2018

Ασφάλεια στο Web: Παρουσίαση-Ανάλυση-Σύγκριση όλων των τεχνικών στα επίπεδα Δικτύου, Μεταφοράς και Εφαρμογής.

Υπεύθυνος Καθηγητής:
Νικόλαος Κατσάκος-Μαυρομιχάλης
Εργασία της Φοιτήτριας:
Χαραλαμποπούλου Παρασκευή 2012-126

ΔΗΛΩΣΗ ΜΗ ΛΟΓΟΚΛΟΠΗΣ ΚΑΙ ΑΝΑΛΗΨΗΣ ΠΡΟΣΩΠΙΚΗΣ ΕΥΘΥΝΗΣ

"Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ενυπογράφως ότι είμαι αποκλειστικός συγγραφέας της παρούσας Πτυχιακής Εργασίας, για την ολοκλήρωση της οποίας κάθε βοήθεια είναι πλήρως αναγνωρισμένη και αναφέρεται λεπτομερώς στην εργασία αυτή. Έχω αναφέρει πλήρως και με σαφείς αναφορές, όλες τις πηγές χρήσης δεδομένων, απόψεων, θέσεων και προτάσεων, ιδεών και λεκτικών αναφορών, είτε κατά κυριολεξία είτε βάση επιστημονικής παράφρασης.

Αναλαμβάνω την προσωπική και ατομική ευθύνη ότι σε περίπτωση αποτυχίας στην υλοποίηση των ανωτέρω δηλωθέντων στοιχείων, είμαι υπόλογος έναντι λογοκλοπής, γεγονός που σημαίνει αποτυχία στην Πτυχιακή μου Εργασία και κατά συνέπεια αποτυχία απόκτησης του Τίτλου Σπουδών, πέραν των λοιπών συνεπειών του νόμου περί πνευματικών δικαιωμάτων.

Δηλώνω, συνεπώς, ότι αυτή η Πτυχιακή Εργασία προετοιμάστηκε και ολοκληρώθηκε από εμένα προσωπικά και αποκλειστικά και ότι, αναλαμβάνω πλήρως όλες τις συνέπειες του νόμου στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δε μου ανήκει διότι είναι προϊόν λογοκλοπής άλλης πνευματικής ιδιοκτησίας."

Όνομα και Επώνυμο Συγγραφέα (Με Κεφαλαία): ΠΑΡΑΣΚΕΥΗ ΧΑΡΑΛΑΜΠΟΠΟΥΛΟΥ

Υπογραφή (Ολογράφως, χωρίς μονογραφή): Χαραλαμπόπουλου Παρασκευή

Ημερομηνία (Ημέρα – Μήνας – Έτος): 16 - Μαΐου - 2018

Περιεχόμενα

Περίληψη.

Ανέκαθεν το θέμα της ασφάλειας του διαδικτύου ήταν ένα σοβαρό θέμα που απασχολούσε και απασχολεί όλους τους χρήστες του διαδικτύου. Παρακάτω στην εργασία θα αναφερθούμε στην δομή του διαδικτύου και πρωτόκολλα που το διέπουν.

Επίσης θα παρουσιαστούν διάφορες επιθέσεις και προβλήματα ασφαλείας που μπορεί να εμφανιστούν στο δίκτυο ή σε πληροφοριακά συστήματα, καθώς και μερικοί τρόποι άμυνας για να καταπολεμηθούν διάφορες κακόβουλες επιθέσεις.

Κατά κύριο λόγο η όλη **σπουδαιότητα** και **ανάλυση** της εργασίας είναι πάνω στο θέμα της ασφάλειας του μοντέλου OSI σε κάθε ένα επίπεδο ξεχωριστά, όπου θα παρουσιαστούν τα προβλήματα ανά επίπεδο που τυχόν προκύπτουν από επιθέσεις καθώς και απαραίτητα μέτρα που θα πρέπει να ληφθούν.

1. Εισαγωγικά

1.1 Ασφάλεια στο World Wide Web – Παγκόσμιος Ιστός

Το World Wide Web είναι ένα σύστημα ανταλλαγής πληροφοριών μέσω Internet και είναι κατασκευασμένο από web servers καιWeb browsers. Οι web servers είναι προγράμματα που διαχειρίζονται και διανέμουν τις πληροφορίες στο Διαδίκτυο, ενώ οι Web browsers βοηθούν τους χρήστες να αποκτούν πρόσβαση στις πληροφορίες των web Servers και να τις προβάλλουν στις οθόνες τους.

Το World Wide Web πρωταρχικά αναπτύχθηκε για την βοήθεια των ερευνητών. Στόχευε στο να βοηθήσει την κοινότητα των ερευνητών στην ανταλλαγή και την δημοσιοποίηση των ερευνών τους. Η χρήση του Web βοήθησε τους ερευνητές να αποφύγουν την χρονοβόρα και δαπανηρή μέθοδο τις δημοσιοποίησης των ερευνητικών αποτελεσμάτων στις επιστημονικές εφημερίδες. Οι παράκαμψη της δημοσιοποιήσεις διαφόρων ερευνών, διαφημίσεων ή οτιδήποτε άλλο στις εφημερίδες, παρέχει σημαντική διευκόλυνση. Χιλιάδες χρήστες πια δημοσιοποιούν στον Παγκόσμιο Ιστό οτιδήποτε θέλουν για ενημέρωση, προβολή, διαφήμιση κλπ. Επιπλέον χρήση του web κάνουν οι οργανισμοί να μπορούν να διανέμουν εμπιστευτικά έγγραφα στους συνεργάτες ή πελάτες τους όπου κι αν βρίσκονται.

Η χρήση του web βέβαια είναι δυνατόν να γίνει και πιο εξειδικευμένη, με την ενσωμάτωση προγραμμάτων σε ηλεκτρονικές σελίδες. Τα προγράμματα αυτά δημιουργούνται με τη χρήση του πρωτοκόλλου Common Gateway Interface (CGI). Τα CGI Scripts μπορούν να είναι πολύπλοκα όπως χρηματικές συναλλαγές μέσω Διαδικτύου ή πιο απλά, όπως για παράδειγμα θα μπορούσε να είναι ένας μετρητής που μετράει τους επισκέπτες τις σελίδας.

Ιδιαίτερα ευνοημένο με την τεράστια απήχηση του Web έχει φανεί το ηλεκτρονικό εμπόριο. Πολλές εταιρίες το χρησιμοποιούν ως μέσω προώθησης των προϊόντων τους. Κατασκευάζουν ηλεκτρονικές σελίδες που μοιάζουν με εικονικά καταστήματα, παρέχουν τιμοκαταλόγους, προσφέρουν παρουσίαση των προϊόντων και ειδικές φόρμες που συμπληρώνει με τα στοιχεία του ο πελάτης.

Όπως είδαμε και ήδη βέβαια γνωρίζουμε, μιας και όλοι μας χρησιμοποιούμε αυτήν την υπηρεσία με διαφόρους τρόπους, το World

Wide Web είναι μια από τις πιο χρησιμοποιούμενες εφαρμογές. Παρά ταύτα παρουσιάζει σημαντικά προβλήματα ασφαλείας.

- Ένας πιθανός εισβολέας μπορεί εκμεταλλευόμενος ατέλειες (bugs) του Web ή των CGI scripts να αποκτήσει παράνομη πρόσβαση σε προσωπικά αρχεία του serverή ακόμα χειρότερα να αποκτήσει ολόκληρο τον έλεγχο του server.
- Με την εισβολή κάποιου παράνομα είναι δυνατόν οι εμπιστευτικές πληροφορίες που βρίσκονται αποθηκευμένες στονWeb server ή που ανταλλάσσονται μεταξύ Web server–Browserνα υποπέσουν σε υποκλοπή ή να διανεμηθούν σε μη εγκεκριμένα άτομα. Όλο αυτό, όπως μπορούμε να φανταστούμε, θα δημιουργούσε τεράστιο πρόβλημα.
- Ένας Web Serverπου πιθανόν να λειτουργεί κακόβουλα μπορεί να αποκτήσει μη εξουσιοδοτημένη πρόσβαση σε απόρρητες πληροφορίες του Client.

Καθένα από τα παραπάνω προβλήματα ή όποιο άλλο πιθανώς προκύψει χρήζει διαφορετικής αντιμετώπισης. Πολλές φορές βέβαια οι λύσεις μπορεί να είναι αλληλοσυγκρουόμενες. Διάφορα προβλήματα ασφαλείας και λύσεις αντιμετώπισης θα αναλύσουμε παρακάτω στην εργασία.

1.2 Ασφαλής Λειτουργία ενός Web Server.

Μια δύσκολη κατάσταση που πρέπει να αντιμετωπίζουν διαρκώς οι Web Servers είναι πως πρέπει να δέχονται και να εξυπηρετούν ανώνυμες αιτήσεις από άγνωστους υπολογιστές σε όλο το Internet και να παραδίδουν άμεσα την ζητούμενη πληροφορία. Έτσι δημιουργείται η δυνατότητα εύκολα κάποιος κακόβουλος να το εκμεταλλευτεί για να αποκτήσει παράνομη πρόσβαση. Γενικότερα, **δεν υπάρχει το τέλειο λογισμικό, όλα περικλείουν κάποιους κινδύνους στην χρήση τους.**

Οι Web Servers είναι περίπλοκα και εξειδικευμένα προγράμματα, πολλοί χρησιμοποιούν πηγαίο κώδικα που είναι ελεύθερα διαθέσιμος στο Internet. Αυτό μπορεί μεν να καθιστά εύκολη την επιθεώρηση του προγράμματος άλλα δίνει και την δυνατότητα σε κάποιον που έχει αρκετές γνώσεις να βρει να αδύναμα σημεία του Web Server.

Η ενσωμάτωση CGIscripts στουςWeb servers παρόλο που προσθέτει επιπλέον χαρακτηριστικά και δυνατότητες δημιουργεί και σημαντικά θέματα ασφαλείας. Επειδή οι περισσότεροι χρήστες δεν είναι εξοικειωμένοι με την σύνταξη ενός ασφαλούς CGIscript υπάρχει πιθανότητα λόγω σφαλμάτων να περιέχουν αδυναμίες που επιτρέψουν σε έναν επιτιθέμενο να εκτελέσει οποιαδήποτε εντολή επιθυμεί. Ένα παράδειγμα προβλήματος είναι ο Web Server να έχει ρυθμιστεί ώστε η πρόσβαση του να περιορίζεται σε αρχεία μιας συγκεκριμένης λίστας άλλα παρ' όλα αυτά ένας χρήστης χωρίς τις απαραίτητες γνώσεις να εγκαταστήσει ένα CGIscript που παραβλέπει την αρχική ρύθμιση και θα επιτρέπει την ανάγνωση οποιουδήποτε αρχείου.

Όσον αφορά τώρα το εμπόριο υπάρχουν αρκετά λειτουργικά συστήματα, μερικά από αυτά είναι πιο ικανά να χρησιμοποιηθούν στους Web servers από άλλα. Για την καλύτερη απόδοση έχει παρατηρηθεί ότι πρέπει να χρησιμοποιείται ένας υπολογιστής που θα τρέχει μόνο τον Web Server και καμία άλλη εφαρμογή, να μην δέχεται απομακρυσμένες συνδέσεις και να μην χρησιμοποιεί έτοιμη scripting language (ειδική γλώσσα προγραμματισμού που χρησιμοποιείται για προγράμματα σε ειδικό περιβάλλον). Λαμβάνοντας αυτό υπόψη μπορούμε να υποστηρίξουμε πως τα κατάλληλα συστήματα είναι τα MS-Windowsκαι τα Macintoshαλλά παρέχουν ελάχιστα εργαλεία και ευκολία. Τέλος, πρέπει να θυμόμαστε ότι **σημαντικό παράγοντα παίζει και το προσωπικό** που διαχειρίζεται το εκάστοτε σύστημα. Ένας έμπειρος χρήστης οποιουδήποτε συστήματος ακόμα και μέτριας απόδοσης μπορεί να ανταπεξέλθει καλύτερα από έναν αρχάριο χρήστη του πιο αποδοτικού συστήματος.

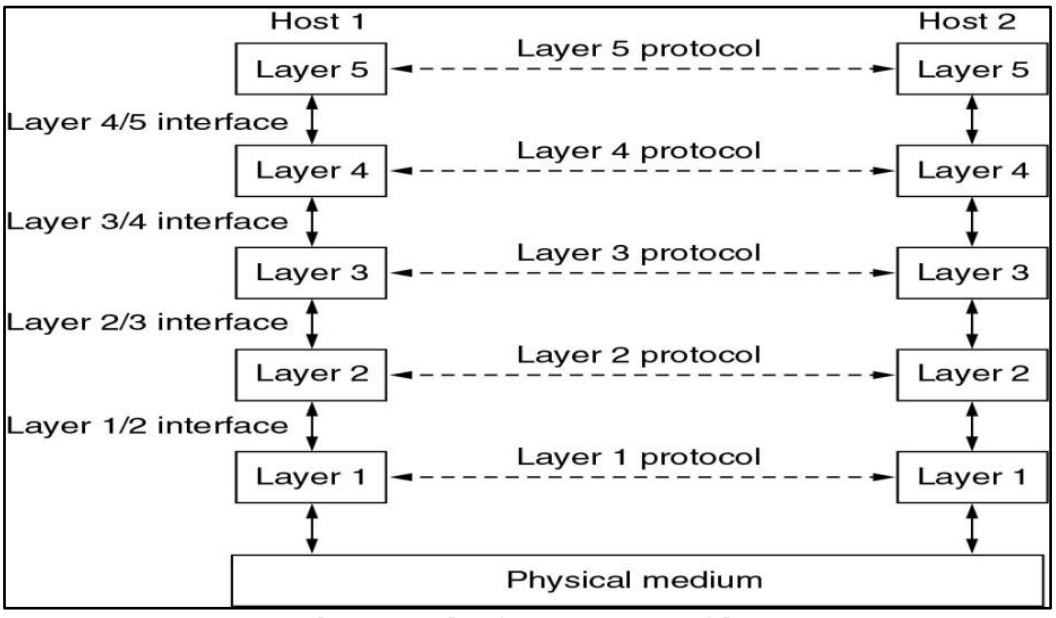
Υπάρχουν ορισμένα **κριτήρια** που πρέπει να ληφθούν υπόψη πριν την κατασκευή οποιουδήποτε ασφαλούς Web Server.

1. Τα CGI Scripts που τρέχουν στον serverπρέπει να ελεγχθούν διεξοδικά ώστε να πραγματοποιούν αυστηρά την λειτουργία που είναι προορισμένα να κάνουν.
2. Σε περίπτωση που ένας επιτιθέμενος κάνει κατάληψη στον server θα πρέπει να μην είναι δυνατόν να μπορέσει να κάνει το ίδιο και στους υπολογιστές του υπόλοιπου δικτύου αλλά να περιοριστεί στον server.
3. Δεν θα πρέπει να επιτρέπεται οι χρήστες του δικτύου να εκτελούν προγράμματα στον υπολογιστή που βρίσκεται ο server.

2. Το μοντέλο Open System Interconnection - OSI

2.1 Ιεραρχίες πρωτοκόλλων

Για να μειωθεί η πολυπλοκότητα, τα περισσότερα δίκτυα οργανώνονται σε μια στοίβα επιπέδων, με το ένα επίπεδο να βρίσκεται πάνω από το άλλο. Τα χαρακτηριστικά κάθε επιπέδου όπως το όνομα, τα περιεχόμενα και η λειτουργικότητα διαφέρουν από δίκτυο σε δίκτυο. Ο στόχος κάθε επιπέδου είναι να προσφέρει κάποιες υπηρεσίες στο ανώτερο του επίπεδο. Όταν το επίπεδο n ενός δικτύου επικοινωνεί με το επίπεδο n ενός άλλου, οι κανόνες και συμβάσεις που χρησιμοποιούνται ονομάζονται «**πρωτόκολλο του επιπέδου**». Κατά κύριο λόγο, **πρωτόκολλο (protocol)** είναι μια συμφωνία ανάμεσα στα επικοινωνούντα μέρη για το πώς πρέπει να διεξάγεται η επικοινωνία. Τέλος, κανένα δεδομένο δεν μεταδίδεται άμεσα από το επίπεδο n ενός δικτύου, στο επίπεδο ενός άλλου. Αντίθετα, κάθε δεδομένο ή πληροφορία μεταβιβάζεται στο επίπεδο που βρίσκεται κάτω από αυτό μέχρι να φτάσουμε στο κατώτερο επίπεδο που είναι το φυσικό επίπεδο. Μέσω του φυσικού μέσου εκτελείται και η πραγματική επικοινωνία.
Σε κάθε ζεύγος συνοριακών επιπέδων υπάρχει μια **διασύνδεση (Interface)**, η οποία ορίζει τις βασικές λειτουργίες και υπηρεσίες τις οποίες παρέχει το κατώτερο επίπεδο στο ανώτερο. Ο καθορισμός ξεκάθαρων διασυνδέσεων ανάμεσα στα επίπεδα είναι από τα πιο σημαντικά ζητήματα που λαμβάνουν υπόψη τους οι σχεδιαστές των δικτύων. Με αποτέλεσμα να κάνουν ξεκάθαρο το γεγονός πως κάθε επίπεδο θα εκτελεί ένα αυστηρά καθορισμένο σύνολο λειτουργιών.



Εικόνα 1: Επίπεδα και Διασυνδέσεις

Το σύνολο των επιπέδων και των πρωτοκόλλων ονομάζεται **αρχιτεκτονική δικτύου** (network architecture). Η αρχιτεκτονική θα πρέπει να περιέχει αρκετές πληροφορίες μιας και παίζει πολύ σημαντικό ρόλο στο να βοηθήσει τον κατασκευαστή να γράψει ένα πρόγραμμα ή να κατασκευάσει το υλικό κάθε επιπέδου. Όλη αυτή η διαδικασία θα πρέπει να τηρηθεί αυστηρά γιατί στόχος είναι να ακολουθείται κατά κανόνα το κατάλληλο πρωτόκολλο. Οι διασυνδέσεις εξαρτώνται από το κάθε μηχάνημα που βρίσκονται και δεν είναι μέρος της αρχιτεκτονικής, το σημαντικότερο λοιπόν είναι κάθε μηχάνημα να μπορεί να ανταπεξέλθει σωστά σε οποιοδήποτε πρωτόκολλο χρειαστεί.
Κάθε σύστημα χρησιμοποιεί συγκεκριμένη λίστα πρωτοκόλλων και κάθε πρωτόκολλο λειτουργεί σε ξεχωριστό επίπεδο, αυτή η λίστα ονομάζεται **στοίβα πρωτόκολλων**.

2.2 Σχεδιαστικά ζητήματα των επιπέδων.

Πριν γίνει η τελική σχεδίαση ενός δικτύου επιπέδων πρέπει να ληφθούν υπόψη κάποια σημαντικά **σχεδιαστικά κριτήρια**.

- Πρώτο και πιο σημαντικό είναι η αξιοπιστία, ένα δίκτυο θα πρέπει να είναι ικανό να λειτουργεί αξιόπιστα ακόμα και όταν τυχόν επιμέρους τμήματα του λειτουργούν αναξιόπιστα.
- Θα πρέπει να ληφθεί υπόψη κάποιος μηχανισμός για την εύρεση σφαλμάτων. Οι πληροφορίες που τυχόν θα λαμβάνονται με σφάλμα θα πρέπει να μεταδίδονται ξανά μέχρι να ληφθούν σωστά. Κάποιοι πιο ισχυροί κώδικές παρέχουν διόρθωση σφαλμάτων όπου αυτόματα ανακτάται το σωστό μήνυμα από τα λανθασμένα bit που είχαν ληφθεί. Αυτοί οι μηχανισμοί χρησιμοποιούνται στα χαμηλότερα επίπεδα για την προστασία των πακέτων που στέλνονται καθώς και συμπληρωματικά στα ανώτερα επίπεδα για έλεγχο των πακέτων που παρελήφθησαν αν έφτασαν σωστά.
- Άλλο ζήτημα είναι η εύρεση μιας λειτουργικής διαδρομής μέσω του δικτύου. Σε ένα δίκτυο είναι δυνατό να υπάρχουν πολλές διαδρομές για την μετάδοση των πακέτων και ιδιαίτερα σε αρκετά μεγάλα δίκτυα που μερικές διαδρομές ή δρομολογητές μπορεί να είναι εκτός λειτουργίας. Άρα σκεπτόμενοι όλο αυτό καταλαβαίνουμε ότι είναι σημαντική η απόφαση για την διαδρομή που θα ακολουθηθεί. Αυτό το ζήτημα ονομάζεται **Δρομολόγηση – Routing**, και αφορά την απόφαση που θα πρέπει να είναι ικανό να

λάβει αυτόματα το δίκτυο για την διαδρομή που θα ακολουθήσουν τα πακέτα.

- Η **διευθυνσιοδότηση** είναι ένα άλλο ζήτημα. Πραγματεύεται δίκτυα όπου υπάρχουν πολλοί υπολογιστές και το κάθε ένα επίπεδο χρειάζεται μηχανισμούς αναγνώρισης του αποστολέα ή του παραλήπτη. Η διευθυνσιοδότηση λειτουργεί και στα χαμηλά και στα υψηλά επίπεδα.
- Ένα άλλο ζήτημα της ανάπτυξης είναι ότι οι τεχνολογίες δικτύωσης έχουν διάφορους περιορισμούς. Για παράδειγμα υπάρχουν διαφορές ως προς το μέγεθος των μηνυμάτων ή την σειρά μετάδοσης των μηνυμάτων. Όλο αυτό το ζήτημα ονομάζεται **διαδικτύωση** και έχει ως λύση τον κατακερματισμό του μηνύματος, την μετάδοση και την επανασυναρμολόγηση του.
- Ένα θέμα που έχει επηρεάσει τους κατασκευαστές είναι η εξέλιξη των δικτύων. Με την πάροδο του χρόνου τα δίκτυα εξελίσσονται και πρέπει να δημιουργούνται νέες τεχνικές για την ενσωμάτωση των νέων τεχνολογιών στο ήδη υπάρχον δίκτυο. Μια λύση είναι η διαίρεση του συνολικού προβλήματος και η απόκρυψη των λεπτομερειών υλοποίησης. Αυτό ονομάζεται **διαστρωμάτωση πρωτοκόλλων.**
- Κύριο ζήτημα που πρέπει να διερευνηθεί είναι **ο έλεγχος ροής**. Αυτό το ζήτημα αφορά στο να αποτρέψουμε έναν γρήγορο αποστολέα να κατακλύσει έναν παραλήπτη με πακέτα που δεν μπορεί λόγω φόρτου να διαχειριστεί. Στην ουσία το πρόβλημα βρίσκεται στο ότι το δίκτυο είναι υπερφορτωμένο επειδή πολλοί υπολογιστές θέλουν να στείλουν ταυτόχρονα μεγάλο όγκο πληροφορίας και το δίκτυο δεν μπορεί να την διαχειριστεί όλη. Η υπερφόρτωση του δικτύου ονομάζεται **συμφόρηση (congestion)**. Μια λύση για την συμφόρηση είναι ο κάθε υπολογιστής να μειώνει τις απαιτήσεις του όταν αντιμετωπίζεται αυτό το πρόβλημα.
- Η **παράδοση σε πραγματικό χρόνο** είναι ένα θέμα που απασχολεί. Αυτό σημαίνει ότι δεδομένα που πρέπει να παραδοθούν άμεσα και με καλή ποιότητα να παραδίδονται όπως έχει ζητηθεί. Για παράδειγμα η live μετάδοση θα πρέπει να έχει έγκαιρη και χωρίς σφάλματα μετάδοση για να έχει το δίκτυο ορθή απόδοση. Η παράδοση σε πραγματικό χρόνο εξυπηρετεί υπηρεσίες που χρειάζονται υψηλή διεκπεραιωτική ικανότητα.

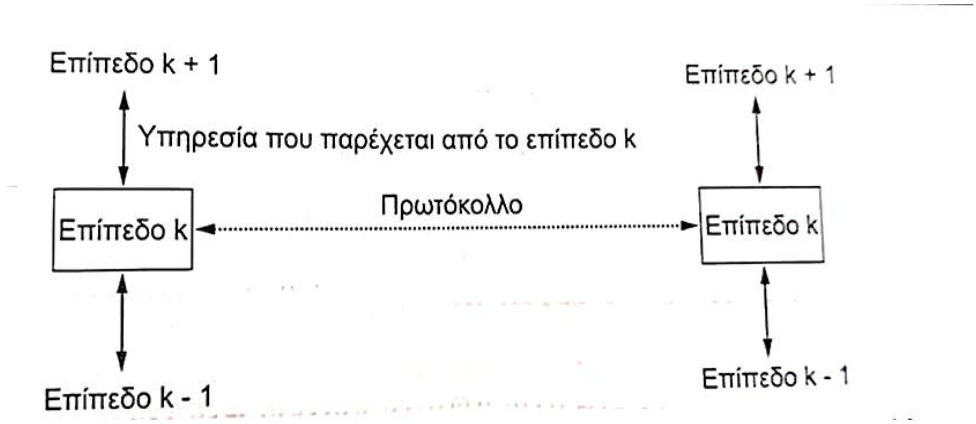
– Τελευταίο άλλα και πιο σημαντικό είναι το ζήτημα της **προστασίας** απέναντι σε οποιαδήποτε απειλή. Μια από τις κυριότερες απειλές που προκύπτει αρκετά συχνά είναι η υποκλοπή δεδομένων. Για την αποφυγή απειλών υπάρχουν διάφοροι μηχανισμοί. Όπως η εμπιστευτικότητα, οι μηχανισμοί πιστοποίησης ταυτότητας που εμποδίζουν κάποιον κακόβουλο να υποδυθεί την ταυτότητα κάποιου τρίτου και τέλος οι μηχανισμοί ακεραιότητας πληροφοριών που αποτρέπουν την παράνομη τροποποίηση πληροφοριών.

2.3 Υπηρεσίες και Πρωτόκολλα.

Οι υπηρεσίες και τα πρωτόκολλα πολλές φορές μπορεί να συγχέονται αλλά στη πραγματικότητα είναι διαφορετικές έννοιες. **Η υπηρεσία (service)** είναι ένα σύνολο θεμελιωδών λειτουργιών που παρέχονται από ένα επίπεδο στο αμέσως ανώτερο του. Η υπηρεσία είναι αυτή που ορίζει ποιες λειτουργίες είναι προετοιμασμένο να εκτελέσει το εκάστοτε επίπεδο για λογαριασμό των χρηστών, αλλά δεν περιλαμβάνει καμία πληροφορία για τον τρόπο που πραγματοποιούνται αυτές οι λειτουργίες. Συμπερασματικά, η υπηρεσία ασχολείται με την διασύνδεση δυο επιπέδων, με το κατώτερο επίπεδο να προσφέρει μια υπηρεσία ενώ το ανώτερο να την δέχεται και να την χρησιμοποιεί.

Το **πρωτόκολλο** αντίθετα, είναι ένα σύνολο κανόνων που διέπουν την μορφή και την σημασία των πακέτων που μεταδίδονται ανάμεσα στις διάφορες οντότητες των επιπέδων. Οι οντότητες αυτές χρησιμοποιούν διάφορα πρωτόκολλα για να υλοποιήσουν τις εκάστοτε λειτουργίες των υπηρεσιών τους. Κάθε φορά έχουν την δυνατότητα να αλλάζουν τα πρωτόκολλα κατά όπως θέλουν αρκεί να μην επηρεάζεται η λειτουργία τους απέναντι στους χρήστες.

Άρα οι υπηρεσίες σχετίζονται με τις διασυνδέσεις ανάμεσα στα επίπεδα ενώ αντιθέτως το πρωτόκολλο σχετίζεται με τα πακέτα που στέλνονται ανάμεσα σε ομότιμες οντότητες διάφορων μηχανημάτων.



Εικόνα 2: Σχέση Υπηρεσίας - Πρωτοκόλλου

Εν κατακλείδι, οι υπηρεσίες αφορούν τις διασυνδέσεις ανάμεσα στα επίπεδα ενώ τα πρωτόκολλα σχετίζονται με τα πακέτα μου μεταφέρονται ανάμεσα στις ομότιμες οντότητες, άρα αυτές οι δυο έννοιες δεν πρέπει να συγχέονται.

2.4 Το Μοντέλο OSI

Το μοντέλο OSI βασίζεται σε μια πρόταση που αναπτύχθηκε από τον Διεθνή Οργανισμό Προτύπων (International Standards Organization / ISO) για την τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στα διάφορα επίπεδα των δικτύων. **OSI** σημαίνει Διασύνδεση Ανοικτών Συστημάτων (Open System Interconnection), λόγω του ότι ασχολείται με την διασύνδεση ανοικτών συστημάτων, δηλαδή συστημάτων που είναι ανοικτά στην επικοινωνία με άλλα συστήματα.

Το μοντέλο OSI αποτελείται από επτά επίπεδα, οι αρχές που εξετάστηκαν για να καταλήξουμε σε αυτά τα επίπεδα είναι οι εξής:

1. Όπου χρειάζεται μια διαφορετική λογική αφαίρεση πρέπει να δημιουργείται ένα επίπεδο.
2. Κάθε επίπεδο θα πρέπει να εκτελεί μια καθορισμένη λειτουργία.
3. Τα σύνορα των επιπέδων πρέπει να επιλέγονται και να ορίζονται ώστε να ελαχιστοποιείται η ροή πληροφοριών στη διασύνδεση των επιπέδων.
4. Το πλήθος των επιπέδων θα πρέπει να είναι μικρό ώστε η αρχιτεκτονική να μην γίνεται περίπλοκη, αλλά ταυτόχρονα το πλήθος να είναι αρκετά μεγάλο ώστε να μην χρειάζεται να μπλέκονται πολλές λειτουργίες στο ίδιο επίπεδο.

5. Η λειτουργία κάθε επιπέδου πρέπει να επιλέγεται στοχεύοντας στον καθορισμό διεθνώς τυποποιημένων πρωτοκόλλων.

Τα επτά επίπεδα του μοντέλου αναφοράς OSI είναι τα εξής :

1) Φυσικό Επίπεδο

2) Επίπεδο Ζεύξης Δεδομένων

3)Επίπεδο Δικτύου

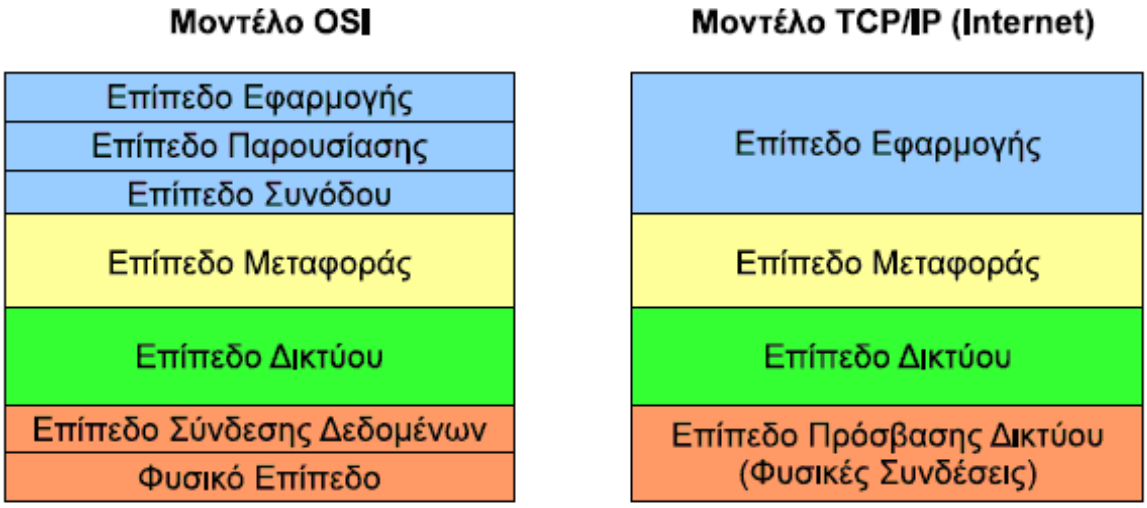
4)Επίπεδο Μεταφοράς

5)Επίπεδο Συνόδου

6)Επίπεδο Παρουσίασης

7) Επίπεδο Εφαρμογής

Όπως φαίνονται στην πιο κάτω εικόνα.



Εικόνα 3 : Αριστερά: Μοντέλο Αναφοράς ISO-OSI επτά επιπέδων
Δεξιά: Στοίβα πρωτοκόλλων Διαδικτύου πέντε επιπέδων

Φυσικό Επίπεδο

Το Φυσικό Επίπεδο (Physical Layer) ασχολείται με την μετάδοση δυαδικών ψηφίων μέσω ενός καναλιού επικοινωνίας. Σαν μέσα μετάδοσης χρησιμοποιούνται ο αέρας ή χάλκινα καλώδια (ομοαξονικά, ή συνεστραμμένων ζευγών, οπτικές ίνες). Η ακολουθία των bit μπορεί να ομαδοποιηθεί σε λέξεις κώδικα ή σύμβολα και να μετατραπεί στο

φυσικό σήμα (ηλεκτρικό, οπτικό), το οποίο διαδίδεται πάνω στο φυσικό μέσο μετάδοσης.
Οι τεχνολογίες του Φυσικού Επιπέδου βρίσκονται στο χαμηλότερο επίπεδο και ασχολούνται με τα πραγματικά 0 και 1 που αποστέλλονται στο δίκτυο. Παίρνουν τα bit στην είσοδό τους και τα εκπέμπουν στην έξοδό τους, μετατρέποντας τα στην κατάλληλη μορφή για το μέσο μετάδοσης και εκτελώντας την κατάλληλη κωδικοποίηση, όπου αυτό απαιτείται.

Επίπεδο Ζεύξης

Στόχος του επιπέδου αυτού είναι να παρέχει υπηρεσίες στο επίπεδο δικτύου, αξιοποιώντας τις υπηρεσίες που λαμβάνει από το φυσικό επίπεδο. Καθορίζεται από πρωτόκολλα υπεύθυνα για την μετάδοση δεδομένων στο τηλεπικοινωνιακό κανάλι αποτελούμενο από ένα φυσικό μέσο (πχ καλώδιο). Ασχολείται με την παράδοση πλαισίων μεταξύ συσκευών του δικτύου. Εφαρμόζεται μόνο στα πλαίσια του τοπικού δικτύου, έξω από αυτό είναι δουλειά των υψηλότερων επιπέδων. Άρα το επίπεδο ζεύξης προσφέρει την δυνατότητα μεταφοράς δεδομένων κατά μήκος την φυσικής ζεύξης. Υπάρχει πιθανότητα η μεταφορά να είναι αναξιόπιστη. Αρκετά πρωτόκολλα ζεύξης δεν έχουν απάντηση επιβεβαίωσης επιτυχούς λήψης δεδομένων και άλλα δεν έχουν καν μορφή checksum για τον έλεγχο τυχόν λάθος μετάδοσης. Σε τέτοια περίπτωση, εμφανίζονται τα ανώτερα επίπεδα παρέχοντας έλεγχο ροής και λαθών καθώς και επιβεβαίωση λήψης-επανεκπομπής.

Επίπεδο Δικτύου (Network Layer)

Το επίπεδο δικτύου ασχολείται με την δρομολόγηση πακέτων επιπέδου δικτύου, των λεγόμενων δεδομενογραμμάτων (datagrams) από έναν υπολογιστή σε έναν άλλο. Το πρωτόκολλο επιπέδου μεταφοράς του Διαδικτύου (TCP ή UDP) σε έναν υπολογιστή προέλευσης μεταφέρει ένα τμήμα επιπέδου μεταφοράς και μια διεύθυνση προορισμού στο επίπεδο δικτύου. Το επίπεδο δικτύου παρέχει κατόπιν την υπηρεσία παράδοσης του τμήματος στο επίπεδο μεταφοράς του υπολογιστή προορισμού.
Το επίπεδο δικτύου περιλαμβάνει το γνωστό **Πρωτόκολλο IP** (IP Protocol), το οποίο ορίζει τα πεδία μέσα στο δεδομενόγραμμα, καθώς και το πώς τα τερματικά συστήματα και οι δρομολογητές δρουν σ΄ αυτά τα πεδία. Το πρωτόκολλο IP είναι μοναδικό και έτσι όλα τα συστατικά του Διαδικτύου που έχουν ένα επίπεδο δικτύου πρέπει να το εκτελούν. Το επίπεδο δικτύου του Διαδικτύου περιέχει επίσης πρωτόκολλα δρομολόγησης, τα οποία καθορίζουν τις διαδρομές που ακολουθούν τα δεδομενογράμματα από τις προελεύσεις στους

προορισμούς. Το Διαδίκτυο αποτελείται από πολλά πρωτόκολλα δρομολόγησης. Αν και το επίπεδο δικτύου περιέχει το πρωτόκολλο IP και αρκετά ακόμα πρωτόκολλα δρομολόγησης, έχει καθιερωθεί να αναφερόμαστε σ΄αυτό ως επίπεδο IP, κάτι που αντανακλά το γεγονός ότι το IP είναι η βάση που στηρίζεται όλο το Διαδίκτυο.

Επίπεδο Μεταφοράς (Transport Layer)

Η βασική λειτουργία του επιπέδου μεταφοράς είναι να δέχεται δεδομένα από το ανώτερο επίπεδο. Αν χρειάζεται τα χωρίζει σε μικρότερες μονάδες, τα μεταβιβάζει στο επίπεδο δικτύου και εξασφαλίζει ότι όλα τα τμήματα φτάνουν σωστά στο άλλο άκρο. Επίσης το επίπεδο αυτό μεταφέρει μηνύματα επιπέδου εφαρμογής ανάμεσα σε άκρα της εφαρμογής (end to end).
Στο Διαδίκτυο υπάρχουν δυο πρωτόκολλα μεταφοράς, **το TCP και το UDP**, όπου και τα δύο μπορούν να μεταφέρουν μηνύματα επιπέδου εφαρμογής. **Το TCP** παρέχει μια συνδεσμική υπηρεσία στις εφαρμογές του. Αυτή η υπηρεσία περιλαμβάνει εγγυημένη παράδοση μηνυμάτων επιπέδου εφαρμογής στον προορισμό και έλεγχο ροής. Το TCP επίσης χωρίζει μεγάλα μηνύματα σε μικρότερα τμήματα και χρησιμοποιεί ένα μηχανισμό ελέγχου συμφόρησης, έτσι ώστε μια προέλευση να ρυθμίζει τον ρυθμό μετάδοσης αντίστοιχα όταν το δίκτυο είναι σε συμφόρηση. Το πρωτόκολλο **UDP** παρέχει στις εφαρμογές του μια ασυνδεσμική υπηρεσία, η οποία είναι μια απλή υπηρεσία, που δεν παρέχει αξιοπιστία, έλεγχο ροής και έλεγχο συμφόρησης. Έχει καθιερωθεί να αναφερόμαστε σε ένα πακέτο επιπέδου μεταφοράς ως **τμήμα (segment**).

Επίπεδο Συνόδου

Το επίπεδο αυτό επιτρέπει στους χρήστες διαφορετικών συσκευών να εγκαθιστούν συνόδους μεταξύ τους. Μέσω μιας συνόδου είναι δυνατή η μεταφορά δεδομένων παρέχοντας κάποιες επιπρόσθετες υπηρεσίες από ότι στο επίπεδο μεταφοράς. Μια σύνοδος καθιστά εφικτή την σύνδεση ενός χρήστη με ένα απομακρυσμένο σύστημα κατακερματισμού χρόνου (timesharing) ή επίσης να μεταφέρει ένα δεδομένο μεταξύ δυο συσκευών. Μια σύνοδος μπορεί να επιτρέψει την κίνηση του καναλιού επικοινωνίας είτε προς την μια κατεύθυνση (**μονόδρομο κανάλι**) είτε και στις δυο (**αμφίδρομο κανάλι**). Τέλος, μια ακόμα υπηρεσία που παρέχει είναι ο **συγχρονισμός**. Αν η ανταλλαγή δεδομένων μεταξύ δυο συσκευών διαρκέσει αρκετή ώρα μπορεί να υπάρξει πρόβλημα. Σε περίπτωση που μια μεταφορά αναγκαστικά διακοπεί θα πρέπει να ξεκινήσει από την αρχή χωρίς αυτό να εγγυάται πως δεν θα υπάρξει πρόβλημα αυτή την φορά. Έτσι το επίπεδο Συνόδου έχει εγκαταστήσει σημεία ελέγχου στο κανάλι,

ώστε σε περίπτωση κατάρρευσης να μεταδοθούν μόνο τα δεδομένα από το τελευταίο σημείο ελέγχου.

Επίπεδο Παρουσίασης

Το επίπεδο αυτό βρίσκεται πιο κοντά στις απαιτήσεις και τα προβλήματα του χρήστη. Εκτελεί συγκεκριμένες λειτουργίες που του έχουν ζητηθεί από τον χρήστη για την εύρεση μιας λύσης που χρειάζεται. Το επίπεδο παρουσίασης ενδιαφέρεται για την σωστή σύνταξη και σημασιολογία των μεταδιδόμενων πληροφοριών και όχι μόνο για την αξιόπιστη μετακίνηση όπως τα υπόλοιπα επίπεδα. Τέλος, το επίπεδο αυτό ασχολείται και με την συμπίεση των δεδομένων για να ελαττώσει τον αριθμό των bits που πρόκειται να μεταδοθούν, για να επιτευχθεί αυτό είναι πιθανό να χρειαστεί κρυπτογράφηση με σκοπό την μυστικότητα και την γνησιότητα των δεδομένων.

Επίπεδο Εφαρμογής (Application Layer)

Το επίπεδο εφαρμογών (Application Layer) αποτελείται από μια ποικιλία πρωτοκόλλων που απαιτούνται συχνά από τους χρήστες. Το πιο διαδεδομένο πρωτόκολλο εφαρμογής είναι το **Πρωτόκολλο Μεταφοράς Υπερ-κειμένου ή HTTP** (Hyper Text Transfer Protocol), το οποίο είναι η βάση του Παγκοσμίου Ιστού. Όταν ένα πρόγραμμα φυλλομέτρησης (browser) χρειάζεται μια ιστοσελίδα, στέλνει το όνομα της επιθυμητής σελίδας στον διακομιστή χρησιμοποιώντας το πρωτόκολλο HTTP και ο διακομιστής επιστρέφει στη συνέχεια τη σελίδα. Επιπλέον ένα διαδεδομένο πρωτόκολλο στο επίπεδο Μεταφοράς είναι το **FTP** που χρησιμοποιείτε για υποστήριξη μεταφοράς αρχείων ανάμεσα σε δύο απομακρυσμένα τερματικά συστήματα.

2.5 Το μοντέλο αναφοράς TCP/IP

Το δίκτυο ARPANET ήταν ένα δίκτυο μεταγωγής πακέτων που χρηματοδοτήθηκε από το υπουργείο άμυνας των Η.Π.Α στα τέλη της δεκαετίας του ΄60. Πρωτεύων στόχος ήταν να συνδέονται μαζί πολλά διαφορετικά συστήματα και δίκτυα. Έμφαση δόθηκε στη δυνατότητα του δικτύου να παραμένει λειτουργικό ακόμη κι αν μεγάλα τμήματα του έβγαιναν εκτός λειτουργίας. Το 1983 χρησιμοποιήθηκαν τα πρωτόκολλα TCP/IP ως βασικά και σταδιακά εξελίχθηκε στο γνωστό μας Internet.

Το **TCP/IP** (Transmission Control Protocol /Internet Protocol, δηλαδή Πρωτόκολλο Ελέγχου Μετάδοσης/Πρωτόκολλο Διαδικτύου) είναι μια συλλογή πρωτοκόλλων επικοινωνίας στα οποία βασίζεται κατά κύριο λόγο το Διαδίκτυο. Αυτή η συλλογή πρωτοκόλλων είναι οργανωμένη σε **επίπεδα (**layers). Το καθένα από τα οποία απαντά σε συγκεκριμένα προβλήματα μεταφοράς δεδομένων και παρέχει μια καθορισμένη υπηρεσία στα υψηλότερα επίπεδα. Τα ανώτερα επίπεδα είναι πιο κοντά στη λογική του χρήστη και εξετάζουν πιο αφηρημένα δεδομένα, στηρίζονται στα πρωτόκολλα των κατώτερων επιπέδων για την μετάφραση δεδομένων σε μορφές οι οποίες είναι δυνατόν να διαβιβαστούν με φυσικά μέσα.

Το μοντέλο TCP/IP χρησιμοποιεί διαστρωματωμένη αρχιτεκτονική τεσσάρων επιπέδων.

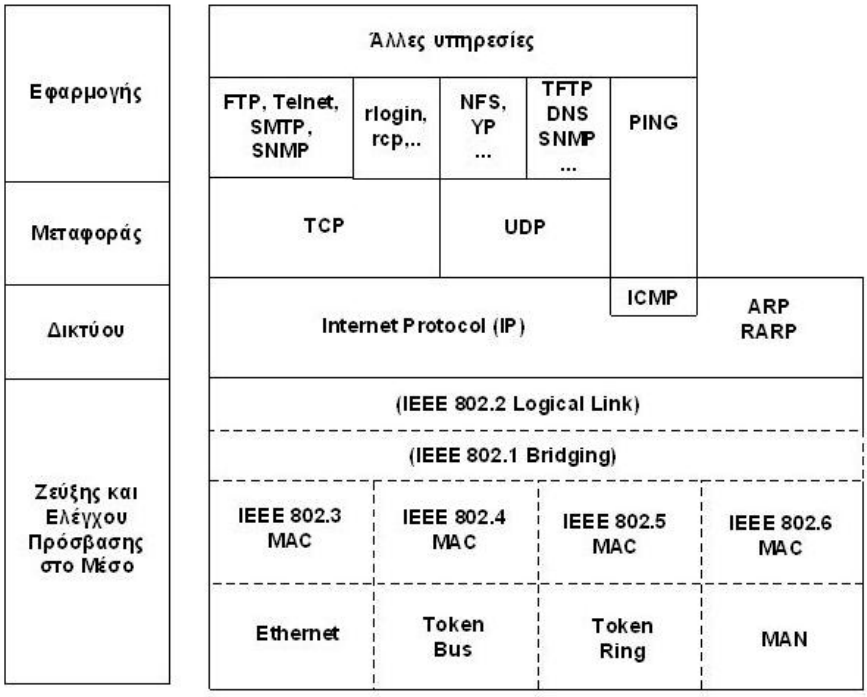
2.6 TCP/IP Layers

1. Εφαρμογών (αντιστοιχεί στα επίπεδα Εφαρμογής, Παρουσίασης και Συνόδου του OSI)
2. Μεταφοράς (αντιστοιχεί στο Μεταφοράς του OSI)
3. Διαδικτύου (αντιστοιχεί στο Δίκτυο του OSI)
4. Συνδέσμου.

Το μοντέλο TCP/IP δεν έχει επίπεδα συνδιάλεξης ή παρουσίασης. Δεν συμπεριλήφθησαν στο μοντέλο μιας και δεν θεωρήθηκε ότι θα χρειαστούν, για τις περισσότερες εφαρμογές τα επίπεδα αυτά έχουν μικρή χρησιμότητα.

Το επίπεδο εφαρμογών

Το επίπεδο εφαρμογών (applicationlayer) βρίσκεται πάνω από το επίπεδο μεταφοράς και περιέχει όλα τα πρωτόκολλα ανωτέρου επιπέδου. Στις αρχές σε αυτό περιλαμβάνονταν το **ηλεκτρονικό ταχυδρομείο** (SMTP), η **μεταφορά αρχείων** (FTP) και το **εικονικό τερματικό σύνδεσης απομακρυσμένων υπολογιστών** (TELNET). Με το πέρασμα του χρόνου έχουν προστεθεί κι άλλα πολλά πρωτόκολλα όπως το Σύστημα **Ονομάτων Περιοχών** (DNS) όπου χρησιμοποιείται για την αντιστοίχιση ονομάτων υπολογιστών υπηρεσίας σε διευθύνσεις δικτύου, όπως και το **HTTP** που είναι το πρωτόκολλο για την παροχή σελίδων στον Παγκόσμιο Ιστό, και τέλος το πρωτόκολλο **RTP** που χρησιμοποιείται για την παράδοση πολυμέσων σε πραγματικό χρόνο (πχ. ήχος και ταινίες).



Εικόνα 4: Το μοντέλο TCP / IP με κάποια από τα πρωτόκολλα που υποστηρίζει.

Το επίπεδο μεταφοράς

Το επίπεδο που βρίσκεται πάνω από το επίπεδο διαδικτύου στο μοντέλο TCP/IP ονομάζεται επίπεδο μεταφοράς (transport layer). Έχει σχεδιαστεί για να επιτρέπει στις ομότιμες οντότητες στους υπολογιστές υπηρεσίας προέλευσης και προορισμού να συνομιλούν, όπως γίνεται και στο επίπεδο μεταφοράς του μοντέλου OSI. Σε αυτό το επίπεδο είναι ορισμένα δυο πρωτόκολλα μεταφοράς. Το πρώτο είναι το **Πρωτόκολλο Μετάδοσης ή TCP** (Transmission Control Protocol), είναι ένα αξιόπιστο συνδεσμοστρεφές πρωτόκολλο το οποίο επιτρέπει σε μια ροή byte που προέρχεται από μία μηχανή να παραδίδεται χωρίς σφάλματα σε οποιαδήποτε άλλη μηχανή στο Διαδίκτυο. Το πρωτόκολλο τεμαχίζει την εισερχόμενη ροή byte σε διακριτά μηνύματα και μεταφέρει το καθένα από αυτά στο επίπεδο διαδικτύου. Τέλος, η διεργασία –παραλήπτης του TCP ανασυναρμολογεί τα μηνύματα που λαμβάνει σε μία ροή εξόδου. Επιπλέον το TCP χειρίζεται και τον **έλεγχο ροής**, δηλαδή εξασφαλίζει ότι ένας γρήγορος αποστολέας δεν θα μπορεί να κατακλύσει έναν αργό παραλήπτη με περισσότερα μηνύματα από όσα μπορεί να ανταπεξέλθει.

Το δεύτερο πρωτόκολλο στο επίπεδο αυτό είναι το **Πρωτόκολλο Αυτοδύναμων Πακέτων χρήστη ή UDP** (User Datagram Protocol), είναι ένα αναξιόπιστο ασυνδεσμικό πρωτόκολλο το οποίο προορίζεται

για εφαρμογές που δεν χρειάζονται την παράδοση των πακέτων με την σωστή σειρά ή τον έλεγχο ροής του TCP μιας και επιθυμούν να παρέχουν δικούς τους μηχανισμούς. Γίνεται χρήση για εφαρμογές όπου η γρήγορη παράδοση είναι πιο σημαντική από την ακριβή παράδοση (πχ μετάδοση ομιλίας και βίντεο).

Το επίπεδο διαδικτύου

Το επίπεδο διαδικτύου (Internet layer) είναι το θεμέλιο ολόκληρης της αρχιτεκτονικής και αντιστοιχεί στο επίπεδο δικτύου του μοντέλου επιπέδων δικτύου OSI. Σκοπός του είναι να επιτρέπει στους υπολογιστές υπηρεσίες να εισάγουν τα πακέτα τους σε οποιοδήποτε δίκτυο και αυτά να μεταφέρονται ανεξάρτητα προς το προορισμό τους ο οποίος πιθανόν να βρίσκεται σε ένα διαφορετικό δίκτυο. Τα πακέτα μπορεί να φτάσουν ακόμη και με διαφορετική σειρά από αυτή με την οποία στάλθηκαν. Στην περίπτωση αυτή είναι δουλειά των ανώτερων επιπέδων να αναδιατάξουν τα πακέτα, εάν είναι επιθυμητή η παράδοση των πακέτων με τη σειρά. Το επίπεδο διαδικτύου ορίζει μια επίσημη μορφή για τα πακέτα και ένα επίσημο πρωτόκολλο, το οποίο ονομάζεται **Πρωτόκολλο Διαδικτύου ή IP** (Internet Protocol), καθώς και ένα συνοδευτικό πρωτόκολλο που ονομάζεται **Πρωτόκολλο Μηνυμάτων Ελέγχου Διαδικτύου ή ICMP** (Internet Control Message Protocol). Η δουλειά του επιπέδου διαδικτύου είναι να παραδίδει τα πακέτα IP εκεί όπου πρέπει να πάνε. Τα βασικά ζητήματα είναι η δρομολόγηση των πακέτων καθώς και η αποφυγή συμφόρησης.

Το επίπεδο συνδέσμου

Οι διάφορες απαιτήσεις του μοντέλου TCP/IP οδήγησαν στην επιλογή ενός δικτύου μεταγωγής πακέτων που βασίζεται σε ένα ασυνδεσμικό επίπεδο το οποίο θα λειτουργεί πάνω σε διαφορετικά δίκτυα. Το χαμηλότερο επίπεδο του μοντέλου ονομάζεται επίπεδο συνδέσμου (linklayer) και περιγράφει τι θα πρέπει να κάνουν διάφοροι σύνδεσμοι όπως οι σειριακές γραμμές και το Ethernet προκειμένου να ανταπεξέλθουν στις ανάγκες του ασυνδεσμικού επιπέδου διαδικτύου. Το επίπεδο που περιγράφεται δεν πρόκειται για ένα κανονικό επίπεδο με την κλασσική έννοια του όρου, αλλά για μια διασύνδεση μεταξύ υπολογιστών υπηρεσίας και συνδέσμων μετάδοσης.

2.7 Σύγκριση OSI-TCP/IP.

Τα μοντέλα OSI και TCP/IP έχουν πολλά κοινά σημεία. Η βασικότερη ομοιότητα τους είναι πως βασίζονται σε μια στοίβα πρωτοκόλλων,

όπως επίσης μοιάζει και η λειτουργικότητα των επιπέδων τους. Δηλαδή τα επίπεδα μέχρι και το επίπεδο μεταφοράς χρησιμεύουν για μεταφορά απ' άκρου εις άκρο διεργασιών που επικοινωνούν. Ενώ, τα επίπεδα που βρίσκονται πάνω από το επίπεδο μεταφοράς χρησιμοποιούν τις υπηρεσίες του επιπέδου μεταφοράς και στρέφονται προς τις εφαρμογές.

Ομοιότητες:

- Και τα δύο μοντέλα περιγράφονται από επίπεδα.
- Σε κάθε επίπεδο δρουν διάφορα πρωτόκολλα.
- Σε κάθε επίπεδο μπορούν να δρουν παραπάνω από ένα πρωτόκολλα.
- Κοινή λειτουργική επιπέδων.

Όμως παρά τις ομοιότητες τους υπάρχουν και σημεία όπου διαφέρουν. Στο επίκεντρο των διαφορών τους βρίσκονται τρείς έννοιες. **Οι Υπηρεσίες, οι Διασυνδέσεις και τα Πρωτόκολλα.**
Μεγάλη σημασία έχει το επίπεδο OSI που έκανε σαφή τη διαφορά ανάμεσα σε αυτές τις έννοιες.
Όπως προαναφέραμε κάθε επίπεδο υλοποιεί κάποιες υπηρεσίες για το επίπεδο που βρίσκεται πάνω από αυτό και κάθε υπηρεσία καθορίζει τι κάνει κάθε επίπεδο. Η διασύνδεση ενημερώνει τις διεργασίες που βρίσκονται στα ανώτερα επίπεδα από αυτό πώς να το προσπελάσουν. Ούτε οι υπηρεσίες ούτε η διασύνδεση έχουν σχέση με τρόπο λειτουργίας του επιπέδου εσωτερικά. Τελευταία, τα ομότιμα πρωτόκολλα που χρησιμοποιούνται σε ένα επίπεδο είναι δουλειά του εκάστοτε πακέτου. Ένα θετικό των ομότιμων πρωτοκόλλων είναι πως κάθε επίπεδο μπορεί να χρησιμοποιήσει οποιοδήποτε πρωτόκολλο θέλει αρκεί να κάνει σωστά τις λειτουργίες που είναι προγραμματισμένο να κάνει. Αντιθέτως, το μοντέλο αυτό έκανε σαφή διάκριση ανάμεσα στις υπηρεσίες, τις διασυνδέσεις και τα πρωτόκολλα. Αυτό μπορεί να βασιστεί στο γεγονός πως οι πραγματικές και συνήθεις υπηρεσίες που προσφέρει το επίπεδο διαδικτύου είναι η αποστολή και λήψη πακέτων IP.

Μια άλλη διαφορά είναι στο θέμα της επικοινωνίας. Το μοντέλο TCP / IP έχει ασυνδεσμικό τρόπο επικοινωνίας στο επίπεδο δικτύου αλλά υποστηρίζει και ασυνδεσμικό τρόπο επικοινωνίας και συνδεσμοστρεφές στο επίπεδο μεταφοράς αφήνοντας τον χρήστη να επιλέξει. Αντίθετα, στο μοντέλο OSI υποστηρίζεται και ασυνδεσμική και συνδεσμοστρεφείς επικοινωνία στο επίπεδο δικτύου αλλά στο επίπεδο μεταφοράς μόνο συνδεσμοστρεφή.

Διαφορές:

1. Το πρότυπο OSI θεωρείται πιο πλήρες.
2. Έχουν διαφορετικό αριθμό επιπέδων (το μοντέλο OSI έχει 7 ενώ το TCP/IP έχει 4).
3. Το TCP/IP έτυχε μεγαλύτερης αποδοχής.
4. Το TCP/IP εδραιώθηκε στο χώρο των εμπορικών δικτύων υπολογιστών καθώς και στο Internet, ενώ το OSI λειτουργεί ως επί το πλείστον με εκπαιδευτικό χαρακτήρα για την σαφέστερη μελέτη ενός δικτύου.
5. Υποστηρίζεται διαφορετική επικοινωνία (ασυνδεσμική – συνδεσμοστρεφής) στα επίπεδα δικτύου και μεταφοράς.

3. Ασφάλεια στο επίπεδο Ζεύξης

3.1 ARPspoofing – Πλαστοπροσωπία ARP.

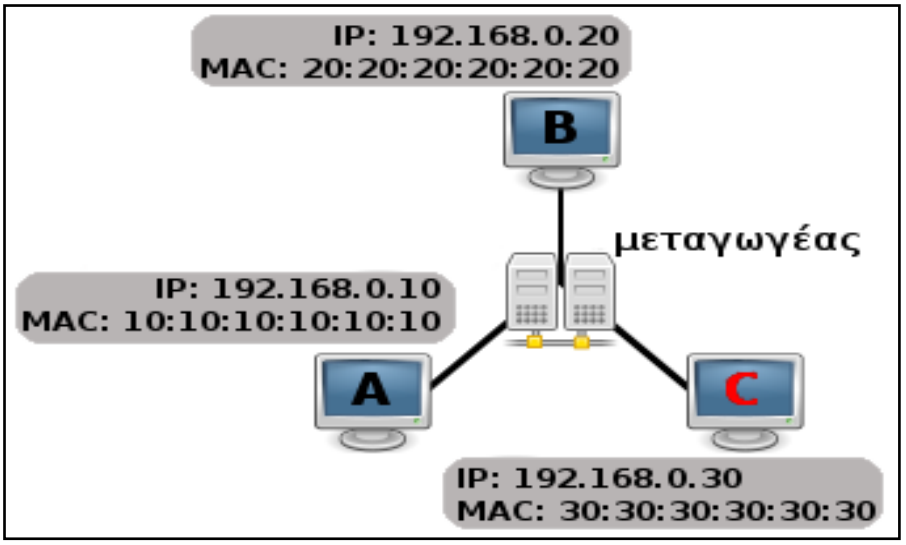
Η επίθεση ARP spoofing είναι ένας τύπος παραβίασης σε δίκτυο υπολογιστών βασιζόμενο στο ARPπρωτόκολλο.

Ο επιτιθέμενος χρήστης μπορεί, μεταδίδοντας λανθάνοντα πακέτα ARPνα ξεγελάσει άλλους χρήστες ώστε να στείλουν χωρίς να το αντιληφθούν τα data frames (πλαίσια δεδομένων) τους σε άλλον υπολογιστή. Έτσι, έχει τη δυνατότητα να παρακολουθήσει την επικοινωνία (man in the middle attack) μεταξύ :

1. Ενός host και του Διαδικτύου.
2. Δυο host.
3. Ενός hostκαι ενός υποδικτύου.

Επίσης, μπορεί να παρακολουθήσει και οποιοδήποτε συνδυασμό των αναφερόμενων.

- **Παράδειγμα παραβίασης - Man in the middle**



Εικόνα 5 Προσομοίωση παραδείγματος Man in the Middle

Σκοπός του συστήματος C είναι να μπει ανάμεσα στον A και B. Για να το πραγματοποιήσει αυτό στέλνει πακέτα ARP στον A με διεύθυνση IP192.168.0.20 και MAC 30:30:30:30:30:30. Άρα όταν ο A θελήσει να στείλει δεδομένα στον B θα χρησιμοποιήσει την διεύθυνση MAC του C. Με την ίδια λογική εξαπατά και τον B ώστε στον κατάλογο ARP να βρίσκεται το ζεύγος διευθύνσεων 192.168.0.10 - 30:30:30:30:30:30 αντί του 192.168.0.10 – 10:10:10:10:10:10.

Αμέσως μετά, ο A στέλνει τα πακέτα με αποδέκτη τον B στον κακόβουλο χρήστη C και αντίστροφα. Παρ' όλα αυτά, ο C πρέπει επίσης να δρομολογήσει όποιο πακέτο δεν τον ενδιαφέρει ή δεν χρειάζεται πια στον τελικό αποδέκτη ώστε οι δυο hosts να μην καταλάβουν ότι η επικοινωνία τους παρακολουθείται και παρεμποδίζεται.

Αποφυγή

Για να μπορέσει να δράσει μια τέτοια επίθεση θα πρέπει ο επιτιθέμενος να βρίσκεται στο ίδιο υποδίκτυο με τους host που θέλει να εξαπατήσει και να αποτελείται από μεταγωγείς. Ο διαχειριστής συστήματος έχει τη δυνατότητα να αποτρέψει τέτοιου είδους παραβιάσεις παρακολουθώντας τον κατάλογο ARP για οποιαδήποτε περίεργη αλλαγή μπορεί να υπάρξει. Αυτό μπορεί να πραγματοποιηθεί κρατώντας ιστορικό των παλαιότερων καταχωρήσεων και να

συγκριθούν με τις τωρινές εγγραφές. Επίσης υπάρχουν διάφορα εργαλεία που πραγματοποιούν αυτόματα τον έλεγχο αυτόν και σε περίπτωση ανάγκης προειδοποιούν τον διαχειριστή.

3.2 Επιθέσεις Παρακολούθησης (Sniffing).

Η επίθεση αυτή χρησιμοποιεί ένα **Packet sniffer** ή σκέτο sniffer όπως αλλιώς λέγεται. Αυτό είναι ένα λογισμικό που παρέχει τη δυνατότητα παρακολούθησης των πακέτων ενός δικτύου. Καθώς μεταφέρονται τα πακέτα μπορεί κάποιο πακέτο που πληροί συγκεκριμένα κριτήρια να γίνει αντιληπτό και να καταγραφεί σε ένα αρχείο. Σε πολλές περιπτώσεις μπορεί να χρησιμοποιηθεί από συγκεκριμένες ομάδες (πχ μηχανικοί δικτύων, διαχειριστές συστημάτων) χρησιμοποιούν αυτό το λογισμικό νόμιμα για την καταγραφή ή την βελτιστοποίηση της κίνησης ενός δικτύου.

Πως λειτουργεί

Η πλειοψηφία των προσωπικών υπολογιστών συνδέονται σε ένα τοπικό δίκτυο (LAN), γεγονός που σημαίνει ότι μοιράζονται μια κοινή σύνδεση με άλλους υπολογιστές. Αν δεν χρησιμοποιείται **μεταγωγέας – switch**, το οποίο είναι μια συσκευή που φιλτράρει και ξαναστέλνει τα πακέτα κατά μήκος του LAN, τότε η κίνηση ενός πακέτου που προορίζεται για έναν συγκεκριμένο τομέα του δικτύου θα μεταδοθεί σε κάθε συνδεδεμένο υπολογιστή στο δίκτυο. Άρα τα δεδομένα γίνονται ορατά και από τον υπολογιστή που προορίζονταν και από όλους τους άλλους γειτονικούς υπολογιστές.

Το snifferαναγκάζει τον υπολογιστή και πιο συγκεκριμένα την κάρτα δικτύου να δώσει σημασία και σε αυτά τα πακέτα που προορίζονταν για άλλους υπολογιστές. Για να το καταφέρει αυτό θέτει τη κάρτα **Διασύνδεσης Δικτύου–NIC** (η κάρτα αυτή συνδέει έναν υπολογιστή σε ένα δίκτυο υπολογιστών) σε μια ειδική κατηγορία που ονομάζεται promiscuousmode- **Αδιάκριτη Λειτουργία.** Όταν η NICβρίσκεται σε αυτήν την λειτουργία τότε ένα μηχάνημα μπορεί να βλέπει όλα τα δεδομένα που μεταδίδονται στον τομέα του. Σε αυτή την κατάσταση λειτουργίας απαιτούνται ανώτερα δικαιώματα χρήστη – root.

Υπάρχουν διάφορες δυνατότητες για την κίνηση των πακέτων στο Δίκτυο:

1. Να γίνει επιλογή συγκεκριμένων πακέτων, ώστε να διαγνωστεί και να αντιμετωπιστεί τυχόν πρόβλημα.
2. Τα πακέτα να εξετάζονται λεπτομερώς.
3. Τα πακέτα να μετριούνται ώστε να προστίθενται το συνολικό τους μέγεθος για μια συγκεκριμένη περίοδο ώστε να έχουμε μια καλή εικόνα για το πόσο φορτωμένο ή όχι είναι το δίκτυο. Το αποτέλεσμα μπορεί να παρουσιαστεί είτε με μετρήσεις είτε γραφικά.

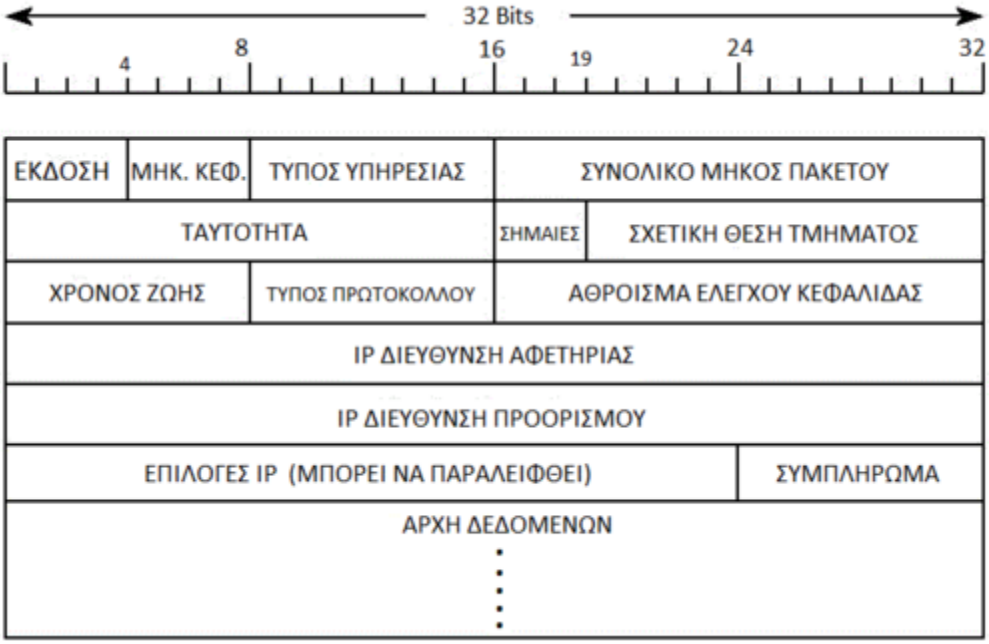
4. Ασφάλεια στο Επίπεδο Δικτύου

4.1 IPV4-IPV6

Η πρώτη μεγάλης κλίμακας έκδοση του Πρωτοκόλλου IP, ήταν η έκδοση 4 **(IPv4)** η οποία είναι η επικρατέστερη μέχρι και σήμερα σε όλο το Διαδίκτυο. Ωστόσο, τα τελευταία χρόνια, λόγω του ότι δεν επαρκούν πλέον οι διευθύνσεις έχει αναπτυχθεί η έκδοση του πρωτοκόλλου 6 (**IPv6**) η οποία είναι εν ενεργεία, χρησιμοποιείται και εξαπλώνεται σταδιακά ανά τον κόσμο.

Το πρωτόκολλο IP έκδοσης 4.

Η έκδοση 4 είναι αυτή που κυριαρχεί στο Διαδίκτυο για αυτό ξεκινάμε πρώτα την αναφορά μας από αυτή.



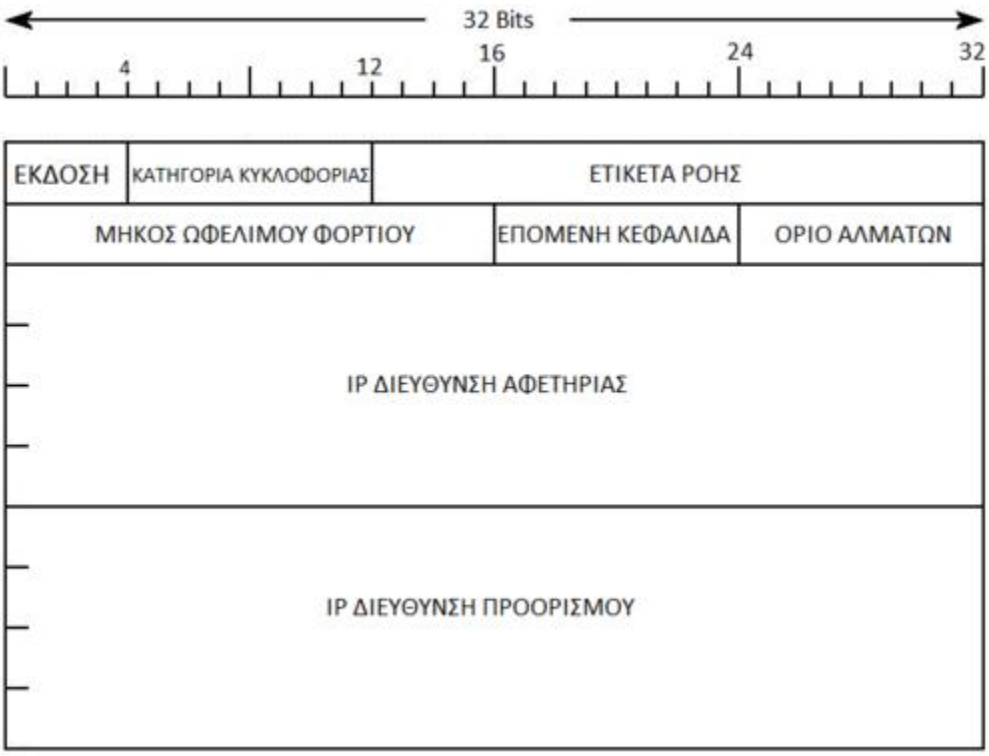
Εικόνα 6: Αρχιτεκτονική πρωτοκόλλου IPv4

Το IPv4 είναι η τέταρτη έκδοση του πρωτοκόλλου Ιντερνέτ, αλλά είναι το πρώτο που χρησιμοποιείται ευρέως. Χρησιμοποιεί ένα 32 bit σύστημα που επιτρέπει να δώσει 4.294.967.296 μοναδικές διευθύνσεις IP. Το IPv4 έχει τέσσερις διαφορετικές κλάσεις που είναι χωρισμένες στις παρακάτω κατηγορίες A, B , C και D. Μία **διεύθυνση** του πρωτοκόλλου IPv4 μοιάζει κάπως έτσι **207. 141. 130. 240**. Το IPv4 χρησιμοποιεί μια μάσκα υποδικτύου, λόγω του μεγάλου αριθμού των υπολογιστών που χρησιμοποιούνται σήμερα. Η **μάσκα υποδικτύου** βοηθά στη μείωση του αριθμού των μοναδικών IP που χορηγούνται σε επιχειρήσεις, εταιρείες, και γενικότερα σε κέντρα με πολλούς υπολογιστές.

4.2 IPv6

Ο λόγος για τον οποίο χρειάζεται να μεταβούμε από IPv4 σε IPv6 είναι λόγω του πληθυσμού του κόσμου που μεγαλώνει ραγδαία καθώς και η αύξηση υπολογιστών που δημιουργεί την ανάγκη για περισσότερες διεύθυνσης IP.

Το IPv6 είναι το επόμενο επίπεδο των IP's. Από ότι φαίνεται η έκδοση 6, θα είναι κατά πάσα πιθανότητα το επόμενο ευρέως διαδεδομένο πρωτόκολλο Internet. Σε σύγκριση με το IPv4 το οποίο επιτρέπει μόνο 4.294.967.296 μοναδικές διευθύνσεις, το IPv6 που χρησιμοποιεί ένα σύστημα 128-bit που θα μπορεί να δώσει 340 - ενδεκάκις εκατομμύρια, ο αριθμός αυτός είναι τόσο μεγάλος που αν το σκεφτούμε υπάρχουν πιο πολλές μοναδικές διευθύνσεις IP από τα αστέρια στο σύμπαν.



Εικόνα 7: Αρχιτεκτονική IPv6.

4.3 Ασφάλεια IP – IPSec

Σήμερα που η ασφάλεια αποτελεί βασική προτεραιότητα, οι ερευνητές του Διαδικτύου έχουν στρέψει την προσοχή τους στη σχεδίαση νέων πρωτοκόλλων επιπέδου δικτύου, που θα παρέχουν υπηρεσίες ασφάλειας δικτύου. Ένα από αυτά τα πρωτόκολλα είναι το IPSec, ένα από τα δημοφιλέστερα ασφαλή πρωτόκολλα επιπέδου δικτύου, το οποίο χρησιμοποιείται ευρέως **σε Εικονικά Δίκτυα** (Virtual Private Networks, VPN).

Το Internet αποτελεί αντικείμενο πολλών και διαφορετικών τύπων επιθέσεων όπως αυτών της απώλειας του απόρρητου, της ακεραιότητας των δεδομένων, της πλαστοπροσωπίας και της άρνησης παροχής υπηρεσιών. Ο στόχος του IPSec είναι η αντιμετώπιση όλων αυτών των προβλημάτων μέσα στην ίδια την υποδομή του δικτύου χωρίς να είναι αναγκαία η εγκατάσταση και η ρύθμιση ακριβών μηχανημάτων και λογισμικού.

Η Ασφάλεια IPSec αποτελεί ένα αξιοσημείωτο κομμάτι της ασφάλειας λόγω του ότι παρέχει ασφάλεια και κρυπτογράφηση στο επίπεδο IP. Η δομή της αποτελείται δυο τύπους δεδομένων στα πακέτα. Την **επικεφαλίδα πιστοποίησης – AH (Authentication Header)** και για **το φορτίο ενθυλάκωσης ασφάλειας – ESP (Encapsulating Security Payload)**. Η **κεφαλίδα** παρέχει υπηρεσίες ακεραιότητας δεδομένων ενώ το **φορτίο ενθυλάκωσης** ασφάλειας παρέχει πιστοποίηση ταυτότητας και ακεραιότητα δεδομένων. Τέλος η IPSec ορίζει κάποιες παραμέτρους για την καλύτερη επικοινωνία μεταξύ συσκευών όπως η διαχείριση των κλειδιών και οι συσχετισμοί ασφαλείας (association security).

4.4 Ενθυλάκωση

Ονομάζεται η διαδικασία με την οποία στα δεδομένα προστίθεται μια επικεφαλίδα (AH –Application Header) η οποία περιέχει την απαιτούμενη πληροφορία για το αντίστοιχο πρωτόκολλο του N-επιπέδου του δεύτερου ανοικτού επιπέδου.

Η διαδικασία συνεχίζεται προς τα κάτω έως το επίπεδο 2 το οποίο προσθέτει την επικεφαλίδα και μια «ουρά» (trailer) η οποία αποτελείται από μια ακολουθία ελέγχου πλαισίου (FLC – Frame Check Sequence) που χρησιμεύει για ανίχνευση λαθών.

Το επίπεδο 2 παράγει μια μονάδα που ονομάζεται «πλαίσιο» (frame) και μεταδίδεται δια μέσου του φυσικού επιπέδου στο μέσο μετάδοσης. Με την λήψη του πλαισίου από τον αποδέκτη, δηλαδή το δεύτερο σύστημα, θα ακολουθηθεί η αντίστροφη διαδικασία.

Καθώς τα δεδομένα ανεβαίνουν ιεραρχία κάθε επίπεδο προχωρά σε τρείς ενέργειες :

1. Αφαιρεί την αντίστοιχη εξωτερική επικεφαλίδα.
2. Ενεργεί επί της πληροφορίας πρωτοκόλλου που περιέχεται σε αυτή.
3. Τέλος, προωθεί το υπόλοιπο τμήμα στο αμέσως ανώτερο επίπεδο.

Σε κάθε βήμα της διαδικασίας είναι δυνατό ένα επίπεδο, εφόσον πληροί τις απαιτήσεις του, να τμηματοποιήσει τη μονάδα δεδομένων που λαμβάνει από το ανώτερο επίπεδο. Σε μια τέτοια περίπτωση, τα τμήματα που θα προκύψουν θα πρέπει να επανασυνδεθούν στο αντίστοιχο επίπεδο του άλλου συστήματος και εν συνεχεία να

προωθηθούν, σαν μια ενιαία μονάδα δεδομένων, στο αμέσως επόμενο επίπεδο του.

Η ανταλλαγή δεδομένων μεταξύ δυο ομότιμων οντοτήτων μπορεί να γίνει με δυο τρόπους. Ο πρώτος χρειάζεται μια εκ των προτέρων λογική σύνδεση, η οποία θα δημιουργεί την έννοια των νοητών κυκλωμάτων (VCs – Virtual Circuits). Αυτή η έννοια είναι γνωστή ως "προσανατολισμός προς σύνδεση" (CO-Connection Oriented). Ο δεύτερος τρόπος, πριν από την μεταφορά δεδομένων δεν συμβαίνει κανενός είδους διαπραγμάτευση μεταξύ των οντοτήτων, είναι γνωστός ως «χωρίς σύνδεσης» (CL-Connectionless) τρόπος μεταφοράς.

Ο **έλεγχος ροής** συμβάλλει έτσι ώστε να μην παρουσιάζονται φαινόμενα υπερχείλισης. Είναι μια λειτουργία που εκτελείται από μια (N)-οντότητα με στόχο τον περιορισμό του μεγέθους της ροής των δεδομένων που δέχεται από μια άλλη (N)-οντότητα.

Ο **έλεγχος λάθους** αφορά τους μηχανισμούς ανίχνευσης και διόρθωσης λαθών που συμβαίνουν κατά τη μετάδοση μονάδων δεδομένων μεταξύ ίσων οντοτήτων.

Η **πολυπλεξία** συμβαίνει, όταν δύο ή περισσότερα επίπεδα αρχιτεκτονικής απασχολούν ένα προσανατολισμένο - προς - σύνδεση πρωτόκολλο.

Η όλη διαδικασία μπορεί να γίνει σε δυο διευθύνσεις:

- Πολυπλεξία προς τα άνω

Σε μια τέτοια περίπτωση, πολύ-πλέκονται πολλαπλές (N)- συνδέσεις, διαμοιράζοντας έτσι μια μοναδική (N-1) σύνδεση. Η πολυπλεξία αυτή προτιμάται σε περιπτώσεις που είναι επιθυμητή η χρήση της συγκεκριμένης (N-1) σύνδεσης, ή σε περιπτώσεις που πρέπει να δοθούν πολλαπλές (N) συνδέσεις σε ένα περιβάλλον, στο οποίο υπάρχει μια μόνο απλή (N-1) σύνδεση.

- Πολυπλεξία προς τα κάτω

Στην περίπτωση αυτή μια μοναδική (N) σύνδεση δημιουργείται πάνω σε πολλαπλές (N-1) συνδέσεις, αποτέλεσμα της τεχνικής αυτής, είναι ο

διαμοιρασμός της κίνησης της (N) - σύνδεσης και η γενικότερη αύξηση της αξιοπιστίας και της απόδοσης της διασύνδεσης

4.5 Ορισμός IPSec

Μπορούμε πλέον να υποστηρίξουμε πως το IPSec είναι ένα πρωτόκολλο ανοικτών προδιαγραφών για την διασφάλιση του απορρήτου των επικοινωνιών. Διασφαλίζει την **εμπιστευτικότητα**, την **ακεραιότητα** και την **αυθεντικότητα** των επικοινωνιών σε ένα IPδίκτυο.
Παρέχει **κρυπτογράφηση** και **πιστοποίηση επιπέδου δικτύου** παρέχοντας μια λύση ασφάλειας μέσα στην ήδη υπάρχων αρχιτεκτονική του δικτύου.

4.6 Χρήση της IPSec

1. Απώλεια απορρήτου – Loss of Privacy

Ο μεγαλύτερος ανασταλτικός παράγοντας επικοινωνίας μεταξύ δυο επιχειρήσεων ή οποιονδήποτε οντοτήτων είναι το να έχει καταφέρει κάποιος να εισχωρήσει στο δίκτυο και να παρακολουθεί εμπιστευτικά δεδομένα που διακινούνται. Χωρίς να έχουμε κρυπτογραφήσει το μήνυμα μου μεταδίδεται τότε είναι εύκολη λεία για οποιονδήποτε καταφέρει να εισχωρήσει παράνομα στο δίκτυο. Η πιο συνηθισμένη περίπτωση που συναντάται είναι η επίθεση Packet sniffers. Στην οποία οι εισβολείς εγκαθιστώντας Packet sniffers συλλέγουν ονόματα, κωδικούς και οποιαδήποτε πληροφορία και τα αντικαθιστούν με άλλες λειτουργιές. Περαιτέρω πληροφορίες θα αναλύσουμε παρακάτω.

2. Απώλεια ακεραιότητας δεδομένων

Υπάρχει περίπτωση μέσα στο δίκτυο να ανταλλάσσονται πληροφορίες που δεν είναι εμπιστευτικές και δεν μας ενδιαφέρει και ιδιαίτερα αν κάποιος τρίτος μπορούσε να της δει, όμως μας ενδιαφέρει ιδιαίτερα αν αυτός ο τρίτος προσπαθούσε να αλλοιώσει το περιεχόμενο που μεταφέρεται. Άρα θα πρέπει να ληφθούν κάποια μέτρα διασφάλισης της ακεραιότητάς τους.

3. Άρνηση παροχής υπηρεσιών – Denial of Service

Αυτό το μέτρο αφορά οργανισμούς και άτομα που εκμεταλλεύονται το Διαδίκτυο. Τα τελευταία χρόνια όλο και περισσότεροι hackersβρίσκουν αδυναμίες στο πρωτόκολλο TCP / IP που τους δίνει την δυνατότητα να επιτίθενται στις μηχανές του συστήματος. Άρα οι οργανισμοί θα πρέπει να διασφαλίσουν την διαθεσιμότητα του συστήματός τους.

4. Πλαστοπροσωπία – Identity Spoofing

Πέρα από το να προστατεύσουμε τα δεδομένα μας στο διαδίκτυο θα πρέπει να προστατεύσουμε και την ταυτότητα μας μέσα σε αυτό. Υπάρχει περίπτωση ένας κακόβουλος χρήστης να αποκτήσει πρόσβαση και να κλέψει την ταυτότητα κάποιου με αποτέλεσμα να αποκτήσει πρόσβαση σε προσωπικές εμπιστευτικές πληροφορίες (IPSpoofing). Για να το αποφύγουμε μπορούν να χρησιμοποιηθούν συστήματα που θα βασίζονται στην IPδιεύθυνση και θα αναγνωρίζουν μοναδικά τους χρήστες.

4.7 IP Spoofing

Η επίθεση αυτή βασίζεται στις σχέσεις εμπιστοσύνης μεταξύ των δικτύων και των συστημάτων στο Internet. Η επίθεση αυτή γίνεται από τον root λογαριασμό του επιτιθέμενου host προς τον root λογαριασμό του θύματος.

Για την καλύτερη κατανόηση της επίθεσης θα χρησιμοποιήσουμε τους εξής συμβολισμούς για την πιο κάτω ανάλυση :

A: Ο host στόχος

B: Ο έμπιστος host (ο Α εμπιστεύεται τον Β)

X: Ο απροσέγγιστος host (δεν είναι δυνατόν να λάβει μηνύματα που προορίζονται για αυτόν)

Z: Ο επιτιθέμενος host

Για να ξεκινήσει η επίθεση θα πρέπει ο επιτιθέμενος host Z να πάρει την ταυτότητα ενός έμπιστου host ως προς τον A. Στην συνέχεια, απενεργοποιεί τον έμπιστο αυτόν host B εξαπολύοντάς του μια TCP/SYN επίθεση άρνησης υπηρεσίας. Έτσι επιτυγχάνει να ξεκινήσει έναν διάλογο με τον στόχο A προσποιούμενος ότι είναι ο έμπιστος B.

Ο host Z στέλνει μεταμφιεσμένα (spoofed) IP datagrams στον A τα οποία βρίσκουν το στόχο τους. Και αυτό συμβαίνει επειδή το IP είναι ασυνδεσμικό πρωτόκολλο επομένως κάθε datagram στέλνεται στον προορισμό του ανεξάρτητα από το εάν έχει υπάρξει σύνδεση μεταξύ των 2 hosts. Αφού ο B έχει δεχθεί επίθεση τα datagrams που στέλνει πίσω ο A δεν φτάνουν ποτέ στον προορισμό B αλλά παρ' ολαυτά ούτε ο Z μπορεί να τα δει. Τα datagrams προέρχονται από το Επίπεδο Δικτύου και εκεί πρέπει να κατευθυνθούν οι απαντήσεις , όταν τα datagrams δρομολογηθούν στον host B και η πληροφορία αρχίσει να αποπλέκετε , φτάνει στο TCP και καταστρέφεται εφόσον ο B δεν μπορεί να απαντήσει. Ο Z δεν μπορεί να δει αυτά που έστειλε ο A αλλά μπορεί να τα προβλέψει και έτσι συνεχίζει την επικοινωνία του με τον A.

Σημαντική και απαραίτητη **προϋπόθεση** για την επίθεση είναι η γνώση ενός τουλάχιστον host που εμπιστεύεται ο A. Σε περίπτωση που ο A δεν έχει κανέναν έμπιστο host τότε η επίθεση τελειώνει πριν καν αρχίσει. Στη συνέχεια πρέπει ο Z να αποκτήσει μια πρώτη ιδέα σχετικά με το ποιος είναι ο 32-bitαριθμός ακολουθίας στα TCP segments που αποστέλλει ο A. Για να επιτευχθεί αυτό, συνδέεται με την πραγματική του διεύθυνση σε μια TCP port (πχ SMTP) και πραγματοποιεί μαζί του ένα τριπλό handshake, αποθηκεύοντας τον ISN (Initialsequence Number) που χρησιμοποίησε ο A. Η διαδικασία αυτή επαναλαμβάνεται αρκετές φορές και οι ISNs επίσης αποθηκεύονται. Ο Z υπολογίζει το μέσο χρόνο κυκλικού ταξιδιού (Round Trip Time, RTT) των πακέτων από αυτόν στον A και πάλι σε αυτόν, μιας και το Round Trip Time είναι απαραίτητο για την πρόβλεψη του επόμενου ISN. Μέχρι αυτή η στιγμή, ο επιτιθέμενος host Z έχει στη διάθεσή του τα εξής στοιχεία : γνωρίζει τον τελευταίο ISN

που χρησιμοποίησε ο Α, ξέρει με τι ρυθμό αυξάνονται οι αριθμοί ακολουθίας και τέλος γνωρίζει πόσος περίπου χρόνος θα χρειαστεί ώστε ένα IP datagram να μεταφερθεί στο Internet ώστε να φτάσει στον προορισμό Α, που συνήθως ο χρόνος είναι το μισό του RTT μιας και τις περισσότερες φορές οι δρόμοι είναι συμμετρικοί.

Χρησιμοποιώντας τις πιο πάνω πληροφορίες ο επιτιθέμενος προχωράει στο **δεύτερο επίπεδο της επίθεσης**. Συμβολίζοντας με Z(B) τον Z που παριστάνει τον Β έχουμε :

1. Z(B) ---SYN → A
2. B ← SYN/ACK --- A
3. Z(B) --- ACK→ A
4. Z(B) ---PSH* → A

(*Με PSH συμβολίζουμε πως όταν είναι αληθές δίνεται εντολή στον παραλήπτη να προωθήσει τα δεδομένα που έχει καταχωρήσει στην ουρά του, στην εφαρμογή όσο γίνεται πιο γρήγορα.)

Στο βήμα 1 ζητείτε σύνδεση του host Z παριστάνοντας τον Β. Μέτα ο επιτιθέμενος πρέπει να αφήσει ένα χρονικό περιθώριο στον Α ώστε να στείλει το SYN/ACK πακέτο το οποίο ο Z δεν μπορεί να το δει. Στο ακόλουθο βήμα 3ο Z στέλνει ένα ACK στον Α με τον αριθμό ακολουθίας που έχει προβλέψει συν 1 διότι κάνει επιβεβαίωση. Ανάλογα την πρόβλεψη του Z στο βήμα 3, υπάρχουν 3ης διαφορετικές περιπτώσεις αντίδρασης του Α.

1) Αν ο αριθμός ακολουθίας είναι ακριβώς αυτός που περίμενε το TCP, τότε τα εισερχόμενα δεδομένα τοποθετούνται στην επόμενη διαθέσιμη θέση στον καταχωρητή.

2) Αν ο αριθμός ακολουθίας είναι μικρότερος από την αναμενόμενη τιμή, τα bytes θεωρούνται προϊόν αναμετάδοσης και απορρίπτονται.

3) Αν ο αριθμός ακολουθίας είναι μεγαλύτερος από την αναμενόμενη τιμή αλλά μέσα στα όρια του πεδίου window τα bytes δεδομένων θεωρούνται πως ήρθαν νωρίτερα από ότι έπρεπε οπότε αποθηκεύονται προσωρινά από το TCP το οποίο περιμένει την άφιξη των bytes που υπολείπονται.

–έξω από τα όρια του πεδίου window, τότε το segment απορρίπτεται και το TCP στέλνει πίσω ένα segment που θα αναγράφει τον αναμενόμενο αριθμό ακολουθίας.

Τέλος αν έχει γίνει σωστή πρόβλεψη του ACK ο Α παραβιάζεται και μπορεί να αρχίσει η μεταφορά των δεδομένων του βήματος 4. Μετά την παραβίαση ο επιτιθέμενος εισάγει ένα **backdoor**στο σύστημα το όποιο θα του επιτρέψει έναν ευκολότερο τρόπο εισβολής.

Μέτρα Πρόληψης

Μια πρώτη λύση είναι η χρήση ενός καλά διαμορφωμένου δρομολογητή με τη δυνατότητα **φιλτραρίσματος** (packet filtering **router**). Είναι απαραίτητο οι χρήστες του LAN να μην αναπτύσσουν σχέσεις εμπιστοσύνης με κανέναν από τους hosts εκτός του LAN. Επιπλέον, το **IPSpoofing**είναι δυνατόν να **αποτραπεί** εάν όλα τα πακέτα που εισέρχονται ή εξέρχονται από το δίκτυο αυθεντικοποιούνται ή και να κρυπτογραφούνται. Τέλος, καλό θα ήταν να βρεθεί ένας μηχανισμός ώστε ο ISN να μη μπορεί να προβλεφθεί.

4.8 Firewalls

Το firewall είναι ένας μηχανισμός ο οποίος ελέγχει την πρόσβαση προς και από το δίκτυο. Είναι ένα ενδιάμεσο στοιχείο από το περνάει όλη η δικτυακή κίνηση. Τα firewalls μπορεί να είναι υλοποιημένα ως **λογισμικό** είτε ως **δικτυακές συσκευές**. Ορόλος τους είναι να ελέγχουν την δικτυακή κίνηση και να αποκόπτουν την επικοινωνία όποτε κριθεί απαραίτητο. Η πλειοψηφία των firewallsπου έχουν υλοποιηθεί ελέγχουν την εισερχόμενη ροή, ωστόσο μόνο τα πιο εξεζητημένα ελέγχουν και την εξερχόμενη. Η εισερχόμενη κίνηση είναι σαφώς πιο επικίνδυνη αυτό όμως δεν σημαίνει ότι και η εξερχόμενη δεν μπορεί να κρύβει κινδύνους. Όπως

για παράδειγμα δεν θα ήθελε κανείς να έχει έναν ιό δούρειο ίππο που καταγράφει τα στοιχεία της πιστωτικής του κάρτας και να τα στέλνει σε κάποιον άλλο υπολογιστή. Αυτή λοιπόν, είναι μια κίνηση εξερχόμενης κίνησης η οποία μπορεί μόνο από firewalls που περιέχουν και έλεγχο εξερχόμενης κίνησης.

Τα **firewalls λογισμικού** αποτελούν την συχνότερη και πιο φτηνή περίπτωση. Τον έλεγχο έχουν οι χρήστες αν και αυτό μπορεί να μην είναι αρκετά βολικό μιας και ο χρήστης μπορεί να μην έχει τις γνώσεις που απαιτούνται με αποτέλεσμα άθελα του να επιτρέψει εισερχόμενη ή εξερχόμενη ροή την οποία κανονικά θα ήθελε να αποκόψει. Υπάρχει επίσης ενδεχόμενο κάποιο firewall να αποκλείει κάποιο πρόγραμμα που ο χρήστης θέλει να τρέξει, με αποτέλεσμα να μειώνει το επίπεδο προστασίας του firewall.

Τα **firewalls δικτυακής συσκευής** κατά πλειοψηφία έχουν μεγαλύτερη απόδοση και παρέχουν μεγαλύτερη ασφάλεια στους χρήστες που το χρησιμοποιούν. Αυτό συμβαίνει επειδή ρυθμίζονται από εξειδικευμένο χρήστη ο οποίος διαθέτει την απαιτούμενη τεχνογνωσία και επιτρέπει μόνο την κίνηση που πρέπει. Ένα μειονέκτημα είναι πως όλα τα μηχανήματα τα οποία προστατεύονται από το firewall εξαρτώνται από τις ρυθμίσεις συσκευής. Δηλαδή, οποιαδήποτε αλλαγή χρειαστεί να γίνει θα γίνει από την συσκευή και όχι τοπικά στο σύστημα. Βέβαια, οποιοδήποτε τέτοιο μειονέκτημα κι αν υπάρχει υπερκαλύπτετε από το μέγεθος της ασφάλειας που προσφέρεται. Τέλος μην ξεχνάμε πως το κόστος μιας τέτοιας υλοποίησης είναι αρκετά υψηλό.

Μια ακόμα πιο ολοκληρωμένη και ασφαλής τεχνική θα ήταν να υπήρχε μια συσκευή firewall αλλά και κάθε μηχάνημα να είχε εγκατεστημένο ένα firewall λογισμικού. Έτσι, το αποτέλεσμα της ασφάλειας θα ήταν διπλάσιο μιας και θα είχαμε δυο επίπεδα δικτυακής προστασίας.

Αποκρινόμενοι στις ολοένα και αυξανόμενες νέες απειλές και απαιτήσεις των χρηστών οι εταιρείες firewall έχουν εισάγει καινούργια χαρακτηριστικά. Αυτά τα χαρακτηριστικά διαφέρουν ανάλογα την χρήση, μερικά είναι τα εξής:

– **Εργαλεία Διαχείρισης και Διαμόρφωσης των firewalls**, ανάλογα την κατηγορία του firewallχρησιμοποιούνται και διαφορετικά πρωτόκολλα. Μερικά συστήματα επιτρέπουν τον

έλεγχο ορθότητας μέσω διάφορων πρωτοκόλλων όπως το SMTP, το SNMP και το HTTP μέσω διαδικτύου. Τέλος άλλες κατηγορίες firewall χρησιμοποιούν GUIs (Graphical User Interfaces) για την ευκολία των διαχειριστών στη διαμόρφωση τους.

- **Network Address Translation, σε μια τέτοια διαδικασία Μετάφρασης Διεύθυνσης Δικτύου** το firewall αντικαθιστά τις IPδιευθύνσεις των πακέτων με διαφορετικές. Αυτό συμβαίνει για λόγους ασφάλειας. Το NAT έχει την δυνατότητα να κρύβει την ύπαρξη συγκεκριμένων συστημάτων στο εσωτερικό του δικτύου όπως επίσης και την δομή του εσωτερικού του δικτύου. Επίσης ένα άλλο χαρακτηριστικό, βέβαια όχι τόσο σχετικό με την ασφάλεια είναι , η δυνατότητα να μετατρέπει hosts δικτύου με μη μοναδικές διευθύνσεις σε hostsμε μοναδικές διευθύνσεις. Αυτό έχει ως σκοπό να αποκρύπτονται οι εσωτερικές διευθύνσεις.
- **Καινούργια Proxies και υπηρεσίες**, προσθέτονται ολοένα και περισσότερα proxiesμε σκοπό την επέκταση της λειτουργικότητας των firewalls. Αν δεν υπάρχουν τα κατάλληλα proxies οι υπηρεσίες που παρέχονται θα είναι μειωμένες και όλος ο φόρτος θα είναι στους διαχειριστές του συστήματος.
- **Καταγραφή και έλεγχος ορθότητας**, οι πλειοψηφία των firewalls παρέχει μηχανισμούς καταγραφής λειτουργιών και ελέγχου ορθότητας. Με την βοήθεια του ελέγχου ορθότητας επεξεργάζονται την ήδη καταγεγραμμένη πληροφορία και την παρουσιάζουν με έναν πιο απλοϊκό τρόπο. Επίσης παρέχουν προειδοποιητικούς μηχανισμούς που ενημερώνουν σε πραγματικό χρόνο τους διαχειριστές για κακόβουλες λειτουργίες που επιχειρούνται στο firewall.

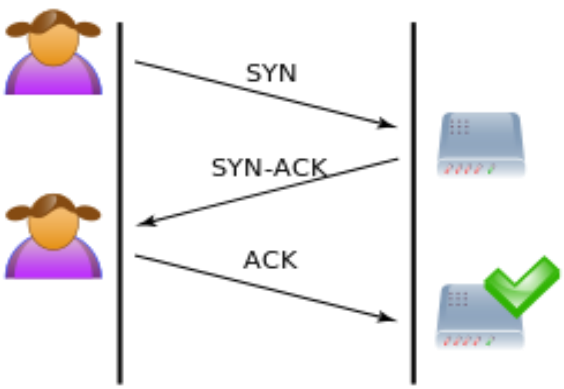
5. Ασφάλεια στο επίπεδο μεταφοράς

5.1 Προβλήματα Ασφαλείας στο TCP/IP.

Ένα TCP/IP δίκτυο πολλές φορές μπορεί να αντιμετωπίσει αρκετά προβλήματα ασφαλείας. Αρκετά προβλήματα από αυτά (ανάλογα την σπουδαιότητα τους) απασχολούν είτε τους διαχειριστές συστημάτων, είτε τους απλούς χρήστες ενός δικτύου. Μερικά από αυτά το προβλήματα ασφαλείας και τους τρόπους αντιμετώπισης θα αναλύσουμε παρακάτω.

5.2 TCP/SYNFLOODING – Πλημμύρισμα με SYN Πακέτα

Η επίθεση TCP/SYNFLOODING είναι μια επίθεση άρνησης πρόσβασης κατά την οποία ο επιτιθέμενος αποστέλλει πολλαπλές αιτήσεις SYN προς το θύμα και έχει ως αποτέλεσμα την μη ανταπόκριση των serversσε αιτήσεις για νέες συνδέσεις από clients.



Για να **δημιουργηθεί μία** σύνδεση **TCP** από έναν υπολογιστή (πελάτης - client) σε έναν άλλο (διακομιστής - server) θα πρέπει οι δύο υπολογιστές να εμπλακούν σε μία διαδικασία που ονομάζεται **τριμερής χειραψία** (three-wayhandshake), η οποία περιληπτικά έχει ως εξής:

1. Ο πελάτης (client) ζητά την δημιουργία μίας σύνδεσης στέλνοντας έναν πακέτο TCP SYN στον διακομιστή (server). Το όνομα του πακέτου προέρχεται από την λέξη syncronize που σημαίνει συγχρονισμός.
2. Ο διακομιστής απαντά στην αίτηση του πελάτη στέλνοντάς του ένα πακέτο TCP SYN-ACK, από την αγγλική λέξη acknowledge που σημαίνει αναγνώριση, αποδοχή.
3. Ο πελάτης απαντά με ένα πακέτο TCP ACK δηλώνοντας ότι αποδέχεται και αυτός την σύνδεση.

Η επίθεση έχει ως εξής:

1. Ο επιτιθέμενος αποστέλλει στον διακομιστή-θύμα πολλαπλά πακέτα TCP SYN.
2. Ο διακομιστής θεωρεί ότι τα πακέτα αυτά προέρχονται από κανονικό χρήστη, οπότε απαντά με πακέτα SYN-ACK σύμφωνα με την διαδικασία χειραψίας του πρωτοκόλλου TCP.
3. Ο επιτιθέμενος όμως δεν αποστέλλει πακέτα ACK για να ολοκληρωθεί η χειραψία, αλλά αφήνει τον διακομιστή να περιμένει.

Επειδή για κάθε ημιτελή σύνδεση TCP ο διακομιστής ξοδεύει υπολογιστικούς πόρους, μετά από κάποιο συγκεκριμένο αριθμό τέτοιων συνδέσεων ο διακομιστής φτάνει στα όριά του και δεν μπορεί να εξυπηρετήσει τους νόμιμους χρήστες. Αυτή η κατάσταση ονομάζεται **άρνηση υπηρεσιών (DOS – Denial of Service).**

Η επίθεση SYN flooding είναι διαδεδομένη και το μεγαλύτερο μέρος των σημερινών δικτύων υπολογιστών μπορεί να ανταπεξέλθει με επιτυχία. Βασική όμως προϋπόθεση για να επιτύχει η επίθεση είναι ο διακομιστής να δεσμεύσει πόρους του συστήματος αμέσως μόλις δεχθεί το πρώτο ACK πακέτο και όχι μετά το τέλος της τριμερής χειραψίας.

Για την αντιμετώπιση αυτής της επίθεσης υπάρχουν διάφοροι τρόποι:

- **Φιλτράρισμα.**
  Μιας και το δίκτυο προωθεί τα πακέτα με βάση την διεύθυνση προορισμού τους, ο μόνος τρόπος για την πιστοποίηση της προέλευσης ενός πακέτου είναι η χρήση φιλτραρίσματος της εισόδου με βάση την πηγή (input source filtering) είτε χρησιμοποιώντας firewalls.
- **Καταγραφή του αριθμού των συνδέσεων** που έχει ξεκινήσει κάθε πελάτης (client) και η απαγόρευση δημιουργίας νέων συνδέσεων όταν ο αριθμός αυτός ξεπεράσει κάποιο προκαθορισμένο όριο.

5.3 Επίθεση με UDP πακέτα

Η επίθεση αυτή είναι γνωστή ως **UDP packet storm – Καταιγίδα UDP πακέτων**. Η χρήση του UDP για επιθέσεις άρνησης υπηρεσίας δεν είναι τόσο απλή όσο με το πρωτόκολλο ελέγχου μετάδοσης (TCP). Παρόλαυτα, μια επίθεση πλημμύρας UDP μπορεί να ξεκινήσει στέλνοντας ένα μεγάλο αριθμό πακέτων UDP σε τυχαίες θύρες σε απομακρυσμένο κεντρικό υπολογιστή. Ένας μεγάλος αριθμός UDP πακέτων αποστέλλεται σε ένα σύστημα, με αποτέλεσμα την μείωση της απόδοσης του συστήματος που λαμβάνει την πληθώρα των πακέτων. Έτσι, για μεγάλο αριθμό πακέτων UDP, το σύστημα θα αναγκαστεί να στείλει πολλά πακέτα ICMP, οδηγώντας το τελικά στο να μην είναι προσβάσιμο από τους χρήστες.

Αντιμετώπιση

Η επίθεση αυτή μπορεί να αντιμετωπιστεί με την **ανάπτυξη τείχους προστασίας** στα κυρίως σημεία ενός δικτύου ώστε να φιλτράρει την ανεπιθύμητη κίνηση στο δίκτυο. Το πιθανό θύμα δεν λαμβάνει και δεν αποκρίνεται ποτέ στα κακόβουλα πακέτα UDP επειδή το τείχος προστασίας τα σταματά. Ωστόσο μπορεί να υπάρξουν φορές που το τείχος προστασίας να είναι επιρρεπές σε κάποια επίθεση πλημμύρας μιας και μπορούν να πραγματοποιήσουν συγκεκριμένο αριθμό ελέγχων κάθε φορά.

5.4 Η επίθεση Ping of Death και Teardrop

Αυτές οι επιθέσεις εκμεταλλεύονται τις αδυναμίες του πρωτοκόλλου TCP-IPκαι του λογισμικού που το χρησιμοποιεί για επικοινωνία μέσω Internet.
Η επίθεση **Ping of Death** αφορά την αποστολή πακέτων δεδομένων μεγαλύτερων του μέγιστου των 65,536 που επιτρέπονται από το TCP-IP. Όταν ο υπολογιστής λάβει ένα τέτοιο πακέτο είναι πιθανό να αντιμετωπίσει πρόβλημα λειτουργίας.

Λύση:
Διόρθωση της έκδοσης του λογισμικού από τους κατασκευαστές με τέτοιο τρόπο ώστε τα συστήματα να μην είναι ευπαθή σε τέτοιες επιθέσεις.

Γενικότερα τα μηνύματα στέλνονται διασπασμένα σε πακέτα τα οποία επανασυντίθενται στο αρχικό μήνυμα στον υπολογιστή λήψης. Η επίθεση **Teardrop**παράγει μηνύματα τα οποία αποτελούνται από αντικρουόμενες πληροφορίες για την σειρά των πακέτων. Αυτό αποτελεί πρόβλημα γιατί ο υπολογιστής που θα τα λάβει θα βρεθεί σε σύγχυση και θα προσπαθήσει να επανασυναρμολογήσει τη σειρά των πακέτων.

5.5 Ασφάλεια Επιπέδου Μεταφοράς, TLS – Transport Layer Security

Το TLS είναι ένα πρωτόκολλο που πιστοποιεί πως κατά την επικοινωνία server – client μέσω Διαδικτύου δεν πρόκειται να υπάρχει μεσολάβηση κάποιου τρίτου με σκοπό την υποκλοπή δεδομένων και πληροφοριών. Το TLS θα μπορούσε κάποιος να υποστηρίξει πως είναι ο διάδοχος του SSL. Όπως και το SSL είναι πρωτόκολλο κρυπτογράφησης και λειτουργεί ως ενδιάμεσο πρωτόκολλο μεταξύ επιπέδου εφαρμογής και επιπέδου μεταφοράς. Το TLS αποτελείται από δυο επιμέρους επίπεδα. Το TLS Record Protocol και TLS Hand shake Protocol.

Και τα δυο επίπεδα χρησιμοποιούν το πιστοποιητικό X.509 και μέσω ασύμμετρης κρυπτογραφίας αυθεντικοποιούν το άλλο μέρος της επικοινωνίας ανταλλάσσοντας ένα συμμετρικό κλειδί. Το κλειδί λειτουργεί για να κρυπτογραφήσει την μεταφερόμενη πληροφορία μεταξύ των δυο πλευρών, εξασφαλίζοντας έτσι την εμπιστευτικότητα

των δεδομένων και των κωδικών αυθεντικοποιήσης μηνυμάτων. Κάποιες εκδόσεις του πρωτοκόλλου συναντώνται αρκετά συχνά σε διάφορες εφαρμογές, όπως στην πλοήγηση στο διαδίκτυο, στο ηλεκτρονικό ταχυδρομείο, στα άμεσα μηνύματα και στην τηλεφωνία μέσω διαδικτύου. Παρόλο που είναι ιδιαίτερα αποδοτικό σε έμπιστα δίκτυα για την πιστοποίηση ταυτότητας, αποτελεί ανίκανη τεχνική για δίκτυα αβέβαιης ασφαλείας μιας και είναι ευάλωτο σε επιθέσεις MITM (man in the middle attack).

Στη στοίβα πρωτοκόλλων IP τα πρωτόκολλα SSL και TLS κρυπτογραφούν τα δεδομένα της σύνδεσης στο επίπεδο εφαρμογής. Σε μοντέλα παρόμοια του OSI τα δυο αυτά πρωτόκολλα αρχικοποιούνται στο πέμπτο επίπεδο δηλαδή το επίπεδο συνόδου και δρουν στο επίπεδο 6, στο επίπεδο παρουσίασης δηλαδή. Στο επίπεδο συνόδου πραγματοποιείται μια χειραψία μέσω της ασύμμετρης κρυπτογράφησης και το κλειδί συνόδου. Μέσω του TLS πρωτοκόλλου επιτρέπεται στις εφαρμογές client – server να επικοινωνούν μέσω του δικτύου. Για να επιτευχθεί σωστή επικοινωνία θα πρέπει ο client να δείχνει στον server την εγκαθίδρυση της TLS σύνδεσης. Για να γίνει αυτό, υπάρχουν 2 τρόποι. Πρώτα, είναι η χρήση διαφορετικού κάθε φορά αριθμού θύρας για το TLS όταν αυτό συνδέεται. Και ο δεύτερος τρόπος είναι, ο client να ζητήσει από τον server να αλλάξει την σύνδεση του με το TLS χρησιμοποιώντας τον κατάλληλο μηχανισμό πρωτοκόλλου, όπως για παράδειγμα τον STARTTLS. Που χρησιμεύει για ηλεκτρονικό ταχυδρομείο και ειδήσεις.

Πλεονεκτήματα

Τα σημαντικότερα πλεονεκτήματα του TLS με το SSL σχετίζονται με το πώς αυτά τα δυο πρωτόκολλα έχουν αναπτυχθεί. Βάσει αυτών των πλεονεκτημάτων μπορούμε να υποστηρίξουμε και την αντικατάσταση του SSL από το TLS.

- Είναι προς τα πίσω συμβατό, γεγονός που σημαίνει πως χρησιμοποιείται για την ασφάλεια του πελάτη όταν αυτός υποστήριζε το SSL.
- Προστατεύει δεδομένα που προέρχονται από ηλεκτρονικό ταχυδρομείο και οικονομικές συναλλαγές.

- Με την παρουσία του βοηθάει να γίνεται αντιληπτό πότε συνδέεται κάποιος με τον server και όχι με κάποιον τρίτο που έχει ως στόχο κάποια κακόβουλη ενέργεια.
- Για μεγαλύτερη αξιοπιστία, η όποια ανταλλαγή μηνυμάτων πραγματοποιείται στο διαδίκτυο ελέγχονται τα μηνύματα.
- Λειτουργεί χωρίς την συμβολή κάποιου λειτουργικού συστήματος.
- Και τέλος είναι εύκολο στη χρήση και η πιο διαδεδομένα χρησιμοποιούμενη μέθοδος ασφαλείας, ως αποτέλεσμα να χρησιμοποιείται από τους περισσότερους περιηγητές.

Εν κατακλείδι, είναι σαφές ότι με τη χρήση του TLS πρωτοκόλλου είναι δυνατή η διατήρηση ασφαλείας των δεδομένων του συστήματος και προφυλάσσει τους χρήστες από επιθέσεις ενδιάμεσων χρηστών. Γεγονός που είναι ιδιαίτερα σημαντικό για οικονομικές συναλλαγές ή προσωπικά στοιχεία.

Πέρα των θετικών που αναλύσαμε, το TLS όπως και κάθε πρωτόκολλο έχει κάποια μειονεκτήματα.

Μειονεκτήματα

- Το σημαντικότερο μειονέκτημα είναι ο αυξημένος φόρτος στην CPU, μιας και οι τεχνικές κρυπτογράφησης δημοσίου κλειδιού απαιτούν έντονη χρήση της. Επομένως, όταν χρησιμοποιείται το SSL τότε αυτομάτως δημιουργείται μια καθυστέρηση με αποτέλεσμα την μείωση της απόδοσης του συστήματος. Βέβαια, όταν μιλάμε για μείωση της απόδοσης είναι συνδεδεμένη με τον χρόνο που συνδέονται ή διαρκούν κάποιες συνδέσεις.
- Δεν είναι δυνατόν να προσδιοριστεί η ταυτότητα του αποστολέα, αλλά μόνο η διαδρομή/ μονοπάτι προς τον αποστολέα.
- Κρυπτογραφεί τα μηνύματα μόνο κατά την διαδικασία μεταγωγής τους και όχι σε όλη την διαδικασία ανάμεσα στον αποστολέα – παραλήπτη.
- Υπάρχει πιθανότητα το TLS να μην αναγνωρίσει τυχόν firewall και να θεωρήσει ότι είναι κάποιος κακόβουλος τρίτος και υπόκειται σε επίθεση Man in the Middle.
- Τέλος, μπορεί να υπάρξει καθυστέρηση λόγω συντήρησης. Επειδή το περιβάλλον του TLS είναι περίπλοκο απαιτεί συχνά από τον διαχειριστή συστήματος εργασίες συντήρησης.

6. Ασφάλεια στο επίπεδο εφαρμογής

6.1 DNS Spoofing

Όταν το software σε έναν host χρειάζεται να μετατρέψει ένα domainname σε διεύθυνση, στέλνει ένα ερώτημα εύρεσης διεύθυνσης-address lookup query, σε έναν DNS server. Όταν ένας client συνδεθεί με έναν host που διαθέτει ένα domain name, ο client πρέπει να μετατρέψει το όνομα σε IP διεύθυνση. Ο client εμπιστεύεται το DNS σύστημα ώστε να επιστρέψει τη σωστή διεύθυνση, αλλά και το σύστημα δρομολόγησης ώστε να παραδώσει τα δεδομένα στο προορισμό τους. Το ίδιο θα συμβεί και όταν ο host χρειαστεί να μετατρέψει μια IP διεύθυνση σε domain name, τότε απευθύνει ένα ερώτημα εύρεσης ονόματος – reverse lookup query.

Ένας DNS server είναι πιθανό να έχει παραβιαστεί από κάποιον cracker. Όταν πραγματοποιηθεί ερώτημα σύνδεσης με τον server, ο server στέλνει αίτηση στον DNS Server ώστε να μάθει ποιο domain name αντιστοιχεί στην αίτηση που ήρθε από μια δεδομένη IP address. Ο DNS server εάν είναι παραβιασμένος μπορεί να επιστρέψει το όνομα ενός έμπιστου domain και κατ' επέκταση έμπιστου host.

Προς αποφυγή για να ελαττωθεί ο κίνδυνος, μερικοί servers θα πρέπει να ρυθμιστούν ώστε να κάνουν έναν έξτρα έλεγχο για κάποιον client. Δηλαδή αφού εντοπίσουν τον host, ο server στέλνει αίτηση εύρεσης της IP διεύθυνσης που αντιστοιχεί στο host όνομα. Εάν οι δύο διευθύνσεις η αρχική και η τελική δεν συμφωνούν η αίτηση σύνδεσης με τον server απορρίπτεται. Οι πίνακες που περιέχουν τα ονόματα hosts και οι πίνακες που περιέχουν IP διευθύνσεις για συγκεκριμένα ονόματα, βρίσκονται συνήθως σε διαφορετικά αρχεία και σε διαφορετικούς name servers. Με αποτέλεσμα να είναι δυσκολότερο για έναν εισβολέα να χρειαστεί να ελέγξει και τους δύο DNS Servers.

6.2 Επίθεση Σπασίματος Συνθηματικών – Password Cracking.

Όπως είναι γνωστό ένας καλός τρόπος ασφάλειας είναι η χρήση κάποιου password. Βέβαια όσο περνάει ο καιρός υπάρχουν όλο και περισσότερα προγράμματα για “σπάσιμο” των passwords. Τέτοια προγράμματα συγκρίνουν το αρχείο των passwords ενός συστήματος με ένα λεξικό κρυπτογραφημένων passwords. Αυτή η επίθεση λειτουργεί καλύτερα σε αδύναμους κωδικούς.

6.3 Επίθεση βόμβα e-mail

Αυτή η επίθεση περιλαμβάνει ένα email το οποίο περιλαμβάνει είτε ένα πολύ μεγάλο κείμενο είτε ένα πολύ μεγάλο επισυναπτόμενο αρχείο. Συνήθως τέτοια email στέλνονται σε συμμετέχοντες σε ομάδες νέων ή σeforums, με τους οποίους ο επιτιθέμενος μπορεί να είχε κάποια διαφωνία. Αυτά τα μηνύματα μπορεί να είναι απλά ενοχλητικά γιατί μπορεί να φορτώνει αρκετή ώρα χωρίς να μας δείξει τίποτα. Ωστόσο μπορεί να υπάρξουν και σοβαρότερες επιπτώσεις όπως τέτοια μηνύματα να σταλούν κατά συρροή σε έναν mail server με στόχο να τον απενεργοποιήσουν λόγω υπερβολικού φορτίου.

6.4 WORM – Σκουλήκι

Είναι κακόβουλο λογισμικό το οποίο μεταδίδεται άμεσα μέσω κάποιας δικτυακής υποδομής όπως τα τοπικά δίκτυα είτε μέσω ηλεκτρονικού ταχυδρομείου. Η ιδιότητα που το χαρακτηρίζει είναι ότι πολλαπλασιάζεται αυτόματα στο εκάστοτε σύστημα που βρίσκεται. Αυτό, του δίνει τη δυνατότητα να αποστέλλει κωδικούς ή προσωπικά δεδομένα ώστε αυτός που θα κάνει την επίθεση να έχει πρόσβαση στη σύνδεση δικτύου. Επίσης όταν το δίκτυο δέχεται τέτοιου είδους επίθεση επιβαρύνεται λόγω του ότι φορτώνεται με άχρηστη δραστηριότητα.

6.5 Δούρειος Ίππος

Ο Δούρειος Ίππος είναι ένα κακόβουλο πρόγραμμα που ξεγελάει το χρήστη ότι εκτελεί μια χρήσιμη λειτουργία ενώ στη πραγματικότητα εγκαθιστά κρυφά στον υπολογιστή του άλλα κακόβουλα προγράμματα. Κρύβουν μέσα τους κακόβουλο κώδικα ο οποίος μπορεί να μολύνει τον υπολογιστή. Εξωτερικά μοιάζουν με προγράμματα τα οποία εκτελούν κάποια έμπιστη και χρήσιμη λειτουργία, όταν όμως εκτελεστεί το πρόγραμμα τότε ενεργοποιείται ο κακόβουλος κώδικας και μολύνεται ο υπολογιστής. Αποτέλεσμα της μόλυνσης αυτής είναι η εγκατάσταση κάποιου προγράμματος που επιτρέπει σε μη εξουσιοδοτημένους χρήστες να έχουν πρόσβαση στον μολυσμένο υπολογιστή χρησιμοποιώντας τον για επιθέσεις σε τρίτους.

6.6 Ιοί

Οι ιοί είναι ένα είδος κακόβουλου κώδικα που θέτει σε κίνδυνο την ασφάλεια του συστήματος και χρησιμοποιούνται για μια ποικιλία διαφορετικών ενεργειών.
Ένας ιός είναι ένα πρόγραμμα το όποιο συμπεριλαμβάνει τον εαυτό του σε αρχεία τα οποία υπάρχουν στον υπολογιστή, αλλιώς ονομάζεται **μόλυνση**. Μετά την εγκατάσταση του ιού στον υπολογιστή, έχει τη δυνατότητα να αντιγράψει τον εαυτό του και σε άλλα αρχεία.

Υπάρχουν 3 κατηγορίες ιών:

- **Εκτελέσιμος ιός,** ο οποίος είναι ένας ιός που προστίθεται σε ένα εκτελέσιμο αρχείο ο οποίο όταν εκτελεστεί θα εκτελεστεί και ο κώδικας του ιού. Με αποτέλεσμα αυτός ο κώδικας να κάνει κάποια κακόβουλη ενέργεια.
- **Ιός δεδομένων,** ο οποίος μολύνει ένα αρχείο που περιέχει δεδομένα αντί για εκτελέσιμο κώδικα. Αυτό συμβαίνει γιατί τα δεδομένα αυτά είναι συνδεδεμένα με κάποιο πρόγραμμα το οποίο χρειάζεται τα δεδομένα για να εκτελέσει τη λειτουργία του.

- **Ιοί οδηγών συσκευών,** αυτή η κατηγορία ιών επηρεάζει τους οδηγούς συσκευών ενός λειτουργικού συστήματος που χρησιμοποιούνται για τον χειρισμό διάφορων στοιχείων του υπολογιστή (πχ ο δίσκος).

6.7 Antivirus.

Τα antivirus είναι προγράμματα τα οποία τρέχουν σε ένα σύστημα και ελέγχουν κάθε διεργασία που εκτελείται για να δουν αν η διεργασία που εκτελείται πρόκειται για μια νόμιμη διεργασία ή μια διεργασία κακόβουλη που έχει χαρακτηρισθεί ως ιός, σκουλήκι ή δούρειος ίππος.

Σήμερα υπάρχουν αρκετά τέτοια προγράμματα τα οποία έχουν διάφορους τρόπους λειτουργίας. Ο πιο συχνός είναι με τη χρήση Signatures. Όσα προγράμματα λειτουργούν με τον τρόπο αυτό ελέγχουν για διεργασίες που εκτελούν συγκεκριμένη ακολουθία ενεργειών και έχει αναγνωριστεί ως παράνομη. Μόλις μια τέτοια ακολουθία εκτελεστεί, τότε αυτομάτως το πρόγραμμα που την εκτέλεσε θεωρείται ιός και η εκτέλεση του παρεμποδίζεται από το antivirus. Η χρήση antivirusδεν πρέπει ποτέ να λείπει από κανένα σύστημα μιας και είναι θεμελιώδης λίθος του πλάνου ασφαλείας.

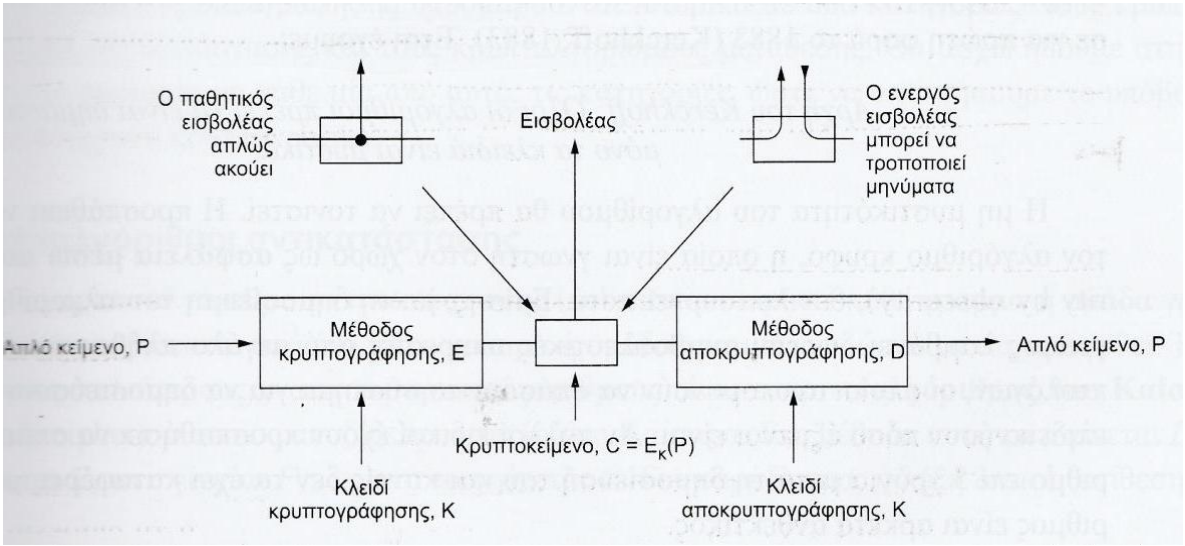
Παρόλο που τα antivirus προγράμματα αυξάνουν σε μεγάλο βαθμό την ασφάλεια των συστημάτων, έχουν και αρκετά **μειονεκτήματα**. Το βασικότερο είναι η εξάρτηση από τον κατασκευαστή. Αυτό το αναφέρουμε γιατί, ιοί και κακόβουλα προγράμματα εξελίσσονται συνεχώς. Έτσι πρέπει να βγαίνουν διαρκώς signaturesγια αυτά ώστε να είναι δυνατόν για τα antivirus να τα αναγνωρίσουν. Το πιο κρίσιμο σημείο είναι το πόσο γρήγορα θα προσφέρει την ενημέρωση των signatures αυτών η εταιρεία κατασκευής. Όσο πιο γρήγορα ανακοινωθούν τα νέα signatures, τόσο πιο σύντομα θα προστατευθεί ο υπολογιστής. Ο χρόνος που θα μεσολαβήσει μέχρι αυτή την ενημέρωση είναι πολύ κρίσιμος. Επίσης, είναι σημαντικός και ο τρόπος με τον οποίο γίνεται ο έλεγχος κάθε διεργασίας. Κάθε antivirus πρόγραμμα πιθανόν να έχει διαφορετικά αποτελέσματα στην ανίχνευση μιας απειλής. Δηλαδή, ανάλογα με τον μηχανισμό ελέγχου θα ανιχνεύουν λιγότερες ή περισσότερες απειλές από κάποια άλλα.

Κάνοντας λοιπόν στον εαυτό μας την ερώτηση «**Ποιο είναι το καλύτερο antivirus πρόγραμμα;**», τότε δεν θα μπορούσαμε να

δώσουμε απάντηση μιας και δεν υπάρχει. Έχει παρατηρηθεί πως το βασικότερο πρόβλημα των antivirus προγραμμάτων δεν έχει να κάνει με τον τρόπο λειτουργίας του αλλά με τους χρήστες. Αυτό συμβαίνει γιατί όσο καλό και αν είναι το antivirus πρόγραμμα που χρησιμοποιούμε και όσο συχνά κι αν βγουν ενημερώσεις, αν ο χρήστης δεν ενημερώσει το πρόγραμμά του τότε αφήνει τον υπολογιστή του εκτεθειμένο σε κίνδυνο. Επομένως, η προστασία που παρέχεται είναι υποδεέστερη από αυτήν που έχει δυνατότητες να προσφέρει το πρόγραμμα.

6.8 Κρυπτογραφία

Η κρυπτογραφία από παλιά διακρίνεται σε δυο κατηγορίες. Στους **κρυπταλγόριθμους** και στους **κώδικες**. Ένας **κρυπταλγόριθμος** είναι ο μετασχηματισμός χαρακτήρα προς χαρακτήρα ή αλλιώς bit προς bit. Από την άλλη ο **κώδικας** αντικαθιστά μια λέξη με μια άλλη ή ένα σύμβολο. Βέβαια η χρήση κώδικα δεν χρησιμοποιείται πια. Κάνοντας μια αναδρομή στην ιστορία ο στρατός ήταν αυτός που έπαιξε τον πιο σημαντικό ρόλο στην εξέλιξη της κρυπτογραφίας. Πρώτα ξεκίνησε την κρυπτογραφία μέσω στρατιωτικών υπαλλήλων και μετά κατά την έλευση των υπολογιστών έγιναν οι απαιτούμενοι μετασχηματισμοί.



Εικόνα 8 Αρχιτεκτονική της Κρυπτογραφίας.

Τα μηνύματα προς κρυπτογράφηση αναφέρονται ως **απλό κείμενο.** Μετασχηματίζονται από μια συνάρτηση που χρησιμοποιεί ως

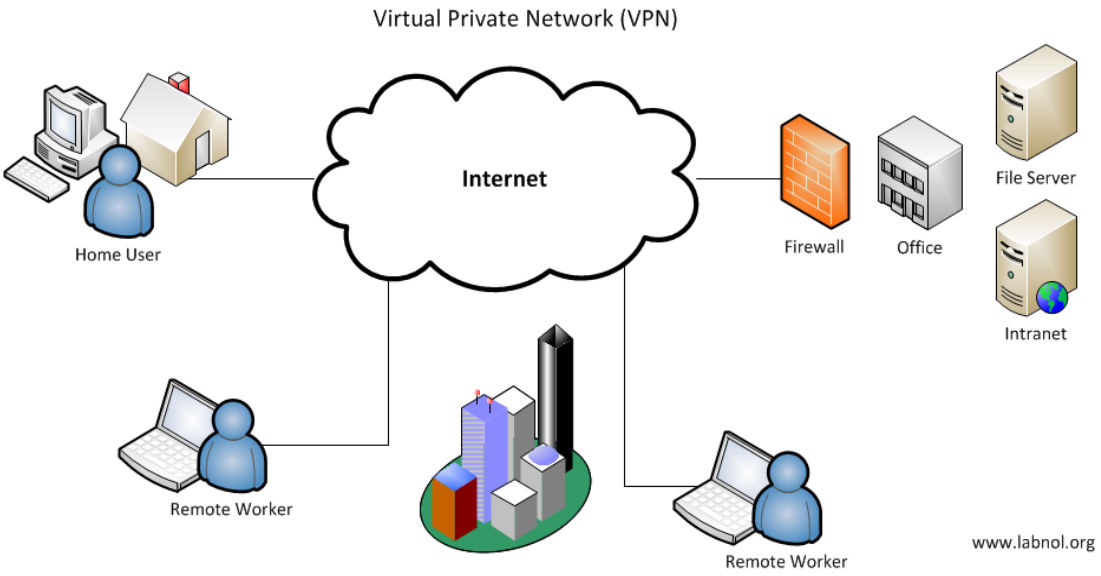
παράμετρο ένα **κλειδί key**. Η έξοδος της διαδικασίας κρυπτογράφησης ονομάζεται **κρυπτοκείμενο** και μεταδίδεται συχνά μέσω ραδιοκυμάτων. Υποστηρίζετε πως ο εισβολέας ακούει και αποτυπώνει πιστά το πλήρες κρυπτοκείμενο, όμως δεν γνωρίζει ποιο είναι το κλειδί αποκρυπτογράφησης αντιθέτως με τον επιθυμητό παραλήπτη. Ένας εισβολέας χωρίζεται σε δυο κατηγορίες, τον παθητικό και τον ενεργητικό. **Παθητικός** είναι ο εισβολέας που μόνο ακούει το κανάλι επικοινωνίας ενώ **ο ενεργητικός** καταγράφει τα μηνύματα και τα αναπαράγει αργότερα είτε εισάγει τα δικά του είτε τροποποιεί το αρχικό μήνυμα πριν παραδοθεί στον παραλήπτη. Η τεχνική σπασίματος των κρυπταλγορίθμων ονομάζεται **κρυπτανάλυση** (cryptanalysis) ενώ η τεχνική της επινόησής τους είναι γνωστή ως **κρυπτολογία**. Για την καλύτερη κατανόηση το απλό κείμενο (P), το κρυπτοκείμενο (C) και τα κλειδιά (K) συσχετίζονται με μια συνάρτηση. Χρησιμοποιούμε τον τύπο $\mathbf{C= E_k(P)}$ [*1] για να δείξουμε ότι το **κρυπτοκείμενο** C δίνεται από την κρυπτογράφηση του απλού κειμένου P με χρήση του κλειδιού K. Παρομοίως η **αποκρυπτογράφηση** του C για να λάβουμε ξανά το απλό κείμενο παριστάνεται με τον τύπο $\mathbf{P=D_k(C)}$ [*2] **.** Άρα μέσω τύπου **1** και **2** ισχύει: $\mathbf{D_k(E_k(P)) = P}$

Με την παράσταση αυτή συμπεράνουμε πως οι E και D είναι απλώς μαθηματικές συναρτήσεις και το μόνο δύσκολο σημείο είναι ότι είναι συναρτήσεις παραμέτρων. Η μια παράμετρος είναι το κλειδί που γράφεται ως δείκτης για να διακρίνεται και από την άλλη παράμετρο που είναι το μήνυμα.

Η Κρυπτογραφία βέβαια δεν είναι μόνο μια κατηγορία που μπορούμε να αναλύσουμε, αλλά χωρίζετε σε πολλούς κλάδους. Υπάρχουν οι **κρυπταλγόριθμοι αντικατάστασης** όπου κάθε γράμμα αντικαθίστανται με κάποιο άλλο, οι **κρυπταλγόριθμοι μετάθεσης** που αναδιατάσσουν τα γράμματα, **το σημειωματάριο μιας χρήσης** που μετατρέπεται το απλό κείμενο σε μια ακολουθία bit και επίσης διαλέγουμε μια τυχαία ακολουθία bit και τέλος υπολογίζουμε την αποκλειστική διάζευξη (or, xor) των 2 ακολουθιών. Τ**ο DES – Πρότυπο Κρυπτογράφησης Δεδομένων** που χρησιμοποιεί διάφορα στάδια κρυπτογράφησης. Το **AES είναι ένα Προηγμένο Πρότυπο Κρυπτογράφησης** δηλαδή μια εξέλιξη του DES.

6.9 Εικονικά Ιδιωτικά Δίκτυα

Παλαιότερα, πριν ακόμα εδραιωθούν τα δημόσια δίκτυα δεδομένων τα μεγάλα εργοστάσια και οι εταιρείες μίσθωναν γραμμές της τηλεφωνικής εταιρείας ανάμεσα σε όλα ή σε μερικά ζεύγη των τοποθεσιών τους. **Ιδιωτικό Δίκτυο (private network)** ονομάζεται ένα δίκτυο που είναι κατασκευασμένο από εταιρικούς υπολογιστές και μισθωμένες τηλεφωνικές γραμμές. Τα ιδιωτικά δίκτυα είναι αρκετά ασφαλή και δουλεύουν άριστα, με τον μοναδικό όρο οι γραμμές που λειτουργούν στο δίκτυο και χρησιμοποιούνται να είναι οι μισθωμένες. Έτσι, δεν μπορεί να διαρρεύσει καμία πληροφορία και οι εισβολείς θα πρέπει να παγιδεύσουν τις γραμμές για να μπουν στο δίκτυο γεγονός που είναι αρκετά δύσκολο. Βέβαια παρόλη την ασφάλεια και αξιοπιστία που παρέχει έχει και **μειονεκτήματα.** Πρώτο και κύριο είναι το μεγάλο κόστος υλοποίησης, μιας και η μίσθωση μιας γραμμής T1 ανάμεσα σε δύο σημεία κοστίζει μεγάλο χρηματικό ποσό ενώ επιπλέον μια γραμμή T3 κοστίζει ακόμα περισσότερο. Όταν με τον καιρό έκαναν την εμφάνισή τους τα δημόσια δίκτυα και η χρήση του Διαδικτύου πολλές επιχείρησης θέλησαν να μεταφερθούν σε αυτό , χωρίς όμως να επιθυμούν να αφήσουν την ασφάλεια του ιδιωτικού δικτύου. Η ζήτηση αυτή οδήγησε στην επινόηση των **Εικονικών Δικτύων – VPN**, τα οποία είναι δίκτυα επικάλυψης πάνω από τα δημόσια δίκτυα αλλά με την πλειοψηφία των ιδιοτήτων που έχουν τα ιδιωτικά δίκτυα. **Εικονικά** ονομάζονται επειδή πρόκειται απλώς για μια ψευδαίσθηση. Μια λύση είναι η κατασκευή VPN απευθείας μέσω Διαδικτύου. Η υλοποίηση αυτή επιτυγχάνεται με το να εξοπλίσουμε κάθε γραφείο με firewalls και να δημιουργηθούν σήραγγες μέσω Διαδικτύου σε όλα τα ζεύγη των γραφείων. Ένα μεγάλο πλεονέκτημα είναι πως οι σήραγγες μπορούν να εγκαθίστανται κατόπιν αιτήματος έτσι ώστε να περιλαμβάνουν για παράδειγμα τον υπολογιστή κάποιου που ταξιδεύει ή απλώς δουλεύει από το σπίτι του μέσω σύνδεσης με το internet.



Εικόνα 9 Εικονικό Ιδιωτικό Δίκτυο.

Όταν ενεργοποιείται το σύστημα, κάθε ζεύγος firewalls – Αντιπυρικών ζωνών θα πρέπει να αρχίσει να διαπραγματεύεται το ζεύγος των συσχετίσεων ασφαλείας (SA). Με τον όρο **συσχετίσεων ασφαλείας (SA)** εννοούμε τις υπηρεσίες, τις καταστάσεις λειτουργίας, τους αλγόριθμους και τα κλειδιά. Όταν γίνεται χρήση του IPSec για τις σήραγγες τότε η κίνηση ανάμεσα σε δυο ζεύγη γραφείων γίνεται σε μια μόνο κρυπτογραφημένη και πιστοποιημένη SA, ώστε να μπορεί να παρέχεται έλεγχος ακεραιότητας και μυστικότητα. Αφού εγκατασταθούν οι SA μπορεί να ξεκινήσει η κίνηση της κυκλοφορίας. Ένα πακέτο που βρίσκεται σε κίνηση κατά μήκος μιας σήραγγας VPN μπορεί να θεωρηθεί ως ένα απλό πακέτο από έναν δρομολογητή συνδεδεμένο στο Διαδίκτυο.

Τέλος, ένα κυρίαρχο πλεονέκτημα των VPN είναι ότι είναι διαφανή για όλο το εύρος του λογισμικού. Τα firewalls εγκαθιδρύουν και διαχειρίζονται τις SA. Για την διευθέτηση των αντιπυρικών ζωνών υπεύθυνος και ενήμερος είναι μόνο ο διαχειριστής του συστήματος.

6.10 Ασφάλεια Ηλεκτρονικού Ταχυδρομείου

Αν και το email είναι από τις πιο παλιές υπηρεσίες, δεν εγγυάται ιδιαίτερη ασφάλεια αφού η υποκλοπή μπορεί να γίνει εύκολα. Το ηλεκτρονικό ταχυδρομείο σταδιακά αντικαθιστά το συμβατικό ταχυδρομείο. Γεγονός που σημαίνει πως τα ηλεκτρονικά μηνύματα

είναι εύκολο να υποκλαπούν, και όλη αυτή η διαδικασία να μην πέσει στην αντίληψη κανενός μιας και ίσως δεν καταλάβουμε αν το μήνυμα που λάβαμε ήταν το αρχικό που στάλθηκε.

Το ηλεκτρονικό ταχυδρομείο χρησιμοποιεί το Πρωτόκολλο Μεταφοράς Απλού Ταχυδρομείου – SMTP/Simple Mail Transfer Protocol. **Το SMTP**είναι υπεύθυνο για:

- Την μεταφορά των μηνυμάτων από τον χρήστη σε έναν server ηλεκτρονικού ταχυδρομείου.
- Την προώθηση του μηνύματος από έναν server ηλεκτρονικού ταχυδρομείου σε έναν άλλον.

Το κυρίαρχο πρόβλημα ασφαλείας στο γεγονός ότι τα SMTP πακέτα είναι **Ευαίσθητα σε επιθέσεις sniffing** (υποκλοπή των πακέτων που διέρχονται από έναν κόμβο) και – **Μη κρυπτογραφημένα**.

Ο επιτιθέμενος είναι δυνατόν:

- Να υποκλέψει πληροφορίες σχετικά με το περιεχόμενο των μηνυμάτων που στάλθηκαν ή έλαβε ο χρήστης.
- Όπως επίσης να πάρει τον κωδικό πρόσβασης που χρησιμοποιήθηκε.

Πολλοί θα ήθελαν να στέλνουν ηλεκτρονικό ταχυδρομείο το οποίο θα μπορεί να διαβαστεί μόνο από τον επιθυμητό παραλήπτη και από κανέναν άλλο. Η επιθυμία αυτή οδήγησε πολλά άτομα να εφαρμόσουν στη χρήση του ηλεκτρονικού ταχυδρομείου τις κρυπτογραφικές αρχές που αναφέραμε πιο πάνω με στόχο το ασφαλή ηλεκτρονικό ταχυδρομείο. Για την επίτευξη αυτού του στόχου χρησιμοποιούνται δυο ευρέως διαδεδομένα συστήματα, **το PGP και το S/MIME**.

6.11 PGP – Pretty Good Privacy

Το PGP είναι ένα λογισμικό κρυπτογράφησης υψηλής ασφάλειας. Έχει το πλεονέκτημα ότι είναι συμβατό με διάφορα λειτουργικά συστήματα όπως τα Linux,Unix, MSDos και άλλα. Υποστηρίζει την ανταλλαγή μηνυμάτων εξασφαλίζοντας την προστασία απορρήτου και την πιστοποίηση ταυτότητας σε συνδυασμό με την ευκολία λειτουργίας. **Προστασία απορρήτου** σημαίνει ότι πρέπει να ελεγχθεί πως ο μόνος που θα έχει πρόσβαση στο μήνυμα είναι αυτός όπου και προορίζεται το μήνυμα. Αντίστοιχα, **πιστοποίηση ταυτότητας**

σημαίνει να γίνεται έλεγχος πως τα μηνύματα προέρχονται όντως από αυτόν που υποστηρίζει πως τα έστειλε.

Η όλη **ευκολία χρήσης** που προ αναφέραμε βασίζεται στο γεγονός ότι η διασφάλιση του απορρήτου και η πιστοποίηση ταυτότητας επιτυγχάνονται χωρίς την δυσκολία διαχείρισης κλειδιών. Μιας και είναι βασισμένο σε μια τεχνολογία που ονομάζεται **Κρυπτογράφηση Δημοσιών Κλειδιών** (public key). Εκτελεί τις λειτουργίες των δημοσίων κλειδιών γρηγορότερα σε σχέση με άλλα προγράμματα.

6.12 S/MIME – Secure Mime

Το πρωτόκολλο S/MIME είναι μια τελευταία εξειδίκευση του πρωτοκόλλου MIME και εξελίχθηκε για την ασφαλή ανταλλαγή ηλεκτρονικών μηνυμάτων. Έχει ως στόχο να καταπολεμήσει την υποκλοπή και να είναι φιλικό στη χρήση. Προσκολλάται εύκολα στο πρωτόκολλο MIMEμέσω κρυπτογραφικών τυποποιήσεων που είναι το Public Key Crypto graphy Standars – PKCS. Έχει γίνει κοινά αποδεκτό λόγω των εννοιών που πρεσβεύει όπως η ακεραιότητα των δεδομένων, η αυθεντικότητα και η διαφύλαξη του απορρήτου.

Το S/MIME χρησιμοποιείται από διάφορα προγράμματα ηλεκτρονικού ταχυδρομείου για την χρήση κρυπτογραφικών υπηρεσιών στα αποστέλλοντα μηνύματα. Παρέχει την δυνατότητα σε διάφορες οντότητες να χρησιμοποιούν προγράμματα κατάλληλα ώστε ένα μήνυμα που κρυπτογραφήθηκε με ένα συγκεκριμένο πρόγραμμα να μπορεί να αποκρυπτογραφηθεί με ένα άλλο. Με τις νέες εκδόσεις του συγκεκριμένου πρωτόκολλου που αναπτύσσονται υπάρχει η δυνατότητα να δρα σε συνδυασμό με άλλα πρωτόκολλα όπως το HTTP,FTP,SET για καλύτερα αποτελέσματα.

6.13 S/HTTP (Secure Hyper Text Transfer Protocol)

Το World Wide Web (WWW) είναι ένα σύστημα πολυμέσων ευρέως διαδεδομένο. Το βασικό πρωτόκολλο που χρησιμοποιεί είναι HTTP. Πολλές δικτυακές εφαρμογές βασίζονται στο πρότυπο client/server του WWW, οι οποίες απαιτούν την πιστοποίηση ταυτότητας των δυο επικοινωνούντων υπολογιστών και την δυνατότητα ανταλλαγής

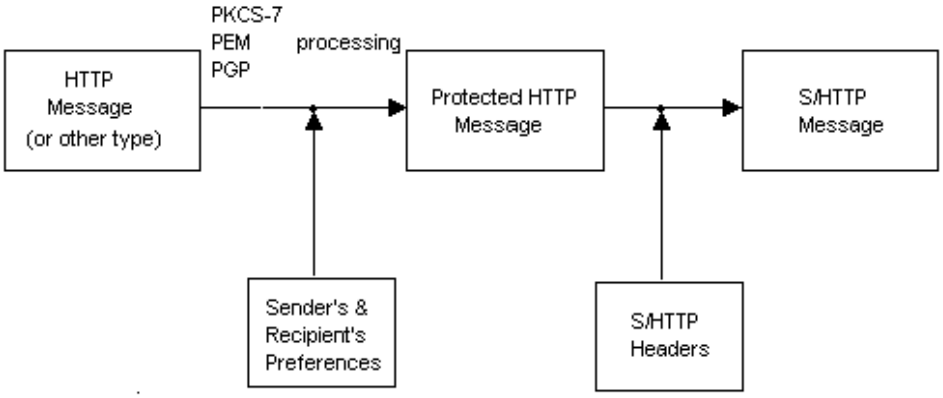
ιδιαίτερων πληροφοριών. Βέβαια ένα μειονέκτημα είναι πως οι HTTP εφαρμογές έχουν ελάχιστη υποστήριξη για κρυπτογραφικούς μηχανισμούς, παρόλο που είναι απαραίτητοι για ασφαλής μεταφορές πληροφορίας. Σκοπός της πρωταρχικής σχεδίασης του ήταν ένα ευέλικτο πρόγραμμα που αποτελείται από αρκετούς μηχανισμούς και αλγόριθμους και την δυνατότητα εξέλιξη τους.

Το πρωτόκολλο S/HTTP έχει κάποια βασικά χαρακτηριστικά:

- Υποστηρίζει **πληθώρα μηχανισμών ασφαλείας** μεταξύ clients καιservers. Τους παρέχει **συμμετρικές δυνατότητες** δηλαδή οι πληροφορίες και οι απαιτήσεις είτε του clientείτε του server αντιμετωπίζονται με ακριβώς ίδιο τρόπο.
- Δεν απαιτεί ο clientαπό τη μεριά του **πιστοποιητικά δημοσίων κλειδιών** μιας και υποστηρίζει και τη χρήση συμμετρικών κλειδιών. Αυτό θα ήταν χρήσιμο σε περίπτωση που γινόταν μια βιαστική ιδιωτική συναλλαγή χωρίς να έχει προηγηθεί η ανταλλαγή έγκυρου ζεύγους κλειδιών.
- Το S/HTTPσε αντίθεση με το HTTP υποστηρίζει από **άκρο εις άκρο ασφάλεια συναλλαγών**, γεγονός που σημαίνει ότι καμία πληροφορία δεν μπορεί να μεταδοθεί στο δίκτυο απροστάτευτη.
- Δίνει την δυνατότητα να **επιλεχθεί το είδος της παρεχόμενης προστασίας** όπως κρυπτογράφηση, ψηφιακές υπογραφές, κτλ.

Τρόπος λειτουργίας

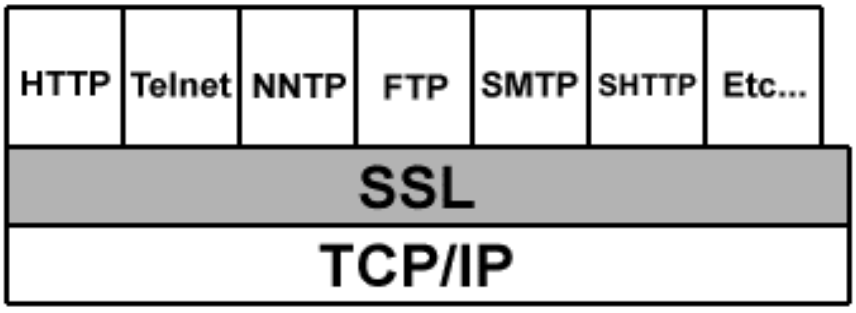
Βήμα1: Ξεκινά η προετοιμασία του μηνύματος. Η δημιουργία ενός μηνύματος αποτελείται από 3ης παραμέτρους. **Πρώτα** το μήνυμα που θα προστατευτεί μπορεί να είναι ένα httpμήνυμα ή κάποιο άλλο αντικείμενο. **Δεύτερον**, πρέπει να είναι καθορισμένες οι προτιμήσεις του παραλήπτη. Και **τέλος** να είναι καθορισμένες και γνώστες οι κρυπτογραφικές προτιμήσεις του αποστολέα. Οι προτιμήσεις είτε θα έχουν καθοριστεί σε προηγούμενη επικοινωνία είτε βασίζονται σε προ ρυθμίσεις. Ο αποστολέας λαμβάνει υπόψη του τις προτιμήσεις αποστολέα και παραλήπτη και αποφασίζει για τους μηχανισμούς που θα χρησιμοποιηθούν καθώς και για τα κλειδιά. Στο HTTPμήνυμα προστίθενταιS/HHTPεπικεφαλίδες και παράγεται το τελικό μήνυμα.



Εικόνα 10 Μετατροπή ενός HTTP μηνύματος σε SHTTP.

Βήμα 2: Στη τελική διαδικασία ξεκινά η παραλαβή του μηνύματος. Για την επεξεργασία του μηνύματος που παραλήφθηκε υπάρχουν 3ης παράμετροι. **Πρώτο** και κύριο το S/HTTP μήνυμα. **Μετά ακολουθούν** οι κρυπτογραφικές προτιμήσεις του παραλήπτη που προαναφέραμε στο βήμα1. **Έπειτα**, οι κρυπτογραφικές προτιμήσεις του αποστολέα που θα τις είχε δηλώσει πρωτύτερα ή θα ήταν οι τρέχων. Για την κατανόηση του μηνύματος ο παραλήπτης διαβάζει τις S/HTTP επικεφαλίδες και με την βοήθεια των προσυμφωνημένων κλειδιών προσπαθεί να κατανοήσει τους κρυπτογραφικούς μετασχηματισμούς που εφαρμόστηκαν. Όταν προβεί σε όλες αυτές τις διαδικασίες τότε έχουμε σαν αποτέλεσμα πια ένα HTTP μήνυμα.

6.14 Πρωτόκολλο Ασφαλείας SSL – Secure Socket Layer



Εικόνα 11 Θέση πρωτοκόλλου SSL.

Η ανάπτυξη του πρωτοκόλλου SSL πρωτοεμφανίστηκε το 1994, με στόχο την ασφαλή επικοινωνία ευαίσθητων πληροφοριών, όπως στοιχεία τραπεζών ή προσωπικές πληροφορίες. Κατά τη διάρκεια του χρόνου μετασχηματίστηκε σε ένα πιο εξελιγμένο πρωτόκολλο το SSLversion 3.0.Το SSL έχει υλοποιηθεί για να παρέχει ασφαλή και έμπιστη επικοινωνία μεταξύ συστημάτων client-server. Η εξασφάλιση της ασφάλειας παρέχεται με ένα συνδυασμό μεθόδων. Πρώτα από όλα με κρυπτογράφηση όλων των μηνυμάτων στο SSL Record Protocol. Επίσης υποστηρίζεται πληθώρα κρυπτογραφικών μηχανισμών και ψηφιακών υπογραφών για την κάλυψη οποιονδήποτε αναγκών. Μια σημαντική επίσης μέθοδος είναι η πιστοποίηση ταυτότητας αναγκαστικά του serverκαι προαιρετικά του client μέσω πιστοποιητικών από έγκυρες αρχές έκδοσης. Τέλος, υποστηρίζεται η ακεραιότητα των δεδομένων μέσω της τεχνικής MACs / Message Authentication Codes. Που σημαίνει πως κανείς δεν θα μπορεί να μεταβάλλει οποιαδήποτε πληροφορία χωρίς να γίνει αντιληπτό. Παρόλη την ευκολία χρήσης και της μεγάλης αποδοτικότητας του SSL, όταν εμφανίστηκε η version 3, κάλυψε αρκετές αδυναμίες του SSL2. Ήταν σχεδιαστικά καλύτερη και κάλυπτε μεγαλύτερο φάσμα εφαρμογών. Βέβαια όπως και να ΄χει το SSL προτιμάτε καλύτερα και βρίσκεται στην κορυφή οποιουδήποτε πρωτοκόλλου μεταφοράς μιας και είναι ανεξάρτητο από την ύπαρξη TCP/IP και υποστηρίζεται από πρωτόκολλα όπως το FTP, HTTP και για σύνδεση με απομακρυσμένους υπολογιστές (Telnet).

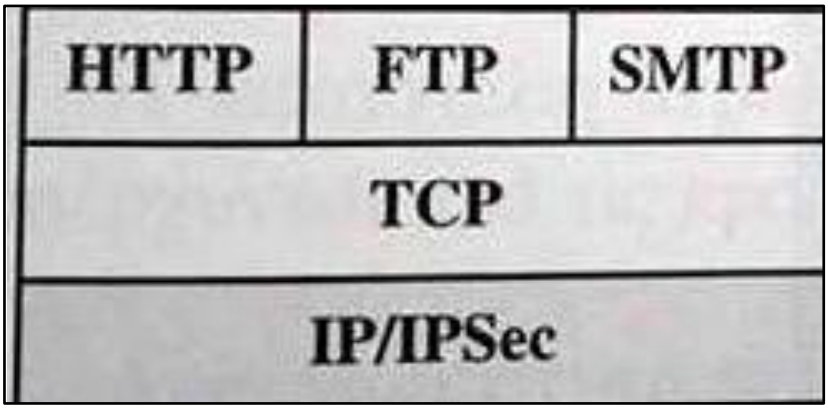
6.15 Πρωτόκολλο PCT

Το πρωτόκολλο αυτό δημιουργήθηκε από την Microsoftμε σκοπό την αποφυγή παρεμβολής τρίτων σε συνδέσεις client/server. Το PCT λειτουργεί ως εξής, είτε ο server είτε ο client αυθεντικοποιείται, ενώ

παράλληλα ο ένας έχει το δικαίωμα να ζητήσει την αυθεντικοποίηση του άλλου. Μπορούμε να θεωρήσουμε πως το PCT στη λειτουργία του είναι παρόμοιο με το SSl. Πάνω από αυτό μπορεί να βρίσκεται οποιοδήποτε πρωτόκολλο υψηλού επιπέδου. Επίσης είναι ανεξάρτητο από το εκάστοτε πρωτόκολλο εφαρμογής που θα χρησιμοποιείται.

Τρόπος λειτουργίας:

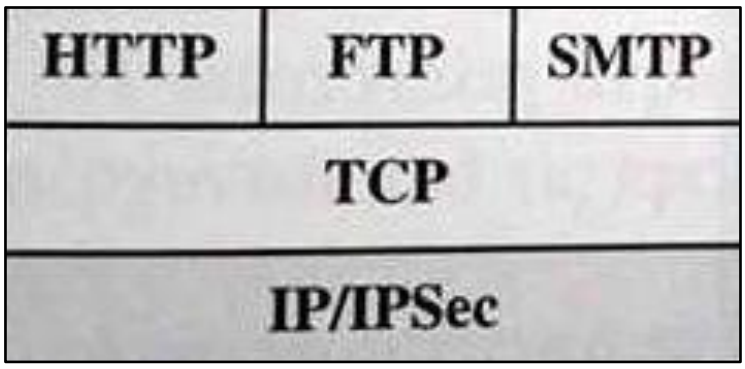
Κάθε δεδομένο μεταδίδεται ως εγγραφή μεταβλητού μήκους, όπου η καθεμία από αυτές έχει μια επικεφαλίδα. Οι εγγραφές αυτές χρησιμοποιούνται για να μεταφέρουν τα μηνύματα του PCTπρωτοκόλλου, όπως για παράδειγμα μηνύματα λαθών ή μηνύματα διαχείρισης κλειδιών κ.α. Επιπλέον μπορεί να μεταφέρει και μηνύματα της εφαρμογής. Οι ανταλλαγές εγγραφών μεταξύ αποστολέα – παραλήπτη ομαδοποιούνται σε **συνδέσεις** οι οποίες ομαδοποιούνται σε **συνόδους** (sessions). Το πρώτο βήμα για να επιτευχθεί μια σύνδεση είναι το **handshake−χειραψία**, στην ουσία ανταλλάσσονται μια ακολουθία από handshakeμηνύματα τα οποία συνεννοούνται για ένα κλειδί επικοινωνίας για την σύνδεση τους. Επιπλέον διαπραγματεύονται και τις κατάλληλες αυθεντικοποιήσεις πιστοποιημένων μη συμμετρικών κλειδιών. Στο τελικό στάδιο και μόλις τελειώσει η μετάδοση των δεδομένων που προέρχονται από το πρωτόκολλο εφαρμογής, όλα τα δεδομένα κρυπτογραφούνται με την χρήση κλειδιών που χρησιμοποιήθηκαν στο handshake που προαναφέραμε. Στη κρυπτογράφηση των δεδομένων κρυπτογραφούνται ακόμα και τα μηνύματα λάθους ή διαχείρισης κλειδιών που τυχόν υπάρχουν. Ακολουθεί η διαδικασία της αυθεντικοποίησης και το PCT πιστοποιεί την ακεραιότητα των μηνυμάτων με την χρήση MAC. Τέλος να αναφέρουμε πως το πρωτόκολλο που θεωρεί έμπιστο και χρησιμοποιεί το PCTγια την μετάδοση των εγγραφών και κατά την φάση του handshakeείναι το TCP.



Εικόνα 12 Επίπεδο Δικτύου

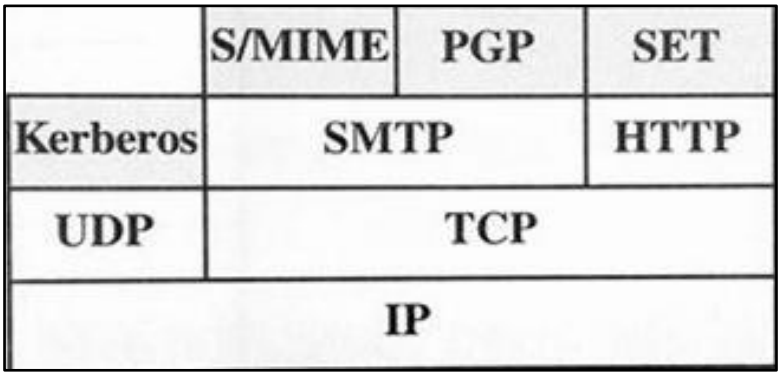
Για την ασφάλεια ιστού όπως και είδαμε υπάρχει ένα μεγάλο πλήθος πιθανών προσεγγίσεων. Πολλές από αυτές μπορεί να είναι παρόμοιες ως προς τους μηχανισμούς που χρησιμοποιούν και τις υπηρεσίες που παρέχουν, διαφέρουν όμως ως προς την εμβέλεια εφαρμογής τους και ως προς την θέση μέσα στη στοίβα πρωτοκόλλων TCP/IP.

Όπως έχουμε προαναφέρει, η χρήση του πρωτοκόλλου IP Security παρέχει αρκετή ασφάλεια. Τα πλεονεκτήματα του είναι ότι παρέχει γενικές λύσεις, διαφάνεια ως προς τους χρήστες και τις εφαρμογές και τέλος δίνει την δυνατότητα φιλτραρίσματος δηλαδή να γίνετε επεξεργασία IP sec μόνο για επιλεγμένες πληροφορίες.



Εικόνα 13Επίπεδο Μεταφοράς.

Εφαρμογή ασφαλείας πάνω από το επίπεδο TCP μπορούν να παρέχουν τα πρωτόκολλα SSL (Secure Socket Layer - Ασφαλές επίπεδο υποδοχών) και το TLS (Transport Layer Security – Ασφάλεια επιπέδου μεταφοράς). Υπάρχουν δυο τρόποι ως προς την υλοποίηση. Πρώτον, για ποιο γενικά το SSL ή το TLS αντίστοιχα, μπορεί να παρέχεται ως κομμάτι της ομάδας πρωτόκολλων της εκάστοτε ομάδας πρωτοκόλλων με αποτέλεσμα να είναι διαφανές για τις εφαρμογές. Αλλιώς, μπορεί να είναι ενσωματωμένο σε πακέτα όπως για παράδειγμα ο φυλλομετρητής Microsoft Internet Explorer που είναι εξοπλισμένος με το SSL όπως και διάφοροι άλλοι διακομιστές ιστού.



Εικόνα 14 Επίπεδο Εφαρμογής

Σε κάθε τέτοια εφαρμογή είναι ενσωματωμένες οι υπηρεσίες ασφαλείας. Στην πιο πάνω εικόνα φαίνονται διάφορα παραδείγματα πρωτοκόλλων αυτής της αρχιτεκτονικής. Το θετικό αυτής της προσέγγισης είναι ότι κάθε υπηρεσία είναι προσαρμοσμένη στις συγκεκριμένες ανάγκες τις εκάστοτε εφαρμογής. Το πιο διαδεδομένο πρωτόκολλο αυτής της αρχιτεκτονικής είναι το πρωτόκολλο SET, για ασφαλής ηλεκτρονικές συναλλαγές.

7. Συμπερασματική κατανόηση ασφαλείας του μοντέλου OSI.

7.1 Φυσικό επίπεδο – Physical layer.

Το φυσικό επίπεδο είναι υπεύθυνο για την επικοινωνία μεταξύ τερματικών σταθμών. Ασχολείται με την κωδικοποίηση και την μετάδοση δεδομένων. Παρόλη την σπουδαιότητα του είναι αρκετά ευάλωτο σε επιθέσεις.

Για την διατήρηση της ασφάλειας τα δεδομένα θα πρέπει να βρίσκονται πίσω από «ισχυρές κλειδαριές» ώστε να παρακολουθείται (με κωδικούς PIN, με καταγραφή βίντεο κτλ), να ελέγχεται και να καταγράφεται η πρόσβαση.

Παραδείγματα πιθανών αποτελεσμάτων μετά από κάποια ανεπιθύμητη επίθεση είναι

–Απώλεια ισχύος

– Φυσική κλοπή δεδομένων και υλικού

– Μη εξουσιοδοτημένες αλλαγές στο λειτουργικό περιβάλλον

– Αποσύνδεση των συνδέσεων φυσικών δεδομένων

– Μη ανιχνεύσιμη παρακολούθηση δεδομένων

Απαραίτητα μέτρα - έλεγχοι που πρέπει να ληφθούν.

–Ηλεκτρονικοί μηχανισμοί κλειδώματος για καταγραφή και λεπτομερή εξουσιοδότηση

– Ασφαλή κλειδώματα με PIN και κωδικούς πρόσβασης

– Βιομετρικά στοιχεία ελέγχου ταυτότητας

– Κρυπτογραφία οποιασδήποτε αποθηκευμένης πληροφορίας

7.2 Επίπεδο ζεύξης – Data link layer

Ασχολείται με τα στοιχεία των μεταδόσεων μεταξύ δυο άμεσα συνδεδεμένων σταθμών, επιπλέον ασχολείται με το θέμα της τοπολογίας όπου πολλοί σταθμοί θα μπορούν να μοιράζονται ένα μέσο. Από αυτό το επίπεδο προετοιμάζονται τα πακέτα δεδομένων για μετάδοση από το φυσικό στρώμα. Χρησιμοποιεί διεύθυνσης MAC και VLAN όπως επίσης και πρωτόκολλα WAN. Λόγω της μεγάλης αλληλεπίδρασης του με μια ποικιλία μέσων και υλικών εξαρτάται σε μεγάλο βαθμό από το πρωτόκολλο διαλειτουργικότητας. Χρησιμοποιώντας όμως κάποιο κακώς σχεδιασμένο πρωτόκολλο διαλειτουργικότητας μπορεί να υπάρξει πρόβλημα ασφαλείας. Για την διασφάλιση τη ασφάλειας θα μπορούσε να χρησιμοποιηθούν πρωτόκολλα κρυπτογράφησης για την εξακρίβωση της ταυτότητας των έγκυρων χρηστών και την προστασία από μη εξουσιοδοτημένη πρόσβαση. Το πιο διαδεδομένο πρόβλημα του επιπέδου είναι οι επιθέσεις sniffing. Τέτοια θέματα ασφαλείας βρίσκονται στο πρωτόκολλο ARP το οποίο καθορίζει τη σχέση μεταξύ των τοπικών σταθμών που είναι δυνατόν να επικοινωνούν. Το ARP δεν έχει κανένα μέσο για έλεγχο ταυτότητας ή επικύρωση των δεδομένων. Οποιοσδήποτε σταθμός του τοπικού επιπέδου θελήσει μπορεί να διεκδικήσει οποιαδήποτε διεύθυνση IP. Οι επιθέσεις πάνω σε αυτό το πρωτόκολλο χρησιμοποιούν unicast μεταδόσεις κατά συγκεκριμένων στόχων, γνωστή ως πλαστογράφηση ARP. Έτσι ευνοούνται οι επιθέσεις «man-in-the-middle».

Παραδείγματα πιθανών αποτελεσμάτων μετά από κάποια ανεπιθύμητη επίθεση είναι

–Πλαστογράφηση διευθύνσεων MAC, ο σταθμός απαιτεί την ταυτότητα κάποιου άλλου

– Η καταστρατήγηση του VLAN δηλαδή ο σταθμός επιβάλλει άμεση επικοινωνία με άλλους σταθμούς παρακάμπτοντας τους λογικούς ελέγχους όπως τα υποδίκτυα και τα τείχη προστασίας

– Οι διακόπτες ενδέχεται να πλημυρίσουν την κυκλοφορία σε όλες τις VLAN θύρες και όχι να τις προωθήσουν επιλεκτικά στις κατάλληλες

θύρες επιτρέποντας έτσι την παρακολούθηση των δεδομένων από οποιαδήποτε συσκευή είναι συνδεδεμένη σε VLAN

Απαραίτητα μέτρα - έλεγχοι που πρέπει να ληφθούν.

–Φιλτράρισμα των διευθύνσεων MAC και κατάλληλο προσδιορισμό σταθμών με διεύθυνση και παραπομπή σε φυσική θύρα ή λογική πρόσβαση

– Να μην γίνεται χρήση VLANs για μετάδοση ασφαλή δεδομένων, θα πρέπει να γίνονται μέσω μηχανισμών όπως firewalls

– Οι ασύρματες εφαρμογές θα πρέπει να αξιολογούνται προσεχτικά για οποιαδήποτε μη εξουσιοδοτημένη πρόσβαση

- Ενσωματωμένη κρυπτογράφηση, έλεγχος ταυτότητας και φιλτράρισμα MAC θα μπορούσε να εφαρμοστεί σε ασφαλή δίκτυα

7.3 Επίπεδο Δικτύου – NetworkLayer

Το επίπεδο αυτό ασχολείται με την τοπολογία των εργασιών στο Διαδίκτυο. Δηλαδή ασχολείται με το να καθορίσει ποια διαδρομή θα πρέπει να λάβει ένα πακέτο για να φτάσει σε έναν τελικό προορισμό μέσω διάφορων πολλαπλών συνδέσεων δεδομένων και διαδρομών. Χρησιμοποιεί διευθύνσεις IP για τον εντοπισμό κόμβων και τη δρομολόγηση.
Πρωτόκολλα όπως το ARP διευκολύνουν αυτή τη διαδικασία, χαρτογραφώντας το στρώμα 2 στις διευθύνσεις των τριών επιπέδων και λέγοντας στο τρίτο επίπεδο ποιο είναι το στρώμα συνδέσμου για να ακολουθηθεί η κατάλληλη διαδρομή. Σε αντίθετη περίπτωση τα πρωτόκολλα όπως το IP θα αναγνωρίσουν το ανώτερο επίπεδο μετάδοσης όπως το TCP ή UDP προκειμένου να κατευθύνει το στρώμα τέσσερα ως προς τον τρόπο με τον οποίο τα εισερχόμενα δεδομένα πρέπει να αντιμετωπιστούν.

Το τρίτο επίπεδο είναι το τελευταίο στρώμα που έχει μια φυσική επικοινωνία με τον πραγματικό κόσμο. Ένας δεδομένος κεντρικός

υπολογιστής θα έχει ένα μόνο επίπεδο τριών διευθύνσεων , αυτό τείνει να κάνει το τρίτο επίπεδο να απευθύνεται όχι μόνο στην τοπολογία του δικτύου αλλά και στην ταυτότητα των κόμβων.

Σε ένα τείχος προστασίας η διεύθυνση είναι η ειδική τιμή σε έναν κανόνα φιλτραρίσματος με ορισμένους κανόνες που τις χρησιμοποιούν ως ένα μοναδικό αναγνωριστικό διευθύνσεων που έχουν οριστεί ως μη έγκυρες. Έτσι, απαγορεύονται τα εισερχόμενα πακέτα από εξωτερικές πηγές και ζητάει μια διεύθυνση πηγής από ένα εσωτερικό δίκτυο, το λεγόμενο spoofing. Προκειμένου να ικανοποιηθούν όλοι οι ρόλοι που έχει το επίπεδο καθίσταται θέμα ασφαλείας. Στο τομέα της δρομολόγησης τα περισσότερα πρωτόκολλα έχουν μόνο στοιχειώδης επίπεδο ασφάλειας. Σε μια καθημερινή ανταλλαγή πληροφοριών μπορεί οι δυο πλευρές να συνομιλούν αλλά δεν γνωρίζουν αν τα δρομολόγια που ακολουθούν οι πληροφορίες έχουν πολλαπλασιαστεί με αποτέλεσμα την μη εξουσιοδοτημένη πρόσβαση τρίτων. Η ταυτότητα είναι ένας κλασσικός παράγοντας για επίθεση, τα περισσότερα πρωτόκολλα δεν έχουν ενσωματωμένα μέσα για τον έλεγχο ταυτότητας των διευθύνσεων προέλευσης .

Ο κύριος έλεγχος ασφαλείας του τρίτου επιπέδου πραγματοποιείτε πρωτίστως από το τοίχος προστασίας όταν αυτό βέβαια έχει ρυθμιστεί σωστά, ώστε να επιτρέπει μόνο την απαραίτητη διέλευση της κυκλοφορίας. Οι τεχνολογίες κρυπτογράφησης και ελέγχου ταυτότητας, όπως το IPSec μπορούν να χρησιμοποιούνται επιπλέον για την πιο αξιόπιστη αναγνώριση της πηγής των επικοινωνιών IP. Οι δρομολογητές θα πρέπει να ακολουθούν αυστηρές πολιτικές όσον αφορά την ανταλλαγή δρομολογίων και να χρησιμοποιούν αξιόπιστα μέσα για την επαλήθευση της επικοινωνίας. Το διαδίκτυο, τα μητρώα διαδρομών και η Βάση Δεδομένων δρομολόγησης (RADB) προσφέρουν τα μέσα για εγγραφή στις αναγγελίες διαδρομών. Επίσης το RADB παρέχει πληροφορίες φιλτραρίσματος που επιτρέπουν την δημιουργία πολιτικών για την επιβεβαίωση της διαδρομής από άλλες πηγές.

Παραδείγματα πιθανών αποτελεσμάτων μετά από κάποια ανεπιθύμητη επίθεση είναι

- Υποκλοπή δρομολογίων – Διάδοση εσφαλμένης τοπολογίας δικτύου.
- IP Address Spoofing – Αποστολή εσφαλμένης Διεύθυνσης πηγής σε κακόβουλα πακέτα.
- Ευπάθεια αναγνώρισης ταυτότητας και πόρων.

Απαραίτητα μέτρα - έλεγχοι που πρέπει να ληφθούν.

- Έλεγχοι επιπέδου δικτύου.
- Χρήση κατά της παραποίησης και της εσφαλμένης δρομολόγησης.
- Firewalls με ισχυρή πολιτική φίλτρων και αντί – spoof.
- Λογισμικό παρακολούθησης ARP / Broadcast.

7.4Επίπεδο Μεταφορών – TransportLayer.

Ασχολείται με την μετάδοση ροών δεδομένων στα χαμηλότερα στρώματα του μοντέλου. Γίνεται λήψη ροών δεδομένων από τα ψηλότερα επίπεδα, γίνεται μεταφορά τους και επανασυναρμολόγηση, έπειτα ακολουθεί η μετάδοση των εισερχόμενων πακέτων δεδομένων πίσω σε ανώτερα στρώματα. Υπάρχουν πρωτόκολλα μεταφοράς σχεδιασμένα για υψηλή αξιοπιστία και μηχανισμούς χρήσης ώστε να διασφαλιστεί ότι τα δεδομένα θα φτάσουν συνολικά στον προορισμό τους, όπως το πρωτόκολλο TCP ή το πρωτόκολλο UDP που επιλέγει να μειώσει τα έξοδα και εξαρτάται από τις καλύτερες προσπάθειες των χαμηλότερων στρωμάτων για την παράδοση των δεδομένων και των ανώτερων στρωμάτων να εξασφαλιστεί η επιτυχία στα επίπεδα που απαιτείται.
Με τα πρωτόκολλα μεταφοράς μπορεί να εφαρμοστεί έλεγχος ροής, ποιότητα εξυπηρέτησης και έλεγχοι ροής για την κάλυψη των αναγκών μετάδοσης. Μερικά πρωτόκολλα μεταφοράς, όπως το TCP και το UDP που προαναφέραμε, χρησιμοποιούν την έννοια των αριθμών port για να επιτρέψουν πολλαπλές ταυτόχρονες συνομιλίες μεταξύ πολλών προορισμών σε πρωτόκολλα ή εφαρμογές. Άλλα πρωτόκολλα όπως το ICMP μπορεί να βασίζονται σε δεδομένα υψηλότερου επιπέδου για την

ταξινόμηση της πολυπλεξίας. Επειδή το στρώμα μεταφοράς βρίσκεται εκεί όπου τα δεδομένα επικοινωνίας ενός host είναι πολυπλεγμένα και ταξινομημένα, χρησιμοποιείται συχνά σαν κύριο μέσο εξυπηρέτησης αναγνώρισης εντός ενός δεδομένου κεντρικού σταθμού.

Ορισμένα από τα βασικά σημεία ευπάθειας που διαπιστώθηκαν στο στρώμα μεταφοράς οφείλονται στην κακή διαχείριση μη προσδιορισμένων καταστάσεων που προκύπτουν. Πολλά πρωτόκολλα μεταφοράς υλοποιούνται με βάση την πεποίθηση ότι θα ασχολούνται με την καλή και σωστή επικοινωνία των ανώτερων και των κατώτερων επιπέδων, το οποίο δεν ισχύει αν το υποθέσουμε από την μεριά των κακόβουλα επιτιθέμενων. Με αποτέλεσμα τα πρωτόκολλα να υπόκεινται απροσδόκητες ή σκόπιμες εισροές ή χειρισμούς εκμετάλλευσης. Η συμπεριφορά ενός ξενιστή όταν παρουσιάζονται πακέτα TCP και UDP με αυθαίρετα περιεχόμενα, μπορούν να χρησιμοποιήσουν «δακτυλικό αποτύπωμα» ενός λειτουργικού συστήματος και επιλέγει πιο επικεντρωμένες επιθέσεις λόγω των διαφορών απόκρισης μεταξύ διαφορετικών λειτουργικών συστημάτων και στοίβες δικτύου.

Ένα άλλο θέμα ευπάθειας έγκειται στη χρήση και επαναχρησιμοποίηση θυρών για πολλαπλές λειτουργίες. Αυτό συμβαίνει συχνά στα Windows όπου διάφορες λειτουργίες όπως κοινή χρήση εκτυπώσεων, απομακρυσμένη διαχείριση, μηνύματα LAN, και άλλες εφαρμογές όπου χρησιμοποιούν αρκετές θύρες UDP και TCP. Επειδή υπάρχουν αρκετές θύρες είναι δύσκολο να ελεγχθεί και να περιοριστεί η πρόσβαση από ένα τείχος προστασίας. Εάν υπάρχει κάποια λειτουργία τότε οι θύρες του τείχους προστασίας ανοίγουν και τα περισσότερα αν όχι όλα τα δεδομένα ρέουν ανεξέλεγκτα. Αυτή η υπερφόρτωση περιορίζει την αποτελεσματικότητα των δικτυακών ελέγχων όπως τα τείχη προστασίας. Τα περισσότερα πρωτόκολλα μετάδοσης δημιουργήθηκαν με έμφαση στη χρησιμότητα και την εκτέλεση, ως εκ τούτου συνήθως δεν εφαρμόζουν ισχυρούς ελέγχους για την επικύρωση της πηγής μετάδοσης ή ότι ένα πακέτο αποτελεί νόμιμο μέρος της συνομιλίας. Αυτό μπορεί να προκαλέσει πακέτα που μπορούν να παρεμποδίσουν ή να ανακατευθύνουν την ροή μετάδοσης. Ορισμένα πρωτόκολλα όπως το UDP μπορούν εύκολα να παραπλανηθούν και να ξεγελαστούν λόγω έλλειψης αλληλουχίας, άλλα πρωτόκολλα όπως το TCP είναι πιο δύσκολο να ξεγελαστούν λόγω του πιο εκτεταμένου έλεγχου ροής και έλεγχου ακεραιότητας. Σε τέτοια

πρωτόκολλα η ακεραιότητα σχετίζεται περισσότερο με την τυχαία απώλεια δεδομένων λόγω σφαλμάτων παρά από σκόπιμη επίθεση στο πρωτόκολλο, με αποτέλεσμα τέτοια πρωτόκολλα να πέφτουν θύμα πιο εξελιγμένων επιθέσεων. Μια τέτοια επίθεση θα μπορούσε να είναι η αεροπειρατεία της συνόδου TCP, όπου ο επιτιθέμενος πρέπει να μαντέψει παράγοντες όπως αρχικά και TCP ακολουθίες αριθμών, στη συνέχεια να εισάγει ψεύτικα πακέτα ώστε να διαχειριστεί τη ροή δεδομένων διακόπτοντας έτσι τη ροή δεδομένων ανώτερων επιπέδων. Με μια τέτοια επίθεση μπορεί να αποκτηθεί έλεγχος μονής κατεύθυνσης άλλα οι πληροφορίες δεν θα επιστραφούν στον εισβολέα, εκτός και αν χρησιμοποιηθεί το κανάλι ελέγχου για να ανοίξει πρόσθετα κανάλια επίθεσης.

Τα τείχη προστασίας είναι ο πιο συνηθισμένος έλεγχος στο επίπεδο αυτό, οι κανόνες κάθε τείχους προστασίας πρέπει να είναι γραμμένοι ώστε να είναι όσο το δυνατόν πιο αυστηροί. Αυτό σημαίνει ότι τα πρωτόκολλα στρώματος μεταφοράς πρέπει να καθορίζονται ξεχωριστά σε κανόνες, όπου βέβαια αυτό είναι δυνατόν, αντί να επιτρέπουν οποιαδήποτε επικοινωνία. Όσο αφορά την επικοινωνία TCP/IP πρέπει να γράφονται κανόνες και να εφαρμόζονται για τα πρωτόκολλα όπως το TCP/UDP/ICMP όπως και οι αριθμοί θυρών τους. κάποιοι ισχυρότεροι μηχανισμοί έχουν αναπτυχθεί ώστε οι επιθέσεις να καθίσταται πιο δύσκολο να συμβούν. Κάποιες βελτιώσεις στον αριθμό ακολουθίας TCP με ανάθεση με βάση τη παραγωγή τυχαίων αριθμών παρά να χρησιμοποιούνται αυθαίρετες και προβλέψιμες ακολουθίες. Το τείχος προστασίας CiscoPIX παρέχει έναν τυχαίο αριθμό ακολουθίας TCP για την κυκλοφορία που περνάει ως μέρος του αλγορίθμου NATAdaptive Security Algorithm ώστε οι ακολουθίες να εξακολουθούν να είναι μη τυχαίες και προβλέψιμες.

Παραδείγματα πιθανών αποτελεσμάτων μετά από κάποια ανεπιθύμητη επίθεση είναι

- Ανεπαρκής αντιμετώπιση απροσδιόριστων συνθηκών.
- Οι διαφορές στην εφαρμογή του πρωτοκόλλου μεταφοράς επιτρέπουν την «αποτύπωση δακτυλικών αποτυπωμάτων».
- Η υπερφόρτωση των αριθμών θυρών περιορίζει την ικανότητα φιλτραρίσματος.
- Οι μηχανισμοί μετάδοσης μπορεί να υποβληθούν σε πλαστογράφηση και επίθεση βασισμένη σε επεξεργασμένα πακέτα .

Απαραίτητα μέτρα - έλεγχοι που πρέπει να ληφθούν.

– Αυστηροί κανόνες τείχους προστασίας που περιορίζουν την πρόσβαση σε συγκεκριμένα πρωτόκολλα μετάδοσης.
– Ισχυρότεροι μηχανισμοί ταυτοποίησης μετάδοσης.

7.5 Επίπεδο Συνόδου – Session Layer

Το επίπεδο αυτό ασχολείται με την οργάνωση των επικοινωνιών δεδομένων σε λογικές ροές. Παίρνει τα αιτήματα για την αποστολή δεδομένων από τα υψηλότερα στρώματα και ελέγχει την έναρξη και την παύση της επικοινωνίας με τον απομακρυσμένο host. Εν συνεχεία, παρουσιάζει τις ροές δεδομένων στο επίπεδο μεταφοράς κάτω από το σημείο εκκίνησης. Ασχολούνται ως επί το πλείστον με θέματα πρόσβασης και προσβασιμότητας. Ασχολείται επίσης με τον έλεγχο ροής υψηλότερων τάξεων ώστε να περιορίσει την ταχύτητα με την οποία εισέρχονται ή εξέρχονται τα δεδομένα.

Καθώς ασχολείται με την δημιουργία και τον έλεγχο της πρόσβασης στο υψηλότερο επίπεδο προκύπτει το ζήτημα της αδειοδότησης και της πρόσβασης ως φυσική αδυναμία. Τέτοια παρόμοια προβλήματα προκύπτουν και σε πρωτόκολλα χαμηλότερων επίπεδων όπως το RPC και το COBRA που παρέχουν ένα ευρύ φάσμα υπηρεσιών μέσω ενός καναλιού που περιορίζει την ικανότητα των χαμηλότερων στρωμάτων του δικτύου να ελέγχει την πρόσβαση στους πόρους. Όσο αυτά τα πρωτόκολλα δεν παρέχουν ισχυρή ασφάλεια εσωτερικά γίνονται εύκολα στόχος για κατάχρηση. Πολλά πρωτόκολλα έχουν έλλειψη από ισχυρή προστασία της αδειοδότησης, όπως το πρότυπο TELNET και FTP όπου μεταδίδουν ονόματα χρήστη και κωδικούς πρόσβασης επιτρέποντας έτσι σε επίπεδα κάτω από αυτό να παρακολουθούν την επικοινωνία. Πρωτόκολλα με ισχυρότερη προστασία κωδικών πρόσβασης συχνά πέφτουν θύματα κρυπτογραφικών ή αδυναμία διαχείρισης των κωδικών πρόσβασης και του ελέγχου ταυτότητας.

Όσο μεγάλη προστασία διαπιστευτηρίων και να υπάρχει είναι πολύ συνηθισμένο ότι οι κωδικοί είναι αδύναμοι και υπόκεινται εύκολα σε επιθέσεις. Το επίπεδο συνόδου μπορεί να επιδεινώσει αυτό το πρόβλημα με κακή ή ακόμα και ανύπαρκτη καταγραφή των αποτυχημένων προσπαθειών πρόσβασης , επιτρέποντας έτσι σε έναν εισβολέα απεριόριστες και εν τέλει μη ανιχνεύσιμες προσπάθειες. Διάφοροι μηχανισμοί στο επίπεδο αυτό μπορούν να χρησιμοποιηθούν ώστε να καταγραφούν κάποια ονόματα χρηστών. Ορισμένες υπηρεσίες όπως το SIP και άλλα πρωτόκολλα Voiceover IP αντιμετωπίζουν παρόμοια προβλήματα με τον προσδιορισμό της έγκυρης κυκλοφορίας, βασίζονται σε πρωτόκολλο UDP για τις επιδόσεις τους επίσης πρέπει να εφαρμόσουν την αναγνώριση της συνόδου μεταφοράς.

Όπως φαίνεται, το ζήτημα της ταυτότητας είναι ένα σοβαρό θέμα σε όλα τα επίπεδα του μοντέλου, με τα χαρακτηριστικά κάθε στρώματος να χρησιμοποιούνται συχνά για την αναγνώριση και την εξουσιοδότηση. Για τις ιδιωτικές επικοινωνίες τα ασφαλή κανάλια και οι συνεδρίες πιστοποίησης είναι ουσιώδης. Τεχνολογίες κρυπτογράφησης επιτρέπουν τόσο την αξιόπιστη αναγνώριση απομακρυσμένων client- server, όσο και μέσα προστασίας για την ανταλλαγή δεδομένων μακριά από αδιάκριτες πηγές. Κωδικοί πρόσβασης και άλλα διαπιστευτήρια θα πρέπει να αποθηκεύονται και να μεταβιβάζονται σε κρυπτογραφημένη μορφή ώστε να αποτρέπεται η παρακολούθηση και η κλοπή, επιπλέον οι λογαριασμοί χρηστών θα πρέπει να έχουν ημερομηνίες λήξης βασιζόμενες στη χρήση και σε καθορισμένο χρόνο ώστε μετά το πέρας να απαιτείται ενημέρωση των διαπιστευτηρίων και η επανεξέταση της πρόσβασης.

Παραδείγματα πιθανών αποτελεσμάτων μετά από κάποια ανεπιθύμητη επίθεση είναι

- Αδύναμοι ή ανύπαρκτοι μηχανισμοί ελέγχου ταυτότητας.
- Παρακολούθηση και μη εξουσιοδοτημένη χρήση σε κωδικούς πρόσβασης και στο αναγνωριστικό χρήστη.
- Η ταυτοποίηση της συνόδου μπορεί να δεχθεί spoofing (πλαστογραφία)
- Οι απεριόριστες προσπάθειες μπορεί να προκαλέσουν επιθέσεις βίαιης δύναμης στα διαπιστευτήρια (brute-force-attack)

Απαραίτητα μέτρα - έλεγχοι που πρέπει να ληφθούν.

- Κρυπτογραφημένη ανταλλαγή κωδικών πρόσβασης και αποθήκευση.
- Συγκεκριμένη λήξη των λογαριασμών.
- Περιορισμός των αποτυχημένων προσπαθειών περιόδου λειτουργίας μέσω του μηχανισμού χρονισμού.

7.6 Επίπεδο Παρουσίασης - Presentation Layer

Ασχολείται με την οργάνωση των δεδομένων που διαβιβάζονται από το στρώμα εφαρμογής στο δίκτυο. Επιτρέπει την τυποποίηση των δεδομένων και την επικοινωνία μεταξύ διαφορετικών υπολογιστών, όπως πλατφόρμες με διαφορετικά δυαδικά συστήματα αναπαράστασης αριθμών ή σύνολα χαρακτήρων. Το επίπεδο αυτό μπορεί να ελέγχει επίσης όποιες βελτιώσεις στο στρώμα δικτύου όπως η συμπίεση ή η κρυπτογράφηση. Το επίπεδο αυτό είναι καλά κρυμμένο μέσα σε εφαρμογές και λειτουργικά συστήματα. Μπορούμε να πούμε πως το επίπεδο παρουσίασης είναι όλες οι διεπαφές που υλοποιούνται ή καλούνται από μια εφαρμογή για την προετοιμασία και την παρουσίαση δεδομένων στο δίκτυο. Πολλές εφαρμογές κάνουν χρήση των SSL και TLS για ασφαλή επικοινωνία με χρήση ισχυρής πιστοποίησης ταυτότητας, κρυπτογράφησης δεδομένων και άλλων βασικών λειτουργιών αξιοπιστίας στην κρυπτογραφία.

Οι ευπάθειες σε αυτό το στρώμα συχνά προέρχονται από αδυναμίες ή ελλείψεις στην υλοποίηση των λειτουργιών του στρώματος παρουσίασης. Οι επιτιθέμενοι εκμεταλλευόμενοι την έμμεση εμπιστοσύνη και την απλή λειτουργικότητα των συστημάτων, τροφοδοτούν απρόσμενες ή παράνομες εισροές επιτυγχάνοντας έτσι ανεπιθύμητα αποτελέσματα.

Μια γνωστή αδυναμία αναγνωρισμένη ως ευπάθεια συμβολοσειράς μορφοποίησης είναι όταν τα τρωτά σημεία των συμβολοσειρών μορφής εκμεταλλεύονται εφαρμογές που χρησιμοποιούν πληροφορίες που

παρέχονται από το χρήστη για τη βάση των εισροών σε βιβλιοθήκες I/O, έτσι ώστε η ροή δεδομένων που παρέχει ο χρήστης να μπορεί να ελέγχει τον τρόπο με τον οποίο τα δεδομένα αυτά μεταδίδονται, διαμορφώνονται ή αποθηκεύονται κατά την μετάδοση.

Οι υπηρεσίες κρυπτογράφησης μπορούν να πέσουν θύμα αδυναμιών της εφαρμογής ή του βασικού σχεδιασμού, κάποιοι ασφαλείς διακομιστές ιστού που χρησιμοποιούν SSL είχαν σφάλματα στην υποκείμενη κρυπτογραφία της εφαρμογής SSL δημιουργώντας έτσι θεωρητική και πρακτική εκμετάλλευση της ασφάλειας.

Η κρυπτογραφία είναι ένας γρήγορα αναπτυσσόμενος στόχος και οι δυνατότητες της τεχνολογίας και του υλικού αναπτύσσονται συνεχώς. Η κρυπτογραφική ισχύς των υπηρεσιών προστασίας δεδομένων στο στρώμα παρουσίασης θα πρέπει να επιλέγεται προσεχτικά και να επανεξετάζεται συχνά.

Παραδείγματα πιθανών αποτελεσμάτων μετά από κάποια ανεπιθύμητη επίθεση είναι

- Ο κακός χειρισμός της απροσδόκητης εισερχόμενης ροής μπορεί να οδηγήσει σε διακοπές λειτουργίας ή στην εκτέλεση αυθαίρετων οδηγιών.
- Τα κρυπτογραφικά ελαττώματα μπορούν να χρησιμοποιηθούν για να παρακάμψουν την προστασία.

Απαραίτητα μέτρα - έλεγχοι που πρέπει να ληφθούν.

- Προσεχτική προδιαγραφή και έλεγχος εισερχόμενης εισόδου σε εφαρμογές ή λειτουργίες .
- Ο διαχωρισμός των λειτουργιών εισόδου χρήστη και ελέγχου προγράμματος. Οποιαδήποτε εισερχόμενη κίνηση θα πρέπει να ελέγχεται κατάλληλα και να μεταφέρεται στην κατάλληλη είσοδο.
- Προσεχτική και συνεχής επανεξέταση λύσεων κρυπτογραφίας για την εξασφάλιση ασφάλειας έναντι απειλών.

7.7 Επίπεδο Εφαρμογής – Application Layer

Ασχολείται με τις λειτουργίες υψηλού επιπέδου των προγραμμάτων που μπορούν να χρησιμοποιούν το δίκτυο. Σε αυτό το επίπεδο εμφανίζονται όλες οι λειτουργίες που δεν σχετίζονται άμεσα με τη λειτουργία του δικτύου.

Το άνω άκρο της στοίβας είναι το πιο ανοιχτό του συνόλου των στρωμάτων και μπορεί να θεωρηθεί ότι δεν καλύπτει όλα τα ζητήματα των άλλων έξι επιπέδων. Κάποια προσανατολισμένα προς τον χρήστη πρωτόκολλα όπως το DNS, η μεταφορά αρχείων (HTTP,FTP), τα μηνύματα (SMTP) και η απομακρυσμένη πρόσβαση (TELNET) λειτουργούν εντός του μοντέλου και «σκοπεύουν» σε υψηλότερα επίπεδα.
Το επίπεδο εφαρμογής θεωρείται ως το πεδίο που λαμβάνεται η αλληλεπίδραση του χρήστη και οι λειτουργίες υψηλού επιπέδου λειτουργούν πάνω από το επίπεδο του δικτύου. Όπως και στο φυσικό στρώμα, η ανοιχτή φύση του επιπέδου αυτού ομαδοποιεί πολλές απειλές μαζί στο τέλος της στοίβας. Μια από τις πρωταρχικές απειλές είναι η κακή ή και ανύπαρκτη σχεδίαση ασφαλείας της βασικής λειτουργίας μιας εφαρμογής. Ορισμένες εφαρμογές ενδέχεται να χειρίζονται χωρίς ασφάλεια τις ευαίσθητες πληροφορίες τοποθετώντας τες σε δημόσια προσβάσιμα αρχεία ή την κωδικοποίηση τους σε «κρυμμένες» περιοχές που εμφανίζονται επιπόλαια σε σημεία, όπως σε κώδικα HTML μιας φόρμας ιστού. Τα προγράμματα αυτά μπορεί να έχουν κρυμμένα backdoors ή συντομεύσεις που παρακάμπτουν τα άλλα ασφαλή στοιχεία ελέγχου και παρέχουν μη εξουσιοδοτημένη πρόσβαση. Οι εφαρμογές με αδυναμίες ή μη πιστοποίηση είναι πρωταρχικοί στόχοι για μη εξουσιοδοτημένη χρήση. Το πρωτόκολλο TFTP χρησιμοποιείται εκτεταμένα για εκκίνηση ασύρματων σταθμών εργασίας και για διαχείριση συσκευών δικτύου αλλά δεν απαιτεί κανένα όνομα χρήστη ή κωδικό πρόσβασης στις πληροφορίες . Διάφορες εφαρμογές μπορεί να βασίζονται σε ανυπόληπτα κανάλια για την εξακρίβωση της ταυτότητας. Το UnixrLogin, rsh και άλλα, χρησιμοποιούν συνήθως την εμπιστοσύνη μιας λίστας απομακρυσμένων ξενιστών και απομακρυσμένους χρήστες χωρίς ισχυρό μέσο επαλήθευσης της ταυτότητας. Τα ονόματα DNS μπορούν να αλλοιωθούν ή οι διακομιστές DNS να διακυβεύονται. Οι αιτήσεις συχνά παρέχουν υπερβολική πρόσβαση στους πόρους επιτρέποντας

έτσι αποφυγή ελέγχου για την υπερβολική πρόσβαση και την αποτροπή της διαφθοράς ή της απώλειας δεδομένων. Η έλλειψη λεπτομερών ελέγχων οδηγεί σε πολλά συστήματα δεδομένων που έχουν πρόσβαση σε μια "όλα ή τίποτα" βάση αναγκάζοντας έτσι τους διαχειριστές να δώσουν απεριόριστη ή καθόλου πρόσβαση. Οι υπερβολικά περίπλοκοι έλεγχοι πρόσβασης ενδέχεται να φαίνεται ότι προστατεύουν την πρόσβαση, αλλά στην ουσία αποτυγχάνουν να αποτρέψουν την μη εξουσιοδοτημένη πρόσβαση.

Οι χρήστες ενδέχεται να παρέχουν μη αναμενόμενες εισροές στο περιβάλλον εφαρμογής, το οποίο αν δεν αντιμετωπιστεί σωστά θα μπορούσε να οδηγήσει σε απροσδόκητες συμπεριφορές. Ένας κακόβουλος χρήστης μπορεί να είναι σε θέση να χρησιμοποιήσει σφάλματα και ελαττώματα του προγράμματος ώστε να αποκτήσει πρόσβαση σε πόρους και δεδομένα.

Μερικοί από τους πιο διαδεδομένους ελέγχους στο επίπεδο εφαρμογής βασίζονται σε ισχυρές πρακτικές σχεδίασης τόσο στο σχεδιασμό όσο και στην υλοποίηση εφαρμογών. Οι αιτήσεις πρέπει να χρησιμοποιήσουν την ασφάλεια εγκαταστάσεων που είναι διαθέσιμα σε χαμηλότερα επίπεδα δικτύου, ελέγχονται προσεχτικά τα εισερχόμενα και τα εξερχόμενα δεδομένα και υποθέτοντας πως είναι πιθανό να δεχτούν επίθεση οι επικοινωνίες, απαιτείται χρήση ισχυρού ελέγχου ταυτότητας και κρυπτογράφησης για την επικύρωση και την προστασία δεδομένων. Οι εφαρμογές θα πρέπει επίσης να υλοποιούν στην εφαρμογή τους δικούς τους ελέγχους ασφαλείας επιτρέποντας έτσι τον λεπτομερή έλεγχο για την πρόσβαση σε πόρους και δεδομένα, χρησιμοποιώντας ιδανικά έναν μηχανισμό που είναι απλός και επιτυγχάνει ισορροπία μεταξύ χρηστικότητας και αποτελεσματικότητας. Γενικότερα, μια λεπτομερής καταγραφή και η δυνατότητα του ελέγχου πρέπει να είναι ένα χαρακτηριστικό που δεν θα λείπει από καμία εφαρμογή που χειρίζεται ευαίσθητες πληροφορίες.

Η δοκιμή και η αναθεώρηση είναι επίσης κρίσιμα στοιχεία ελέγχου. Λόγω της μεγάλης ποικιλίας τόσο των προβλημάτων όσο και των λύσεων, των προτύπων και των πρακτικών η εφαρμογή δεν θα είναι σε θέση να αντιλαμβάνεται όλες τις πιθανές ανατροπές. Οι προγραμματιστές συχνά θα έχουν αντικρουόμενα κίνητρα σχετικά με τις εφαρμογές τους και σε ένα δομημένο περιβάλλον προγραμματισμού οι δοκιμές ασφαλείας είναι κρίσιμα μέρη ενός ασφαλούς κύκλου ζωής ανάπτυξης λογισμικού (SDLC). Στην πρόσοψη του υλικού, τα

συστήματα ανίχνευσης εισβολών (IDS) μπορούν να παρατηρήσουν δεδομένα σχετικά με την επισκεψιμότητα για γνωστά προφίλ δραστηριότητας δικτύου που μπορεί να ανιχνεύσει ευάλωτους χρήστες, εφαρμογές ή επικείμενες επιθέσεις καθώς και ανεπιθύμητη κυκλοφορία εφαρμογών.

Τέλος, πολλά συστήματα τείχους προστασίας βασισμένα στον κεντρικό υπολογιστή, περιλαμβάνουν τα μέσα για τον έλεγχο πρόσβασης των εφαρμογών στο δίκτυο, αυτός ο έλεγχος είναι χρήσιμος για τη αποτροπή μη εξουσιοδοτημένης ή συγκαλυμμένης χρήσης πόρων δικτύου από τοπικά προγράμματα .

Προς αποφυγή των προαναφερθέντων θα πρέπει να γίνονται κάποιοι έλεγχοι

- Ζητήματα ανοιχτού σχεδίου επιτρέπουν την ελεύθερη χρήση των πόρων εφαρμογής
- Τα ελαττώματα σχεδιασμού και τα backdoors παρακάμπτουν τα στοιχεία ελέγχου ασφαλείας.
- Οι ανεπαρκείς έλεγχοι ασφαλείας επιβάλουν την προσέγγιση “όλα η τίποτα” με αποτέλεσμα είτε υπερβολική πρόσβαση είτε ανεπαρκή.
- Υπερβολικά περίπλοκοι έλεγχοι ασφαλείας εφαρμογών τείνουν να παρακάμπτονται εύκολα ή να είναι δυσκολονόητοι.
- Οι λανθασμένες λογικές του προγράμματος ενδέχεται να χρησιμοποιηθούν κατά λάθος ή σκόπιμα για να προκαλέσουν ανεπιθύμητη συμπεριφορά στα προγράμματα.

Απαραίτητα μέτρα - έλεγχοι που πρέπει να ληφθούν

- Έλεγχοι πρόσβασης επιπέδου εφαρμογής για τον καθορισμό και την επιβολή της πρόσβασης στην εφαρμογή. (οι έλεγχοι θα πρέπει να είναι λεπτομερείς και ευέλικτοι αλλά κυρίως απλοί ώστε να αποτρέψουν τα προβλήματα πολυπλοκότητας .
- Πρότυπα, δοκιμές και επανεξέταση του κώδικα εφαρμογής και της λειτουργικότητας.
- Συστήματα IDS για την παρακολούθηση των αιτημάτων και της δραστηριότητας.

– Ορισμένα συστήματα τείχους προστασίας βασισμένα σε κεντρικούς υπολογιστές μπορούν να ρυθμίζουν την κυκλοφορία μέσω εφαρμογής, εμποδίζοντας μη εξουσιοδοτημένη ή συγκαλυμμένη χρήση του δικτύου.

Επεκτείνοντας το μοντέλο

Μοντέλο 9 επιπέδων

Το πρότυπο επτά επιπέδων που προαναφέραμε είναι αρκετά επαρκείς για τους σκοπούς του δικτύου, άλλα όταν μιλάμε για έννοιες ασφαλείας πληροφοριών χρειάζεται περισσότερη οργάνωση. Μερικές τέτοιες έννοιες λοιπόν δεν συμπεριλαμβάνονται στο μοντέλο, έχει υποστηριχτεί λοιπόν ότι για την καλύτερη αναπαράσταση αυτά τα δύο στοιχεία/έννοιες να προστεθούν ως δύο πρόσθετα στρώματα. Το **επίπεδο οκτώ** αφορά την αλληλεπίδραση των ανθρώπων με τις εφαρμογές και το **επίπεδο εννέα** πολιτικές που ελέγχουν τις ενέργειες των ανθρώπων. Βέβαια αυτή η θεωρία πέφτει σε αντίφαση μιας και το λογικό θα ήταν ο χρήστης να είναι στην κορυφή των επιπέδων ώστε να είναι «κυρίαρχος» όλων των διαδικασιών και όχι στο επίπεδο οκτώ. Όμως ο μηχανικός ασφαλείας ξέρει ότι ακόμα και οι ενέργειες ενός χρήστη θα πρέπει να καθοδηγούνται πάντα από καλά οργανωμένες και προσεχτικά ανεπτυγμένες πολιτικές. Είναι λογικό βέβαια ένας χρήστης να μην συμμορφώνεται πάντα με αυτές τις πολιτικές αλλά υπάρχουν επίσης ώστε να θέτουν όρια όταν βλέπουν ότι οι σωστές πολιτικές παρακάμπτονται.

Σχετικά με την προσέγγιση του μοντέλου 9 επιπέδων μπορούμε να εξετάσουμε την ιδανική πολιτική ασφαλείας και ώστε να είναι ανεξάρτητη των επιπέδων, η πολιτική αυτή θα πρέπει να ισχύει σε όλες τις πλατφόρμες και εφαρμογές ανεξάρτητα από τις εκάστοτε ιδιαιτερότητες και τέλος να ταιριάζουν σε κάθε είδος χρήστη, από έναν ανώνυμο χρήστη Internet μέχρι τους πιο έμπειρους διαχειριστές και στελέχη.

Ένα πρόβλημα που προκύπτει στην εφαρμογή πολιτικών ασφαλείας στο επίπεδο 9 είναι πως εφαρμόζεται έλεγχος πάνω από το επίπεδο του χρήστη και μετά λειτουργεί αυτοτελώς πάνω από τα άλλα στρώματα. Οι χρήστες μπορούν βέβαια να εφαρμόσουν αυτή την πολιτική σε όλα τα επίπεδα, κάνοντας χρήση διάφορων εφαρμογών διαχειριστή, τείχους προστασίας για να οριστούν οι κανόνες φιλτραρίσματος, έτσι

επιτρέπεται η ροή της επικοινωνίας στο μοντέλο παρόλο που θα μπορούσε να θεωρηθεί λιγάκι αφηρημένο.

Μια άλλη εναλλακτική άποψη είναι ότι το ανώτερο στρώμα της πολιτικής καλύπτει όλες τις στρώσεις σαν ομπρέλα και απλώνεται γύρω τους για να ελέγξει την ταυτοποίηση των πιθανών απειλών και κινδύνων σε κάθε συγκεκριμένο στρώμα ξεχωριστά και προτείνοντας αυτόματα ελέγχους που θα πρέπει να εφαρμοστούν.

Εν κατακλείδι

Παραπάνω έχουμε αναφέρει πολλά κατά την παρουσίαση του μοντέλου OSI επτά επιπέδων και την χρήση του ως εργαλείο ασφαλείας πληροφοριών και καλύψαμε όλο το φάσμα της αξιοπιστίας δεδομένων.

Στο πλαίσιο ασφαλείας, το μοντέλο εννέα επιπέδων μπορεί να εφαρμοστεί υπολογίζοντας τόσο τα δυνατά σημεία όσο και τις αδυναμίες των συστημάτων και των εφαρμογών. Το μοντέλο αυτό γίνεται δεκτό και υπό συζήτηση από τους χρήστες με τα τρωτά του σημεία και με τις αδυναμίες του. Εξάλλου η όλη ιδέα του μοντέλου αυτού δεν είναι να περιγράψει ολόκληρες τις έννοιες και το τοπίο για το μοντέλο αυτό αλλά να χρησιμεύσει ως βάση για περαιτέρω βελτίωση και επέκταση.

Η κατανόηση του μοντέλου OSI μας δίνει μια καλύτερη εκτίμηση των απειλών που ενδέχεται να αντιμετωπίσουν τα δίκτυα μας. Κατανοώντας το μοντέλο OSI αρχίζουμε να κατανοούμε και την προσέγγιση που θα πρέπει να λάβουμε. Ο στόχος είναι να καταφέρουμε να δούμε τα δίκτυα μας ως μεμονωμένα στοιχεία, να χωρίσουμε το δίκτυο μας ως μεμονωμένα ζητήματα ώστε να διαιρέσουμε τον κίνδυνο και να τον καταπολεμήσουμε καλύτερα βασιζόμενοι τα τρωτά σημεία του συστήματός μας.

Τέλος να αναφέρουμε ότι στην καθημερινότητα μας και στον πρακτικό κόσμο της δικτύωσης και της ασφάλειας, τείνουμε να έχουμε μια κλίση προς τα πράγματα που λειτουργούν καλύτερα και ίσως και πιο απλά.

8.Συμπεράσματα.

Το Internet πλέον στις μέρες μας αποτελεί ένα παγκόσμια επεκτεινόμενο δίκτυο υπολογιστών και μπορούμε σίγουρα να υποστηρίξουμε πως αποτελεί θεμελιώδη λίθο της «κοινωνίας της πληροφορίας». Πλέον το διαδίκτυο χρησιμοποιείται για εντελώς διαφορετικό σκοπό από ότι αρχικά δημιουργήθηκε, δεν απευθύνεται μόνο σε επιστήμονες, ερευνητές ή ειδικούς αλλά σε ένα σωρό απλούς χρήστες. Η μεγάλη απήχηση του οφείλεται επίσης στο γεγονός ότι οι υπηρεσίες που παρέχει είναι φιλικές και εύχρηστες και μπορεί εύκολα ο χρήστης να ανταπεξέλθει χωρίς ιδιαίτερες γνώσεις.Όπως προαναφέραμε στην αρχή της εργασίας, με την εμφάνιση της υπηρεσίας του World Wide Web η επικοινωνία βελτιώθηκε σημαντικά δίνοντας έτσι την δυνατότητα να επικοινωνούν οι χρήστες αλληλεπιδραστικά. Με την συνεχή ανάπτυξη και εξέλιξη που παρουσιάζει, οι περισσότερες υπηρεσίες που παρέχει έχουν βελτιωθεί παρέχοντας στον χρήστη ένα περιβάλλον ευχάριστο, γρήγορο και εύκολο. Το WWW υποστηρίζει δημοφιλείς αλλά εξεζητημένες υπηρεσίες όπως εμπορικές, ηλεκτρονικές συναλλαγές και τήλε-εκπαίδευση. Κάθε είδους χρήστης, από εμπορικές εταιρείες, οργανισμούς, ειδησεογραφικά πρακτορεία, ερευνητικά και ακαδημαϊκά ιδρύματα σε όλο τον κόσμο έχουν «πλημμυρίσει» το www με τις σελίδες τους.

Παράλληλα όμως, ενώ η χρήση του World Wide Web φαντάζει ιδανική δεν αργούν να εμφανιστούν τα πρώτα προβλήματα. Αρχίζουν να καταπατώνται δικαιώματα όπως της ελεύθερης διακίνησης ιδεών στο διαδίκτυο. Αυτό συμβαίνει γιατί ενώ ο καθένας μπορεί να δημιουργήσειweb σελίδες για τον εκάστοτε σκοπό, αρχίζει να εμφανίζεται ασελγές περιεχόμενο, εθνικιστικό ή γενικότερα προσβλητικό. Οι επιπτώσεις και τα προβλήματα που εμφανίζονται δεν είναι φυσικά μόνο κοινωνικά. Το μεγαλύτερο μέρος του προβλήματος αποτελούν οι **τεχνολογικές επιθέσεις**, όλη αυτή η τεράστια και ανεξέλεγκτη μετάδοση πληροφορίας αρχίζει να εγκυμονεί κινδύνους. Είναι πιθανό και ανησυχητικό στους υπεύθυνους πως όλες αυτές οι μαζικές πληροφορίες και ο τεράστιος όγκος των δεδομένων κάποια στιγμή θα κατακλύσουν το διαδίκτυο και θα καταρρεύσει. Μέγιστο ζήτημα ασφαλείας επίσης αποτελεί η ανάγκη για ασφάλεια των επικοινωνιών. Τα μεταφερόμενα δεδομένα είτε πληροφορίες είτε

συναλλαγές θα πρέπει να κρυπτογραφούνται και να παρέχεται ασφάλεια και προστασία των υπολογιστικών συστημάτων. Ακόμα και σήμερα που το Internetέχει υποστεί αυτή την τόσο μεγάλη εξέλιξη δεν είναι λίγες οι φορές που έχει καταπατηθεί η ασφάλεια και έχουν γίνει υποκλοπές ή τροποποίηση περιεχομένων.

Η χρήση του μοντέλου Open Systems Interconnection, όπως παρουσιάστηκε σε αυτήν την εργασία από την πλευρά της ασφάλειας, μπορεί να βοηθήσει τον αναγνώστη να κατανοήσει και κυρίως να κατηγοριοποιήσει την πληθώρα των απειλών αλλά και των τρόπων άμυνας που υπάρχουν ανάλογα με το σε ποιο επίπεδο (layer) κατά OSIαναφέρονται. Είναι μειονέκτημα το γεγονός ότι ενώ το Open System Interconnection, διδάσκεται σε όλα τα Πανεπιστήμια και αποτελεί το σημείο αναφοράς για όλους τους κατασκευαστές δικτυακού υλικού και συσκευών, σπανίως εμφανίζεται να λαμβάνεται υπόψη στην παρουσίαση των απειλών και των τρόπων αμύνης στον τομέα του Information Security. Θεωρούμε ότι αυτή η εργασία αποτελεί μια φιλότιμη προσπάθεια προς αυτή την κατεύθυνση.

Βιβλιογραφίες.

1. Διάλεξη Γεώργιος Ν. Μπάρδης 2008 Δίκτυα Η/Υ 1. Εισαγωγή στα Δίκτυα Επικοινωνιών.
2. Εκδόσεις Κλειδάριθμος. Πέμπτη Αμερικανική Έκδοση. Δίκτυα Υπολογιστών. Συγγραφείς: Tatenbaum – Wetherall.
3. Ασφάλεια Πληροφοριακών Συστημάτων. Εκδόσεις Νέων Τεχνολογιών. Επιστημονική επιμέλεια: Σωκράτης Κάτσικας, Δημήτρης Γκρίτζαλης, Στέφανος Γκρίτζαλης.
4. Δικτύωση Υπολογιστών. Τέταρτη Έκδοση.
   JamesF. Kurose – KeithW. Ross.
   Επιστημονική επιμέλεια: Α. Μανίτσαρης, Ι. Μαυρίδης, Π. Φουληράς. Εκδόσεις: Μ. Γκιούρδας.
5. Neuman Clifford. Kerberos: An Authentication Service for Computer Networks.
6. Βασικές Αρχές Ασφάλειας Δικτύων. Εκδόσεις Κλειδάριθμος. WilliamStallings. Εφαρμογές και πρότυπα. Τρίτη Αμερικανική Έκδοση.
7. Ηλεκτρονικόβιβλίο. Applying the OSI Seven Layer Network Model to Information Security.Copyright SANS Institute.
8. Understanding Security Using the OSI Model. Copyright SANS Institute.