ΤΕΧΝΟΛΟΓΙΚΟ ΕΚΠΑΙΔΕΥΤΙΚΟ ΙΔΡΥΜΑ ΗΠΕΙΡΟΥ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗ Τ.Ε

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ: ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

ΟΝΟΜΑΤΕΠΩΝΥΜΟ ΣΠΥΔΑΣΤΗ: ΝΤΙΣΙΟΥ ΒΑΣΙΛΙΚΗ

ΑΜ ΣΠΟΥΔΑΣΤΗ: 10755

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΡΙΖΟΣ ΓΕΩΡΓΙΟΣ

Άρτα – 2016 –

ΠΕΡΙΛΗΨΗ

Η παρούσα εργασία ασχολείται με την ασφάλεια δικτύων. Ασχολείται με όλες εκείνες τις μεθόδους και πρωτόκολλα που έχουν αναπτυχθεί κατά καιρούς με απώτερο σκοπό την ασφάλεια των πληροφοριών που διακινούνται στα δίκτυα.
Τα πρωτόκολλα αναφέρονται – όχι με την αναλυτική τους λειτουργία – αλλά σε τόσο έκταση έτσι ώστε να γίνει κατανοητή ο τρόπος λειτουργίας και χρησιμότητας τους.
Σε όσα πρωτόκολλα είναι δυνατόν γίνεται και μια παρουσίαση παραδείγματος.
Τέλος, θα δοθούν συμπεράσματα βασισμένα σε όλα αυτά που χρησιμοποιήθηκαν (άρθα, εργασίες, βιβλία κτλ) για την εργασία.

ΛΙΣΤΑ ΕΙΚΟΝΩΝ:

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Στην παρούσα εργασία , θα ασχοληθούμε τα δίκτυα και την ασφάλεια τους.

Το πρώτο κεφάλαιο αναφέρεται στις εισαγωγικές έννοιες των δικτύων υπολογιστών. Δεν μπορούμε να αφιερώσουμε χρόνο στην ασφάλεια δικτύων υπολογιστών , εάν προηγουμένως δεν υπάρχουν οι βάσει. Έτσι, λοιπόν, σε αυτό το κεφάλαιο γίνεται αναφορά σε όλες εκείνες τις βασικές έννοιες και γνώσεις που πρέπει να γνωρίζει κάποιος πριν προχωρήσει στην ανάγνωση της παρούσας εργασίας.
Πώς ξεκίνησαν τα δίκτυα , τι περιλαμβάνουν τα δίκτυα και ποιες είναι οι βασικές αρχιτεκτονικές που υποστηρίζουν καθώς επίσης και τα είδη των δικτύων αναλύονται στο πρώτο κεφάλαιο
Στη συνέχεια , στο δεύτερο κεφάλαιο θα γίνει μια αναφορά σε όλους αυτούς τους κινδύνους που αντιμετωπίζουν τα δίκτυα. Οι κίνδυνοι και οι απειλές είναι αυτοί οι παράγοντες που έδρασαν καταλυτικά στην δημιουργία της έννοιας ασφάλεια δικτύων. Άλλωστε , γνωρίζοντας από τι κινδυνεύουμε μπορούμε και από μόνοι μας να λάβουμε κάποια μέτρα προστασίας και ασφάλειας.
Στο τρίτο και τελευταίο κεφάλαιο , αναλύονται οι μέθοδοι που χρησιμοποιούνται για την ασφάλεια δικτύων. Η επισκόπηση αυτών των μεθόδων ξεκινάνε με τον όρο κρυπτογράφηση.
Η κρυπτογράφηση ήταν γνωστή και στην αρχαιότητα με πιο απλή μορφή αυτό είναι σίγουρο. Ένα χαρακτηριστικό παράδειγμα κλασικής μεθόδου κρυπτογράφησης είναι ο Αλγόριθμος Κρυπτογράφησης του Καίσαρα. Αυτός ο αλγόριθμος δεν περιλαμβάνει τίποτα άλλο παρά την ολίσθηση των γραμμάτων των μηνύματος προς τα αριστερά. Όπως είναι φυσικό, ένας τέτοιος αλγόριθμος για το γραπτό λόγο να είναι λίγο επίπονος για τα υπολογιστικά συστήματα όμως δεν επαρκεί. Στη συνέχεια, και ξεπερνώντας τους εθιμοτυπικούς αλγορίθμους κρυπτογράφησης , γίνεται αναφορά στις σύγχρονες μεθόδους.
Αναλύονται εκτενώς η κάθε μια κατηγορία. Είναι βασικό να παρατηρηθεί ότι αυτοί οι αλγόριθμοι είναι θεμελιώδεις. Και αυτό διότι είναι οι βάσεις για όλες τις μεθόδους ασφαλείας και πρωτοκόλλων που θα αναφερθούν παρακάτω.
Σε κάθε ενότητα του τρίτου κεφαλαίου υπάρχουν και τα αντίστοιχα συμπεράσματα από τις μεθόδους και τα πρωτόκολλα που παρουσιάζονται.
Για περαιτέρω εμβάθυνση σε όλα αυτά που θα παρουσιαστούν στην παρούσα

εργασία συνίσταται η επισκόπηση της βιβλιογραφίας και του παραρτήματος με τις ιστοσελίδες καθώς επίσης και η παρακολούθηση συγγραμμάτων που αναφέρονται στην Κρυπτογραφία.

ΚΕΦΑΛΑΙΟ 1ο: ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ – ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ

Στο κεφάλαιο αυτό , θα προσπαθήσουμε να δώσουμε μια εικόνα για την έννοια των δικτύων που συναντάται στην καθημερινότητα μας τόσο συχνά. Θα ξεκινήσουμε από την ιστορική αναδρομή και θα συνεχίσουμε με την αναλυτική αναφορά των τύπων δικτύων έτσι ώστε να είμαστε σε θέση , στα επόμενα κεφάλαια να αναλύσουμε τους κινδύνους και να επικεντρωθούμε στην ασφάλεια δικτύων.

1.1. ΙΣΤΟΡΙΚΗ ΑΝΑΔΡΟΜΗ: ΠΩΣ ΦΤΑΣΑΜΕ ΣΤΑ ΣΗΜΕΡΙΝΑ ΔΙΚΤΥΑ

Τα δίκτυα , από το Internet έως και τα ασύρματα δίκτυα που όλοι σήμερα χρησιμοποιούμε κατά κόρον σήμερα, δεν είχαν αθόλου την μορφή που γνωρίζουμε σήμερα. Αλλά, ας πάρουμε τα πράγματα με τη σειρά τους. Καταρχάς , θα πρέπει να γίνει σαφές τι εννοούμε με τον όρο «Δίκτυο» και συγκεκριμένα «Δίκτυα υπολογιστών» στο κόσμο της Πληροφορικής. «*Δίκτυα υπολογιστών καλούμε ένα σύνολο ανεξάρτητων διασυνδεδεμένων υπολογιστών και άλλων ηλεκτρονικών συσκευών (εκτυπωτές, modem, plotters,) που είναι ικανές να ανταλλάξουν πληροφορίες.» {Πηγή: Γεωργίου κα,}*.
Αφού δόθηκε ο ορισμός των Δικτύων Υπολογιστών ας ξεκινήσουμε την ιστορική μας αναδρομή για αν δούμε τα βήματα και ι προσπάθειες που χρειάστηκαν για να φτάσουμε στα σημερινά δεδομένα.

1.1.1. ΤΟ ΔΙΚΤΥΟ ARPANET ΚΑΙ ΤΟ ΥΠΟΥΡΓΕΙΟ ΑΜΥΝΗΣ ΤΩΝ ΗΠΑ

Η πρώτη προσπάθεια δημιουργίας ενός δίκτυο, δηλαδή την σύνδεση δύο υπολογιστών με απώτερο σκοπό την αποστολή δεδομένων. Και η προσπάθεια αυτή ούτε ο χρόνος ούτε ο τόπος ήταν τυχαία. Η χώρα που ξεκίνησε το επιχείρημα αυτό ήταν η Αμερική κατά τη διάρκεια του ψυχρού πολέμου, και ο σκοπός αυτού του εγχειρήματος ήταν να προστατέψουν τις πληροφορίες τους από τους Ρώσους. Έτσι, λοιπόν, δημιούργησαν την ομάδα ARPA (Advanced Research Project Agency) η οποία ανήκε στο Υπουργείο Αμύνης των ΗΠΑ.

Υπό αυτές τις συνθήκες, λοιπόν, το 1969 κατασκευάστηκε το πρώτο δίκτυο στον κόσμο τον γνωστό και ως ARPANET το οποίο και αποτελεί τον

προάγγελο του Internet. Το δίκτυο αυτό ήταν η σύνδεση 4 κόμβων οι οποίοι βρίσκονταν σε πανεπιστήμια της Αμερικής. Η ταχύτητα του 'πρωτόγονου' αυτού δικτύου ήταν μόλις τα 50 kbps , ταχύτητα που αποτελεί σήμερα σχεδόν εφιαλτική, αλλά για το πρώτο δίκτυο στο κόσμο αποτελούσε την έναρξη των dialup υπηρεσιών.

Η πορεία και η εξέλιξη του δικτύου αυτού δεν σταματάει εκεί. Στη συνέχεια, το δίκτυο αυτό πήγε στα χέρια της επιστημονικής κοινότητας των πανεπιστημίων η οποία κατάφερε να φτάσει στο σημερινό Διαδίκτυο (Internet). Ταυτόχρονα, κατασκευάστηκαν, πρωτόκολλα για την υποστήριξη του δικτύου αυτού, πρωτόκολλα τα οποία έως και σήμερα στον 21^{ο} αιώνα αποτελούν τον ακρογωνιαίο λίθο των δικτύων υπολογιστών.

1.2. ΒΑΣΙΚΑ ΔΟΜΙΚΑ ΣΤΟΙΧΕΙΑ ΤΩΝ ΔΙΚΤΩΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Μετά την σύντομη ιστορική αναδρομή στην απαρχή των δικτύων, καλό θα ήταν σε αυτό το σημείο να γίνει αναφορά στα δομικά στοιχεία από τα οποία απαρτίζονται όλα τα δίκτυα έτσι ώστε να είμαστε σε θέση στη συνέχεια να αναλύσουμε και τα είδη δικτύων που συναντάμε σήμερα.

Δομικά στοιχεία , τα οποία και συναντάμε σε όλο το φάσμα των δικτύων που θα δούμε και παρακάτω, είναι τα εξής:

- Υπολογιστικό σύστημα το οποίο μπορεί να είναι από έναν υπολογιστή έως και έναςserver (εξυπηρετητής).
- Κόμβος (node). Κάθε συσκευή που συμμετέχει σε ένα δίκτυο.
- Περιφερειακές συσκευές δίκτυο όπως είναι οι εκτυπωτές.
- Υποδίκτυο επικοινωνίας που αφορά τον τρόπο με τον οποίο γίνεται η σύνδεση των γραμμών μετάδοσης . *{Πηγή: Πολυμέσα- Δίκτυα}*.

1.3. ΠΡΩΤΟΚΟΛΛΑ

Κάθε δίκτυο για να μπορέσει να αποδώσει τα μέγιστα, πρέπει να ακολουθεί κάποιους κανόνες. Αυτοί οι κανόνες για τη συμπεριφορά του δικτύου όσο αφορά την κίνηση των δεδομένων ονομάζονται πρωτόκολλα. Όπως αναφέρθηκε και προηγουμένως, από το πρώτο είδος δικτύου, το ARPANET γεννήθηκε η ανάγκη κατασκευής πρωτοκόλλων. Συγκεκριμένα, στο

ARPANET χρησιμοποιήθηκε το πρωτόκολλο NCP που όμως παρουσίαζε αρκετά προβλήματα.

Αυτό που πρέπει να καταλάβουμε με τα δίκτυα είναι ότι χωρίζονται σε επίπεδα. Η στρωματοποίηση των επιπέδων ενός δικτύου είναι βασική προϋπόθεση για να μπορέσει να εξυπηρετήσει το σκοπό του. Για την επικοινωνία μεταξύ αυτών των επιπέδων δημιουργήθηκαν τα πρωτόκολλα. Είναι , όπως προαναφέραμε κανόνες για το πώς θα μεταδοθεί πχ η πληροφορία στο φυσικό μέσο, ή ακόμα ακόμα πως θα αποδοθεί στον χρήστη η πληροφορία αφού γνωρίζουμε ότι 'ταξιδεύει' με τη μορφή δυαδικών ψηφίων. Για αυτό και είναι ιδιαίτερα σημαντικό να αναφέρουμε τους βασικούς αντιπρόσωπους πρωτοκόλλων, ή καλύτερα ομάδα πρωτοκόλλων ξεκινώντας από το μοντέλο αναφοράς OSI και στη συνέχεια στο μοντέλο αναφοράς TCP/IP το οποίο και χρησιμοποιείται κατά κόρον στα σημερινά δίκτυα..

1.3.1. ΤΟ ΜΟΝΤΕΛΟ ΑΝΑΦΟΡΑΣ OSI.

Το μοντέλο OSIήταν μια προσπάθεια για την ομαδοποίηση των πρωτοκόλλων στα διάφορα επίπεδα που υπήρχαν στα έως τότε δίκτυα. Προτάθηκε από τον Διεθνή Οργανισμό Τυποποίησης (ISO) το 1984. Το μοντέλο OSI ήταν κατάλληλο επίσης για την διασύνδεση δικτύων μεταξύ τους. Αποτελούνταν από 7 επίπεδα τα οποία και φαίνονται στην παρακάτω εικόνα.

Εικόνα 1 - Επίπεδα Μοντέλου OSI*{Πηγή: http://panacea.med.uoa.gr }*

Ας αναλύσουμε λίγο τα παραπάνω επίπεδα για να γίνει κατανοητή η λειτουργία του μοντέλου αναφοράς.OSI.

- **Φυσικό επίπεδο:** Είναι το χαμηλότερο επίπεδο στο μοντέλο αυτό και ασχολείται με τη μετάδοση πληροφορίας μέσω των υλικών που χρησιμοποιούνται στο δίκτυο (ή δίκτυα).
- **Επίπεδο Ζεύξης Δεδομένων:**Είναι το επίπεδο το οποίο ελέγχει την ορθή και αξιόπιστη μετάδοση της πληροφορίας χρησιμοποιώντας πλαίσιο επιβεβαίωσης (acknowledgmentframe).
- **Επίπεδο Δικτύου:**Είναι υπεύθυνο για τον καθορισμό της διαδρομής και τελικώς τη δρομολόγηση των πακέτων. Εδώ αξίζει , να αναφέρουμε ότι τα δεδομένα , που όπως είναι γνωστό, είναι ακολουθίες από 0 και 1 , και τεμαχίζονται στα λεγόμενα πακέτα με σκοπό να μπορέσουν να μεταδοθούν στο φυσικό μέσο το οποίο έχει περιορισμένο εύρος.
- **Επίπεδο Μεταφοράς:** Είναι το επίπεδο στο οποίο γίνεται ο τεμαχισμός της πληροφορίας σε πακέτα που αναφέρθηκε παραπάνω. Επίσης, εξασφαλίζει ότι όλα τα πακέτα φτάνουν σωστά στο άλλο άκρο της επικοινωνίας.
- **Επίπεδο Συνόδου (ή Συνδιάλεξης):**Ουσιαστικά είναι αυτό το επίπεδο το οποίο και 'ανοίγει' διόδους επικοινωνίας μεταξύ του παραλήπτη και του αποστολέα.

- **Επίπεδο Παρουσίασης:**Το επίπεδο αυτό μετατρέπει τα δεδομένα που καταφθάνουν σε αυτά, μορφοποιώντας τα κατάλληλα.
- **Επίπεδο Εφαρμογής:**είναι το επίπεδο με το οποίο έρχεται σε επαφή ο χρήστης. Σε αυτό η παρουσίαση των δεδομένων γίνεται σε μορφή κατανοητή από το χρήστη. Αποτελείται από πολλά πρωτόκολλα όπως το HTTP (Hyper – Text Transfer Protocol) το οποίο τα συναντάμε σε οποιοδήποτε φυλλομετρήτη όταν θέλουμε να επισκεφτούμε μια ιστοσελίδα.

1.3.2. ΜΟΝΤΕΛΟ ΑΝΑΦΟΡΑΣ TCP/IP.

Το μοντέλο OSI που προαναφέρθηκε , χρησιμοποιείται και σήμερα αλλά σε σπάνιες περιπτώσεις. Το μοντέλο πρωτοκόλλων, που χρησιμοποιείται σε οποιοδήποτε δίκτυο θέλουμε να κατασκευάσουμε, δεν είναι παρά το μοντέλο αναφοράςTCP/IP. Το μοντέλο αυτό, ήρθε να λύσει τα προβλήματα που είχαν αναπτυχθεί από την εξέλιξη της τεχνολογίας και των δικτύων. Ενώ το μοντέλο αναφοράς OSIέβρισκε πλήρη εφαρμογή σε οποιοδήποτε δίκτυο, όταν προσπαθούσαν να ενώσουν διαφορετικά δίκτυα μεταξύ τους, δυστυχώς το OSI τους εγκατέλειπε. Για να λυθεί αυτό τα πρόβλημα, δηλαδή να μπορούν να συνδεθούν διάφορα δίκτυα διαφορετικά μεταξύ τους, όπως πχ δίκτυα ασύρματα και δίκτυα ενσύρματα, οι δίκτυα με διαφορετικές τοπολογίες, προτάθηκε και κατασκευάστηκε το μοντέλο αναφοράς TCP/IP.

Το μοντέλο αυτό είναι μια ομάδα πρωτοκόλλων που το κάθε ένα είναι προσανατολισμένο για μια συγκεκριμένη δραστηριότητα ανάλογα του επιπέδου που βρίσκεται. Τα επίπεδα στο μοντέλο αυτό είναι 4 αντί 7 και είναι τα εξής:

Εικόνα 2 - Μοντέλο OSIvsΜοντέλο TCP/IP{*Πηγή:* ***http://docplayer.gr/10016887-Kefalaio-7-7-1-7-4-e-p-a-n-a-l-i-ps-i-epikoinoniako-ypodiktyo-tcp-udp-sel-220-241.html*** }

Όπως παρατηρούμε και στην Εικόνα 2, ορισμένα επίπεδα του μοντέλου OSI ενσωματώθηκαν σε ένα στο αντίστοιχο μοντέλο TCP/IP. Ένα από τα σημαντικά πλεονεκτήματα του μοντέλουTCP/IP είναι ότι το τελευταίο επίπεδο δεν έχει ρητές αναφορές στο τρόπο διασύνδεσης και αυτό του επιτρέπει να χρησιμοποιείται σε οποιοδήποτε είδους δικτύου. Και αυτός είναι ο λόγος για τον οποίο και έχει καθιερωθεί.

Προαναφέραμε ότι αυτό το μοντέλο αναφοράς είναι μια ομάδα πρωτοκόλλων που χρησιμοποιούνται ανά επίπεδο. Σε αυτό το μοντέλο συναντάμε, γνωστά και ευρέως χρησιμοποιημένα πρωτόκολλα όπως το HTTP. Ας δούμε όμως, πιο αναλυτικά, ποια είναι τα πρωτόκολλα αυτά και πώς ακριβώς χρησιμοποιούνται.

- **Επίπεδο Πρόσβασης Δικτύου:** Είναι το χαμηλότερο επίπεδο στο μοντέλο αυτό. Εκεί συναντάμε πρωτόκολλα όπως το Ethernet το οποίο είναι πρωτόκολλο για τα τοπικά δίκτυα.
- **Επίπεδο Δικτύου:** Σε αυτό το επίπεδο συναντάται , το πρωτόκολλο IP (Internet Protocol) το οποίο χρησιμοποιείται για την δρομολόγηση των πακέτων τόσο μέσα στο ίδιο το δίκτυο τόσο και ανάμεσα σε διάφορα δίκτυα συνδεδεμένα μεταξύ τους. Είναι υπεύθυνο ουσιαστικά για την μετάδοση της πληροφορίας από τον αποστολέα στον παραλήπτη. Σε αυτό το επίπεδο

υπάρχει και το πρωτόκολλο ICMP (Interne tControl Message Protocol) το οποίο παράγει μηνύματα προς τα πρωτόκολλα του επόμενου επιπέδου για τυχόν προβλήματα στο δίκτυο.

- **Επίπεδο Μεταφοράς:** Είναι το επίπεδο στο οποίο κυρίως χρησιμοποιείται το TCP (Transfer Control Protocol). Το πρωτόκολλο, είναι πάρα πολύ σημαντικό γιατί είναι το πρωτόκολλο το οποίο εξασφαλίζει την αξιόπιστη μεταφορά των πακέτων. Είναι αυτό που περιμένει ανταπόκριση από τον αποστολέα , για την λήψη των πακέτων. Εάν αποτύχει κάποιο πακέτο, είναι υπεύθυνο για την επαναμετάδοση του στο δίκτυο. Το πρωτόκολλο αυτό εξασφαλίζει ουσιαστικά την μεταφορά της πληροφορίας χωρίς απώλειες . για αυτό και χρησιμοποιείται από πολλές εφαρμογές όπως πχ από το email. Βέβαια, εδώ συναντάμε και το UDP (User Datagram Protocol) το οποίο δεν είναι τόσο αξιόπιστο με το προαναφερθέν πρωτόκολλο και ούτε επαναμεταδίδει τυχόν απολεσθέντα πακέτα πληροφορίας. Επομένως, ποιος ο λόγος ύπαρξης του? Επειδή το TCP είναι επιφορτισμένο με πολλές ευθύνες και επειδή καθυστερεί (κλάσματα δευτερολέπτου) τη μετάδοση ολόκληρης της πληροφορίας, όταν δεν είναι σημαντική η ποιότητα της πληροφορίας αλλά η ταχύτητα της μετάδοσης της τότε χρησιμοποιείται το UDP. Χαρακτηριστικό παράδειγμα είναι η μετάδοσης φωνής πχ Onlineραδιόφωνο.
- **Επίπεδο Εφαρμογής:** Το ανώτερο επίπεδο του μοντέλου αυτού και το επίπεδο με το οποίο έρχεται σε επαφή ο χρήστης. Σε αυτό το επίπεδο , χρησιμοποιεί εφαρμογές που αυτές με τη σειρά τους χρησιμοποιούν τα δικά τους πρωτόκολλα προκειμένου να εκπληρώσουν τη χρηστικότητα τους. Κάποια από αυτά τα πρωτόκολλα είναι:
  - **HTTP(Hypertext Transfer Protocol):** Πρωτόκολλο το οποίο χρησιμοπθοιείται για τη μεταφορά υπερκειμένου μέσω του Παγκόσμιου Ιστού με τη χρήση των φυλλομετρητών (browsers). Το συναντάμε σε κάθε πληκτρολόγηση διεύθυνσης μιας ιστοσελίδες στο αντίστοιχο πλαίσιο διεύθυνσης του φυλλομετρητή. Υπάρχει και το HTTPS το οποίο παρέχει ασφαλή σύνδεση και την οποία θα αναλύσουμε παρακάτω.
  - **SMTP(Simple Message Transfer Protocol):**Είναι το πρωτόκολλο του οποίο ‘κρύβεται’ πίσω από την αποστολή οποιουδήποτε ηλεκτρονικού ταχυδρομείου.

- **FTP(File Transfer Protocol):** Πρωτόκολλο που χρησιμοποιείται για τη μεταφορά αρχείων από ένα υπολογιστή που λειτουργεί ως server σε έναν άλλο που λειτουργεί ως client.
- **VOIP(Voice Over Internet Protocol):** Είναι το πρωτόκολλο το οποίο χρησιμοποιείται στη τηλεφωνία μέσω διαδικτύου. Η πιο γνωστή εφαρμογή στην οποία βρίσκει εφαρμογή το πρωτόκολλο αυτό δεν είναι άλλη από το SKYPE. Εδώ αξίζει να αναφερθεί ότι το SKYPE χρησιμοποιήθηκε αρχικά για την τηλεφωνία μέσω διαδικτύου. Δηλαδή, παρέχοντας χαμηλές χρεώσεις μπορούσε οποιοσδήποτε να καλέσει σε οποιοδήποτε σταθερό στο κόσμο αρκεί να διαθέτει πρόσβαση στο διαδίκτυο και ακουστικά και μικρόφωνο. Η σημερινή χρήση του που συμπεριλαμβάνει και το βίντεο ήταν μια προσθήκη αρκετά αργότερα όταν η τεχνολο9ία φυσικών μέσων επέτρεψε την μετάδοση εικόνας.

Εννοείται ότι υπάρχουν πληθώρα άλλων πρωτοκόλλων σε αυτό το επίπεδο όμως επικεντρωθήκαμε στα πιο ‘διάσημα’ πρωτόκολλα του.

1.4. ΚΑΤΗΓΟΡΙΟΠΟΙΗΣΗ ΔΙΚΤΥΩΝ

Στη συνέχεια, θα γίνει αναφορά για την κατηγοριοποίηση των δικτύων. Θα επικεντρωθούμε περισσότερο σε δύο κατηγοριοποιήσεις που αφορούν την τεχνολογία μετάδοσης και η κλίμακα των δικτύων.

- Κατηγοριοποίηση με βάση την τεχνολογία μετάδοσης.
  - Συνδέσεις εκπομπής.

    Σε αυτές τις συνδέσεις, το δίκτυο (ή τα δίκτυα) έχουν ένα κανάλι επικοινωνίας. Αυτό σημαίνει ότι όλα τα πακέτα πληροφορίες θα περάσουν από τους υπολογιστές του δικτύου μέχρι να φτάσουν στον αποστολέα. Κάθε φορά κάθε υπολογιστής λαμβάνει το πακέτο και εξετάζει εάν το πακέτο προορίζεται για αυτόν. Εάν ναι, τότε το λαμβάνει και αποδεσμεύει το κανάλι από το πακέτο. Διαφορετικά , το

επανατοποθετεί στο κανάλι για τον επόμενο προορισμό που θα ακολουθήσει την ίδια διαδικασία.

- Συνδέσεις από σημείο σε σημείο.

  Σε αυτές τις συνδέσεις το πακέτο για να φτάσει στο προορισμό του πρέπει να περάσει από άλλους ενδιάμεσους σταθμούς καθώς επίσης και ενδιάμεσα άλλα δίκτυα.

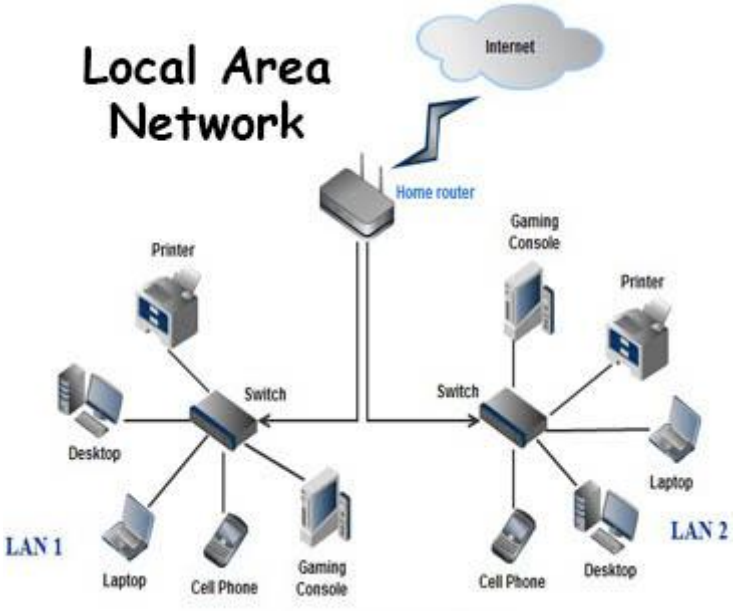
- Κατηγοριοποίηση με βάση την κλίμακα.

Ανάλογα με την περιοχή που καλύπτουν τα δίκτυα κατατάσσονται στα εξής:

- Τοπικά Δίκτυα (LAN – Local Area Network).

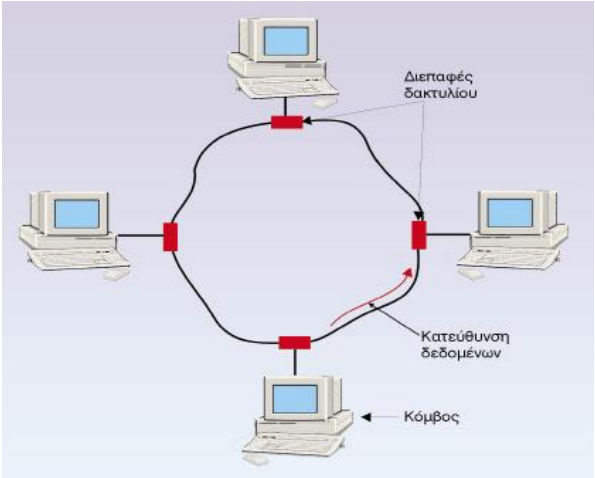
  Τα δίκτυα αυτά συνήθως είναι ιδιωτικά. Έχουν εύρος από μια αίθουσα, ένα κτίριο μέχρι κάποια , λίγα μεν, χιλιόμετρα. Οι ταχύτητες σε αυτά τα δίκτυα κυμαίνονται από MB/s έως και κάποια GB/s.

  Χρησιμοποιούνται από εταιρείες έτσι ώστε να έχουν πρόσβαση σε κοινόχρηστους πόρους όπως εκτυπωτές.



Εικόνα 3 - Τοπικά Δίκτυα (LAN) {*Πηγή:* ***http://www.computer-networking-success.com/computer-lan-network.html#sthash.kQ8L5H6l.dpbs*** }

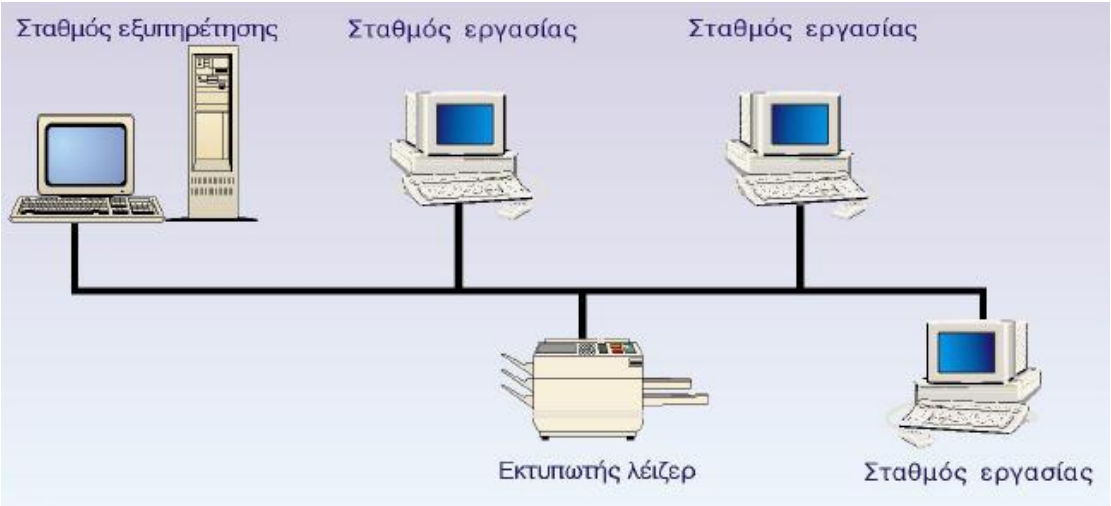
Χαρακτηριστικό των τοπικό δικτύων είναι η τοπολογία τους. Τοπολογία είναι ο τρόπος με τον οποίο τοποθετούνται οι υπολογιστές και όχι μόνο και ουσιαστικά καθορίζουν και τον τρόπο μετάδοσης της πληροφορίας. Το πρώτο είδος τοπολογίας ονομάζεται δακτύλιος (Token Ring).



Εικόνα 4 - Τοπολογία Δακτυλίου. {*Πηγή:* ***https://diktuateecr.wordpress.com***}

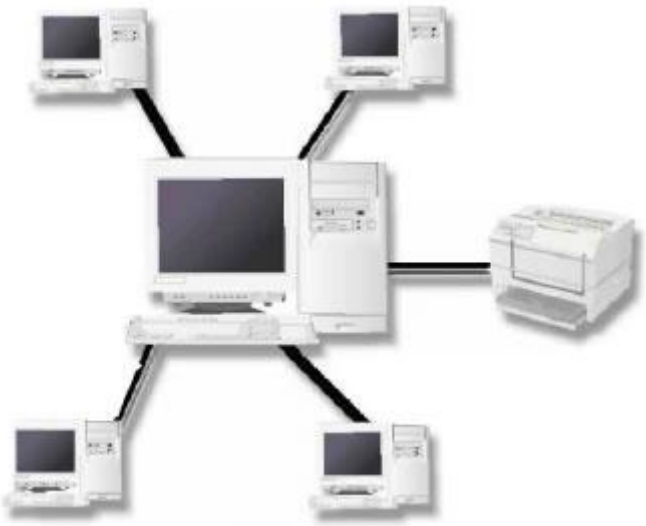
Το χαρακτηριστικό αυτής της τοπολογίας είναι ότι κάθε συσκευή συνδέεται κυκλικά στο δίκτυο. Τα πακέτα θα αναγκαστούν να περάσουν ίσως και από όλες τις συσκευές μέχρι το πακέτο να καταλήξει στον σωστό αποδέκτη. Αυτός με τη σειρά του θα το στείλει πάλι πίσω στον αποστολέα για να το αποσύρει από το δίκτυο.

Άλλη τοπολογία η οποία χρησιμοποιείται είναι η τοπολογία Διαύλου ή Αρτηρίας (Bus).Όπως αφήνει να εννοηθεί η ονομασία της τοπολογίας, όλες οι συσκευές που δικτύου συνδέονται στη σειρά με ένα καλώδιο. Ο αποστολέας ‘στέλνει’ το πακέτο του στο δίαυλο και οι συσκευές ‘ακούνε’ τη πληροφορία. Όμως, το πακέτο θα το κάνει λήψη μόνο η συσκευή που η διεύθυνση του ταυτίζεται με τη διεύθυνση που ‘κουβαλάει’ το πακέτο. Παρακάτω , παρουσιάζεται εικονικά η τοπολογία Δίαυλος (Bus).



Εικόνα 5 - Τοπολογία Διαύλου (Bus) {*Πηγή:* ***https://diktuateecr.wordpress.com*** }

Τελευταίο είδος τοπολογίας είναι η τοπολογία Αστέρα (Star). Σε αυτήν την τοπολογία , οι συσκευές είναι συνδεδεμένες με έναν κεντρικό υπολογιστή. Εάν μια συσκευή θέλει να αποστείλει πληροφορία σε οποιαδήποτε άλλη συσκευή στο δίκτυο τότε αυτή η πληροφορία θα περάσει από τον κεντρικό κόμβο. Ένα από τα βασικά πλεονεκτήματα αυτής της τοπολογίας έναντι των παραπάνω είναι ότι οποιοδήποτε πρόβλημα και να προκύψει σε κάποια συσκευή, το δίκτυο δεν θα 'καταρρεύσει' αλλά θα μπορέσει να λειτουργήσει για τις υπόλοιπες συσκευές στο δίκτυο. Βέβαια, δεν ισχύει το ίδιο εάν το πρόβλημα προκύψει στο κεντρικό κόμβο!!

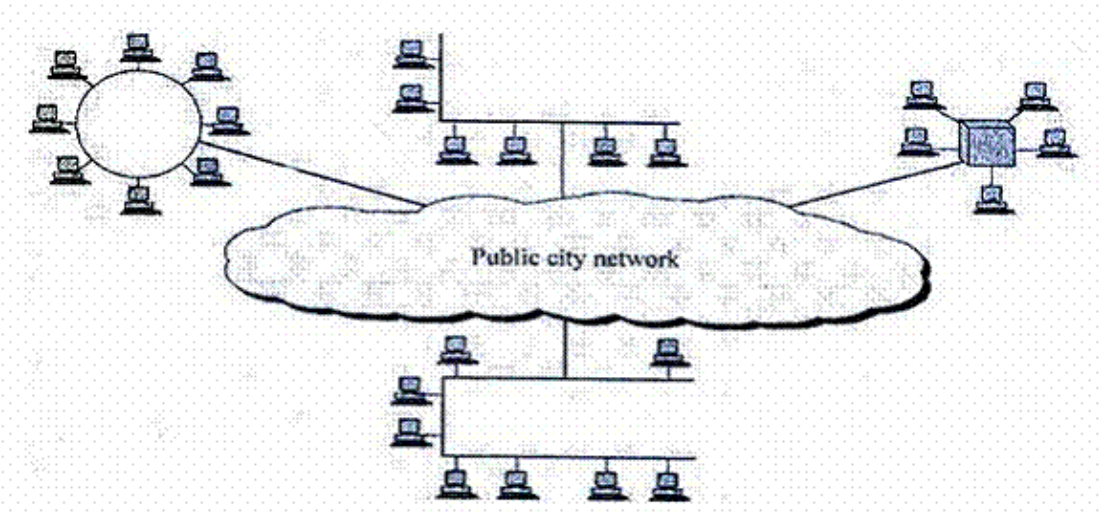


Εικόνα 6 - Τοπολογία Αστέρα {*Πηγή:* ***http://ebooks.edu.gr/modules/ebook/show.php/DSGL-C127/577/3749,16441/***}

Ο τύπος της τοπολογίας που θα επιλεγεί σε κάθε τοπικό δίκτυο εξαρτάται από πολλούς παράγοντες όπως ο πιο βασικός είναι η ταχύτητα αλλά και το κόστος της κατασκευής.

- Μητροπολιτικά Δίκτυα (MAN – Metropolitan Area Networks)

Στην προηγούμενη παράγραφο αναφερθήκαμε στα LAN. Τα μητροπολιτικά δίκτυα (MAN) είναι ουσιαστικά διευρυμένα LAN. Ενώ τα LAN καλύπτουν ένα μέγεθος έως λίγων χιλιομέτρων, τα μητροπολιτικά δίκτυα ουσιαστικά καλύπτουν το μέγεθος μιας πόλης. Μπορούμε να πούμε ότι τα μητροπολιτικά δίκτυα είναι επί της ουσίας πολλά τοπικά δίκτυα συνδεδεμένα μεταξύ τους.



Εικόνα 7 - Μητροπολιτικό Δίκτυο (MAN) {*Πηγή:* ***http://lyk-vatheos.eyv.sch.gr/Ergasies/2006-2007/tech_plir_A/Diktya07.htm*** }

- Δίκτυα Ευρείας Περιοχής (WAN – Wide Area Network)

Προηγουμένως αναφέρθηκε ότι εάν θέλουμε να επικοινωνήσουν οι συσκευές που ανήκουν σε μια εταιρεία προτιμάται η κατασκευή ενός τοπικού δικτύου. Για μια πόλη , προτιμάται ένα μητροπολιτικό δίκτυο. Τι γίνεται στη περίπτωση που θέλουμε συσκευές από διαφορετικά τοπικά δίκτυα , από διαφορετικά μητροπολιτικά δίκτυα με μια αρκετή χιλιομετρική απόσταση μεταξύ τους να επικοινωνήσουν ; Σε αυτήν την περίπτωση, έχουμε να κάνουμε με τα Δίκτυα Ευρείας Περιοχής (WAN). Είναι τα δίκτυα που έχουν πια κατακλύσει την καθημερινότητα μας χωρίς βέβαια να το συνειδητοποιούμε. Τα δίκτυα αυτά είναι ουσιαστικά τοπικά δίκτυα τα οποία

ενώνονται μεταξύ τους μέσω ψηφιακών τηλεφωνικών γραμμών καθώς επίσης και με οπτικές ίνες. Βέβαια, η εξέλιξη των WAN δεν έγινε μέσα σε μια στιγμή αλλά πέρασε από πολλές διαφορετικές τεχνολογίες. Από ιστορικής απόψεως, και όχι μόνο, αναφέρονται αυτοί οι σταθμοί.:

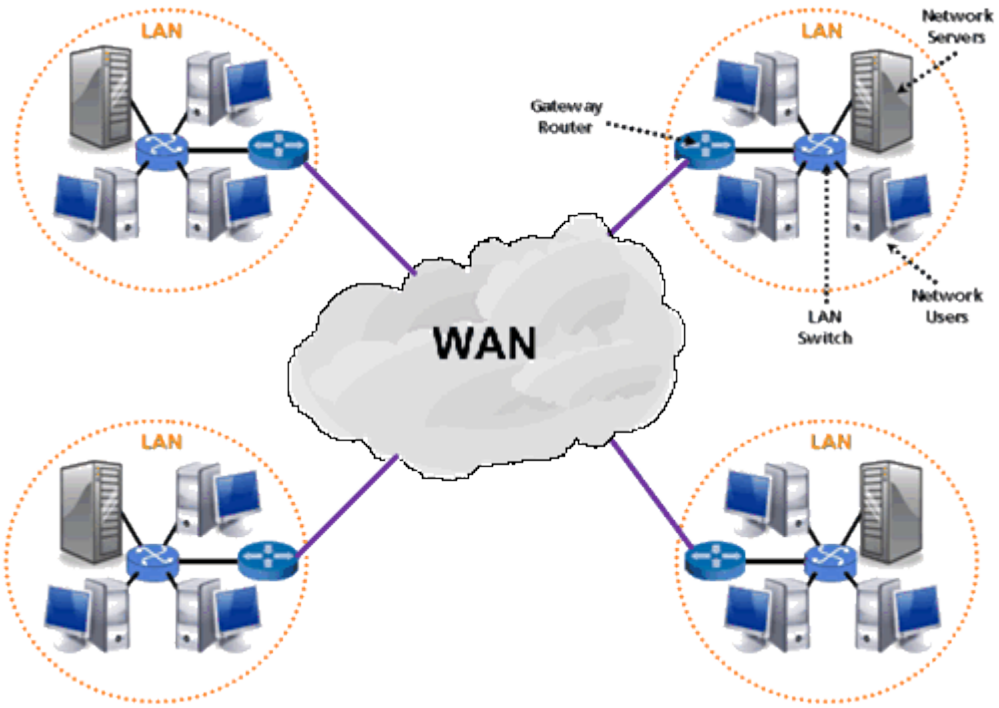
1ος σταθμός: Επιλεγόμενες τηλεφωνικές γραμμές (PSTN)

2ος σταθμός: Μισθωμένες γραμμές

3ος σταθμός: ISDN (Integrated Services Digital Networks – Ψηφιακό Δίκτυο Ενοποιημένων Υπηρεσιών)

4ος σταθμός: xDSL – Ο τελευταίος σταθμός είναι και αυτός που απολαμβάνουμε τα οφέλη του σήμερα.

Χαρακτηριστικό παράδειγμα ενός Δικτύου Ευρείας Περιοχής είναι το γνωστό μας Διαδίκτυο (Internet).



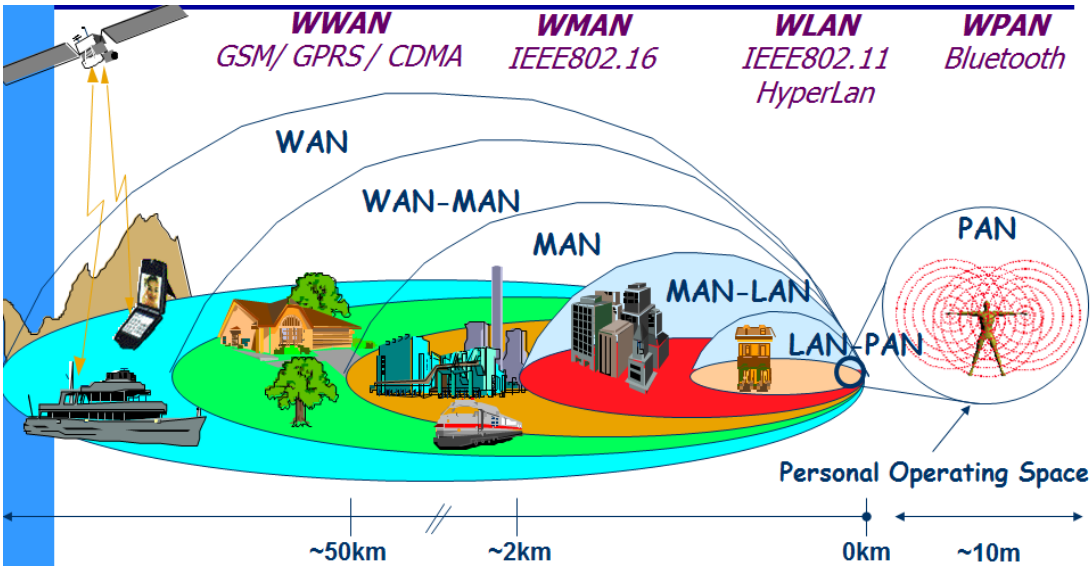
Εικόνα 8 – WAN {*Πηγή:* http://www.netprivateer.com/lanwan.html }

Πριν ολοκληρωθεί αυτή η ενότητα καλό θα ήταν να γίνει και μια αναφορά και στα ασύρματα δίκτυα που τόσο πια χρησιμοποιούμε καθημερινά. Από το σπίτι μας μέχρι στη δουλειά μας ακόμα και στη διασκέδαση μας, παντού πια συνδεόμαστε σε ασύρματα δίκτυα τα λεγόμενα WiFi για να μπορέσουμε να ενημερωθούμε και όχι μόνο. Ας δούμε τι είναι αυτά τα ασύρματα δίκτυα λίγο πιο αναλυτικά.

- Ασύρματα Δίκτυα

  Τα ασύρματα δίκτυα είναι η προσπάθεια μείωσης του κόστος αφού δεν απαιτούν καλωδιακή εγκατάσταση. Βέβαια, ασύρματα δίκτυα αφορούν και τις δορυφορικές επικοινωνίες αλλά και την τηλεπικοινωνία. Παρόλα αυτά, στα ασύρματα δίκτυα υπολογιστών , μπορούν να αναπτυχτούν όλοι οι παραπάνω τύποι δηλαδή μπορούμε να έχουμε ασύρματα τοπικά δίκτυα (WLAN), ασύρματα μητροπολιτικά δίκτυα (WMAN) καθώς και ασύρματα δίκτυα ευρείας περιοχής (WWAN).Εδώ, μπορούμε να αναφέρουμε και τα ασύρματα προσωπικά δίκτυα που είναι γνωστά ως WPAN

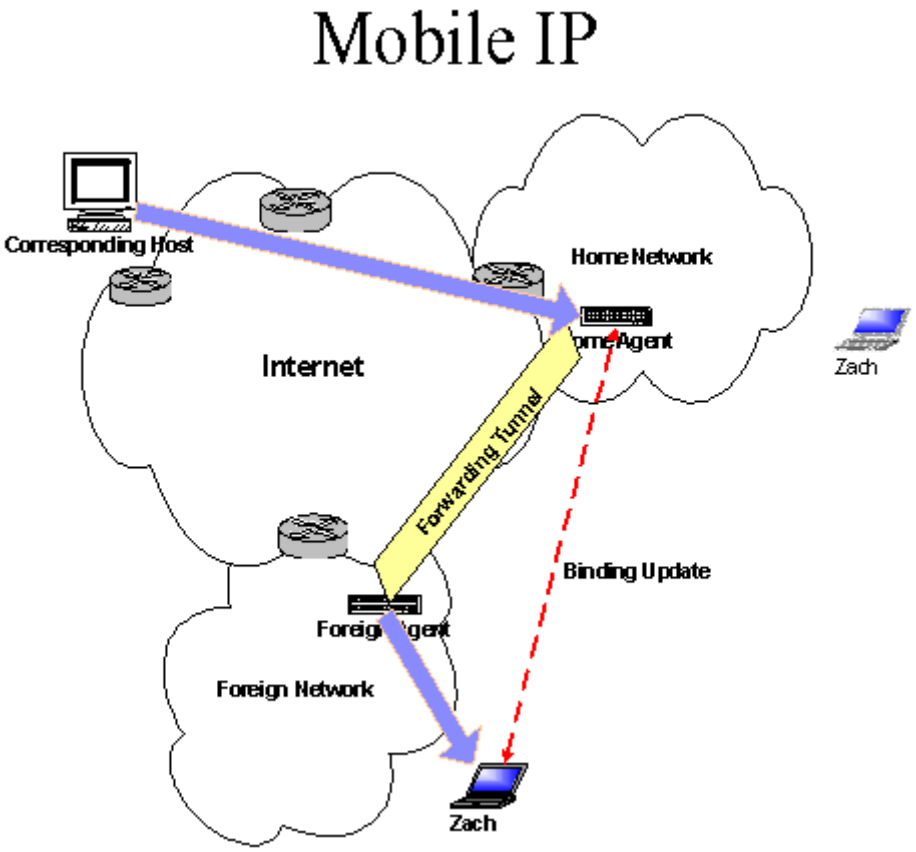
  Ως δίκτυα , για να μπορέσουν να επιτρέψουν την επικοινωνία μεταξύ δύο ή περισσοτέρων συσκευών, απαιτούνται κάποια πρωτόκολλα. Συνήθως, στα ασύρματα δίκτυα κάθε τύπος έχει και το δικό του σύνολο πρωτοκόλλων. Ας δούμε κάποια από αυτά στην παρακάτω εικόνα:



Εικόνα 9 - Πρωτόκολλα ασύρματων δικτύων {*Πηγή:* *http://www.cpe.ku.ac.th/~anan/publications/Publication-Document/WLAN Designand Implementation-KMITNBJan2004.ppt* }

Όπως παρατηρούμε και από την παραπάνω εικόνα, ανάλογα τη απόσταση που θέλουμε να καλύψουμε χρησιμοποιούμε τα αντίστοιχα ασύρματα είδη δικτύων.Επίσης, να σημειωθεί ότι όπου χρησιμοποιείται το πρωτόκολλο IEEE802.11 τότε μιλάμε για το Wi-Fi.

Βέβαια, ασύρματο δίκτυο είναι και το λεγόμενο MobileIP.Το τελευταίο δίκτυο μας παρέχει δυνατότητες σύνδεσης ακόμα και εν κινήσει. Βασικά, αυτό είναι και το βασικό πλεονέκτημα του. Η δυνατότητα του να παρέχει αδιάκοπτη σύνδεση σε συνεχόμενη κίνηση.



Εικόνα10 - Mobile IP Network {*Πηγή:* ***http://seminarprojecttopics.blogspot.gr/2012/06/mobile-ip-for-wireless-devices.html***}

ΚΕΦΑΛΑΙΟ 2ο : ΑΔΥΝΑΜΙΕΣ- ΑΠΕΙΛΕΣ ΣΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Μετά τις εισαγωγικές έννοιες, και πριν προχωρήσουμε στην ανάλυση της ασφάλειας δικτύων, θα πρέπει να γίνει μια αναφορά για ποιο λόγο χρειάζεται και είναι αναγκαία η ασφάλεια στα δίκτυα. Ποιοι είναι αυτοί οι κίνδυνοι και ποιες οι απειλές για τα δίκτυα υπολογιστών.

2.1. ΚΙΝΔΥΝΟΙ ΓΙΑ ΤΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Πριν προχωρήσουμε στους κινδύνους που ελλοχεύουν στα δίκτυα αλλά και την ασφάλεια τους, θα πρέπει να γίνει αναφορά τι πρέπει να προστατευτεί.

Στην καθημερινότητα μας, πολλά πράγματα κινδυνεύουν και τείνουμε να τα προστατέψουμε. Αυτά είναι τα αγαθά μας. Αγαθά μπορεί να είναι χρήματα, κοσμήματα , αυτοκίνητο κοκ. Τι , όμως, κινδυνεύει σε ένα δίκτυο υπολογιστών; Τι θεωρείται αγαθό?

«Πληροφοριακός πόρος ή Αγαθό ονομάζεται κάθε αντικείμενο ή πόρος που ανήκει ή υποστηρίζει ένα πληροφοριακό σύστημα και το οποίο αξίζει να προστατευτεί. Υπάρχουν διάφορες κατηγορίες αγαθών:

- *Φυσικά αγαθά: όπως είναι οι υπολογιστές , Κτήρια κτλ*
- *Αγαθά δεδομένων: Αρχεία*
- *Αγαθά Λογισμικού: Λειτουργικά συστήματα, Λογισμικό εφαρμογών» (Μάγκος, 2007).*

Όπως προαναφέρθηκε, για κάθε αγαθό ελλοχεύουν κάποιοι κίνδυνοι. Ο κίνδυνος στα δίκτυα υπολογιστών αποτελείται από δύο έννοιες. Την έννοια της απειλής και την έννοια της αδυναμίας.

«Με τον όρο αδυναμία αναφερόμαστε στα σημεία του πληροφοριακού συστήματος που αφήνουν περιθώρια για παρεμβάσεις. Συνήθως, οι αδυναμίες οφείλονται σε ανεπάρκεια γνώσεων του ανθρώπινου δυναμικού ή ακόμα και από δυσλειτουργίες του ίδιου του συστήματος.

Με τον όρο απειλές αναφερόμαστε σε γεγονότα ή ενέργειες που έχουν ως αποτέλεσμα την κατάρρευση του συστήματος. Οι απειλές μπορεί να προέρχονται από φυσικά *γεγονότα όπως πυρκαγιές είτε από ανθρώπινες ενέργειες που μπορεί να είναι είτε σκόπιμες είτε τυχαίες»*

(Αρβανίτης, Κόλυβας, Ούτσιος, 2012)

Για τα δίκτυα υπολογιστών , όμως, θα αναφερθούμε εκτενώς στις απειλές και το είδος των απειλών αυτών.

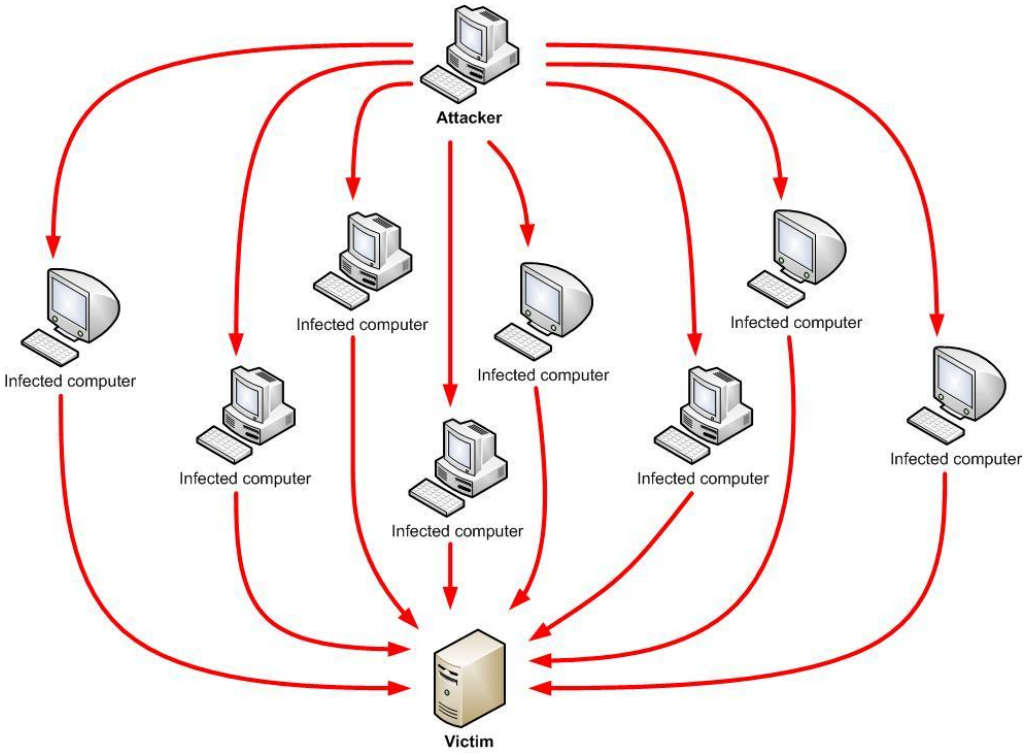
2.2. ΑΝΑΛΥΣΗ ΑΠΕΙΛΩΝ ΓΙΑ ΔΙΚΤΥΑ ΥΠΟΛΟΓΙΣΤΩΝ

Στα δίκτυα υπολογιστών διακινούνται, όπως προαναφέρθηκε στο προηγούμενο κεφάλαιο, τεράστιες ποσότητες πληροφοριών από το ένα άκρο έως το άλλο άκρο του δικτύου. Αυτές τις πληροφορίες έχουν στόχο οι απειλές οι οποίες προέρχονται από εσκεμμένες ανθρώπινες ενέργειες. Ας δούμε κάποιες από αυτές:

- Άρνηση παροχής υπηρεσιών (Denial of Service):

  Σε αυτήν την απειλή επιτυγχάνεται η εξάντληση των πόρων του δικτύου. Ένα παράδειγμα άρνησης παροχής υπηρεσιών είναι όταν κατακλύζεται τα κανάλια του δικτύου μας με άπειρα μηνύματα χωρίς κανέναν παραλήπτη με αποτέλεσμα την υπερφόρτωση του δικτύου. Έτσι, τα ‘πραγματικά’ μηνύματα μπορούμε να πούμε ότι ‘κολλάνε’ στην κίνηση του δικτύου.

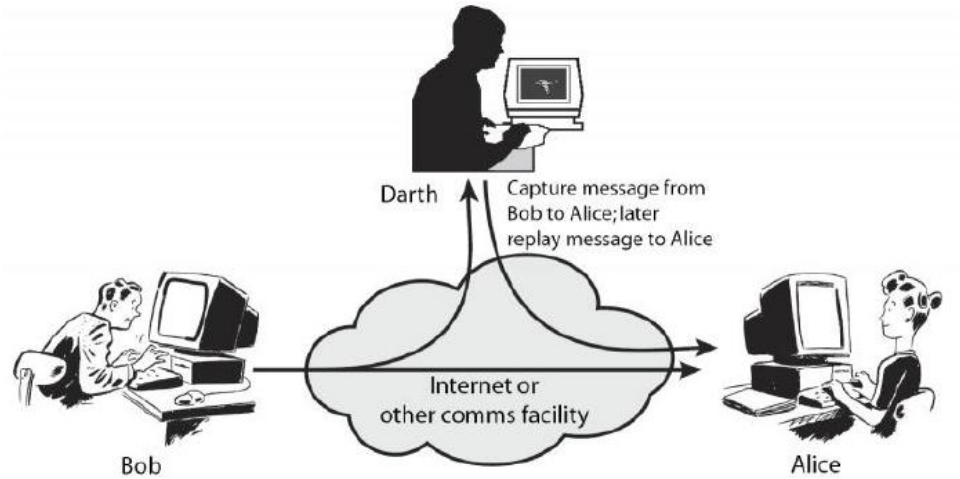
  Ένα άλλο παράδειγμα άρνησης παροχής υπηρεσιών και εξάντλησης των πόρων είναι τα μηνύματα να κατακλύσουν τους δρομολογητές / εξυπηρετητές του εκάστοτε δικτύου με αποτέλεσμα την υπερφόρτωση τους και την τελική του ‘κατάρρευση’ τους και ταυτόχρονα την αναποτελεσματικότητα του δικτύου. Ας μην ξεχνάμε ότι οι δρομολογητές ειδικά όταν έχουμε διαφορετικά δίκτυα που πρέπει να επικοινωνήσουν μεταξύ τους είναι μείζονος σημασίας μια που είναι αυτοί που καθορίζουν τη δρομολόγηση του πακέτου έτσι ώστε να φτάσει στο σωστό προορισμό. Επομένως , μια τυχόν κατάρρευση τέτοιου δρομολογητή θα διακόψει και την επικοινωνία μεταξύ δύο ή περισσοτέρων δικτύων.



Εικόνα 11 - Άρνηση Παροχής Υπηρεσιών (DenialOfService) {*Πηγή: https://www.ebankingabersicher.ch/en/your-security-contribution/extended-protection/denial-of-service-attack* }

- Μεταμφίεση (Masquerade):

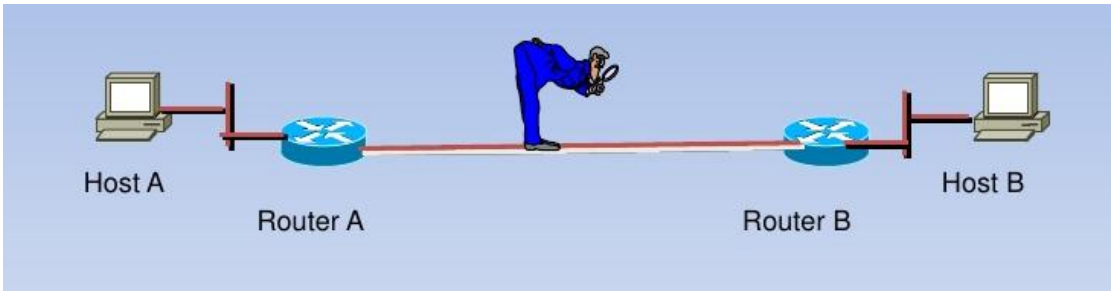
  Η μεταμφίεση είναι η τακτική κατά την οποία ο επιτιθέμενος δεν ανήκεις το δίκτυο μας. Αλλά είναι ικανός να διακινεί την πληροφορία του στο δικό μας δίκτυο και το δίκτυο να τον αναγνωρίζει ως μέλος του. Δεν του αποτρέπει την πρόσβαση και έτσι μπορεί η πληροφορία του να ληφθεί από οποιοδήποτε συσκευή του δικτύου.



Εικόνα 12 - Masquerade(Μεταμφίεση) {*Πηγή: http://www.allsyllabus.com/aj/note/Computer_Science/Computer%20Networks%20-%20II/Unit5/What%20is%20Network%20Security.php#.V7oF86IdpdI* }

- Παρακολούθηση Δικτύου (Network Packet Snifing):

  Γνωρίζουμε ότι στο δίκτυο κινούνται αρκετές πληροφορίες. Κάποιες από αυτές είναι κωδικοποιημένες κάποιες όμως κυκλοφορούν σαν απλό κείμενο. Έτσι, λοιπόν, η παρακολούθηση του δικτύου έχει ως απώτερο σκοπό την υποκλοπή αυτών των πληροφοριών. Κάποιες από αυτές μπορεί να είναι κωδικοί (passwords). Πώς όμως γίνεται η υποκλοπή των πληροφοριών; Η παρακολούθηση του δικτύου γίνεται καθιστώντας έναν υπολογιστή του δικτύου ικανό να δέχεται όλα τα πακέτα του. Όπως γνωρίζουμε, πολλά πακέτα κυκλοφορούν σε ένα δίκτυο αλλά ο προορισμός συνήθως είναι κάποιος (ή κάποιοι) υπολογιστής. Όλες οι υπόλοιπες ενδιάμεσες συσκευές 'βλέπουν' τα πακέτα αλλά επειδή ο προορισμός τους δεν ταιριάζει με τη δική τους (IPaddress / Ethernet address) τα απορρίπτουν. Όμως, στην παρακολούθηση δικτύου γίνεται ακριβώς το αντίθετο. Ο υπολογιστής που έχει καθοριστεί από τον επιτιθέμενο, δέχεται όλα τα πακέτα, τα έχει ως αντίγραφα (την πληροφορία που φέρουν πάντα) και τα επανατοποθετεί στο δίκτυο.

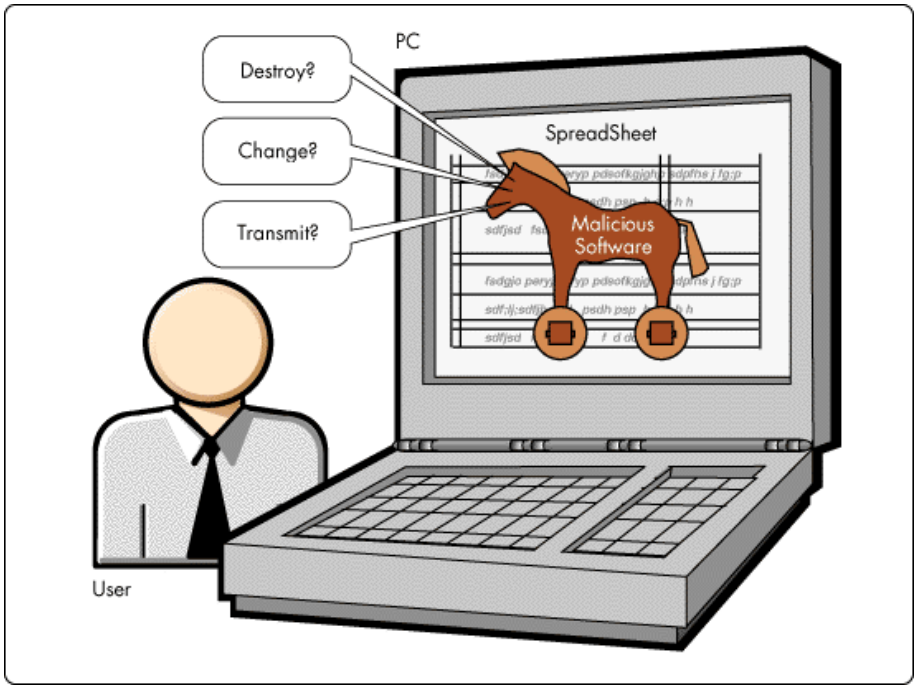


Εικόνα 13 - Παρακολούθηση Δικτύων {*Πηγή:* ***http://www.slideshare.net/superfun/packet-sniffers*** }

- Κακόβουλα Λογισμικά (Malware):

  Σε οποιοδήποτε δίκτυο, όπως και στο Διαδίκτυο , μπορούμε να συναντηθούμε κακόβουλα λογισμικά. Κακόβουλα λογισμικά θεωρούνται εκείνα τα προγράμματα που έχουν ως σκοπό την αναστάτωση του δικτύου και της εκάστοτε συσκευής καθώς και την υποκλοπή προσωπικών και σημαντικών πληροφοριών. Στο Internet , ειδικά, συναντάμε αρκετά από αυτά τα λογισμικά. Όπως , ιούς (virus), 'σκουλήκια' (worms). Το πιο επικίνδυνα όμως όσο αφορά τις πληροφορίες που διακινούνται στο δίκτυο είναι:

  - Trojan Horses(Δούρειοι Ίπποι): Είναι προγράμματα τα οποία φαίνονται χρήσιμα όμως παρόλα αυτά κρύβουν εντολές σε γλώσσα μηχανής έτσι ώστε να ανιχνεύει και να βρίσκει πληροφορίες και να τις αποστέλλει στον δημιουργό του Δούρειου Ίππου.



Εικόνα 14 - TrojanHorse (Δούρειος Ίππος) {*Πηγή:* *https://theworldofwindows.blogspot.gr/2009/07/windows-tips-and-tricks-how-trojan.html* }

- Spyware(Λογισμικό κατασκοπείας): Είναι ένα πρόγραμμα που εγκαθίσταται χωρίς να το γνωρίζει ο χρήστης. Τρέχει στο παρασκήνιο και απώτερο σκοπό έχει την καταγραφή όλων των κινήσεων και δεδομένων της εκάστοτε συσκευής που έχει εγκατασταθεί. Η διαφορά με το Δούρειο Ίππο είναι ότι ένα πρόγραμμα ασφαλείας μπορεί να το εντοπίσει και να αφαιρέσει από τη συσκευή. Δυστυχώς, το spyware όχι μόνο δεν είναι εμφανές αλλά εμποδίζει και τον εντοπισμό του.

Hacking:

Όλα τα δίκτυα λαμβάνουν πολύ σοβαρά το θέμα ασφάλεια των πόρων τους. Όμως, ο hacker είναι το άτομο το οποίο μπορεί να ‘εισβάλλει’ στο δίκτυο, να καλύψει την ασφάλεια του. Οι λόγοι που γίνεται hacking είναι είτε για να βρουν και να ενημερώσουν τους διαχειριστές του δικτύου για τυχόν αδυναμίες συστήματος και ασφαλείας, όπως έγινε στη περίπτωση του CERN που άτομα έσπασαν το τείχος προστασίας και έπειτα τους ενημέρωσαν και του συμβούλεψαν για την κάλυψη των κενών ασφαλείας. Από την άλλη πλευρά υπάρχει και το hacking που χρησιμοποιείται για την υποκλοπή σημαντικών πληροφοριών με απώτερο σκοπό συνήθως το χρηματικό και όχι μόνο.

Έτσι, λοιπόν, διαπιστώνουμε ότι οι απειλές είναι αρκετές και ότι με οποιοδήποτε τρόπο πρέπει να προστατεύσουμε τους πόρους του συστήματος. Οι τρόποι είναι πολλού και θα αναφερθούν αναλυτικά στο επόμενο κεφάλαιο.

ΚΕΦΑΛΑΙΟ 3ο : ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

Σε αυτό το κεφάλαιο θα αναφερθούμε σε όλες αυτές τις μεθόδους και τεχνικές που αναπτύχθηκαν για την προστασία των αγαθών του δικτύου από τις απειλές. Πριν γίνει εκτενή αναφορά στις μεθόδους ασφαλείας των δικτύων , θα ήταν φρόνιμο να αναφέρουμε μια σειρά από ορισμούς που θα μας βοηθήσουν στις παρακάτω ενότητες.

3.1. ΕΙΣΑΓΩΓΙΚΕΣ ΕΝΝΟΙΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ

Πριν αρχίσουμε να αναλύουμε τις μεθόδους ασφάλειας για τα δίκτυ υπολογιστών, είναι φρόνιμο να αναφερθούμε σε κάποιες έννοιες βασικές .

- Εξουσιοδότηση: είναι η παροχή άδειας σε έναν χρήστη έτσι ώστε να είναι σε θέση να έχει πρόσβαση στα δεδομένα. Το ποιος θα έχει πρόσβαση στα δεδομένα είναι απόφασης του διαχειριστή του δικτύου καθώς και του ιδιοκτήτη του δικτύου και των δεδομένων.
- Εμπιστευτικότητα (Confidentiality) : όταν το δίκτυο εγγυάται ότι τα δεδομένα του δεν θα αποκαλυφθούν σε κάποιον μη εξουσιοδοτημένο χρήστη.
- Ακεραιότητα (Integrity): όταν το δίκτυο εγγυάται ότι τα δεδομένα δεν θα υποστούν επεξεργασία/τροποποίηση από μη εξουσιοδοτημένους χρήστες.
- Αυθεντικότητα (Authentication):Είναι η διαδικασία κατά την οποία ένας χρήστης πρέπει να αποδείξει την ταυτότητα του, ότι είναι εξουσιοδοτημένος χρήστης προκειμένου να έχει πρόσβαση στα δεδομένα.
- Μη άρνηση ταυτότητας (Nonrepudiation): Κάθε εξουσιοδοτημένος χρήστης έχει συγκεκριμένες προσβάσεις στα δεδομένα.

Σε αυτές τις έννοιες θα γίνει αναφορά πολύ συχνά στις παρακάτω ενότητες , οι οποίες θα ασχοληθούν εκτενώς με τις τεχνικές ασφάλειας των δικτύων.

3.2. ΑΣΦΑΛΕΙΑ ΔΙΚΤΥΩΝ - ΚΡΥΠΤΟΓΡΑΦΗΣΗ

Τα πακέτα δεδομένων που κυκλοφορούν σε ένα δίκτυο είναι ευανάγνωστα με την έννοια ότι κυκλοφορούν όπως ακριβώς εστάλησαν. Αυτή τη μορφή την ονομάζουμε Plaintext. Όπως, είναι λογικό σε αυτή τη μορφή οι πληροφορίες είναι εύκολα να διαβαστούν από τυχόν επιτιθέμενους. Έτσι , λοιπόν, για να προστατευτούν αυτές οι

πληροφορίες χρησιμοποιείται η κρυπτογράφηση. Η κρυπτογράφηση είναι η μετατροπή των πληροφοριών σε μορφή που καταλαβαίνει μόνο ο αποδέκτης. Μπορούμε να πούμε ότι το μήνυμα είναι σε ακαταλαβίστικη μορφή για τον επιτιθέμενο. Να αναφερθεί ότι η ακαταλαβίστικη μορφή του μηνύματος στο κόσμο της Πληροφορικής ονομάζεται ciphertext.

Η αποκρυπτογράφηση γίνεται στη μεριά του αποδέκτη. Και αυτός λαμβάνει το μήνυμα σε ακαταλαβίστικη μορφή (για τον υπολογιστή μιλάμε πάντα). Όμως, διαθέτει το κατάλληλο 'κλειδί', για να μπορέσει να το μετατρέψει στην κανονική του μορφή. Επίσης, συνήθως, οι περισσότεροι αλγόριθμοι κρυπτογράφησης χρησιμοποιούν και μια συνάρτηση για να μπορούν να παράγουν τα επιθυμητά αποτελέσματα.

Εικόνα 15 - Κρυπτογράφηση – Αποκρυπτογράφηση {*Πηγή:* ***http://resources.infosecinstitute.com/windows-cryptography-api/***}

Για την κρυπτογράφηση έχουν κυκλοφορήσει και χρησιμοποιηθεί αρκετοί αλγόριθμοι που θα αναλυθούν στις παρακάτω ενότητες.

3.2.1. ΑΛΓΟΡΙΘΜΟΙ ΑΝΤΙΚΑΤΑΣΤΑΣΗΣ

Οι αλγόριθμοι αυτοί , όπως διαπιστώνεται και από την ονομασία της κατηγορίας τους είναι πιο πολύ ιστορικοί παρά χρηστικοί τη σήμερον εποχή μια που τα δεδομένα είναι ακόμα πιο σημαντικά για προστασία και επίσης υπάρχουν περισσότερα προγράμματα που σπάνε εύκολα πια τους αλγορίθμους αυτούς.

- ***Αλγόριθμος Ceaser Cipher:*** είναι ένας απλός αλγόριθμος κρυπτογράφησης που αντικαθιστά το κάθε ένα γράμμα του μηνύματος με κάποιο άλλο και η αναφορά του είναι πιο πολύ ιστορική. Ουσιαστικά, η αντικατάσταση γίνεται με ολίσθηση αριστερά τόσα γράμματα όσα επιλέγει ο χρήστης. Το πόσα γράμματα θα ολισθήσει για την κρυπτογράφηση είναι προαποφασισμένο και από τα δύο μέρη επικοινωνίας (αποστολέα και αποδέκτη).
  Όπως είναι λογικό, αυτός ο αλγόριθμος είναι πολύ εύκολα να ΄σπάσει΄ και να διαβαστεί από τον επιτιθέμενο. Για αυτό το λόγο και δεν χρησιμοποιείται πια στα σύγχρονα δίκτυα υπολογιστών.

Εικόνα 16 - Παράδειγμα λειτουργίας CeaserCipher {*Πηγή:* *http://datagenetics.com/blog/july42015/index.html*

Αλγόριθμος Vigenere: Ο αλγόριθμος αυτός κατασκευάστηκε από τον Γάλλο συνονόματο Blaisede Vigenere. Η λειτουργία του στηρίζεται τώρα σε ένα κλειδί το οποίο περιλαμβάνει πολλά γράμματα και όχι μόνο ένα όπως ο αλγόριθμος Ceaser. Το μήκος του κλειδιού δεν είναι συνήθως μεγαλύτερο από τη λέξη που θέλουμε να κρυπτογραφήσουμε και αυτό σημαίνει ότι η λέξη κλειδί κάνει κύκλους. Όπως είναι λογικό, εάν βρεθεί το μήκος του κλειδιού τότε ο αλγόριθμος αυτός είναι πάραπολύ εύκολο να σπάσει και να παραδώσει τα δεδομένα στον

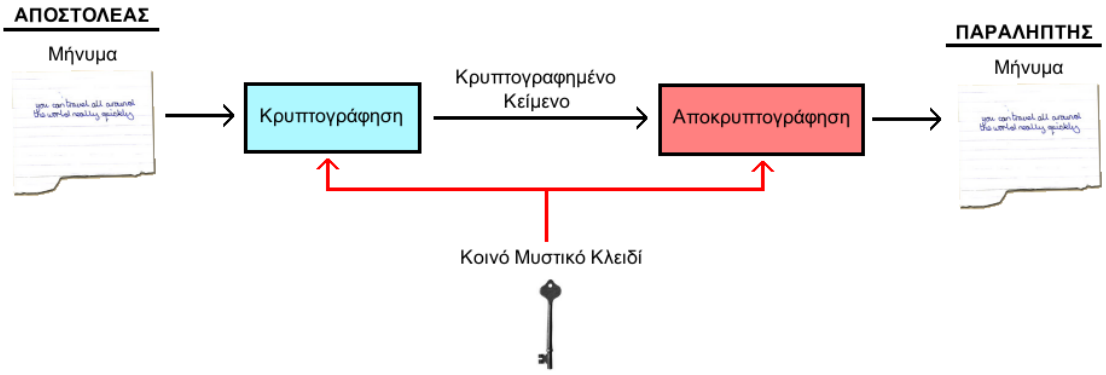
επιτιθέμενο. Για αυτό και αυτός δεν χρησιμοποιείται σήμερα στα δίκτυα υπολογιστών και όχι μόνο.

Plaintext:	ATTACKATDAWN
Key:	LEMONLEMONLE
Ciphertext:	LXFOPVEFRNHR

Εικόνα 17 - Αλγόριθμος Vigenere (Πηγή: http://www.codeproject.com/Articles/63432/Classical-Encryption-Techniques }

3.2.2. ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΣΥΜΜΕΤΡΙΚΟΥ ΚΛΕΙΔΙΟΥ

Στην κρυπτογράφηση συμμετρικού κλειδιού και οι δύο πλευρές, δηλαδή και αυτός που αποστέλλει το κρυπτογραφημένο μήνυμα αλλά και ο δέκτης που θα πρέπει να το αποκρυπτογραφήσει χρησιμοποιούν το ίδιο μυστικό κλειδί.



Εικόνα 18 - Κρυπτογράφηση Συμμετρικού Κλειδιού { *Πηγή: https://el.wikipedia.org/wiki/Κρυπτογράφηση_Συμμετρικού_Κλειδιού* }

}

Σήμερα , κυρίως οι αλγόριθμοι συμμετρικού κλειδιού διαχωρίζονται σε δύο κατηγορίες ανάλογα τον τρόπο με τον οποίο κρυπτογραφούν την πληροφορία. Υπάρχουν οι:

a) *Αλγόριθμοι ροής (streamcipher):*Είναι οι αλγόριθμοι οι οποίοι κρυπτογραφούν/αποκρυπτογραφούν την πληροφορία Bitπρος bit.
b) *Αλγόριθμοι Τμημάτων (Blockciprhers):* Είναι οι αλγόριθμοι οι οποίοι κρυπτογραφούν/αποκρυπτογραφούν την πληροφορία κατά τμήματα.

Υπάρχουν πολλοί αλγόριθμοι συμμετρικού κλειδιού που χρησιμοποιούνται και σήμερα στην ασφάλεια δικτύων και όχι μόνο. Κάποιοι από αυτούς είναι:

1. DES(DataEncryptionStandard): αλγόριθμοςπουπροτάθηκε το 1977. Χρησιμοποιεί μυστικό κλειδί μεγέθους 64 Bit. Έτσι , το αρχικό μήνυμα 'κόβεται' σε τμήματα (άρα ανήκει στους blockciprhers) των 64 bit.
2. AES:Προτάθηκε γιανα αντικαταστήσει τον αλγόριθμο DES. Ο συγκεκριμένος αλγόριθμος χρησιμοποιεί μυστικό κλειδί 128 bitκαι όπως και ο παραπάνω αλγόριθμος έτσι και αυτός σπάει το μήνυμα σε τμήματα για να το κρυπτογραφήσει. Υποστηρίζει όμως και κλειδιά μήκους 192 και 256 bit.
3. IDEA(InternationalDataEncryptionAlgorithm):Προτάθηκετο1991καιαποτελεί έναν αλγόριθμο με κλειδί μήκους 128 bit και αυτός. Η διαφορά του με τους υπόλοιπους και κυρίως με τον κυρίαρχο DES είναι ότι χρησιμοποιεί διαφορετικές συναρτήσεις.«*Συγκεκριμένα χρησιμοποιεί τη δυαδική πράξη XOR, τη δυαδική πρόσθεση ακεραίων των 16 – bit και το δυαδικό πολλαπλασιασμό ακεραίων των 16- bit*.» (Λυκούδης, 2012). Αξίζει να σημειωθεί ότι ο συγκεκριμένος αλγόριθμος έχει αποδείξει την αντοχή τους σε διάφορες απόπειρες 'σπασίματος' του.
4. 3DES: είναι επέκταση του DES. Χρησιμοποιεί και ένα δεύτερο κλειδί γιανα διασφαλίσει την ασφάλεια της κρυπτογράφησης που προκύπτει από τον απλό DES.
5. RC5: προτάθηκε το 1994 και είναι ένας από τους πιο γρήγορους αλγορίθμους συμμετρικού κλειδιού. Αξίζει να αναφερθεί ότι είναι η βάση που στηρίχτηκε ο RSA που θα γνωρίσουμε παρακάτω.

3.2.2.1. ΣΥΜΠΕΡΑΣΜΑΤΑ

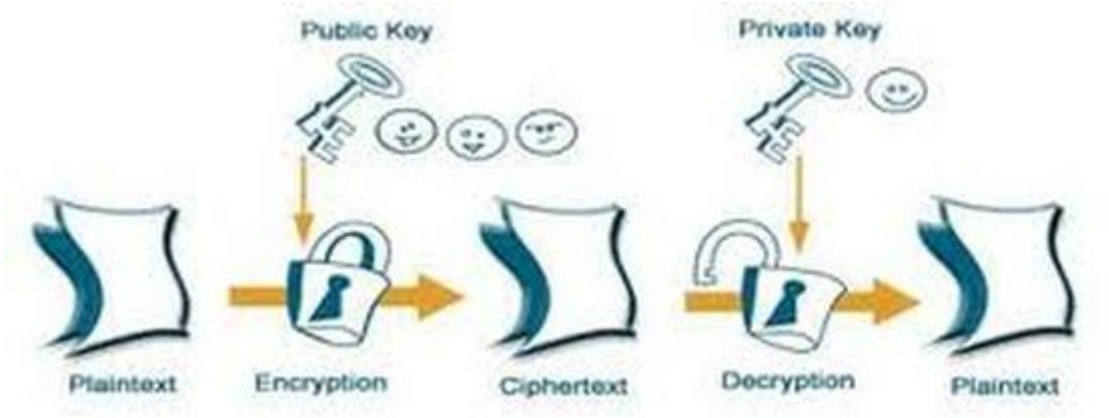
Οι αλγόριθμοι συμμετρικού κλειδιού χρησιμοποιούνται έως και σήμερα. Το πιο σημαντικό για την αποδοτικότερη ασφάλεια των πληροφοριών μας είναι το μέγεθος κλειδιού. Όσο μεγαλύτερο τόσο πιο δύσκολο θα είναι στον εκάστοτε επιτιθέμενο να το αποκωδικοποιήσει. Βέβαια, μεγαλύτερο μήκος κλειδιών σημαίνει και περισσότερο χρόνο τόσο για την κρυπτογράφηση όσο και για την αποκρυπτογράφηση. Αλλά, στον 21^{ο} αιώνα με τις ταχύτητες των επεξεργαστών να ακμάζουν αυτό δεν είναι θέμα. Το βασικό μειονέκτημα όμως των συμμετρικών κρυπτογραφικών αλγορίθμων είναι ότι πρέπει το μυστικό κλειδί να είναι γνωστό και από τις δύο μεριές. Δηλαδή, να γίνει μια ανταλλαγή του τρόπου κρυπτογράφησης με αποτέλεσμα να απαιτείται μια εγκαθίδρυση ασφαλούς σύνδεσης μεταξύ των δύο μερών που θέλουν να επικοινωνήσουν και αυτό δεν είναι πάντα εφικτό. Παρόλα αυτά κάποιοι από τους προαναφερόμενους αλγορίθμους έδειξαν ‘αξιοθαύμαστη’ αντοχή σε διάφορες επιθέσεις.

3.2.3. ΚΡΥΠΤΟΓΡΑΦΗΣΗ ΔΗΜΟΣΙΟΥ (ΑΣΥΜΜΕΤΡΟΥ) ΚΛΕΙΔΙΟΥ

Σε αυτήν την κατηγορία κρυπτογράφησης ανήκουν κείνοι οι αλγόριθμοι που χρησιμοποιούν δύο διαφορετικά κλειδιά. Το ένα ονομάζεται **δημόσιο κλειδί (publickey)** και το γνωρίζουν όλοι όσοι ανήκουν στο δικτύου. Καθένας όμως από τους συμμετέχοντες κατέχει και ένα **ιδιωτικό κλειδί (privatekey)** το οποίο είναι προσωπικό.Εννοείται ότι από το δημόσιο κλειδί δεν μπορεί κάποιος να παράγει και να βρει το ιδιωτικό κλειδί της εκάστοτε συσκευής. Επίσης, τα κλειδιά αυτά μεταξύ τους συνδέονται με μαθηματική συνάρτηση όπως και αυτοί που αναφέραμε στη προηγούμενη ενότητα.

Παραδείγματος χάριν, κατά κανόνα, έστω ότι θέλει να επικοινωνήσει ο Α με τον Β. και οι δύο κατέχουν το κοινό δημόσιο κλειδί αλλά ο καθένας ξεχωριστά κατέχει και ένα ιδιωτικό κλειδί. Εάν θέλει να στείλει , λοιπόν, ο Α στον Β , κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του Β. Όμως, μόνο ο Β και με το ιδιωτικό του κλειδί είναι σε θέση να διαβάσει δηλαδή να αποκρυπτογραφήσει τα μήνυμα που του στέλνει ο Α.

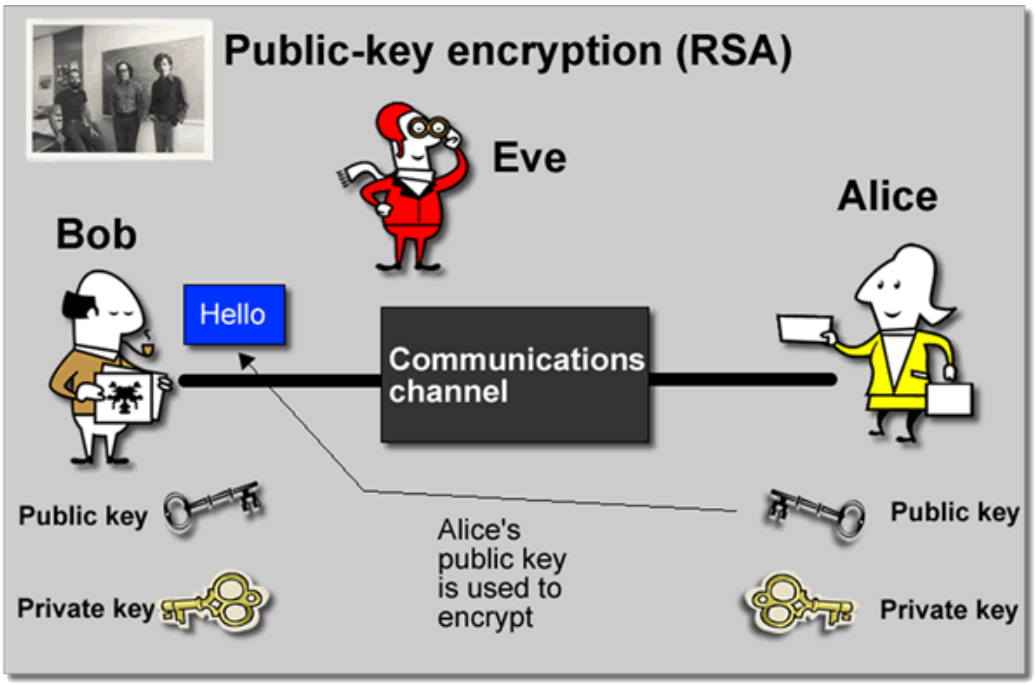
Με βάση αυτή τη λειτουργία, έχουν κατασκευαστεί και προταθεί και χρησιμοποιηθεί πάρα πολύ αλγόριθμοι , από τους οποίους κάποιους από αυτούς θα τους γνωρίσουμε παρακάτω.



Εικόνα 19 - Κρυπτογράφηση Δημοσίου Κλειδιού {Πηγή: http://bpliroftest.weebly.com/eta-kapparhoupsilonpitauomicrongammarhoalphaphiiotaalpha-sigmaetamuepsilonrhoalpha.html }

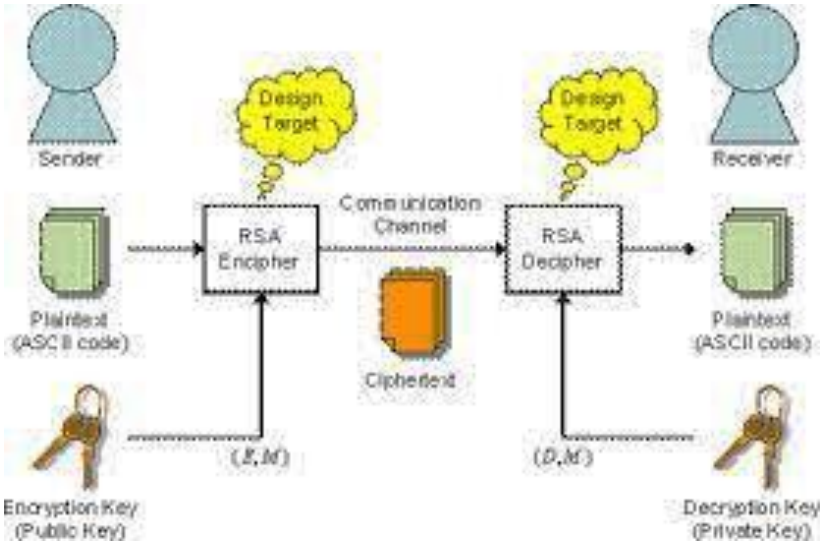
3.2.3.1. ΑΛΓΟΡΙΘΜΟΣ RSA

Ο αλγόριθμος RSAπροτάθηκε το 1977 και πήρε το όνομα του από τα αρχικά των επιθέτων των δημιουργών του: RiverR, ShamirAκαι AdlemanL.
Ο συγκεκριμένος αλγόριθμος μπορεί να ειπωθεί ότι είναι ο πιο γνωστός της κατηγορίας αυτής. Χρησιμοποιείται επίσης ευρέως.



Εικόνα 20 - Αλγόριθμος RSA {Πηγή: *http://www.itportal.in/2011/11/rsa-algorithm-information-security-be.html* }

Η λειτουργία του στηρίζεται στο ότι χρησιμοποιεί κλειδιά μήκους 512,1024 ή ακόμα και 2048bit. Τα κλειδιά αυτά προκύπτουν από την εφαρμογή μιας μαθηματικής συνάρτησης. Η συνάρτηση αυτή που είναι γνωστή ως συνάρτηση Euler παίρνει δύο τυχαίους πρώτους αριθμούς και παράγει το κρυπτογραφημένο μήνυμα με τη χρήση του δημοσίου κλειδιού.



Εικόνα 21 - Λειτουργία αλγορίθμους RSA{Πηγή: *https://globlib4u.wordpress.com/2013/10/16/rsa-public-key-encryption-system/* }

Είναι αξιοθαύμαστο ότι όσο μεγαλύτεροι είναι οι πρώτοι αριθμοί και όσο μεγαλύτερο είναι το μέγεθος του δημοσίου κλειδιού που χρησιμοποιείται τόσο μεγαλύτερο χρόνο χρειάζεται να 'σπάσει' κάποιος το κρυπτογραφημένο μήνυμα. Παρόλα αυτά , δεν σημαίνει και ότι ο χρόνος παρασκευής του κρυπτογραφημένου μηνύματος είναι ο ίδιος. Αντιθέτως , είναι αρκετά γρήγορος ειδικά με τις σημερινές υπολογιστικές δυνατότητες.

Παρακάτω , φαίνεται είναι ένα παράδειγμα χρόνου προστασίας του μηνύματος μας ανάλογα με τους πρώτους αριθμούς (p,q) που επιλέγονται και το μήκος του κλειδιού (n).

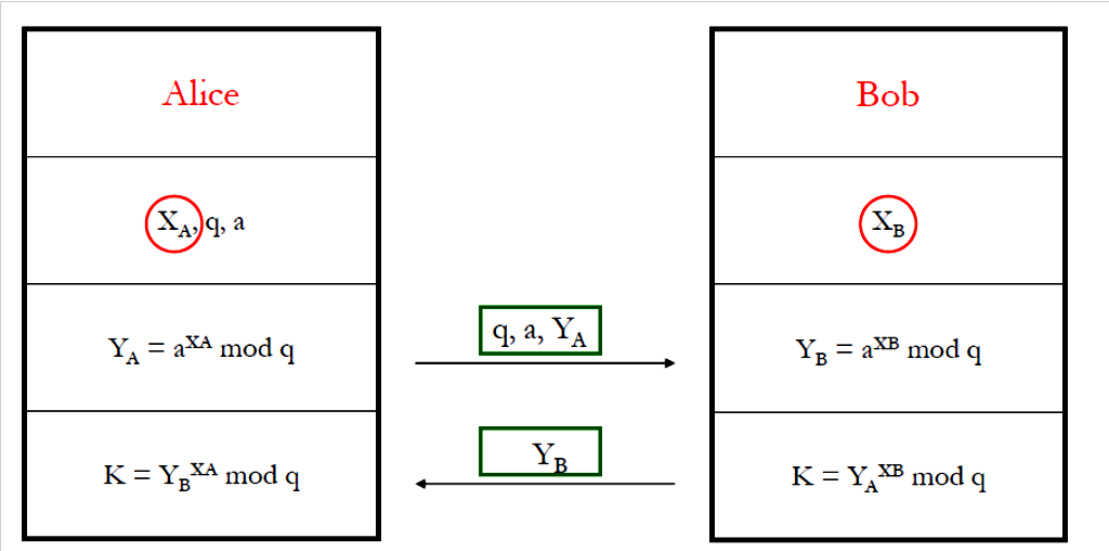
p, q	*n*	χρόνος προστασίας
256 bits	512 bits	Μερικές εβδομάδες
512 bits	1024 bits	50-100 χρόνια
1024 bits	2048 bits	> 100 χρόνια
2048 bits	4096 bits	Περίπου την ηλικία του σύμπαντος

Εικόνα 22 - Χρόνος προστασίας του RSA με διάφορους συνδυασμούς πρώτων αριθμών και κλειδιού {Πηγή: *https://openeclass.teimes.gr/modules/document/file.php/CIED194/lecture05.pdf* }

3.2.3.2. ΑΛΓΟΡΙΘΜΟΣ DIFFIE - HELLMAN

Ο αλγόριθμος αυτός είναι από τους πιο δυνατούς και χρηστικούς λόγω της ικανότητας του να προστατεύει τα κλειδιά που ανταλλάσσονται. Η προστασία που προσφέρει έγκειται στο γεγονός ότι χρησιμοποιεί διακριτούς λογαρίθμους που είναι δύσκολο να υπολογιστούν και κατ'επέκταση να εντοπιστούν και να χρησιμοποιηθούν για να αποκρυπτογραφηθεί το μήνυμα.

Η διαδικασία είναι αρκετά πολύπλοκη για αυτό και δεν θα διερευνηθεί σε βάθος ο συγκεκριμένος αλγόριθμος, παρά μόνο θα δοθεί ένα μικρό παράδειγμα του.

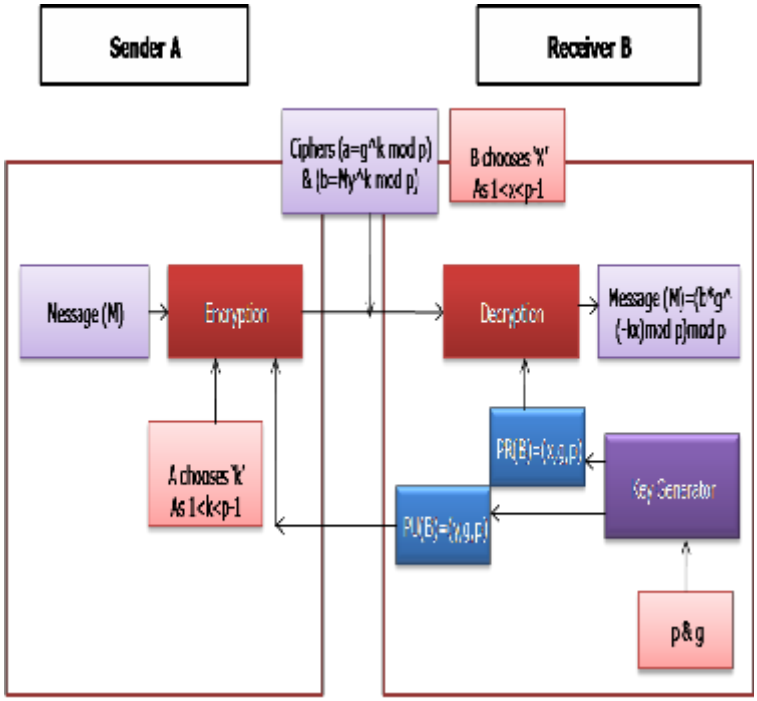


Εικόνα 23 - Αλγόριθμος Diffie – Hellman {Πηγή: http://users.uom.gr/~kpsannis/Lecture-Encrypt-Key-Exchange.pdf }

Στην παραπάνω εικόνα τα X_Aκαι X_Bείναι τα ιδιωτικά κλειδιά του αποστολέα και του παραλήπτη αντίστοιχα. Τοα είναι ένας αριθμός ενώ το q είναι η λεγόμενη πρωτογενής ρίζα. Αυτά μπαίνουν στην συνάρτηση και παράγουν το Ya και Y_B.Αυτό που είναι πολύ σημαντικό είναι ότι και στα ιδιωτικά κλειδιά εφαρμόζονται οι διακριτοί λογάριθμοι και έτσι είναι πολύ δύσκολο να εντοπισθεί και να αποκρυπτογραφηθεί το μήνυμα ακόμα και αν ο επιτιθέμενος καταφέρει να μάθει τα υπόλοιπα στοιχεία που εμπλέκονται όπως το qή το a.

3.2.3.3. ΑΛΓΟΡΙΘΜΟΣ ELGAMAL

Ο αλγόριθμος αυτός βασίζεται όπως και οι προηγούμενοι σε δύσκολους υπολογιστικούς λογαρίθμους. Βέβαια το αποτέλεσμα αυτών των υπολογισμών είναι διπλάσιο σαν αποτέλεσμα και αυτό είναι ένα βασικό πλεονέκτημα του. Λόγω ακριβώς της πολυπλοκότητας των υπολογισμών του, σε αυτή την εργασία δεν θα γίνει περαιτέρω ανάλυση του.



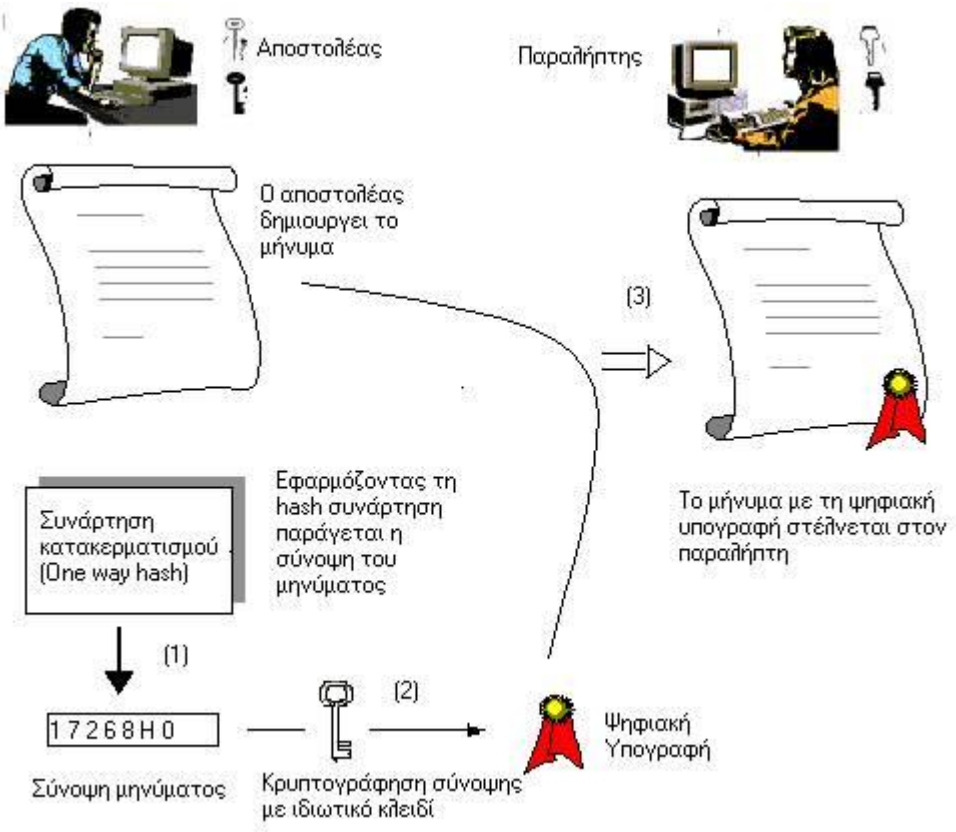
Εικόνα 24 - Αλγόριθμος Elgamal {Πηγή: http://www.ijser.org/paper/Elgamals-Algorithm-in-Cryptography.html }

Σε αυτούς τους αλγορίθμους του δημοσίου κλειδιού, συγκαταλέγονται και δύο τεχνικές διασφάλισης κυρίως της πιστοποίησης της ταυτότητας του χρήστη (και όχι της ασφάλειας) και όχι μόνο. Είναι τεχνικές που χρησιμοποιούνται σε ένα από τα μεγαλύτερα δίκτυα το Δίκτυο. Παρόλα αυτά , θα γίνει μια μικρή αναφορά σε αυτά λόγω της επιπλέον προστασίας που παρέχουν στα δεδομένα και κατά επέκταση και στα δίκτυα.

3.2.4. ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ ΚΑΙ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΣΤΟ ΜΕΓΑΛΥΤΕΡΟ ΔΙΚΤΥΟ – ΔΙΑΔΙΚΤΥΟ

Η ψηφιακή υπογραφή έρχεται για να πιστοποιήσει την ταυτότητα του αποστολέα. Όπως ακριβώς και με την χειρόγραφη υπογραφή που συμπληρώνει ένα έγγραφο για τη νομιμότητα του, έτσι ακριβώς και η ψηφιακή συμπληρώνει μπορούμε να πούμε τους διάφορους αλγορίθμους ασφαλείας. Η ψηφιακή υπογραφή χρησιμοποιεί τον RSA τον οποίο και αναφέραμε παραπάνω. Συγκεκριμένα, η διαδικασία της ψηφιακής υπογραφής είναι η εξής:

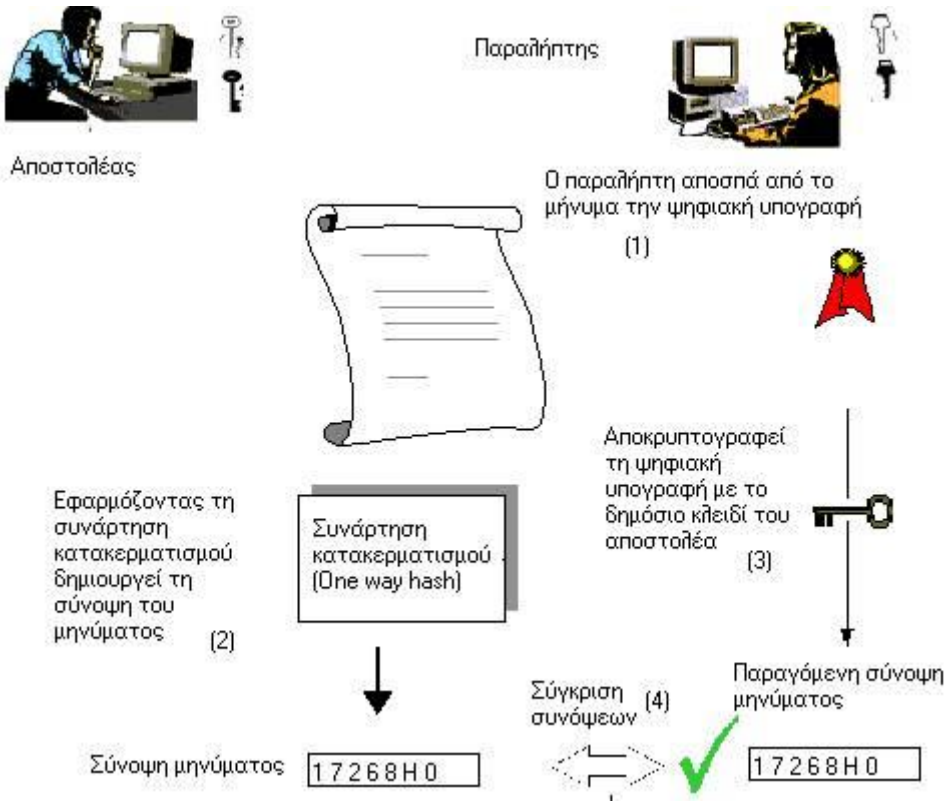
- Το μήνυμα περνάει από μια συνάρτηση μαθηματική η οποίακαλείται ***συνάρτηση κατακερματισμού (hashfunction)***.
- Η συνάρτηση αυτή δέχεται ένα μήνυμα κάποιου μεγέθους και δίνει ως αποτέλεσμα ένα σταθερού μήκους αποτέλεσμα. Το αποτέλεσμα αυτό ονομάζεται ***σύνοψη μηνύματος***. Αξίζει να αναφερθεί ότι το αποτέλεσμα της συνάρτησης είναι μη αντιστρέψιμο.
- Η σύνοψη αυτή συνοδεύεται μαζί με το μήνυμα.
  Αυτή είναι η διαδικασία κατά τη διάρκεια της αποστολής.



Εικόνα 25 - Ψηφιακή Υπογραφή (Αποστολέας) {Πηγή: *http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html* }

Στην παραλαβή , γίνεται η εξής διαδικασία:

- Ο παραλήπτης δέχεται το μήνυμα με την ψηφιακή υπογραφή. Στη δική του συσκευή , παράγεται για το ίδιο μήνυμα μια άλλη σύνοψη μηνύματος χρησιμοποιώντας την συνάρτηση κατακερματισμού. Εάν οι δύο συνόψεις είναι ίδιες τότε ο παραλήπτης είναι σίγουρος για τις προθέσεις του αποστολέα καθώς και την ταυτότητα του.



Εικόνα 26 - Ψηφιακή Υπογραφή (Παραλήπτης) {Πηγή: *http://www.eett.gr/opencms/opencms/EETT/Electronic_Communications/DigitalSignatures/IntroEsign.html* }

Να αναφέρουμε ότι η ψηφιακή υπογραφή βρίσκει εφαρμογή και στην Ελλάδα και μάλιστα με ειδικό νομοσχέδιο που υποχρεώνει τις αντίστοιχες δημόσιες υπηρεσίες και τους εργαζόμενους τους να εκδώσουν ψηφιακές υπογραφές και να τις συμπεριλαμβάνουν σε οποιαδήποτε έγγραφο δημοσίου περιεχομένου.

Από την άλλη υπάρχει το ψηφιακό πιστοποιητικό. Και αυτό βρίσκει μεγάλη εφαρμογή στο Διαδίκτυο για αυτό και γίνεται αναφορά και σε αυτό.

Το ψηφιακό πιστοποιητικό είναι κρυπτογραφημένη πληροφορία πιστοποίησης ενός χρήστη ή ενός οργανισμού. Κάθε φορά που επισκεπτόμαστε ένα site τότε το ψηφιακό πιστοποιητικό ανασύρεται και αποκωδικοποιείται από τον browser του χρήστη για να επιβεβαιώσει την ασφαλή του σύνδεση.

3.2.5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Οι αλγόριθμοι δημοσίου – ιδιωτικούκλειδιού (ασύμμετρης κρυπτογράφησης) που είδαμε σε αυτήν την ενότητα υπερτερούν σε ένα από το πιο βασικό θέμα όσο αφορά την ασφάλεια: την μονιμότητα των κλειδιών τους. Τα ζεύγη αυτά μπορούν να παραμείνουναναλλοίωτα καθώς και προστατευμένα. Βέβαια, τα κλειδιά είναι μεγαλύτερα σε μήκος σε σύγκριση με κείνους της αλλά από την άλλη όσο μεγαλύτερο το μήκος τόσο πιο περίπλοκη η διαδικασία κρυπτογράφησης και κατ'επέκταση δυσκολότερη η επιτυχής υποκλοπή των μηνυμάτων.

Βέβαια, με την ανάπτυξη της τεχνολογίας έρχεται και η έντονη ανάγκηπερισσότερης ασφάλειας των δεδομένων και των δικτύων. Για αυτό και τα τελευταία χρόνιαγίνεταιλόγος για την υβριδική κρυπτογράφηση. Η Υβριδική κρυπτογράφηση είναι ουσιαστικά ο συνδυασμός των δύο κατηγοριών αλγορίθμων κρυπτογράφησης. Δηλαδή είναι ο συνδυασμός της συμμετρικής και της ασύμμετρης κρυπτογράφησης. Ένα παράδειγμα χρήσης της υβριδικής κρυπτογράφησης είναι ο αλγόριθμος SSL (SecureSocketsLayer) που χρησιμοποιείται σε όλες τις ασφαλείς συνδέσεις. Σε οποιοδήποτε browser , ο SSL εμφανίζεται ως λουκέτο και είναι η ένδειξη ότι οποιεσδήποτε πληροφορίες και να εκχωρήσουμε στο συγκεκριμένο ιστότοπο , θα μεταδοθεί μέσω του Διαδικτύου μέχρι το serverκρυπτογραφημένο. Με τη βοήθεια του SSL , ήρθε και το e-banking.Εκατομμύρια πια πελάτες τραπεζών εμπιστεύονται διαδικτυακές εφαρμογές για την ενημέρωση - και όχι μόνο – των λογαριασμών τους χωρίς να τρέμουν στην πιθανότητα υποκλοπής στοιχείων. Ο SSL πια βρίσκει εφαρμογή σε οποιαδήποτε φόρμα επικοινωνίας και καταχώρησης προσωπικών κωδικών (YahooMail, Gmail, Facebook κοκ).

Εικόνα 27 - Υβριδική κρυπτογράφηση – SSL {Πηγή: *https://www.awardspace.com/ssl-certificates/what-is-ssl-certificate*}

3.3. ΔΙΚΤΥΑΚΑ ΗΛΕΚΤΡΟΝΙΚΑ ΑΝΑΧΩΜΑΤΑ – FIREWALLS

Για τη διαμοίραση των πληροφοριών , η κατασκευή και η ύπαρξη ενός δικτύου είναι απαραίτητη και αναγκαία. Όπως έχει προαναφερθεί όμως οι κίνδυνοι είναι πολλοί. Έτσι , λοιπόν, άλλο ένα μέτρο ασφαλείας των δικτύων είναι τα λεγόμενα δικτυακά ηλεκτρονικά αναχώματα ή αλλιώς firewalls ή αλλιώς τείχη προστασίας. Κάποια από αυτά έρχονται να καλύψουν τα κενά ασφαλείας μεταξύ των δικτύων και άλλα χρησιμοποιούνται κυρίως για τη διασφάλιση της πληροφορίες μεταξύ των εσωτερικού δικτύου μιας εταιρείας (intranet) και του Διαδικτύου. Τα διάφορα firewalls που κυκλοφορούν για μεγάλα δίκτυα και εταιρείες πουλούνται από τις αντίστοιχες κατασκευαστικές εταιρείες όπως WatchGuard, CISCOκοκ.
Ας δούμε τι ακριβώς είναι αυτά τα firewalls και πώς χρησιμοποιούνται.

3.3.1. ΤΙ ΕΣΤΙ FIREWALL ΚΑΙ ΠΟΙΑ Η ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ

Το Firewall(Τείχος Προστασίας) είναι ένα σύνολο προγραμμάτων ή συσκευών που εγκαθιδρύονται στο μεταίχμιο δύο δικτύων. Η βασική του ευθύνη είναι ουσιαστικά να ελέγχει ,να επιτρέπει ή να απορρίπτει πληροφορίες και δεδομένα που εισέρχονται και εξέρχονται μεταξύ των δικτύων. Το firewall συνήθως το χρησιμοποιούμε μεταξύ ενός εσωτερικούδικτύου μιας εταιρείας για παράδειγμα και μεταξύ του Διαδικτύου. Αυτό συμβαίνει διότι οι ανάγκη διασύνδεσης στο Διαδίκτυο είναι μεγάλη αλλά επίσης και ο κίνδυνος είναι μεγάλος για τα δεδομένα της εταιρείας.

Γενικά η λειτουργία του firewall βασίζεται σε δρομολογητές και εξυπηρετητές. Όταν ένα δίκτυο έμπιστο όπως το προαναφερόμενο εσωτερικό δίκτυο εταιρείας ζητάει

πρόσβαση σε ένα μη έμπιστο δίκτυο όπως το Διαδίκτυο τότε αναλαμβάνει το firewall. Το «φίλτρο» εκείνο το οποίο αποφασίζει για τη διαχείριση των πληροφοριών. Για να αποδίδει όμως τα μέγιστα ένα τείχος προστασίας πρέπει να έχουν τεθεί από την δημιουργία του δικτύου και τον διαχειριστή του , σαφής κανόνες λειτουργίας για τις συσκευές εντός του δικτύου και εντός του δικτύου της εταιρείες. Χωρίς σαφής παραμετροποίηση των firewalls, ο κίνδυνος παραβίασης αυξάνεται.

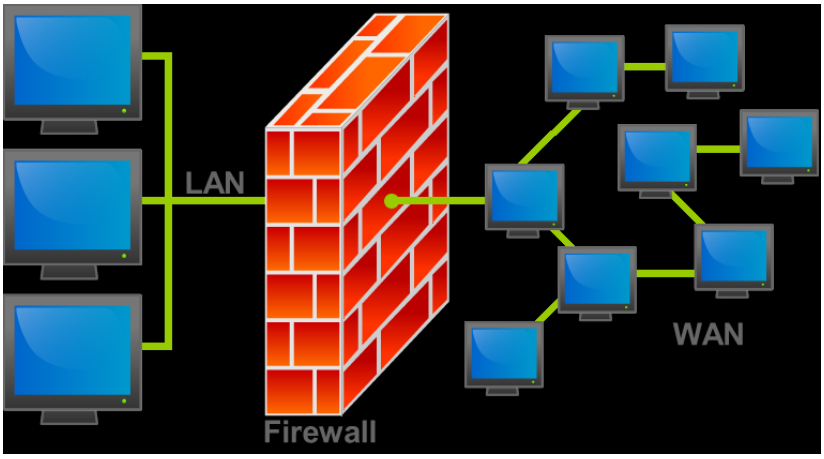
Έτσι για παράδειγμα, όταν ένας χρήστης του εσωτερικού δικτύου ζητήσει πρόσβαση σε μια εφαρμογή του Διαδικτύου που όμως είναι επικίνδυνη για υποκλοπή πληροφοριών, το firewall αποφασίζει να μην του παρέχει πρόσβαση. Στο επίπεδο εφαρμογών όπως σε αυτό το παράδειγμα , το firewallαποφασίζει με βάση τα ports των εφαρμογών και που έχει θέσει ο διαχειριστής του δικτύου να αποκλείονται.

Το παραπάνω παράδειγμα ήταν ένας εκ των τεσσάρων ελέγχων που αναλαμβάνουν τα αναχώματα. Συγκεκριμένα ήταν ο έλεγχος υπηρεσιών.

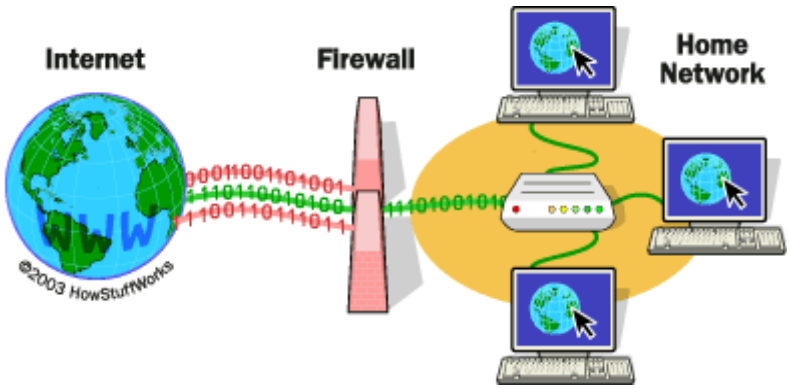
Ο επόμενος έλεγχος είναι ο έλεγχος κατεύθυνσης που αποφασίζει σε από ποιο και σε ποιο σημείο τωνεμπλεκόμενων δικτύων επιτρέπεται η παροχή υπηρεσιών.

Ο έλεγχος χρηστών ουσιαστικά δίνει τη δυνατότητα μόνο σε συγκεκριμένους χρήστες να χρησιμοποιούν μια υπηρεσία. Συνήθως , χρησιμοποιείται για τα άτομα εντός του εσωτερικού δικτύου.

Και τέλος έχουμε τον έλεγχο συμπεριφοράς κατά τον οποίο το τείχος προστασίας μπορεί να αποκόψει την πρόσβαση σε μια υπηρεσία ή ένα κομμάτι της.
(Κατσικάς, 2001).



Εικόνα 28 - FirewallΜεταξύ Δικτύων {Πηγή: *http://www.bullguard.com/bullguard-security-center/pc-security/computer-security-resources/how-does-a-firewall-work.aspx* }



Εικόνα 29- Firewall(Δικτύου και Διαδικτύου) {Πηγή: *http://computer.howstuffworks.com/firewall.htm* }

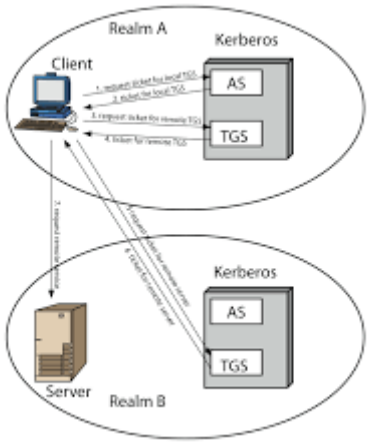
3.4. ΣΥΣΤΗΜΑΤΑ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ ΣΕ ΚΑΤΑΝΕΜΗΜΕΝΑ ΔΙΚΤΥΑ ΚΑ ΣΥΣΤΗΜΑΤΑ

Τα συστήματα αυθεντικοποίησης παρέχουν ασφάλεια στα δίκτυα. Είναι υπεύθυνα για την πιστοποίηση του χρήστη. Η πιστοποίηση ουσιαστικά περιλαμβάνει τον προσδιορισμό και την επιβεβαίωση της ταυτότητας του χρήστη. Για τα συστήματα αυτά έχουν αναπτυχθεί διάφορα πρωτόκολλα πιστοποίησης αυθεντικότητας τα οποία μερικά θα δούμε παρακάτω.

3.4.1. KERVEROS

Το σύστημα Kerverosαναλαμβάνει την πιστοποίηση μιας συσκευής σε ένα server με το πλεονέκτημα ότι αυτή η πιστοποίηση δεν θα είναι ευάλωτη σε επιθέσεις τρίτων. Η λειτουργία του Kerveros βασίζεται στην ιδέα ότι η πληροφορία για την ταυτοποίηση του χρήστη στον δρομολογητή/εξυπηρετητή είναι κρυπτογραφημένη.

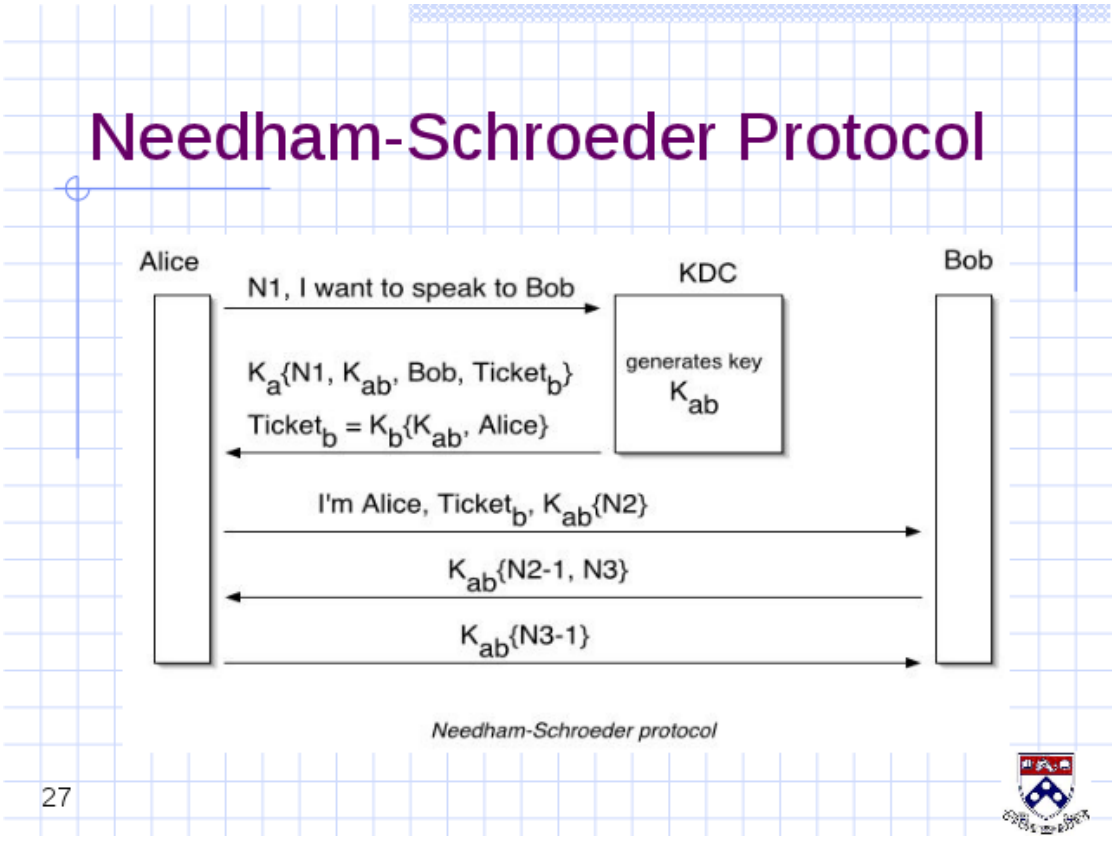
Η κρυπτογράφηση που ακολουθείται είναι με βάση τον αλγόριθμο DES δηλαδή χρησιμοποιεί συμμετρική κρυπτογράφηση. Αυτό προσδίδει ένα πλεονέκτημα ότι το κρυπτογραφημένο μήνυμα μόνο εάν αποκρυπτογραφηθεί με το ίδιο κλειδί της κρυπτογράφησης θα δώσει το αρχικό μήνυμα.



Εικόνα 30 – Kerveros {Πηγή: *https://www.cs.ucy.ac.cy/courses/EPL674/lectures/Authentication-ch15-GR.pdf* }

3.4.2. ΠΡΩΤΟΚΟΛΛΟ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ NEEDHAM- SCHROEDER

Το πρωτόκολλο αυτό είναι ουσιαστικά και η βάση του Kerveros. Περιλαμβάνει συμμετρική κρυπτογράφηση μεταξύ δύο μερών που θέλουν να επικοινωνήσουν. Η προστασία που παρέχει στοχεύει στην προστασία της διαμοίρασης του κοινού κλειδιού τους.Τα δύο άκρα που θέλουν να επικοινωνήσουν μπορεί να ανήκουν και σε ξεχωριστά δίκτυα αλλά ακόμα και στο ίδιο το δίκτυο. Βέβαια, όπως προαναφέρθηκε, η προστασία λαμβάνεται για την επικοινωνία μεταξύ δύο ξένων δικτύων και κυρίως μέσω Διαδικτύου.



Εικόνα 31 - Πρωτόκολλο Needham – Schroeder {Πηγή: http://people.man.ac.uk/~zlsiial/docs/kerberos/img26.html }

Το πώς λειτουργεί το συγκεκριμένο πρωτόκολλο παρουσιάζεται στην παραπάνω εικόνα. Ας επεξηγήσουμε λίγο τη διαδικασία:

- Έστω ότι τα δύο μέρη που θέλουν να επικοινωνήσουν είναι η Alice (A) και ο Bob(B). Συνηθίζεται στη βιβλιογραφία των δικτύων και της κρυπτογραφίας στα παραδείγματα να χρησιμοποιούν την Alicekαι τον Bob.

- Τα K_aκαθώς και το K_bείναι κλειδιά της Alice και του Bob αντίστοιχα και χρησιμοποιούνται για την επικοινωνία με τον ενδιάμεσο serverπου δεν φαίνεται μεν στην εικόνα.
- Χρησιμοποιώντας κατάλληλες συναρτήσεις παράγονται τα N1 κτλ
- Και τέλος , παράγεται το συνδυασμένο κλειδί K_{ab}με το οποίο και γίνεται κρυπτογραφημένη η πιστοποίηση και η επικοινωνία και των δύο πλευρών.

Παρόλα αυτά, κινδυνεύει από επιθέσεις επανάληψης. Επιθέσεις επαναλήψεις σημαίνει όταν το μήνυμα που αποστέλλεται, αντιγράφεται και αποστέλλεται ξανά.

3.4.3. ΠΡΩΤΟΚΟΛΛΟ SPX

Το πρωτόκολλο αυτό είναι υβριδικής κατασκευής. Χρησιμοποιεί κρυπτογραφία συμμετρικού και ασύμμετρου κλειδιού και συγκεκριμένα τον RSAκαι DES.Εν συντομία , λοιπόν, ο συνδυασμός αυτός έχει ως εξής:

- Έστω ο χρήστης Alice(A)θέλει να επικοινωνήσει και να συνδεθεί με server. Όπως γνωρίζουμε, πρέπει να ακολουθηθεί η διαδικασίας ταυτοποίησης. Έτσι , λοιπόν, βάζοντας τα στοιχεία της αυτά κρυπτογραφούνται με τη βοήθεια μιας συνάρτησης κατατεμαχισμού και έτσι δημιουργεί μια σύνοψη μηνύματος βασιζόμενο στα στοιχεία που έδωσε η Alice.
- Από την άλλη μεριά , η αποκρυπτογράφηση γίνεται με το ιδιωτικό κλειδί του παραλήπτη.
  Και έτσι , συνδυάζονται δύο τεχνικές για την περισσότερη ασφάλεια.

Αυτά ήταν κάποια από τα πρωτόκολλα αυθεντικοποίησης που χρησιμοποιούνται στα δίκτυα. Επίσης , σε αυτή την κατηγορία συγκαταλέγονται και οι : TESS, SESAME .Η διαδικασία που ακολουθείται για αυτά τα πρωτόκολλα είναι αρκετά πολύπλοκη και έγκειται στα πλαίσια της κρυπτογραφίας παρά της ασφάλειας δικτύων. Για αυτό και η αναφορά σε αυτά έγινε επιλεκτικά και συνοπτικά.

3.5. ΑΣΦΑΛΕΙΑ ΣΤΟ INTERNET

Όλοι οι παραπάνω τρόποι και μηχανισμοί ασφαλείας απευθύνονται σε οποιοδήποτε δίκτυο ή δίκτυα και τις συσκευές που θέλουν να επικοινωνήσουν. Αν και έγινε και αναφοράστη προστασία επικοινωνίας μεταξύ internet και εσωτερικού δικτύου, παρόλα αυτά, λόγω το ότι το Διαδίκτυο είναι πια γεγονός της καθημερινότητας μας, θα αφιερώσουμε λίγες σελίδες παραπάνω για τα πρωτόκολλα και τους αλγορίθμους ασφαλείς που χρησιμοποιούνται σε αυτό το μεγάλο δίκτυο, το Internet.

3.5.1. ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΕΠΙΠΕΔΟ ΔΙΚΤΥΟΥ

Όταν άρχισε να εξελίσσεται και να μεγαλώνει το Διαδίκτυο, διαπιστώθηκε πόσο ευάλωτο ήταν στις επιθέσεις. Οι πληροφορίες που διακινούνταν έπρεπε με κάποιο τρόπο να προστατευτούν. Για αυτό το λόγο προέβησαν στη δημιουργία κάποιων πρωτοκόλλων ασφαλείας. Κάποια από αυτά τα πρωτόκολλα είναι το SP3, NSVP αλλά το πιο σημαντικό ήταν το IPSec.

Το IPSec ουσιαστικά εγκαθιδρύεται στο 3^{o} επίπεδο του TCP/IP, δηλαδή στο επίπεδο δικτύου εκεί όπου βρίσκεται και το αντίστοιχο πρωτόκολλο δρομολόγησης των πακέτων IP. Προτάθηκε το 1992 από την InternetEngineeringTaskForce(IETF). Και έκτοτε εφαρμόζεται σε όλες τις εκδόσεις του IP όπως το IPv6. Το συγκεκριμένο πρωτόκολλο αναπτύχθηκε για να παρέχει μυστικότητα και ακεραιότητα δεδομένων. Για να το επιτύχει χρησιμοποιεί κρυπτογράφηση συμμετρικού κλειδιού.

Ας δούμε πως το επιτυγχάνει.

Το IPSec έρχεται να προσθέσει δύο επιπλέον επικεφαλίδες στα πακέτα τα οποία ενσωματώνονται στα IP πακέτα. Συγκεκριμένα, χρησιμοποιεί την επικεφαλίδα πιστοποίησης ταυτότητας –authenticationHeader (AH) . Η επικεφαλίδα αυτή χρησιμοποιεί συνάρτηση κατακερματισμού αντι ψηφιακών υπογραφών . Με αυτό τον τρόπο επιτυγχάνεται η ακεραιότητα των δεδομένων αλλά και η γρήγορη ταχύτητα στην μεταφορά των πακέτων.

Η άλλη επικεφαλίδα είναι το Φορτίο ενθυλάκωσης –EncapsulatingSecurityPayload (ESP) και επιτυγχάνεται η προστασία της ακεραιότητας και της ταυτότητας των δεδομένων.

(http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ipsec.htm

Επίσης, μαζί με το IPSec προτάθηκε και το πρωτόκολλο διαχείρισης κλειδών γιατί όπως αναφέρθηκε το πρώτο χρησιμοποιεί κρυπτογράφηση συμμετρικού κλειδιού. Άρα με κάποιο τρόπο πρέπει να διασφαλιστεί και η προστασία των κλειδιών κατά την ανταλλαγή. Προτάθηκε , λοιπόν , το πρωτόκολλοIKMP (Internet Key Management Protocol).Τα δύο αυτά πρωτόκολλα χρησιμοποιούνται δημιουργώντας αυτό που ονομάζεται σύναψη ασφαλείας – Security Association (SA).

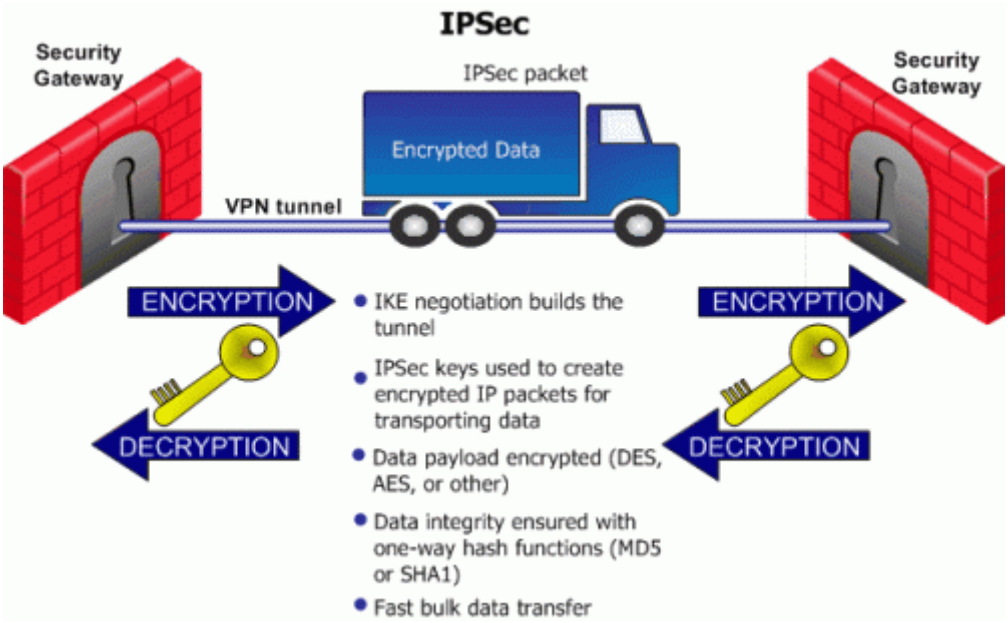
Έτσι, λοιπόν, κατά την εγκαθίδρυση της επικοινωνίας, καθορίζεται ο τρόπος λειτουργίας. Υπάρχουν δύο τρόποι λειτουργίας. Υπάρχει η λειτουργία μεταφοράς κατά την οποία προστατεύονται τα παραπάνω πρωτόκολλα του δικτύου και η λειτουργία της σήραγγας που προστατεύονται τα πακέτα IP. Το ποια λειτουργία θα επιλεγεί εξαρτάται από τις συνθήκες και τις απατήσεις της επικοινωνίας. (Κατσικάς, 2001).

Ας δούμε ένα παράδειγμα για να μπορέσουμε να κατανοήσουμε την χρησιμότητα των παραπάνω.

- Ο Bob στέλνει τα δεδομένα του προς την Alice
- Όταν ο δρομολογητής του Bob δει τα πακέτα ελέγχει τη πολιτική ασφάλειάς τους και αντιλαμβάνεται ότι αυτά πρέπει να είναι κρυπτογραφημένα.
- Η προ-ρυθμισμένη πολιτική ασφάλειας λέει επιπλέον ότι ο δρομολογητής της Alice πρέπει να είναι το τελικό σημείο τηςIPSecσήραγγας.
- Ο δρομολογητής του Bob κοιτάει να δει εάν έχει εγκαθιδρυμένη μια IPSec SA με το δρομολογητή της Alice.
- Σε περίπτωση που μια τέτοια δεν υπάρχει, τότε ζητάει μία.

  Εάν υπάρχει στους δρομολογητές τους έτοιμη SA τότε αυτή εγκαθιδρύεται. Τι γίνεται όμως όταν δεν υπάρχει? Τότε, οι δύο δρομολογητές επικοινωνούν για να ανταλλάξουν ψηφιακά πιστοποιητικά με σκοπό της εγκαθίδρυση μιας SA. Μόλις γίνει η εγκαθίδρυση της SA, τότε προχωρούν στο επόμενο βήμα το οποίο είναι η συμφωνία των αλγορίθμων κρυπτογράφησης και πιστοποίησης που θα χρησιμοποιηθεί από εδώ και πέρα στην επικοινωνία μεταξύ Bob και Alice. Και το τελευταίο βήμα είναι το IPSec να δημιουργήσει τις δικές του επικεφαλίδες και να τις ενσωματώσει στα IP πακέτα ενώ από τη μεριά της Alice, να γίνει αποθυλάκωση για να φανερωθεί το μήνυμα στο παραλήπτη.

(http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ipsec.htm).



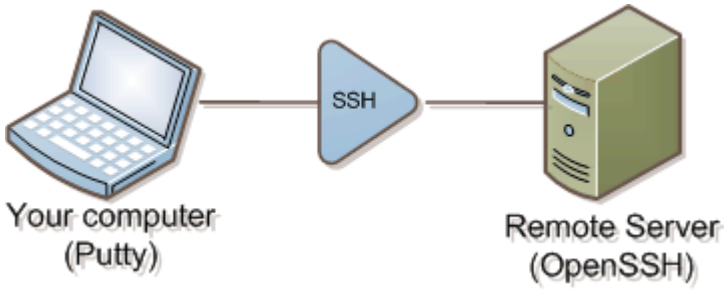
Εικόνα 32 - Λειτουργία IPSec {Πηγή: *https://sc1.checkpoint.com/documents/R77/CP_R77_VPN_AdminGuide/13847.htm* }

3.5.2. ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑΣ ΣΤΟ ΕΠΙΠΕΔΟ ΜΕΤΑΦΟΡΑΣ

Αφού αναφερθήκαμε στα πρωτόκολλα ασφαλείας που μεσολαβούν στο επίπεδο Δικτύου, ας δούμε και ποια πρωτόκολλα χρησιμοποιούνται για την ασφάλεια στο επίπεδο μεταφοράς. Στο επίπεδο μεταφοράς σύμφωνα με το μοντέλο TCP/IP, υπάρχουν τα πρωτόκολλα μεταφοράς TCP καθώς και UDP.Έτσι, λοιπόν, για την προστασία των δεδομένων που ταξιδεύουν σε πακέτα, προτάθηκαν και σε αυτήν την περίπτωση αρκετά πρωτόκολλα όπως το SP4 ή τοTLSP. Όμως, εμείς θα επικεντρωθούμε στα πιο σημαντικά και νεότερα πρωτόκολλα ασφαλείας όπως το SSH , SSLκαι TLS.

3.5.2.1. SECURE SHELL (SSH) PROTOCOL

Το SSH(SecureShell): το πρωτόκολλο αυτό χρησιμοποιείται κυρίως για να εγκαθίδρυση μια απομακρυσμένη σύνδεση με έναν υπολογιστή. Το SSH παρέχει μεγάλη ασφάλεια παρόλο που η σύνδεση η απομακρυσμένη είναι επισφαλείς. Έτσι, επιτυγχάνεται, και η προστασία ακεραιότητας και εμπιστευτικότητας των δεδομένων. Τα κλειδιά που χρησιμοποιεί είναι ήδη προκαθορισμένα και δεν διανέμονται εκείνη τη στιγμή της σύνδεσης.
(Κατσικάς, 2001).



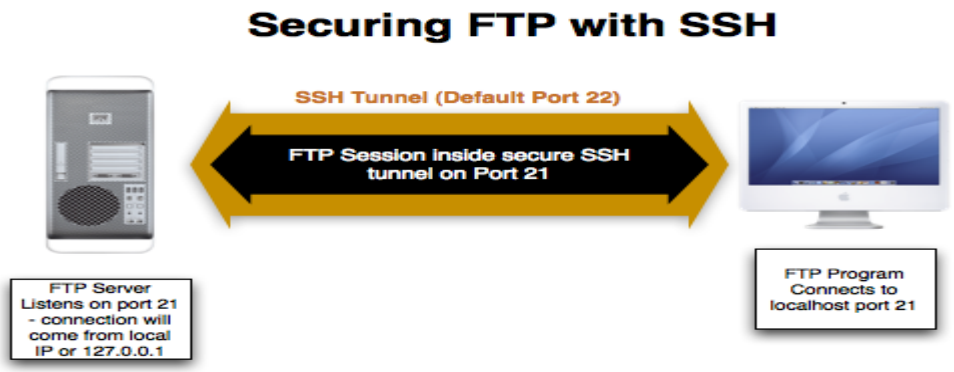
Εικόνα 33 - Σύνδεση SSH {Πηγή: http://www.ytechie.com/2008/05/set-up-a-windows-ssh-tunnel-in-10-minutes-or-less/ }

Έτσι, λοιπόν, έστω ένας χρήστης που θέλει να επικοινωνήσει με έναν απομακρυσμένο υπολογιστή είτε σε κάποιο σημείο του υποδικτύου είτε στο Internet. Χρησιμοποιώντας το πρωτόκολλο SSH, συνδεόμαστε στον υπολογιστή. Θα μας ζητηθεί ο κωδικός σύνδεσης τον οποίον και έχουμε προμηθευτεί. Στη συνέχεια και πληκτρολογώντας το πρωτόκολλο SSH θα μας ωθήσει στην επικύρωση του hostvalidation παρακινώντας μας να προσθέσουμε την συσκευή με την οποία συνδεθήκαμε στον κατάλογο με τους γνωστούς υπολογιστές. Με αυτόν τον τρόπο, το πρωτόκολλο SSL μας παρέχει την προστασία από την περίπτωση του IPSpoofing.Δηλαδή, την περίπτωση που ένας άλλος υπολογιστής υποκρίνεται ότι είναι αυτός στον οποίο και θέλουμε να συνδεθούμε. Το SSH μας προφυλάσσει από αυτό βγάζοντας κατάλληλο μήνυμα όπως το παρακάτω:

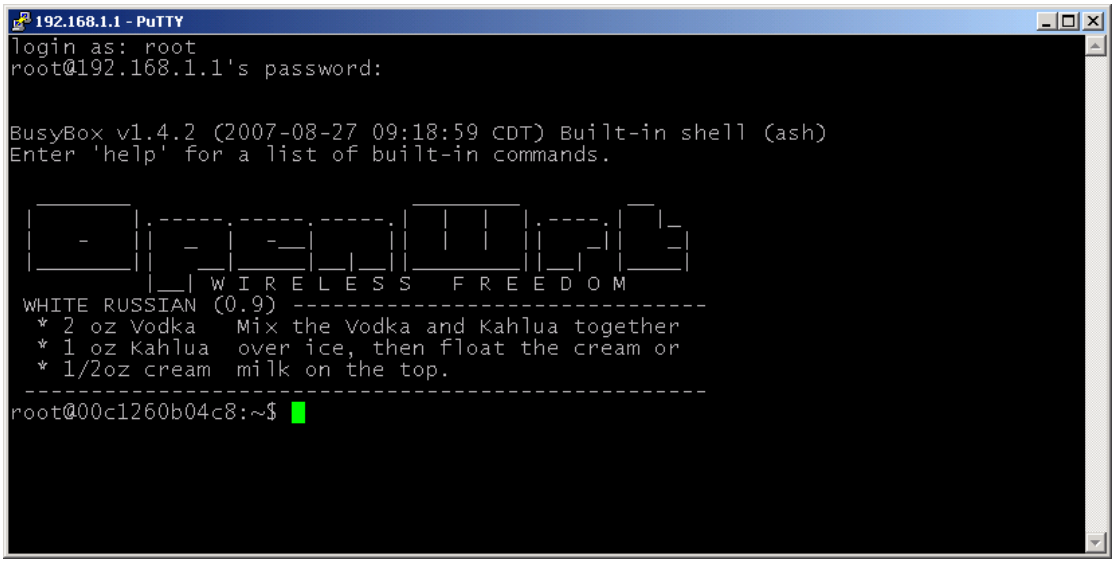
```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: POSSIBLE DNS SPOOFING DETECTED!                    @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The RSA host key for arvo.suso.org has changed,
and the key for the according IP address 216.9.137.122
is unchanged. This could either mean that
DNS SPOOFING is happening or the IP address for the host
and its host key have changed at the same time.
Offending key for IP in /home/suso/.ssh/known_hosts:10
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!            @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
96:92:62:15:90:ec:40:12:47:08:00:b8:f8:4b:df:5b.
Please contact your system administrator.
Add correct host key in /home/suso/.ssh/known_hosts to get rid of this message.
Offending key in /home/suso/.ssh/known_hosts:53
RSA host key for arvo.suso.org has changed and you have requested strict
checking.
Host key verification failed.
```

Εικόνα 34 - Μήνυμα SSH σε περίπτωση IPSpoofing {Πηγή: http://www.cs.uoi.gr/~gkappes/files/tutorials/ssh.pdf }

Επίσης, το SSH πρωτόκολλο χρησιμοποιείται σε συνδυασμό άλλα πρωτόκολλα στο επίπεδο εφαρμογών όπως είναι το FTP (FileTransferProtocol).Αλλά δεν θα αναφερθούμε σε αυτήν την ένωση σε αυτήν την ενότητα.



Εικόνα 35 - FTP&SSH {Πηγή:*http://www.sant-media.co.uk/2010/05/achieve-secure-ftp-sftp-with-dreamweaver-using-ssh-tunneling/* }



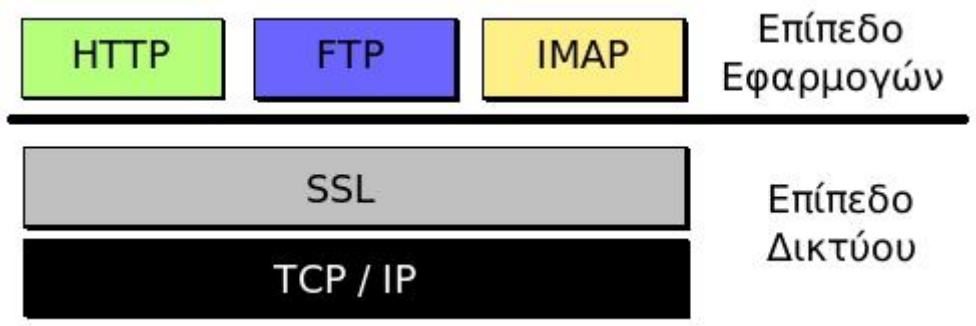
Εικόνα 36 - Άποψη σύνδεσης με πρωτόκολλο SSH {Πηγή: ***https://en.wikipedia.org/wiki/Secure_Shell*** }

3.5.2.2. SECURE SOCKET LAYER PROTOCOL (SSL)

Στο πρωτόκολλο αυτό έγινε μια μικρή αναφορά στις παραπάνω ενότητες. Σε αυτήν τώρα, θα δούμε εκτενέστερα τη λειτουργία του και τη χρηστικότητα του. Ας τα πάρουμε από την αρχή.

Το πρωτόκολλο αυτό προτάθηκε από την εταιρεία Netscape, η οποία ήταν αυτή που κυκλοφόρησε τον πρώτο browsertον NetscapeNavigator, το 1994. Ο σκοπός της δημιουργίας του είναι η ασφαλής διακίνηση μεταξύ δικτύων και κυρίως του Διαδικτύου, ευαίσθητων πληροφοριών όπως είναι οι κωδικοί (passwords), αριθμοί πιστωτικών καρτών κτλ.
Το SSL ουσιαστικά εγκαθιδρύεται μεταξύ των επιπέδων μεταφορά και δικτύου και παρέχει υπηρεσίας κρυπτογράφησης στα πακέτα και στα δεδομένα που αυτά φέρουν. Η κρυπτογράφηση που παρέχει βασίζεται στους αλγορίθμους δημοσίου κλειδιού για αυτό και μπορεί να χρησιμοποιεί κατά βούληση κάποιον από αυτούς όπως ο RSAπχ. «*Θα μπορούσαμε να μπούμε ότι παρέχει πιστοποίηση του server από τον client, την πιστοποίηση του client από τον server και την εγκαθίδρυση ασφαλούς κρυπτογραφημένου διαύλου επικοινωνίας μεταξύ των δύο μερών.*» (http://ru6.cti.gr/ru6/system/files/bouras_site/ergasies_foithtwn/TLS_protocol_kollia.pdf?language=el).

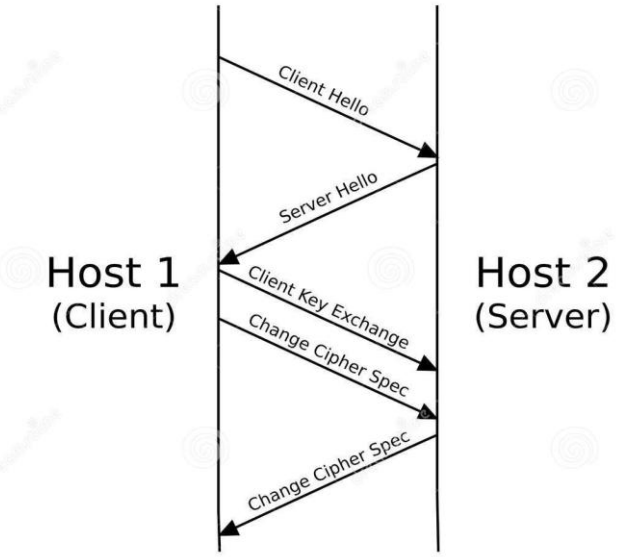
Το SSL το συναντάμε σε πρωτόκολλα του επιπέδου εφαρμογής και κατά κόρον στο πρωτόκολλο HTTP (HyperText Trasfer Protocol). Το χρησιμοποιεί το συγκεκριμένο πρωτόκολλο έτσι ώστε να εξασφαλίσει ότι οι πληροφορίες που αποστέλλονται από τον client στον server δεν θα υποκλαπούν κατά τη διάρκεια της μετάδοσης τους στο δίκτυο. Για αυτό και το συναντάμε αρκετά συχνά στις διατραπεζικές ηλεκτρονικές συναλλαγές αλλά και οπουδήποτε χρειάζεται να δώσουμε ευαίσθητες πληροφορίες.



Εικόνα 37 – SSL { Πηγή:*https://el.wikipedia.org/wiki/SSL*}

Ας δούμε όμως πώς πραγματοποιείται αυτή η ασφαλής ανταλλαγή πληροφοριών μεταξύ client και server.

Έστω ότι ο χρήστης θέλει να συνδεθεί με μια τοποθεσία η οποία προστατεύεται από το πρωτόκολλο SSL. Κάνει δηλαδή μια αίτηση στο SSLWebServer και ξεκινάει η εγκαθίδρυση της συνόδου μεταξύ του χρήστη και του server. Αυτή η σύνοδος ονομάζεται SSLhandshaking (χειραψία). Η χειραψία παραγοντοποιείτο σε δύο μέρη. Στο πρώτο μέρος, γίνεται η συμφωνία για την χρήση κρυπτογραφικών αλγορίθμων και έτσι αποστέλλεται το κλειδί καθώς επίσης γίνεται και η πιστοποίηση του server. Στο δεύτερο μέρος της χειραψίας SSL, ζητείται συνήθως η ταυτότητα του χρήστη. Μόλις ταυτοποιηθεί ο χρήστης τότε η χειραψία ολοκληρώνεται και μπορεί πια να αρχίσει να γίνεται η μεταφορά των πληροφοριών χωρίς φόβο κλοπής τους.



Εικόνα 38 - SSLXειραψία {Πηγή: *https://gr.dreamstime.com/ssl-tsl-image41256404* }

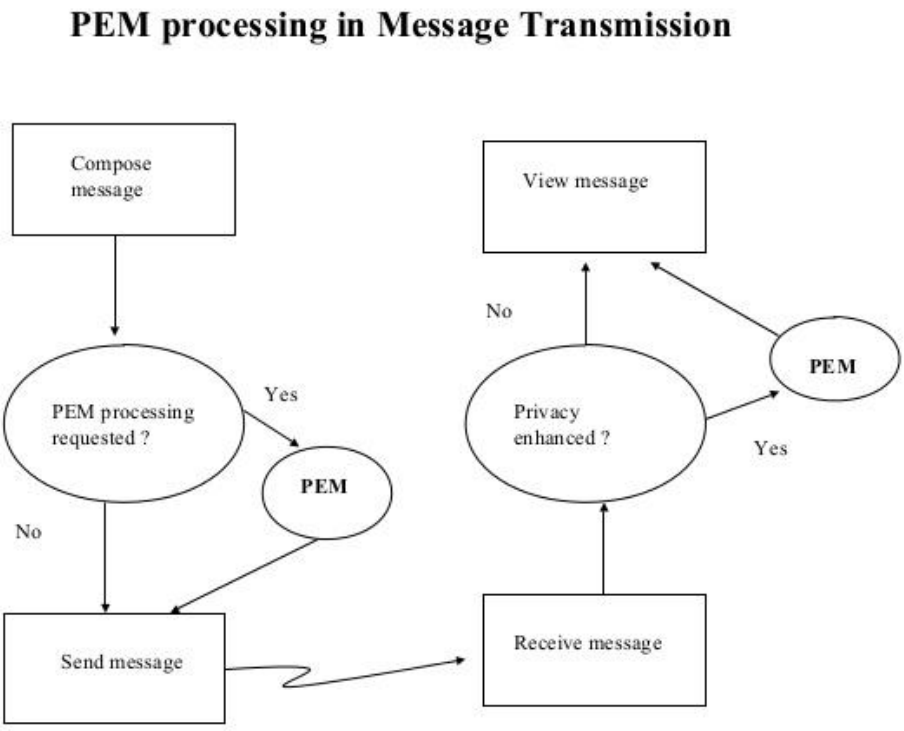
Το SSL έχει αποδειχθεί ότι είναι ιδιαίτερο ανθεκτικό σε αρκετές περιπτώσεις επιθέσεων ακόμα και των πιο 'βίαιων'. Σε αρκετές από τις επιθέσεις όπως (BruteForceAttack κοκ) είναι ισχυρό διότι χρησιμοποιεί κλειδιά μήκους 128 bit. Και όπως είχαμε προαναφέρει όσο μεγαλύτερο το μήκος των κλειδιών τόσο δυσχεραίνει η θέση των επιτιθέμενων διότι τα πιθανά κλειδιά είναι εκατοντάδες.
Όμως εκεί όπου αδυναμεί είναι στις επιθέσεις POODLE. Σε αυτές τις επιθέσεις , ο επιτιθέμενος εξαναγκάζει χρησιμοποιώντας τις κατασκευαστικές αδυναμίες του SSL και κυρίως της version 3.0, να αποκαλύψει τις πληροφορίες που έχει κρυπτογραφήσει. Επειδή, όμως, αυτή η αδυναμία του είναι πολύ σημαντική δημιουργήθηκε το πρωτόκολλο TLS που ήρθε να 'μπαλώσει' το κενό ασφαλείας του SSL.

Εικόνα 39 - SSL/TLS {Πηγή: *http://www.golgi.io/security-ssl-tls/* }

3.5.3. ΠΡΩΤΟΚΟΛΛΑ ΑΣΦΑΛΕΙΑ ΣΤΟ ΕΠΙΠΕΔΟ ΕΦΑΡΜΟΓΗΣ

Και φτάσαμε στο επίπεδο εφαρμογής. Στο επίπεδο αυτό συναντώνται όλα εκείνα τα πρωτόκολλα τα οποία είναι το Telnet–απομακρυσμένη πρόσβαση, SMTP – το πρωτόκολλο για την αποστολή ηλεκτρονικού ταχυδρομείου, FTP- πρωτόκολλο για τη μεταφορά αρχείων μεταξύ υπολογιστών σε διαφορετικά δίκτυα κοκ.

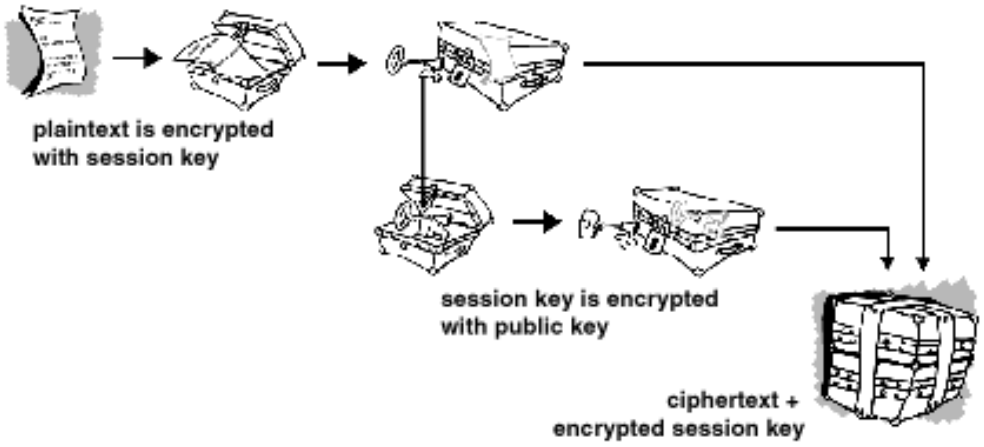
- SecureTelnet: Είναι η ασφαλής λειτουργία του Telnet. Πρόκειται για μια κωδικοποιημένη εφαρμογή και αποστολή στοιχείων. Συγκεκριμένα , χρησιμοποιεί τον αλγόριθμο Difiie-Hellman.
- SecureE-mail: Το πρωτόκολλο το οποίο χρησιμοποιείται στο ηλεκτρονικόταχυδρομείοονομάζεταιSMTP – SimpleMailTransferProtocol δηλαδή αποστολή απλού email. Αυτό σημαίνει ότι το μήνυμα μας κυκλοφορεί μεσα στα διάφορα δίκτυα και δρομολογητές με την μορφή απλού κειμένου. Το απλό κείμενο είναι πολύ εύκολα να αντιγραφεί και στη συνέχεια να υποκλαπεί η πληροφορία που περιέχει. Και αυτό διότι δεν περιέχει κάποια κρυπτογράφηση. Θα μπορούσαμε να πούμε ότι οτιδήποτε γράφουμε ακριβώς έτσι ταξιδεύει μέσα στο φυσικό μέσο των δικτύων.
  Όπως είναι φυσικό , δεν είναι αυτό που επιθυμούμε – να υποκλέπτει κανείς τα περιεχόμενα των μηνυμάτων μας. Για αυτό , λοιπόν, έχουν αναπτυχθεί διάφοροι τρόποι προστασίας αυτών των μηνυμάτων.
  Σήμερα, ισχύουν τρία είδη ασφάλειας: το PEM (PrivacyEnhancedMail), το PGP (PrettyGoodPrivacy) και το MIME. Ας δούμε λίγα πράγματα για το πώς λειτουργεί το καθένα από αυτά.
  - PEM: Προτάθηκε το 1993. Αποτελείται από δύο τμήματα. Την επικεφαλίδα η οποία και περιέχει τις πληροφορίες του μηνύματος. Όπως πχ ποιος αλγόριθμος κρυπτογράφησης χρησιμοποιήθηκε κτλ. Το δεύτερο τμήμα από το οποίο αποτελείται ονομάζεται τμήμα κειμένου και όπως είναι φανερό από το όνομα του περιέχει το μήνυμα μας μόνο που είναι κρυπτογραφημένο.
    Αξίζει να σημειωθεί ότι η συγκεκριμένη τακτική παρέχει αυθεντικοποίηση, εμπιστευτικότητα και πιστοποίηση. Παρακάτω, φαίνεται αναλυτικά η λειτουργία του.



Εικόνα 40 - Λειτουργία του PEM {Πηγή: http://www.slideshare.net/afiqefendy/network-security-chapter-7 }

- PGP(PrettyGoodPrivacy): ToPGP είναι και αυτό ένα σύστημα κρυπτογράφησης. Το αξιοθαύμαστο σε αυτήν την περίπτωση είναι ότι αποτελεί ένα υβριδικό σύστημα κρυπτογράφησης. Είχαμε κάνει αναφορά στην υβριδική κρυπτογράφηση στις παραπάνω ενότητες. Πρόκειται για συνδυασμό και των δύο κατηγοριών δηλαδή και του συμμετρικού και του δημόσιου κλειδιού. Ας δούμε τη λειτουργία του.
  Αρχικά, το μήνυμα μας συμπιέζεται για λόγο και ταχύτητας αλλά κι ότι έτσι παράγεται μεγαλύτερη ακρίβεια στην κρυπτογράφηση. Στη συνέχεια, το συμπιεσμένο μήνυμα θα κρυπτογραφηθεί με τη βοήθεια ενός κλειδιού (sessionkey) το οποίο και δημιουργείται τυχαία από την κίνηση του ποντικιού και των πλήκτρων που έχουμε επιλέξει. Για αυτό και το κλειδί αυτό είναι μιας φοράς αφού τόσο οι συνδυασμοί κινήσεων όσο και τα πλήκτρα κάθε φορά εναλλάσσονται χωρίς να ακολουθούν κάποιο συγκεκριμένο μοτίβο. Μόλις γίνει η κρυπτογράφηση του προς αποστολή μηνύματος , τότε στέλνεται στον παραλήπτη – πάντα κρυπτογραφημένο- το κλειδί που παρήχθηκε έτσι ώστε να

είναι σε θέση να ακολουθήσει την αντίστροφη πορεία για την αποκρυπτογράφηση του μηνύματος.
(http://www.pgpi.org/doc/pgpintro/#p10).



Εικόνα 41 - PGPΛειτουργία {Πηγή: *https://users.ece.cmu.edu/~adrian/630-f04/PGP-intro.html* }

Αξίζει να σημειωθεί ότι το PGP υποστηρίζει τα εξής μήκη κλειδιών:

- Μήκος 512bits
- Μήκος 768 bits
- Μήκος 1024 bits τα οποία εκτός του ότι χρησιμοποιούνται σε στρατιωτικές εφαρμογές , πια είναι και το standard μήκος κλειδιών που χρησιμοποιεί παγκοσμίως.
  (Κατσικάς, 2001)

- MIME: Το συγκεκριμένο πρότυπο χρησιμοποιεί αλγορίθμους κρυπτογράφησης όπως DES , 3DESκαι RC2 για την κρυπτογράφηση του μηνύματος.

3.5.4. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από ότι παρατηρούμε, λόγω της ανάγκης μας για ασφάλεια , εμπιστευτικότητα και προστασία των δεδομένων μας και πληροφοριών μας, σχεδιάστηκαν , προτάθηκαν και εφαρμόστηκαν πολλοί αλγόριθμοι και πρότυπα ασφαλείας. Αυτά τα πρότυπα βρίσκουν εφαρμογή και σε οποιοδήποτε δίκτυο αλλά βέβαια και στο Διαδίκτυο.

Τα πρότυπα και πρωτόκολλα που αναφέρονται στις παρούσες ενότητες δεν είναι παρά κάποια από όλα αυτά που κατά καιρούς έχουν εφαρμοστεί. Για λεπτομέρειες όσο αφορά τη λειτουργία τους, καλό θα ήταν να ακολουθηθούν οι σύνδεσμοι στο παράρτημα.

3.6. ΑΣΦΑΛΕΙΑ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

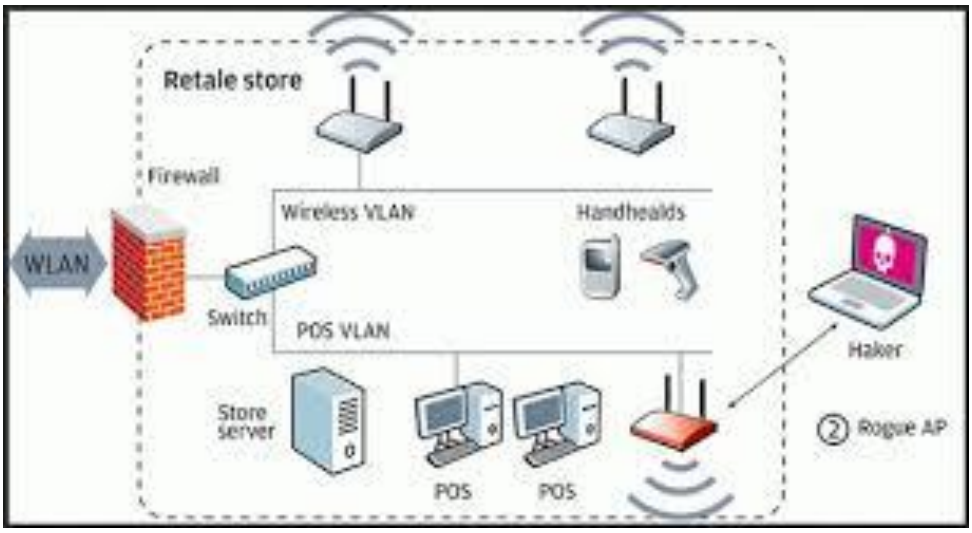
Στην εισαγωγική ενότητα , είχε αναφερθεί μεταξύ των άλλων και τα ασύρματα δίκτυα. Όμως, πριν προβούμε στην ανάλυση της ασφάλειας σε αυτά τα δίκτυα, καλό θα ήταν να αναφέρουμε τους κινδύνους που αντιμετωπίζουν.

3.6.1. ΚΙΝΔΥΝΟΙ ΣΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Δυστυχώς, τα ασύρματα δίκτυα μπορούμε να πούμε ότι είναι πιο επιρρεπής στις επιθέσεις από τρίτους διότι τα πακέτα πληροφοριών ταξιδεύουν στον αέρα κυριολεκτικά εν αντιθέσει με το φυσικό μέσο που ούτος ή άλλως έχει περιορισμούς λόγω κατασκευής. Ας πάμε να δούμε τις απειλές.

- Επιθέσεις με στόχο την συλλογή πληροφοριών:
  Αυτές οι επιθέσεις έχουν σαν στόχο, να συλλέξουν πληροφορίες όσο αφορά τις μεθόδους κρυπτογράφησης καθώς και τον τρόπο λειτουργίας των router. Συλλέγοντας πληροφορίας για το πώς μεταδίδεται μια πληροφορία , καθιστά πιο εύκολη την υποκλοπή της πληροφορίας.
- Επιθέσεις με στόχο τα πακέτα πληροφοριών:
  Αυτή η μέθοδος έχει αναφερθεί και ως packetsniffing. Ουσιαστικά, ο επιτιθέμενος συλλέγει όλα τα πακέτα του ασύρματου δικτύου με απώτερο σκοπό να μπορέσει να διαβάσει τα περιεχόμενα τους.
- Επιθέσεις μη εξουσιοδοτημένης πρόσβασης:
  Ο επιτιθέμενος προσπαθεί να βρειέναν τρόπο να εισχωρήσει στο ασύρματο δίκτυο και να υποκλέψει όλες τις πληροφορίες του. Ουσιαστικά πρόκειται για έναν μη εξουσιοδοτημένο χρήστη , δηλαδή έναν χρήστη εκτός από αυτούς που τους έχει δοθεί συγκεκριμένη άδεια με συγκεκριμένη πρόσβαση από τον διαχειριστή.
- ΕπιθέσειςMan – In – The _ Middle – Attack:
  Οεπιτιθέμενος ουσιαστικά παίρνει το ρόλο του διαμεσολαβητή. Δηλαδή παρουσιάζεται ως serverστο χρήστη και ως χρήστης στον server.
- Επιθέσεις Άρνησης Παροχής Υπηρεσιών:
  Αυτές οι επιθέσεις είναι ακριβώς ίδιες όπως τις περιγράψαμε και σε προηγούμενη ενότητα. Με το βομβαρδισμό από πακέτα δεδομένων, το δίκτυο είναι ανήμπορο να αντεπεξέλθει και έτσι δεν μεταδίδει και ουσιαστικά δεν

λειτουργεί. Βέβαια, ένας άλλος τρόπος να γίνει αυτή η επίθεση, μια που μιλάμε για ασύρματα δίκτυα, είναι ουσιαστικά να υπερφορτωθεί το κανάλι με σήματα – κυρίως άχρηστα-.
(http://docplayer.gr/3170474-Asfaleia-sta-asyrmata-topika-diktya-wpa-wpa2.html).



Εικόνα 42 – Εεπιθέσεις [Πηγή: http://blog.jammer-store.com }

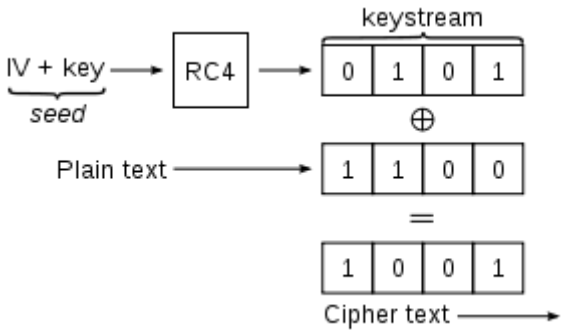
3.6.2. ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ ΓΙΑ ΤΑ ΑΣΥΡΜΑΤΑ ΔΙΚΤΥΑ

Στην εποχή που διανύουμε, όλοι μας η καθημερινότητα 'κρέμεται' από τα δίκτυα. Είτε στο σπίτι, είτε στη δουλειά είτε στο καφέ είτε στη βόλτα θέλουμε να είμαστε συνδεδεμένοι. Έτσι, είμαστε υπό το καθεστώς των ασύρματων δικτύων. Όμως, δεν θα ήταν τόσο ευρέως χρησιμοποιούμενα εάν δεν έπαιρναν και τις κατάλληλες προφυλάξεις – όσο δύναται- για την προστασία των δεδομένων και πληροφοριών μας.

Όταν άρχισε η επανάσταση των ασύρματων δικτύων προτάθηκε το πρωτόκολλο ασφαλείας WEP. Το πρωτόκολλο αυτό είναι κρυπτογράφησης και χρησιμοποιεί το RC4 για την δουλειά αυτή. Η χρήση αυτού του συμμετρικού αλγορίθμου κρυπτογράφησης ευνοεί την εμπιστευτικότητα των δεδομένων. Και αυτό επιτυγχάνεται διότι ο αλγόριθμος αυτός παράγει μια ακολουθία από Bit που συνδυάζεται με τη συνάρτηση xor και με το μήνυμα που κρυπτογραφήθηκε με το κλειδί του αλγορίθμου.

Το δυστύχημα σε αυτό το πρωτόκολλο είναι ότι χρησιμοποιεί κλεδί κρυπτογράφησης

είναι μόλις 40 bit μήκος. Έτσι γίνεται ευάλωτο σε επιθέσεις. Αυτό το μειονέκτηματου WEP τον άφησε πίσω ξεχασμένο αφού τον αντικατέστησε το νέο πρωτόκολλο ασφάλειας WPA.



Εικόνα 43 - Αναλυτική απόδοση λειτουργίας WEP {Πηγή: https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy }

Το επόμενο βήμα στην προστασία των ασύρματων δικτύων ήταν το WAP και σήμερα το WAP2. Το WAP(Wi-FiProtectedarea) είναι ένα πρωτόκολλο που ήρθε να καλύψει τα κενά ασφαλείας του WEP. Χρησιμοποιεί και αυτό το ίδιο αλγόριθμο κρυπτογράφησης RC4 μόνο που το κλειδί του έχει πια μήκος 128bits.
Το ιδιαίτερο σε αυτό το πρωτόκολλο είναι ότι χρησιμοποιεί ένα άλλο πρωτόκολλο το οποίο αναλαμβάνει δυναμικά την ανανέωση των κλειδιών που χρησιμοποιεί το WPA. Έτσι , με αυτόν τον τρόπο τα κλειδιά δεν είναι ποτέ ίδια και μειώνεται η πιθανότητα εντοπισμού των κλειδιών. Η διαδικασία αυθεντικοποίησης και λειτουργίας του WPAδεν θα μας απασχολήσει σε αυτήν την εργασία.

3.7. ΣΥΜΠΕΡΑΣΜΑΤΑ

Σύμφωνα με τα παραπάνω βλέπουμε ότι την προσπάθεια να προστατευτούν τα δεδομένα γίνεται όλο και πιο έντονη.
Σε όλο το φάσμα των δικτύων, τοπικών, ευρείας περιοχής , ασυρμάτων, παρουσιάζονται πρωτόκολλα ασφαλείας. Αρκετά από αυτά έχουν πια καθιερωθεί λόγω της ικανότητας τους να προστατεύουν τα δεδομένα σχεδόν σε όλες τις επιθέσεις που έχουν προαναφερθεί.
Σε άλλα πάλι δίκτυα, όπως αυτά στα ασύρματα, η προστασία των δεδομένων είναι ακόμα αμφιλεγόμενη.
Με βάση όλα αυτά, μπορούμε με βεβαιότητα πια να πούμε ότι όχι μόνο ζούμε στην εποχή της πληροφορίας και της τεχνολογίας αλλά και της ασφάλειας της πληροφορίας. Μπορούμε πια με άνεση να εκτελούμε τις καθημερινές ανάγκες όπως πληρωμή δανείων, αγορά αγαθών κτλ από το σπίτι μας και μόνο με ένα κλικ.
Η ανασφάλεια της υποκλοπής είναι πια μηδαμινή αρκεί βέβαια να γνωρίζουμε και πως προστατευόμαστε αλλά κυρίως από τι κινδυνεύουμε.
Η ασφάλεια των δικτύων είναι πια συνυφασμένη με την ανάπτυξη της τεχνολογίας.

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1]. Tanenbaum S, & Wetherall D,2012, *«Δίκτυα Υπολογιστών»,* Αθήνα: Κλειδάριθμος

[2 Αρβανίτης Κ, Κολυβάς Γ & Ούτσιος .Σ, (2012),*«Τεχνολογία Δικτύων Υπολογιστών»* , Αθήνα: Παιδαγωγικό Ινστιτούτο

[3]. Γεωργακόπουλος Κ, (2007), *«Τεχνολογίες Σύγχρονων Ασύρματων Δικτύων Δεδομένων»,* Καβάλα: ΤΕΙ ΚΑΒΑΛΑΣ

[4] Γεωργίου Θ, Κάππος Ι.,Λαδιάς Α, κ.α, *«Πολυμέσα – Δίκτυα»*, Αθήνα: Οργανισμός Διδακτικών Βιβλίων

[5].Καγιάς Μ, (2006), *«Μετάδοση Δεδομένων και Δίκτυα Υπολογιστών- Το Ανεπίσημο Βοήθημα»*, Χανιά: Μανώλης Καγιάς

[6]. Κάτσικας Σ., (2001), *«Ασφάλεια Δικτύων»,* Πάτρα: Ελληνικό Ανοικτό Πανεπιστήμιο

[7]. Λυκούδης Κ., (2012), *«Συμμετρικοί αλγόριθμοι Κρυπτογράφησης Δεδομένων – Η περίπτωση του αλγορίθμου AES»*, Πάτρα: Πανεπιστήμιο Πατρών.

[8]. Πρέβες Ν, (2008), *«Ασύρματα Δίκτυα Υπολογιστών»,* Αθήνα: Εκδόσεις Νέων Τεχνολογιών

[9].Σάνδρος Β., (2012), *«Φορητότητα Δικτύων – Βελτιστοποίηση Δρομολόγησης»*, Θεσσαλονίκη: Πανεπιστήμιο Μακεδονίας

ΠΑΡΑΡΤΗΜΑ ΙΣΤΟΣΕΛΙΔΩΝ

1. https://sites.google.com/site/eisagogestadiktyaypologiston1/diadiktyo-internet/e-istoria-tou-diadiktyou { Ανακτήθηκε στις 3/6/2016 }
2. http://ecourse.uoi.gr/course/view.php?id=1103 { Ανακτήθηκε στις 3/6/2016 }
3. http://www.pi-schools.gr/programs/ktp/previous_version/book2/04_1.pdf { Ανακτήθηκε στις 3/6/2016 }
4. http://docplayer.gr/10016887-Kefalaio-7-7-1-7-4-e-p-a-n-a-l-i-ps-i-epikoinoniako-ypodiktyo-tcp-udp-sel-220-241.html { Ανακτήθηκε στις 3/6/2016 }
5. http://users.ionio.gr/~emagos/networks/msc/5/5-TCPIP%20-%202sel.pdf { Ανακτήθηκε στις 3/6/2016 }
6. http://eclass.sch.gr/modules/document/file.php/T58111/%CE%A4%CE%BF%20%CF%80%CF%81%CF%89%CF%84%CF%8C%CE%BA%CE%BF%CE%BB%CE%BB%CE%BF%20TCP-IP.pdf {Ανακτήθηκε στις 5/6/2016}
7. https://semfe.gr/files/users/184/topika_diktya.pdf {Ανακτήθηκε στις 5/6/2016}
8. http://teacher-nik.freeservers.com/NetworksTopology1.htm {Ανακτήθηκε στις 7/6/2016}
9. https://diktuateecr.wordpress.com/tag/%CE%A4%CE%BF%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1-%CE%B4%CE%B1%CE%BA%CF%84%CF%85%CE%BB%CE%AF%CE%BF%CF%85/ {Ανακτήθηκε στις 7/6/2016}
10. http://blogs.sch.gr/lykmakro/files/2013/01/%CE%A4%CE%BF%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B5%CF%82-%CE%B4%CE%B9%CE%BA%CF%84%CF%8D%CF%89%CE%BD.pdf {Ανακτήθηκε στις 7/6/2016}
11. http://thebook.homeunix.com/node22.html {Ανακτήθηκε στις 13/6/201
12. http://www.noesis.edu.gr/%CE%B5%CF%80%CE%B9%CF%83%CF%84%CE%AE%CE%BC%CE%B7-%CE%BA%CE%B1%CE%B9-%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE

%B3%CE%AF%CE%B1/%CF%85%CF%80%CE%BF%CE%BB%CE%BF%CE%B3%CE%B9%CF%83%CF%84%CE%AD%CF%82/%CF%84%CE%B5%CF%87%CE%BD%CE%BF%CE%BB%CE%BF%CE%B3%CE%AF%CE%B1/%CE%B4%CE%AF%CE%BA%CF%84%CF%85%CE%B1-%CE%B5%CF%85%CF%81%CE%B5%CE%AF%CE%B1%CF%82-%CF%80%CE%B5%CF%81%CE%B9%CE%BF%CF%87%CE%AE%CF%82-wan/ {Ανακτήθηκε στις 13/6/2016}

13. http://www.cse.uoi.gr/~epap/asurmata/downloads/lect6.pdf {Ανακτήθηκε 16/6/2016}
14. http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/114/tlp_000385.pdf?sequence=1 {Ανακτήθηκε στις 2/7/2016}
15. http://195.130.124.90/~emagos//networks/msc/4/4-asirmata%20-%202sel.pdf {Ανακτήθηκε στις 2/7/2016}
16. http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/114/tlp_000385.pdf?sequence=1 {Ανακτήθηκε στις 5/7/2016}
17. http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/163/tlp_000437.pdf?sequence=1{Ανακτήθηκε στις 5/7/2016}
18. https://eclass.upatras.gr/modules/document/file.php/CULTURE110/Enotita_5.pdf {Ανακτήθηκε στις 8/7/2016}
19. http://resources.infosecinstitute.com/windows-cryptography-api/{Ανακτήθηκε στις 10/7/2016}
20. http://teachers.teicm.gr/chilas/files/D_III/public_key_cryptography.pdf {Ανακτήθηκε στις 10/7/2016}
21. users.uom.gr/~steph/material/crypto/HAC_Ch01.pdf {Ανακτήθηκε στις 10/7/2016}
22. https://www.cs.ucy.ac.cy/courses/EPL674/lectures/ch09-GR-Public-Key-Ciphers.pdf{Ανακτήθηκε στις 11/7/2016}
23. http://195.130.124.90/~emagos//security/3/Simeioseis-Kryptografia.pdf {Ανακτήθηκε στις 14/7/2016}

24. http://nemertes.lis.upatras.gr/jspui/bitstream/10889/5467/1/%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CE%AF%20%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CE%B9%20%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7%CF%82%20%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD.pdf {Ανακτήθηκε στις 15/7/2016}

25. http://cgi.di.uoa.gr/~klimn/cryptography/Lab/Lab-7.pdf {Ανακτήθηκε στις 15/7/2016}

26. http://teachers.teicm.gr/chilas/files/D_III/General_intro_to_security.pdf {Ανακτήθηκε στις 20/7/2016}

27. http://www.icsd.aegean.gr/website_files/proptyxiako/525297129.pdf {Ανακτήθηκε στις 20/7/2016}

28. https://www.cs.ucy.ac.cy/courses/EPL674/lectures/ch01GR.pdf {Ανακτήθηκε στις 20/7/2016}

29. http://nemertes.lis.upatras.gr/jspui/bitstream/10889/5467/1/%CE%A3%CF%85%CE%BC%CE%BC%CE%B5%CF%84%CF%81%CE%B9%CE%BA%CE%BF%CE%AF%20%CE%91%CE%BB%CE%B3%CF%8C%CF%81%CE%B9%CE%B8%CE%BC%CE%BF%CE%B9%20%CE%9A%CF%81%CF%85%CF%80%CF%84%CE%BF%CE%B3%CF%81%CE%AC%CF%86%CE%B7%CF%83%CE%B7%CF%82%20%CE%94%CE%B5%CE%B4%CE%BF%CE%BC%CE%AD%CE%BD%CF%89%CE%BD.pdf {Ανακτήθηκε στις 20/7/2016}

30. http://www.image.ntua.gr/meleti172KTP/?q=node/23 {Ανακτήθηκε στις 22/7/2016}

31. http://cgi.di.uoa.gr/~klimn/cryptography/Lab/lab-1.pdf {Ανακτήθηκε στις 22/7/2016}

32. https://www.cs.ucy.ac.cy/courses/EPL674/lectures/ch03-GR-Block-Ciphers.pdf {Ανακτήθηκε στις 22/7/2016}

33. https://repository.kallipos.gr/bitstream/11419/1031/1/05_Chapter_07.pdf {Ανακτήθηκε στις 22/7/2016}

34. http://cgi.di.uoa.gr/~klimn/cryptography/chapter_4-Public_Key_Cryptography.pdf {Ανακτήθηκε στις 25/7/2016}

35. http://bpliroftest.weebly.com/eta-kapparhoupsilonpitauomicrongammarhoalphaphiiotaalpha-sigmaetamuepsilonrhoalpha.html {Ανακτήθηκε στις 25/7/2016}

36. http://cgi.di.uoa.gr/~klimn/cryptography/Lab/Lab-6.pdf {Ανακτήθηκε στις 1/8/2016}

37. http://cgi.di.uoa.gr/~klimn/cryptography/Lab/Lab-10.pdf {Ανακτήθηκε στις 1/8/2016}

38. https://openeclass.teimes.gr/modules/document/file.php/CIED194/lecture05.pdf {Ανακτήθηκε στις 1/8/2016}

39. https://www.ceid.upatras.gr/webpages/faculty/papaioan/dchmnt/2015-16/ita/lectures/lec2.pdf{Ανακτήθηκε στις 4/8/2016}

40. http://www.comsol.gr/dat/04FFDD5A/file.pdf {Ανακτήθηκε στις 6/8/2016}

41. http://crypto.di.uoa.gr/class/Kryptographia/Semeioseis_files/6_digitalsig_handout_gr.pdf{Ανακτήθηκε στις 6/8/2016}

42. http://www.image.ntua.gr/meleti172KTP/?q=node/23{Ανακτήθηκε στις 9/2016}

43. http://apothetirio.teiep.gr/xmlui/bitstream/handle/123456789/5013/1271.pdf?sequence=1{Ανακτήθηκε στις 9/8/2016}

44. http://www.comsol.gr/dat/04FFDD5A/file.pdf {Ανακτήθηκε στις 17/8/2016}

45. https://www.cs.ucy.ac.cy/courses/EPL674/lectures/Authentication-ch15-GR.pdf {Ανακτήθηκε στις 17/8/2016}

46. http://eclass.opencourses.teicm.gr/eclass/modules/document/file.php/TMC112/12_IPsec.pdf {Ανακτήθηκε στις 17/8/2016}

47. http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ipsec.htm {Ανακτήθηκε στις 17/8/2016}

48. http://www.cs.uoi.gr/~gkappes/files/tutorials/ssh.pdf {Ανακτήθηκε στις 22/8/2016}

49. http://ru6.cti.gr/ru6/system/files/bouras_site/ergasies_foithtwn/TLS_protocol_kollia.pdf?language=el{Ανακτήθηκε στις 22/8/2016}

50. http://www.islab.demokritos.gr/gr/html/ptixiakes/kostas-aris_ptyxiakh/Phtml/ssl.htm {Ανακτήθηκε στις 22/8/2016}

51. http://www.icsd.aegean.gr/website_files/proptyxiako/871591340.pdf {Ανακτήθηκε στις 22/8/2016}

52. http://www.csee.umbc.edu/~woodcock/cmsc482/proj1/pem.html {Ανακτήθηκε στις 22/8/2016}

53. https://www.acsac.org/secshelf/book001/17.pdf {Ανακτήθηκε στις 2/9/2016}

54. http://www.pgpi.org/doc/pgpintro/ {Ανακτήθηκε στις 2/9/2016}

55. http://www.cse.uoi.gr/~epap/asurmata/downloads/lect6.pdf {Ανακτήθηκε στις 2/9/2016}

56. http://opencourses.uoa.gr/modules/document/file.php/DI34/%CE%94%CE%B9%CE%B4%CE%B1%CE%BA%CF%84%CE%B9%CE%BA%CF%8C%20%CF%80%CE%B1%CE%BA%CE%AD%CF%84%CE%BF/%CE%A0%CE%B1%CF%81%CE%BF%CF%85%CF%83%CE%B9%CE%AC%CF%83%CE%B5%CE%B9%CF%82/PDF/Lecture-10.pdf {Ανακτήθηκε στις 2/9/2016}

57. http://docplayer.gr/3170474-Asfaleia-sta-asyrmata-topika-diktya-wpa-wpa2.html {Ανακτήθηκε στις 2/9/2016}

58. http://searchmobilecomputing.techtarget.com/definition/WAP {Ανακτήθηκε στις 2/9/2016}