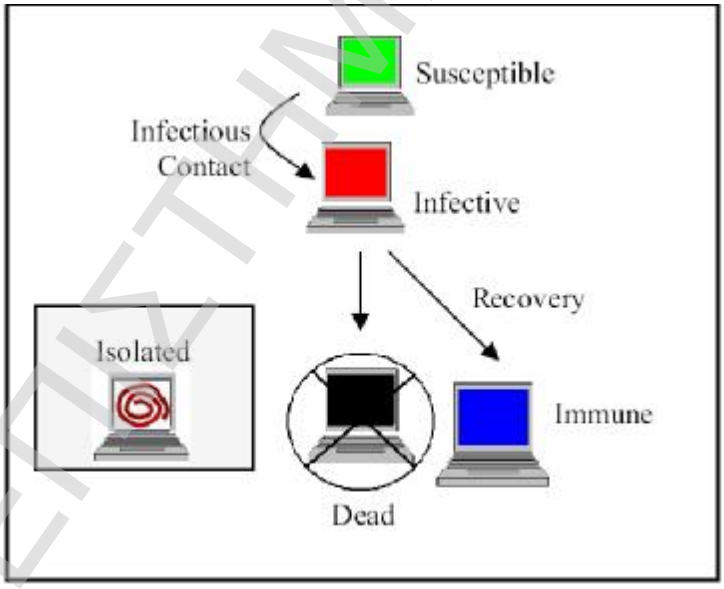
την κοινή πεποίθηση, η ακραία μολυσματικότητα σε ένα δικτυακό σκουλήκι επηρεάζει αρνητικά την εξάπλωση του.

Άλλη μια παράμετρος η οποία προκύπτει από τις παραπάνω εξισώσεις είναι το ρ, το οποίο περιγράφει τον σχετικό ρυθμό απομάκρυνσης **(relative removal rate)** και ορίζεται ως

$$\rho = \frac{\gamma}{\beta} \quad \textbf{(5)}$$

Το ξέσπασμα μίας επιδημίας είναι εφικτό μόνο αν το μέγεθος του αρχικά μολυσμένου πληθυσμού είναι $\mathbf{S_0 > \rho}$. Οι διαφορικές εξισώσεις του Γενικού Επιδημιολογικού Μοντέλου ισχύουν όταν τα εξεταζόμενα συστήματα συνδέονται καθολικά μεταξύ τους σχηματίζοντας ένα ομογενή γράφο. Σε άλλες τοπολογίες η καμπύλη του ρυθμού εξάπλωσης, παρότι διατηρεί την ίδια μορφή, απαιτεί περισσότερο χρόνο για να προσεγγίσει τα ίδια ποσοστά εξάπλωσης.

Όσον αφορά τις πιθανές καταστάσεις που μπορεί να βρίσκεται ένας κόμβος σε αυτά τα μοντέλα είναι μία εκ των **5** διαφορετικών όπως αυτές απεικονίζονται και στο Σχήμα **47.**




**Σχήμα 47. Καταστάσεις που μπορεί να βρίσκεται ο υπολογιστής**

1. Υγιείς **(**ούτε μολυσμένος ούτε με ανοσία **(**εννοώντας ενημερωμένο **antivirus))**
2. Μολυσμένος
3. Απομονωμένος **(** υπολογιστής εκτός δικτύου**)**
4. Με ενημερωμένο **antivirus (**έχει ανοσία**)**

**5.** Νεκρός **(**έχει γίνει **format)**

Ένας υγιής υπολογιστής μολύνεται κατά την επικοινωνία του με ένα μολυσμένο ενώ θεωρούμε ότι θεραπεύεται αν είτε γίνει **format** ή ενημερωθεί το **antivirus** που χρησιμοποιεί **(**δηλαδή αν πεθάνει ή αποκτήσει ανοσία**).** Οι απομονωμένοι υπολογιστές δεν επικοινωνούν με άλλους υπολογιστές και κατ' αυτό τον τρόπο δεν μπορούν ούτε να μολυνθούν αλλά ούτε και να μολύνουν άλλους υπολογιστές**.** Έτσι οι παράγοντες που επηρεάζουν την διάδοση της μόλυνσης είναι οι ακόλουθοι **[23](**Σχήμα **48):**

**Ø** Η πύλη εισόδου του κακόβουλου λογισμικού

**Ø** Η στρατηγική επιλογής νέων στόχων

**Ø** Απόσταση επίθεσης**.** Μέγιστη απόσταση όπου ένας υπολογιστής μπορεί να μολύνει ένα άλλο**.** Αυτή η απόσταση δεν είναι κατ' ανάγκη χωρική μπορεί π.χ ένας υπολογιστής να μολύνει μόνο **pc** που βρίσκονται στο ίδιο δίκτυο με αυτόν ή γειτονικά κτλ**.**

**Ø** Αριθμός επιθέσεων στην μονάδα του χρόνου**.** Πόσες επιθέσεις δηλαδή εξαπολύει ένας κόμβος κατά την διάρκεια της μέρας**.**

**Ø** Αποτελεσματικότητα επίθεσης**.** Καθορίζει πόσο πιθανό είναι ένας υγιής κόμβος να μολυνθεί κατά την επικοινωνία του με ένα μολυσμένο**.**

**Ø** Περίοδος μόλυνσης**.** Η χρονική διάρκεια κατά την οποία ένας υπολογιστής παραμένει μολυσμένος**.**

**Ø** Το αρχικό πλήθος υγιών**-** μολυσμένων κόμβων

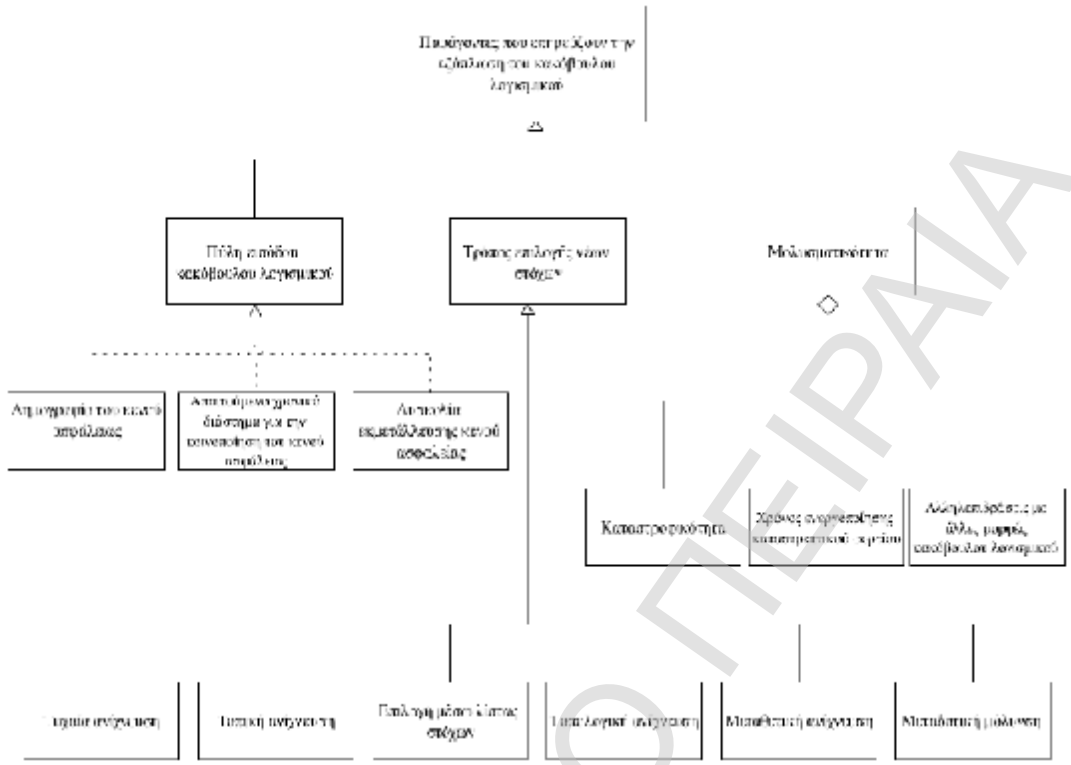
**Ø** Πιθανότητα θανάτου**.** Είναι η πιθανότητα να γίνει **format** σε ένα **pc** μετά από την μόλυνσή του**.**

Επιπλέον παράγοντες που πρέπει να ληφθούν υπόψη είναι οι ακόλουθοι**:**

**Ø** Γκρουπ στα οποία ανήκει **(**είτε το **pc** εννοώντας δίκτυα ή ο ιδιοκτήτης του π.χ**.** σε ποια **mail** γκρουπ κτλ**).**

**Ø** Ενημέρωση **antivirus (**συχνότητα και καθυστέρηση**)**

**Ø** Απομόνωση κόμβου **(**στρατηγικές απομόνωσης**)**

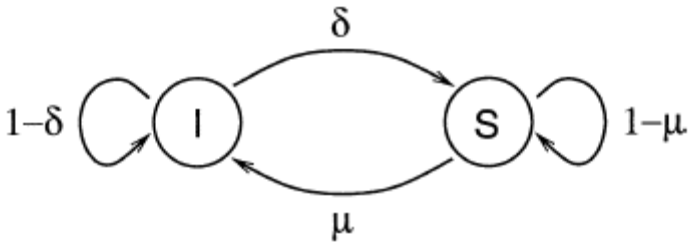


**Σχήμα 48. Παράγοντες που επηρεάζουν την εξάπλωση του κακόβουλου λογισμικού.**

Στην συνέχεια θα εξετάσουμε αναλυτικότερα κάποιες παραλλαγές των γνωστότερων επιδημιολογικών μοντέλων**.**

### 5.4.1 Το SIS μοντέλο σε δίκτυα ελεύθερης κλίμακας

Το μοντέλο αυτό είναι και από τα πιο δημοφιλή μιας και έχει δανειστεί από την επιστήμη της επιδημιολογίας όσον αφορά βιολογικούς ιούς**.** Σε αυτό το μοντέλο κάθε κόμβος αποτελεί μια ξεχωριστή οντότητα και κάθε ακμή **(**σύνδεσμος**)** αναπαριστά μία σύνδεση μέσω της οποίας ο ιός μπορεί να διαδοθεί σε άλλα συστήματα**.** Κάθε κόμβος μπορεί να βρίσκεται σε μία εκ των δύο καταστάσεων**:** υγιής**-**ευπαθείς **(susceptible)** ή μολυσμένος **(infected).** Κάθε χρονική στιγμή ένας υγιής κόμβος μπορεί να μολυνθεί με ένα ρυθμό μ εφόσον είναι συνδεμένος με έναν ή περισσότερους κόμβους**.** Αντίστοιχα ένας μολυσμένος κόμβος μπορεί να γίνει ξανά υγιής με ένα ρυθμό δ ορίζοντας έτσι ένα ρυθμό διάδοσης του ιού τον οποίο και συμβολίζουμε με λ**=**μ**/**δ **[82](**Σχήμα **49).**




**Σχήμα 49. Διάγραμμα ροής SIS μοντέλου**

Χωρίς να κάνουμε κάποια γενίκευση μπορούμε να θέσουμε το δ**=1** έτσι ώστε το μοντέλο που προκύπτει να αναπαριστά την περίπτωση ύπαρξης προγράμματος προστασίας στην οποία όλοι οι μολυσμένοι κόμβοι γίνονται τελικά υγιείς**.** Το ζητούμενο λοιπόν σε αυτή την περίπτωση είναι η εύρεση ενός επιδημικού κατωφλίου λ**c** τέτοιο ώστε για οποιαδήποτε τιμή του λ μεγαλύτερη από αυτό**,** η διάδοση της μόλυνσης να γίνετε επίμονη ενώ για τιμές του λ μικρότερες αυτού του κατωφλίου η μόλυνση να εξασθενεί με εκθετικό ρυθμό**.**

Στατιστικά δεδομένα εξάπλωσης πραγματικών ιών σε δίκτυα ελεύθερης κλίμακας**, (**δηλαδή για δίκτυα όπου η πιθανότητα ένας κόμβος να είναι συνδεμένος με άλλους **n,** δίνεται από τον τύπο **P(n)=n**$^{-k}$ όπου το **k** κυμαίνεται από **2** έως **3)** οδηγούν στο συμπέρασμα ότι όλοι οι επίμονοι ιοί οδηγούνται σε κορεσμό με πολύ μικρό ποσοστό ανθεκτικότητας επηρεάζοντας μόνο ένα πολύ μικρό ποσοστό επί του συνολικού αριθμού των υπολογιστών**.** Αυτό το γεγονός έρχεται σε αντιπαράθεση με τις θεωρητικές προβλέψεις **(**εκτός βέβαια της σπάνιας περίπτωσης όπου όλοι οι ιοί έχουν ρυθμό διάδοσης απειροελάχιστα μεγαλύτερο από την τιμή του κατωφλίου λ**c).** Το γεγονός αυτό αποδεικνύει ότι παρόλο που το εν λόγο μοντέλο είναι αρκετά διδακτικό δεν επαρκεί για την αναπαράσταση του πραγματικού φαινομένου**.**

Το ντετερμινιστικό αυτό μοντέλο είναι ομογενές **(**δηλαδή κάθε κόμβος έχει την ίδια πιθανότητα να θεραπευτεί ή να μεταδώσει την μόλυνση **)** και προτάθηκε από τον **Ross (1915).** Ουσιαστικά αυτό που κάνει είναι η δημιουργία μια καμπύλης **(**γραφικής παράστασης**)** όπου προβλέπει τον αφανισμό της επιδημίας οποτεδήποτε ο βασικός ρυθμός αναπαραγωγής **(**έστω **R)** είναι μικρότερος της μονάδας**,** ενώ διατήρηση αυτής αν **R>1** οποτεδήποτε η αρχική αναλογία των μολυσμένων κόμβων είναι θετική**.**

Το στοχαστικό **SIS** μοντέλο προτάθηκε από τους **Weiss** και **Dishon (1971) [130].** Και ουσιαστικά είναι μια συνεχούς χρόνου **Markov** αλυσίδα γεννήσεων και θανάτων η οποία χρησιμοποιείται για την μοντελοποίηση επιδημιών**,** την διάδοση φημών καθώς και για την μοντελοποίηση των χημικών αντιδράσεων**.**

Η μακροχρόνια συμπεριφορά των ντετερμινιστικών και στοχαστικών μοντέλων **SIS** είναι τελείως διαφορετική. Στο στοχαστικό μοντέλο η επιδημία εξαλείφεται με πιθανότητα **1** ανεξάρτητα από τις παραμέτρους του μοντέλου. Ωστόσο το χρονικό διάστημα που μεσολαβεί μέχρι την εξάλειψη της επιδημίας εξαρτάται από την μόλυνση και από τον ρυθμό με τον οποίο οι κόμβοι γίνονται και πάλι υγιείς, και το αυτό διάστημα μπορεί να είναι πολύ μεγάλο.

Τα επιδημικά μοντέλα για ιούς υπολογιστών έχουν ερευνηθεί τουλάχιστον από το **1988.** Ο **Murray (1988) [94]** φαίνεται να είναι ο πρώτος που πρότεινε την συσχέτιση μεταξύ των επιδημιολογικών μοντέλων και της διάδοσης των ιών των υπολογιστών παρόλο που δεν είχε προτείνει κάποιο συγκεκριμένο μοντέλο. Για να ακολουθήσουν οι **Kephart** και **White (1991,1993) [73]** καθώς και ο **Kephart (1993) [72]** που πρότειναν την χρήση του **SIS** μοντέλου για την μοντελοποίηση της διάδοσης των ιών των υπολογιστών.

### 5.4.2 Το μοντέλο SIS με επανεισαγωγή.

Έστω **n** είναι ο αριθμός των υπολογιστών, **r** ο ρυθμός μόλυνσης κάθε υγιή κόμβου, και **c** ο ρυθμός θεραπείας των μολυσμένων κόμβων. Το μοντέλο αυτό μπορεί να παρομοιαστεί με μια **(Markov)** αλυσίδα, συνεχούς χρόνου **n+1** καταστάσεων όπου κάθε κατάσταση προσδιορίζει των αριθμό των μολυσμένων κόμβων. Μπορούμε να αναπαραστήσουμε την διαδικασία ως μια διεργασία γεννήσεων- θανάτων με ρυθμό γεννήσεων $\lambda_i = r_i(n-1)$ και ρυθμό θανάτων ίσο με $\mu_i = c_i$, για $i = 1,\ldots n-1$. Η παράμετρος **c** εκφράζει τον ρυθμό θεραπείας για ένα κόμβο ενώ η μεταβλητή **r** εκφράζει τον ρυθμό μόλυνσης από ένα συγκεκριμένο μολυσμένο κόμβο σε ένα συγκεκριμένο υγιή.

Οι **Kephart** και **White** μελέτησαν ένα παρόμοιο μοντέλο τόσο αναλυτικά όσο και με χρήση προσομοίωσης και διαπίστωσαν ότι υπό ορισμένες συνθήκες ο πληθυσμός των μολυσμένων κόμβων μεγάλωνε γρήγορα. Στην πραγματικότητα στα αρχικά στάδια της επιδημίας η εξάπλωση αυτής γίνεται με εκθετικό ρυθμό ενώ μετά από αυτό το στάδιο βρίσκεται σε ισορροπία. Ωστόσο όπως έχουμε ήδη αναφέρει η καταστολή της επιδημίας είναι βέβαιη και έτσι αυτή η κατάσταση ισορροπίας δεν είναι παρά ένα μεταβατικό στάδιο.

Το μοντέλο που θα μελετήσουμε σε αυτό το σημείο είναι το γνωστό **SIS** με επανεισαγωγή **(**δηλαδή κάθε μολυσμένος κόμβος μόλις θεραπευτεί μπορεί να μολυνθεί εκ νέου από ένα άλλο ιό**).** Η διαδικασία αυτή μπορεί να παραλληλιστεί με το μεταβατικό στάδιο ενός επιδημιολογικού μοντέλου, στην αρχή οι δύο διαδικασίες είναι πανομοιότυπες μέχρι η επιδημιολογική διαδικασία χωρίς επανεισαγωγή να αφανιστεί, ενώ στην συνέχεια η επιδημία με επανεισαγωγή γίνεται πάλι ενεργή

επιδημία μετά από κάποιο τυχαίο διάστημα αναμονής**.** Για το λόγο αυτό η επιδημία με επανεισαγωγή θα έχει πάντα μεγαλύτερο ή ίσο πληθυσμό μολυσμένων κόμβων**.** Όπως φαίνεται και από την ακόλουθη φόρμουλα **(Ross) [107]**

$$P_0 = \frac{1}{1+\sum_{i=1}^{n} \frac{l_0 l_1 \ldots l_{i-1}}{m_0 m_1 \ldots m_i}},$$

$$P_k = P_0 \frac{l_0 l_1 \ldots l_{k-1}}{m_0 m_1 \ldots m_k}$$

Υπολογίζοντας τον παράγοντα στο $\mathbf{P_k}$ έχουμε

$$\frac{l_0 l_1 \ldots l_{k-1}}{m_0 m_1 \ldots m_k} = \frac{ar^{k-1}(n-1)!}{kc^k (n-k)!}$$

Εκτελώντας επιπρόσθετους υπολογισμούς με την βοήθεια του **Mathematica** καταλήγουμε σε

$$P_0 = \frac{c}{\mathrm{c} + \mathrm{a}_p F_q [\{1, 1, \mathrm{n} - 1\},\{2\},-\frac{r}{c}]}$$

Όπου $\mathbf{a_pF_q}$ είναι μία γενικευμένη υπεργεωμετρική συνάρτηση **(Wolfram) [133].** Σε αυτή την περίπτωση **p=3** και **q=1.** Παρόμοια

$$P_k = \frac{ar^{k-1}(n-1)!}{kc^{k-1}(n-k)!(\mathrm{c} + \mathrm{a}_p F_q [\{1, 1, \mathrm{n} - 1\},\{2\},-\frac{r}{c}])}$$

Αυτές οι εξισώσεις μπορούν να χρησιμοποιηθούν για τον υπολογισμό πολλών παραμέτρων**.**

$$P_0 = \frac{1}{1+\sum_{k=1}^{n} \frac{ar^{k-1}(n-1)!}{kc^k (n-k)!}} = \frac{c}{\mathrm{c+a(n-1)!}\sum_{k=1}^{n} \frac{(r/c)^{k-1}}{k(n-k)!}}$$

Γράφοντας το άθροισμα ως

$$\int f(x)dx = \sum_{i=0}^{n-1} \frac{x^{n-1}}{i!} \square\, x^n e^{\frac{1}{x}},$$

$$f(x) = \sum_{i=1}^{n} \frac{x^{i-1}}{i(n-i)!} = \sum_{i=0}^{n-1} \frac{x^{n-i-1}}{(n-i)i!}$$

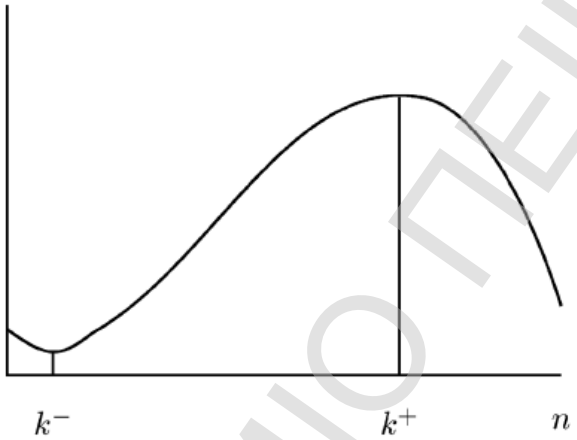
Έτσι διαφορίζοντας και τα δύο άκρα παίρνουμε

$$f(x) \propto x^{n-1} e^{\frac{1}{x}} (1+x)$$

Και τελικά

$$P_0 = \frac{c}{c + a(n-1)!(\frac{r}{c})^n e^{\frac{r}{c}} (\frac{r}{c}+1)}$$

Καταλήγοντας στο ακόλουθο διάγραμμα διακύμανσης **(**Σχήμα **50)**




**Σχήμα 50. Διάγραμμα διακύμανσης P.**

Υπολογίζοντας τώρα τον λόγο**:**

$$\frac{P_{k+1}}{P_k} = \frac{(a \cdot r^k (n-1)!) \cdot (k \cdot c^k (n-k)!}{(c^{k+1}(k+1)(n-k-1)!) \cdot (a \cdot r^{k-1}(n-1)!)} = \frac{kr(n-k)}{(k+1)c}$$

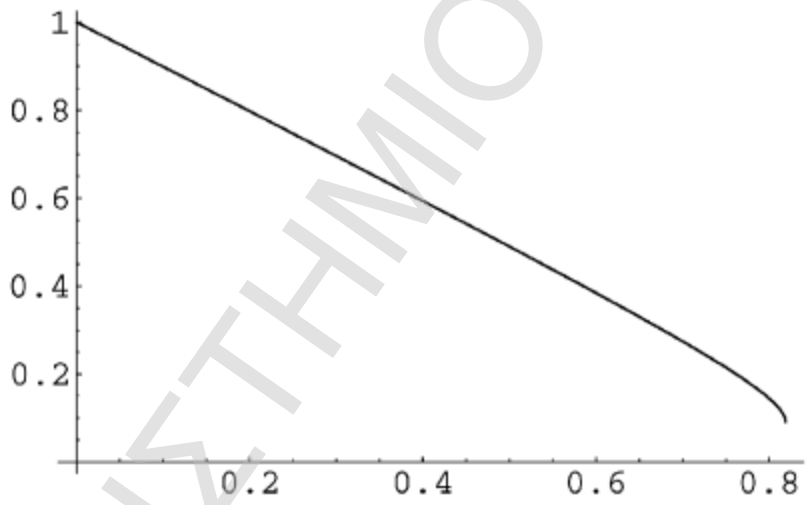
για να αντιληφθούμε ο λόγος είναι μεγαλύτερος μικρότερος ή ίσος με την μονάδα λύνουμε ως προς **k**

$$\frac{kr(n-k)}{(k+1)c} = 1 \Leftrightarrow$$
$$rnk - rk^2 = ck + c \Leftrightarrow$$
$$rk^2 + (c - rn)k + c = 0 \Leftrightarrow$$
$$k^{\pm} = \frac{-(c-rn) \pm \sqrt{(c-rn)^2 - 4rc}}{2r}$$

Έτσι ο λόγος είναι μεγαλύτερος της μονάδας στο διάστημα που ορίζεται μεταξύ των δύο λύσεων και άρα η πιθανότητα $\mathbf{P_k}$ αυξάνεται εντός αυτού του διαστήματος**.** Αντίθετα εκτός αυτού του διαστήματος μειώνεται**.** Επιλέγοντας τον παράγοντα επανεισαγωγής αρκετά μεγάλο η πιθανότητα να βρισκόμαστε στην κατάσταση μηδέν μπορεί να είναι όσο μικρή επιλέξουμε έτσι σε αυτή την περίπτωση εμείς

επιλέγουμε $\left[k^{+}\right]$**.** Παρατηρήστε ότι τα $\left[k^{\pm}\right]$ είναι ανεξάρτητα του παράγοντα επανεισαγωγής **a.**

Επιπλέον κάνοντας την παρατήρηση ότι οι παράγοντες που καθορίζουν το $\left[k^{\pm}\right]$ είναι κατά τι λιγότερο από τον μισό πληθυσμό $\frac{-(c-rn)}{2r}=\frac{n}{2}-\frac{c}{2r}$ ενώ το κλάσμα $\frac{\sqrt{(c-rn)^2-4rc}}{2r}$ είναι ελαφρά μικρότερο από τον πρώτο όρο**.** Καταλήγουμε έτσι στο συμπέρασμα ότι το διάστημα όπου οι πιθανότητες αυξάνονται καλύπτει σχεδόν το εύρος ολόκληρου του πληθυσμού**,** αν οι μεταβλητές **r,c** παραμετροποιηθούν κατάλληλα **(**Σχήμα **51).** Το διάγραμμα αυτό προκύπτει για **r=1, n=100** ως συνάρτηση του **c**




**Σχήμα 51. Διάγραμμα ευπαθών –μολυσμένων κόμβων. Το ποσοστό των μολυσμένων κόμβων αναπαριστάται στον άξονα ψ.**

Μικρό **c/r**

Αν ο ρυθμός θεραπείας είναι μικρός σε σύγκριση με τον ρυθμό μόλυνσης διαισθητικά θα περιμέναμε να παραμένει το μεγαλύτερο ποσοστό του πληθυσμού μολυσμένο**.** Αυτό μας οδηγεί στην παρατήρηση ότι η κατανομή **Poisson** πιθανός να είναι κατάλληλη για την μοντελοποίηση του πληθυσμού των υγιών κόμβων**.**

Ενδιάμεσο **c/r (**κανονική προσέγγιση**)**

Για να επιτύχουμε μια καλύτερη ισορροπία μεταξύ του ρυθμού θεραπείας και μόλυνσης λαμβάνουμε την περίπτωση όπου $\lambda_n$**=c/r**$\to\infty$ καθώς **n**$\to\infty$**.** Καθώς η κατανομή **Poisson** γίνετε ασυμπτωτικά κανονική**,** ο μέσος όρος συγκλίνει στο άπειρο και όπως είναι αναμενόμενο ο αριθμός των μολυσμένων υπολογιστών **(**μεταξύ **n**

συνολικά υπολογιστών**)** προσεγγίζει την κανονική κατανομή για ρυθμούς του $\lambda_n$**=c/r**$\rightarrow\infty$**.**

Μεγάλο **c/r (**Κανονικό και λογαριθμικό όριο**)**

Σε αυτή την περίπτωση ο ρυθμός θεραπείας αυξάνει σχεδόν γραμμικά σε σχέση με το μέγεθος του πληθυσμού**.** Από την ανάλυση αυτής της περίπτωσης συμπεραίνουμε ότι ένα σταθερό ποσοστό του πληθυσμού μολύνεται**.** Έστω **a*n** το πλήθος των μολυσμένων υπολογιστών με **0<a<1** ενώ **c*a*n** ο ρυθμός θεραπείας και **r*a*(1-a)*n** ο ρυθμός μόλυνσης**,** είναι δυνατό να πετύχουμε ισορροπία στο σύστημα μας με κατάλληλη επιλογή των παραμέτρων**.**

### 5.4.3 SIDR μοντέλο

Εξαιτίας της ιδιαίτερης σημασίας αυτού του μοντέλου αναλύεται με λεπτομέρεια στο κεφάλαιο **5.**

### 5.4.4 Παραλλαγές

Δεδομένου ενός δικτύου και ενός μοντέλου διάδοσης ιών με ένα αρχικό πλήθος μολυσμένων κόμβων εμείς ενδιαφερόμαστε να ανοσοποιήσουμε το μικρότερο δυνατό πλήθος κόμβων έτσι ώστε στο εναπομείναν δίκτυο να είναι συγκρατημένη η διάδοση της μόλυνσης**.** Σε αυτό το σημείο θα εξετάσουμε **2** διαφορετικούς τύπους μοντέλων το ανεξάρτητο σειριακό μοντέλο **Kempe et al [66]** και τα **SIS** μοντέλα **(**μοντέλα δυναμικής διάδοσης**) [97].**

Ξεκινώντας με την πρωτοποριακή εργασία των **Kermack** και **McKendric [75]** όπου καθιερώνουν την πρώτη στοχαστική θεωρεία διάδοσης των επιδημιών που αποδεικνύει την ύπαρξη επιδημικού κατωφλίου το οποίο και καθορίζει αν η επιδημία θα εξαπλωθεί η θα τερματιστεί**.** Ένας μεγάλος αριθμός εργασιών επικεντρώνεται στην παροχή αναλυτικών εκφράσεων για επιδημικά κατώφλια για διαφορετικά μοντέλα διάδοσης και διαφορετικές κατηγορίες δικτύων **[22].**

Σε ομογενή δίκτυα ένας αποτελεσματικός μηχανισμός καταστολής της διάδοσης των επιδημιών είναι η θεραπεία τυχαίων κόμβων στο δίκτυο **[16].** Ωστόσο η μέθοδος αυτή είναι ανεπαρκής για δίκτυα ελεύθερης κλίμακας λόγω της ύπαρξης κόμβων με υψηλή συνδεσιμότητα**.** Παρόλα αυτά ακόμα και γι' αυτά τα δίκτυα μπορεί να αποδειχθεί ότι υπάρχει επιδημικό κατώφλι**.** Μία καλή πρακτική για την αντιμετώπιση της εξάπλωσης των επιδημιών σε αυτά τα δίκτυα είναι να θεραπεύουμε αυτούς τους κόμβους που παρουσιάζουν υψηλή συνδεσιμότητα έτσι ώστε να οδηγηθούμε σε εξασθένιση της διάδοσης της επιδημίας**.**

Σε περιπτώσεις όπου η τοπολογία των δικτύων δεν είναι γνωστή ο **Cohen [34]** έδειξε ότι η ανοσοποίηση τυχαίων ακολουθιών με τυχαίους κόμβους είναι καλύτερη από την ανοσοποίηση τυχαίων κόμβων.

Τέλος ο **Aspen [9]** υιοθετεί την προσέγγιση ότι οι κόμβοι του γράφου ενεργούν εγωιστικά και μελετούν στρατηγικές εμβολιασμού βασισμένες στην θεωρία των παιγνίων. Επίσης λαμβάνουν υπόψη συγκεντρωτικές εκδοχές του προβλήματος και εισάγουν το πρόβλημα κατάτμησης του αθροίσματος των τετραγώνων όπου καταλήγουν σε ένα αλγόριθμο πολυωνυμικού χρόνου $O(\log^2 n)$.

#### 5.4.4.1 Το γενικό περιβάλλον εργασίας.

Το πρόβλημα της ανοσοποίησης έχει τις εξής παραμέτρους:

Ø Το δίκτυο στο οποίο λαμβάνει χώρα και η διάδοση. Η μοντελοποίηση του γίνετε ως ένας γράφος **G=(V,E)**. Θεωρούμε ότι ο γράφος δεν έχει κατεύθυνση αν και τα περισσότερα από τα αποτελέσματα στα οποία καταλήγουμε ισχύουν και για κατευθυνόμενους γράφους.

Ø Το μοντέλο διάδοσης του ιού.

Ø Ο αλγόριθμος ανοσοποίησης όπου μπορεί να θεραπεύει ένα σύνολο κόμβων του δικτύου με στόχο την ελαχιστοποίηση της διάδοσης του ιού. Ένας θεραπευμένος κόμβος δεν μπορεί ούτε να κολλήσει αλλά ούτε και να μεταδώσει ιούς. Έτσι μπορούμε να θεωρήσουμε ότι οι θεραπευμένοι κόμβοι αφαιρούνται από το δίκτυο. Το κόστος του αλγόριθμου ανοσοποίησης είναι ίσο με το πλήθος των κόμβων που έχουν θεραπευθεί.

Ø Ο αντίπαλος, που έχει τη γνώση του αλγόριθμου διάδοσης ιών, και τοποθετεί **r** αντίγραφα του ιού στο δίκτυο ώστε να μεγιστοποιηθεί η διάδοση του. Θα χρησιμοποιήσουμε το **Ar** για να προσδιορίσουμε ένα τέτοιο ξενιστή. Ο ξενιστής μπορεί επίσης να έχει τη γνώση των επιλογών που γίνονται από τον αλγόριθμο ανοσοποίησης. Καλούμε έναν τέτοιο ξενιστή προσαρμοστικό ξενιστή. Εξετάζουμε επίσης έναν τυχαίο ξενιστή που τοποθετεί τα αντίγραφα ιών ομοιόμορφα και τυχαία.

#### 5.4.4.2 Το ανεξάρτητο σειριακό μοντέλο.

Το μοντέλο αυτό είναι μια διακριτού χρόνου ειδική περίπτωση του **SIR** μοντέλου. Την χρονική στιγμή **t=0** ο ξενιστής τοποθετεί **r** ιούς σε ορισμένους κόμβους του γράφου. Από αυτή την χρονική στιγμή και έπειτα αν ένας κόμβος έστω **i** μολυνθεί για πρώτη φορά **(**την χρονική στιγμή **t)** του δίνεται μία και μόνο ευκαιρία να προσβάλει κάθε ένα από τους **j** γείτονές του που παραμένουν υγιείς. Η πιθανότητα του να μολύνει ο κόμβος **i** τον κόμβο **j** θα συμβολίζεται ως **pij**. Αν ο κόμβος **i**

επιτύχει να μολύνει τον κόμβο **j** την χρονική στιγμή **t** τότε αυτός μολύνεται την χρονική στιγμή **t+1** διαφορετικά ο κόμβος **i** δεν δοκιμάζει ποτέ ξανά να τον μολύνει**.** Κατά αυτό τον τρόπο συνεχίζει και η διαδικασία της μόλυνσης έως ότου να μην υπάρχουν πλέον κόμβοι να μολυνθούν**.** Όπως εύκολα μπορείτε να αντιληφτείτε το χρονικό διάστημα αυτό είναι πεπερασμένο με άνω όριο την χρονική στιγμή **n,** όπου **n** είναι το πλήθος των κόμβων του δικτύου**.**

Αυτό το μοντέλο αποτελεί μία ειδική περίπτωση του **SIR** μοντέλου στην οποία ο χρόνος πλέον είναι διακριτό μέγεθος και κάθε μολυσμένος κόμβος παραμένει σε αυτή την κατάσταση για μία ακριβώς χρονική στιγμή**.**

Ας υποθέσουμε λοιπόν ότι ο γράφος μας συμβολίζεται ως **G** και έστω N**r** είναι ένα υποσύνολο του**,** που αποτελείται από **n** μολυσμένου κόμβους**.** Γενικά δοσμένου ενός γράφου **G** θα συμβολίζουμε με **S(Nr,G)** το αναμενόμενο πλήθος των μολυσμένων κόμβων**.** Επιπλέον έστω $S_r(G) = \max_{N_r} S(N_r, G)$ να προσδιορίζει το μέγιστο αναμενόμενο αριθμό μολυσμένων κόμβων**.** Το υποσύνολο A**r=argmax$_{Nr}$S(Nr,G)** προσδιορίζει τις επιλογές των προσαρμοστικών ξενιστών ενώ συμβολίζουμε με **Sr(G)** την διάδοση της επιδημίας στο **G.** Μπορούμε να δώσουμε αντίστοιχους ορισμούς για την επιδημική διάδοση μέσω τυχαίων ξενιστών**.** Σε αυτή την περίπτωση ορίζουμε $\hat{S}_r(G) = E_N[S(N_r, G)]$ την αναμενόμενη επιδημική διάδοση**.**

Έχοντας αυτά ως δεδομένα ορίζουμε τα παρακάτω προβλήματα θεραπείας**.**

Δοθέντος ενός γράφου **G,** ενός αριθμού **r** αρχικών ιών να βρεθεί ένας αριθμός **k** άνοσων κόμβων στο γράφο τέτοιος ώστε η επιδημική διάδοση **Sr(G')** στον γράφο **G'** να ελαχιστοποιηθεί

Δοθέντος ενός γράφου **G,** ενός αριθμού **r** αρχικών ιών να βρεθεί ένας αριθμός **k** άνοσων κόμβων στο γράφο τέτοιος ώστε η επιδημική διάδοση $\hat{S}_r(G')$ στον γράφο **G'** να ελαχιστοποιηθεί

#### 5.4.4.3 Μοντέλα δυναμικής διάδοσης

Τα μοντέλα που θα εξετάσουμε αποτελούν ειδικές περιπτώσεις του **SIS** μοντέλου**.** Θεωρούμε την διάδοση του ιού ως μία δυναμική διαδικασία γεννήσεων και θανάτων που λαμβάνει χώρα με την πάροδο του χρόνου**.** Ο ιός διαδίδεται συνέχεια στο δίκτυο αλλά μπορεί και να πεθαίνει**.** Ποιο συγκεκριμένα ένας μολυσμένος κόμβος **I** μεταδίδει τον ιό σε ένα κόμβο **j** με πιθανότητα διάδοσης β**,** ενώ την ίδια στιγμή ένας

μολυσμένος κόμβος μπορεί να θεραπευτεί με πιθανότητα δ. Ο λόγος β/δ ορίζει τον ρυθμό μόλυνσης του ιού.

Έστω ότι M είναι η μήτρα γειτνίασης του γράφου **G** και λ**1(**M**)** η μεγαλύτερη ιδιοτιμή του M. Κατόπιν, ο όρος **β/δ < 1/λ$_1$(M)** είναι ικανοποιητικός για τη γρήγορη αποκατάσταση του συστήματος. Ακριβέστερα το ακόλουθο θεώρημα μπορεί να αποδειχθεί **[127]**.

Θεώρημα **1**

Δοσμένου ενός γράφου **G** με μήτρα γειτνίασης **M** και ρυθμό μόλυνσης **β/δ**, εάν **β/δ < 1/λ$_1$ (M)** τότε ο αναμενόμενος ο χρόνος μέχρι την εξάλειψη των ιών είναι λογαριθμικός και σχετίζεται με τον αριθμό των κόμβων στο σύστημα, ενάντια σε έναν προσαρμοστικό ξενιστή.

Επιπλέον, για πολλά είδη γράφων, ο ανωτέρω όρος είναι επίσης απαραίτητος για τη γρήγορη αποκατάσταση, δηλ., εάν **β/δ < 1/λ$_1$**, ο αναμενόμενος χρόνος μέχρι να εξαλειφτεί ο ιός είναι εκθετικός στο μέγεθος του συστήματος **[48]**. Κατά συνέπεια, έχει νόημα η θεώρηση ενός επιδημικού κατωφλίου του δικτύου, το οποίο καθορίζει εάν μια επιδημία θα εξαπλωθεί, ή θα εξασθενίσει γρήγορα.

Μια αυστηρή ανάλυση του δυναμικού προτύπου ανάγεται στο πρόβλημα της λύσης ενός μη γραμμικού συστήματος, το οποίο είναι δύσκολο να λυθεί αναλυτικά. Έτσι, εξετάζουμε επίσης ένα πολλαπλών αντιγράφων μοντέλο, το οποίο είναι ευκολότερο να αναλυθεί. Σε αυτό το πρότυπο υποθέτουμε ότι κάθε κόμβος μπορεί να έχει πολλαπλάσια αντίγραφα του ιού. Ακριβέστερα, συμβολίζουμε με **u$^t$** ένα **n** διάστατο διάνυσμα το οποίο περιγράφει την κατάσταση του δικτύου την χρονική στιγμή **t**, όπου **u$_i^t$** είναι ο αριθμός των αντιγράφων του ιού στον κόμβο **i** την χρονική στιγμή **t**.

Κατά την χρονική στιγμή **t = 0**, **u$_i^0$** είναι ο αριθμός αντιγράφων του ιού που έχουν προέλθει από τον ξενιστή στον κόμβο **i**. Στο βήμα **t**, το σύστημα εξελίσσεται ως εξής. Για κάθε κόμβο **i** στο δίκτυο, και για κάθε ένα από **u$_i^t$** αντίγραφα του ιού στον κόμβο **i**, ένα αντίγραφο του ιού διαδίδεται στον κόμβο **j** με πιθανότητα β. Κατόπιν, τα αντίγραφα των ιών καταστρέφονται με πιθανότητα **1-**δ. Εάν **Δ=β + diag(1-**δ,…**1-**δ**)** και $\hat{u}^t$ είναι η αναμενόμενη κατάσταση του συστήματος στο βήμα **t**, τότε $\hat{u}^t = \Delta \hat{u}^{t-1}$. Επομένως, το σύστημα είναι απολύτως γραμμικό και μπορούμε να αποδείξουμε το ακόλουθο θεώρημα.

Θεώρημα **2**. Δοσμένου ενός γράφου **G** με μήτρα γειτνίασης **M** και ρυθμό μόλυνσης **β/δ**, ο αναμενόμενος χρόνος μέχρι ο ιός να πεθαίνει είναι λογαριθμικός στον αριθμό

κόμβων στο σύστημα εάν **β/δ<1/λ$_1$(M),** ενώ είναι απεριόριστος εάν **β/δ<1/λ$_1$(M),** ενάντια σε έναν προσαρμοστικό ξενιστή**.**

Συνεχίζοντας θα καθορίσουμε το ακόλουθο πρόβλημα ανοσοποίησης για το δυναμικό μοντέλο**.**

Πρόβλημα **3 (THRESHOLDMAXIMIZATION).** Δεδομένου ενός γράφου **G,** και ενός ρυθμού μόλυνσης **β/δ,** ανοσοποιούμε τον ελάχιστο αριθμό κόμβων μέσα στο **G,** έτσι ώστε **β/δ<1/λ$_1$(M'),** όπου **M'** είναι η μήτρα γειτνίασης του ανοσοποιημένου γράφου**.**

## 5.4.5 Στρατηγικές ανοσοποίησης

### 5.4.5.1 Το ανεξάρτητο σειριακό πρότυπο. Ελαχιστοποιώντας την διάδοση της επιδημίας

Σε αυτό το τμήμα θα μελετήσουμε κάποιους αλγόριθμους για την ανοσοποίηση δικτύων**.** Στην αρχή θα μελετήσουμε ένα αλγόριθμο για το πρόβλημα **1,** ελαχιστοποίηση της επιδημίας**.** Θεωρούμε λοιπόν την περίπτωση όπου **k** κόμβοι είναι αρχικά ανοσοποιημένοι ενάντια σε έναν ξενιστή που τοποθετεί μόνο ένα ιό **(r = 1).** Το βασικό χαρακτηριστικό του αλγορίθμου**, (**το οποίο βασίζεται στην παρατήρηση του **Kempe et Al)[66],** είναι η πιθανολογική διαδικασία της διάδοσης ιών ως δειγματοληψία όλων των $2^{/E/}$ πιθανών γράφων σύμφωνα με τη διανομή που καθορίζεται από τις πιθανότητες $p_{ij}$ και στην συνέχεια η εκτέλεση του ντετερμινιστικού σειριακού μοντέλο στο δειγματοληπτικά επιλεγμένο γράφο**.** Όταν ένας κόμβος **i** μολύνεται τότε κάθε μη μολυσμένος σε αυτό το βήμα **j,** γείτονας του **i,** μολύνεται επίσης με πιθανότητα $p_{ij}$ **.** Αυτή η διαδικασία είναι ισοδύναμη με μια διαδικασία όπου κάθε ακμή **(i, j)** είναι ενεργή στο γράφο με πιθανότητα $p_{ij}$ και ο ιός διαδίδεται μόνο μέσω αυτών των ενεργών ακμών**.** Αντίστοιχα αυτό είναι ισοδύναμο με τη δειγματοληψία ενός γράφου **X** από το σύνολο όλων των υποσυνόλων του **G,** όπου κάθε ακμή **(i, j)** του **G** είναι παρούσα μέσα στον **X** με πιθανότητα $p_{ij}$ **,** ενώ η διάδοση του ιού γίνετε ντετερμινιστικά στον **X.**

Δοσμένου ενός γράφου **X (**που επιλέγεται από τον **G** όπως περιγράφτηκε στην προηγούμενη παράγραφο**)** εάν ο ξενιστής τοποθετήσει έναν ιό στον κόμβο **u,** ο αριθμός των μολυσμένων κόμβων **s({u},X),** είναι ο αριθμός των κόμβων του **X** που συνδέονται με τον **u.** Κατόπιν**,** η αναμενόμενη εξάπλωση της επιδημίας **S({u}, G)** στον **G** με την αρχική τοποθέτηση του ιού στον κόμβο **u** μπορεί να εκφραστεί ως εξής

$$S(\{u\},G)=\sum_{X}\Pr[X]s(\{u\},X)$$

Όπου **Pr[**X**]** είναι η πιθανότητα της λήψης του γράφου **X** από τον **G** όταν η δειγματοληψία γίνεται με βάση τις ακμές με πιθανότητα $p_{ij}$**.** Επομένως δοσμένου του **G,** μπορούμε να υπολογίσουμε το **S({u}, G)** χρησιμοποιώντας την ανωτέρω εξίσωση**.**

Συμβολίζουμε με $G|_{w1,w2,\ldots}$ τον γράφο που προκύπτει μετά από την ανοσοποίηση των κόμβων **w1,w2, …** του **G.** Ας υποθέσουμε ότι αρχικά θέλουμε να ανοσοποιήσουμε μόνο έναν κόμβο **(k = 1).** Για όλους τους υποψήφιους κόμβους **w1** που θα ανοσοποιηθούν**,** μπορούμε να υπολογίσουμε την τιμή $S(G|w_1) = \max_u S(\{u\}, G|w_1)$**,** η οποία είναι η χειρότερη δυνατή περίπτωση **(**από όλες τις δυνατές αρχικές τοποθετήσεις ιών**)** εξάπλωσης της επιδημίας εάν ο κόμβος $w_1$ επιλεχθεί να ανοσοποιηθεί**.**

Κατόπιν επιλέγουμε να ανοσοποιήσουμε τον κόμβο **w** ο οποίος ελαχιστοποιεί την διάδοση της επιδημίας που διαδίδεται **S(G|w).** Σε περίπτωση που θελήσουμε να ανοσοποιήσουμε **k > 1** κόμβους προχωράμε σε μια άπληστη μέθοδο**:** πρώτα ανοσοποιούμε τον κόμβο **w1** που ελαχιστοποιεί το **S(Gjw1 )** και στην συνέχεια βρίσκουμε τον βέλτιστο κόμβο **w2** για να ανοσοποιηθεί στον γράφο **G|w1 (**δηλαδή βρίσκουμε τον κόμβο **w2** που ελαχιστοποιεί το **S(G|w1,w2 )** λαμβάνοντας υπόψη την επιλογή του $w_1$ στο προηγούμενο βήμα**,** και συνεχιζόμαστε κατ**'** αυτό τον τρόπο έως ότου επιλέξουμε κ κόμβους**.**

Άλλος ένας αλγόριθμος είναι να ανοσοποιηθούν οι κόμβοι που αποσυνδέουν τον γράφο σε μικρού μεγέθους συνδεδεμένα συστατικά**,** δεδομένου ότι μια τέτοια κατάτμηση περιορίζει τον ιό όσο το δυνατόν περισσότερο**.** Το μειονέκτημα ωστόσο αυτής της στρατηγικής είναι ότι οι κόμβοι με τον υψηλότερο βαθμό συνδέσεων δεν αποσυνδέουν απαραιτήτως τον γράφο στα μικρότερα δυνατά συνδεδεμένα συστατικά**.**

Χρόνος εκτέλεσης**:** Ο συνολικός χρόνος εκτέλεσης του άπληστου αλγόριθμου**,** για ένα γράφο με **n** κόμβους και **m** ακμές είναι $O(Q(n^2 + nm)k)$**,** όπου **k** είναι ο αριθμός των κόμβων που θα ανοσοποιηθούν και **Q** είναι ο αριθμός των δειγμάτων ανά επανάληψη**.**

**1)** Ελαχιστοποιώντας την αναμενόμενη διάδοση της επιδημίας

Σε αυτό το τμήμα θα εξετάσουμε τις τροποποιήσεις που απαιτούνται στον ανωτέρω **'**άπληστο**'** αλγόριθμο προκειμένου να εξεταστεί το πρόβλημα της ελαχιστοποίησης της αναμενόμενης διάδοσης της επιδημίας στο δίκτυο**.** Δοσμένου ενός γράφου **X** με **c** συνδεδεμένα συστατικά μεγεθών $n_1,\ldots,n_c$**,** τέτοια ώστε $n_1+\ldots+n_c = n$**,** και $f_i = n_i/n$ για $i = 1,\ldots,c$ συμβολίζουμε με $s\hat{}(X)$ την αναμενόμενη διάδοση της επιδημίας στον **X.** Υποθέτοντας ότι ο ξενιστής τοποθετεί έναν ιό στο γράφο**,** ο ιός θα μολύνει το

σύνολο των **i-**οστών συνδεδεμένων συστατικών με πιθανότητα $\mathbf{f_i}$ και το μέγεθος της διάδοσης θα είναι ακριβώς $\mathbf{n_i}$**.** Έτσι

$$\hat{S} = (X) = \sum_{i=1}^{c} f_i \; n_i = \frac{1}{n} \sum_{i=1}^{c} n_i^2$$

Από την ανωτέρω εξίσωση**,** είναι προφανές γιατί αυτός ο αλγόριθμος συσχετίζεται με το πρόβλημα του αθροίσματος των τετραγώνων **[9],** όπως έχουμε ήδη αναφέρει**.**

Ο άπληστος αλγόριθμος για την αναμενόμενη ελαχιστοποίηση της επιδημίας είναι παρόμοιος με αυτόν που περιγράψαμε ήδη**.** Οι κόμβοι ανοσοποιούνται ένας σε κάθε βήμα μέχρι να επιλεχθούν κ συνολικά κόμβοι**.** Για να επιλέξουμε έναν κόμβο για να ανοσοποιήσουμε**,** χρησιμοποιούμε την εξίσωση $\hat{S}(G'|_w) = \sum \Pr[X] \hat{s}(X|_w)$**.**

Υπολογίζουμε το $\hat{S}(G'|_w)$ για όλους τους κόμβους **w** και επιλέγουμε αυτόν που έχει την μικρότερη τιμή**.** Ο συνολικός χρόνος εκτέλεσης του αλγορίθμου είναι **O(Q(n + m)k).**

**2)** Δυναμικά μοντέλα διάδοσης

Σε συνέχεια τον όσον έχουμε δει έως τώρα το επιδημικό κατώφλι για το μοντέλο δυναμικής διάδοσης είναι ίσο με την αντίστροφη μεγαλύτερη ιδιοτιμή του πίνακα γειτνίασης **M.** Επομένως**,** ο στόχος του αλγορίθμου ανοσοποίησης είναι να μειώσει αυτή την ιδιοτιμή**,** ενώ παράλληλα να ελαχιστοποιεί τις πιθανές ζημιές στο δίκτυο**.**

Θα συμβολίσουμε με $\lambda_1$**,** και $\mathbf{w_1}$ την μεγαλύτερη ιδιοτιμή και το αντίστοιχο ιδιοδιάνυσμα του πίνακα Μ**.** Επίσης συμβολίζουμε με $\mathbf{a_i}$ το **i-**οστό διάνυσμα του **M.** Το γινόμενο $\lambda_1$***** $\mathbf{w_1(i)}$ είναι η τιμή της προβολής του διανύσματος $\mathbf{a_i}$ στο ιδιοδιάνυσμα **w1.** Η τιμή του $\lambda_1$ συλλαμβάνει τη συλλογική δύναμη της ευθυγράμμισης των διανυσμάτων γραμμών με το διάνυσμα $\mathbf{w_1}$**.** Το ιδιοδιάνυσμα $\mathbf{w_1}$ είναι το διάνυσμα με το οποίο τα σημεία είναι πιο ισχυρά ευθυγραμμισμένα**.** Ο κόμβος **i** με τη μέγιστη τιμή $\mathbf{w_1(i)}$ αντιστοιχεί στο διάνυσμα γραμμής που είναι περισσότερο ευθυγραμμισμένο με το διάνυσμα $\mathbf{w_1}$**.** Επομένως**,** αφαιρώντας το **i,** αναμένουμε μια μεγάλη διαταραχή στην ευθυγράμμιση με το $\mathbf{w_1}$ οδηγώντας σε μια μεγάλη μείωση της ιδιοτιμής του $\lambda_1$**.** Στο πρότυπο πολλαπλών αντιγράφων η τιμή του $\mathbf{w_1(i)}$ καθορίζει τον ρυθμό με τον οποίο ο κόμβος **i** συσσωρεύει τα αντίγραφα του ιού**.** Μετά από αρκετά χρονικά βήματα**,** ο κόμβος με την μεγαλύτερη τιμή $\mathbf{w_1(i)}$ θα είναι και ο κόμβος με το μεγαλύτερο αριθμό από αντίγραφα ιών**.**

Ο αλγόριθμος που προτείνεται**,** ο οποίος και ονομάζεται **EIG,** είναι ο ακόλουθος**.** Προχωράμε με επαναλήψεις**,** όπου σε κάθε επανάληψη έχουμε ως είσοδο ένα πίνακα **B.** Στην πρώτη επανάληψη θέτουμε**,** **B = M** και υπολογίζουμε την

μεγαλύτερη ιδιοτιμή $\lambda_1$ και το αντίστοιχο ιδιοδιάνυσμα $\mathbf{w_1}$ του **B.** Επίσης θέτουμε ως επιδημικό κατώφλι τον λόγο β**/**δ. Εάν λοιπόν β**/**δ**<**$\lambda_1$ ο αλγόριθμος τερματίζει**,** διαφορετικά**,** αναζητούμε τον κόμβο **i** με τη μέγιστη τιμή στο ιδιοδιάνυσμα $\mathbf{w_1}$**,** και τον αφαιρούμε από τον γράφο**,** δηλαδή αφαιρούμε την αντίστοιχη σειρά και στήλη από τον **B.** Ο προκύπτων πίνακας αποτελεί είσοδο για την επόμενη επανάληψη**.** Ο χρόνος εκτέλεσης του αλγορίθμου είναι **O(kT),** όπου **k** είναι ο αριθμός κόμβων που έχουν αφαιρεθεί και **T** είναι ο χρόνος που χρειάζεται για να υπολογιστεί η πρώτη ιδιοτιμή και το ιδιοδιάνυσμα**.** Εάν είναι αραιός ο γράφος ο χρόνος είναι ανάλογος του πλήθους των ακμών του γράφου**.**

Μια σημαντική παρατήρηση αποτελεί το γεγονός ότι η κυρίαρχη ιδιοτιμή του γράφου μας δίνει μια ένδειξη για τη συνδεσιμότητα του γράφου**.** Μεγάλες ιδιοτιμές αντιστοιχούν σε γράφους με πολλές συνδέσεις**.** Οι κόμβοι με τη μέγιστη τιμή μέσα στο πρώτο ιδιοδιάνυσμα είναι και αυτοί που παρουσιάζουν την μεγαλύτερη συνδεσιμότητα**.** Η αφαίρεση αυτών των κόμβων προκαλεί μείωση της συνδεσιμότητας στον γράφο**.** Σημειώστε ότι οι τιμές των ιδιοδιανυσμάτων παρέχουν πληροφορίες για τη συνολική δομή του γράφου και αυτός είναι ένας από τους λόγους για τους οποίους ο αλγόριθμός αυτός**,** αποδίδει γενικά καλύτερα από τον απλό **MAXDEGREE** που αφαιρεί τους κόμβους με το μέγιστο βαθμό**,** ο οποίος λαμβάνει υπόψη μόνο τοπικές πληροφορίες**.**

# 6 Το μοντέλο PSIDR

## 6.1 Το προοδευτικό PSIDR μοντέλο

Βασιζόμενοι στις ιδέες που αποκομίστηκαν από τα προηγούμενα πρότυπα, ένα νέο επιδημιολογικό πρότυπο παρουσιάζεται που μοντελοποιεί τις πραγματικές διαδικασίες που λαμβάνουν χώρα στις επιδημίες των ιών των υπολογιστών. Ξεκινώντας εξετάζουμε τα χαρακτηριστικά ενός τυπικού ξεσπάσματος. Συνεχίζοντας, συμπεριλαμβάνουμε τις πτυχές των πραγματικών ξεσπασμάτων στο **PSIDR (**προοδευτικό Ευπαθής-Μολυσμένος-Ανιχνευμένος-Αφαιρεμένος**)** μοντέλο, αρχικά με έναν άτυπο τρόπο και έπειτα αναλυτικά. Ο καθορισμός του προτύπου **PSIDR** συνοδεύεται επίσης με μια αναφορά για τις σχετικές λεπτομέρειες των διάφορων παραμέτρων του. Ένα τρίτο τμήμα αναφέρει τις πτυχές που δεν περιλαμβάνονται στο πρότυπο. Ενώ κλείνουμε με μια συνοπτική περίληψη.

### 6.1.1 Η χρονική πορεία ενός τεχνολογικού ξεσπάσματος

Φανταστείτε την ακολουθία γεγονότων που συμβαίνουν όταν ένα σκουλήκι προσπαθεί να μολύνει ένα τεχνολογικό δίκτυο. Για λόγους απλότητας, το εξεταζόμενο δίκτυο εδώ είναι το δίκτυο ηλεκτρονικού ταχυδρομείου μιας μεγάλης εταιρίας. Μια υπόθεση είναι ότι όλοι οι υπολογιστές στο δίκτυο έχουν κάποιο είδος του λογισμικού προστασίας από ιούς. Αυτό το λογισμικό μπορεί να ενημερώνεται με μία συχνότητα, για παράδειγμα μια φορά την ημέρα, για να σιγουρευτούμε ότι και οι πιο πρόσφατες υπογραφές ιών συμπεριλαμβάνονται στο εν λόγο λογισμικό **(**ΛΠΥ**)**.

Το πρώτο γεγονός που συμβαίνει είναι η αρχική μόλυνση. Παραδείγματος χάριν, ένας υπάλληλος ανοίγει ένα αρχείο **(**εκτελέσιμο**)** που έχει επισυναφτεί σε ένα ηλεκτρονικό μήνυμα που στάλθηκε από κάποιον εκτός της επιχείρηση. Αυτό το πρόγραμμα, μόλις εκτελεσθεί, στέλνεται σε μερικές από τις επαφές του υπαλλήλου **(**έστω, στις πρώτες δέκα διευθύνσεις στο βιβλίο διευθύνσεων**)**. Εάν κάποιες από αυτές τις επαφές είναι στην πραγματικότητα κατάλογοι αλληλογραφίας **(**κατάλογοι επαφών**)**, τότε το δικτυακό σκουλήκι έχει τη δυνατότητα να μολύνει όλες τις επαφές που απαριθμούνται σε αυτό. Μόλις λάβουν οι άλλοι χρήστες τα σταλμένα μηνύματα ηλεκτρονικού ταχυδρομείου, μερικοί απ' αυτούς μπορεί ή και όχι να το ανοίξουν αμέσως, ανάλογα με διάφορους παράγοντες **(**όπως οι προσωπικές συνήθειες, κ.λπ.**)**.

Προτού να μπορέσει το σκουλήκι να καθαριστεί από τους υπολογιστές, πρέπει να ανιχνευθεί πρώτα. Η ανίχνευση θα είναι ιδιαίτερα δύσκολη όταν το σκουλήκι δεν

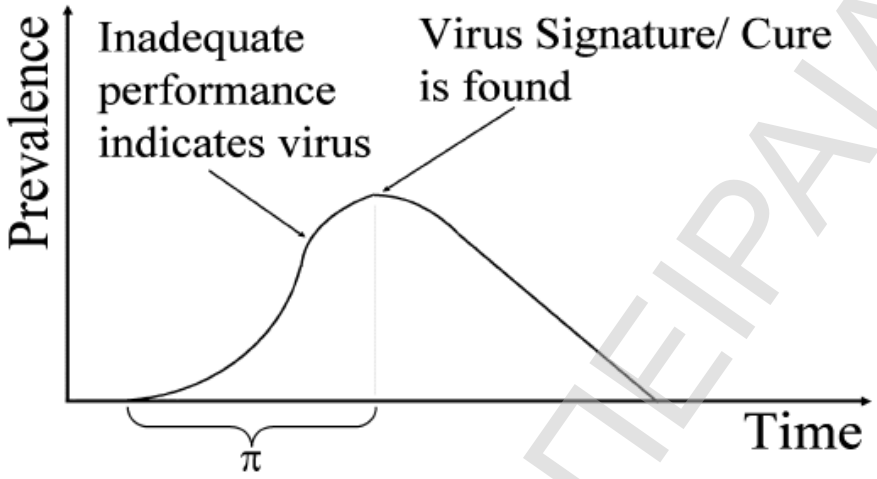
επιβάλλει άμεσα καθόλου ωφέλιμο φορτίο στις μηχανές. Επιπλέον, το λογισμικό προστασίας της εταιρίας θα ανιχνεύσει μόνο τα σκουλήκια (ιούς) για όποια έχει τις υπογραφές. Επομένως, μόλις εντοπιστούν μερικά στιγμιότυπα ενός ιού, οι εταιρίες παραγωγής λογισμικών προστασίας θα προσπαθήσουν να εξαγάγουν την υπογραφή των ιών και να την καταστήσουν διαθέσιμη έτσι ώστε όλοι οι υπολογιστές να μπορούν να ενημερώσουν το λογισμικό τους.

Τα πρώτα στιγμιότυπα του σκουληκιού θα γίνουν αντιληπτά για διάφορους λόγους. Σε μερικές περιπτώσεις, η απόδοση του δικτύου μειώνεται επειδή τα διάφορα αντίγραφα του σκουληκιού καταναλώνουν πάρα πολύ εύρος ζώνης **(bandwith)**. Σε άλλες περιπτώσεις, το ωφέλιμο φορτίο το οποίο έχει επιβληθεί δείχνει σαφώς ότι υπάρχει μια μόλυνση. Επιπρόσθετα υπάρχουν και άλλοι τρόποι με τους οποίους ένας θα μπορούσε να ανιχνεύσει ένα ξέσπασμα, όπως για παράδειγμα η κατοχή του "ολοήμερου προσωπικού" ή ακόμα με έλεγχο από τους προμηθευτές των **antivirus**. Από αυτήν την στιγμή, οι χρήστες γνωρίζουν την απειλή, και αρχίζει να διαμορφώνεται ένα σχέδιο για την καταστολή της. Μόλις είναι διαθέσιμη η υπογραφή, οποιοσδήποτε χρήστης συνδεθεί στον υπολογιστή του μπορεί να ενημερώσει αυτόματα το λογισμικό προστασίας του με τη τελευταία υπογραφή.

Δεδομένου ότι όλο και περισσότεροι χρήστες ενσωματώνονται με την νέα υπογραφή, οι ευπαθείς υπολογιστές αποκτούν σταδιακά ανοσία ενάντια στο σκουλήκι, ενώ οι μολυσμένοι υπολογιστές βαθμιαία ανιχνεύονται. Σε ένα μεγάλο εταιρικό δίκτυο, η χαρακτηριστική αντίδραση όταν βρίσκεται μια μηχανή να είναι μολυσμένη είναι η επίκληση της τεχνικής υποστήριξης για τον πλήρη καθαρισμό. Συνήθως, η πρώτη ενέργεια που λαμβάνει χώρα είναι η απομόνωση του υπολογιστή έτσι ώστε να μην μπορεί να μεταδώσει την μόλυνση. Δηλαδή ο μολυσμένος υπολογιστής μεταβαίνει από μία κατάσταση μόλυνσης σε μια κατάσταση μόλυνσης όπου δεν είναι δεν μπορεί να μεταδώσει την μόλυνση (κατάσταση ανιχνευμένης μόλυνσης).

Η διάρκεια αυτής της κατάστασης εξαρτάται τώρα από πόσο γρήγορα ο ειδικός τεχνικός θα καθαρίσει τον υπολογιστή από την μόλυνση. Μπορεί να πάρει από μερικά λεπτά μέχρι μερικές ώρες (ή ακόμα και τις ημέρες). Μόλις καθαριστεί ο υπολογιστής, συνδέεται πάλι στο δίκτυο και είναι ήδη ανοσοποιημένος σε περαιτέρω μολύνσεις επειδή έχει πλέον τη νέα υπογραφή ιών στους ορισμούς του ΛΠΥ του. Έτσι η μόλυνση εξαλείφεται όταν ανοσοποιούνται όλοι οι υπολογιστές. Στην πράξη, πάντα υπάρχουν μερικές μολύνσεις λόγω της ελλιπούς ανοσοποίησης ή επειδή μερικοί χρήστες δεν είναι ενήμεροι της απειλής. Εάν η επικράτηση του ιού σχεδιαστεί συναρτήσει του χρόνου, θα προκύψει ένα διάγραμμα σαν αυτό που

παρουσιάζεται στο Σχήμα **52.** Είναι εμφανείς η ακολουθία των γεγονότων που περιγράφηκε η οποία και αποτελεί τη βάση του προτύπου **PSIDR (**Σχήμα **52).**




**Σχήμα 52. Χρονική εξάπλωση ενός επιδημικού ξεσπάσματος**

### 6.1.2 Το PSIDR μοντέλο.

Σε αυτό το τμήμα, παρουσιάζεται πώς οι προαναφερθείσες πτυχές ενσωματώνονται στο πρότυπο. Σύμφωνα με το προοδευτικό πρότυπο ευπαθούς-μολυσμένου-ανιχνευμένου-αφαιρεμένου, τα επιδημικά γεγονότα στα δίκτυα υπολογιστών μπορούν να διαιρεθούν σε δύο χρονολογικές περιόδους (όπως παρουσιάζονται και στο προηγούμενο σχήμα):

- Η περίοδος προ της αντίδρασης. Στην αρχή, ο πρώτος ιός μολύνει μια μηχανή στο δίκτυο. Για τις επόμενες μερικές ημέρες (ή ώρες), ο ιός διαδίδεται ελεύθερα στο δίκτυο χωρίς την παρατήρηση του από τους περισσότερους χρήστες. Με βάση τους όρους του **PSIDR**, αυτό διαμορφώνεται ως ένα θετικό ποσοστό γέννησης β και καμία θεραπεία. Οι ευπαθείς κόμβοι επομένως μολύνονται με πιθανότητα β εάν έρθουν σε επαφή (επικοινωνήσουν) με έναν μολυσμένο κόμβο.

- Η περίοδος αντίδρασης. Μετά από κάποιο χρόνο, ο ιός ανιχνεύεται σε μερικούς υπολογιστές και λαμβάνονται άμεσες ενέργειες για την αποτροπή περεταίρω εξάπλωσης αλλά και για την θεραπεία των ήδη μολυσμένων κόμβων. Έτσι εξάγεται η υπογραφή και περιλαμβάνεται σε ένα ορισμένο ποσοστό των ΛΠΥ των υπολογιστών του δίκτυου. Μηχανές που δεν ήταν μολυσμένες γίνονται αυτόματα άνοσες στον ιό, ενώ αυτές που έχουν ήδη μολυνθεί ανιχνεύονται σε ένα ορισμένο ποσοστό (ανάλογα με πόσο συχνά γίνεται η ενημέρωση του ΛΠΥ). Αυτές οι μηχανές είναι έπειτα απομονωμένες, θεραπευμένες και ανοσοποιημένες ενάντια σε περαιτέρω μόλυνση. Πάλι, στο πρότυπο **PSIDR** αυτή η περίοδος διαμορφώνεται

με το ίδιο ποσοστό γέννησης όπως πριν, αλλά αυτή τη φορά οι ευπαθείς κόμβοι γίνονται ανοσοποιημένοι σε ένα ποσοστό μ, και οι μολυσματικοί κόμβοι ανιχνεύονται σε ένα ποσοστό μ και θεραπεύονται έπειτα με ένα ποσοστό δ.

Το ποσοστό μ αντιπροσωπεύει την ταχύτητα της διανομής της υπογραφής του ΛΠΥ.

Η μόνη λεπτομέρεια που αφήνεται είναι ο χρόνος όταν το σύστημα μεταβαίνει από την προ αντίδρασης περίοδο στην περίοδο αντίδρασης. Στο πρότυπο **PSIDR,** αυτό το χρονικό διάστημα αναπαρίσταται από μια παράμετρο π, η οποία μπορεί να πάρει μια αυθαίρετη τιμή. Αυτή η παράμετρος αντιπροσωπεύει το χρονικό διάστημα που μεσολαβεί από την χρονική στιγμή της πρώτης μόλυνσης έως την χρονική στιγμή έκδοσης της υπογραφής.

#### 6.1.2.1 Συνεισφορές του προτύπου PSIDR

Όσον αφορά τα πρότυπα **SIS, SIR** και **SEIR,** το πρότυπο **PSIDR** περιγράφεται καλύτερα ως μια ακολουθία καταστάσεων με ρυθμούς μεταβάσεων μεταξύ αυτών. Η ακόλουθη περιγραφή δίνει έμφαση σε διάφορους παράγοντες όπου λαμβάνονται υπόψη κατά τη μοντελοποίηση της διάδοσης ιών σε δίκτυα υπολογιστών. Αυτές είναι οι κύριες συνεισφορές του προτύπου **PSIDR** στα γενικά επιδημιολογικά πρότυπα.

- "Μεταβλητότητα του ρυθμού θεραπείας. Αρχικά, κανένας μολυσμένος υπολογιστής δεν θεραπεύεται. Μόνο μετά από μια ορισμένη χρονική περίοδο όπου τα στιγμιότυπα του ιού αρχίζουν να προσδιορίζονται και να απομακρύνονται από τους μολυσμένους οικοδεσπότες τους. Στο **PSIDR** πρότυπο, το επιδημικό γεγονός διαιρείται κατ' αυτό τον τρόπο σε δύο χρονολογικές περιόδους αντίστοιχα αποκαλούμενες ως προ της αντίδρασης και περίοδος αντίδρασης. Στην πρώτη περίοδο, οι ιοί διαδίδονται με ένα ποσοστό β και δεν απομακρύνονται **(**οι ρυθμοί ανίχνευσης **(**μ**)** και θεραπείας **(**δ**)** είναι μηδενικοί**)**. Κατόπιν, σε κάποιο χρόνο που καθορίζεται από την παράμετρο π, το σύστημα μεταπηδά στη δεύτερη περίοδο όπου οι μολυσμένοι οικοδεσπότες μπορούν τώρα να θεραπεύονται **(**τα ποσοστά ανίχνευσης και θεραπείας παίρνουν αντίστοιχα σταθερές μη μηδενικές τιμές**)**. Τα προηγούμενα επιδημικά πρότυπα δεν υπολόγιζαν αυτό το είδος μεταβλητότητας του ποσοστού θεραπείας.
- Ευθείες μεταβάσεις από το **S** στο **R.** Από τη στιγμή που η υπογραφή των ιών είναι διαθέσιμη, οι ευπαθείς υπολογιστές μπορούν να γίνουν άνοσοι χωρίς να μεταβούν στη μολυσμένη κατάσταση εάν το λογισμικό ΛΠΥ στους ευπαθείς οικοδεσπότες ενημερώνεται πριν προλάβει να τους μολύνει ο ιος. Στο πρότυπο **PSIDR,** αυτό αντιπροσωπεύεται από τις πιθανές ευθείες μεταβάσεις από το **S** στο **R** κατά τη διάρκεια της περιόδου αντίδρασης. Συγκεκριμένα, σε αυτήν την περίοδο,

ένας ευπαθής οικοδεσπότης γίνεται αφαιρούμενος σε ένα ποσοστό μ. Οι άμεσες μεταβάσεις όπως αυτή δεν περιλήφθηκαν στα παλαιότερα πρότυπα.

- Κατάσταση ανίχνευσης. Σε αυτή την περίοδο, μολυσμένοι (αλλά ακόμα λειτουργικοί) υπολογιστές ανιχνεύονται μόνο όταν ενημερώνεται το λογισμικό με την νέα υπογραφή. Μόλις ανιχνευθεί, ο χρήστης (ή τεχνικός) το απομονώνει από το δίκτυο και φροντίζει για την αποκατάστασή του. Στο πρότυπο **PSIDR**, αυτό μοντελοποιείται με την παρεμβολή μίας νέας κατάστασης (αποκαλούμενου **"D"** για **detected)** μεταξύ των I και **R** καταστάσεων. Στην περίοδο αντίδρασης, οι μολυσμένοι υπολογιστές γίνονται ανιχνευμένοι σε ένα ποσοστό μ (δεδομένου ότι εξαρτάται από την ενημέρωση του ΛΠΥ), και αφαιρούμενος έπειτα σε ένα ποσοστό δ. Η κατάσταση **D** αντιπροσωπεύει την περίοδο όπου ο μολυσμένος υπολογιστής αποκαθίσταται από έναν τεχνικό (ή με άλλα μέσα). Ο συνυπολογισμός αυτού του σταδίου είναι ένα κατάλληλο χαρακτηριστικό του προτύπου **PSIDR**, το οποίο δεν αναφέρεται σε άλλα πρότυπα.

Σημαντική είναι η επισήμανση ότι τα παραδοσιακά μοντέλα **SIS**, **SIR** και πρότυπα **SEIR** δεν λαμβάνουν υπόψη τους τις τρεις προαναφερθείσες πτυχές στον απολογισμό. Στο πρότυπο **PSIDR**, το επιδημικό γεγονός διαμορφώνεται έτσι σαν ένα **S->I** σύστημα που γίνεται, μετά από χρόνο **t =** π, ένα **S->I->D->R** σύστημα με πιθανές μεταβάσεις του τύπου **S-> R**. Ο λόγος για τον οποίο το πρότυπο καλείται προοδευτικό είναι τώρα σαφής: είναι λόγω της προόδου (ή της αλλαγής) στη δυναμική του συστήματος. Το πρότυπο παρουσιάζεται αναλυτικά στο επόμενο τμήμα.

### 6.1.2.2 Ορισμός του πρότυπου PSIDR

Σε αυτό το πρότυπο, υποθέτουμε ότι ο αριθμός των υπολογιστών στο δίκτυο **(N)** είναι σταθερός.

**Η προ αντίδρασης περίοδος**

Για **t <** π, ο ακόλουθος περιορισμός πρέπει να ικανοποιείται:

**S(t) + I(t) = N (1)**

και οι διαφορικές εξισώσεις που περιγράφουν το σύστημα δίνονται από:

$$\frac{dS}{dt} = -\beta SI \quad (2)$$

$$\frac{dI}{dt} = \beta SI \quad (3)$$

Στην πραγματικότητα είναι δυνατό να συναχθεί η δεύτερη εξίσωση από την πρώτη και αντίστροφα.

**Η περίοδος αντίδρασης**

Την χρονική στιγμή **t** ≥ π ισχύει ο ακόλουθος περιορισμός.

**S(t) + I(t) + D(t) + R(t) = N (4)**

Δεδομένου ότι υπάρχουν περισσότερες από δύο καταστάσεις, μπορούμε να αναπαραστήσουμε την εξέλιξη του δικτυού μέσα από ένα σύστημα συνδεμένων διαφορικών εξισώσεων:

$\frac{dS}{dt}$ **= −βSI − μS (5)**

$\frac{dI}{dt}$ **= βSI − μI (6)**

$\frac{dD}{dt}$ **= μI − δD (7)**

$\frac{dR}{dt}$ **= δD + μS (8)**

Μπορούμε να αποδείξουμε ότι **dS/dt + dI/dt + dD/dt + dR/dt = 0** που συνεπάγεται ότι το σύστημα ικανοποιεί την εξίσωση **4**

Τέλος οι αρχικοί περιορισμοί του συστήματος είναι **S(0) > 0, I(0) > 0, D(0) = 0,** και **R(0) = 0.**

### 6.1.2.3 Εκτίμηση κόστους

Ένα πλεονέκτημα του τρέχοντος προτύπου είναι ότι προτείνει έναν φυσικό και αποδοτικό τρόπο εκτίμησης διαφόρων ειδών κόστους σχετιζόμενων με το επιδημικό γεγονός.

**1.** Κόστος αποκατάστασης. Το κόστος που σχετίζεται με την αποκατάσταση των υπολογιστών συσχετίζεται με το χρονικό διάστημα που χρειάζεται για να καθαριστούν οι υπολογιστές καθώς και με το πλήθος αυτόν **(**δηλ. το πλήθος των μολυσμένων υπολογιστών που έχουν ανιχνευθεί**).** Επομένως, αυτό το κόστος μετράται ως ποσό του αριθμού των ανιχνευμένων υπολογιστών για κάθε χρονική στιγμή **(**η περιοχή κάτω από την καμπύλη υπολογίζεται ως ολοκλήρωμα **Riemann):**

Κόστος αποκατάστασης **=** $\int_{p}^{T} D(t)dt \approx \sum_{p}^{T} D(t)$ **(9)**

**2.** Κόστος διανομής**.** Το κόστος της διανομής δίνεται από την περιοχή κάτω από την καμπύλη του αριθμού μολυσμένων κόμβων κάθε χρονική στιγμή**.** Αντιπροσωπεύει το ποσό του δικτύου που επηρεάστηκε σε όλο το ξέσπασμα**.** Είναι ένα σύνθετο μέτρο του πόσοι υπολογιστές είναι μολυσμένοι και για πόσο καιρό είναι μολυσμένοι**.** Αποτυπώνει έτσι πολλές πληροφορίες για το κόστος του ξεσπάσματος**.** Ομοίως με το κόστος αποκατάστασης**,** το κόστος διανομής δίνεται από**:**

κόστος διανομής**=** $\int_{p}^{T} I(t)dt \approx \sum_{p}^{T} I(t)$ **(10)**

**3.**Μέγιστος αριθμός μολυσμένων κόμβων**.** Αυτό είναι επίσης μια ενδιαφέρουσα μεταβλητή δεδομένου ότι δίνει μια ιδέα για τη χειρότερη κατάσταση του συστήματος**.** Πράγματι**,** η διάσπαση μπορεί να παραγάγει παρόμοιες τιμές για τα πολύ διαφορετικά επιδημικά γεγονότα**,** όπου ο μέγιστος αριθμός μολυσμένων κόμβων μπορεί να διαφοροποιηθεί περισσότερο μεταξύ των τύπων των γεγονότων**.**

Πλήθος μολυσμένων κόμβων**=** $\max(I(t))\Big|_{t=t_0}^{t=T}$ **(11)**

**4.** Χρονική διάρκεια μέχρι την ανοσοποίηση**.** Τα πραγματικά δίκτυα είναι σπάνια εντελώς ανοσοποιημένα αλλά μπορούν να γίνουν συνήθως κυρίως άνοσοι σε ένα σκουλήκι**.** Κατά συνέπεια**,** ο χρόνος που μεσολαβεί για να ανοσοποιηθεί το **95%** των υπολογιστών του δικτύου υπολογίζεται αντί αυτού**:** αυτό το επίπεδο **(95%)** επιλέγεται κάπως αυθαίρετα τα επίπεδα **90%** ή **99%** θα μπορούσαν επίσης να έχουν επιλεχτεί**.** Μπορεί να είναι συμφέρων να ανοσοποιηθεί το δίκτυο όσο το δυνατόν γρηγορότερα και να αποτρέπει οποιοδήποτε μεγάλο ξέσπασμα**.** Ο χρόνος που χρειάζεται για την πλήρη ανοσοποίηση μετράται συναρτήσει των παραμέτρων διαμόρφωσης**.**

Εκτός από τη μέτρηση των παραδοσιακών ποσοτήτων**,** όπως είναι ο αριθμός των ευπαθών ή**/**και το πλήθος των μολυσμένων κόμβων σε κάθε χρονική στιγμή**,** αυτά τα τέσσερα κόστη μπορούν να μετρηθούν και να χρησιμοποιηθούν για την πρόταση καλύτερων στρατηγικών αντίδρασης**.** Σημειώστε ότι πρότυπα **SIS**, **SIR** ή **SEIR** δεν παρέχουν οποιαδήποτε ένδειξη σχετικά με τον καθορισμό του κόστους**.**

### 6.1.2.4 Λεπτομέρειες του προτύπου

Σε αυτό το τμήμα**,** οι διάφορες πτυχές του προτύπου εξετάζονται λεπτομερέστερα για να γίνει εμφανής η σύνδεσή του με τα πραγματικά επιδημικά γεγονότα**.**

Το ποσοστό β θεωρείται ότι είναι σταθερό και εξαρτάται από πόσο γρήγορα ο ιός μπορεί να διαδίδεται σε νέους οικοδεσπότες**.** Παραδείγματος χάριν**,** ο ιός **Code Red (CRv2)** μπορούσε να ελέγχει εκατοντάδες διευθύνσεις **IP** ανά δευτερόλεπτο **[91]**. Αντίθετα**,** τα σκουλήκια ηλεκτρονικού ταχυδρομείου θεωρούνται πολύ πιο αργά**.**

Η παράμετρος π αντιπροσωπεύει το χρόνο που λαμβάνεται για να παραχθεί μια υπογραφή. Προφανώς, στο τρέχον πλαίσιο, αυτή η παράμετρος εξαρτάται από πόσο γρήγορα πραγματοποιείται η δημιουργία αντίμετρων για την προερχόμενη από ιό επίθεση. Εντούτοις, αυτή είναι μια παράμετρος της οποίας η αξία θα μειωνόταν πιθανώς με την χρήση αυτοματοποιημένων συστημάτων για την ασφάλεια του υπολογιστή. Έχει νόημα επομένως η προσομοίωση του ξεσπάσματος για τις διαφορετικές τιμές του π προκειμένου να υπολογιστούν οι σχετικές αξίες των αυτόνομων συστημάτων ασφάλειας.

Εάν **t <** π, το ποσοστό μ **= 0**, όταν **t** ≥ π, το μ παίρνει μια συγκεκριμένη θετική τιμή όπου μ **<<** β. Αυτό συμβαίνει επειδή συχνά η ενημέρωση των ΛΠΥ γίνεται μόνο μια φορά ή δύο φορές την ημέρα, ενώ το σκουλήκι διαδίδεται πολύ γρηγορότερα **(**εκατοντάδες διευθύνσεις ανά δευτερόλεπτο παραδείγματος χάριν**).** Το ποσοστό ανίχνευσης επηρεάζεται επίσης από το γεγονός ότι δεν είναι όλοι οι υπολογιστές σε λειτουργία κάθε ημέρα. Στο παρόν πλαίσιο, θα μπορούσαμε να αξιολογήσουμε την επίδραση μιας δυναμικής πολιτικής όπου η ενημέρωση των ΛΠΥ θα ήταν συχνότερη, ή πιο σπάνια όπου η ενημέρωση θα εκτελείται μία φορά την εβδομάδα παραδείγματος χάριν.

Από την χρονική στιγμή της διανομής της υπογραφής, το ποσοστό θεραπείας εξαρτάται κυρίως από τον αριθμό των τεχνικών του προσωπικού που είναι διαθέσιμοι για να εξετάσουν την επιδημία, τον χρόνο που χρειάζεται για να θεραπεύσει έναν υπολογιστή, καθώς και το χρονικό διάστημα που κάθε μέλος του προσωπικού μπορεί να ξοδέψει στο πρόβλημα. Επίσης, επειδή δεν είναι πάντα αποτελεσματικές οι θεραπείες, μερικοί υπολογιστές δεν μπορούν να θεραπευτούν την πρώτη φορά. Στη σημερινή δικτυακή πραγματικότητα, οι περισσότερες θεραπείες εκτελούνται χειροκίνητα, το οποίο σημαίνει ότι το ποσοστό θεραπείας θα είναι πολύ χαμηλότερο από το ποσοστό γέννησης. Εδώ πάλι, η επίδραση από τα αυτόνομα συστήματα ασφάλειας μπορεί να αξιολογηθεί, όπου το ποσοστό θεραπείας δ πιθανός να αυξάνεται.

#### 6.1.2.5 Περιορισμοί του μοντέλου

Το πρότυπο **PSIDR** επεκτείνει τα προηγούμενα πρότυπα για να προσφέρει έναν καλύτερο απολογισμό των τεχνολογικών επιδημιών. Εντούτοις, εδώ παρουσιάζονται μερικές πτυχές που δεν υπολογίζει.

Ø Μεταβλητότητα του ρυθμού θεραπείας δ. Στην πραγματικότητα, όσο περισσότεροι μολυσμένοι υπολογιστές υπάρχουν τόσο περισσότεροι άνθρωποι ανατίθενται για την καταπολέμησή του. Δηλαδή δ∞**I** όπου είναι πιθανό να επηρεάσει το χρόνο που απαιτείται για να την απομάκρυνση του ιού. Η ακριβής

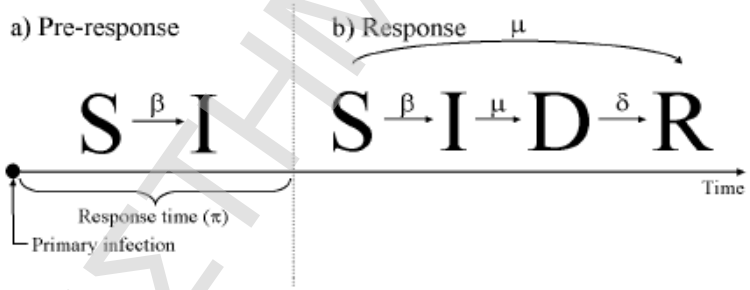
σχέση μεταξύ του I και δ μπορεί να είναι γραμμική ή μη γραμμική. Το πρότυπο **PSIDR** μπορεί εύκολα να επεκταθεί με ένα μεταβλητό ρυθμό θεραπείας.

**Ø** Μεταβλητότητα του ρυθμού γεννήσεων β. Στην περίπτωση των αυτόματα μεταδιδόμενων σκουληκιών, ο ρυθμός διάδοσης καθορίζεται εν μέρη από το πόσο γρήγορα το σκουλήκι θα εξετάσει τη νέα διεύθυνση **IP**. Παραδείγματος χάριν, στην περίπτωση του **CodeRed**, το σκουλήκι ήταν προγραμματισμένο να σταματήσει να ψάχνει νέους οικοδεσπότες τα μεσάνυχτα της **20**ης Ιουλίου. Άλλα σκουλήκια είχαν επίσης αυτό το χαρακτηριστικό προκαλώντας έτσι μεταβλητότητα του ρυθμού γεννήσεων.

Άλλοι περιοδικοί παράγοντες. Μερικά σκουλήκια επιφέρουν ζημιές περιοδικά. Για παράδειγμα, το σκουλήκι **Klez.e** προκαλούσε καταστροφές μόνο σε μολυσμένους υπολογιστές την **6**η μέρα κάθε μονού μήνα **(**Ιανουάριος, Μάρτιος,κτλ.**)[53].**

## 6.2 Προσομοίωση

Αυτό το κεφάλαιο εκθέτει τα διάφορα πειράματα προσομοίωσης που γίνονται με το **PSIDR** πρότυπο. Ας ανακεφαλαιώσουμε την αλυσίδα των γεγονότων που περιλαμβάνονται στο πρότυπο **PSIDR,** όπως αυτά παρουσιάζονται στο Σχήμα **53:**




**Σχήμα 53. Η χρονική εξέλιξη του PSIDR μοντέλου**

**1.** Περίοδος προ αντίδρασης **(S -> I).**Στην αρχή, ένα σκουλήκι μολύνει μια μηχανή στο δίκτυο. Για τις επόμενες μερικές ημέρες **(**ή ώρες**),** το σκουλήκι διαδίδεται ελεύθερα στο δίκτυο χωρίς την παρατήρησή του από τους περισσότερους χρήστες.

**2.** Περίοδος αντίδρασης **(S → I → D → R, S → R).** Μετά από κάποιο χρόνο, το σκουλήκι ανιχνεύεται σε μερικούς υπολογιστές και λαμβάνεται άμεση δράση για την αποτροπή της περαιτέρω εξάπλωσης καθώς και για την θεραπεία των μολυσμένων υπολογιστών. Κατόπιν δημιουργείτε μια υπογραφή σκουληκιών και περιλαμβάνεται σε ένα ορισμένο ποσοστό του πλήθους των ΛΠΥ στο δίκτυο. Υπολογιστές που δεν ήταν μολυσμένοι γίνονται αυτόματα άνοσοι στο σκουλήκι, ενώ οι μολυσμένοι υπολογιστές ανιχνεύονται σε ένα ορισμένο ποσοστό **(**ανάλογα με το πόσο συχνά

γίνετε η ενημέρωση του ΛΠΥ**).** Αυτές οι μηχανές έπειτα απομονώνονται**,** καθαρίζονται και ανοσοποιούνται ενάντια σε περαιτέρω μόλυνση**.**

Το **PSIDR** πρότυπο περιέχει πολλές ελεύθερες παραμέτρους**,** οδηγώντας έτσι σε πολλές διαφορετικές παραμετροποιήσεις που μπορούν να δοκιμαστούν προκειμένου να επιτευχθεί μια επαρκής κατανόηση του προτύπου**.** Εδώ μόνο ένα υποσύνολο των τιμών εξερευνάται για να παρουσιαστεί η βασική δυναμική του προτύπου**.**

Το πρώτο σύνολο πειραμάτων προορίζεται να δώσει μια γενική επισκόπηση του προτύπου**.** Ο χρόνος που μεσολαβεί μέχρι την αρχική ανίχνευση **(**π**)** τίθεται σε διαφορετικές τιμές για την παρουσίαση της επίδρασης αυτού του παράγοντα**.**

Στο δεύτερο μέρος**,** τιμές για διαφορετικές παραμέτρους όπως ο χρόνος που μεσολαβεί μέχρι την αρχική ανίχνευση **(**π**),** ο ρυθμός ανίχνευσης και ανοσοποίησης **(**μ**),** και ρυθμός θεραπείας **(**δ**) -** ποικίλουν μεταξύ των προσομοιώσεων**.** Η έμφαση δίνεται στην αλληλεπιδράσεων της ανάμειξης του π και μ**,** π και δ**,** και μ και δ παραμέτρων**.** Οι τρέχων στρατηγικές για να την αντιμετώπιση των ιών μοντελοποιούνται με αυτές τις παραμέτρους**,** και έναν από τους κύριους στόχους να είναι η αξιολόγηση της αποδοτικότητας αυτών των μεθόδων**.**

Ένας νέος τρόπος να αντιμετωπιστούν οι επιδημίες είναι να επιβραδυνθεί η διάδοση των ιών **[132].** Στο παρόν πλαίσιο, αυτή η στρατηγική μπορεί να εξεταστεί με τη μίμηση πιο αργών ποσοστών γέννησης **(**β**).** Ένα τρίτο σύνολο πειραμάτων ερευνά αυτό το ζήτημα**.** Μία κατάλληλη μελέτη αυτής της επίδρασης πρέπει να περιλαμβάνει τις προσομοιώσεις των αλληλεπιδράσεων μεταξύ του β και των παραμέτρων π δ**,** και μ**.**

Τέλος**,** συγκρίνεται το **SIR** πρότυπο με το **PSIDR** πρότυπο όταν π **= 0** με στόχο να παρουσιαστεί η επιρροή των άμεσων μεταβάσεων από το **S** στο **R (**ένα από κύρια χαρακτηριστικά γνωρίσματα του **PSIDR** προτύπου**).** Αντίθετα από το **SIS** πρότυπο**,** η προσοχή δεν εστιάζεται ρητά στην ύπαρξη ενός πιθανού επιδημιολογικού κατώτατου ορίου**.**

### 6.2.1 Μεθοδολογία

Δέκα διαφορετικά δίκτυα ελεύθερης κλίμακας **(SF) 6250** κόμβων και ενός ομοιογενούς **(HM)** δικτύου χρησιμοποιούνται στις προσομοιώσεις**.** Η κατάσταση όλων των κόμβων ενημερώνεται σε κάθε χρονική στιγμή **(**παράλληλη αναπροσαρμογή**)** για τουλάχιστον **150** επαναλήψεις**.** Τα χρονικά βήματα διαιρούνται σε **10** μικρά χρονικά κομμάτια προκειμένου να προσεγγιστεί η συνοχή και ο μη συγχρονισμός μέσα το σύστημα**.** Όπως και στο **[100],** οι προσομοιώσεις επαναλαμβάνονται τουλάχιστον **100** φορές **(**μέχρι και **1000** φορές**)** στην περίπτωση

των δικτύων ελεύθερης κλίμακας **SF.** Λόγω της ευρωστίας τους στο θόρυβο**,** μόνο **50** επαναλήψεις γίνεται για τα ομοιογενή δίκτυα**.**

Σε κάθε χρονική στιγμή **,** το πλήθος των μολυσμένων**,** ανιχνευμένων και αφαιρεμένων υπολογιστών μετριέται αντίστοιχα για να παρέχει τα ακατέργαστα στοιχεία**.** Τα τέσσερα διαφορετικά κόστη που αναφέραμε προηγουμένως υπολογίζονται από αυτά τα δεδομένα**.**

#### 6.2.1.1 Κανόνας ενημέρωσης

Η ενημέρωση εκτελείται σύμφωνα με το πρότυπο **PSIDR:**

**1.** Στην προ αντίδρασης περίοδο **(t <** π**),** ένας κόμβος είναι μολυσμένος σε ένα ποσοστό β εάν είναι συνδεμένος με τουλάχιστον έναν μολυσμένο κόμβο**.**

**2.** Στην περίοδο αντίδρασης **(t ≥** π**),** οι ευπαθείς κόμβοι γίνονται ή μολυσμένοι σε ένα ποσοστό β ή αφαιρεμένοι σε ένα ποσοστό μ. Συγχρόνως**,** οι ήδη μολυσμένοι κόμβοι ανιχνεύονται σε ένα ποσοστό μ και οι ανιχνευμένοι κόμβοι είναι αφαιρούνται σε ένα ποσοστό δ**.**

#### 6.2.1.2 Εκτίμηση των παραμέτρων

Αντί του υπολογισμού των συγκεκριμένων τιμών για κάθε μια από τις παραμέτρους β δ**,** μ και π**,**

οι τιμές τους προσεγγίζονται με τον ακόλουθο τρόπο**.**

• Ρυθμός εξάπλωσης**.** Δεδομένου ότι τα σκουλήκια διαδίδονται αρκετά γρηγορότερα από ότι ανιχνεύονται ή αφαιρούνται**,** η τιμή του β πρέπει να είναι υψηλότερη από την ανίχνευση **(**μ**)** και του ρυθμού θεραπείας **(**δ**).**

• Χρόνος αντίδρασης**.** Ο αριθμός των χρονικών βημάτων πριν από μια αρχική ανίχνευση **(**π**),** δεν περιορίζεται από οποιαδήποτε από τις άλλες παραμέτρους**.** Κατά συνέπεια**,** τιμές στο διάστημα **0** ≤ π ≤ **20** και επίσης π**=** **40** χρησιμοποιούνται για την παροχή μιας γενικής εκτίμησης της επίδρασης αυτής της παραμέτρου**.**

• Ρυθμός ανίχνευσης**.** Η τιμή του ρυθμού ανίχνευσης είναι μεταξύ του ρυθμού γέννησης και θεραπείας εξαιτίας του γεγονότος ότι είναι μερικώς αυτοματοποιημένος **(**το ΛΠΥ η ενημέρωση γίνεται αυτόματα τουλάχιστον μια φορά καθημερινά από το λογισμικό**).**

• Ρυθμός θεραπείας**.** Επειδή η θεραπεία απαιτεί τη χειρωνακτική εργασία**,** είναι μάλλον αργή**:** η θεραπεία μερικών ντουζίνων υπολογιστών μπορεί να διαρκέσει και ημέρες**.** Επομένως**,** ο ρυθμός θεραπείας τίθεται σε χαμηλές τιμές**.** Στις ακόλουθες προσομοιώσεις**,** οι διάφορες τιμές για το δ κυμαίνονται μεταξύ δ **= 0.03** και δ **=**

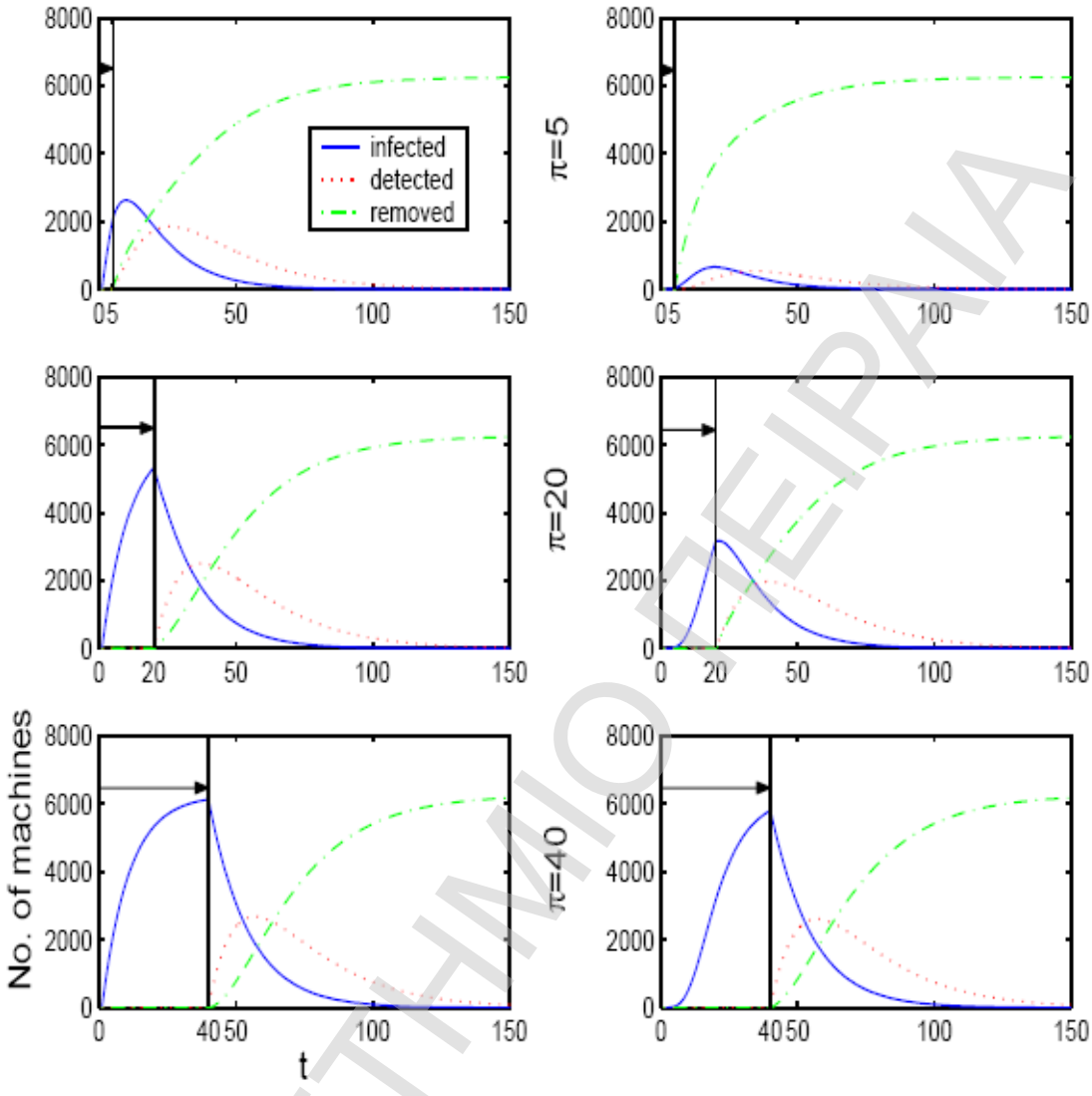
**0.10.** Το πραγματικό ποσοστό θεραπείας **(**δηλ**.** στα πραγματικά δίκτυα**)** είναι πιθανώς κάπου κοντά στο χαμηλότερο όριο δ **= 0.03.**

### 6.2.2 Αποτελέσματα

#### 6.2.2.1 Γενική επισκόπηση του μοντέλου

Ο αριθμός μολυσμένων υπολογιστών αυξάνει σταθερά**,** και παρουσιάζει μια αιχμή κοντά στο **t =** π**,** ενώ κατόπιν αργά μειώνεται στο μηδέν**.** Αντίθετα**,** ο αριθμός ανιχνευμένων κόμβων παραμένει μηδέν μέχρι την περίοδο αντίδρασης**,** κατόπιν αυξάνεται έως ότου φθάνει σε μια ορισμένη αιχμή**,** που ακολουθεί αργή καθοδική πορεία στο μηδέν**.** Τέλος**,** ο αριθμός των ανοσοποιημένων θεραπευμένων**/**άνοσων κόμβων αυξάνεται από την χρονική στιγμή **t =** π έως ότου κορεστεί όλο το δίκτυο**.**

Ο αριθμός των μολυσμένων κόμβων στο **PSIDR** πρότυπο ακολουθεί μια παρόμοια πορεία σε αντίθεση με το **SIR** πρότυπο **(**βλ**. [92])**. Δηλαδή υπάρχει μια αιχμηρή αύξηση που ακολουθείται από το μια αργή μείωση**,** που τελειώνει τελικά στο μηδέν**.** Η εκθετική αύξηση στην επικράτηση **(**Σχήμα **54)** έχει παρατηρηθεί στην περίπτωση του ξεσπάσματος του σκουληκιών **Code Red[26]** τον Ιούλιο του **2001.**




**Σχήμα 54. Επισκόπηση του PSIDR μοντέλου**

Τα ομογενή δίκτυα εμφανίζονται στα αριστερά και τα **SF** δίκτυα στα δεξια. Από επάνω προς τα κάτω, π **= 5 , 20, 40 (**β **= 0 .1 ,** δ **= 0.05 ,** μ **= 0.07).** Αρχικά, ένας κόμβος είναι μολυσμένος, και ο ιός διαδίδεται ελεύθερα στο δίκτυο. Την χρονική στιγμή **t =** π, ο αριθμός των ανιχνευμένων και αφαιρούμενων υπολογιστών αρχίζει να αυξάνεται καθώς αρχίζει να λειτουργεί το ΛΠΥ. Συγχρόνως, ο αριθμός των μολυσμένων κόμβων μειώνεται. Συνολικά, τα **SF** δίκτυα επηρεάζονται λιγότερο από τον ιό σε σχέση με τα ομογενή δίκτυα Α.Μ. για μικρό π.

Ένα άλλο ενδιαφέρον χαρακτηριστικό γνώρισμα είναι η οξύτητα της αιχμής στο μέγιστο αριθμό των μολυσμένων κόμβων. Πράγματι, η αιχμή εμφανίζεται ομαλότερη όταν λίγοι κόμβοι είναι μολυσμένοι, και αιχμηρότερη όταν μολύνονται σχεδόν όλοι οι κόμβοι. Η παρουσία αυτής της αιχμής είναι σημαντική καθώς στις πραγματικές επιδημίες υπολογιστών, μια τέτοια ισχυρή αιχμή δεν παρατηρείται **[25].** Επομένως, θα μπορούσε να είναι ένα τεχνούργημα που δημιουργήθηκε από

το πρότυπο, το οποίο θα πρότεινε ότι το **PSIDR** πρότυπο δεν είναι κατάλληλο για να συλλαμβάνει πραγματικά ξεσπάσματα. Αυτή η αιχμή μπορεί να οφείλεται σε δύο διαφορετικούς παράγοντες:

**1.** Ο αριθμός των πρόσφατα μολυσμένων κόμβων είναι μικρός όταν είναι οι περισσότεροι κόμβοι είναι ήδη μολυσμένοι. Κατά συνέπεια, στην πράξη, το ποσοστό γέννησης είναι πραγματικά μικρό σε αυτές τις περιπτώσεις. Επίσης, εάν το ίδιο το ποσοστό γέννησης είναι μικρό έναντι των άλλων ποσοστών, αυτό το είδος αιχμής μπορεί να εμφανιστεί ακόμα και όταν ο αριθμός μολυσμένων κόμβων είναι χαμηλός.

**2.** Ο αριθμός των κόμβων που μεταβαίνουν στην φάση της θεραπείας **(**διέλευση από το **I** στο **D)** ακολουθεί δυωνυμικό νόμο με πιθανότητα μ. Επομένως ο αριθμός των μηχανών που θεραπεύονται σε ένα ενιαίο χρονικό βήμα αναμένονται να είναι **D(t+ 1) -D(t) = I**μ. Καθώς ο αριθμός των μολυσμένων κόμβων πλησιάζει το μέγεθος του δικτύου, το **I** φθάνει τη μέγιστη τιμή του, ως εκ τούτου ο αριθμός των πρόσφατα ανιχνευμένων κόμβων σε ένα ενιαίο χρονικό βήμα είναι το μέγιστο αυτή τη στιγμή.

Στις προσομοιώσεις, ο συνδυασμός αυτών των δύο παραγόντων πιθανώς να παράγει αυτή την αιχμή. Αυτή η επίδραση αναμένεται σε οποιαδήποτε πεπερασμένα δίκτυα, αλλά δεν πρέπει να είναι παρόν σε ένα άπειρο δίκτυο. Σε ένα πραγματικό πεπερασμένο δίκτυο **(**όπως το Διαδίκτυο**)**, συχνά παρατηρείται ότι τα σκουλήκια έχουν μια χαμηλή επικράτηση **[100]**. Επιπλέον, τυπικά τα σκουλήκια διαδίδονται πολύ γρηγορότερα από ότι θεραπεύονται. Επομένως, η απουσία της αιχμηρής ακμής μπορεί να εξηγηθεί από τον πρώτο προαναφερθέντα παράγοντα **(**μικρός αριθμός μολυσμένων ακμών και υψηλότερο ποσοστό γέννησης από τα ποσοστά ανίχνευσης */*θεραπείας**)**.

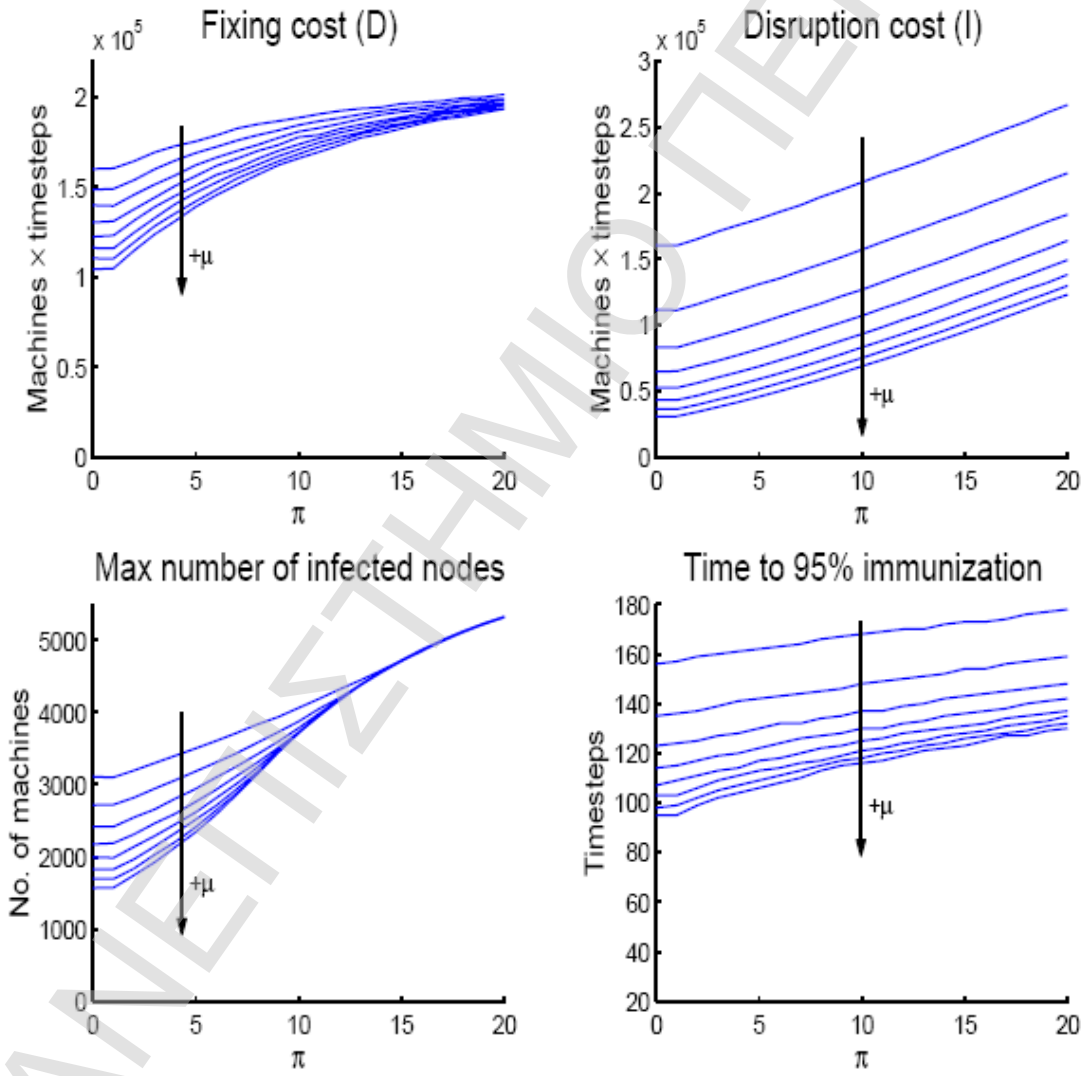
Τέλος, για ένα σχετικά χαμηλό π, ο αριθμός μολυσμένων υπολογιστών είναι μικρότερος στα **SF** δίκτυα απ' ό,τι στα ομογενή δίκτυα.. Πράγματι, παίρνει περισσότερο χρόνο στο σκουλήκι για να μολύνει ένα **SF** δίκτυο επειδή, σε αυτό το δίκτυο, το σκουλήκι δεν μπορεί να φθάσει σε όλους τους γειτονικούς κόμβος από οποιοδήποτε μολυσμένο κόμβο. Εντούτοις, όταν ο χρόνος που μεσολαβεί μέχρι την αρχική ανίχνευση είναι μεγάλος, το σκουλήκι έχει αρκετό χρόνο να διαδοθεί σε όλο το δίκτυο, και κατόπιν να εξασθενησεί, στην επικράτηση ακολουθεί μια παρόμοια πορεία βημάτων για τα ομογενή και τα **SF** δίκτυα. Αυτό οφείλεται στο γεγονός ότι οι πιθανότητες της ανίχνευσης και της θεραπείας είναι ανεξάρτητες από την τοπολογία.

Γενικά, το πρότυπο **PSIDR** φαίνεται να προσαρμόζεται στη διαισθητική εικόνα του πώς τα πραγματικά ξεσπάσματα εμφανίζονται στα τεχνολογικά δίκτυα. Επιπλέον, είναι συμβατό με τα υπάρχοντα στοιχεία για την επικράτηση σκουληκιών.

#### 6.2.2.2 Αποτελέσματα του έλεγχου των παραμέτρων (π, μ, δ) στα κόστη

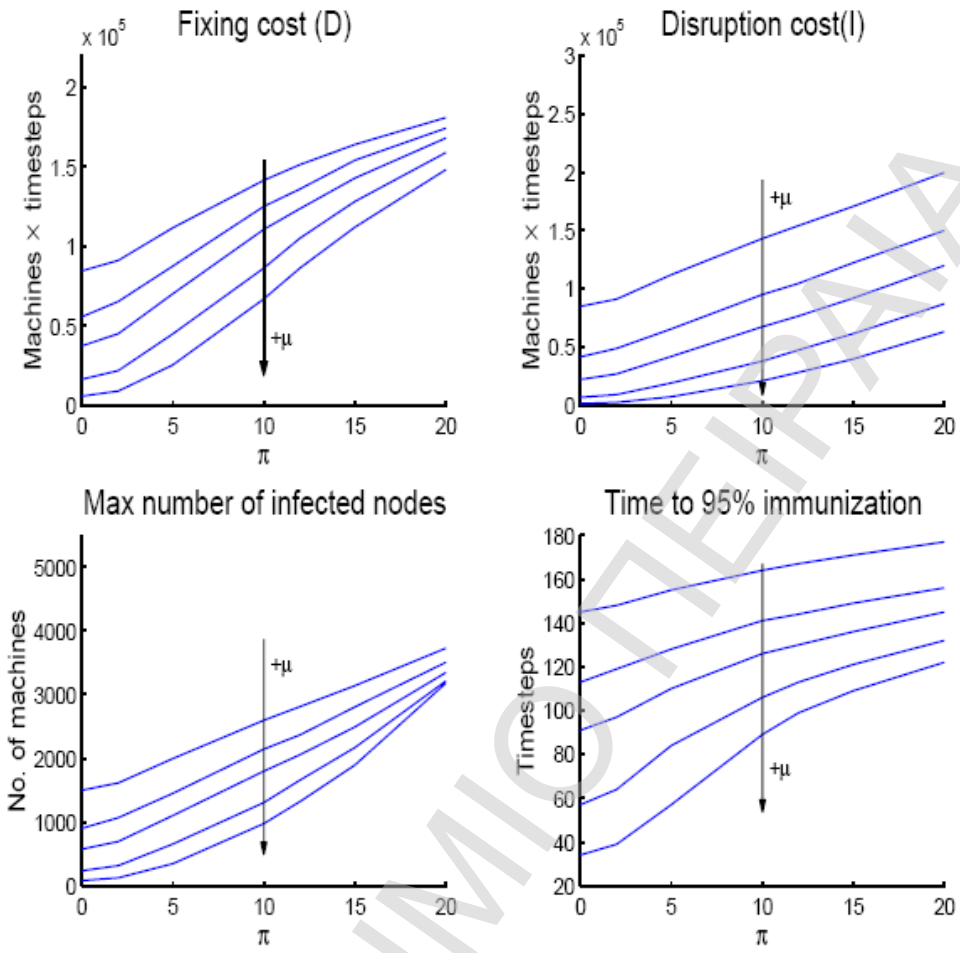
Αλληλεπιδράσεις μεταξύ π και μ

Αυτό το τμήμα αφορά τις αλληλεπιδράσεις μεταξύ του χρόνου απόκρισης **(**π**)** και του ρυθμού ανίχνευσης **(**μ**).** Τα ακόλουθα σχήματα **(**Σχήμα **55)** εκθέτουν τις τιμές για ομοιογενή και τα **SF** δίκτυα αντίστοιχα**.**




**Σχήμα 55. Το κόστος ως συνάρτηση του π και μ σε 6250 κόμβους σε ομογενή δίκτυα(β = 0 .1, δ = 0.03) στα διαστήματα από 0 ≥ π≥ 20 και 0.03≥μ≥ 0 .10 (από πάνω προς τα κάτω)**

Οι αλληλεπιδράσεις είναι σαφώς παρούσες. Προκειμένου να ωφεληθεί από την επίδραση της αύξησης του μ, ο χρόνος απόκρισης π πρέπει να κρατηθεί όσο το δυνατόν μικρότερος **(**Σχήμα **56).**




**Σχήμα 56. Το κόστος ως συνάρτηση του π και μ σε 6250 κόμβους σε SF δίκτυα(β = 0 .1, δ = 0.03) για π = 0 ,2,.5 ,10 ,12 ,15, και, 20 και μ = 0.03 ,0.04 ,0.05 ,0.07 και 0 .10 (από πάνω προς τα κάτω).**

Μια παρόμοια κατάσταση παρατηρείται και στα ομοιογενή δίκτυα, αν και τα κόστη τείνουν να είναι μικρότερα.

Η κύρια επίδραση στα κόστη οφείλεται στο χρόνο απόκρισης **(**π**).** Δηλαδή μειώνοντας το χρόνο απόκρισης μειώνονται όλα τα κόστη.

Η αύξηση του ποσοστού ανίχνευσης θα μειώσει επίσης όλα τα κόστη. Μια μικρή αύξηση στο ποσοστό ανίχνευσης μ **(**από μ **= 0.03** μ **= 0.04)** βελτιώνει πολύ το κόστος διάσπασης και τον χρόνο ανοσοποίησης. Η επίδραση του μ είναι παρούσα στο κόστος επιδιόρθωσης και μέγιστη επικράτηση μόνο για τις χαμηλές τιμές του π στα ομογενή Α.Μ. Η ίδια αλληλεπίδραση μεταξύ μ και π παρατηρείται για τα δίκτυα **SF,** αν και σε μικρότερο βαθμό. Αυτό συμβαίνει επειδή τα ομογενή δίκτυα δεν μπορούν να ωφεληθούν από την ανοσοποίηση όταν οι περισσότεροι κόμβοι είναι ήδη μολύσμένοι.

Εφαρμόζοντας αυτά τα αποτελέσματα στον πραγματικό κόσμο, είναι σημαντικό να γίνεται άμεσα διαθέσιμη η υπογραφή του ΛΠΥ μετά από τις πρώτες-πρώτες

μολύνσεις σκουληκιών. Επίσης, οι δαπάνες θα βελτιωθούν με την ταχύτερη διανομή της υπογραφής των **antivirus.**

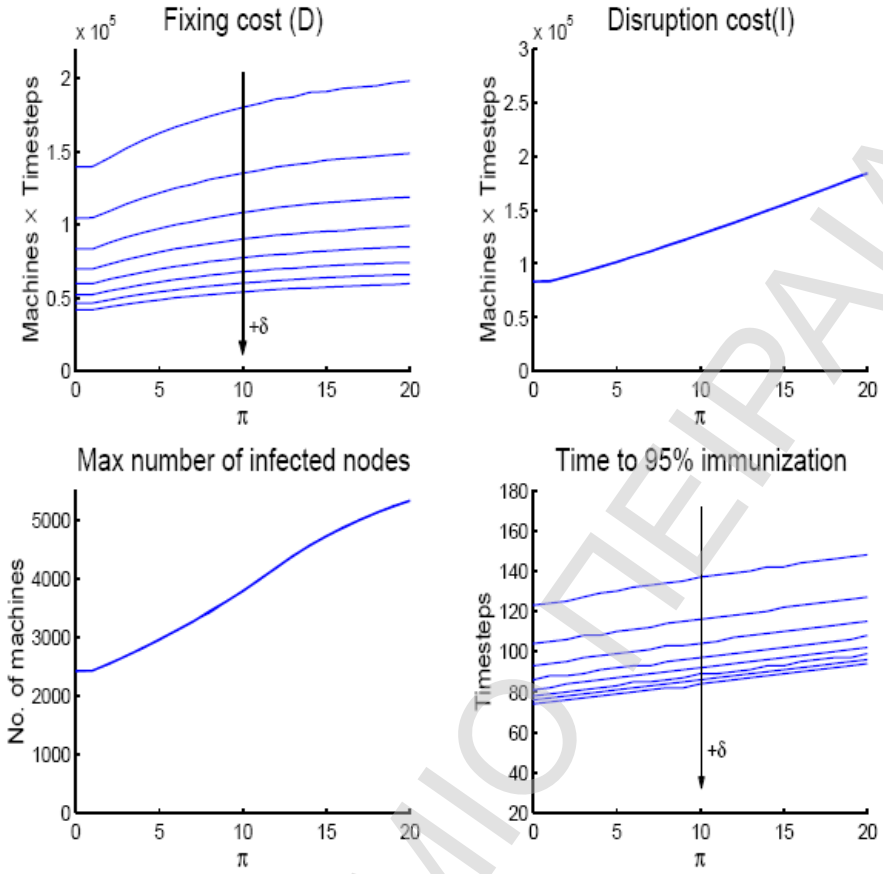
Αλληλεπίδρασης μεταξύ π και δ

Αυτό το τμήμα αφορά τις αλληλεπιδράσεις μεταξύ του χρόνου απόκρισης **(**π**)** και του ρυθμού θεραπείας **(**δ**).** Τα ακόλουθα εκθέτουν τις τιμές για ομογενή και **SF** δίκτυα αντίστοιχα.

Γενικά, η μείωση του χρόνου απόκρισης **(**π**)** μειώνει όλα τα κόστη. Ο ρυθμός θεραπείας **(**δ**)** δεν επηρεάζει ούτε τη διάδοση ούτε τη μέγιστη επικράτηση. Εντούτοις, μια αύξηση του ρυθμού θεραπείας μειώνει το κόστος επισκευής και το χρόνο της ανοσοποίησης. Αυτό κωδικοποιείται πραγματικά στο **PSIDR** πρότυπο: ο ρυθμός θεραπείας δεν είναι προορισμένος να ελέγχει τις μεταβάσεις από ή προς την φάση I: μεταφέρει μόνο τις μονάδες από την φάση **D** στην φάση **R.** Οι δύο παράγοντες αλληλεπιδρούν μη γραμμικά στο κόστος επισκευής. Δηλαδή η μείωση του χρόνου απόκρισης έχει μια μεγαλύτερη επίδραση στο κόστος επισκευής για χαμηλές τιμές του δ. Πάλι, η διατήρηση του χρόνου απόκρισης όσο το δυνατόν χαμηλότερα είναι μια προτεραιότητα, αλλά μια μεγάλη αύξηση στο ποσοστό θεραπείας **(**από δ **= 0.03** σε δ **= 0 .10)** θα βελτιώσει σημαντικά μερικά από τα κόστη.

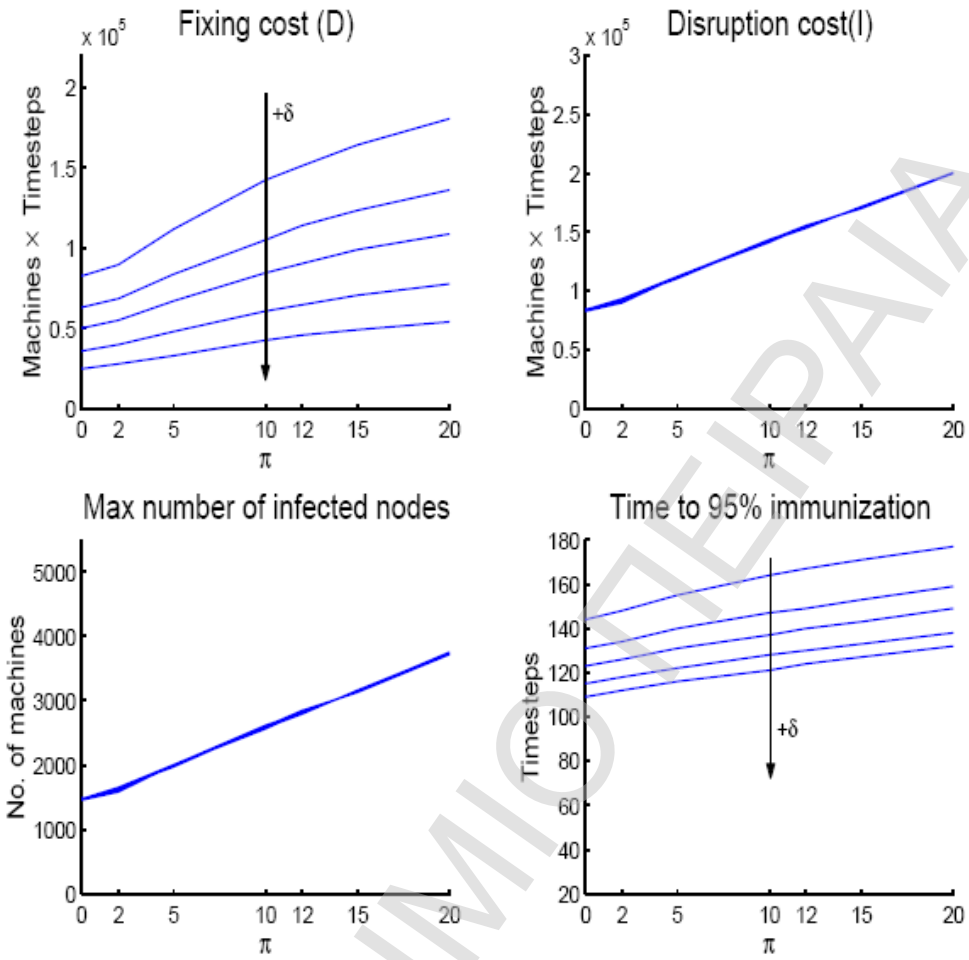
Η μέγιστη επικράτηση είναι υψηλότερη στα ομογενή απ' ό,τι στα **SF** δίκτυα. Το αντίθετο ισχύει για τη διάσπαση. Αυτό σημαίνει ότι η μόλυνση είναι πιο διεσπαρμένη στο χρόνο για τα **SF** δίκτυα αλλά δεν είναι ποτέ τόσο οξέα όπως είναι στα ομογενή δίκτυα. Ένα παρόμοιο φαινόμενο έχει παρατηρηθεί στην περίπτωση του προτύπου **SIS [98].** Αυτό απεικονίζει το γεγονός ότι η μόλυνση είναι εγγενώς αργή στα δίκτυα **SF.** Αυτό το φαινόμενο πιθανώς θα μειωνόταν με τη χρησιμοποίηση ενός υψηλότερου ρυθμού ανίχνευσης, επειδή οι ευπαθείς κόμβοι θα μετέβαιναν έπειτα στην φάση αφαίρεσης αντί να περιμένουν να μολυνθούν από το σκουλήκι. Αυτό το παράδειγμα υπολογίζει επίσης τον πιο μακροχρόνιο χρόνο ανοσοποίησης που παρατηρείται στα **SF** δίκτυα σε αντιδιαστολή με τα ομογενή.

Εφαρμόζοντας αυτά τα αποτελέσματα στον πραγματικό κόσμο, είναι πάλι σημαντικό να γίνετε η υπογραφή των σκουληκιών διαθέσιμη το συντομότερο δυνατόν. Εάν το κόστος επισκευής και ο χρόνος ανοσοποίησης είναι οι κύριες ανησυχίες, η θεραπεία των μολυσμένων υπολογιστών γρηγορότερα θα βελτιώσει δραστικά αυτά τα κόστη.




**Σχήμα 57. Το κόστος ως συνάρτηση του π και δ σε 6250 κόμβους ΗΜ δικτύου(β = 0 .1, μ = 0.05) για τα διαστήματα 0 ≥π≥ 20 και 0.03≥ δ≥ 0 .10 (από πάνω προς τα κάτω).**

Το ποσοστό θεραπείας δεν επηρεάζει τη διάσπαση και το μέγιστη επικράτηση όπως αναμένεται από το πρότυπο. Ο χρόνος απόκρισης και το ποσοστό θεραπείας αλληλεπιδρούν στα άλλα κόστη.




**Σχήμα 58. Το κόστος ως συνάρτηση του π και δ σε 6250 κόμβους SF δικτύου(β = 0.1, μ = 0.03) για π = 0 ,2 ,5 ,10,12 ,15, και 20 και μ = 0,03, 0,04, 0,05, 0,07 και, 0,10**

Το ποσοστό θεραπείας δεν επηρεάζει τη διάσπαση και τη μέγιστη επικράτηση όπως αναμένεται από το πρότυπο. Εκτός από το χρόνο για την ανοσοποίηση και τη διάσπαση, τα κόστη είναι χαμηλότερα σε **SF** απ' ότι στα HM δίκτυα. Αυτό οφείλεται στο γεγονός ότι, στα δίκτυα **SF,** το ξέσπασμα είναι πιο διεσπαρμένο στο χρόνο αλλά ποτέ οξύτερος απ' ό,τι στα HM δίκτυα.

Αλληλεπίδραση μεταξύ μ και δ

Αυτό το τμήμα αφορά τις αλληλεπιδράσεις μεταξύ της ανίχνευσης **(**μ**)** και του ρυθμού θεραπείας **(**δ**).** Τα επόμενα διαγράμματα εκθέτουν τις τιμές για τα δίκτυα **HM** και **SF** αντίστοιχα.

Γενικά, η αύξηση του ποσοστού θεραπείας μειώνει το κόστος επιδιόρθωσης, και η αύξηση του ποσοστού ανίχνευσης μ μειώνει το κόστος διάσπασης. Και οι δύο παράγοντες φαίνονται να έχουν μια επίδραση μείωσης στο χρόνο προς την ανοσοποίηση. Αυτό προτείνει ότι η αποδοτική βελτίωση στις στρατηγικές ασφάλειας δεν μπορεί να οριοθετηθεί μόνο σε έναν μηχανισμό, αλλά πρέπει να γίνει και στις δύο πτυχές της αντίδρασης **(**ανίχνευση και θεραπεία**),** προκειμένου να μειωθούν τα

περισσότερα κόστη. Διαφορετικές τοπολογίες φαίνονται να αποκρίνονται με διαφορετικούς τρόπους στις διάφορες παραμέτρους. Στα δίκτυα HM, το ποσοστό ανίχνευσης δεν έχει καμία απολύτως επίδραση στο κόστος αποκατάστασης, αλλά αυτό οφείλεται στο χρόνο απόκρισης π **= 20** που χρησιμοποιήθηκε στην προσομοίωση, ο οποίος ακυρώνει την επίδραση του μ στα HM δίκτυα. Δεδομένου ότι τα **SF** δίκτυα παίρνουν περισσότερο χρόνο να μολυνθούν μπορούν ακόμα να ωφεληθούν από μια αύξηση στο ποσοστό ανίχνευσης **(**οι περισσότεροι κόμβοι είναι διαθέσιμοι για την άμεση ανοσοποίηση**)**. Αυτό εξηγεί επίσης τον παρατηρηθέντα μέγιστο αριθμό μολυσμένων κόμβων, που δεν αλλάζει σαν συνάρτηση του μ στα HM δίκτυα, αλλά το κάνει στα δίκτυα **SF**. Τέλος, η διανομή μπορεί να υπολογιστεί από την ίδια εξήγηση. Εντούτοις, δεν εξηγεί την πραγματικά μεγάλη παρατηρηθείσα βελτίωση κατά την αύξηση του μ από **0,03** σε **0,05** στα **SF** δίκτυα του κόστους διάσπασης. Αυτή η ιδιαίτερη βελτίωση μπορεί να αποδοθεί στην αυξανόμενη πιθανότητα ανοσοποίησης των ιδιαίτερα συνδεδεμένων κόμβων**(**που παρουσιάζουν πολλές συνδέσεις**)** : έχει αποδειχθεί ότι **[41]**, μόλις ανοσοποιηθούν εκείνοι οι κόμβοι, η επικράτηση των ιών μειώνεται πραγματικά γρήγορα.

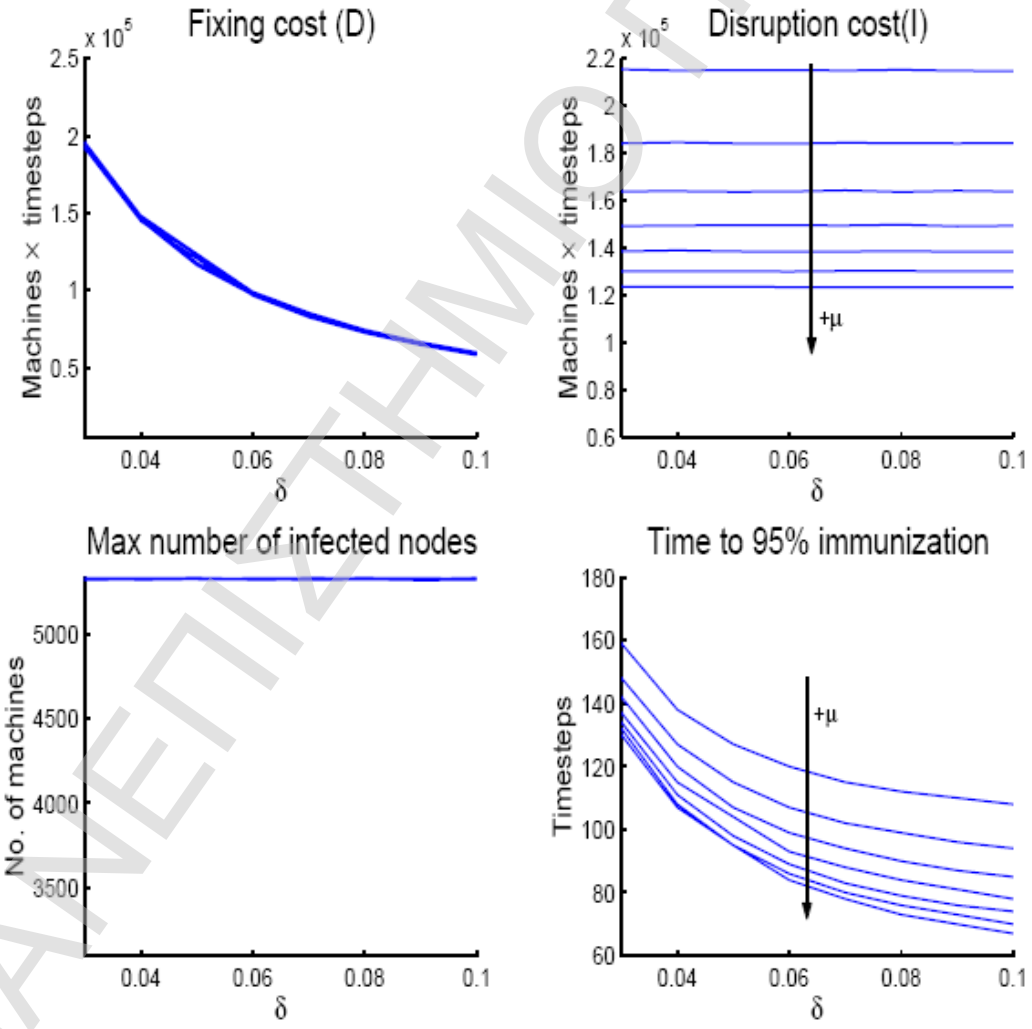
Εφαρμόζοντας αυτά τα αποτελέσματα στον πραγματικό κόσμο, είναι σημαντικό να ενεργούμε και στη διανομή των υπογραφών αλλά και στη θεραπεία για να έχουμε όφελος σε όλα τα κόστη. Ενώ μια γρηγορότερη θεραπεία θα μειώσει το κόστος αποκατάστασης, μια γρηγορότερη διανομή αντιιών θα μειώσει τη διάσπαση. Με την αύξηση της ταχύτητας καθενός παράγοντα, το δίκτυο θα ανοσοποιηθεί γρηγορότερα. Όσον αφορά την τοπολογία δικτύων, είναι σημαντικό να ανοσοποιηθούν οι ιδιαίτερα συνδεδεμένοι κόμβοι.

### 6.2.2.3 Ρυθμός διάδοσης και περιορισμός του ιού.

Ο περιορισμός των ιών αναφέρεται στη στρατηγική με την οποία οι συνδέσεις παρακολούθησης των δικτύων επιφέρουν μείωση της ταχύτητας της διάδοσης του μολυσματικού σκουληκιού. Εδώ, για απλότητα, η κύρια επίδραση του περιορισμού είναι μια μείωση του ρυθμού γέννησης σε μια χαμηλή τιμή**(**β **= 0.05)**. Τα οφέλη του περιορισμού των ιών **(**επιβράδυνση**)** είναι πιθανό να είναι περισσότερα για τα γρήγορα σκουλήκια. Αυτή η υπόθεση εξετάζεται με την εξομοίωση διάφορων ρυθμών γέννησης **(**στο εύρος **0.05 <** β **< 0.14)** σε HM και **SF** δίκτυα. Η πορεία του ξεσπάσματος κατά τη διάρκεια του χρόνου παρουσιάζεται στο πρώτο από τα ακόλουθα σχήματα.

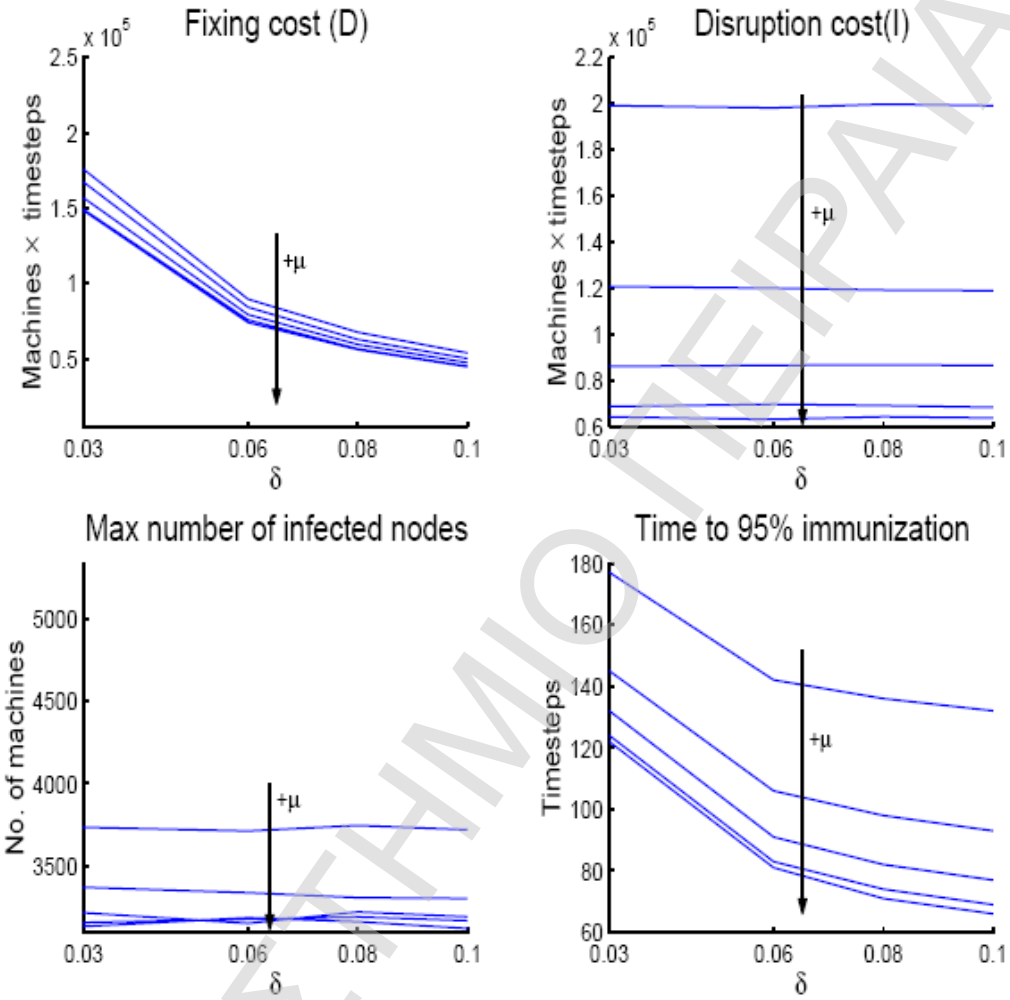
Τα **SF** δίκτυα εμφανίζονται να επηρεάζονται περισσότερο από τα HM δίκτυα από την επιβράδυνση. Το δεύτερο σχήμα παρουσιάζει σαφώς τα αποτελέσματα στα κόστη.

Η επιβράδυνση της διάδοσης έχει ως γενική επίδραση την μείωσης των διαφορετικών κοστών. Από τα ακόλουθα διαγράμματα φαίνεται ότι η επιβράδυνση είναι αποτελεσματικότερη στα γρηγορότερα σκουλήκια, και ειδικότερα σε **SF** δίκτυα. Ο χρόνος για την ανοσοποίηση και το κόστος αποκατάστασης είναι τα πιο βελτιωμένα από την στρατηγική επιβράδυνσης. Αυτό πιθανώς οφείλεται σε έναν ενιαίο φαινόμενο, δηλαδή περισσότεροι υπολογιστές είναι διαθέσιμοι για ανοσοποίηση όταν ο ρυθμός διάδοσης είναι αργός (είναι ανοσοποιημένοι προτού να μολυνθούν). Αν και τα οφέλη εμφανίζονται περιορισμένα στα HM δίκτυα, δεν πρέπει να ξεχάσουμε ότι η τιμή που επιλέγεται για το ρυθμό γέννησης μετά από επιβράδυνση **(β = 0.05)** είναι μάλλον υψηλή. Ο πραγματικός ρυθμός είναι πιθανόν να είναι μικρότερος από αυτόν που επιλέχθηκε εδώ, και βελτιώσεις στα κόστη είναι πιθανό να είναι πιο αξιοσημείωτες.



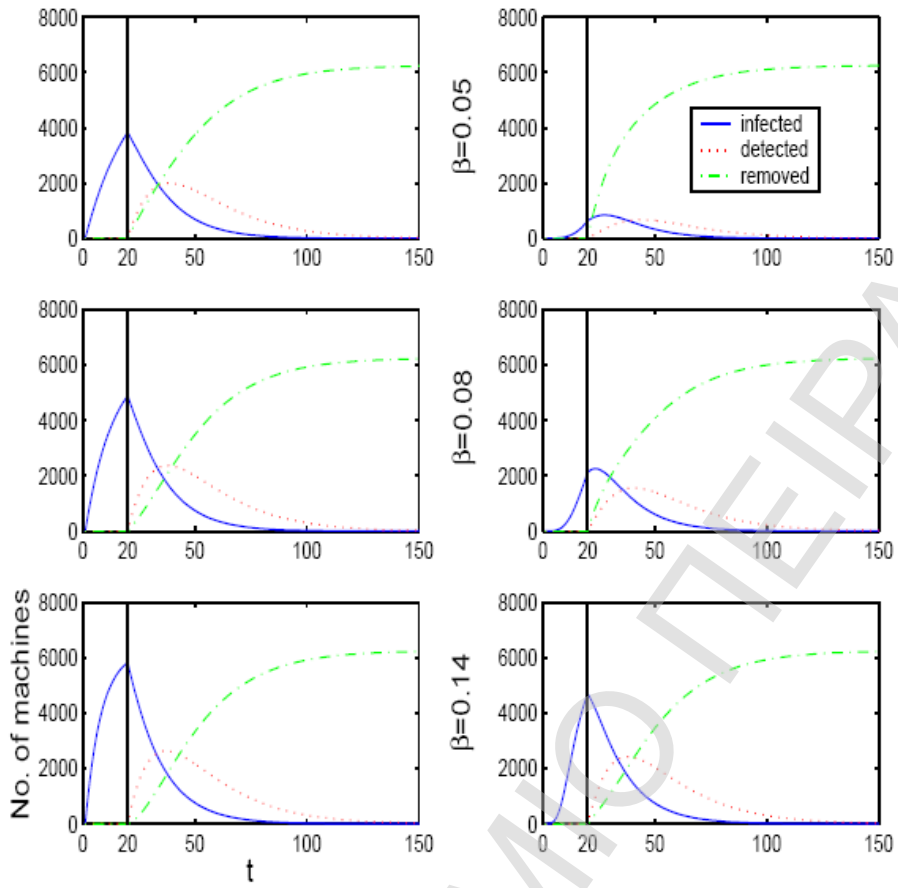

**Σχήμα 59. Το κόστος ως συνάρτηση του μ και δ σε 6250 κόμβους σε HM δίκτυο (β = 0.1, π = 20) για το διάστημα 0.03 ≥ δ≥ 0 .10 και 0.03≥ μ≥ 0 .10 (από πάνω προς τα κάτω).**

Διαφορετικοί παράμετροι συμπεριφέρονται ομοίως σε διαφορετικά κόστη, αλλά αλληλεπιδρούν στο χρόνο για την ανοσοποίηση. Και οι δύο παράγοντες δεν επηρεάζουν το μέγιστο αριθμό μολυσμένων κόμβων.



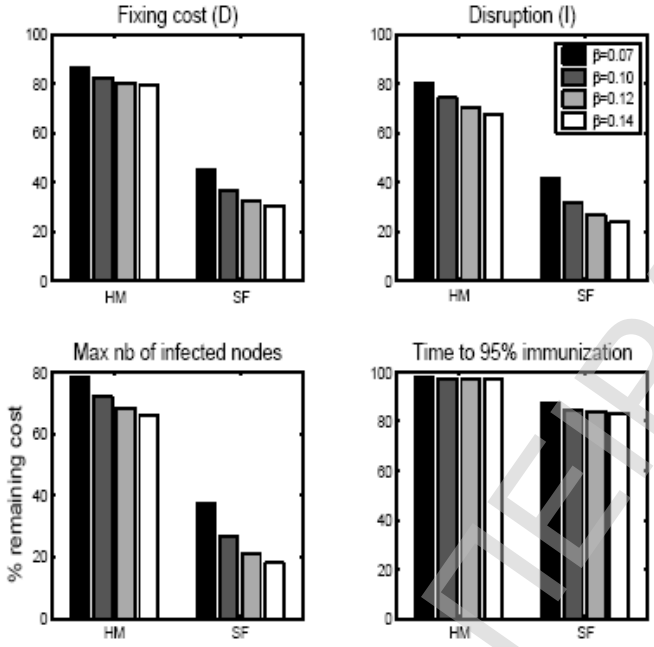

**Σχήμα 60. Το κόστος ως συνάρτηση του μ και δ σε 6250 κόμβους σε SF δίκτυο(β = 0 .1, π = 20) για δ = 0.03, 0.06, 0.08 και 0 .10 και μ = 0.03, 0.05, 0.07, 0.09 και 0 .10 (από πάνω προς τα κάτω).**

Αντίθετα με αυτό που παρατηρείται στα ΗΜ δίκτυα, το ποσοστό ανίχνευσης μ επηρεάζει το μέγιστο αριθμό μολυσμένων κόμβων.




**Σχήμα 61. Το PSIDR μοντέλο ως συνάρτηση του ρυθμού διάδοσης σε HM (αριστερά) και SF δίκτυα (δεξιά) (n=20, μ=0.07 και δ=0.05).**

Μειώνοντας των ρυθμό διάδοσης **(β)** παρουσιάζονται επιπτώσεις στην εξέλιξη του ξεσπάσματος**.** Η επίδραση της μείωσης της ταχύτητας του σκουληκιού είναι σαφέστερη στα δίκτυα **SF.**




**Σχήμα 62. Η επίδραση της επιβράδυνσης των ιών στα κόστη σε HM και SF δίκτυα σε 6250 κόμβους (δ=0.05, μ=0.07, π=50)**

Οι ιστοί αναπαριστούν το κόστος το μετά την μείωση ως ποσοστό του αρχικού κόστους σαν (χωρίς επιβράδυνση). Γενικά, η επιβράδυνση του ιού είναι αποτελεσματικότερο για **SF** δίκτυα και για υψηλότερο β.

### 6.2.2.4 Βέλτιστες στρατηγικές ελέγχου

Γενικά, είναι προτιμητέο να διατηρείτε ο χρόνος απόκρισης (π) όσο το δυνατόν χαμηλότερος. Αυτό συνεπάγεται ότι οι πρώτες περιπτώσεις δράσης ενός σκουληκιού πρέπει να ανιχνευθούν πραγματικά γρήγορα, και να εξαχθεί η υπογραφή του ιού σε πολύ σύντομο χρονικό διάστημα. Αυτοματοποιημένα συστήματα ασφάλειας είναι ενδεδειγμένα δεδομένου ότι η ταχύτητα δράσης τους σε αυτήν την φάση είναι πολύ μεγαλύτερη από τη χειρωνακτική εργασία.

Εάν το κόστος επισκευής είναι η κύρια ανησυχία, η αύξηση του ρυθμού θεραπείας (δ) θα το μειώσει αρκετά. Μια αυτοματοποιημένη διαδικασία επιδιόρθωσης θα ήταν πολύ χρήσιμη να μειώσει αυτό το κόστος.

Εάν το κόστος επιβράδυνσης είναι το σημαντικότερο, τότε ο ρυθμός ανίχνευσης (μ) θα πρέπει να αυξηθεί. Δηλαδή το αντιίκο θα πρέπει να διανεμηθεί γρηγορότερα. Η προσπάθεια να ανοσοποιηθούν οι υπολογιστές που παρουσιάζουν υψηλή συνδεσιμότητα μπορεί επίσης να βοηθήσει στην μείωση της επικράτησης.

Ο χρόνος για την ανοσοποίηση επηρεάζεται από όλους τους παράγοντες ελέγχου (π, μ και δ) δεδομένου ότι συλλαμβάνει την εξέλιξη της ποσότητας των μηχανισμών στο στάδιο της αφαίρεσης. Επομένως, επηρεάζεται από ότι συμβαίνει σε όλες τις

προηγούμενες φάσεις **(**ευπαθής**,** μολυσμένος και ανιχνευμένος**).** Οποιαδήποτε βελτίωση στις στρατηγικές ελέγχου θα έχει έτσι κάποια επίδραση στο χρόνο για την ανοσοποίηση**.**

# 7 Συμπεράσματα- Μελλοντικές κατευθύνσεις

## 7.1 Συμπεράσματα

Λαμβάνοντας υπόψη την εξάρτηση των περισσότερων σύγχρονων κοινωνιών από διάφορες ψηφιακές υποδομές, η ταχεία εξάπλωση του κακόβουλου λογισμικού αποτελεί σημαντικό πρόβλημα. Η ανάπτυξη αλγορίθμων για την βελτίωση της αποτελεσματικότητας των αντιικών προγραμμάτων και των Συστημάτων Ανιχνεύσεως Εισβολέων **(Intrusion Detection Systems)** είναι χρήσιμη, αλλά όχι και αρκετή για το περιορισμό της ταχείας εξάπλωσης κακόβουλου λογισμικού. Η μικροσκοπική ανάλυση είναι ιδανική για την προστασία μεμονωμένων συστημάτων ή για τον καθαρισμό τους, αν έχουν ήδη μολυνθεί από κάποιο είδος κακόβουλου λογισμικού. Από την άλλη πλευρά, για την προστασία διαφόρων κρίσιμων τεχνολογικών υποδομών, όπως τα τηλεπικοινωνιακά και πληροφοριακά συστήματα, καθώς και τα συστήματα ελέγχου, απαιτείται μια γενικότερη στρατηγική προσέγγιση. Στην Ιατρική οι μικροβιολόγοι εργάζονται παράλληλα με τους επιδημιολόγους για την έγκαιρη αναγνώριση νέων απειλών, ώστε να προσφέρουν την βέλτιστη δυνατή προστασία στον ευπαθή πληθυσμό. Σε θέματα επιδημιολογίας υπολογιστών παρόμοιες συνέργειες θα πρέπει να αναπτυχθούν για την προστασία των ψηφιακών υποδομών. Το πρώτο βήμα για το σχεδιασμό αποτελεσματικών περιοριστικών μέτρων στην εξάπλωση του κακόβουλου λογισμικού είναι η πλήρης και βαθιά κατανόηση του τρόπου και των προτύπων διάδοσης του. Η εφαρμογή επιδημιολογικών μοντέλων στις διάφορες μορφές κακόβουλου λογισμικού μπορεί να περιγράψει με ικανοποιητική ακρίβεια την εξάπλωσή του.

Όπως έχει ήδη επισημανθεί, τα μοντέλα αυτά μπορούν να είναι είτε σύνθετα είτε απλά **[20]**. Τα σύνθετα μοντέλα έχουν το πλεονέκτημα των ρεαλιστικών περιπτώσεων δοκιμής, και της παροχής ακριβέστερων προβλέψεων. Εντούτοις, τα απλούστερα μοντέλα μπορούν να οδηγήσουν σε βαθύτερη γνώση και κατανόηση κάτι το οποίο είναι δυσκολότερο να γίνει με ένα σύνθετο πρότυπο.

Παρόλα ταύτα, υπάρχει μία αύξηση της εστίασης στα πρότυπα όπως το **SIS**, **SIR** και **SEIR**. Το πρότυπο **PSIDR** δείχνει ότι τα πιο σύνθετα πρότυπα μπορούν εύκολα να χτιστούν και να αναλυθούν λεπτομερώς για να παρέχουν καλύτερο χαρακτηρισμό των πραγματικών επιδημιών. Σαν αντάλλαγμα, τα αποτελέσματα για το πρότυπο **PSIDR** δίνουν μια καλύτερη κατανόηση των μηχανισμών που θα οδηγήσουν σε έναν αποδοτικό έλεγχο των επιθέσεων από ιούς.

## 7.2 Μελλοντικές κατευθύνσεις

Ακολουθεί μία λίστα κατευθύνσεων που χρίζουν περεταίρω διερεύνησης :

**Ø** Διαφορετικά μεγέθη δικτύων. Οι συγκρίσεις με τα μεγαλύτερα δίκτυα είναι χρήσιμες για την μελέτη των αποτελεσμάτων καθώς και των ιδιότητων των διαφορετικών τοπολογιών **(**κατηγοριών δικτύων**)**. Οι διαφορικές εξισώσεις του Γενικού Επιδημιολογικού Μοντέλου ισχύουν όταν τα εξεταζόμενα συστήματα συνδέονται καθολικά μεταξύ τους σχηματίζοντας ένα ομογενή γράφο. Σε άλλες τοπολογίες η καμπύλη του ρυθμού εξάπλωσης, παρότι διατηρεί την ίδια μορφή, απαιτεί περισσότερο χρόνο για να προσεγγίσει τα ίδια ποσοστά εξάπλωσης.

**Ø** Δημιουργία μοντέλων που να υποστηρίζουν δίκτυα μεταβλητού μεγέθους όπου θα μπορούν να προσομοιώνουν διαφορετικά μοντέλα διάδοσης του ιού με μεταβλητούς ρυθμούς διάδοσης τόσο της μόλυνσης όσο και της ανίχνευσης αλλά και της θεραπείας.

**Ø** Χρήση διαφορετικών μοντέλων διάδοσης αντιιών. Σε ομογενή δίκτυα ένας αποτελεσματικός μηχανισμός καταστολής της διάδοσης των επιδημιών είναι η θεραπεία τυχαίων κόμβων στο δίκτυο **[16]**. Ωστόσο η μέθοδος αυτή είναι ανεπαρκής για δίκτυα ελεύθερης κλίμακας λόγω της ύπαρξης κόμβων με υψηλή συνδεσιμότητα. Μία ιδέα που ξεκίνησε από τον **Kephart** είναι να διαδίδεται η υπογραφή των ιών με τον ίδιο τρόπο που ο ιός διαδίδει στο δίκτυο **[69]**. Η υπογραφή θα εγχεόταν στον υπολογιστή που άρχισε η μόλυνση, και έπειτα θα αφηνόταν να διαδοθεί στους γειτονικούς υπολογιστές. Αυτή η στρατηγική θα είχε το πλεονέκτημα της επίθεσης του ξεσπάσματος στον πυρήνα του.

**Ø** Εξέταση της δύναμη μόλυνσης **(**Η συνάρτηση **F=**βI**,** που μοντελοποιεί το ρυθμό μετάβασης από το διαμέρισμα των ευπαθών ατόμων στο διαμέρισμα των μολυσματικών ατόμων**)** ως συνάρτηση που δεν εξαρτάται από τον απόλυτο αριθμό των μολυσμένων ατόμων, αλλά από ένα μέρος τους **(**όσον αφορά το συνολικό σταθερό πληθυσμό N**)**: Ο **Capasso** και, κατόπιν, άλλοι συγγραφείς έχουν προτείνει μη γραμμικές δυνάμεις μόλυνσης για να μοντελοποιήσουν πιο ρεαλιστικά τη διαδικασία μετάδοσης της ασθένειας

**Ø** Είναι σημαντικό να τονιστεί ότι στα μοντέλα που χρησιμοποιήσαμε υποθέτουμε ότι η μονιμότητα κάθε ατόμου στις επιδημικές καταστάσεις είναι μια τυχαία μεταβλητή με εκθετική κατανομή. Ποιο σύνθετες και ρεαλιστικές κατανομές **(**όπως κατανομές **Erlang)** μπορούν να χρησιμοποιηθούν.

**Ø** Αναλυτικές προβλέψεις. Οι ιδιότητες του δικτύου στη φάση ανίχνευσης θα μπορούσαν επίσης να μελετηθούν αναλυτικά, ειδικά η πιθανή ύπαρξη επιδημικού ορίου ως συνάρτηση διάφορων παραμέτρων.

**Ø** Τροποποίηση του **PSIDR** μοντέλου έτσι ώστε να μπορέσουμε να συμπεριλάβουμε και μια άλλη αρχική κατάσταση κατά την οποία ορισμένοι κόμβοι έχουν ανοσία ως συνέπεια του γεγονότος ότι πολύ ιοί είναι προσανατολισμένοι σε συγκεκριμένα λειτουργικά συστήματα π.χ. **windows** και άρα υπολογιστές με διαφορετικά λειτουργικά συστήματα δεν μπορούν να μολυνθούν π.χ **linux**, **mac, Solaris, unix.**

# 8 Βιβλιογραφία


**1 Agur, Z. Cojocaru, L. Mazor, G. Anderson, R. and Danon, Y. 'Pulse mass measles vaccination across age cohorts'Proc. Nat. Acad. Sci 1993.**

**2 Allen, Julia H. The CERT Guide to System and Network Security Practices,2001**

**3 Allman, E. and Rhodes, J. Mathematical Models in Biology. Cambridge University Press, 2004.**

**4 Altholz, N. and Stevenson, L. Rootkits for Dummies 2006**

**5 Anagnostakis, K. Greenwald, M. Ioannidis, S. and Keromytis, A. Robust reactions to potential dayzero worms through cooperation and validation. To appear in the Springer International Journal of Information Security (IJIS), ISC'06 Special Issue, 2007.**

**6 Anderson, James P., "Computer Security Threat Monitoring and Surveillance", 1980.**

**7 Andrew S. Tannenbaum,** Δεύτερη Αμερικάνικη Έκδοση, Σύγχρονα Λειτουργικά Συστήματα, Κλειδάριθμος, **2003**

**8 Arce, I. and Levy, E. An analysis of the slapper worm. IEEE Security &Privacy, 2003.**

**9 Aspnes, J. Chang, K. and Yampolskiy, A. Inoculation strategies for victims of viruses and the sum-of-squares partition problem. In SODA, 2005.**

**10 Axelsson, S. Visualisation for intrusion detection hooking the worm. In Proceedings of the 8th European Symposium on Research in Computer Security. SpringerVerlag,2003**

**11 Bailey, M. Cooke, E. Jahanian, F. Watson, D. and Nazario, J. The blaster worm: Then and now. IEEE Security & Privacy, 2005.**

**12 Bailey, N. The mathematical Theory of Infectious Diseases (2nd edition), Charles Griffin and co. Ltd 1975.**

**13 Barford, P. and Yegneswaran, V. A look inside botnets. In Springer, editor,To appear in Series: Advances in Information Security, 2006.**

**14 Bartal, Y. Mayer, A. Nissim, K. and Wool, A. Firmato: A novel firewall management toolkit. In Proceedings of the IEEE Computer Society Symposium on Security and Privacy, 1999.**

15 Barthelemy, M. Barrat, A. PastorSatorras, R. and Vespignani, A. Velocity and hierarchical spread of epidemic outbreaks in scalefree networks, 2004.

16 Barthelemy, M. Barrat, A. Pastor-Satorras, R. and Vespignani, A. Dynamical patterns of epidemic outbreaks in complex heterogeneous networks. Journal of Theoretical Biology, 2005.

17 Bellovin, S. Distributed firewalls, 1999.

18 Bellovin, S. Firewall-friendly FTP. RFC 1579, Internet Engineering Task Force, 1994.

19 Bellovin, Steven M. "Problem Areas for the IP Security Protocols", 1996

20 Billings, L. and Schwartz, I. B.. Exciting chaos with noise: unexpected dynamics in epidemic outbreaks. Journal of Mathematical Biology, 2002.

21 Boguna, M and PastorSatorras, R. Epidemic spreading in correlated complex networks. Physical Review E, 2002

22 Boguna, M. Pastor-Satorras, R. and Vespignani, A.. Epidemic spreading in complex networks with degree correlations. Statistical Mechanics of Complex Networks, 2003.

23 Bonfante, G. Kaczmarek, M. and Marion, J. On abstract computer virology from a recursion theoretic perspective. Journal in Computer Virology 2006.

24 BREYER, R., and RILEY, S.: Switched, Fast, and Gigabit Ethernet, Indianapolis, IN: New Riders, 1999.

25 caida.org. Dynamical graphs of computer prevalence, 2002.

26 caida.org. The spread of the code-red worm (crv2), 2002.

27 Capasso,V. The Mathematical Structure of Epidemic Systems, Springer Verlag 1993.

28 Cheswick, W. Bellovin, S. and Rubin, A.. Firewalls and Internet Security; Repelling the Wily Hacker. Addison-Wesley, Reading, MA, 2003.

29 Coggon, Rose, and Barker. Epidemiology for the Uninitiated, Chapter 8, "Case-control and cross-sectional studies", BMJ(British Medical Journal) Publishing, 1997

30 Cohen, F. Computer viruses – theory and experiments. Computers and Security, 1987.

31 Cohen, F. Computer viruses: Theory and experiments. In Proceedings of the 7th national security conference, pages 240–263, September 1984.

32 Cohen, F. A Short Course on Computer Viruses. Wiley Professional Computing. Wiley, Canada, 1994.

33 Cohen, F. Computer viruses: Theory and experiments. In Proceedings of the 7th national security conference, 1984.

34 Cohen, R. Havlin, S. and Avraham, D.. Efficient immunization strategies for computer networks and populations. Phys Rev Lett., 2003.

35 COLLINS, D., and SMITH, C.: 3G Wireless Networks, New York: McGraw-Hill, 2001.

36 Cox, R. Grosse, E. Pike, R. Presotto, D. and Quinlan, S. Security in plan 9. In Proceedings of the 11th Usenix Security Symposium, CA, USA,2002

37 Daley, D. and Gani, J. Epidemic Modelling. Cambridge University Press, 1999.

38 Daniel, B. Couto, J., Jajodia, S., Popyack, L., and Ningning, W. "ADAM: Detecting Intrusions by Data Mining," Proceedings of the IEEE Workshop on Information Assurance and Security, 2001

39 DAVIS, P.T., and MCGUFFIN, C.R.: Wireless Local Area Networks, New York: McGraw-Hill, 1995.

40 Denning, P. Computers under Attack: Intruders, Worms, and Viruses, Addison – Wesley Publishing Company,1990

41 Deszo, Z and Barabasi, A. Halting viruses in scale free networks,2002

42 DOBROWSKI, G., and GRISE, D.: ATM and SONET Basics, Fuquay-Varina, NC: APDG Telecom Books, 2001.

43 Doraswamy, N. Harkins, D. "IPSec", 2003

44 Ecker, Clint. Massive spyware-based identity theft ring uncovered. 2005

45 eEye Digital Security. Code Red II worm analysis AL20010804, 2005

46 Erbschloe, M. Trojans, worms and spyware. A computer security professional's guide to malicious code. Elsevier Butterworth–Heineman, Oxford UK, 2005

47 Erbschloe, M. Trojans, worms and spyware. A computer security professional's guide to malicious code. Elsevier Butterworth–Heineman, Oxford, 2005

48 Ganesh, A. Massouli, L. and Towsley, D. The effect of network topology on the spread of epidemics. In IEEE INFOCOM, 2005.

49 Gaynor M. and Bradner, S. Firewall enhancement protocol (FEP). RFC 3093, Internet Engineering Task Force, April 2001.

50 Gleeson, B. et al, IP Based Virtual Private Networks, 2000

51 Graunt, J. Natural and Political Observations made upon the Bills of Mortality. John Martyn, London, 1662.

52 Gritzalis S. and Spinellis D. Addressing threats and security issues in World Wide Web technology. In Proceedings CMS '97 3rd IFIP TC6/TC11 International joint working Conference on Communications and Multimedia Security, Chapman & Hall, 1997.

53 Gudmundsson, A.and Chien, E. (Symantec Security Response), 2002

54 Halsall F. Data Communications, Computer Networks and OSI. Addison-Wesley, second edition, 1988

55 Hamzeh, K. et al.,Point-to-Point Tunneling Protocol (PPTP), 1999

56 Hethcote, H. 'Qualitative analyses of communicable disease models',Math. Biosci 1976.

57 Hethcote, H. The mathematics of infectious diseases. SIAM Review, 2000.

58 Hoglund, G. and Butler, J. Rootkits: Subverting the Windows Kernel, 2005

59 Howes, Eric L. "The Spyware Warrior List of Rogue/Suspect Anti-Spyware Products & Web Sites", 2005.

60 Inaba H. Threshold and stability results for an age-structured epidemic model, 1990

61 IZZO, P.: Gigabit Networks, New York: Wiley, 2000.

62 JAIN, R.: FDDI Handbook—High-Speed Networking Using Fiber and Other Media, Boston: Addison-Wesley, 1994.

63 James, F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach, 2007

64 JOHNSON, H.W.: Fast Ethernet—Dawn of a New Network, Englewood Cliffs, NJ: Prentice Hall, 1996.

65 JOVANOVICH M., ANNEXSTEIN F., and BERMAN K.. Scalability issues in large peertopeer networks—a case study of Gnutella. Technical report, ECECS Department, University of Cincinnati, Cincinnati, OH 45221, 2001. Technical Report.

66 Kempe, D. Kleinberg, J. and Tardos, E.. Maximizing the spread of influence through a social network 2003.

67 Kephart, J and White, S. Measuring and modeling computer virus prevalence. In Proceedings of the 1999 IEEE Computer Society Symposium on Research in Security and Privacy, 1999.

68 Kephart, J. How topology affects population dynamics. In Proceedings of Artificial Life 3, New Mexico,USA, June 1992.

69 Kephart, J. A biologically inspired immune system for computers. In Rodney A. Brooks and Pattie Maes, editors, Artificial Life IV: Proceedings of the Fourth International Workshop on the Synthesis and Simulation of Living Systems, 1994.

70 Kephart, J. and White, S. Directedgraph epidemiological models of computer viruses. In Proceedings of the 1991 Computer Society Symposium on Research in Security and Privacy, 1991.

71 Kephart, J. Chess, D and White, S. Computers and epidemiology. IEEE Spectrum, 1993.

72 Kephart, J.O., White, S.R., Chess, D.M. Computers andepid emiology. IEEE Spectrum 30, 1993

73 Kephart, J.O., White, S.R.. Measuring andmod eling computer virus prevalence. In: 1993 IEEE Computer Society Symposium on Research in Security andPrivacy, Oakland, California, 1993

74 Kermack, O. McKendrick .A “A Contribution to the Mathematical Theory of Epidemics, 2000

75 Kermack, W. and McKendrick, A.. A contribution to the mathematical theory of epidemics. Proc. Roy. Soc. Lond., 1927.

76 Kohlenberg, Toby (Ed.), Alder, Raven, Carter, Dr. Everett F. (Skip), Jr., Foster, James C., Jonkman Marty, Raffael, and Poor, Mike, "Snort IDS and IPS Toolkit", 2007

77 KUROSE, J.F. and ROSS, K.W.: Computer Networking: A Top-Down Approach Featuring the Internet, Boston: Addison-Wesley, 2001.

78 Kuznetsov, Y. and Piccardi, C. Bifurcation analysis of periodic SEIR and SIR epidemic models, Journal of Mathematical Biology 1994.

79 KYAS, O. and CRAWFORD, G.: ATM Networks, Upper Saddle River, NJ: Prentice Hall, 2002.

**80 Lachin, J. Matts, J. Wei, L. "Randomization in Clinical Trials: Conclusions and Recommendations", 1998**

**81 Layton, Timothy P. Information Security: Design, Implementation, Measurement, and Compliance,2007**

**82 Leveille, J. 2002. Epidemic spreading in technological networks. Master's thesis, University of Sussex. 2002.**

**83 Leveille, J. Epidemic spreading in technological networks. Hpl2002287, School of Cognitive and Computing Sciences, University of Sussex at Brighton, Bristol, 2002**

**84 Lin, D. "Inexpensive boot sector virus detection and prevention techniques". 2000**

**85 Ludwig, M. Computer Viruses, Artificial Life and Evolution, 1993**

**86 Mayer, A. Wool, A. and Ziskind, E. : A firewall analysis engine. In Proceedings of the IEEE Computer Society Symposium on Security and Privacy, 2000.**

**87 Mayo, J. Computer Viruses, Windcrest,2000**

**88 McNab, C. Network Security Assessment, 2004**

**89 MILLER, P. and CUMMINS, M.: LAN Technologies Explained, Woburn, MA: Butterworth-Heinemann, 2000.**

**90 Moore, D. and Shannon, C. The spread of the codered worm (crv2), 2005**

**91 Moore, D. The spread of the code-red worm (crv2), 2002**

**92 Moreno, Y. Romualdo Pastor-Satorras, and Alessandro Vespignani. Epidemic outbreaks in complex heterogeneous networks. The European Physical Journal B, 2002.**

**93 Murray, J. D. Mathematical Biology, (2nd, corrected edition). Springer Verlag, New York, 1993**

**94 Murray, W. The application of epidemiology to computer viruses,1978**

**95 Onofrio, A. Manfredi, P. and Salinelli. E. 'Vaccinating behaviour, information, and the dynamics of SIR vaccine preventable diseases' Th. Pop. Biol 2007.**

**96 Onofrio, A. 'Mixed pulse vaccination strategy in epidemic model with realistically distributed infectious and latent times', Applied Mathematics and Computation 2004**

97 Pastor R. -Satorras and Vespignani, A.. Epidemics and immunization in scale-free networks. Handbook of Graphs and Networks: From the Genome to the Internet, 2002.

98 Pastor-Satorras ,R. and Vespignani, A. Epidemic dynamics and endemic states in complex networks. Physical Review E, 2001.

99 PastorSatorras, R and Vespignani, A. Epidemic spreading in scalefree networks. Physical Review Letters, 2001.

100 Pastor-Satorras, R. and Vespignani, A. Epidemic spreading in scale-free networks. Physical Review Letters, 2001.

101 PETERSEN, M. Basic Network Types, Petersen Computer Consulting (http://www.pcc-services.com/), 2003

102 Pfleeger , S. and Bloom, G. Canning spam: Proposed solutions to unwanted email, 2005.

103 Pfleeger, C. Security in Computing. PrenticeHall, Inc, Upper Saddle, NJ , USA, 1997.

104 Pildal J, Chan AW, et al. "Comparison of descriptions of allocation concealment in trial protocols and the publihed report: cohort study", 2005

105 Polo, Luciano. "World Wide Web Technology Architecture: A Conceptual Analysis", 2005.

106 Roberts, Paul F. "Spyware-Removal Program Tagged as a Trap, 2005

107 Ross, S.. Stochastic Processes. Wiley, New York, 1996

108 Salus, P. Casting the Net: from ARPANET to Internet and Beyond. Addison-Wesley, 1995

109 SHIRKY, C. What is p2p... and what isnt't. O'Reilly Network, available online at http://www.oreillynet.com/pub/a/p2p/2000/11/24/shirky1whatisp2p.html, 2000.

110 SHIRKY, C., TRUELOVE, K., DORNFEST, R., and GONZE, L., 2001 P2P Networking Overview, 2001.

111 Shoch, J. and Hupp, J. The "worm" programs–early experience with a distributed computation.

112 Skoudis, E. Malware, Fighting Malicious Code. Computer Networking and Distributed Systems. Prentice Hall, NJ, USA, sixth edition, 2004.

113 Spafford, E. The internet worm program: an analysis, 1989

**114 Staniford, S. Moore,D. Paxson, V and Weaver, N. The top speed of flash worms. In WORM '04: Proceedings of the 2004 ACM workshop on Rapid malcode, 2004**

**115 Staniford, S. Paxson, V. and Weaver, N. How to 0wn the internet in your spare time. In Proceedings of the 11th USENIX Security Symposium, 2002**

**116 Szor P. and Ferrie, P. Hunting for metamorphic. In Proceedings of the Virus Bulleting Conference, 2001.**

**117 Szor, P. The Art of Computer Virus Research and Defense. AddisonWesley, Upper Saddle River, NJ, 2005.**

**118 Tanenbaum, A. "Computer Networks" forth edition, 2002**

**119 Thomas, S. SSL and TLS essentials securing the Web. New York: Wiley, 2000**

**120 Townsley, W. et al.,Layer Two Tunneling Protocol "L2TP", 1999**

**121 Trichopoulos, D.. Epidemiology, principles, methods. Scientific Publications Gr. Parisianos, 1982.**

**122 USENIX. How to own the Internet in your spare time, 2002. To appear in proceedings of the 11th USENIX Security Symposium, 2002**

**123 Vacca, J. Internet Security: Secrets, IDG Books Wolrdwide, 1996**

**124 Vandenbroucke, J. In defense of case reports and case series. Ann Intern Med, 2001**

**125 Veiler, R. Professional Rootkits, 2007**

**126 Volchenkov, D. Volchenkova, L. and Blanchard, P. Epidemic spreading in a variety scalefree networks, 2002.**

**127 Wang, Y. Chakrabarti, D. Wang, C. and Faloutsos, C.. Epidemic spreading in real networks: An eigenvalue viewpoint. In SRDS, 2003.**

**128 Watts, S. Epidemics and History. Yale University Press, 1999.**

**129 Weaver, N. Paxson, V, and Staniford, S. A worstcase worm. In Proceedings of the Third Annual Workshop on Economics and Information Security, 2004.**

**130 Weiss, G. Dishon, M. On the asymptotic behavior of the stochastic and deterministic models of an epidemic.**

**131 Williamson, M. Leveille J. An epidemiological model of virus spread and cleanup. Information Infrastructure Laboratory 2003.**

**132 Williamson, M. Throttling viruses: restricting propagation to defeat malicious mobile code. In Proceedings of Applied Computer Security Associates Conference, 2002.**

**133 Wolfram, S. The Mathematica Book, 3rd Edition. Cambridge University Press, New York, 1996**

**134 Zou, C. Gong, W. and Towsley, D. Code red worm propagation modeling and analysis. In Proceedings of the 9th ACM Conference on Computer and Communication Security (CCS), Washington DC, USA, 2002**

**135 Zou, C. Towsley, D. and Gong, W. Email virus propagation modeling and analysis. Technical report, Umass ECE TR03CSE04, 2003**

**136** Αλεξόπουλος, Α. Λαδογιάννης, Γ. "Τηλεπικοινωνίες και Δίκτυα Υπολογιστών" **1987**

**137** Κομνηνός Θεόδωρος, Σπυράκης Παύλος, Ασφάλεια Δικτύων και Υπολογιστικών Συστημάτων, Ελληνικά Γράμματα, **2002**

**138 Jose Vilches, TechSpot.com, The rise of the rootkits has begun, dec 2007 http://www.techspot.com/news/28244-prevx-the-rise-of-the-rootkits-has-begun.html**

**139** Αλέξανδρος Γ., **securitylabs, Phishing** επίθεση «χτυπά» την **Citibank, 2008 http://www.securitylabs.gr/content/view/345/29/**