Α.Τ.Ε.Ι. ΠΑΤΡΑΣ

ΣΧΟΛΗ ΔΙΟΙΚΗΣΗΣ ΚΑΙ ΟΙΚΟΝΟΜΙΑΣ
ΤΜΗΜΑ ΛΟΓΙΣΤΙΚΗΣ

ΘΕΜΑ ΠΤΥΧΙΑΚΗΣ:

«ΑΣΦΑΛΕΙΑ ΜΕΤΑΔΟΣΗΣ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΔΙΑΔΙΚΤΥΟ (INTERNET)»

Εισηγητής: Μουντζούρης Ιωάννης
Σπουδαστής:Κατωπόδης Κωνσταντίνος

ΠΑΤΡΑ 2004

ΠΕΡΙΕΧΟΜΕΝΑ

ΕΙΣΑΓΩΓΗ

Είναι γενικά αποδεκτό ότι το διαδίκτυο(internet) έχει εμφανίσει ραγδαία αύξηση τα τελευταία χρόνια. Οι βασικοί κόμβοι του ήταν κυρίως κατανεμημένοι σε μερικά ακαδημαϊκά ιδρύματα, ερευνητικά εργαστήρια και εταιρείες. Οι χρήστες του διαδικτύου ήταν άνθρωποι που ασχολούνταν κατά κύριο λόγο με την τεχνολογία και τις επιστήμες. Η υποδομή του είχε σχεδιαστεί για να λειτουργεί απλά και αποτελεσματικά, χωρίς να περιλαμβάνει ιδιαίτερους μηχανισμούς ή «δικλίδες» ασφαλείας.
Ασφάλεια: μια λέξη-ακριβέστερα, μια έννοια-που δεν απασχολούσε ιδιαίτερα τους πρώτους κυβερνοναύτες. Βεβαίως, σχετικά νωρίς είχαν εκδηλωθεί κάποια ανησυχητικά φαινόμενα, όπως η διάδοση ιών, μη εξουσιοδοτημένες προσβάσεις σε συστήματα κ.α., ωστόσο τα κρούσματα ήταν μεμονωμένα και- παρά την ταλαιπωρία που προκαλούσαν στους υπεύθυνους διαχειριστές συστημάτων- αντιμετωπίζονταν αποτελεσματικά. Σύντομα, το Διαδίκτυο ξέφυγε από τα στενά ακαδημαϊκά και ερευνητικά πλαίσια, κερδίζοντας τις καρδιές ολοένα και περισσότερων απλών χρηστών, ακόμα και ανθρώπων που δεν είχαν άμεση σχέση με την τεχνολογία και τους υπολογιστές. Η πολυπλοκότητά του ως συστήματος, με την ευρύτερη έννοια, άρχισε να αυξάνει με γοργό ρυθμό, κάνοντας φανερό ότι θα εξαπλωθεί, θα παρεισφρήσει και θα αγκαλιάσει κάθε πλευρά της κοινωνικής και οικονομικής ζωής.
Όπως όμως συμβαίνει και με άλλα συστήματα στη φύση αλλά και στις ανθρώπινες κοινωνίες, από την αύξηση της πολυπλοκότητας δεν προέκυψαν μόνον επιθυμητές «ιδιότητες». Όταν το σύστημα διαβεί ένα συγκεκριμένο κατώφλι- το οποίο, μάλιστα, δύσκολα μπορεί να γίνει διακριτό εκ' των προτέρων-, οι προκύπτουσες ιδιότητες γίνονται δυνητικά επιβλαβείς για τους συμμετέχοντες [και μη] στο σύστημα, ακόμα και για την ίδια την υπόστασή του
Ποια είναι, λοιπόν, τα αρνητικά ή έστω ανησυχητικά φαινόμενα που προκύπτουν από την εξάπλωση του Διαδικτύου; Από όλα όσα μπορεί να παραθέσει κανείς, εμείς θα επικεντρώσουμε την προσοχή μας σε αυτό που αποτελεί και το θέμα του παρόντος αφιερώματος: **στην ασφάλεια.**
Στο Κεφάλαιο 1 αναφερόμαστε στα 8 βασικά αξιώματα της έννοιας "*Ασφάλεια*' και αναλύουμε κάποιους βασικούς για την συνέχεια όρους.
Στο Κεφάλαιο 2 γίνεται μια προσπάθεια προσέγγισης της έννοιας των Δικτύων και της αρχιτεκτονικής τους. Στη συνέχεια αναφερόμαστε στο μοντέλο αναφοράς OSI και στα επίπεδα από τα οποία αποτελείται.
Στο Κεφάλαιο 3 θα αναφερθούμε στις έννοιες της Ταυτοποίησης και Πιστοποίησης και τα μέσα στα οποία αυτές βασίζονται καθώς και στην Πρόσβασης και την Εξουσιοδότηση.

Στο Κεφάλαιο 4 γίνεται αναφορά στο φαινόμενο της Παραβίασης, τις μορφές με τις οποίες εκδηλώνεται και τους τρόπους αντιμετώπισης του.
Στο Κεφάλαιο 5 συναντάμε τα Audit trails (Προγράμματα Παρακολούθησης Ιχνών Χρηστών), τα είδη των Audit αρχείων καθώς και τα εργαλεία για την ανάλυση των Audit trails.
Στο Κεφάλαιο 6 συναντάμε την έννοια της Κρυπτογραφίας όπου και επισημαίνεται η σημασία της στο σύγχρονο διαδικτυακό περιβάλλον. Οι ψηφιακές υπογραφές, τα πιστοποιητικά και οι υπηρεσίες εμπιστοσύνης είναι τα κυριότερα μέρη του κεφαλαίου στα οποία επικεντρώνουμε την προσοχή μας αφού αποτελούν παράλληλα και τα κύρια μέρη του ίδιου του κρυπτογραφικού συστήματος.
Στο Κεφάλαιο 7 αναφερόμαστε στα Ασφαλή Δικτυακά Πρωτόκολλα(Standards) που έχουν αναπτυχθεί για την κρυπτογράφηση της επικοινωνίας εστιάζοντας στα πιο γνωστά από αυτά όπως το SSL, τα PGP&PEM, το PKCS, το S-HTTP, το S-MIME, το X/509.
Τέλος, στο Κεφάλαιο 8 γίνεται μια προσπάθεια ανάλυσης της έννοιας και λειτουργίας, μιας σημαντικής για την ασφάλεια της μετάδοσης δεδομένων στο διαδίκτυο κατηγορίας μηχανισμών, των firewalls. Γίνονται αναφορές στην ασφάλεια που παρέχουν, τις βασικές τεχνικές που χρησιμοποιούν, στην αρχιτεκτονική τους στα πλεονεκτήματα αλλά και στους περιορισμούς τους.

ΚΕΦΑΛΑΙΟ 1^{ο} : Εισαγωγή στην ασφάλεια μετάδοσης δεδομένων στο διαδίκτυο

1.1 Γενικά

Για την ανάπτυξη μιας αποτελεσματικής στρατηγικής ασφάλειας, θα πρέπει να παρακολουθεί κανείς ταυτόχρονα τόσο τις αλλαγές στην τεχνολογία και τις απειλές, οι οποίες ακολουθούν την ταχύτητα εξέλιξης στο internet όσο και ότι συμβαίνει στο ενδοεταιρικό περιβάλλον. Το να αγοράζονται συσκευές ασφαλείας είναι εύκολο, το να γνωρίζουμε όμως τι πραγματικά πρέπει να προστατεύεται και πως, είναι σίγουρα δυσκολότερο.
Απαιτείται μια συνολική μεθοδολογία διαχείρισης της ασφάλειας που να περιλαμβάνει το σχεδιασμό, την ανάπτυξη πολιτικών ασφάλειας και την δρομολόγηση των απαραίτητων διαδικασιών.

- *Τα Πληροφορικά Συστήματα Δεν Είναι Όπως Παλιά.*
  Τα σημερινά πληροφορικά συστήματα προσφέρουν κάθε είδους υπηρεσίες οι οποίες είναι ναι μεν εντυπωσιακές προκαλούν όμως και «αναστάτωση».Μέσα σε ένα π.χ. εταιρικό δίκτυο ταξιδεύουν πλέον δεδομένα φωνής, χρησιμοποιούνται από κοινού αρχεία, ομάδες υπαλλήλων χρησιμοποιούν εφαρμογές διαχείρισης χρόνου κ.λ.π.

Κάθε νέα διαδικτυακή υπηρεσία μπορεί να αποτελεί εργαλείο για αύξηση των πωλήσεων και της ποιότητας στη λειτουργία της εταιρείας γενικότερα.
Ανάμεσα στην τεράστια έκταση αυτού του χώρου του Διαδικτύου και στις παρεχόμενες υπηρεσίες υπάρχουν αναρίθμητες πιθανές οδοί «επίθεσης», δηλαδή συντονισμένης προσπάθειας παραβίασης της ασφάλειας.

1.2 Τα 8 βασικά αξιώματα της ασφάλειας.

Ας δούμε τώρα τα 8 βασικά αξιώματα της ασφάλειας:

1. *Η ασφάλεια υποστηρίζει την αποστολή (σκοπό) του οργανισμού.* Σκοπός της ασφάλειας είναι να προστατεύει τις πολύτιμες πηγές του οργανισμού, όπως οι πληροφορίες, το hardware και το software.
2. *Η ασφάλεια είναι αναπόσπαστο στοιχείο μιας υγιούς διοίκησης.* Όταν οι πληροφορίες ενός οργανισμού και τα πληροφορικά συστήματα του, συνδεθούν με ένα εξωτερικό σύστημα(π.χ. Internet) οι ευθύνες των managers εκτείνονται εκτός του οργανισμού. Αυτό προϋποθέτει γνώση από μέρους τους, ποιες τακτικές ασφάλειας πρέπει να ακολουθηθούν.
3. *Η ασφάλεια συστημάτων πρέπει να είναι αποτελεσματική ως προς το κόστος.* Τα κέρδη και το κόστος της ασφάλειας πρέπει να εξετάζονται προσεχτικά έτσι ώστε να εγγυάται ότι το κόστος αυτής δεν θα ξεπερνά τα αναμενόμενα οφέλη.
4. *Οι ιδιοκτήτες των συστημάτων ασφαλείας έχουν ευθύνες ασφάλειας και έξω από τον οργανισμό τους.* Όταν ένα σύστημα ασφάλειας έχει και εξωτερικούς χρήστες οι ιδιοκτήτες τους έχουν την ευθύνη να μοιραστούν τις απαραίτητες πληροφορίες σχετικά με τα μέτρα ασφάλειας ώστε και οι άλλοι χρήστες να είναι σίγουροι ότι το σύστημα είναι απολύτως ασφαλές.
5. *Οι ευθύνες και η απόδοση ευθυνών στην ασφάλεια θα πρέπει να γίνονται σαφείς.* Η ανάθεση των ευθυνών μπορεί να είναι εσωτερικό θέμα ενός οργανισμού ή και να εκτείνεται και εκτός των ορίων του. Αναλόγως με το μέγεθος του οργανισμού το πρόγραμμα ασφάλειας μπορεί να είναι μεγάλο, μικρό ή και συμπληρωματικό καθήκον ενός διοικητικού υπαλλήλου. Παρ' όλα αυτά ακόμη και οι μικροί οργανισμοί μπορούν να κατασκευάσουν ένα έγγραφο (καταστατικό) που να περιέχει την πολιτική ασφαλείας τους και να αποδίδει σαφείς ευθύνες ασφάλειας.
6. *Η ασφάλεια απαιτεί μια κατανοητή και ολοκληρωμένη προσέγγιση.* Για την αποτελεσματική τους χρήση τα συστήματα ασφάλειας συχνά στηρίζονται στην ορθή χρήση των άλλων συστημάτων. Γι' αυτό και υπάρχουν πολλές τέτοιες αλληλοεξαρτήσεις. Τα σωστά διαλεγμένα διοικητικά, λειτουργικά και τεχνικά όργανα ελέγχου μπορούν να συνεργάζονται, αλλά αν δεν κατανοηθεί η σχέση αλληλοεξάρτησης των συστημάτων ελέγχου μπορούν ακόμα και να υποβαθμίζουν το ένα το άλλο. π.χ. χωρίς την κατάλληλη εκπαίδευση του πότε και πως χρησιμοποιείται ένα πακέτο ανίχνευσης ιών, ο χρήστης μπορεί να τοποθετήσει το πακέτο λάθος άρα και αναποτελεσματικά. Σαν αποτέλεσμα ο χρήστης λανθασμένα πιστεύει ότι αφού το σύστημά του έχει ελεγχθεί μια φορά θα είναι πάντα ασφαλής από ιούς, και εν αγνοία του να εξαπλώσει έναν ιό.

7. *Η ασφάλεια θα πρέπει περιοδικά να επαναξιολογείται.* Οι υπολογιστές και το περιβάλλον στο οποίο λειτουργούν είναι δυναμικό. Υπάρχει μια συνεχής αλλαγή και ανανέωση. Πολλές μορφές αλλαγών επηρεάζουν την ασφάλεια συστημάτων: τεχνολογικές αναπτύξεις, σύνδεση με εξωτερικά δίκτυα, αλλαγές στην αξία ή χρήση πληροφοριών ή η εμφάνιση μιας νέας απειλής.
8. *Η ασφάλεια δέχεται πιέσεις (παραβιάζεται) από κοινωνικούς παράγοντες.* Η ικανότητα της ασφάλειας να υποστηρίζει την απόσταση ενός οργανισμού μπορεί να περιορίζεται από κάποιους κοινωνικούς φορείς. Κοινώς η ασφάλεια είναι συνυφασμένη με ένα σύστημα τεχνολογίας πληροφοριών με το να αναγνωρίζει (ταυτοποιεί) τους χρήστες και να ανιχνεύει τις πράξεις τους. Παρ' όλα αυτά οι προσδοκίες της (privacy) μυστικότητας ποικίλουν και μπορεί να παραβιαστούν με διάφορα μέτρα ασφαλείας. Ενώ τα προσωπικά δεδομένα και η μυστικότητα είναι ένας πολύ σημαντικός παράγοντας, δεν είναι ο μόνος. Η ροή των πληροφοριών μεταξύ π.χ. κυβέρνησης- πολιτών είναι ακόμη μι κατάσταση όπου η ασφάλεια μπορεί να πρέπει να μετασχηματιστεί έτσι ώστε να υποστηρίζει ένα κοινωνικό σκοπό. Επιπρόσθετα κάποια μέτρα ταυτοποίησης και πιστοποίησης μπορεί να θεωρηθούν ως μέτρα εισβολής για κάποιες κουλτούρες και κάποια περιβάλλοντα. Γι' αυτό λοιπόν τα μέτρα ασφάλειας θα πρέπει να επιλέγονται και να εφαρμόζονται αναγνωρίζοντας τα δικαιώματα και τα νόμιμα ενδιαφέροντα των άλλων.

1.3 Βασικοί Όροι.

Για την καλύτερη κατανόηση των όσων πρόκειται να αναφερθούν , όσον αφορά το θέμα της ασφάλειας, ο αναγνώστης θα πρέπει να είναι εξοικειωμένος με τους ακόλουθους όρους-κλειδιά και ορισμούς.
Οι όροι *«υπολογιστές» και «συστήματα υπολογιστών» ή «υπολογιστικά συστήματα» (computer systems)* χρησιμοποιούνται για την αναφορά σε όλο το φάσμα της τεχνολογίας πληροφοριών, συμπεριλαμβανομένων των συστημάτων εφαρμογών και υποστήριξης.
Άλλοι όροι κλειδιά συμπεριλαμβάνουν:
«Ασφάλεια υπολογιστών» (computer security): Η προστασία που παρέχεται σε ένα αυτοματοποιημένο σύστημα πληροφοριών με σκοπό την επίτευξη των εφαρμόσιμων στόχων, της διατήρησης της ακεραιότητας, διαθεσιμότητας και εμπιστευτικότητας των πόρων των συστημάτων πληροφοριών (συμπεριλαμβάνοντας hardware, firmware, πληροφορίες /δεδομένα και τηλεπικοινωνίες).
«Ακεραιότητα»(Integrity): Μια πληροφορία είναι ακέραιη όταν είναι επίκαιρη, ολοκληρωμένη, ακριβής και συνεπής. Παρ' όλα αυτά οι υπολογιστές δεν έχουν την δυνατότητα να παρέχουν ή να προστατέψουν όλες αυτές τις σταθερές. Γι' αυτό στο πεδίο ασφάλειας

του υπολογιστή, η ακεραιότητα θεωρείται ότι πρέπει να διαχωρίζεται σε δύο μορφές: *Ακεραιότητα δεδομένων και ακεραιότητα συστήματος.*
Η *ακεραιότητα δεδομένων* είναι η αξίωση ότι τα προγράμματα και οι πληροφορίες αλλάζουν μόνο με έναν συγκεκριμένο και εξουσιοδοτημένο τρόπο .
Η *ακεραιότητα συστημάτων* είναι η αξίωση ότι ένα σύστημα εκτελεί την προκαθορισμένη του λειτουργία με αμείωτο τρόπο, ελεύθερο και ανεπηρέαστο, από μη εξουσιοδοτημένη παρέμβαση και εκμετάλλευση του. Ο ορισμός της ακεραιότητας αποτελούσε και συνεχίζει να αποτελεί θέμα συζήτησης και ανταλλαγής απόψεων μεταξύ των ειδικών.
«Εμπιστευτικότητα» (Availability): Μία αξίωση που πρεσβεύει ότι ιδιωτικές ή εμπιστευτικές πληροφορίες δεν θα διαρρεύσουν σε μη εξουσιοδοτημένα άτομα.
Ένας ακόμη όρος, στον οποίο θα γίνεται συχνή αναφορά, και στον οποίο το πεδίο εστιάζει περισσότερο το θέμα της ασφάλειας είναι το *Διαδίκτυο(Internet)*, δυο ή περισσότερα δίκτυα δηλαδή, συνδεδεμένα το ένα με το άλλο. Στο κεφάλαιο που ακολουθεί σχετικά με τα δίκτυα θα γίνει αναφορά στη δομή των δικτύων, στα επίπεδα επικοινωνίας και τα πρωτόκολλα (standards).
Βασικοί επίσης όροι στη συνέχεια του συγγράμματος θα είναι:
Η ταυτοποίηση (identification):Οι τρόποι με τους οποίους ένας χρήστης παρέχει μια ισχυριζόμενη ταυτότητα στο σύστημα.
Η πιστοποίηση (authentication):Οι τρόποι απόδειξης της εγκυρότητας αυτού του ισχυρισμού.
Η εξουσιοδότηση (authorization) :Η άδεια χρήσης ενός πόρου σε έναν Η/Υ.
Τα audit trails: τα προγράμματα παρακολούθησης ιχνών χρηστών.
Firewall: Ορίζεται το λογισμικό και ο εξοπλισμός που τοποθετούμενος ανάμεσα στο διαδίκτυο και στο υπό προστασία δίκτυο, επιτρέπει την προσπέλαση των εξωτερικών χρηστών στο προστατευόμενο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά.

1.4. Μια γενική άποψη- Αποτελέσματα

Κατά τη διάρκεια της έρευνας και της καταγραφής στοιχείων για τη δημιουργία συγκεκριμένου συγγράμματος, υπήρξε η ανάγκη του εντοπισμού, είτε μέσα από την διατεθειμένη βιβλιογραφία είτε από άλλες πηγές όπως π.χ. το internet, και καταγραφής διαφόρων πρωτοκόλλων αλλά όχι μια εξαντλητική λίστα, είναι το GSS-API, το TCP/IP, το S/MIME, το SOCKS, το SSC, το X 509, τα οποία όλα στοχεύουν στην προστασία των ανταλλασομένων πληροφοριών στο internet.
Υπάρχουν πολυάριθμα άλλα πρωτόκολλα, αλλά ο σκοπός αυτής της αναφοράς είναι η δημιουργικά μιας πρώτης επαφής του αναγνώστη με τα πρωτόκολλα, όχι με την καθαυτή έννοια τους. Μια πιο σωστή

προσέγγιση των πρωτοκόλλων θα ήταν η παρομοίωση τους με τις ανθρώπινες γλώσσες επικοινωνίας καθώς αυτός είναι ο ρόλος τους μέσα στα δίκτυα, ένας δίαυλος δηλαδή επικοινωνίας.
Ακολουθούν μερικές χρήσιμες διευθύνσεις στο internet όσων αναφορά τα πρωτόκολλα:

- www.diffuse.org/secure.html
- www.w3.org.gr
- www.google.gr
- www-personal.si.umich.edu/~calz/enmlinks
- dir.yahoo.com/computers_and_internet/security_and_encryption

ΚΕΦΑΛΑΙΟ 2° : Δίκτυα

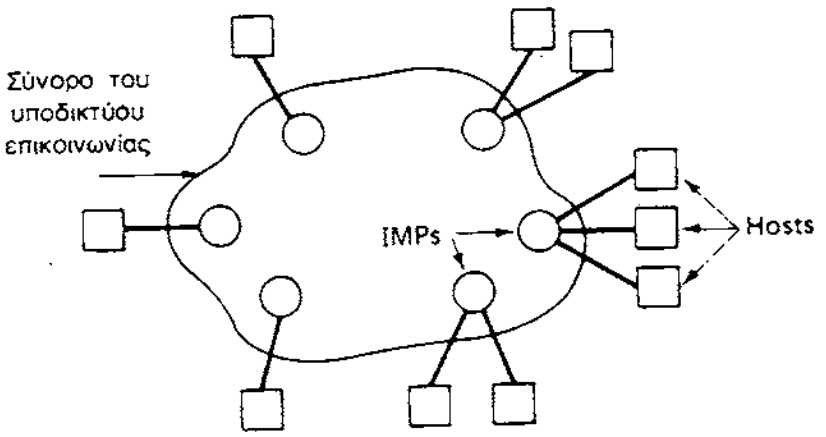
2.1 Γενικά

Σε κάθε δίκτυο υπάρχει μια συλλογή από μηχανήματα που τρέχουν τα προγράμματα του χρήστη και ονομάζονται hosts. Οι hosts συνδέονται μεταξύ τους με ένα υποδίκτυο (communication subnet) του οποίου το έργο είναι η μεταφορά από host σε host. Στο *Σχήμα 1* παρουσιάζεται η σχέση μεταξύ hosts και του υποδικτύου. Στα περισσότερα δίκτυα το υποδίκτυο αποτελείται από τις γραμμές μετάδοσης (transmission lines) και τα στοιχεία μεταγωγής (switching elements). Οι γραμμές μετάδοσης μεταφέρουν bits ανάμεσα στα διάφορα μηχανήματα.

Τα στοιχεία μεταγωγής είναι ειδικοί υπολογιστές που χρησιμοποιούνται για τη σύνδεση δυο η περισσοτέρων γραμμών μετάδοσης. Όταν τα δεδομένα φτάνουν σε μια εισερχόμενη γραμμή το στοιχείο μεταγωγής διαλέγει μια εξερχόμενη γραμμή για να τα μεταδώσει. Η ευρεία ονομασία των στοιχείων μεταγωγής είναι IMPS (Interface Message Processors).

Γενικά υπάρχουν δυο κατηγορίες υποδικτύων:

1. Γενικά κανάλια από σημείο σε σημείο (point to point channels)
2. Με κανάλια εκπομπής (broadcast channels)



Σχ. 1 Σχέση μεταξύ hosts και υποδικτύου.

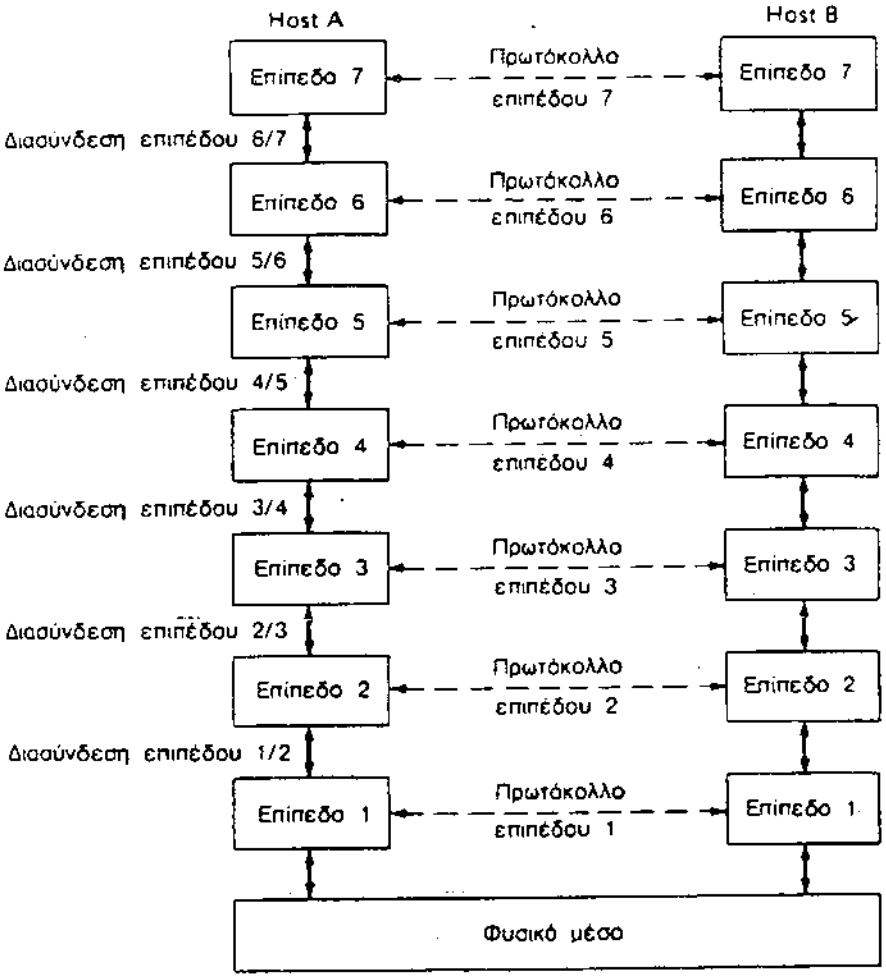
Στην πρώτη κατηγορία, το δίκτυο περιέχει καλώδια ή μισθωμένες τηλεφωνικές γραμμές, που καθεμία συνδέει ένα ζευγάρι IMPS. Όταν ένα μήνυμα στέλνεται από έναν IMP σε ένα άλλο μέσω ενός ή περισσοτέρων IMPS, το μήνυμα λαμβάνεται σε ένα ενδιάμεσο IMP σε όλη του την έκταση, αποθηκεύεται εκεί, έως ότου η γραμμή εξόδου είναι ελεύθερη και μετά προωθείται.

Το δεύτερο είδος αρχιτεκτονικής επικοινωνιών χρησιμοποιεί την εκπομπή-broadcasting. Τα περισσότερα δίκτυα και κάποια δίκτυα ευρείας περιοχής είναι αυτού του είδους. Σε ένα τοπικό δίκτυο το IMP μειώνεται και καταλήγει σε ένα μοναδικό chip ενσωματωμένο μέσα στο host, έτσι ώστε πάντοτε να υπάρχει ένας host για κάθε IMP, σε αντίθεση με το δίκτυο ευρείας περιοχής όπου σε κάθε IMP αντιστοιχούν πολλοί hosts.
Τα συστήματα εκπομπής έχουν μόνο ένα κανάλι επικοινωνίας, το οποίο μοιράζονται όλα τα μηχανήματα που είναι συνδεδεμένα στο δίκτυο. Πακέτα που στέλνονται από οποιονδήποτε υπολογιστή λαμβάνονται από όλους τους υπολογιστές. Ένα πεδίο διεύθυνσης στο πακέτο καθορίζει σε ποιόν απευθύνεται. Με τη λήψη του πακέτου η μηχανή ελέγχει το πεδίο διεύθυνσης. Αν το πακέτο προορίζεται για κάποιο άλλο μηχάνημα απλώς αγνοείται.

2.2 Αρχιτεκτονική Δικτύων

Για την ελάττωση της πολυπλοκότητας της σχεδίασης τα περισσότερα δίκτυα έχουν οργανωθεί σε σειρές από στρώματα ή επίπεδα (layers ή levels) που το καθένα χτίζεται πάνω στο προηγούμενο. Ο αριθμός τους, τα ονόματά τους, τα περιεχόμενά τους και η λειτουργία τους διαφέρουν από δίκτυο σε δίκτυο. Ωστόσο σε όλα τα δίκτυα σκοπός κάθε επιπέδου είναι να προσφέρει συγκεκριμένες υπηρεσίες στα υψηλότερα επίπεδα, απομονώνοντας αυτά τα επίπεδα από τις λεπτομέρειες σχετικά με το πώς πραγματικά υλοποιούνται οι παρεχόμενες υπηρεσίες.
Το επίπεδο «n» μιας μηχανής επικοινωνεί με το επίπεδο «n» μιας άλλης μηχανής. Οι κανόνες και οι συνθήκες αυτής της επικοινωνίας είναι γνωστές ως το πρωτόκολλο του επιπέδου «n» όπως φαίνεται στο *Σχήμα 2.2*. Οι οντότητες που περιλαμβάνονται στα αντίστοιχα επίπεδα σε διαφορετικά μηχανήματα ονομάζονται ομότιμες διεργασίες, οι οποίες είναι αυτές που επικοινωνούν χρησιμοποιώντας το πρωτόκολλο.
Στην πραγματικότητα δεν μεταφέρονται απ' ευθείας δεδομένα από το επίπεδο «n» ενός μηχανήματος στο επίπεδο «n» ενός άλλου. Κάθε επίπεδο περνάει δεδομένα και πληροφορίες ελέγχου στο επίπεδο που βρίσκεται αμέσως κάτω από αυτό μέχρις ότου αυτά φτάσουν στο κατώτατο επίπεδο. Κάτω από το επίπεδο 1 είναι το φυσικό μέσο (physical medium) μέσω του οποίου γίνεται η πραγματική επικοινωνία. Στο *Σχήμα 2* φαίνεται η νοητή επικοινωνία με διακεκομμένες γραμμές, και η φυσική επικοινωνία με συνεχόμενες.
Ανάμεσα σε κάθε ζεύγος γειτονικών επιπέδων υπάρχει μια σύνδεση (interface). Η διασύνδεση καθορίζει ποιες πρωτογενής λειτουργίες και υπηρεσίες προσφέρει ένα επίπεδο στο επίπεδο πάνω από αυτό. Κατά τον σχεδιασμό των δικτύων ένα από τα πιο σημαντικά θέματα είναι ο καθορισμός ξεκάθαρων διασυνδέσεων ανάμεσα στα επίπεδα, έτσι ώστε το κάθε επίπεδο να εκτελεί ένα συγκεκριμένο σύνολο λειτουργιών.

Το σύνολο των επιπέδων και πρωτοκόλλων ονομάζεται αρχιτεκτονική δικτύου. Οι προδιαγραφές της αρχιτεκτονικής θα πρέπει να περιέχουν αρκετές πληροφορίες , ώστε να επιτρέπουν σε ένα κατασκευαστή να γράφει το πρόγραμμα έτσι ώστε αυτό να υπακούει σωστά στο κατάλληλο πρωτόκολλο.



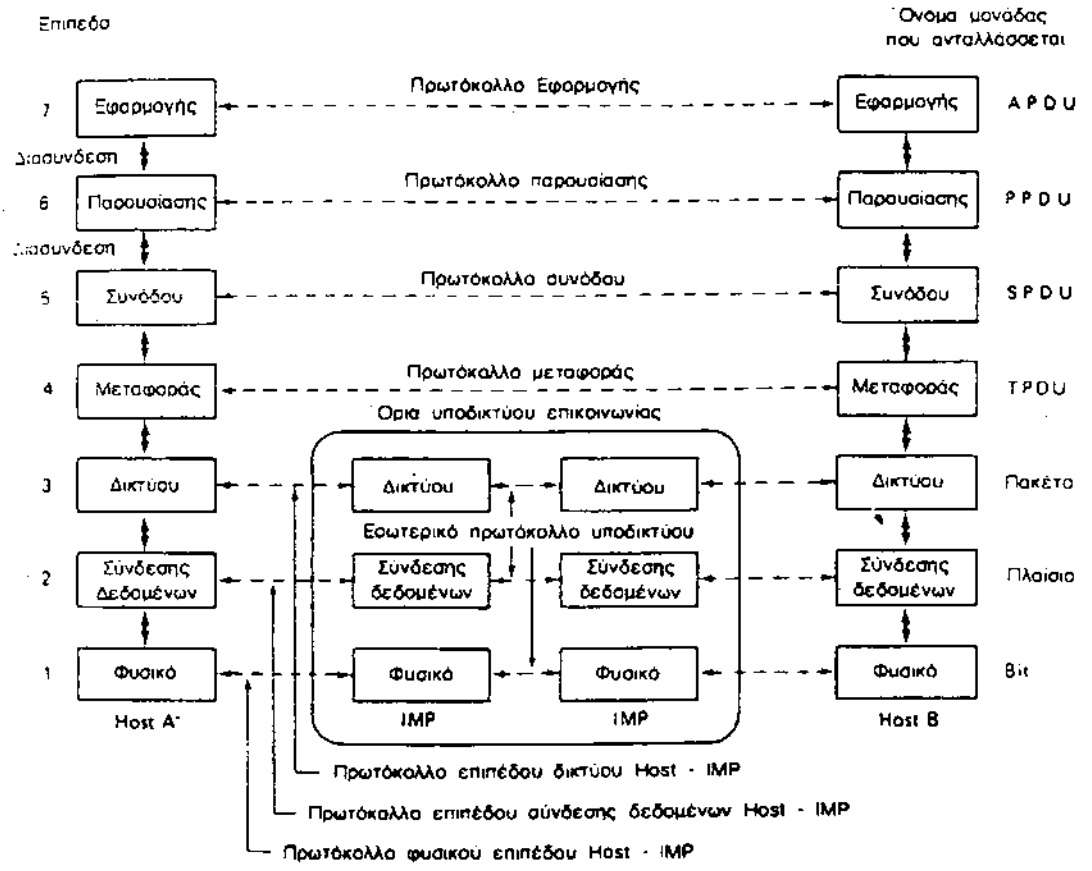
Σχ. 2 Επίπεδα, πρωτόκολλα και διασυνδέσεις.

2.3 Το μοντέλο αναφοράς OSI

Το μοντέλο αναφοράς OSI (Open System Interconnection) ασχολείται με συνδέσεις ανοιχτών συστημάτων, αυτά δηλαδή τα οποία είναι ανοιχτά για επικοινωνία με άλλα συστήματα. Το μοντέλο φαίνεται στο *Σχήμα 3*

Το μοντέλο OSI έχει εφτά επίπεδα. Οι αρχές που εφαρμόζονται για να φτάσουμε σε αυτά είναι οι εξής:

1. Ένα επίπεδο πρέπει να δημιουργείται εκεί όπου χρειάζεται διαφορετικός βαθμός αφαίρεσης.
2. Κάθε επίπεδο πρέπει να εκτελεί μια καλά προσδιορισμένη λειτουργία
3. Η λειτουργία κάθε επιπέδου πρέπει να επιλέγεται με βάση τα καθορισμένα διεθνή τυποποιημένα πρωτόκολλα.
4. Η επιλογή των ορίων των επιπέδων πρέπει να γίνεται με σκοπό την ελαχιστοποίηση της ροής των πληροφοριών μέσω των διασυνδέσεων.
5. Ο αριθμός των επιπέδων θα πρέπει να είναι αρκετά μεγάλος, ώστε διακεκριμένες λειτουργίες να μην χρειάζεται να τοποθετηθούν μαζί στο ίδιο επίπεδο, και αρκετά μικρός ώστε η αρχιτεκτονική να μην γίνεται πολύπλοκη.



Σχ. 3 Η αρχιτεκτονική δικτύου του μοντέλου OSI.

2.3.1. Το Φυσικό Επίπεδο

Το φυσικό επίπεδο ασχολείται με τη μετάδοση ακατέργαστων bits σε ένα κανάλι επικοινωνίας. Τα θέματα σχεδίασης έχουν να κάνουν με τη διασφάλιση ότι, όταν μια πλευρά στέλνει ένα bit 1, αυτό λαμβάνεται από την άλλη ως bit 1 και όχι ως bit 0. Τα θέματα σχεδίασης εδώ ασχολούνται με μηχανικές, ηλεκτρικές και διαδικασιακές συνδέσεις καθώς και το φυσικό μετάδοσης, το οποίο βρίσκεται κάτω από το φυσικό επίπεδο.

2.3.2. Το Επίπεδο Σύνδεσης Δεδομένων (Data Ling Layer)

Η κύρια αποστολή του επιπέδου σύνδεσης δεδομένων είναι να μετασχηματιστεί το ακατέργαστο μέσο μετάδοσης σε μια γραμμή ελεύθερη από σφάλματα στο επίπεδο δικτύου. Αυτό επιτυγχάνεται με τη διάσπαση των δεδομένων εισόδου από τον αποστολέα σε πλαίσια δεδομένων, μετάδοσή τους με τη σειρά και επεξεργασία των πλαισίων επιβεβαίωσης λήψης που επιστρέφονται από τον αποδέκτη. Αφού το φυσικό επίπεδο απλώς αποδέχεται και μεταδίδει ένα συρμό bits, η δημιουργία και αναγνώριση των ορίων των πλαισίων εξαρτάται πλέον από το επίπεδο σύνδεσης δεδομένων. Αυτή μπορεί να επιτευχθεί με την επισύναψη ειδικών ακολουθιών bits στην αρχή και το τέλος των πλαισίων. Αν αυτές οι ακολουθίες των bits μπορούν από σύμπτωση να παρουσιαστούν στα δεδομένα, θα πρέπει να ληφθεί ειδική μέριμνα για την αποφυγή της σύγχυσης.
Η εμφάνιση θορύβου στη γραμμή μπορεί να καταστρέψει ολοκληρωτικά το πλαίσιο. Στην περίπτωση αυτή το λογισμικό του επιπέδου σύνδεσης δεδομένων στη μηχανή της αφετηρίας πρέπει να επαναμεταδώσει το πλαίσιο. Ωστόσο οι πολλαπλές μεταδόσεις του ίδιου πλαισίου δημιουργούν τη δυνατότητα να υπάρξουν αντίγραφα πλαισίων, ένα από τα οποία θα μπορούσε να σταλεί αν καταστραφεί το πλαίσιο επιβεβαίωσης λήψης που επιστρέφει ο δέκτης στον πομπό.
Ένα άλλο θέμα στο επίπεδο σύνδεσης δεδομένων είναι η συγκράτηση ενός γρήγορου πομπού για να μην πλημμυρίσει με δεδομένα έναν αργό δέκτη. Θα πρέπει να εφαρμοστεί κάποιος μηχανισμός ρύθμισης της κυκλοφορίας για να γνωρίζει ο πομπός πόσο χώρο στην ενδιάμεση μνήμη (buffer) έχει ο δέκτης.

2.3.3. Το Επίπεδο Δικτύου

Το επίπεδο δικτύου ασχολείται με τον έλεγχο της λειτουργίας του υποδικτύου. Ένα βασικό θέμα στη σχεδίαση είναι ο καθορισμός του τρόπου δρομολόγησης των πακέτων από την αφετηρία στον προορισμό τους. Οι διαδρομές θα μπορούσαν να βασιστούν σε στατικούς πίνακες

οι οποίοι είναι καλωδιομένοι στο δίκτυο και σπάνια τροποποιούνται. Θα μπορούσαν να οριστούν στην αρχή κάθε συνομιλίας, ή να καθορίζονται εκ νέου για κάθε πακέτο για να απεικονίζουν το τρέχον φορτίο του δικτύου.

Εάν στο υποδίκτυο είναι παρόντα πολλά πακέτα την ίδια χρονική στιγμή θα μπλοκάρει το ένα στην διαδρομή του άλλου δημιουργώντας συμφόρηση (bottleneck). Ο έλεγχος μιας τέτοιας συμφόρησης επίσης ανήκει στο επίπεδο δικτύου.

2.3.4. Το Επίπεδο Μεταφοράς

Η βασική λειτουργία του επιπέδου μεταφοράς είναι η αποδοχή δεδομένων από το επίπεδο συνόδου ή διάσπαση αυτών σε μικρότερες μονάδες αν χρειαστεί, η μεταφορά τους στο επίπεδο δικτύου και η διασφάλιση ότι όλα τα τμήματα φτάνουν σωστά στην άλλη πλευρά.

Υπό κανονικές συνθήκες το επίπεδο μεταφοράς δημιουργεί μια ξεχωριστή σύνδεση δικτύου για κάθε σύνδεση μεταφοράς που απαιτείται από το επίπεδο συνόδου. Αν ωστόσο η σύνδεση μεταφοράς απαιτεί υψηλό ρυθμό εξυπηρέτησης, το επίπεδο μεταφοράς μπορεί να δημιουργήσει πολλαπλές συνδέσεις δικτύου μοιράζοντας τα δεδομένα. Από την άλλη αν η δημιουργία μιας σύνδεσης δικτύου είναι ακριβή το επίπεδο μεταφοράς μπορεί να πολύ πλέκει πολλές συνδέσεις μεταφοράς στην ίδια σύνδεση δικτύου. Ο πιο γνωστός τρόπος σύνδεσης μεταφοράς είναι ένα ελεύθερο από σφάλματα, από σημείο σε σημείο κανάλι, το οποίο παραδίδει μηνύματα με τη σειρά που έχουν σταλεί.

Το επίπεδο μεταφοράς είναι ένα αληθινό επίπεδο από την αφετηρία στον προορισμό ή από άκρο σε άκρο. Ένα πρόγραμμα στη μηχανή αφετηρίας συνομιλεί με ένα παρόμοιο πρόγραμμα της μηχανής προορισμού, χρησιμοποιώντας τις επικεφαλίδες του μηνύματος και τα μηνύματα ελέγχου. Στα κατώτερα επίπεδα τα πρωτόκολλα είναι ανάμεσα σε κάθε μηχανή και στις άμεσα γειτονικές της μηχανές και όχι ανάμεσα σ' αυτές τις τελικές μηχανές αφετηρίας και προορισμού, οι οποίες μπορεί να χωρίζονται από πολλά IMPS. Οι διαφορές ανάμεσα στα επίπεδα 1 έως 3, τα οποία είναι αλυσιδωτά, και στα επίπεδα 4 έως 7, τα οποία είναι από άκρο σε άκρο, φαίνονται στο *Σχήμα 2.3*

2.3.5. Το Επίπεδο Συνόδου

Το επίπεδο συνόδου επιτρέπει στους χρήστες διαφορετικών μηχανημάτων να εγκαθιστούν συνόδους μεταξύ τους. Μια σύνοδος επιτρέπει μια συνήθη μεταφορά δεδομένων, όπως και το επίπεδο μεταφοράς αλλά παρέχει και μερικές πρόσθετες υπηρεσίες.

Μια από αυτές είναι η δυνατότητα διαχείρισης ελέγχου ενός διαλόγου. Οι σύνοδοι μπορούν να επιτρέψουν την κυκλοφορία και προς τις δυο κατευθύνσεις την ίδια στιγμή ή προς την μια κατεύθυνση κάθε στιγμή.
Μια σχετική υπηρεσία συνόδου είναι η διαχείριση κουπονιού. Για μερικά πρωτόκολλα είναι βασικό. Για να μην επιχειρούν και οι δυο πλευρές την ίδια λειτουργία ταυτόχρονα, το επίπεδο συνόδου παρέχει κουπόνια τα οποία μπορούν να ανταλλαγούν. Μόνο η πλευρά που κατέχει το κουπόνι μπορεί να εκτελέσει την κρίσιμη λειτουργία.
Μια ακόμη λειτουργία συνόδου είναι ο συγχρονισμός. Κατά την μεταφορά ενός αρχείου διάρκειας 2 ωρών ανάμεσα σε δυο μηχανές σε ένα δίκτυο με μέσο χρόνο λειτουργίας, μεταξύ 2 καταρρεύσεων σε 1 ώρα, μετά τη διακοπή κάθε μεταφοράς, ολόκληρη η μεταφορά θα πρέπει να αρχίζει ξανά από την αρχή. Γι' αυτό το επίπεδο συνόδου παρέχει έναν τρόπο για την εισαγωγή σημείων ελέγχου, έτσι ώστε μετά την κατάρρευση μόνο τα δεδομένα που ακολουθούν το τελευταίο σημείο ελέγχου πρέπει να επαναληφθούν.

2.3.6. Το Επίπεδο Παρουσίασης

Το επίπεδο παρουσίασης εκτελεί συγκεκριμένες λειτουργίες οι οποίες ζητούνται αρκετά συχνά από τους χρήστες για να εξασφαλίζουν μια γενική λύση γι' αυτούς ώστε να μην αφήνεται κάθε χρήστης να λύνει τα προβλήματα του μόνος του. Ενώ όλα τα κατώτερα επίπεδα ενδιαφέρονται μόνο για την αξιόπιστη μετακίνηση bits από το ένα μέρος στο άλλο, το επίπεδο παρουσίασης ενδιαφέρεται για το συντακτικό και τη σημασιολογία των πληροφοριών.
Ένα τυπικό παράδειγμα υπηρεσίας παρουσίασης είναι η κωδικοποίηση δεδομένων σε ένα κώδικα που συμφωνήθηκε στη διαδρομή. Τα περισσότερα προγράμματα του χρήστη δεν ανταλλάσσουν τυχαίες σειρές bits. Ανταλλάσσουν στοιχεία, όπως ονόματα ανθρώπων, ημερομηνίες, ποσά χρημάτων και τιμολόγια. Αυτά τα στοιχεία παριστάνονται ως σειρές χαρακτήρων, ακέραιοι αριθμοί, αριθμοί κινητής υποδιαστολής και δομές δεδομένων που αποτελούνται από πολλά απλούστερα στοιχεία. Επειδή διαφορετικοί υπολογιστές έχουν διαφορετικούς κώδικες για την αναπαράσταση σειρών χαρακτήρων, ακέραιων κ.λ.π. οι δομές των δεδομένων που θα ανταλλαγούν πρέπει να καθοριστούν με ένα συγκεκριμένο τρόπο, μαζί με την τυποποιημένη κωδικοποίηση που θα χρησιμοποιηθεί «πάνω στο καλώδιο». Η διαχείριση αυτών των αφηρημένων δομών δεδομένων και η μετατροπή τους από την αναπαράσταση που χρησιμοποιείται μέσα στον υπολογιστή στην τυποποιημένη αναπαράσταση δικτύου, αντιμετωπίζεται από το επίπεδο παρουσίασης.

2.3.7. Το Επίπεδο Εφαρμογής

Το επίπεδο εφαρμογής περιέχει μια ποικιλία πρωτοκόλλων που χρειάζονται συχνά. Για παράδειγμα υπάρχουν εκατοντάδες τύποι τερματικών στον κόσμο. Έστω το πρόβλημα κειμενογράφου με πλήρη οθόνη (full screen editor) ο οποίος χρησιμοποιείται σε ένα δίκτυο με πολλούς διαφορετικούς τύπους τερματικών, το καθένα με διαφορετική παρουσίαση οθόνης, διαφορετικές διαδικασίες επεξεργασίας κειμένου κ.λ.π.

Ένας τρόπος επίλυσης του προβλήματος είναι ο καθορισμός ενός αφηρημένου νοητού τερματικού δικτύου. Για το χειρισμό κάθε τύπου τερματικού πρέπει να γραφτεί ένα τμήμα λογισμικού για την αντιστοίχιση των λειτουργιών του νοητού τερματικού πάνω στο πραγματικό. Π.χ. όταν ο editor μετακινεί τον δρομέα στην αριστερή γωνία της οθόνης του νοητού τερματικού, η κίνηση αυτή πρέπει να γίνεται και στο πραγματικό τερματικό. Όλο το λογισμικό του νοητού τερματικού βρίσκεται στο επίπεδο εφαρμογής.

Μια άλλη λειτουργία του επιπέδου εφαρμογής είναι η μεταφορά αρχείων, όπως επίσης και το ηλεκτρονικό ταχυδρομείο, η εισαγωγή εργασιών από απόσταση και διάφορες άλλες γενικού και ειδικού σκοπού ευκολίες.

ΚΕΦΑΛΑΙΟ 3^{Ο} : Ταυτοποίηση και Πιστοποίηση

3.1 Γενικά

Η ταυτοποίηση και πιστοποίηση είναι ένα κρίσιμο συστατικό στοιχείο της ασφάλειας συστημάτων, από τη στιγμή που είναι η βάση για τους περισσότερους τύπους τεχνικών προσβάσεως, αλλά και για την επιβολή απόδοσης ευθυνών. Η ταυτοποίηση και η πιστοποίηση είναι ένα τεχνικό μέτρο που αποτρέπει μη εξουσιοδοτημένα άτομα (ή μη εξουσιοδοτημένες διαδικασίες) από το να εισέλθουν σε ένα σύστημα Τ.Π. Ο έλεγχος προσβάσεως συνήθως απαιτεί το σύστημα να είναι ικανό να αναγνωρίζει και να διακρίνει μεταξύ των χρηστών. Για παράδειγμα, ο έλεγχος προσβάσεως συχνά βασίζεται στο «ελάχιστο προνόμιο», το οποίο αναφέρεται στη χορήγηση στους χρήστες αυτών των προνομίων και μόνο, τα οποία του επαρκούν για την πραγματοποίηση των καθηκόντων τους, και μόνο.

- Ταυτοποίηση είναι οι τρόποι με τους οποίους ένας χρήστης παρέχει μια ισχυριζόμενη ταυτότητα στο σύστημα.
- Πιστοποίηση είναι οι τρόποι απόδειξης της εγκυρότητας αυτού του ισχυρισμού.

Η πιστοποίηση παρουσιάζει αρκετές προκλήσεις: συλλογή στοιχείων πιστοποίησης, μετάδοση των στοιχείων αυτών με ασφάλεια και γνώση κατά πόσο το άτομο που αρχικά πιστοποιήθηκε είναι ακόμη το άτομο που χρησιμοποιεί τον Η/Υ. Για παράδειγμα ένας χρήστης μπορεί να απομακρυνθεί από το τερματικό του όσο είναι ακόμη συνδεδεμένος και κάποιος άλλος να παρέμβει και να το χρησιμοποιήσει.
Υπάρχουν τρεις τρόποι πιστοποίησης της ταυτότητας ενός χρήστη που μπορούν να χρησιμοποιηθούν μόνοι ή σε συνδυασμό.

- Κάτι που μόνο ο χρήστης γνωρίζει
- Κάτι που ο χρήστης κατέχει
- Κάποια ιδιότητα του χρήστη

3.2 Ταυτοποίηση και Πιστοποίηση βασισμένη σε κάτι που γνωρίζει ο χρήστης.

Η πιο κοινή μορφή ταυτοποίησης και πιστοποίησης είναι μια ταυτότητα χρήστη συνδυασμένη με μια λέξη κλειδί (password). Αυτή η τεχνική είναι βασισμένη αποκλειστικά σε κάτι που ο χρήστης γνωρίζει. Υπάρχουν και άλλες τεχνικές εκτός από τα συμβατικά password, που είναι βασισμένες στη γνώση, όπως η γνώση ενός κρυπτογραφικού κλειδιού.

3.2.1 Κωδικοί Πρόσβασης(Passwords.)

Γενικά τα συστήματα λειτουργούν απαιτώντας από το χρήστη να εισάγει την ταυτότητά του και ένα password (ή συνθηματική φράση ή προσωπικό αριθμό ταυτοποίησης). Το σύστημα συγκρίνει το password με ένα προηγούμενο αποθηκευμένο password για αυτή την ταυτότητα χρήστη. Αν ταιριάζουν ο χρήστης πιστοποιείται και του παρέχεται πρόσβαση.

Α. *Πλεονεκτήματα passwords*: Τα passwords παρέχουν επιτυχώς ασφάλεια στα συστήματα Η/Υ εδώ και πολύ καιρό. Έχουν εφαρμοστεί σε πολλά λειτουργικά συστήματα και οι χρήστες είναι εξοικειωμένοι με αυτά. Με σωστή διαχείριση σε ένα ελεγχόμενο περιβάλλον μπορούν να παρέχουν αποτελεσματική ασφάλεια.

Β. *Προβλήματα passwords*: Η ασφάλεια ενός συστήματος που χρησιμοποιεί password εξαρτάται από την διατήρηση του password μυστικού. Δυστυχώς υπάρχουν πολλοί τρόποι το μυστικό να διαρρεύσει. Όλα από τα παρακάτω προβλήματα μπορούν να εκλείψουν με τη βελτίωση των συστημάτων αυτών.

Β1: Μαντεύοντας ή βρίσκοντας το password. Όταν οι χρήστες διαλέγουν οι ίδιοι το password τείνουν να βρίσκουν κάτι εύκολο, για να το θυμούνται, κάτι το οποίο κάνει το password να «μαντευτή». Ονόματα παιδιών, κατοικίδιων, αγαπημένων ομάδων κ.λ.π. είναι κοινά παραδείγματα. Από την άλλη τα ανατεθειμένα passwords είναι συχνά δύσκολο να τα θυμούνται γι' αυτό συνήθως οι χρήστες τα σημειώνουν κάπου. Μια άλλη μέθοδος εύρεσης password είναι η παρατήρηση του χρήστη την ώρα που εισάγει το password ή το P.I.N. συνήθως από κάποιον μέσα στον ίδιο χώρο ή μέσω κάποιου μέσου παρακολούθησης.

Β2: Κοινοποιώντας το password.
Πολλοί χρήστες μοιράζονται το password τους. Μπορεί να δίνουν το password τους σε ένα συνάδελφο για να έχουν και οι δυο πρόσβαση σε κάποια αρχεία. Κατά τη διαδικασία αυτή μπορεί το password να διαρρεύσει και να χρησιμοποιηθεί από λάθος άτομο.

Β3: Μέσω ηλεκτρονικής παρακολούθησης.
Όταν τα password μεταδίδονται μπορεί να παρακολουθηθούν ηλεκτρονικά. Αυτό μπορεί να συμβεί στο δίκτυο που χρησιμοποιείται για τη μετάδοση ή στο τερματικό το ίδιο. Η απλή κρυπτογράφηση δεν λύνει το πρόβλημα, γιατί κρυπτογραφώντας το ίδιο password, θα δημιουργηθεί το ίδιο κρυπτογραφημένο κείμενο' το κρυπτογραφημένο κείμενο γίνεται το password.

Β4: Πρόσβαση στο φάκελο με τα passwords.
Αν ο φάκελος με τα passwords δεν προστατεύεται από ισχυρά κριτήρια προσβάσεως, μπορεί να γίνει down loud. Ακόμα και αν ο φάκελος είναι κρυπτογραφημένος όταν γίνει down loud μπορεί να παραβιασθεί και να βρεθεί το password.

Γ. *Μέθοδοι Προστασίας των Passwords.*
Όπως αναφερθήκαμε και παραπάνω, μερικά από τα βασικά προβλήματα ασφάλειας των passwords μπορούν να εκλείψουν αν ακολουθήσουν κάποιες βασικές αρχές ασφάλειας. Παρ' όλα αυτά τώρα δεν υπάρχει λύση για το πρόβλημα της ηλεκτρονικής παρακολούθησης εκτός από την χρήση πιο προηγμένης πιστοποίησης.

Γ1: Γεννήτριες passwords.
Αν οι χρήστες δεν επιτρέπεται να δημιουργούν τα δικά τους passwords, μπορούν να διαλέξουν εύκολα- να βρεθούν- passwords. Κάποιες γεννήτριες δημιουργούν απλά προφερόμενα passwords άνευ σημασίας και έννοιας για να τα θυμούνται εύκολα οι χρήστες. Παρ' όλα αυτά οι χρήστες τείνουν να σημειώνουν τα δύσκολα passwords.

Γ2: Όρια στις προσπάθειες πρόσβασης.
Πολλά λειτουργικά συστήματα ρυθμίζονται έτσι ώστε να κλειδώνουν την ταυτότητα ενός χρήστη ύστερα από ένα προκαθορισμένο αριθμό από αποτυχημένες προσπάθειες πρόσβασης. Αυτό συμβάλλει στην αποφυγή εύρεσης του password τυχαία.

Γ3: Ιδιότητες των passwords.
Οι χρήστες μπορούν να διδαχθούν, ή το σύστημα να τους αναγκάσει να διαλέγουν passwords:

(1) με ένα συγκεκριμένο ελάχιστο μήκος
(2) με ειδικούς χαρακτήρες
(3) που να μην έχουν σχέση με την ταυτότητά τους
(4) που να μην είναι σε ένα on-line λεξικό.

Όλα τα παραπάνω κάνουν τα passwords πιο δύσκολα να βρεθούν (αλλά πιο πιθανό να σημειωθούν κάπου).

Γ4: Αλλάζοντας passwords.
Η περιοδική αλλαγή των passwords μπορεί να μειώσει τη ζημιά που μπορεί να έχει γίνει από κλεμμένα passwords, και να κάνει τις βίαιες προσπάθειες παραβίασης να πέσουν πάνω σε πιο δύσκολα συστήματα. Οι πολύ συχνές αλλαγές βέβαια μπορεί να είναι ενοχλητικές για τους χρήστες.

Γ5: Τεχνική προστασία των φακέλων password.
Οι τεχνικές ελέγχου προσβάσεως και η κρυπτογραφία «μιας οδού» μπορεί να χρησιμοποιηθεί τον ίδιο τον φάκελο με τα passwords.

3.3. Ταυτοποίηση και Πιστοποίηση βασισμένη σε κάτι που ο χρήστης κατέχει.

Παρότι κάποιες τεχνικές βασίζονται αποκλειστικά σε κάτι που ο χρήστης κατέχει, οι πιο πολλές από τις παρακάτω τεχνικές συνδυάζονται με κάτι που ο χρήστης ξέρει. Αυτός ο συνδυασμός μπορεί να παρέχει σημαντικά ισχυρότερη ασφάλεια παρά κάτι που ο χρήστης κατέχει ή γνωρίζει ξεχωριστά.
Τα αντικείμενα που ο χρήστης κατέχει για τον σκοπό της ταυτοποίησης και πιστοποίησης καλούνται κουπόνια (tokens). Αυτά χωρίζονται σε δυο κατηγορίες: κουπόνια μνήμης και έξυπνα κουπόνια.

3.3.1 Κουπόνια (tokens) μνήμης.

Τα κουπόνια αποθηκεύουν, αλλά δεν επεξεργάζονται, πληροφορίες. Ειδικές συσκευές ελέγχουν την ανάγνωση και γραφή των στοιχείων από και προς τα κουπόνια. Ο πιο κοινός τύπος κουπονιού μνήμης είναι μια μαγνητική ριγέ κάρτα, στην οποία μια λεπτή ρίγα από μαγνητικό υλικό είναι προσαρμοσμένη στην επιφάνειά της (όπως π.χ. στο πίσω μέρος των πιστωτικών καρτών). Μια κοινή εφαρμογή κουπονιού μνήμης για πιστοποίηση σε ένα σύστημα Η/Υ είναι η κάρτα αυτόματου ταμειακού μηχανήματος(Α.Τ.Μ.). Αυτή χρησιμοποιεί ένα συνδυασμό από κάτι που ο χρήστης κατέχει (κάρτα) και κάτι που ο χρήστης γνωρίζει (PIN).
Πλεονεκτήματα συστημάτων κουπονιών μνήμης:
Τα κουπόνια μνήμης όταν χρησιμοποιούνται με PINS παρέχουν σημαντικά περισσότερη ασφάλεια από ότι τα passwords. Επιπρόσθετα, οι κάρτες μνήμης έχουν μικρό κόστος παραγωγής. Για έναν hacker ή άλλον θα ήταν υποκρισία να παριστάνει κάποιον άλλον, ο hacker πρέπει να έχει και ένα ισχύων κουπόνι αλλά και το ανταποκρινόμενο PIN. Αυτό είναι πολύ πιο δύσκολο από την εξασφάλιση του συνδυασμού ισχύοντος password και ταυτότητας χρήστη.
Ακόμη ένα πλεονέκτημα των κουπονιών είναι ότι μπορούν να χρησιμοποιηθούν στην υποστήριξη της παραγωγής πρόσβασης, χωρίς την ανάγκη ο υπάλληλος να εισάγει μια ταυτότητα χρήστη για κάθε συναλλαγή ή άλλο γεγονός από τη στιγμή που το κουπόνι μνήμης μπορεί να ανιχνευθεί επανειλημμένα. Αν το κουπόνι απαιτείται για φυσική είσοδο και έξοδο, τότε τα άτομα θα υποχρεούνται να αφαιρέσουν το κουπόνι όταν απομακρύνονται από τον Η/Υ.
Προβλήματα με τα κουπόνια μνήμης:

Παρά το ότι περίπλοκες σύγχρονες τεχνικές επίθεσης είναι πιθανές ενάντια στα συστήματα κουπονιών μνήμης, τα πιο πολλά προβλήματα σχετίζονται με αυτά αναφέρονται στο κόστος τους, την απώλειά τους, δυσαρέσκεια του χρήστη, και την έκθεση των PINS.

1. Απαιτούνται ειδικοί «αναγνώστες».
   Η ανάγκη για έναν ειδικό αναγνώστη αυξάνει το κόστος της χρήσης κουπονιού μνήμης. Οι αναγνώστες που χρησιμοποιούνται για κουπόνια μνήμης πρέπει να εμπεριέχουν τόσο την φυσική μονάδα που διαβάζει την κάρτα όσο και τον επεξεργαστή που καθορίζει πότε η κάρτα και το PIN είναι έγκυρα. Αν το PIN επικυρωθεί από έναν επεξεργαστή που δεν είναι φυσικά τοποθετημένος με τον ανιχνευτή, τότε η πιστοποίηση των δεδομένων είναι ευαίσθητη.
2. Απώλεια των κουπονιών.
   Η απώλεια του κουπονιού μνήμης π.χ. κάρτας μπορεί να εμποδίσει τον χρήστη από το να συνδεθεί έως ότου αυτή αντικατασταθεί. Το απολεσθέν κουπόνι μπορεί να βρεθεί από κάποιον που να προσπαθήσει να μπει στο σύστημα, ή μπορεί να έχει κλαπεί ή ξεχασθεί. Αν το κουπόνι χρησιμοποιείται σε συνδυασμό με PIN, οποιαδήποτε από τις προηγούμενες μεθόδους αναφορικά με τα προβλήματα των passwords, μπορεί να χρησιμοποιηθεί για την εξεύρεση του PIN. Συχνές μέθοδοι είναι η εύρεση του PIN σημειωμένο πάνω στην κάρτα ή η παρατήρησή του κατά την διάρκεια εισαγωγής του από τον νόμιμο χρήστη.
3. Δυσαρέσκεια Χρήστη.
   Γενικώς οι χρήστες θέλουν οι υπολογιστές να είναι εύκολοι στη χρήση. Πολλοί χρήστες το βρίσκουν άβολο να μεταφέρουν και να επιδεικνύουν έναν κουπόνι. Παρ' όλα αυτά, η δυσαρέσκεια μπορεί να μειωθεί αν συμμεριστούν την ανάγκη για αυξανόμενη ασφάλεια.

3.3.2 Έξυπνα κουπόνια

Ένα έξυπνο κουπόνι επεκτείνει τη λειτουργικότητα ενός κουπονιού μνήμης, συγχωνεύοντας ένα ή περισσότερα ενοποιημένα κυκλώματα μέσα στο κουπόνι το ίδιο. Όταν χρησιμοποιείται για πιστοποίηση, το έξυπνο κουπόνι είναι ακόμη ένα παράδειγμα πιστοποίησης βασισμένης σε κάτι που ο χρήστης κατέχει. Συνήθως απαιτείται και η χρήση κάποιου στοιχείου που ο χρήστης γνωρίζει (PIN) έτσι ώστε το κουπόνι να «κλειδωθεί».
Υπάρχουν διάφοροι τύποι έξυπνων κουπονιών. Γενικά όμως χωρίζονται σε 3 κατηγορίες: τα φυσικά χαρακτηριστικά, επιφάνεια εργασίας, πρωτόκολλα.

- *Φυσικά Χαρακτηριστικά:*

Τα έξυπνα κουπόνια μπορούν να χωριστούν σε 2 γκρουπ: έξυπνες κάρτες και άλλοι τύποι κουπονιών. Μια έξυπνη κάρτα μοιάζει με πιστωτική κάρτα, αλλά εμπεριέχει έναν ενσωματωμένο μικροεπεξεργαστή. Οι έξυπνες κάρτες έχουν προδιαγραφές που καθορίζονται από τον International Standards Organization (ISO). Τα έξυπνα κουπόνια που δεν είναι έξυπνες κάρτες μπορεί να μοιάζουν με υπολογιστές, κλειδιά ή άλλα μικρά φορητά αντικείμενα.

- *Interface: Περιβάλλον επικοινωνίας.*

Τα έξυπνα κουπόνια έχουν χειροκίνητο ή ηλεκτρονικό interface, έτσι ώστε με τη χρήση οθονών και πληκτρολογίων να επιτρέπεται στους ανθρώπους να επικοινωνούν με την κάρτα.

- *Πρωτόκολλα.*

Υπάρχουν πολλά πιθανά πρωτόκολλα που ένα έξυπνο κουπόνι μπορεί να χρησιμοποιήσει για πιστοποίηση. Γενικώς χωρίζονται σε τρεις κατηγορίες:

α) Στατικά κουπόνια: Λειτουργούν παρόμοια με τα κουπόνια μνήμης, εκτός από το ότι οι χρήστες πιστοποιούν τον εαυτό τους στο κουπόνι και ύστερα το κουπόνι πιστοποιεί τους χρήστες στον υπολογιστή.

β) Δυναμικές γεννήτριες passwords: Το κουπόνι που τις χρησιμοποιεί δημιουργεί μια μοναδική λέξη, π.χ. ένα 8ψήφιο password που αλλάζει περιοδικά (κάθε λεπτό).

γ) Προτροπή- Απάντηση: Τα κουπόνια που χρησιμοποιούν πρωτόκολλο προτροπής-απάντησης λειτουργούν έχοντας τον υπολογιστή να δημιουργεί μια προτροπή, όπως μια τυχαία σειρά αριθμών. Τότε, το έξυπνο κουπόνι δημιουργεί μια απάντηση βασισμένη στην προτροπή αυτή. Αυτή στέλνεται πίσω στον υπολογιστή, που πιστοποιεί τον χρήστη βασισμένο στην απάντηση. Το πρωτόκολλο προτροπής απάντησης βασίζεται στην κρυπτογραφία.

3.3.2.1 Πλεονεκτήματα έξυπνων κουπονιών.

Τα έξυπνα κουπόνια προσφέρουν μεγάλη ευελιξία και μπορούν να χρησιμοποιηθούν για να λύσουν πολλά προβλήματα πιστοποίησης. Τα πλεονεκτήματα τους ποικίλουν, εξαρτώμενα από τον τύπο που χρησιμοποιείται. Τα έξυπνα κουπόνια μπορούν να λύσουν το πρόβλημα της ηλεκτρονικής παρακολούθησης αν η πιστοποίηση γίνεται σε ανοικτό δίκτυο με χρήση password «μιας φοράς».

1. Passwords « μιας φοράς»: Τα έξυπνα κουπόνια που χρησιμοποιούν είτε δυναμική γεννήτρια password είτε πρωτόκολλο προτροπής-απάντησης μπορούν να δημιουργήσουν password μιας φοράς. Έτσι κάθε φορά ο χρήστης πιστοποιείται στον υπολογιστή με διαφορετικό password.
2. Μειωμένος κίνδυνος πιστοποίησης: Γενικά, η μνήμη ενός έξυπνου κουπονιού δεν είναι αναγνώσιμη αν δεν εισαχθεί το PIN.

Επιπρόσθετα τα κουπόνια είναι πιο πολύπλοκα, άρα και πιο δύσκολο να παραποιηθούν.

3. Πολύ-εφαρμογές: Τα έξυπνα κουπόνια όπως π.χ. οι έξυπνες κάρτες, παρέχουν ένα τρόπο στους χρήστες να έχουν πρόσβαση σε πολλούς υπολογιστές, χρησιμοποιώντας πολλά δίκτυα με μόνο μια σύνδεση.

3.3.2.2. Προβλήματα έξυπνων κουπονιών.

Όπως και στα κουπόνια μνήμης, πολλά προβλήματα σχετιζόμενα με τα έξυπνα κουπόνια σχετίζονται με το κόστος, τη διοίκηση του συστήματος και τη δυσαρέσκεια του χρήστη.

1. Απαιτείται υψηλός εξοπλισμός καθώς και αυξημένη ανθρώπινη μεσολάβηση: Τα έξυπνα κουπόνια χρησιμοποιούν είτε ηλεκτρονική διασύνδεση είτε ανθρώπινη μεσολάβηση. Η ηλεκτρονική διασύνδεση απαιτεί έναν reader (αναγνώστη) που προϋποθέτει αυξημένο κόστος. Η ανθρώπινη μεσολάβηση για την πραγματοποίηση της διασύνδεσης απαιτεί πολλές ενέργειες από τον χρήστη. Αυτό είναι ιδιαίτερα έντονο στα κουπόνια που χρησιμοποιούν πρωτόκολλο προτροπής-απάντησης όταν ο χρήστης πρέπει να εισάγει την πρόκληση στο δείγμα και την απάντηση στον υπολογιστή.
2. Ουσιώδης διαχείριση: Τα έξυπνα κουπόνια όπως τα passwords και τα κουπόνια μνήμης, απαιτούν ουσιώδη διαχείριση από τον χρήστη.

3.4. Ταυτοποίηση και Πιστοποίηση βασισμένη σε κάποια ιδιότητα του χρήστη.

Οι τεχνολογίες βιομετρικής πιστοποίησης χρησιμοποιούν τα μοναδικά χαρακτηριστικά ενός ατόμου για να πιστοποιήσουν την ταυτότητα του. Αυτά εμπεριέχουν φυσιολογικά χαρακτηριστικά (όπως αποτυπώματα, γεωμετρία χεριού, σχήμα αμφιβληστροειδούς χιτώνα) ή στοιχεία συμπεριφοράς (όπως χροιά φωνής και υπογραφές χειρόγραφες). Η βιομετρική πιστοποίηση που βασίζεται πάνω σε αυτά τα χαρακτηριστικά έχει αναπτυχθεί για αιτήσεις πρόσβασης σε υπολογιστές.
Τα βιομετρικά συστήματα μπορούν να προσφέρουν ένα υψηλό επίπεδο ασφάλειας, η τεχνολογία τους όμως δεν είναι τόσο ώριμη όσο αυτή των δειγμάτων μνήμης και των έξυπνων δειγμάτων. Ατέλειες στα βιομετρικά συστήματα πηγάζουν από την δυσκολία μέτρησης των φυσικών χαρακτηριστικών λόγω ακριβώς της μεταβλητής φύσης τους. Για παράδειγμα η βιομέτρηση φωνής μπορεί να επηρεαστεί από ένα κρυολόγημα του χρήστη που θα αλλοιώσει την χροιά της.

Λόγω λοιπόν των παραπάνω παραγόντων, τα βιομετρικά μέσα πιστοποίησης, σε περιβάλλοντα που απαιτούνται υψηλά επίπεδα ασφάλειας, συνηθίζεται να χρησιμοποιούνται σε συνδυασμό με άλλα μέσα πιστοποίησης.

3.5.Πρόσβαση

Πρόσβαση είναι η δυνατότητα πραγματοποίησης μια ενέργειας με ένα Η/Υ. Τα δικαιώματα πρόσβασης είναι οι βασισμένοι στα συστήματα τρόποι με τους οποίους η δυνατότητα αυτή κατηγορηματικά περιορίζεται ή απαγορεύεται. Τα δικαιώματα πρόσβασης περιγράφουν όχι μόνο ποιος ή τι πρόκειται να έχει πρόσβαση σε ένα συγκεκριμένο σύστημα αλλά και είδος πρόσβασης θα του επιτραπεί. Ακόμη, παρέχουν ένα σύνολο τρόπων τεχνικού ελέγχου των πληροφοριών που ο χρήστης θα χρησιμοποιήσει, των προγραμμάτων που θα τρέξει, και των τροποποιήσεων που θα κάνει.
Συχνά η έννοια της πρόσβασης συγχέεται με αυτή της εξουσιοδότησης όπως και της πιστοποίησης. Εξουσιοδότηση λοιπόν ορίζουνε την άδεια χρήσης ενός πόρου σε ένα Η/Υ. Η άδεια αυτή χορηγείται άμεσα ή έμμεσα, από την εφαρμογή ή τον επικεφαλή του συστήματος.
Όπως και παραπάνω, η πιστοποίηση διαχωρίζεται από την έννοια της πρόσβασης με τον ορισμό της ως το μέσο απόδειξης, (πάντα ως ένα βαθμό), ότι ο χρήστης είναι αυτός που ισχυρίζεται.
Κατά την απόφαση έγκρισης σε κάποιον να χρησιμοποιήσει ένα πόρο του συστήματος τα δικαιώματα πρόσβασης εξετάζουν κατά πόσο ο χρήστης είναι εξουσιοδοτημένος για το τύπο της ζητούμενης πρόσβασης. Το σύστημα χρησιμοποιεί διάφορα *κριτήρια* για να καθορίσει αν η αίτηση για πρόσβαση θα εγκριθεί τα οποία συνήθως χρησιμοποιούνται σε διάφορους συνδυασμούς:

1.Ταυτότητα: Η ταυτότητα είναι συνήθως μοναδική με σκοπό να υποστηρίξει την ατομική λειτουργία, αλλά μπορεί να είναι και η ταυτοποίηση ενός γκρουπ ή και μέσο ανωνυμίας.

2.Ρόλοι: Η πρόσβαση στις πληροφορίες μπορεί ακόμη να ελεγχθεί από τον ρόλο του χρήστη που αναζητεί πληροφορίες. Η διαδικασία προσδιορισμού ρόλων πρέπει να βασίζεται στο πως λειτουργεί ένας οργανισμός.

3.Τοποθεσία: Η πρόσβαση σε συγκεκριμένα συστήματα μπορεί να βασίζεται στην τοποθεσία από όπου αποστέλλεται η αίτηση πρόσβασης. Χρήστες ενός εσωτερικού site ενός οργανισμού πιθανόν να τυγχάνουν ευκολότερης πρόσβασης.

4.Χρόνος: Περιορισμοί σχετικά με την ώρα, τη μέρα, τον μήνα είναι ένας ακόμη τύπος οριοθέτησης της πρόσβασης.

5.Συναλλαγή: Σε οργανισμούς που διεκπεραιώνουν συναλλαγές, πρόσβαση π.χ. σε ένα λογαριασμό χορηγείται μόνο κατά τη διάρκεια της συναλλαγής. Έτσι π.χ. σε ένα Α.Τ.Μ. ο χρήστης κάνοντας μια ερώτηση υπόλοιπου στον λογαριασμό του, έχει πρόσβαση μόνο κατά τη διάρκεια της παροχής της πληροφορίας.

6.Περιορισμοί Υπηρεσιών: Αναφέρονται στις απαγορεύσεις που εξαρτώνται από τις παραμέτρους που μπορεί να ξεπηδήσουν κατά τη χρήση της εφαρμογής ή που έχουν πρώτο τοποθετηθεί από τον κατασκευαστή. π.χ. η χρήση της εφαρμογής από συγκεκριμένο αριθμό χρηστών ή το όριο ανάληψης σε ένα Α.Τ.Μ.

7.Τρόποι Πρόσβασης: Οι κοινοί τρόποι πρόσβασης είναι ανάγνωση, γραφή, εκτέλεση και διαγραφή. Άλλοι πιο εξειδικευμένοι περιέχουν δημιουργία ή αναζήτηση.

3.6. Τεχνική Υλοποίηση

Ένας οργανισμός πρέπει να μελετά εσωτερικές και εξωτερικές τεχνικές πρόσβασης. Ο εσωτερικός έλεγχος πρόσβασης είναι ένας λογικός τρόπος διαχωρισμού τι μπορούν και τι όχι να κάνουν οι χρήστες. Τα εξωτερικά μέτρα ελέγχου πρόσβασης είναι οι τεχνικές ελέγχου της σύνδεσης μεταξύ των συστημάτων και των εξωτερικών, ατόμων, συστημάτων και υπηρεσιών.
Βασικά συστατικά των συστημάτων ελέγχου πρόσβασης οι παρακάτω μηχανισμοί:

1.Λίστες ελέγχου πρόσβασης: Οι λίστες αυτές είναι μια καταχώριση των χρηστών στους οποίους έχει δώσει πρόσβαση σε κάποιο συγκεκριμένο σύστημα.

2.Περιορισμένες Διασυνδέσεις Χρήστη: Η πρόσβαση σε συγκεκριμένες λειτουργίες απαγορεύεται με την μη έγκριση στον χρήστη να απαιτήσει πληροφορίες, λειτουργίες ή άλλες πηγές στις οποίες δεν έχει πρόσβαση.

3.Πύλες Ασφαλείας (Firewalls) : Οι πύλες ασφαλείας μπλοκάρουν ή φιλτράρουν την πρόσβαση μεταξύ δυο δικτύων, συχνά μεταξύ ενός μικρού ιδιωτικού και ενός μεγαλύτερου όπως π.χ. Internet. Επιτρέπουν στους εσωτερικούς χρήστες να συνδέονται με τα εξωτερικά δίκτυα ενώ προστατεύουν τα εσωτερικά συστήματα από έκθεση.

4.Host-based Πιστοποίηση.: Παρέχει πρόσβαση βασισμένη πάνω στην ταυτότητα του host τον οποίο γίνεται η απαίτηση, αντί της ταυτότητας του χρήστη.

ΚΕΦΑΛΑΙΟ 4^{Ο}: Παραβίαση.

4.1. Γενικά.

Τα υπολογιστικά συστήματα είναι ευαίσθητα σε πολλές απειλές που μπορούν να επιβάλλουν διάφορους τύπους ζημιών οδηγώντας σε σημαντικές απώλειες. Οι ζημιές αυτές έχουν ακτίνα δράσης από απλά λάθη που επηρεάζουν την ακεραιότητα της βάσης δεδομένων έως και φωτιές που καταστρέφουν ολόκληρα συστήματα. Η ακρίβεια στην εκτίμηση των απωλειών σχετιζομένων με την ασφάλεια δεν είναι δυνατή. Λόγω του ότι πολλές απώλειες είτε μένουν κρυφές ή δεν ανακαλύπτονται ποτέ λόγω συγκάλυψης.
Για τον έλεγχο των κινδύνων κατά την λειτουργία ενός υπολογιστικού συστήματος πληροφοριών, οι managers και οι χρήστες πρέπει να γνωρίζουν τις ευαισθησίες του συστήματος και τις απειλές που πιθανόν θα αντιμετωπίσουν. Η γνώση αυτή θα τους επιτρέψει να εφαρμόσουν τα μέτρα ασφάλειας με το μικρότερο δυνατό κόστος.

4.2. Λάθη και Παραλείψεις.

Τα λάθη και οι παραλείψεις είναι μια σημαντική απειλή για τα δεδομένα και την ασφάλεια του συστήματος. Αυτά τα λάθη δεν δημιουργούνται μόνο από υπαλλήλους που πραγματοποιούν εκατοντάδες συναλλαγές καθημερινά αλλά και από κάθε χρήστη που δημιουργεί και εκδίδει στοιχεία. Σε κάποιες περιπτώσεις το λάθος είναι η ίδια απειλή, όπως η εισαγωγή ενός λάθος δεδομένου ή ένα προγραμματιστικό λάθος που καταστρέφει το σύστημα. Τα λάθη μπορεί να προκύψουν κατά τη διάρκεια όλων των φάσεων του κύκλου ζωής ενός συστήματος. Σε μια έρευνα του Robert Courtney, σύμβουλος ασφάλειας συστημάτων Η/Υ και πρώην μέλος του Computer Security System and Privacy Board, κατέληξε στο ότι 65% των απωλειών των οργανισμών ήταν αποτέλεσμα λαθών και παραλείψεων. Η έρευνα αφορούσε οργανισμούς τόσο του ιδιωτικού όσο και του δημοσίου τομέα.
Προγραμματιστικά και αναπτυξιακά λάθη, συχνά καλούμενα «bugs" μπορούν να αποδειχθούν από ήπια ως καταστροφικά. Σε μια μελέτη του 1989 για το Mouse Committee on Science, Space and Technology, με τίτλο "Bugs in the Program" το προσωπικό του Subcommittee of Investigations and Oversight συνόψισε το πρόβλημα ως εξής:
«Καθώς οι δαπάνες μεγαλώνουν, την ίδια πορεία ακολουθούν και οι ανησυχίες σχετικά με την αξιοπιστία, το κόστος και την ακρίβεια των μεγαλύτερων και πιο πολύπλοκων συστημάτων software. Αυτές οι ανησυχίες μεγαλώνουν καθώς οι Η/Υ πραγματοποιούν πιο κρίσιμες εργασίες, όπου τα λάθη μπορούν να προκαλέσουν οικονομικές αναταραχές, ατυχήματα ή σε πιο ακραίες καταστάσεις, θανάτους».

Από τη δημοσίευση αυτής της μελέτης, η βιομηχανία software έχει αλλάξει σημαντικά, με ριζικές αλλαγές στην ποιότητα, Οι βασικές αρχές όμως και τα προβλήματα που παρουσιάζει η μελέτη παραμένουν λόγω της ίδιας της φύσης των υπολογιστικών συστημάτων.

4.3. Απάτη και κλοπή.

Τα υπολογιστικά συστήματα μπορούν συχνά να γίνουν μέσα εκμετάλλευσης με σκοπό την απάτη και τη κλοπή. Για παράδειγμα, χρήστες μπορεί μέσω ενός Η/Υ να αποσπούν μικρά ποσά από μεγάλο αριθμό χρηματικών λογαριασμών, στηριζόμενοι στο ότι οι μικρές απώλειες δεν ερευνούνται. Τα οικονομικής φύσης συστήματα δεν είναι τα μόνα που κινδυνεύουν. Στόχο αποτελούν όλα τα συστήματα που παρέχουν πρόσβαση σε σημαντικές πηγές (απογραφικά συστήματα, συστήματα σχολικών βαθμολογιών, τηλεφωνικές γραμμές).
Η απάτη ή η κλοπή διαπράττεται από το εσωτερικό ή το εξωτερικό περιβάλλον. Το U.S Department of Justice' s Computer Crime Unit διατείνεται ότι «η μεγαλύτερη απειλή για τα συστήματα προέρχεται από το εσωτερικό του οργανισμού», Οι εσωτερικού υπάλληλοι, από απλοί χρήστες ως μέλη του τεχνικού επιτελείου, είναι λογικό λόγω της οικειότητας τους με την χρήση και λειτουργία του συστήματος να είναι σε ευνοϊκότερη θέση για την διάπραξη της απάτης. Μεγάλο επίσης κίνδυνο αποτελούν και οι πρώην υπάλληλοι, των οποίων η πρόσβαση δεν έχει τερματίσει σε τελικό βαθμό, των οποίων τα κίνητρα όπως π.χ. αντεκδίκηση μπορεί να τους οδηγήσουν σε προσπάθειες απάτης ή κλοπής.

4.4. Σαμποτάζ υπαλλήλων.

Οι υπάλληλοι είναι πιο εξοικειωμένοι με τους υπολογιστές του οργανισμού στον οποίο εργάζονται με την έννοια ότι γνωρίζουν ποιες πράξεις μπορούν να προκαλέσουν, τη μεγαλύτερη ζημιά, βλάβη ή σαμποτάζ. Το νούμερο των περιπτώσεων σαμποτάζ από υπαλλήλους πιστεύεται ότι είναι πολύ μικρότερο από αυτό των κλοπών, το κόστος όμως αυτών μπορεί να είναι αρκετά υψηλό.
Κοινά παραδείγματα σαμποτάζ υπαλλήλων:

- Καταστροφή hardware ή εγκαταστάσεων
- Εγκατάσταση "login bombs" που καταστρέφουν προγράμματα και δεδομένα
- Λάθος εισαγωγή στοιχείων και δεδομένων
- Καταστροφή συστημάτων
- Διαγραφή δεδομένων
- Παρακράτηση, απόκρυψη και αλλαγή δεδομένων.

Ο Martin J.Prouse, εκδότης του Sabotage in the American Workplace, αναφέρει ότι τα κίνητρα του σαμποτάζ έχουν ακτίνα από τον αλτρουισμό έως την εκδίκηση:
Όσο οι άνθρωποι νιώθουν εξαπατημένοι, βαριεστημένοι, σε κίνδυνο ή προδομένοι στη δουλειά τους, το σαμποτάζ θα χρησιμοποιείται ως η απευθείας μέθοδος επίτευξης ικανοποίησης στο χώρο εργασίας.

4.5. Hackers.

Ο όρος hackers συχνά αναφερόμενος και ως crackers αναφέρεται στους χρήστες που εισβάλλουν σε συστήματα χωρίς εξουσιοδότηση. Η απειλή των hackers θα πρέπει να λαμβάνεται υπ' όψιν από τους οργανισμούς γιατί ενώ οι τρέχουσες απώλειες από επιθέσεις hackers είναι σημαντικά μικρότερες από αυτές των σαμποτάζ και των κλοπών από το εσωτερικό περιβάλλον, το πρόβλημα των hackers είναι σοβαρό και εξαπλώνεται.
Μελέτες του National Research και του Council National Security Telecommunications Advisory Committee έδειξαν πως η δραστηριότητα των hackers δεν περιορίζεται στην απάτη. Περιέχει ακόμη την ικανότητα παραβίασης των τηλεπικοινωνιακών συστημάτων, με αποτέλεσμα τον υποβιβασμό ή και την διάλυση της διαθεσιμότητας του συστήματος.
Η απειλή των hackers συχνά λαμβάνει μεγαλύτερη προσοχή από άλλες πιο συνήθης και επικίνδυνες απειλές. Οι κυριότεροι λόγοι είναι οι εξής:

- Πρώτον, η απειλή των hackers είναι μια πιο πρόσφατα αντιμετωπίσιμη απειλή. Οι οργανισμοί ανησυχούσαν πάντα για τις πράξεις των δικών τους υπαλλήλων και μπορούσαν να χρησιμοποιούν πειθαρχικά μέτρα για να μειώνουν αυτή την απειλή. Τα μέτρα όμως αυτά είναι αναποτελεσματικά απέναντι στους εξωτερικούς εισβολείς που δεν αποτελούν πεδίο δράσης των κανονισμών του οργανισμού.
- Δεύτερον, οι οργανισμοί δεν γνωρίζουν τους σκοπούς του hacker-κάποιοι hackers απλά περιηγούνται, κάποιοι κλέβουν , κάποιοι καταστρέφουν .Αυτή η ανικανότητα αναγνώρισης των σκοπών τους κάνει τις επιθέσεις των hackers απεριόριστες.
- Τρίτον, οι επιθέσεις των hackers κάνουν τους ανθρώπους να νιώθουν ευαίσθητοι, ακριβώς λόγω της ανωνυμίας τους. Ο hacker μπορεί να επιτεθεί στον οργανισμό, την επιχείρηση ή και στον απλό ιδιώτη από παντού αρκεί να έχει στην διάθεση του το κατάλληλο λογισμικό και γνώση. Αυτή η ιδιότητά του κάνει την επίθεση απρόβλεπτη και μη αντιμετωπίσιμη.

4.6. Ιοί και σκουλήκια.

4.6.1. Ιοί στο PC

Στις μέρες της Amiga και των PC XT ο μόνος τρόπος για να «κολλήσεις» κάποιο ειδεχθές πρόγραμμα ήταν να χρησιμοποιήσεις μολυσμένες δισκέτες κυρίως με παιχνίδια. Τότε το να κολλήσεις έναν ιό ήταν κάτι το συνηθισμένο μέχρι και γοητευτικό (θυμάστε ένα μπαλάκι που έκανε βόλτες στην οθόνη;). Βέβαια, το αστείο τέλειωνε όταν ανακάλυπτες ότι οι δισκέτες σου ή ο σκληρός δίσκος σου ήταν άχρηστα. Η κατάσταση άλλαξε δραματικά με την είσοδο του Internet στη ζωή μας, και συγκεκριμένα με το e-mail. Το ηλεκτρονικό ταχυδρομείο εκμηδένισε τις αποστάσεις και έκανε την επικοινωνία ανάμεσα στους εταιρικούς και τους οικιακούς χρήστες πολύ εύκολη και ευχάριστη υπόθεση. Το e-mail όμως είναι προς το παρόν το κυριότερο μέσο για τη μετάδοση κάθε είδους ιών και σκουληκιών, μετατρέποντάς τα σε πραγματική επιδημία λόγω της μεγάλης ταχύτητας με την οποία εξαπλώνονται. Προτού αρχίσετε (ακόμα μια φορά) να τραβάτε τα μαλλιά σας, θα πρέπει να σας πούμε ότι στην συντριπτική τους πλειονότητα οι ιοί, τα σκουλήκια και οι δούρειοι ίπποι δεν μπορούν να προκαλέσουν καμία ζημιά, εάν δεν τρέξετε τα εκτελέσιμα αρχεία /script που τα μεταφέρουν. Η κακόβουλη αυτή εφαρμογή μπορεί να έχει καλυφθεί κάτω από το μανδύα μιας εικόνας ή ενός κειμένου word, παραπλανώντας σας ή κάνοντας πολύ δύσκολο τον εντοπισμό της από το χρήστη. Ας πάρουμε όμως τα πράγματα από την αρχή. Όταν αναφερόμαστε σε ιούς, εννοούμε προγράμματα τα οποία έχουν δημιουργηθεί για να εισέλθουν στον υπολογιστή χωρίς την έγκρισή μας και μολύνουν άλλα αρχεία. Ανάλογα με τη φύση του ιού, οι συνέπειες από τη μόλυνση μπορεί να είναι μηδαμινές έως και καταστροφικές. Ο ιός θα προσπαθήσει να αναπαραχθεί και να εξαπλωθεί, μολύνοντας όσο περισσότερα αρχεία ή άλλους υπολογιστές σε τοπικό επίπεδο ή στο Internet. Υπάρχουν αρκετά είδη ιών: α) αυτοί που προσβάλουν τον τομέα εκκίνησης μιας δισκέτας ή ενός σκληρού δίσκου (boot sector viruses) και είναι σχετικά σπάνιοι σήμερα, β) αυτοί που περιέχονται σε εκτελέσιμα αρχεία (Program/File viruses), γ) αυτοί που εκμεταλλεύονται τις γλώσσες μακροεντολών, όπως π.χ., του Word και του Excel(Micro viruses), και δ) οι πολυμορφικοί, οι οποίοι μπορεί να ανήκουν σε μερικές ή όλες τις προαναφερθείσες κατηγορίες. Υπάρχει και μια ειδική κατηγορία ιών, η οποία εκμεταλλεύεται αδυναμίες γνωστών εφαρμογών, όπως, για παράδειγμα, το Outlook Express, με αποτέλεσμα ένα απλό e-mail κειμένου να μπορεί να κάνει τη ζημιά. Βέβαια οι ιοί αυτοί είναι σπάνιοι και παροπλίζονται με την εγκατάσταση νεότερων εκδόσεων των προβληματικών εφαρμογών. Σε αυτό το σημείο θα σας προτρέψουμε και πάλι να αναβαθμίζεται στη νεότερη έκδοση όλες τις εφαρμογές σας, ειδικά αυτές που σχετίζονται με το Internet. Με αυτό τον τρόπο μειώνετε αρκετά τις πιθανότητες μόλυνσης.

4.6.2. Σκουλήκια-Worms

Τα σκουλήκια (worms) κάνουν χρήση των υπηρεσιών του δικτύου, με ιδιαίτερη προτίμηση στο ηλεκτρονικό ταχυδρομείο, για να πολλαπλασιάζονται και να εξαπλώνονται. Συνήθως δεν μολύνουν αρχεία από τον υπολογιστή που περνούν. Πολύ γνωστές περιπτώσεις, όπως αυτές των Melissa και Love Letter, εξαπλώθηκαν στο δίκτυο με αστραπιαίο ρυθμό. Μάλιστα, το Melissa worm έχει αρχίσει ένα νέο γύρο αυτή τη φορά ως έγγραφο του Office για Mac. Η μέθοδος επίθεσης είναι εξαιρετικά ύπουλη, αφού μόλις καταφέρουν να διεισδύσουν σε ένα υπολογιστή, στέλνουν τα μολυσμένα και καμουφλαρισμένα e-mail σε όλα τη λίστα επαφών του Outlook. Έτσι, ο ανυποψίαστος χρήστης λαμβάνει ένα e-mail από κάποιον γνωστό του και δείχνοντας εμπιστοσύνη ανοίγει το επισυναπτόμενο αρχείο και μαζί και τον ασκό του Αιόλου. Η μαζική αποστολή e-mail, εκτός από την κατασπατάληση του ήδη μικρού εύρους ζώνης του modem σε ατομικό επίπεδο, επιβαρύνει δραματικά τους κεντρικούς διακομιστές αλληλογραφίας του Internet, με αποτέλεσμα να βγαίνουν εκτός λειτουργίας.

4.6.3 Ασπίδες προστασίας

Παρά την ύπαρξη 48.372 ιών, σύμφωνα με το Norton Antivirus, εάν τηρηθούν μερικοί βασικοί κανόνες, ελαχιστοποιούμε τον κίνδυνο μόλυνσης. Εκτός από την αναβάθμιση των εφαρμογών που σχετίζονται με το Internet, είναι πλέον επιβεβλημένη η εγκατάσταση στον υπολογιστή σας κάποιας εφαρμογής προστασίας από τους ιούς. Μετά την εγκατάσταση θα πρέπει να γίνεται εβδομαδιαία ενημέρωση από τους δημιουργούς(μέσω Internet κατά προτίμηση), ώστε να υπάρχει αυξημένο επίπεδο προστασίας απέναντι και στους νεότερους των ιών.
Με την τεράστια εξάπλωση των ιών και των σκουληκιών που χρησιμοποιούν τα e-mail για να εξαπλωθούν, θα πρέπει το αντι-ιικό σας να είναι ικανό να ελέγχει και την εισερχόμενη αλληλογραφία σας. Με αυτό τον τρόπο συλλαμβάνονται τα κακόβουλα προγράμματα, προτού φτάσουν στο ηλεκτρονικό σας γραμματοκιβώτιο. Βέβαια, οι εφαρμογές προστασίας δεν λειτουργούν πάντα καλά, με συνέπεια να παρουσιάζονται περιστασιακά προβλήματα λήψης της αλληλογραφίας σας, αλλά μπροστά στον υπαρκτό κίνδυνο τα συγκεκριμένα προβλήματα είναι αποδεκτά.
Γενικά, ΜΗΝ εκτελείτε επισυναπτόμενα αρχεία, εάν δεν είστε απόλυτα σίγουροι για την καθαρότητά τους. Ακόμα και αν φαίνονται αθώα(μια εικόνα JPG, για παράδειγμα) ή προέρχονται από γνωστό αποστολέα, δεν αποκλείεται το αρχείο να είναι εκτελέσιμο και να έχει την μορφή picture.jpg.exe(όπως π.χ., συμβαίνει σε ένα πρόσφατο δούρειο ίππο του ICQ). Να ξεκαθαρίσουμε ακόμη μια φορά ότι ελάχιστες είναι οι πιθανότητες να μολυνθείτε ανοίγοντας απλώς ένα e-mail για να το

διαβάσετε. Θα πρέπει να εκτελεστεί ο επισυναπτόμενος, καμουφλαρισμένος, κακόβουλος κώδικας. Προσοχή χρειάζεται με τα αρχεία word και excel που λαμβάνετε, τα οποία καλό θα είναι να περνούν από έλεγχο για μακροϊούς. Επίσης, θα πρέπει να προσέξετε και τις διάφορες εφαρμογές που εγκαθίσταται, ειδικά εάν προέρχονται από αμφιλεγόμενες πηγές.
Όλα τα παραπάνω είναι πολύ καλά για την πρόληψη. Τι πρέπει να κάνετε όμως στην περίπτωση που ανακαλύψετε ότι έχετε μολυνθεί από κάποιον ιό; Εάν έχετε γίνει στόχος κάποιου ιού ή κάποιου σκουληκιού που εξαπλώνεται μέσω e-mail, είναι πολύ πιθανό να έλθουν σε επαφή μαζί σας οι άτυχοι ή τυχερού παραλήπτες του ιού. Καλό θα ήταν όμως να έλθετε και εσείς σε επαφή μαζί τους, για να τους ειδοποιήσετε εφόσον το ανακαλύψετε και επιβεβαιώσετε ότι πρόκειται για ιό. Μάθετε να παρατηρείται βασικά χαρακτηριστικά και συμπεριφορές του υπολογιστή σας. Εάν ξαφνικά αρχεία εμφανίζονται ή εξαφανίζονται, το σύστημα γίνεται πιο αργό, μειώνεται η διαθέσιμη μνήμη, εφαρμογές αρνούνται να τρέξουν ή παράξενα μηνύματα εμφανίζονται στην οθόνη σας, είναι καιρός να αρχίσετε να ανησυχείτε. Η αμέσως επόμενη κίνηση είναι να ελέγξετε τον υπολογιστή σας με κάποιο αντι-ιικό (σας παραθέτουμε μερικά από τα καλύτερα). Αφού εντοπιστεί ο ιός και καθαρίσει το σύστημά σας, καλό θα ήταν να δημιουργήστε δισκέτες ασφαλείας, διαδικασία η οποία συνήθως προσφέρεται από το αντι-ιικό πρόγραμμα που χρησιμοποιείτε. Οι δισκέτες αυτές σας δίνουν τη δυνατότητα να εκκινήσετε το σύστημά σας και να κάνετε έλεγχο για ιούς, ενώ μπορεί να παρέχουν και αντίγραφα των τομέων εκκίνησης του σκληρού σας δίσκου σε περίπτωση μόλυνσης του boot sector.

4.6.4. Ιοί πέρα από το PC

Η αυξανόμενη ανάπτυξη της αγοράς των υπολογιστών χειρός αλλά και η σύγκλισή τους με τα κινητά τηλέφωνα ανοίγουν για τους ιούς το δρόμο και προς αυτές τις συσκευές. Ήδη έχει εμφανιστεί το πρώτο κρούσμα-το οποίο είναι και αρκετά «άγριο»- στο Palm OS. Συγκεκριμένα, ο ιός καλύπτεται κάτω από ένα πολύ γνωστό παιχνίδι, το οποίο, εάν τρέξει ο χρήστης, του καταστρέφει απλώς τα περιεχόμενα της μνήμης του. Βέβαια, από τη φύση τους οι υπολογιστές της συγκεκριμένης κατηγορίας δεν είναι πρότυπα ασφάλειας δεδομένων, αφού ο αποθηκευτικός χώρος έχει τη μορφή μνήμης Flash. Γι' αυτόν το λόγο επιβάλλεται η συχνή αντιγραφή ασφάλειας της μνήμης και των περιεχομένων της στο PC. Έτσι, μπορείτε πολύ εύκολα να επαναφέρετε τα δεδομένα σας(φυσικά, όποια από αυτά έχουν αποθηκευτεί στον υπολογιστή παλάμης μετά την αντιγραφή και πριν χτυπήσει ο ιός, θα χαθούν). Ήδη τα πρώτα αντιβιοτικά έχουν κάνει την εμφάνισή τους για το Palm OS και τα Windows CE, ενώ η συνέχεια αναμένεται ενδιαφέρουσα.

Στο στρατόπεδο των κινητών τηλεφώνων επικρατεί σχετική ηρεμία, αφού η σημερινή (τεχνολογική) μορφή των συσκευών δεν ευνοεί την ανάπτυξη ιών. Βέβαια προσφάτως ήλθαν στο φως της δημοσιότητας ειδήσεις για πιθανή ύπαρξη κάποιου ιού που ξαναχτυπά τα κινητά. Κάτι τέτοιο δεν ισχύει, απλώς έχουμε να κάνουμε με μια κακόβουλη εκμετάλλευση ελαττωμάτων ή τρυπών στο λογισμικό ορισμένων κινητών τηλεφώνων. Ένας κωδικός, ο οποίος στέλνεται ως smart message, είναι δυνατόν να προκαλέσει το πάγωμα της συσκευής, με μόνη λύση επαναφοράς στην κανονική λειτουργία την αφαίρεση της μπαταρίας. Πρόκειται για μια κλασική επίθεση DOS. Περισσότερα ευάλωτα είναι τα κινητά που έχουν αρκετά «ανοιχτό» λογισμικό και μπορούν να δεχτούν λογότυπα δικτύων, μελωδίες και εικονομηνύματα μέσω SMS.

4.6.5 Δούρειοι ίπποι-Trojan horses

Δεν θα ήταν υπερβολή, αν λέγαμε ότι ο μεγαλύτερος κίνδυνος μετά τους ιούς, για την πλειονότητα των χρηστών Internet, προέρχονται από δούρειους ίππους [Trojan horses]. Πρόκειται για προγράμματα που αποτελούνται από δύο μέρη, τον πελάτη και τον διακομιστή. Ο διακομιστής «φωλιάζει» με κάποιον τρόπο στον υπολογιστή του θύματος και ο πελάτης τρέχει στο μηχάνημα του θύτη. Από τη στιγμή που ο πελάτης του υπό επίθεση υπολογιστή συνδεθεί με το Internet, το Trojan- διακομιστής, που τρέχει σιωπηρά στο υπόβαθρο [background], στέλνει ένα σήμα το οποίο λαμβάνει το Trojan-πελάτης [στο μηχάνημα του θύτη]. Στη συνέχεια εγκαθιδρύεται μεταξύ τους μια συνεδρία και ο κράκερ αποκτά πρόσβαση στον υπολογιστή-στόχο. Τώρα, ο μακρόθεν έλεγχος του επιτιθέμενου στο άλλο μηχάνημα ποικίλει, αναλόγως του Trojan. Ο πρώτος μπορεί απλώς να παίζει να παίζει με τα νεύρα του ανυποψίαστου χρήστη, π.χ., ανοιγοκλείνοντας το πορτάκι του CD-ROM ή εμφανίζοντας γαργαλιστικά μηνύματα στην οθόνη του. Μπορεί όμως να του διαγράψει αρχεία ή ακόμα και να του προκαλέσει ζημιές στο υλικό του υπολογιστή, όπως π.χ., να του διαγράψει το BIOS ή να «χτυπήσει» τις κεφαλές του σκληρού δίσκου. Μια άλλη, ύπουλη λειτουργία των δούρειων ίππων είναι η παρακολούθηση και η καταγραφή των πλήκτρων που πιέζει το θύμα. Το Trojan- διακομιστής παρακολουθεί συνεχώς τις κινήσεις του χρήστη. Έτσι, όταν εκείνος πληκτρολογεί κωδικούς πρόσβασης ή αριθμούς πιστωτικών καρτών, το πρόγραμμα τα καταγράφει για να τα στείλει αργότερα στο θύτη.

Πως όμως μπορεί να «μπει» ένα Trojan στον υπολογιστή μας;

Ο συνηθέστερος τρόπος είναι να έρχεται ως επισυναπτόμενο σε κάποιο e-mail ή να βρίσκεται κρυμμένο μέσα σε κάποιο άλλο πρόγραμμα, π.χ., σε ένα παιχνίδι freeware ή shareware, σε κάποιο χρήσιμο, διάσημο εργαλείο κ.λ.π. Υπάρχουν δυο τρόποι για να αποφεύγουμε τα Trojan. Ο πρώτος είναι να χρησιμοποιούμε ένα πρόγραμμα "Antivirus" ή "Anti

Trojan". Πολλά προγράμματα του είδους μπορούν να τα ανιχνεύουν όταν τα κατεβάζουμε- ακόμα και στην περίπτωση που είναι ήδη εγκατεστημένα και στο PV μας- και να τα διαγράφουν. Ο άλλος τρόπος είναι να χρησιμοποιούμε ένα προσωπικό firewall. Κάθε φορά που ένα Trojan- διακομιστής θα προσπαθεί να «βγει» στο Internet, το firewall θα μας ειδοποιεί αναλόγως. Είναι προφανές ότι ο συνδυασμός των δυο προηγούμενων μεθόδων παρέχει τη μέγιστη προστασία. Τέλος είναι καλό να κατεβάζουμε στον υπολογιστή μας μόνο «έμπιστα» προγράμματα, από γνωστούς, επίσημους δικτυακούς τόπους.

ΚΕΦΑΛΑΙΟ 5^{Ο}: AUDIT TRAILS (Προγράμματα Παρακολούθησης Ιχνών Χρηστών).

5.1. Γενικά.

Τα audit trails διατηρούν ένα αρχείο της δραστηριότητας του συστήματος. Σε συνδυασμό με τα κατάλληλα εργαλεία και τις διαδικασίες, τα audit trails μπορούν να συμβάλλουν στον εντοπισμό παραβιάσεων ασφαλείας, προβλημάτων απόδοσης και ελαττωμάτων στις εφαρμογές.
Τα audit trails μπορούν να χρησιμοποιηθούν τόσο ως υποστήριξη για κανονικές λειτουργίες ενός συστήματος, όσο και ως ένα είδος ασφάλειας ή σαν και τα δύο. Σαν ένα είδος ασφάλειας, διατηρούνται αλλά δεν χρησιμοποιούνται αν δεν χρειάζεται, ενώ σαν υποστήριξη λειτουργιών χρησιμοποιούνται για να βοηθούν τους επικεφαλείς συστημάτων κατά τον έλεγχο των συστημάτων για τυχόν επιθέσεις, ζημιές ή τεχνικά προβλήματα.
Τα audit trails παρέχουν ένα σύνολο τρόπων για την πραγματοποίηση διαφόρων σχετιζόμενων με την ασφάλεια σκοπών, περιλαμβανομένων:

- του εντοπισμού εισβολέων,
- της ατομικής απόδοσης ευθυνών,
- της αναπαράστασης των γεγονότων
- της ταυτοποίησης του προβλήματος.

Εντοπισμός Εισβολέων:
Αν τα audit trails έχουν σχεδιαστεί και εφαρμοστεί για την καταγραφή των κατάλληλων πληροφοριών μπορούν να βοηθήσουν στον εντοπισμό των εισβολέων. Οι εισβολείς μπορούν να εντοπιστούν σε πραγματικό χρόνο παρακολουθώντας τα αρχεία των audits trails κατά τη δημιουργία τους ή μετά το γεγονός εξετάζοντας τα audits αρχεία σε στοίβες.

Ατομική Απόδοση Ευθυνών:
Τα audit trails είναι ένας τεχνικός μηχανισμός που βοηθά τους managers να διατηρούν τον έλεγχο των πράξεων του κάθε χρήστη όχι κατά την πραγματοποίηση τους αλλά υπό το φάσμα της παρακολούθησης τους άρα και της απόδοσης των αποτελεσμάτων τους.- Έτσι ενώ οι χρήστες δεν μπορούν να παρεμποδιστούν από την χρήση πληροφοριών και δεδομένων στα οποία έχουν νομική και εξουσιοδοτημένη πρόσβαση , η ανάλυση των audit trails μπορεί να χρησιμοποιηθεί για την εξέταση των πράξεών τους.
Η γνώση λοιπόν από τη μεριά των χρηστών ότι οι πράξεις τους καταγράφονται από τα audit trails μειώνει την όποια επιθυμία για εξαπάτηση του οργανισμού από μέρους του και καθιστά ευκολότερη την εποπτεία από την μεριά του manager.

Αναπαράσταση Γεγονότων:
Τα audit trails χρησιμοποιούνται επίσης για την αναπαράσταση των γεγονότων αν προκύψει κάποιο πρόβλημα. Η χρήση τους υποστηρίζει την « μετά το γεγονός» έρευνα για το πώς, πότε και γιατί οι φυσιολογικές λειτουργίες σταματήσουν. Η ανάλυση τους συχνά ξεχωρίζει τις λειτουργικά λάθη (όπου το σύστημα λειτούργησε απολύτων σωστά και σύμφωνα με τον προγραμματισμό του) από τα λάθη του συστήματος.
Ταυτοποίηση Προβλήματος:
Τα audit trails μπορούν ακόμη να χρησιμοποιηθούν σαν on-line εργαλεία, για να βοηθήσουν στην ταυτοποίηση προβλημάτων άλλων, εκτός των εισβολών όπως παρουσιάζονται. Αυτό συχνά αναφέρεται σαν παρακολούθηση σε πραγματικό χρόνο. Μια ανάλυση των audit trails μπορεί να πιστοποιήσει ότι το σύστημα λειτούργησε φυσιολογικά (ότι δηλαδή το λάθος μπορεί να προέκυψε από λειτουργικό λάθος).

5.2. Audits Trails Lots (καταγραφές).

Ένα σύστημα μπορεί να διατηρήσει μια σειρά διαφορετικών audit trails ταυτόχρονα. Γενικά υπάρχουν δυο είδη audit αρχείων: (Α) ένα αρχείο κάθε πληκτρολόγησης συχνά καλούμενο παρακολούθηση πληκτρολόγησης και (Β) ένα ημερολόγιο γεγονότων.

(Α)Παρακολούθηση Πληκτρολόγησης:
Είναι η διαδικασία που χρησιμοποιείται για την προβολή την καταγραφή των πληκτρολογήσεων που πραγματοποιούνται από τον χρήστη και των απαντήσεων του υπολογιστή κατά τη διάρκεια μιας εργασίας. Η παρακολούθηση πληκτρολόγησης θεωρείται μια ειδική περίπτωση audit trails. Παραδείγματα θεωρούνται η παρατήρηση των χαρακτήρων καθώς πληκτρολογούνται από τους χρήστες, η ανάγνωση του e-mail των χρηστών και η παρατήρηση άλλων καταγεγραμμένων πληροφοριών που έχουν εισαχθεί από τους χρήστες.

(Β)Audit γεγονότα:
Τα audit αρχεία συστήματος γενικά χρησιμοποιούνται για την παρακολούθηση της απόδοσης των συστημάτων. Τα audit trails των εφαρμογών χρησιμοποιούνται για να διακρίνουν ελαττώματα σ' αυτές, ή παραβιάσεις της πολιτικής ασφάλειας μέσα σε αυτές. Τα audit αρχεία χρηστών χρησιμοποιούνται για να καθιστούν τους χρήστες υπεύθυνους για τις πράξεις τους. Μια ανάλυση των audit αρχείων χρηστών μπορεί να αποκαλύψει μια ποικιλία παραβιάσεων, με ακτίνα από απλό ξεφύλλισμα, έως προσπάθειες εμφύτευσης Trojan horses ή απάντησης μη εξουσιοδοτημένων προνομίων.
Ας δούμε τα τρία βασικά είδη audit trails:

1. Audit trails επιπέδου συστήματος.
Ένα audit trail συστήματος πρέπει να έχει την ικανότητα να αναγνωρίζει αποτυχημένες προσπάθειες σύνδεσης, ειδικά αν το σύστημα δεν θέτει όριο για τον αριθμό των προσπαθειών αυτών. Δυστυχώς κάποια audit trails επίπεδου συστήματος δεν μπορούν να ανιχνεύσουν προσπάθειες σύνδεσης, άρα και να τις καταγράψουν για μετέπειτα ανάλυση. Αυτά τα audit trails μπορούν μόνο' να παρακολουθήσουν και να καταγράψουν επιτυχημένες προσπάθειες σύνδεσης και τις ενέργειες που ακολουθούν.

2. Audit trails επιπέδου εφαρμογής.
Τα audit trails επιπέδου συστήματος μπορεί να μην έχουν την ικανότητα να ανιχνεύσουν και να καταγράψουν γεγονότα μέσα στις εφαρμογές, ούτε να παρέχουν τις απαραίτητες λεπτομέρειες. Γενικά, τα audit trails επίπεδου εφαρμογής παρακολουθούν και καταγράφουν τις ενέργειες του χρήστη, συμπεριλαμβάνοντας το άνοιγμα και κλείσιμο των αρχείων δεδομένων, ειδικές ενέργειες όπως ανάγνωση, δημιουργία, διαγραφή αρχείων, και εκτύπωση αναφορών.

3. Audit trails χρήστη.
Τα audit trails χρήστη συνήθως καταγράφουν: (1) όλες τις εντολές που ξεκινούν από τον χρήστη, (2) όλες τις προσπάθειες ταυτοποίησης και πιστοποίησης και (3) τα αρχεία και τις πηγές όπου έχει επιτευχθεί η πρόσβαση.

5.3. Εργαλεία για την ανάλυση των audit trails.

Πολλοί τύποι εργαλείων έχουν σχεδιαστεί ώστε να βοηθήσουν στην μείωση του όγκου των πληροφοριών που περιέχονται στα audit αρχεία, όπως και για να ξεχωρίζουν τις χρήσιμες πληροφορίες από της λιγότερης σημασίας.

- Εργαλεία μείωσης όγκου audit αρχείων. Είναι επεξεργαστές σχεδιασμένοι να μειώνουν τον όγκο των audit αρχείων ώστε να διευκολύνουν την εξέτασή τους. Πριν μια τέτοια εξέταση, τα εργαλεία αυτά μπορούν να απομακρύνουν τα όχι μεγάλης σημασίας αρχεία, όσον αναφορά την ασφάλεια.
- Εργαλεία ανίχνευσης τάσεων /αλλαγών. Ερευνούν για ανωμαλίες στην συμπεριφορά του χρήστη ή του συστήματος. Για παράδειγμα, αν ένας χρήστης συνήθως συνδέεται στις εννιά το πρωί, αλλά κάποιο πρωί εμφανίζεται να έχει συνδεθεί στις τέσσερις και μισή αυτό μπορεί να υποδεικνύει ένα πρόβλημα το οποίο πρέπει να εξετασθεί.

- Εργαλεία ανίχνευσης «υπογραφών επίθεσης». Ανιχνεύουν για μια «υπογραφή επίθεσης», που είναι μια ειδική σειρά γεγονότων ενδεικτικά μιας προσπάθειας μη εξουσιοδοτημένης. Ένα απλό παράδειγμα θα ήταν επαναλαμβανόμενες αποτυχημένες προσπάθειες σύνδεσης.

ΚΕΦΑΛΑΙΟ 6^{Ο}: Κρυπτογραφία

6.1 Γενικά.

Για πολλούς ειδικούς, ασφάλεια χωρίς κρυπτογραφία είναι...μισή ασφάλεια. Ακόμα κι αν έχουμε θωρακίσει τον υπολογιστή μας σε βαθμό που να μην «μπαινοβγαίνει» κανείς σε αυτόν χωρίς έγκριση, από τη στιγμή που κάποιοι μπορεί να αποκαλύπτουν και να ερμηνεύουν τα δεδομένα μας στον «αέρα», τότε έχουμε χάσει το μισό παιχνίδι. Λύση αποτελεί η κρυπτογράφηση. Με την κρυπτογράφηση των δεδομένων μας, κάποιος που επιθυμεί να τα υποκλέψει, αδυνατεί να εξάγει πληροφορίες από αυτά.

6.2. Κρυπτογραφία στην εποχή της πληροφορίας.

Σε γενικές γραμμές, μπορούμε να ορίσουμε ένα σύστημα κρυπτογράφησης (cryptographic system) ως ένα μηχανισμό ή αλγόριθμο μετατροπής δεδομένων από μια αρχική μορφή (plaintext) σε μια νέα (cipher text) από την οποία δεν προκύπτει νόημα. Η διαδικασία της κρυπτογράφησης (encryption) απαιτεί την παρουσία ενός κλειδιού (key, στο εξής ke) που δεν είναι τίποτα άλλο από μια ακολουθία χαρακτήρων (string). Η αντίστροφη διαδικασία, η αποκρυπτογράφηση (decryption) απαιτεί επίσης την παρουσία ενός κλειδιού, στο εξής kd. Όταν ισχύει ke=kd μιλάμε για **συμμετρική** κρυπτογραφία, ενώ όταν ke#kd για **ασύμμετρη** κρυπτογραφία ή αλλιώς **δημοσίου κλειδιού**.

Η συμμετρική κρυπτογραφία εφαρμόζεται κυρίως σε μικρά δίκτυα με περιορισμένο αριθμό χρηστών και βασίζεται στην εχεμύθεια, μεταξύ χρηστών που ανταλλάζουν μηνύματα όσον αφορά την αποκάλυψη του κλειδιού σε κάποιον τρίτο.

Σε ένα σύστημα κρυπτογραφίας δημοσίου κλειδιού, οι διαδικασίες κρυπτογράφησης και αποκρυπτογράφησης είναι διαχωρισμένες, υπό την έννοια ότι τα κλειδιά ke και kd είναι διαφορετικά. Κάθε χρήστης ενός τέτοιου συστήματος διαθέτει ένα τουλάχιστον ζεύγος κλειδιών: το ένα ονομάζεται δημόσιο (δ) και το άλλο ιδιωτικό ή μυστικό (μ).

Η γνώση του δ επιτρέπει την κρυπτογράφηση του μηνύματος ενώ για την αποκρυπτογράφηση απαιτείται το μ. Αντίστροφα, η κρυπτογράφηση με το μ, αποκρυπτογραφείται μόνο με το δ.

Από τα προηγούμενα γίνεται φανερό το πλεονέκτημα της ασύμμετρης κρυπτογραφίας έναντι της συμμετρικής, που δεν είναι άλλο από τη διανομή του δημόσιου κλειδιού. Οποιοσδήποτε μπορεί να πάρει το δημόσιο κλειδί ενός χρήστη και να του στέλνει κρυπτογραφημένα μηνύματα, τα οποία «ξεκλειδώνουν» μόνο με το αντίστοιχο μυστικό κλειδί του πρώτου.

Λόγω του ότι ο συμμετρικός αλγόριθμος είναι γενικά πολύ γρηγορότερος από τον ασύμμετρο, σε πολλές πρακτικές εφαρμογές ακολουθείται η μέση οδός, οι υβριδικές μέθοδοι κρυπτογράφησης. Ενώ για την κρυπτογράφηση των δεδομένων ακολουθείται συμμετρικός αλγόριθμος, το κλειδί κρυπτογραφείται, με ασύμμετρο αλγόριθμο. Έτσι, συνδυάζεται το πλεονέκτημα της ταχύτητας της συμμετρικής κρυπτογραφίας με την ασφαλή διανομή του κλειδιού, βάσει των μηχανισμών της ασύμμετρης κρυπτογραφίας.

6.3. Ψηφιακές Υπογραφές.

Τα πλεονεκτήματα της ασύμμετρης (ή υβριδικής) κρυπτογραφίας είναι προφανή, ωστόσο υπάρχει ένα σοβαρό ζήτημα. Ας υποτεθεί ότι παραλαμβάνω ένα μήνυμα ή αρχείο από το χρήστη με ηλεκτρονική διεύθυνση panos@somewhere.net. Υπό φυσιολογικές συνθήκες δεν έχω λόγω να μην εμπιστευθώ τον αποστολέα. Ωστόσο, ένας κακόβουλος χρήστης, μπορεί με ένα e-mail faker πρόγραμμα να μου στείλει μήνυμα με αυτή τη διεύθυνση, να προβεί δηλαδή σε ηλεκτρονική πλαστοπροσωπία, για διάφορους σκοπούς, ενάντια στα δικά μου συμφέροντα.

Αυτό ξεπερνιέται με τη χρήση ψηφιακών υπογραφών (digital signatures). Πριν μιλήσουμε γι' αυτές όμως, ας αναφερθούμε στις συναρτήσεις hash. Πρόκειται για μηχανισμούς που στην είσοδό τους δέχονται ένα οποιοδήποτε μήνυμα ενώ στην έξοδό τους δίνουν ένα αλφαριθμητικό σταθερού μήκους. Εάν το μήνυμα εισόδου μεταβληθεί έστω και ελάχιστα σε σχέση με το προηγούμενο, τότε το αλφαβητικό εξόδου διαφέρει εντελώς.

Ας υποθέσουμε τώρα ότι ο κάτοχος της διεύθυνσης panos@somewhere.net θέλει να μου στείλει ένα μήνυμα (M) και εγώ να είμαι βέβαιος για τη γνησιότητα του. Τότε ο Πάνος δεν έχει παρά να υπογράψει το M. Γι' αυτό τροφοδοτεί αρχικά το M σε μια hash, συνάρτηση, έστω h, παίρνοντας το αλφαριθμητικό εξόδου h(M), τη λεγόμενη σύνοψη μηνύματος. Στη συνέχεια κρυπτογραφεί το h(M) με το μυστικό του κλειδί (μ), λαμβάνοντας έτσι το cipher text s=μ[h(M)]. Όταν το λάβω, για να επικυρώσω την ταυτότητα του αποστολέα, βρίσκω το δημόσιο κλειδί του Πάνου, (δ). Στη συνέχεια χρησιμοποιώντας την ίδια hash, υπολογίζω το h(M) και το συγκρίνω με το δ(s), δηλαδή με το δ[μ[h(M)]]. Αν ισχύει δ(s)=h(M) δέχομαι την υπογραφή ως έγκυρη.

Με την παραπάνω διαδικασία βεβαιώνομαι για τρία πράγματα. Πρώτον ότι το e-mail προήλθε από τον Πάνο αφού μόνο εκείνος μπορούσε να υπολογίσει την υπογραφή s, όντας ο μοναδικός κάτοχος του μυστικού κλειδιού μ. Δεύτερον, από τη στιγμή που ο Πάνος υπέγραψε το μήνυμα M, αυτό δεν θα μπορούσε να αλλάξει στο παραμικρό αφού τότε θα άλλαζε και το h(M) που θα υπολόγιζα άρα η υπογραφή θα ήταν άκυρη

με δ(s)#h(M). Τέλος, ο Πάνος δεν μπορεί να ισχυρισθεί ότι δεν έγραψε το Μ, αφού ανά πάσα στιγμή μπορώ να δείξω ότι δ(s)=h(M).

6.3.1. Αλγόριθμος Περίληψης Μηνύματος MD5

Ο αλγόριθμος MD5 δέχεται σαν input ένα αυθαίρετου μήκους και παράγει σαν output μια περίληψη μηνύματος 128 bit του input. Ο αλγόριθμος MD5 προορίζεται για εφαρμογές ψηφιακών υπογραφών, όπου ένας μεγάλος φάκελος πρέπει να συμπιεστεί με ασφαλή τρόπο πριν κρυπτογραφηθεί με ένα ιδιωτικό κλειδί κάτω από ένα κρυπτοσύστημα δημοσίου κλειδιού όπως το PKCS.Εικάζεται ότι είναι υπολογιστικά αδύνατη η παραγωγή 2 μηνυμάτων που να έχουν την ίδια περίληψη ή η παραγωγή οποιουδήποτε μηνύματος που να έχει προκαθορισμένη και δοσμένη κατεύθυνση περίληψης.

6.4. Αρχές Πιστοποίησης.

Ας υποθέσουμε τώρα ότι παίρνουμε το δημόσιο κλειδί του Πάνου, από κάποιον κατάλογο on-line, ώστε να το χρησιμοποιώ για να του στέλνω κρυπτογραφημένα μηνύματα. Αν όμως ένας cracker γνωρίζει τα στοιχεία του Πάνου και έχει βάλει το δικό του δημόσιο κλειδί στη θέση του Πάνου, κάθε e-mail που θα στέλνω στη διεύθυνση panos@somewhere.net, ο cracker θα μπορεί να το υποκλέπτει και να το διαβάζει αφού στην ουσία θα το έχω κρυπτογραφήσει με το δικό μου κλειδί.
Έτσι λοιπόν θα πρέπει να υπάρχει μια αρχή διαχείρισης των δημόσιων κλειδιών, που να διασφαλίζει ότι το δημόσιο κλειδί δ1 ανήκει στο χρήστη Χ1, το δ2 στον Χ2 κ.λ.π.
Συνήθως η αντιστοίχιση ενός χρήστη στο δημόσιο κλειδί του παρέχεται από ένα πιστοποιητικό (certificate). Το πιστοποιητικό διανέμει η λεγόμενη Αρχή Πιστοποίησης (Certification Authority ή CA) που δεν είναι τίποτα άλλο από έναν οργανισμό ή εταιρεία. Μια τέτοια εταιρεία έχει την ευθύνη της δημιουργίας, της διανομής, της ανάκλησης, της διαχείρισης γενικά των πιστοποιητικών.
Έτσι, ο όποιος ενδιαφερόμενος, θα απευθυνθεί σε μια Αρχή Πιστοποίησης, όπως είναι η Verisign (www.verisign.com). Η Αρχή θα ελέγξει με κάποιον τρόπο την ταυτότητα του, καθώς και ότι το δημόσιο κλειδί (δ) που προσκομίζει του ανήκει. Ακολουθεί η σύνταξη ενός κειμένου, το οποίο θα περιλαμβάνει στοιχεία που τον αφορούν (π.χ. ονομ/μο, δ/νση, e-mail κ.λ.π.), το κλειδί δ, καθώς και άλλα χρήσιμα στοιχεία όπως π.χ. η ημερομηνία που το πιστοποιητικό παύει να ισχύει (expiration date). Στη συνέχεια η Αρχή πιστοποίησης υπογράφει το πιστοποιητικό με το δικό της κλειδί, δημιουργώντας έτσι το πιστοποιητικό του ατόμου. Τώρα, όποιος θέλει το δημόσιο κλειδί του

ατόμου αυτού καθώς και να επιβεβαιώσει ότι είναι δικό του, τότε παίρνει πρώτα το πιστοποιητικό του από ένα κατάλογο on-line. Επαληθεύει την ψηφιακή υπογραφή της Αρχής Πιστοποίησης και αν είναι εντάξει, βεβαιώνεται για τη γνησιότητα του δημόσιου κλειδιού.
Ο λόγος για τον οποίο οι χρήστες εμπιστεύονται μια Αρχή Πιστοποίησης είναι ότι κάποιος άλλος φορέας εγγυάται για την αξιοπιστία της. Για τον τελευταίο φορέα να εγγυάται κάποιος άλλος κ.λ.π., δημιουργώντας έτσι μια αλυσίδα εμπιστοσύνης, στη ρίζα της οποίας υπάρχει μια καθολικά αποδεκτή Αρχή.

6.4.1. Certificates- Πιστοποιητικά.

Ας αναφερθούμε τώρα κάπως εκτενέστερα στην έννοια των πιστοποιητικών.
Ένα από τα κυριότερα τεχνικά στοιχεία στην ασφάλεια μετάδοσης πληροφοριών είναι και το certificate το οποίο είναι ένα ηλεκτρονικό αρχείο που καταχωρεί ένα δημόσιο κλειδί μαζί με το όνομα του συνδρομητή και επιβεβαιώνει ότι ο επίδοξος συνδρομητής που θα εμφανίζεται πάνω στο certificate είναι ο κάτοχος του ανταποκρινόμενου ιδιωτικού κλειδιού.
Ο παραλήπτης ενός certificate μπορεί να χρησιμοποιήσει το δημόσιο κλειδί, καταχωρημένο στο certificate, για να επιβεβαιώσει ότι η ψηφιακή υπογραφή είχε δημιουργηθεί με το ανταποκρινόμενο ιδιωτικό κλειδί. Εάν μια τέτοια επιβεβαίωση είναι επιτυχής, παρέχεται η ασφάλεια ότι η ψηφιακή υπογραφή έχει δημιουργηθεί από τον ιδιοκτήτη του δημόσιου κλειδιού που αναγράφεται στο certificate, και ότι το μήνυμα δεν έχει τροποποιηθεί από την στιγμή που έχει ψηφιακά υπογραφεί.
Η πιο ευρέως γνωστή και αποδεκτή μορφή certificates είναι αυτή που προσδιορίζεται από το ISO/IEC JTC1SC21 γνωστή ως X.509 version 3. Παρέχει υποστήριξη για μια ευρεία γκάμα εφαρμογών και θεωρείται ότι εφαρμόζεται για την υποστήριξη ενός ελαστικού trust μοντέλου ανταποκρινόμενο στις απαιτήσεις του χρήστη. Το X.509V3 είναι γενικά αποδεκτό σαν το «γενικού σκοπού σχήμα certificate δημόσιου κλειδιού».
Δεν είναι εύκολο να προβλεφθεί ο τρόπος με τον οποίο θα αναπτυχθεί η χρήση των certificates. Παράγοντες όπως η αποδοχή από τους χρήστες, η δημόσια πολιτική και η υποστήριξη των πωλητών θα είναι όλοι πολύ σημαντικοί. Ακόμη είναι πιθανόν να υπάρξει ένας πολλαπλασιασμός των τύπων certificates εφάμιλλων του X.509V3 και γίνονται βήματα για την έναρξη των διαδικασιών, όπως η εγγραφή των διάφορων παραλλαγών certificates, για την ελαχιστοποίηση των ποικιλιών τους.
Ο βαθμός κατά τον οποίο ένας χρήστης certificate μπορεί να εμπιστευθεί τον δεσμευτικό χαρακτήρα ενός certificate- ανάμεσα σε ένα όνομα και ένα δημόσιο κλειδί- εξαρτάται από πολλούς παράγοντες

όπως η πολιτική του certification, οι διαδικασίες πιστοποίησης, οι διαδικασίες ελέγχου και ασφάλειας και οι διαδικασίες όπως και η πολιτική διαχείρισης ιδιωτικού κλειδιού. Μια πολιτική certificate επιτρέπει στους χρήστες ενός certificate να αποφασίσουν πόση εμπιστοσύνη μπορούν να έχουν στο certificate.

Ένα κλειδί certificate γενικά περιέχει:

- Πληροφορίες σχετικά με τα σχετιζόμενα κλειδιά, συμπεριλαμβανομένων ανιχνευτών κλειδιών, δείκτες απαγορευμένης χρήσης κλειδιού και δείκτες πολιτικής certificate.
- Εναλλακτική ονόματα για ένα θέμα certificate καθώς και επιπρόσθετες πληροφορίες σχετικά με ένα θέμα certificate.

Μια άλλη μορφή certificate αντί του «full certificate" είναι αυτή του Simple Public Key Infrastructure Certificate (SPKI) – ή αλλιώς «Simple Certificate». Αυτή παρέχει μια συγκεκριμένη εξουσία σε ένα δημόσιο κλειδί αντί να το δέσει με μια ταυτότητα. Π.χ. ένα SPKI certificate μπορεί να δώσει άδεια σε ένα δημόσιο κλειδί να πιστοποιήσει logins σε ένα ορισμένο δίκτυο, για ένα ορισμένο host και για μια συγκεκριμένη περίοδο.

6.5.Υπηρεσίες Εμπιστοσύνης (Trust Services).

6.5.1. Ένα σύστημα εμπιστοσύνης (Trust System)

Ένα σύστημα εμπιστοσύνης είναι ένα περιβάλλον όπου οντότητες (Διοικήσεις, Επιχειρήσεις, Καταναλωτές) ανταλλάσσουν ή συναλλάσσονται μεταξύ τους με την προυπόθεση όλες οι οντότητες είναι αυτές που ισχυρίζονται ότι είναι, ότι δραστηριοποιούνται σύμφωνα με τις λειτουργικές τους υποχρεώσεις και ότι όλες οι συναλλαγές είναι ασφαλείς.

Θα πρέπει να σημειωθεί ότι η «ασφάλεια» είναι ένας υποκειμενικός όρος, αλλά μπορεί να προσδιοριστεί σαν μια αποδεκτή ισορροπία από απειλές εναντίων της ασφαλούς φύλαξης μιας συγκεκριμένης κατάστάσης.

Κέντρο ενός συστήματος εμπιστοσύνης είναι ένα αποδεκτό επίπεδο ασφάλειας για ένα ανατεθέν έργο ή δραστηριότητα.

Στην ανοιχτή και ελεύθερη ανταλλαγή πληροφοριών και συγκεκριμένα στο πλαίσιο του Ηλεκτρονικού εμπορίου (E- commerce) ένα σύστημα εμπιστοσύνης περιλαμβάνει την παρουσία ενός ή περισσοτέρων « τρίτων μερών» που δρουν σαν «μεσάζων» μεταξύ των συναλλασσομένων οντοτήτων. Αυτοί οι «μεσάζοντες» καλούνται Έμπιστα Τρίτα Μέρη (Trusted Third Parties ή TTPS).

Τα TTPS είναι παρόντα στα παραδοσιακά περιβάλλοντα ανταλλαγών π.χ. μια τράπεζα σαν TTP μεταξύ πωλητή και αγοραστή, ή μια εταιρεία συναγερμών σαν μεταξύ του σπιτιού και της αστυνομίας κ.λ.π.

6.5.2. TTPS

6.5.2.1. Managers και Εφαρμογή.

Η λειτουργία ενός TTP είτε εξωτερικά είτε εσωτερικά παρεχόμενη, μόνο να προσθέσει αξία μπορεί όταν οι χρήστες των υπηρεσιών διαβεβαιώνονται για την ποιότητα της εφαρμογής του TTP. Τα παρακάτω θέματα καλούνται «διαβεβαιώσεις» ως προς αυτή την ποιότητα, και η εφαρμογή τους θα πρέπει να ελέγχεται πριν την έναρξη ενός συστήματος που περιλαμβάνει TTP.

- Εμπιστοσύνη
- Διαπίστευση του TTP
- Ποιότητα των παρεχόμενων υπηρεσιών
- Έλεγχος και Έλεγχος και υπευθυνότητα
- Συμμόρφωση με κανονισμούς
- Συμβόλαιο με εταιρεία παροχής
- Διαφάνεια
- Πολιτική κατασκευής.

6.5.2.2. Βασικές Υποχρεώσεις.

Υπάρχει ένας αριθμός νομικών θεμάτων ιδιαίτερου ενδιαφέροντος όσον αναφορά τα TTPS.

- Αρχειοθέτηση και Ανάκτηση: Το επίπεδο των απαιτήσεων για ανάκτηση αρχείου. Το συμβόλαιο με ένα TTP θα πρέπει να είναι σαφές σχετικά με θέματα διατήρησης κλειδιών που χρησιμοποιούνται για απόκρυψη, πιστοποίηση και ψηφιακές υπογραφές, αν αυτά χρειαστεί να αναπαραχθούν πολλά χρόνια μετά τις συναλλαγές για τις οποίες είχαν χρησιμοποιηθεί.
- Υποχρέωση: Υποχρέωση του TTP να περιλαμβάνει στο συμβόλαιο εγγυήσεις σχετικά με την όποια συν λειτουργία του συστήματος ή ζημιά κατά την λειτουργία.
- Μυστικότητα: Ινστιτούτα διαφόρων αρμοδιοτήτων, ειδικά των σχετιζόμενων με οικονομικά και ηθικά επαγγέλματα, είναι υποχρεωμένα να προστατεύουν τα προσωπικά δεδομένα των ατόμων ή των οντοτήτων. Αυτές οι υποχρεώσεις είναι κάποιες φορές σε αντίθεση με την απαίτηση επιβολής νόμου στην πρόσβαση πληροφοριών.

6.5.2.3. Βασικές Υπηρεσίες.

Οι βασικές υπηρεσίες ενός TTP είναι: δημιουργία κρυπτογραφικού υλικού, διανομή κλειδιού, επαναποστολή κλειδιού, πιστοποίηση, καθοδήγηση κ.λ.π. Συχνά όλα αυτά περιέχονται σε αυτό που αποκαλείται « Υποδομή Δημόσιου Κλειδιού».

6.6. Τα Κύρια Μέρη Εμπιστοσύνης.

6.6.1. APIS

Τα APIS πρέπει να είναι διαθέσιμα για ένα αριθμό διασυνδέσεων κρυπτογραφικών υπηρεσιών για την υποστήριξη των υπηρεσιών εμπιστοσύνης περιλαμβάνοντας:

- Παράδοση δημόσιου κλειδιού και διασύνδεση επιβεβαίωσης
- Εξουσία τοπικής εγγραφής
- Δημοσίευση βεβαιώσεων και λίστες επαναποστολής βεβαιώσεων.

6.6.2. Έξυπνες Κάρτες.

Τα standards χρειάζονται συστατικά εμπιστοσύνης όπως έξυπνες κάρτες που απαιτούνται για την υποστήριξη της ασφάλειας των διαφημιστικών και οικονομικών συναλλαγών και πληρωμών που έχουν σχέση με κάρτες.
Οι έξυπνες κάρτες είναι οι πλέον κατάλληλες για να φιλοξενούν κλειδιά ασφαλείας. Αυτό επιτρέπει την κινητή χρήση και παρέχει κάποια πλεονεκτήματα σε όρους ασφαλείας π.χ. είναι ίσως πιο δύσκολο να κλαπεί μια κάρτα παρά να αποκτήσουμε πρόσβαση σε ένα P.C. Για επιπρόσθετη ασφάλεια οι έξυπνες κάρτες μπορούν να περιλαμβάνουν τεχνικές PIN.

6.6.3. Χαρακτηρισμός.

Το ακριβές περιεχόμενο των πληροφοριών που ανταλλάσσονται μεταξύ μερών είναι συχνά άγνωστο. Γι' αυτό ακόμη κι αν ο παραλήπτης διαβεβαιώνεται από την πηγή, το τελικό περιεχόμενο μπορεί να είναι ανεπιθύμητο. Ο χαρακτηρισμός ή τοποθέτηση «ετικέτας» είναι ο τρόπος περιγραφής του περιεχόμενου χωρίς ο παραλήπτης να πρέπει να ανοίξει το «πακέτο» για να το εξετάσει. Το κλειδί σε ένα σύστημα χαρακτηρισμού είναι το είδος των δεδομένων που θα παρέχονται στην ετικέτα και τι θα λένε αυτά τα δεδομένα. Και τα δυο είναι σημαντικά και

καθορίζουν το αν ο παραλήπτης θα προχωρήσει στην αποδοχή και άνοιγμα του πακέτου ή όχι.

Διάφορα standards και προδιαγραφές.

- ANSI X9.5 –Επεκτάσεις στα certificates Δημόσιου Κλειδιού και CRLS.
- ANSI X9.57 –Certificate management για Οικονομικές Υπηρεσίες.
- ISO/IEC 9594-8: 1995: Τεχνολογία Πληροφοριών- Διασύνδεση Ανοιχτών Συστημάτων- Κατάλογος: Πλαίσιο Εργασίας Πιστοποίησης (ITU-T Recommendation X.509). ορισμός του X.509 certificate για δημόσια κλειδιά.
- ISO/IEC 14888: Ψηφιακές υπογραφές με παράρτημα. Το μέρος 3 προσδιορίζει τους βασισμένους σε certificate μηχανισμούς.
- PKCS#6 που περιγράφει ένα σχήμα για certificates που έχουν επεκταθεί.

ΚΕΦΑΛΑΙΟ 7^{Ο}: Πρωτόκολλα-Standards.

7.1. Ασφάλεια Εφαρμογών Διαδικτύου.

Υπάρχουν διάφορες τεχνικές που μπορούν να εφαρμοστούν ώστε να επιτευχθεί το επιθυμητό επίπεδο ασφάλειας των πληροφοριών που είναι αποθηκευμένες σε ένα πληροφοριακό σύστημα και μεταδίδονται στο διαδίκτυο. Τέτοιες είναι οι εφαρμογές κρυπτογράφησης για αυθεντικοποίηση των χρηστών, η κρυπτογραφημένη μεταφορά των δεδομένων, ο έλεγχος πρόσβασης και τα ασφαλή δικτυακά πρωτόκολλα.

Ο έλεγχος πρόσβασης βασίζεται στην αυθεντικοποίηση των χρηστών που ζητούν πρόσβαση στα δεδομένα, με χρήση ψηφιακών πιστοποιητικών που έχουν εκδοθεί από μια αρχή έκδοσης πιστοποιητικών στα πλαίσια μιας Υποδομής Δημοσίου Κλειδιού. Συνήθως τα συστήματα πληροφορικής εξετάζουν αν πρέπει να επιτραπεί η πρόσβαση σε πόρους περιορισμένης χρήσης προτρέποντας τους χρήστες να εισάγουν userid /password και /ή απαιτώντας οι υπολογιστές να διαθέτουν συγκεκριμένες δικτυακές διευθύνσεις (δηλ. IP address πιστοποίηση). Αυτοί οι τρόποι διαχείρισης προσπέλασης έχουν αρκετές δυσκολίες. Π.χ. ο κάθε χρήστης πρέπει να απομνημονεύει έναν συνεχώς αυξανόμενο αριθμό κωδικών οι οποίοι αλλάζουν συχνά και /ή μπορεί μόνο να χρησιμοποιήσει υπολογιστές συνδεδεμένους σε ένα συγκεκριμένο πανεπιστήμιο ή επιχείρηση. Χρησιμοποιώντας πιστοποιητικά για την αυθεντικοποίηση της ταυτότητας των ατόμων που ζητούν πρόσβαση σε πόρους περιορισμένης χρήσης, επιλύονται τα προαναφερθέντα προβλήματα.

Από τη άλλη μεριά, η ύπαρξη των κινδύνων που εγκυμονεί η μετάδοση των δεδομένων μέσα από ανοιχτά δίκτυα, όπως το διαδίκτυο, οδήγησε στην ανάπτυξη ασφαλών δικτυακών πρωτοκόλλων για την κρυπτογράφηση της επικοινωνίας.

7.2. Το πρωτόκολλο SSL

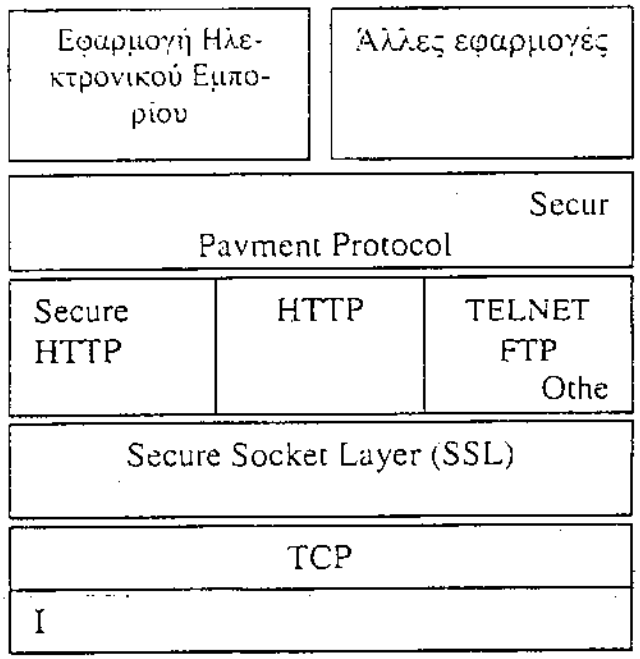
Το SSL (Security Socket Layer) είναι ένα πρωτόκολλο για τη μεταφορά δεδομένων μεταξύ δύο συσκευών, που αναπτύχθηκε για να παρέχει ιδιωτικότητα και ακεραιότητα των πληροφοριών στο Internet. Το SSL διαχειρίζεται την εμπιστευτικότητα και την ακεραιότητα του καναλιού μετάδοσης (με κατάλληλη κρυπτογράφηση των δεδομένων), καθώς και την αυθεντικοποίηση του εξυπηρετητή, αλλά και του πελάτη όταν είναι απαραίτητο.

Το SSL είναι ένα πρωτόκολλο ασφάλειας που σχεδιάστηκε από την Netscape, για να παρέχει ασφάλεια κατά την μετάδοση ευαίσθητων δεδομένων με βάση το πρωτόκολλο TCP/IP. Παρέχει υπηρεσίες:

- κρυπτογράφησης δεδομένων
- αυθεντικοποίηση εξυπηρετητή
- ακεραιότητα (integrity) των μηνυμάτων που μεταδίδονται στο διαδίκτυο.

Η κρυπτογράφηση γίνεται χωρίς να απαιτείται αλληλεπίδραση με τον χρήστη. Η έκδοση SSL 2.0 υποστηρίζει μόνο αυθεντικοποίηση εξυπηρετητή 9server authentication), ενώ η έκδοση SSL 3.0 παρέχει επιπλέον και αυθεντικοποίηση πελάτη (client authentication). Το πρωτόκολλο SSL χρησιμοποιεί το TCP IP για τη μεταφορά των δεδομένων και είναι ανεξάρτητο από την εφαρμογή που χρησιμοποιείται από τον τελικό χρήστη. Γι' αυτό το λόγο μπορεί και παρέχει υπηρεσίες ασφάλειας σε πρωτόκολλα υψηλού επιπέδου όπως TELNET, FTP και HTTP.Στο *Σχ. 4.* φαίνεται η θέση του SSL στην ιεραρχία επιπέδων των πρωτοκόλλων ασφάλειας στο διαδίκτυο.

Ένα άλλο πρωτόκολλο για ασφαλή μετάδοση δεδομένων στον ιστό (WWW) είναι το Secure HTTP (S-HTTP). Ενώ το SSL δημιουργεί μια ασφαλή σύνδεση μεταξύ του πελάτη και του εξυπηρετητή, το S-HTTP σχεδιάστηκε για τη μυστική μετάδοση μεμονωμένων μηνυμάτων. Επομένως, το SSL και το S-HTTP είναι μάλλον συμπληρωματικές παρά ανταγωνιστικές τεχνολογίες.



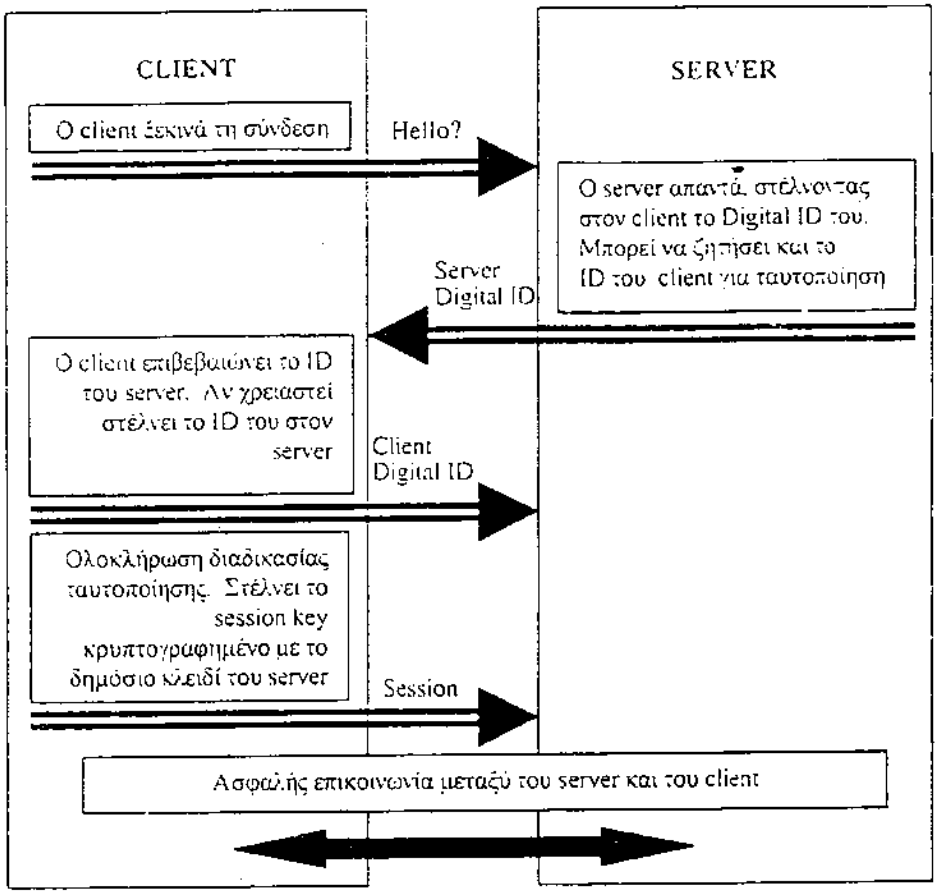
Σχ. 4. Ιεραρχία επιπέδων των πρωτοκόλλων ασφάλειας στο διαδίκτυο

7.2.1. Τρόπος Λειτουργίας του SSL

Το πρωτόκολλο SSL χρησιμοποιεί την RSA κρυπτογράφηση δημοσίου κλειδιού για να εξασφαλίσει την ασφαλή μετάδοση. Έχουμε αναφέρει ότι αυτού του είδους η κρυπτογράφηση χρησιμοποιεί ένα ζεύγος κλειδιών, το δημόσιο κλειδί, για κρυπτογράφηση και αποκρυπτογράφηση. Οποιαδήποτε πληροφορία κρυπτογραφείται με το ένα κλειδί, μπορεί να αποκρυπτογραφηθεί μόνο με το άλλο.
Ένα διαφορετικό κλειδί συνόδου (session key) χρησιμοποιείται σε κάθε σύνδεση πελάτη / εξυπηρετητή. Το κλειδί κάθε συνόδου λήγει με τη συμπλήρωση 24 ωρών ζωής. Το SSL χρησιμοποιείται τη κρυπτογραφία δημοσίου κλειδιού για την ανταλλαγή αυτού του κλειδιού, καθώς και για αμοιβαία ταυτοποίηση των συναλλασσόμενων μερών. Για την κρυπτογράφηση της συνόδου SSL χρησιμοποιεί τη συμμετρική κρυπτογραφία που είναι σαφώς γρηγορότερη.
Όταν ένας παρουσιαστής ιστοσελίδων (πελάτης) συνδεθεί με μια SSL-προστατευόμενη σελίδα, ο SSL- εξυπηρετητής στέλνει μια αίτηση για την έναρξη μιας SSL- συνόδου. Αν ο παρουσιαστής ιστοσελίδων υποστηρίζει το πρωτόκολλο SSL, ενημερώνει τον εξυπηρετητή για αυτό και πιο συγκεκριμένα για:

- την ταυτοποίηση της συνόδου
- τους αλγόριθμους κρυπτογράφησης και
- τις μεθόδους συμπίεσης που υποστηρίζει.

Ο εξυπηρετητής κάνει τις αντίστοιχες επιλογές και έτσι ξεκινά η επικοινωνία,. Αρχικά, γίνεται η ανταλλαγή των ψηφιακών πιστοποιητικών (digital certificates). Ο πελάτης καθορίζει ένα κλειδί συνόδου (session key) που είναι κατάλληλο για τον αλγόριθμο κρυπτογράφησης που επιλέχθηκε. Ο πελάτης με το δημόσιο κλειδί συνόδου και ο δεύτερος με το ιδιωτικό του κλειδί αποκρυπτογραφεί και αποκτά το κλειδί συνόδου



Σχ. 5. Προστατευμένη επικοινωνία client-server.

Το πρωτόκολλο SSL βασίζεται στην ιδέα του ασφαλούς καναλιού επικοινωνίας. Το κανάλι εγγυάται την εμπιστευτικότητα όλων των μηνυμάτων που διακινούνται. Έτσι, το πρωτόκολλο SSL παρέχει την ασφάλεια που απαιτείται κατά την εκκίνηση μιας TCP/IP σύνδεσης. Ο πελάτης και ο εξυπηρετητής κανονίζουν το επίπεδο και ανταλλάσσουν ψηφιακές ταυτότητες για ταυτοποίηση. Όλες οι πληροφορίες, όπως οι HTTP αιτήσεις/ απαντήσεις είναι πλήρως κρυπτογραφημένες. Το ίδιο συμβαίνει και με το URL που ζητά ο πελάτης, τα περιεχόμενα φορμών και άλλες πληροφορίες.

Το HTTP και το HTTP+SSL (https) είναι διαφορετικοί τρόποι κλήσης και άρα χρησιμοποιούν διαφορετικές θύρες (80 και 443 αντίστοιχα), γεγονός που σημαίνει ότι το ίδιο σύστημα μπορεί να «τρέχει» και τα δυο πρωτόκολλα ταυτόχρονα.

Το παραπάνω διάγραμμα *(Σχ.5.)* παριστάνει τη διαδικασία που εγγυάται τη προστατευμένη επικοινωνία μεταξύ των μερών (Web server και client). Οι ανταλλαγές των ψηφιακών ταυτοτήτων γίνεται μέσα σε δευτερόλεπτα.

Επειδή η κυβέρνηση των Ηνωμένων Πολιτειών είχε επιβάλλει περιορισμούς εξαγωγών τεχνολογίας, μέχρι πρότινος τα SSL κλειδιά

εκτός των ΗΠΑ και του Καναδά είχαν μέγεθος 56 bits ή λιγότερο. Ο λόγος ήταν ότι θεωρούσαν αυτή την τεχνολογία ένα στρατιωτικό όπλο. Στις ΗΠΑ και στον Καναδά έχουν μέγεθος που φτάνει τα 128 bits. Όπως είναι φυσικό, όσο μεγαλύτερος είναι ο αριθμός των bits τόσο πιο δύσκολη είναι η αποκρυπτογράφηση. Παρόλα αυτά, σήμερα οι περιορισμοί αυτοί διατηρούνται μόνο για λίγες χώρες στον κόσμο.

7.2.3. Επιβάρυνση από τη Χρήση του SSL

Το SSL χρησιμοποιεί κρυπτογράφηση και αποκρυπτογράφηση πληροφοριών γεγονός που συνεπάγεται κάποιο πλεόνασμα διακινούμενων πληροφοριών. Η χρήση του πρωτοκόλλου αυτού όχι μόνο αυξάνεται το ποσό των δεδομένων που διακινούνται, αλλά δημιουργεί περισσότερα πακέτα και καθυστερεί τη μετάδοση των πληροφοριών. Ειδικότερα, μπορούμε να αναφέρουμε ως αιτίες για την καθυστέρηση:

- την αρχική σύνδεση όπου κανονίζονται οι λεπτομέρειες της σύνδεσης και ανταλλάσσονται κρυπτογραφημένες πληροφορίες.
- Τη διαδικασία κρυπτογράφηση των δεδομένων από τον κάθε υπολογιστή (άκρο της σύνδεσης).
- τα κρυπτογραφημένα δεδομένα, που αποτελούνται από περισσότερα bytes, γεγονός που συνεπάγεται μεγαλύτερο χρόνο μεταφοράς του από το δίκτυο.
- διάφορους άλλους τεχνικούς λόγους που έχουν σχέση με το SSL.

Γι' αυτούς τους λόγους το HTTP με SSL είναι το πιο αργό από το κλασσικό HTTP και πρέπει να χρησιμοποιείται μόνο όταν απαιτείται μυστικότητα και όχι σαν γενική HTTP υπηρεσία.
Το SSL εφαρμόζεται στο επίπεδο συγκεκριμένων Web σελίδων και όχι στο επίπεδο ενός ιστοχώρου (Web site), έτσι ώστε να προστατεύονται μόνο αυτές οι σελίδες που περιέχουν εμπιστευτικά δεδομένα, όπως για παράδειγμα, προσωπικά στοιχεία και πληροφορίες πιστωτικών καρτών.

7.2.4. Ενεργοποίηση SSL

Ένα βασικό στοιχείο για έναν οργανισμό που παρέχει υπηρεσίες στο διαδίκτυο, είναι να λειτουργεί έναν ασφαλή ιστοχώρο (site). Ο λόγος είναι προφανής, αφού τα στοιχεία του χρήστη που μεταφέρονται χωρίς ασφάλεια, μπορούν να κλαπούν. Αν υποστηρίζεται όμως το πρωτόκολλο SSL, το όνομα του χρήστη (user name), ο κωδικός πρόσβασης και κάθε άλλη πληροφορία της συναλλαγής κρυπτογραφείται. Επιπλέον, η χρήση των ψηφιακών

ταυτοτήτων και του SSL αντί των κωδικών πρόσβασης προσφέρει μεγαλύτερη ασφάλεια.
Η βασικότερη απαίτηση για το SSL, είναι να διαθέτει ο εξυπηρετητής πιστοποιητικό (server certificate). Το πιστοποιητικό αυτό ταυτοποιεί τον εξυπηρετητή σε κάθε ενδιαφερόμενο πελάτη και παρέχει τον μηχανισμό σε αυτόν να ξεκινήσει μια ασφαλή σύνοδο. Παρόλο που η ταυτοποίηση του πελάτη δεν είναι απαραίτητη για την έναρξη μιας SSL συνόδου, δεν ισχύει το ίδιο και για τον εξυπηρετητή.
Στο επόμενο κεφάλαιο, περιγράφεται συνοπτικά η διαδικασία ενεργοποίησης του SSL σε έναν εξυπηρετητή. Η διαδικασία περιλαμβάνει τα παρακάτω βήματα:

- Δημιουργία του ζεύγους κλειδιών του εξυπηρετητή με κάποιο δικό του λογισμικό
- Αίτηση για πιστοποιητικό σε κάποια ΑΠ
- Εγκατάσταση πιστοποιητικού
- Ενεργοποίηση του SSL για τον εξυπηρετητή.

7.3. PGP και PEM

Το PGP και το PEM (Pretty Good Privacy Privacy-enhanced Electronic Mail) είναι προγράμματα που επιτρέπουν στον χρήστη και σε ένα δεύτερο μέρος να επικοινωνούν με ένα τρόπο που δεν επιτρέπει στα τρίτα μέρη να τα «διαβάσουν», και που πιστοποιούν ότι το πρόσωπο που στέλνει το μήνυμα είναι αλήθεια αυτό που ισχυρίζεται. Το PGP είναι ένα σύστημα κρυπτογράφησης δημόσιου κλειδιού που αναπτύχθηκε το 1991 στις ΗΠΑ από τον Φιλ Τσίμερμαν και βασίζεται σε ένα μοντέλο παρουσίασης που εξαρτάται από την ακεραιότητα μιας αλυσίδας πιστοποιητικών, των χρηστών των ίδιων. Οι χρήστες και τα κλειδιά τους αναφέρονται από τον έναν χρήστη στον άλλον σχηματίζοντας ένα «δαχτυλίδι» πιστοποίησης ή «δίκτυο εμπιστοσύνης». Στο τέλος ίσως να μη γνωρίζεις το τελευταίο άτομο που μπήκε στο δίκτυο, ελπίζεις όμως κάποιος άλλος να γνωρίζει.
Ένα από τα πλεονεκτήματα του PGP είναι ότι μπορεί να διαλειτουργεί με μια Αρχή Πιστοποίησης πλήρως αποδεκτή από όλα τα μέρη στο χώρο, που μπορεί να εγγυηθεί πιστοποιητικά, που διασφαλίζουν την ταυτότητα του επίδοξου χρήστη.
Το PEM παρέχει τις υπηρεσίες του μέσω της χρήσης κρυπτογράφησης «από άκρη-σε άκρη» μεταξύ διαδικασιών δημιουργίας και αποδοχής. Δεν επιβάλλονται κάποιες ειδικές διαδικαστικές αξιώσεις στο Σύστημα Μεταφοράς Μηνύματος, στα τελικά ή στα ενδιάμεσα sites αναμετάδοσης. Αυτή η προσέγγιση επιτρέπει στις PEM λειτουργίες να ενσωματώνονται επιλεκτικά σε μια βάση site με site ή χρήστη με χρήστη χωρίς να έρχονται σε σύγκρουση με άλλες οντότητες του Internet.

7.4. PKCS

Τα Public-Key Cryptography Standards (PKCS) είναι ένα σετ από standards για κρυπτογραφία δημοσίου κλειδιού, που δημιουργήθηκαν στα RSA Laboratories σε συνεργασία με την Apple, τη Microsoft, τη Lotus, τη Sun και την MIT. Το PKCS προσδιορίζεται σαν μια μέθοδο εφαρμογής των OSI Standards. Είναι συμβατό με το PEM αλλά εκτείνεται και πέρα από το PEM. Ακόμη είναι συμβατό και με το ITU-T X.509 Standards.
Το PKCS περιέχει Standards εφαρμογής τόσο ανεξάρτητου όσο και ειδικού αλγόριθμου. Στους αλγόριθμους που υποστηρίζει συμπεριλαμβάνονται μεταξύ άλλων το RSA και Diffie Helman κλειδί ανταλλαγής. Ακόμη προσδιορίζει έναν ανεξάρτητο αλγόριθμο σύνταξης για ψηφιακές υπογραφές, ψηφιακούς φακέλους και εκτείμενα πιστοποιητικά. Αυτό εμποδίζει κάποιον να εφαρμόσει ένα κρυπτογραφικό αλγόριθμο, πόσο μάλιστα να συμμορφωθεί σε μια σταθερή σύνταξη.

- Η PKCS#1 έκδοση προσδιορίζει τους μηχανισμούς για απόκρυψη και υπογραφή δεδομένων με τη χρήση RSA κρυπτοσυστήματος δημοσίου κλειδιού.
- Η PKCS#3 προσδιορίζει ένα πρωτόκολλο συμφωνίας κλειδιού Diffie Helman.
- Η PKCS#5 περιγράφει μια μέθοδο απόκρυψης ενός string με ένα μυστικό κλειδί προερχόμενο από ένα password.
- Η PKCS#6 περιγράφει ένα σχήμα εκτειμένων πιστοποιητικών.
- Η PKCS#7 προσδιορίζει μια γενική σύνταξη για μηνύματα που περιέχει ψηφιακές υπογραφές και απόκρυψη.
- Η PKCS#8 περιγράφει ένα σχήμα για πληροφορία ιδιωτικού κλειδιού, η οποία περιέχει ένα ιδιωτικό κλειδί για κάποιον αλγόριθμο δημόσιου κλειδιού.
- Η PKCS#9 προσδιορίζει επιλεγμένες ιδιότητες που συμπεριλαμβάνονται στα άλλα PKCS.
- Η PKCS#10 περιγράφει μια σύνταξη για αιτήσεις certificate.

7.5. S-HTTP.

Το S-HTTP (Secure-HTTP) είναι μια επέκταση του Hypertext Transfer Protocol (HTTP) που επιτρέπει την ασφαλή ανταλλαγή φακέλων στο Word Wide Web (W.W.W). Κάθε S-HTTP φάκελος είναι κρυπτογραφημένος και περιέχει ένα ψηφιακό πιστοποιητικό. Για ένα δοσμένο πιστοποιητικό, το S-HTTP είναι μια εναλλακτική λύση έναντι του SSL. Μια μεγάλη διαφορά είναι ότι το S-HTTP επιτρέπει στον πελάτη να στέλνει ένα πιστοποιητικό για να πιστοποιήσει τον χρήστη, ενώ στο SSL μόνο ο server μπορεί να πιστοποιηθεί. Το S-

HTTPχρησιμοποιείται περισσότερο σε περιπτώσεις όπου ο server είναι π.χ. μια τράπεζα και απαιτεί πιστοποίηση από τον πελάτη.
Το S-HTTP δεν χρησιμοποιεί μόνο σύστημα κρυπτογράφησης αλλά υποστηρίζει το σύστημα απόκρυψης δημόσιου κλειδιού RSA. Το SSL λειτουργεί σε να επίπεδο προγράμματος ελαφρά υψηλότερο του TCP, ενώ το S-HTTP στο ακόμη υψηλότερο της HTTP εφαρμογής.
Ένα μεγάλο νούμερο δημοφιλών Web Servers υποστηρίζουν τόσο το S-HTTP όσο και το SSL. Οι νεώτεροι browsers υποστηρίζουν ταυτόχρονα και τα δυο.

7.6. S/MIME

Το S/MIME είναι μια προδιαγραφή για ασφαλές e-mail και σημαίνει Secure/ Multipurpose Internet Mail Exclusions. Σχεδιάστηκε για να προσθέσει ασφάλεια στα e-mail μηνύματα σε MIME μορφή. Οι υπηρεσίες ασφάλειας που παρέχονται είναι πιστοποίηση (με χρήση ψηφιακών υπογραφών) και μυστικότητα (με χρήση απόκρυψης).
Το S/MIME συνδυάζει κρυπτογραφικές κατασκευές με standard πρακτικές e-mail. Ακόμη σημαντικότερο είναι ότι σχεδιάστηκε να είναι διαλειτουργικό έτσι ώστε δυο οποιαδήποτε πακέτα που εμπεριέχουν S/MIME να επικοινωνούν με ασφάλεια. Παρέχει ασφάλεια χρησιμοποιώντας μια υβριδική προσέγγιση, συχνά καλούμενη ως ψηφιακός φάκελος. Το κύριο μέρος της απόκρυψης μηνύματος γίνεται με μια συμμετρική κρυπτογραφική κλείδα και ένας αλγόριθμος δημόσιου κλειδιού χρησιμοποιείται για την ανταλλαγή κλειδιού. Ένας παρόμοιος αλγόριθμος χρησιμοποιείται και για ψηφιακές υπογραφές.
Το S/MIME δεν εξειδικεύεται μόνο στο Internet και μπορεί να χρησιμοποιηθεί σε οποιοδήποτε περιβάλλον ηλεκτρονικού ταχυδρομείου. Προσεχτική εξέταση δόθηκε έτσι ώστε μικρότερες, μυστικές εφαρμογές να μπορούν να αναπτυχθούν και να γίνουν μέρος του Internet αν απαιτείται, κάτι που επιτυγχάνεται με τη δημιουργία ευέλικτων και κλιμακωτών κατευθυντήριων γραμμών.
Σε κάποια περιβάλλοντα, η απόκρυψη της ταυτότητας του αποστολέα είναι απαιτούμενα. Για την αποφυγή της απόσπασης πολύτιμων πληροφοριών κατά της διάρκειας της ανταλλαγής των, από κάποιον «ωτακουστή», αυτά τα περιβάλλοντα χρησιμοποιούν ανώνυμους e-mails, ή πύλες που αφαιρούν την διεύθυνση προέλευσης του e-mail.
Μια ψηφιακή υπογραφή μπορεί να δώσει στον ωτακουστή άλλο ένα κομμάτι δεδομένων για να αναγνωρίσει τον αποστολέα-που είναι και ο υπογράφων.
Το S/MIME αποτρέπει κάτι τέτοιο, επιθέτοντας πρώτα την ψηφιακή υπογραφή και το αυθεντικό μήνυμα σε έναν ψηφιακό φάκελο.

7.7. X.509

Η ITU-T Recommandation X.509 εφαρμογή προσδιορίζει ένα πλαίσιο εργασίας για την παροχή υπηρεσιών πιστοποίησης κάτω από ένα παράδειγμα κεντρικού ελέγχου αντιπροσωπευόμενου από έναν κατάλογο "Directory" . Περιγράφει δυο επίπεδα πιστοποίησης που χρησιμοποιεί ένα password σαν επιβεβαίωση της ισχυριζόμενης ταυτότητας και ισχυρή πιστοποίηση που περιλαμβάνει πιστοποιητικά σχηματιζόμενα με την χρήση κρυπτογραφικών τεχνικών.
Τα πιστοποιητικά χρηστών, που μπορεί να δημιουργηθούν off-line , μπορεί να κρατηθούν μέσα σε έναν directory σαν ιδιότητες και να λαμβάνονται από τους χρήστες του directory με τον ίδιο τρόπο όπως άλλες πληροφορίες. Καθορίζεται μια standard δομή για τα πιστοποιητικά που επιτρέπει τον καθορισμό της έκδοσης, των ψηφιακών υπογραφών, τις λεπτομέρειες της εγκυρότητας, όνομα θέματος. Ακόμη καθορίζεται μια μέθοδος δημιουργίας λιστών ακυρωμένων πιστοποιητικών.
Το Χ. 509 ακόμη, παρέχει τρόπους με τους οποίους τα tokens μπορούν να υπογραφούν μέσα στον directory, αλλά δεν περιέχει ένα συγκεκριμένο standard για ψηφιακές υπογραφές. Το standard επιτρέπει έναν, δυο ή τρεις τρόπους πιστοποίησης. Η κρυπτογράφηση δημόσιου κλειδιού χρησιμοποιείται για ισχυρή πιστοποίηση, αλλά το πλαίσιο εργασίας πιστοποίησης δεν εξαρτάται από την χρήση ενός συγκεκριμένου κρυπτογραφικού αλγόριθμου, αν και δυο χρήστες που επιθυμούν να πιστοποιηθούν πρέπει να υποστηρίζουν τον ίδιο αλγόριθμο.

ΚΕΦΑΛΑΙΟ 8^{Ο}: Firewalls

8.1.Προστασία με Firewalls.

Γενικά η λέξη firewall αποδίδεται σε πυρίμαχους τοίχους που εμποδίζουν την εξάπλωση της φωτιάς από δωμάτιο σε δωμάτιο ή μεταξύ διαμερισμάτων. Στην περίπτωση των υπολογιστών συστημάτων, τα firewalls αποτελούν την αναγκαία λύση προστασίας τους, καθώς αυτά συνδέονται ολοένα και περισσότερο σε δίκτυα τα οποία επίσης είναι συνδεδεμένα στο διαδίκτυο.

Από τη στιγμή που ένα δίκτυο αποκτήσει σύνδεση στο Internet, ανοίγει ένα κανάλι αμφίδρομης επικοινωνίας: οι χρήστες του δικτύου (insiders) αποκτούν επαφή με τον έξω κόσμο, αλλά ταυτόχρονα και οι outsiders, δηλαδή οι εξωτερικοί χρήστες ως προς αυτό το δίκτυο, αποκτούν πλέον δυνατότητα πρόσβασης σε αυτό. Ο τρομακτικός ρυθμός αύξησης του διαδικτύου, προκαλεί ανάλογη αύξηση των πιθανών κινδύνων στα ιδιωτικά (private) δίκτυα που συνδέονται μαζί του. Για τη προστασία τους από διάφορες εισβολές απαιτείται ένας κατάλληλος φράκτης. Ο φράκτης αυτός που καλείται firewall, πρέπει να είναι ικανός να επεξεργάζεται όλη τη κυκλοφορία μηνυμάτων ανάμεσα σε ένα συγκεκριμένο τοπικό ή ιδιωτικό δίκτυο και στο Internet. Στην πραγματικότητα ένα σύστημα firewall ανορθώνει ένα εξωτερικό τοίχο ασφαλείας, οριοθετώντας μια περίμετρο προστασίας. Έτσι προκαλεί ένα σαφή διαχωρισμό ανάμεσα στο προστατευόμενο- εσωτερικό δίκτυο ενός οργανισμού (το οποίο θεωρείται ασφαλές και έμπιστο) και στο εσωτερικό διαδίκτυο(το οποίο θεωρείται μη ασφαλές και μη έμπιστο).

8.2. Σκοπιμότητα.

Ο πρωταρχικός σκοπός των firewall είναι να προστατεύσουν τα δίκτυα από εξωτερικούς εισβολείς, περιορίζοντας τους τα δικαιώματα προσπέλασης σε αυτό, χωρίς να περιορίζουν την προσπέλαση στο εξωτερικό περιβάλλον. Για αυτό τα firewalls παρέχουν ένα περίβλημα προστασίας του δικτύου που το προστατεύουν από απειλές όπως:

- Μη εξουσιοδοτημένη προσπέλαση των δικτυακών πόρων : όταν οι επίδοξοι εισβολείς προσπαθούν να εισχωρήσουν στο δίκτυο και να αποκτήσουν μη εξουσιοδοτημένη προσπέλαση στα αρχεία.
- Άρνηση εξυπηρέτησης: όταν κάποιος εξωτερικός παράγοντας γεμίζει τους διαθέσιμους ελεύθερους χώρους των δίσκων ή υπερφορτώνει τις γραμμές του δικτύου στέλνοντας τις μυριάδες μηνυμάτων σε έναν από τους ξενιστές του δικτύου.

- Προσποίηση (masquerading): όταν τα μηνύματα του ηλεκτρονικού ταχυδρομείου φαίνονται ότι προέρχονται από κάποιον νόμιμο χρήστη ενώ έχουν παραποιηθεί από άλλον με σκοπό την πρόκληση παρεξηγήσεων ή ζημιών.

Ως λύση στα παραπάνω προβλήματα, πέρα από την ολοκληρωτική αποσύνδεση του δικτύου από τον έξω κόσμο, προτείνεται η υλοποίηση μηχανισμών προστασίας, όπως τα firewalls, τα οποία από τη μια φιλτράρουν την προσπέλαση στο δίκτυο, ενώ από την άλλη επιτρέπουν την επικοινωνία με τον έξω κόσμο.

8.3. Ορισμοί

Ένα σύστημα firewall ορίζεται ως το λογισμικό και ο εξοπλισμός που τοποθετούμενος ανάμεσα στο διαδίκτυο και στο υπό προστασία δίκτυο, επιτρέπει την προσπέλαση των εξωτερικών χρηστών στο προστατευόμενο δίκτυο, μόνο εφόσον διαθέτουν συγκεκριμένα χαρακτηριστικά. Έτσι ένα τυπικό σύστημα firewall μπορεί να επιτρέπει επιλεκτικά τη πρόσβαση στους εξωτερικούς χρήστες, βασιζόμενο σε ονόματα χρηστών και συνθηματικά ή σε IP διευθύνσεις ή ακόμη και σε ονόματα επικρατειών (domain names). Αυτός είναι ο κύριος σκοπός του: να κρατήσει τις επικίνδυνες δραστηριότητες μακριά από το προστατευόμενο περιβάλλον.
Ένα firewall μπορεί να θεωρηθεί σαν ένα ζευγάρι μηχανισμών που ο ένας μπλοκάρει τη κυκλοφορία των δεδομένων και ο άλλος επιτρέπει τη ροή τους. Το ποια δεδομένα επιτρέπονται και ποια απορρίπτονται είναι ζήτημα της πολιτικής ελέγχου (control policy) που υποστηρίζει και εξαρτάται από την συγκεκριμένη διαμόρφωσή του (firewall configuration). Ένα σύστημα firewall δεν είναι απλά και μόνο ένας δρομολογητής (router), ένας διανομέας ή διακομιστής (server), ένας οικοδεσπότης (host), ή ένα σύνολο εξοπλισμού και λογισμικού που παρέχει ασφάλεια στα δίκτυα. Οι αληθινές δυνατότητές του γίνονται εμφανείς αν τον θεωρήσουμε ως ένα ισχυρό μέσο υλοποίησης μιας πολιτικής ασφάλειας που καθορίζει τις παρεχόμενες υπηρεσίες και τις επιτρεπτές προσπελάσεις ανάμεσα σε έμπιστες και μη έμπιστες επικράτειες. Η υλοποίηση της πολιτικής ελέγχου προσπέλασης δικτύων (network access policy) γίνεται με την υποχρεωτική κατεύθυνση όλων των επικοινωνιών μέσω του firewall, ώστε να αποτελούν αντικείμενο για παραπέρα εξέταση και καταγραφή από αυτό. Στο *Σχ. 6* φαίνεται μια τυπική διάταξη firewall.

Σχ 6. Τυπική διάταξη firewall.

8.4. Παρεχόμενη Ασφάλεια

Καθώς τα τυπικά δίκτυα (local networks) συνδέονται στο Internet, αποτελεί ζήτημα μεγάλης σημασίας η διασφάλιση της κανονικής λειτουργίας τους από τους νόμιμους και παράνομους χρήστες τους. Η τοποθέτηση ενός firewall συστήματος ανάμεσα στο τοπικό δίκτυο ενός οργανισμού και το διαδίκτυο, παρέχει δυνατότητες ελέγχου στη ροή των πληροφοριών και διασφαλίζει τη σύνδεσή του με το διαδίκτυο, προστατεύοντας εκ' μέρους του οργανισμού:

- Τους πόρους του (υλικό, λογισμικό, δεδομένα) από φθορά, κατάχρηση και κλοπή.
- Την υπόληψή του από τη δημοσιοποίηση αδυναμιών στην ασφάλεια του δικτύου του.
- Την επικρατούσα πολιτική ορθής χρήσης των υπηρεσιών του διαδικτύου από τους εργαζόμενούς του.

Ο πιο συνηθισμένος πάντως λόγος ύπαρξης ενός συστήματος firewall σε έναν οργανισμό είναι η παροχή ενός μηχανισμού ελέγχου προσπέλασης (access control), πρώτου επιπέδου, για τον Web Server. Ένα firewall πρέπει να ελέγχει και να καταγράφει την ροή των επικοινωνιών που διέρχονται μέσα από τον διακομιστή Web. Δηλαδή πρέπει να παρεμβάλλεται και να αποκόπτει όλη την κίνηση των δεδομένων ανάμεσα στον Web server και στο Internet Έτσι είναι σε θέση να προστατεύει τα δεδομένα που δημοσιεύονται από ανεπιθύμητες αλλαγές και να ελέγχει την πρόσβαση στον διακομιστή Web, αποκλείοντας τους μη- εξουσιοδοτημένους χρήστες από ευαίσθητους πόρους του δικτύου.

Ακόμη, ένας οργανισμός μπορεί να χρησιμοποιήσει ένα firewall για να απομονώσει τις επικοινωνίες ανάμεσα στα δίκτυα των επιμέρους τμημάτων του. Για παράδειγμα ένα νοσοκομείο ενδεχομένως να θελήσει να διαχωρίσει το δίκτυο διακίνησης των δεδομένων των ασθενών από το δίκτυο των οικονομικών στοιχείων του. Ένα ή περισσότερα firewalls (intranet firewalls) μπορούν να χρησιμοποιηθούν για να παρέχουν

απομόνωση και ελεγχόμενη προσπέλαση ανάμεσα στα διάφορα μέρη ενός οργανισμού.
Ως ένα σύστημα firewall μπορεί να θεωρηθεί μια διάταξη δρομολόγησης (router), ένας προσωπικός υπολογιστής, ένας διακομιστής, ή ένα σύνολο από διακομιστές, διαμορφωμένοι με τέτοιο τρόπο ώστε να οχυρώνουν μια δικτυακή τοποθεσία (site) ή ένα υποδίκτυο (subnet) από πρωτόκολλα και υπηρεσίες (π.χ. υπηρεσίες FTP, HTTP, e-mail κ.λ.π.) οι οποίες μπορούν να προσβληθούν από διακομιστές εκτός του υποδικτύου. Η συνηθισμένη θέση του είναι ως πύλη υψηλού επιπέδου ακριβώς στο σημείο σύνδεσης του οργανισμού με το Internet. Όπως όμως έχει ήδη αναφερθεί, μπορεί να τοποθετηθεί και ως πύλη χαμηλότερων επιπέδων πρόσβασης, με σκοπό την προετοιμασία επιμέρους τμημάτων του υποδικτύου.
Η εγκατάσταση επιπλέον συστημάτων firewall ως διαχωριστικά των επιμέρους τμημάτων ενός οργανισμού, προσφέρει δυνατότητες διαχωρισμού των εξουσιοδοτήσεων που προσφέρονται στους εσωτερικούς χρήστες, λεπτομερέστερη επίβλεψη τους και γενικότερα υποστήριξη υπευθυνότητας με περισσότερη διακριτικότητα. Με άλλα λόγια, παρέχει μέτρα προστασίας από τους νόμιμους και εσωτερικούς χρήστες του δικτύου, που σύμφωνα και με τις περισσότερες έρευνες αποτελεί τον σημαντικότερο κίνδυνο για την ασφάλεια ενός οργανισμού.

8.5. Βασικές Τεχνικές Προστασίας

Υπάρχουν τρεις βασικές τεχνικές προστασίας:

- πύλες φιλτραρίσματος πακέτων (packet filtering gateways) ή δρομολογητές φιλτραρίσματος (screening routers)
- πύλες κυκλωμάτων (circuit gateways)
- πύλες εφαρμογών (application gateways)

Μια ολοκληρωμένη υπηρεσία firewall συνήθως παρέχεται σε συνδυασμό των παραπάνω βασικών τεχνικών φιλτραρίσματος.

8.5.1. Πύλες Φιλτραρίσματος Πακέτων

Οι πύλες φιλτραρίσματος πακέτων παρέχουν έναν εύκολο και φθηνό τρόπο υλοποίησης ενός βασικού επιπέδου φιλτραρίσματος με πραγματοποίηση ελέγχων των πακέτων (Internet Protocol Packets) ενός δικτύου. Ένα πακέτο είναι μια μικρή μονάδα επικοινωνίας, συνήθως μερικές εκατοντάδες bytes. Ένας δρομολογητής (router) μπορεί να διοχετεύσει χιλιάδες πακέτα μέσα σε ένα δευτερόλεπτο.
Αυτή η τεχνική φιλτραρίσματος είναι η πρώτη που εμφανίσθηκε ως συνοδευτικό εργαλείο λογισμικού για την υποστήριξη επιπλέον

ρυθμίσεων στον αρχικά απλό εξοπλισμό των διατάξεων ή συσκευών δρομολόγησης που δεν είχαν δυνατότητες φιλτραρίσματος των πακέτων.

- Το φίλτρο πακέτων διενεργεί τον έλεγχο εφαρμόζοντας ένα σύνολο κανόνων (rules), οι οποίοι έχουν οριστεί από το διαχειριστή του firewall κατά τη διαμόρφωσή του και οι οποίοι υλοποιούν μια προαποφασισμένη πολιτική ασφάλειας. Κάθε κανόνας έχει δυο βασικά τμήματα:
  1. το πεδίο της ενέργειας και
  2. το πεδίο των κριτηρίων επιλογής.

Οι δυνατές ενέργειες είναι δύο: επιτρέπω (permit, allow) ή σταματώ (block, deny).
Τα κριτήρια επιλογής των πακέτων για τα οποία θα ισχύσει η αντίστοιχη ενέργεια, βασίζονται στις ακόλουθες παραμέτρους:
Διεύθυνση προέλευσης και προορισμού: για τις IP διευθύνσεις μπορούν να χρησιμοποιηθούν και μάσκες διευθύνσεων (address masks) που ομαδοποιούν τις διευθύνσεις.

- Αριθμός θυρίδας προέλευσης και προορισμού: Σε κάθε διακομιστή, οι εκτελούμενες εφαρμογές καταλαμβάνουν συγκεκριμένους αριθμούς θυρίδων επικοινωνίας (port numbers).
- Πρωτόκολλο: Για παράδειγμα, TCP (Transmission Control Protocol), ICMP (Internet Control Message Protocol) ή UDP (User Datagram Protocol).
- Κατεύθυνση: Ανάλογα με το αν εισέρχεται το πακέτο στο ιδιωτικό δίκτυο ή αν εξέρχεται από αυτό.

Από απόψεως αρχιτεκτονικής δικτύου, ο χώρος δράσης τους είναι τα χαμηλότερα στρώματα (network- transport layers) του μοντέλου αναφοράς OSI (OSI reference model) και για αυτό είναι πολύ γρήγορες. Είναι ικανές επίσης να ελέγχουν την κυκλοφορία, ακόμη και στη βάση μιας συγκεκριμένης εφαρμογής (by application), αφού η διεύθυνση που ελέγχει ένας δρομολογητής, μπορεί να είναι ο συνδυασμός της διεύθυνσης δικτύου και του αριθμού θυρίδας εφαρμογής (π.χ. το 21 για εφαρμογές FTP, το 25 για εφαρμογές SMTP, κ.λ.π.).
Η τεχνολογία φιλτραρίσματος πακέτων παρουσιάζει όμως και αρκετούς περιορισμούς:

- Ο έλεγχος που πραγματοποιείται, αφορά κυρίως το είδος κυκλοφορίας του δικτύου, αφού εξετάζονται μόνο οι IP-επικεφαλίδες κάθε πακέτου. Εκεί υπάρχουν οι πληροφορίες δρομολόγησης (όπως η προέλευση και ο προορισμός κάθε πακέτου). Το περιεχόμενο του κάθε πακέτου δεν εξετάζεται, γι' αυτό και η τεχνολογία αυτή είναι κατάλληλη για απλές σχετικά πολιτικές ασφάλειας.
- Δεν προσφέρει επαρκείς μηχανισμούς επίβλεψης (auditing) και ειδοποίησης κινδύνου (alerting).

- Δεν υποστηρίζει εύκολη διαχείριση γιατί υπάρχει περιορισμένος αριθμός κανόνων οι οποίοι μάλιστα απαιτούν κατανόηση των ιδιαιτεροτήτων των πρωτοκόλλων επικοινωνίας. Έτσι είναι αρκετά σύνθετο και δύσκολο έργο η ορθή διαμόρφωσή τους για την εφαρμογή μιας πολιτικής ασφάλειας. Βέβαια διατίθενται κάποια εργαλεία υποστήριξης του έργου των διαχειριστών, που ελέγχουν τη σύνταξη κανόνων, κάνουν λιγότερο άβολο το περιβάλλον επικοινωνίας (interface), κ.λ.π.
- Δεν διαθέτουν συνήθως μηχανισμούς αυθεντικοποίησης σε επίπεδο χρήστη (user level authentication).
- Δεν προστατεύουν από επιθέσεις πλαστογραφίας σε IP και σε DNS διευθύνσεις (IP & DNS address spoofing). Η βασική αδυναμία των μηχανισμών φιλτραρίσματος πακέτων είναι ότι στηρίζοντας στις IP διευθύνσεις, οι οποίες όμως δεν είναι απόλυτα ασφαλείς γιατί συνήθως δεν προστατεύονται.

Σε γενικές γραμμές το επίπεδο ασφαλείας που προσφέρουν είναι χαμηλού επιπέδου. Από την άλλη μεριά πάλι, είναι απλοί, ταχύτατοι, ευέλικτοι και χαμηλού κόστους. Έτσι θεωρούνται ιδανικοί για περιβάλλοντα χαμηλής επικινδυνότητας (low-risk environments). Βεβαίως οι υπηρεσίες που προσφέρουν είναι σημαντικότατες για αυτό και θεωρούνται αναπόσπαστο τμήμα ενός ολοκληρωμένου συστήματος firewall.

8.5.2. Πύλες Κυκλωμάτων

Η χρήση των πυλών κυκλωμάτων σε διατάξεις firewalls αναβαθμίζει σημαντικά την ασφάλεια των δικτύων. Επιτρέπουν τη χρήση εφαρμογών που βασίζονται στα πρωτόκολλα επικοινωνίας TCP και UDP (όπως για παράδειγμα WWW, Telnet, κ.α.) χωρίς να αφήνουν να γίνονται όλα σε επίπεδο πρωτοκόλλου επικοινωνίας.
Οι πύλες κυκλωμάτων λειτουργούν ως εκπρόσωποι (agents) των πρωτοκόλλων επικοινωνίας, μεταβιβάζοντας (relay) την δικτυακή κίνηση μεταξύ δυο υπολογιστών που είναι συνδεδεμένοι μεταξύ τους μέσω ενός ιδεατού κυκλώματος (virtual circuit) του δικτύου. Ένας εσωτερικός χρήστης, για παράδειγμα, μπορεί να συνδέεται με μια θύρα ενός υπολογιστή που βρίσκεται σε ένα εξωτερικό δίκτυο. Η πύλη απλά αντιγράφει bytes από την μια θύρα στην άλλη. Κανονικά η πύλη μεταβιβάζει τα δεδομένα χωρίς να τα εξετάζει, αλλά συνήθως διατηρεί μια καταγραφή της ποσότητας των μεταβιβαζομένων δεδομένων και του προορισμού τους. Σε μερικές περιπτώσεις η σύνδεση μεταβίβασης (relay connection), η οποία με αυτό τον τρόπο διαμορφώνει τελικά ένα «κύκλωμα», λειτουργεί αυτόματα. Άλλες φορές πάλι, χρειάζεται να καθοριστεί στην πύλη η επιθυμητή θύρα προορισμού. Παρόλο που κανονικά οι μεταβιβάσεις θεωρούνται σε περιβάλλοντα TCP, οι πύλες

κυκλωμάτων μπορούν ακόμη να χρησιμοποιηθούν και σε εφαρμογές UDP (User Datagram Protocol).
Ένα από τα μειονεκτήματα αυτών των συστημάτων είναι ότι οι εφαρμογές των πελατών (clients) πρέπει να μετατραπούν πριν να καταστούν έτοιμες για να λειτουργήσουν με μια συγκεκριμένη πύλη κυκλωμάτων.

8.5.3. Πύλες Εφαρμογών.

Οι πύλες κυκλωμάτων και οι πύλες εφαρμογών αναφέρονται και ως proxy server, καθώς και οι δυο συμπεριφέρονται ως εκπρόσωποι (proxies) του υποτιθέμενου πελάτη. Όμως οι πύλες εφαρμογών προχωρούν ακόμη παραπέρα, σε ότι αφορά την ασφάλεια δικτύων. Λειτουργούν στο υψηλότερο στρώμα επικοινωνίας, γνωστό ως το επίπεδο εφαρμογής (application layer). Έτσι έχουν πρόσβαση σε περισσότερες πληροφορίες από ότι τα συστήματα με απλό φιλτράρισμα πακέτων και μπορούν να προγραμματιστούν πιο έξυπνα κάνοντάς τα ικανά να υποστηρίξουν σύνθετες πολιτικές ασφάλειας.
Όλα τα IP-πακέτα που φτάνουν ή που πρέπει να φύγουν, εξετάζονται πρώτα ως προς το περιεχόμενό τους και ανάλογα προωθούνται ή απορρίπτονται. Για το σκοπό αυτό χρησιμοποιούνται προγράμματα που εκτελούνται ως εφαρμογές, οι οποίες ονομάζονται proxies. Κάθε TCP/IP υπηρεσία που θέλουμε να ελέγχεται από το firewall, έχει το δικό της proxy, δηλαδή μια υπηρεσία διαμεσολαβητή (middleman service). Για παράδειγμα, ένας χρήστης προερχόμενος από το Internet, για να αποκτήσει πρόσβαση στην υπηρεσία FTP ενός μηχανήματος του προστατευόμενου δικτύου, θα πρέπει πρώτα να συνδεθεί με την αντίστοιχη proxy εφαρμογή, να ακολουθήσει η αναγνώριση-πιστοποίησή του και στη συνέχεια, αν η πολιτική ασφάλειας του firewall περιέχει για το συγκεκριμένο και αναγνωρισμένο χρήστη τις κατάλληλες εξουσιοδοτήσεις, θα προωθηθεί η σύνδεση με την υπηρεσία FTP που ζήτησε.
Κάθε υπηρεσία proxy, είναι ένα λογισμικό δυο κατευθύνσεων που δρα ταυτόχρονα και σαν εξυπηρετητής (server) και σαν πελάτης (client):

- στους εσωτερικούς χρήστες απαντάει σαν να είναι η εξωτερική σύνδεση που ζήτησαν, ενώ
- στους εξωτερικούς χρήστες αποκρίνεται σαν να είναι η εσωτερική υπηρεσία που θα χρειαστούν.

Στην πραγματικότητα, δηλαδή, ένα τέτοιου τύπου firewall ή συστατικό ενός firewall, εκτελώντας ψευδοεφαρμογές, παρεμβάλλεται μεταξύ των πρωτοκόλλων επικοινωνίας προκειμένου να ελέγχει τη νομιμότητα των επικοινωνιών. Καμία άλλη υπηρεσία δεν μπορεί απευθείας να στείλει ή να λάβει δεδομένα. Αυτός είναι άλλωστε και ο ρόλος του συστήματος firewall, να λειτουργεί δηλαδή ως ένα ισχυρό τείχος ασφαλείας αλλά και ικανό να προσαρμόζεται εύκολα στις ανάγκες επικοινωνίας ενός

δικτύου. Η τεχνολογία αυτή προσφέρει ολοκληρωμένη ασφάλεια με τους ισχυρούς μηχανισμούς αυθεντικοποίησης χρηστών και συστημάτων (entity and origin authentication), καταγραφής (logging) και υποστήριξης υπευθυνότητας (accounting) που διαθέτει. Επιπλέον, προσφέρει πολύ ευκολότερη διαχείριση, αφού οι κανόνες που απαιτεί για τον έλεγχο μιας εφαρμογής είναι πολύ πιο απλοί από αυτούς που θα χρειαζόταν ένα firewall τύπου φίλτρου πακέτων. Αξίζει να σημειωθεί ότι επιπλέον μια από τις παρεχόμενες υπηρεσίες του firewall, μπορεί να είναι και ο έλεγχος της κυκλοφορίας των δεδομένων μέσω IP επικεφαλίδων. Αυτό σημαίνει ότι η πύλη εφαρμογών μπορεί να παίξει και το ρόλο ενός φίλτρου πακέτων δεδομένων, αλλά με χαμηλότερες επιδόσεις στη ταχύτητα ελέγχου των πακέτων.

8.6. Σύγχρονες τεχνολογίες Firewall-Υβριδικές πύλες.

Είναι γενική αίσθηση των διαχειριστών firewalls, ότι για ολοκληρωμένη προστασία απαιτείται η συνδυασμένη δράση των τεχνολογιών επιπέδου πακέτων και επιπέδου εφαρμογής. Έτσι, παρατηρείται μια τάση υιοθέτησης της σύγκλισης αυτών των τεχνολογιών ως ο ιδανικός τρόπος υλοποίησης συστημάτων firewall για περιβάλλοντα μεσαίας έως υψηλής επικινδυνότητας (medium-to-high risk environments).
Ο όρος υβριδικές ή σύνθετες πύλες (hybrid or complex gateways) χρησιμοποιείται για να περιγράψει τα σύγχρονα συστήματα firewall που συνδυάζοντας τα πλεονεκτήματα των προηγούμενων τεχνολογιών / τύπων, προχωρούν ακόμη ένα βήμα παραπέρα. Δυο είναι οι σύγχρονες εναλλακτικές υλοποιήσεις:

- Συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών
- Τεχνολογία Stateful Inspection.

8.6.1. Συνδυασμός φιλτραρίσματος πακέτων με πύλες εφαρμογών.

Έχει ήδη τονιστεί ο σχετικά πρωτόγονος έλεγχος αποκλειστικά των IP-επικεφαλίδων, είναι μια λειτουργία που κάθε firewall χρειάζεται, γιατί σε αρκετές περιπτώσεις αυτός είναι ο πιο κατάλληλος και πιο γρήγορος τρόπος ελέγχου. Έτσι ακόμη και τα καθαρά proxy firewalls διαθέτουν λογισμικό που προσομοιώνει έναν δρομολογητή φιλτραρίσματος. Επειδή όμως αυξάνει κατά πολύ η ασφάλεια ενός συστήματος όταν δεν είναι συγκεντρωμένη η άμυνά του σε ένα μοναδικό σημείο, πολλές φορές ένα proxy-based σύστημα firewall συνδυάζεται με μια επιπλέον διάταξη φίλτρου πακέτων. Το υβριδικό αυτό σύστημα αποκτά παράλληλα ακόμη πιο γρήγορο και πιο αξιόπιστο φιλτράρισμα πακέτων, αφού είναι επιπέδου hardware. Η σύνδεσή τους πρέπει

φυσικά να γίνει εν σειρά έτσι ώστε οι επικοινωνίες να διέρχονται και από τα δυο αυτά συστατικά μέρη του firewall.

8.6.2. Τεχνολογία Stateful inspection

Πρόκειται για μια νέα τεχνολογία, κατηγορίας packet filtering. Όμως επεκτείνεται το απλό IP φιλτράρισμα δίνοντας δυνατότητα να εξετάζεται το κάθε πακέτο στο εσωτερικό του και μάλιστα όχι το κάθε ένα ξεχωριστά και απομονωμένα αλλά ο έλεγχος να γίνεται σε σχέση με προηγούμενες επικοινωνίες. Δημιουργείται δηλαδή μια εσωτερική βάση δεδομένων με πληροφορίες προηγούμενων πακέτων που συνεχώς ενημερώνεται. Με αυτόν τον τρόπο είναι δυνατόν να καταγράφονται πληροφορίες κατάστασης (state information) και συναφείς πληροφορίες (context information) για κάθε επικοινωνία, οπότε, από τον έλεγχό τους και με συνεχή τροφοδοσία από την εξελισσόμενη βάση δεδομένων, επιτρέπεται ή απαγορεύεται μια επικοινωνία με δυναμικό τρόπο.
Ο χώρος δράσης ενός τέτοιου «έξυπνου» (intelligent) firewall εκτείνεται και στα χαμηλά επίπεδα δικτυακής επικοινωνίας, όπου φιλτράρονται τα πακέτα, αλλά και στο επίπεδο εφαρμογής. Σε αυτό το επίπεδο γίνεται η διαχείριση και ο καθορισμός της πολιτικής ασφάλειας μέσω πάλι υπηρεσιών proxy, διαφορετικής όμως κατασκευής από τα firewall τύπου application gateway. Αυτός ο συνδυασμός δράσης υπερέχει σημαντικά έναντι των υπολοίπων, αφού συγκεντρώνει όλα τα πλεονεκτήματα των δυο βασικών τεχνολογιών. Όπως και στα προηγούμενα τύπου firewalls, η εγκατάσταση μιας ξεχωριστής διάταξης δρομολόγησης έχει νόημα μόνο ως κίνηση διασποράς των σημείων αμύνης.

8.7. Σύγκριση Τεχνικών Προστασίας.

Ο όρος firewall αναφέρεται πλέον στις δυο νεότερες τεχνολογίες, δηλαδή σε αυτές που ξεφεύγουν από ένα απλό (stateless) φιλτράρισμα πακέτων. Η σύγκριση που θα επιχειρηθεί στη συνέχεια αφορά τα συστήματα τύπου application gateway και τύπου stateful inspection.
Το μειονέκτημα των πρώτων είναι ότι πρέπει να υπάρχει ένα εξειδικευμένο πρόγραμμα (proxy) για κάθε εφαρμογή που χρειάζεται να «διαπερνά» το firewall. Βέβαια κάθε τέτοιο firewall έρχεται με έναν αριθμό ήδη έτοιμων τέτοιων εφαρμογών για την εξυπηρέτηση των πιο συνηθισμένων υπηρεσιών (όπως FTP, HTTP κ.λ.π.) Πάντως η ανάπτυξη μιας εφαρμογής proxy για μια νέα υπηρεσία είναι μια χρονοβόρα και δύσκολη υπόθεση.
Αυτό το μειονέκτημα έρχονται να καλύψουν τα firewalls δυναμικού φιλτραρίσματος. Η προσθήκη υποστήριξης νέων υπηρεσιών, γίνεται εδώ πιο εύκολα μέσω μιας πανίσχυρης και υψηλού επιπέδου γλώσσας προγραμματισμού (Inspect Language) η οποία έχει τη δυνατότητα να

επεμβαίνει και στο κέντρο της λειτουργίας του firewall, την αποκαλούμενη Inspect Engine. Με αυτό τον τρόπο παρέχεται πολύ σημαντική επεκτασιμότητα (system extensibility). Επιπλέον, η τεχνολογία stateful inspection (και μόνον αυτή) προσφέρει δυνατότητα φιλτραρίσματος για πρωτόκολλα UDP (User Data gram Protocol) και RPC (Remote Procedure Call). Τα πρωτόκολλα αυτά είναι stateless,δηλαδή κάθε μονάδα δεδομένων ταξιδεύει ανεξάρτητα και εφοδιασμένη με πληροφορίες πηγής και προορισμού. Αυτό όμως δυσκολεύει τη δουλειά ενός κλασσικού firewall, γιατί δεν γνωρίζει σε ποια επικοινωνία εντάσσεται το κάθε πακέτο. Η Inspect Engine είναι ικανή να δημιουργεί και να αποθηκεύει τα «συμφραζόμενα» δεδομένα (context data), για να προσφέρει έλεγχο και για τέτοιες επικοινωνίες.
Όμως για όλα αυτά υπάρχει το τίμημα που αφορά την ευκολία δημιουργίας λαθών κατά τη συντήρηση ενός firewall με stateful inspection. Ο διαχειριστής ενός τέτοιου firewall, πρέπει να είναι πολύ προσεκτικός γιατί έχει στη διάθεσή του ισχυρά εργαλεία που αν δεν χρησιμοποιηθούν σωστά, θα επιτρέπεται σε επικίνδυνες υπηρεσίες να διαπερνούν το σύστημα, κάνοντάς το έτσι πιο ευάλωτο. Δεν είναι λοιπόν τυχαίο ότι για τους επίδοξους εισβολείς (intruders, hackers κ.λ.π.) τα συστήματα δυναμικού φιλτραρίσματος πακέτων, αποτελούν τον αγαπημένο τους στόχο. Από την άλλη, θεωρούνται πιο δύσκολα για τη πραγματοποίηση επιτυχημένων επιθέσεων, αν έχουν διαμορφωθεί σωστά.

8.8. Αρχιτεκτονικές Συστημάτων Firewalls.

Ένα ολοκληρωμένο σύστημα firewall μπορεί να αποτελείται από αρκετά συστατικά, χωρίς να είναι και όλα απαραίτητα. Πέντε διαφορετικά μέρη μπορεί κανείς να διακρίνει στη σχεδίαση ενός τέτοιου συστήματος:

- Μηχανισμό φίλτρου πακέτων: για να εμποδίζεται η πορεία των διακινούμενων πακέτων δεδομένων ανάμεσα στο Internet και το ιδιωτικό δίκτυο και να επιτρέπεται η κίνησή τους μέσω του firewall μόνο σε όσα πακέτα ανήκουν σε αποδεκτούς τρόπους επικοινωνίας.
- Λογισμικό υλοποίησης πυλών σε επίπεδο εφαρμογής (application level gateways): ικανό να εμποδίζει τη κυκλοφορία των δεδομένων και να αυθεντικοποιεί (authentication) τους χρήστες σε επίπεδο εφαρμογών TCP IP (όπως οι υπηρεσίες εξυπηρέτησης HTTP, FTP κ.λ.π.).
- Υπηρεσία ονομασίας επικρατειών (Domain Name Service- DNS): ικανή για την απόκρυψη των εσωτερικών IP διευθύνσεων του ιδιωτικού δικτύου από τους χρήστες του διαδικτύου.
- Μηχανισμό διαχείρισης ηλεκτρονικών γραμμάτων: για να διασφαλίζεται ότι η ανταλλαγή ηλεκτρονικών γραμμάτων διεκπεραιώνεται μέσω firewall.

- Ασφαλές λειτουργικό σύστημα: ως βάση του άλλου συστήματος.

Τα συστήματα firewalls συναντώνται με διάφορους τρόπους διαμόρφωσης (configuration)και αρχιτεκτονικής (architecture). Παρέχουν έτσι και διαφορετικά επίπεδα ασφάλειας με το ανάλογο κόστος εγκατάστασης και λειτουργίας. Οι διάφοροι οργανισμοί οφείλουν να επιλέξουν τύπο, ανάλογα με τη σοβαρότητα των κινδύνων που αντιμετωπίζουν. Ακολουθούν οι πιο συνηθισμένες μορφές αρχιτεκτονικής firewall.

8.8.1. Multi-Homed Host

Είναι ένας διακομιστής / οικοδεσπότης (host) που διαθέτει περισσότερες από μια κάρτες δικτύου. Κάθε κάρτα είναι συνδεδεμένη σε ένα τμήμα δικτύου (subnet) που είναι λογικά και φυσικά διαχωρισμένο. Η πιο διαδεδομένη μορφή της είναι με δυο κάρτες δικτύου (dual-homed host). Σε ένα dual-homed firewall, η μια κάρτα είναι συνδεμένη στο εξωτερικό και μη έμπιστο διαδίκτυο, ενώ η άλλη κάρτα συνδέεται με το εσωτερικό και θεωρούμενο ασφαλές δίκτυο. Σημείο προσοχής σε αυτή την αρχιτεκτονική είναι ότι δεν πρέπει να επιτρέπεται η άμεση δρομολόγηση των πακέτων των δεδομένων ανάμεσα στα δυο δίκτυα. Η επικοινωνία τους πρέπει να γίνεται μόνο μέσω του λογισμικού firewall του διακομιστή.

8.8.2. Screened Host

Αυτή η αρχιτεκτονική χρησιμοποιεί έναν διακομιστή που καλείται οχυρό (bastion host) και έναν δρομολογητή φιλτραρίσματος (filtering or screening router). Ο δρομολογητής αυτός είναι έτσι διαμορφωμένος ώστε να στέλνει αποκλειστικά στον bastion host όλες τις προερχόμενες από το εξωτερικό δίκτυο αιτήσεις, όποιον προορισμό και αν είχαν αυτές μέσα στο εσωτερικό δίκτυο. Όλοι λοιπόν οι εξωτερικοί διακομιστές, υποχρεωτικά περνούν μέσω του λογισμικού firewall στο διακομιστή-οχυρό.

8.8.3. Screened Subnet

Πρόκειται ουσιαστικά για την προηγούμενη αρχιτεκτονική μορφή, όπου επιπρόσθετα χρησιμοποιείται ένας δεύτερος δρομολογητής φιλτραρίσματος προκειμένου να διαχωρίσει τον bastion host και το δίκτυο που αυτός βρίσκεται, το οποίο καλείται περιμετρικό δίκτυο, από το υπόλοιπο εσωτερικό δίκτυο. Έτσι παρέχεται ακόμη ένα επίπεδο προστασίας.

8.9. Γενικές Κατευθύνσεις Πολιτικής Ασφάλειας.

Τα κύρια σημεία μιας πολιτικής ασφάλειας μέσω firewalls είναι ότι πρέπει:

- Ένα firewall να διαμορφώνεται έτσι ώστε να αποτελεί τη μόνη ορατή διεύθυνση διακομιστή προς το έξω δίκτυο, ενώ ταυτόχρονα απαιτεί όλες οι συνδέσεις προς και από το εσωτερικό δίκτυο να διέρχονται μέσα από αυτό.
- Οι ισχυροί μηχανισμοί πιστοποίησης χρηστών να εφαρμόζονται σε επίπεδο εφαρμογής (application gateways).
- Οι υπηρεσίες διαμεσολάβησης (proxy) να παρέχουν λεπτομερείς πληροφορίες καταγραφής (logging) σε επίπεδο εφαρμογής.
- Να μην επιτρέπεται η άμεση προσπέλαση στις δικτυακές υπηρεσίες του εσωτερικού δικτύου. Όλες οι αιτήσεις που φτάνουν για υπηρεσίες, όπως TELNET, FTP, HTTP, e-mail κ.λ.π. να διέρχονται μέσω της κατάλληλης υπηρεσίας proxy στο firewall, ανεξάρτητα από το ποιος εσωτερικός διακομιστής είναι ο τελικός προορισμός τους.
- Όλες οι νεοεισερχόμενες υπηρεσίες οφείλουν να διεκπεραιώνονται από υπηρεσίες proxy του firewall. Αν μια νέα υπηρεσία ζητηθεί, αυτή δεν θα είναι διαθέσιμη έως ότου διατεθεί το αντίστοιχο λογισμικό proxy και γίνουν οι έλεγχοι από το διαχειριστή ασφάλειας.
- Όλη η διαχείριση του συστήματος firewall οφείλει να έχει πολύ καλή εμπειρία στα δικτυακά ζητήματα ασφαλείας, καθώς και στη σχεδίαση και υλοποίηση firewalls. Έτσι μπορεί να επιτύχει τη σωστή ρύθμιση και εγκατάστασή του, ενώ ακόμη μπορεί να το διαχειρίζεται με ασφαλή τρόπο. Επιπλέον, οι διαχειριστές οφείλουν σε περιοδική βάση, να επιμορφώνονται και να ενημερώνονται πάνω σε πρακτικές ασφάλειας δικτύων και λειτουργίας συγχρόνων διατάξεων firewalls.
- Να δημιουργούνται σε καθημερινή βάση, εβδομαδιαία και μηνιαία βάση ασφαλή (εφεδρικά) αντίγραφα (backups) του λογισμικού και των δεδομένων του συστήματος firewall, δηλαδή του λογισμικού συστήματος, τω αρχείων ρυθμίσεων, των αρχείων της βάσης δεδομένων, των αρχείων καταγραφής κ.α., έτσι ώστε σε περίπτωση αποτυχίας του συστήματος (system failure) να υπάρχει η δυνατότητα αποκατάστασης της λειτουργίας του χωρίς σημαντικές απώλειες. Τα εφεδρικά αρχεία να φυλάσσονται με ασφάλεια σε αξιόπιστα μέσα που κατόπιν μπορούν να χρησιμοποιηθούν μόνο για ανάγνωση, για να αποφευχθεί η ακούσια διαγραφή / καταστροφή τους. Μόνο το κατάλληλο προσωπικό να έχει φυσική πρόσβαση σε αυτά.
- Τουλάχιστον ένα ακόμη σύστημα firewall, έτοιμο προς χρήση και με τις σωστές ρυθμίσεις να κρατείται εκτός λειτουργίας ως εφεδρεία.

8.10. Πλεονεκτήματα και Περιορισμοί.

8.10.1. Πλεονεκτήματα από τη Χρήση Firewalls.

Ένα firewall σε λειτουργία, δεν είναι μόνο ένα απλό συστατικό του δικτύου, αλλά αποτελεί την υλοποίηση μιας στρατηγικής για τη προστασία των συνδεδεμένων στο διαδίκτυο πόρων ενός οργανισμού, εξασφαλίζοντας ότι όλες οι επικοινωνίες από και προς το Internet είναι σύμφωνες με την προκαθορισμένη πολιτική ασφάλειας του οργανισμού. Αυτό αποτελεί την πρώτη και σημαντικότερη ωφέλεια από τη χρήσης τους. Όμως σπουδαίες είναι και οι υπόλοιπες επιμέρους ωφέλειες που παρέχει ένα σύστημα firewall, όπως το ότι:

- Επιτρέπει αποτελεσματικά την επιβολή της πολιτικής ασφάλειας (policy enforcement) που θέλουμε να εφαρμόσουμε στο σύστημά μας. Η διαμόρφωση και η παραμετροποίηση που υποστηρίζει μας βοηθά να ορίσουμε ποιος χρήστης θα έχει πρόσβαση σε πιο πόρο. Παράλληλα μέσω των διαθέσιμων εργαλείων του για καταγραφή και επίβλεψη, έχουμε μια πλήρη εικόνα των προσπαθειών (επιτυχών και ανεπιτυχών) σύνδεσης η οποία θα χρησιμεύσει στη συντήρηση ή και στη μετατροπή της πολιτικής ασφάλειας, ειδικότερα για χρήστες με «ύποπτη» συμπεριφορά. Χωρίς firewalls, η εφαρμογή της πολιτικής εξαρτάται από τη διάθεση συνεργασίας των χρηστών, αφού η ασφάλεια ενός δικτύου αντιμετωπίζεται ξεχωριστά από το κάθε τμήμα του. Βέβαια, η ασφάλεια ενός οργανισμού λίγο-πολύ εξαρτάται από τους χρήστες του και τη συμμόρφωσή τους στους προβλεπόμενους κανόνες, αλλά με κανένα τρόπο δεν πρέπει να εξαρτάται από τους εξωτερικούς χρήστες του διαδικτύου.
- Προστατεύει από ευπαθείς υπηρεσίες δικτύων. Είναι γνωστό ότι τα πρωτόκολλα επικοινωνίας του διαδικτύου παρουσιάζουν εγγενή προβλήματα ασφάλειας. Η εγκαθίδρυση ενός συστήματος firewall προσφέρει δυνατότητες φιλτραρίσματος που ελαχιστοποιούν τους κινδύνους. Ακόμη μπορεί και καλύπτει γνωστές ρωγμές ασφάλειας (όπως οι επιθέσεις αδυναμίας εξυπηρέτησης) στο κατώτερο επίπεδο των λειτουργικών συστημάτων. Έτσι, κάποια αδύνατα σημεία για την ασφάλεια του δικτύου, που έχουν ήδη τύχει εκμετάλλευσης από διάφορους εισβολείς, έρχεται να τα προστατέψει η χρήση των firewalls.
- Αποτελεί μέσο καταγραφής (logging) για τη χρήση και συναγερμού (alarming) για την παράνομη χρήση δικτύου. Οι πληροφορίες που καταγράφονται είναι πολύτιμες λόγω της θέσης του firewall (καθώς είναι το μοναδικό σημείο σύνδεσης με το έξω δίκτυο) και για αυτό είναι ακριβής και αξιόπιστες, καθώς τεκμηριώνουν την ικανότητα ή όχι του ίδιου του firewall για αποτροπή των επιθέσεων που συνέβησαν και κρίνουν την

καταλληλότητα της πολιτικής ασφάλειας που εφαρμόζεται. Επιπλέον, τα στατιστικά χρήσης του δικτύου είναι χρήσιμα και στις διαδικασίες ανάλυσης κινδύνων (risk analysis) και ανάλυσης απαιτήσεων δικτύου (network requirement analysis). Ένα firewall μπορεί ακόμη μα τις δυνατότητες επεξεργασίας των πληροφοριών αυτών που διαθέτει, να εντοπίσει ύποπτες δραστηριότητες και να αντιδράσει με προαποφασισμένες ενέργειες, όπως το κλείσιμο της σύνδεσης ή η ενημέρωση του διαχειριστή ασφάλειας με e-mail.

- Επιβάλλει ελεγχόμενη προσπέλαση (controlled access) στους πόρους ενός εσωτερικού δικτύου. Για παράδειγμα, κάποιοι διακομιστές ενδέχεται να προσφέρονται για επικοινωνία με το Internet, ενώ άλλοι όχι.
- Προσφέρει διευρυμένη ιδιωτικότητα (enhanced privacy). Για παράδειγμα αποκρύπτει λεπτομέρειες σχετικές με τη διάρθρωση του εσωτερικού δικτύου. Έτσι, οι εξωτερικοί παρατηρητές (intruders) δυσκολεύονται στις ενδεχόμενες προσπάθειές τους να «ξεφύγουν» από τα όρια χρήσης του δικτύου που έχουν καθοριστεί. Γενικότερα, υπάρχουν πάντοτε πληροφορίες που ενώ θεωρούνται αβλαβείς, περιέχουν σημαντικά στοιχεία για έναν επιδέξιο εισβολέα που θέλει να επιχειρήσει επίθεση. Έτσι, μέσω του firewall, πολλοί οργανισμοί σταματούν τις προσπάθειες για κακόβουλες χρήσεις των υπηρεσιών, όπως Finger και DNS (Domain Name Service). Η πρώτη δίνει πληροφορίες σχετικά με τους χρήστες ενός δικτύου, όπως το πότε συνδέθηκαν για τελευταία φορά, αν διαβάσανε το ηλεκτρονικό τους ταχυδρομείο, κ.λ.π., οι οποίες παρέχουν πληροφορίες στους εισβολείς σχετικές με το πόσο συχνά ένα σύστημα χρησιμοποιείται ή αν εκείνη τη στιγμή υπάρχουν συνδεδεμένοι ενεργοί χρήστες. Η υπηρεσία DNS από την άλλη, παρέχει πληροφορίες για τις δικτυακές τοποθεσίες του συστήματος, όπως τα ονόματα των τόπων και οι IP διευθύνσεις του. Η μη δημοσιοποίηση τους στο διαδίκτυο, αφαιρεί σίγουρα χρήσιμα στοιχεία από όσους τα συμβουλεύονται.
- Συγκεντρώνει υπηρεσίες ασφάλειας σε μια καλά ορισμένη και οχυρωμένη περιοχή (concentrated security). Ελαχιστοποιεί τη ζώνη κινδύνου (zone risk) ενός οργανισμού εφόσον μια ευρεία περιοχή των μηχανημάτων του παύει να απειλείται άμεσα. Ουσιαστικά το ίδιο το firewall αποτελεί τη μοναδική ζώνη κινδύνου για τον οργανισμό. Άμεση συνέπεια το γεγονός αυτού, είναι η ευκολία διαχείρισης ασφάλειας και γενικότερα μια οικονομία κλίμακας αφού δεν απατούνται επεμβάσεις σε όλους τους διακομιστές κάθε φορά που γίνονται ρυθμίσεις λόγω αλλαγών στο λογισμικό των εφαρμογών ή της ασφάλειας. Η ενημέρωση- συντήρηση αφορά κυρίως το σύστημα firewall. Για παράδειγμα, η εγκατάσταση πρόσθετου λογισμικού

πιστοποίησης(όπως τα συστήματα συνθηματικών μιας χρήσης, δεν χρειάζεται να γίνει σε κάθε διακομιστή ξεχωριστά, αλλά να γίνει μια φορά στο firewall.

- Αρκετά σύγχρονα συστήματα firewall προσφέρουν ως επιπλέον υπηρεσία τη λειτουργία του ως πύλες κρυπτογράφησης (encrypting gateways). Δηλαδή, παρέχουν ταυτόχρονα δυνατότητες κρυπτογράφησης των επικοινωνιών μεταξύ των διακομιστών που προστατεύουν. Ακόμη και εξωτερικά συστήματα μπορούν να συνομιλήσουν σε κρυπτογραφημένη μορφή, αρκεί να εγκαταστήσουν το ανάλογο λογισμικό πελάτη και να παρουσιάσουν τα σχετικά διαπιστευτήρια που προέρχονται από το διαχειριστή του firewall. Ένας τέτοιος λογικός διαχωρισμός των δικτύων μέσω firewalls και τεχνικών κρυπτογράφησης δημιουργεί τα λεγόμενα εικονικά ιδιωτικά δίκτυα (Virtual Private Networks- VPN). Η κρυπτογράφηση μπορεί να είναι επιλεκτική, ανάλογα με την αιτούμενη από το διαδίκτυο υπηρεσία και η διαχείρισή της ν α είναι ενσωματωμένη με τα υπόλοιπα χαρακτηριστικά των firewall, έτσι ώστε να είναι δυνατή η εκμετάλλευση όλων των βοηθημάτων που υποστηρίζονται για τη κατασκευή των κανόνων ελέγχου προσπέλασης, τη καταγραφή- παρακολούθηση των ενεργειών, κ.λ.π.

8.10.2. Περιορισμοί των Firewalls

τα συστήματα firewalls δεν αποτελούν πανάκεια για τα προβλήματα ασφάλειας στο διαδίκτυο. Υπάρχουν κίνδυνοι που ξεφεύγουν από τις δυνατότητές τους:

- Δεν προστατεύουν από τους εσωτερικούς χρήστες (π.χ. από τους υπαλλήλους του οργανισμού). Εφόσον ένα εσωτερικό μηχάνημα μπορεί να επικοινωνήσει με ένα άλλο, κάνοντας χρήση πρωτοκόλλου διαδικτύου, χωρίς να «περάσει» μέσα από το firewall, οποιαδήποτε ζημιά μπορεί να προκληθεί χωρίς να γίνει αντιληπτό από αυτό. Απαιτούνται επιπλέον μηχανισμοί πιστοποίησης και ελέγχου προσπέλασης για τους χρήστες και τις δραστηριότητες των συστημάτων τους. Τα intranet firewalls ελαχιστοποιούν ανάλογους κινδύνους, παρακολουθώντας την κυκλοφορία ανάμεσα στα διάφορα τμήματα ενός οργανισμού.
- Μπορούν να προστατεύσουν ένα περιβάλλον, μόνον όταν ελέγχουν πλήρως την περίμετρό του. Δηλαδή, δεν πρέπει να υπάρχουν συνδέσεις (π.χ. μέσω modem) που να μην διοχετεύονται μέσω του firewall. Στην περίπτωση που έστω και ένας εσωτερικός διακομιστής μπορέσει να αποκτήσει τέτοια εξωτερική σύνδεση, ολόκληρο το εσωτερικό δίκτυο τίθεται σε κίνδυνο.

- Δεν είναι εντελώς άτρωτα, μπορούν να διαπεραστούν. Οι κατασκευαστές των συστημάτων firewalls τα κρατούν μικρά και απλά έτσι ώστε ο πιθανός εισβολέας να μην αποκτήσει στη συνέχεια τον έλεγχο επικίνδυνων εργαλείων όπως τα προγράμματα μεταγλώττισης (compilers), τα προγράμματα σύνδεσης (linkers) κ.λ.π. Όμως σε καμία περίπτωση δεν πρέπει να θεωρείται ότι είναι ικανά μόνα τους να εξασφαλίσουν την απόκρουση όλων των εξωτερικών επιθέσεων. Πρέπει να θεωρούνται απλώς σαν μια ισχυρή πρώτη γραμμή άμυνας.
- Αποτελούν για έναν οργανισμό, το πιο ορατό σημείο του προς τον έξω κόσμο. Έτσι μοιραία είναι και ο πιο ελκυστικός στόχος επίθεσης. Απαραίτητη επομένως είναι η οργάνωση άμυνας εις βάθος, με επιπλέον επίπεδα προστασίας.
- Διαθέτουν από περιορισμένο έως ελάχιστο έλεγχο πάνω στο περιεχόμενο των εισερχόμενων μηνυμάτων. Έτσι σε επιθέσεις όπως αυτές των ιών και παρόμοιου κινδύνου κώδικα, χρειάζονται επιπλέον μέτρα προστασίας.
- Απαιτούν σωστή εγκατάσταση, προσεκτικές ρυθμίσεις και συνεχείς ενημερώσεις στη διαμόρφωσή τους ανάλογα με τις αλλαγές που παρουσιάζουν το εσωτερικό δίκτυο και οι συνδέσεις του με τον έξω κόσμο. Ακόμη, πρέπει να μελετώνται οι εγγραφές των αρχείων καταγραφής για τον έλεγχο της απόδοσής τους και για τον εντοπισμό πιθανών δυσλειτουργιών τους. Αλλιώς δημιουργείται μια εσφαλμένη αίσθηση ασφάλειας με αποτέλεσμα μια σχετικά εύκολη διείσδυση να αφήνει απροστάτευτους τους θεωρούμενους ασφαλείς εσωτερικούς πόρους.

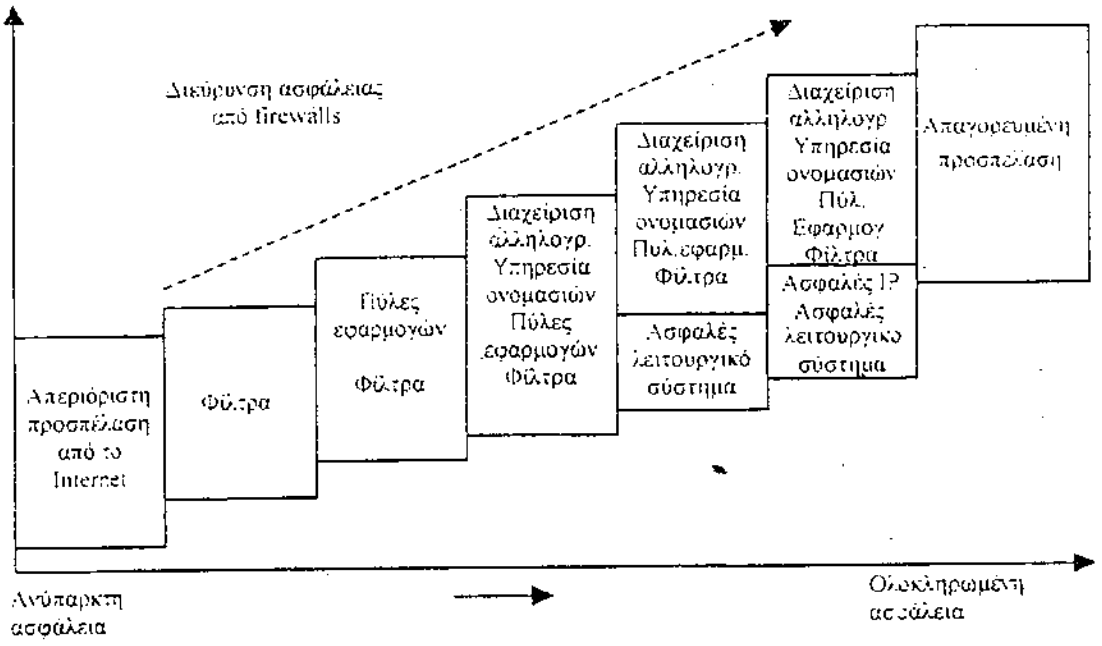
8.11. Αποδεκτή Λειτουργικότητα Συστημάτων Firewalls.

Ένα σύστημα firewall θα πρέπει να ικανοποιεί τις ακόλουθες προϋποθέσεις:

- Να απορρίπτει κάθε πακέτο που ρητά κάποιος κανόνας δεν επιτρέπει να περάσει. Αυτή είναι εξ' ορισμού (by default) ρύθμιση για τα περισσότερα firewalls και επιβάλλει στο διαχειριστή τους να διευκρινίσει ποιες ακριβώς επικοινωνίες είναι αποδεκτές.
- Να κρατάει τους εξωτερικούς χρήστες έξω από το προστατευόμενο δίκτυο. Αν για παράδειγμα, πρέπει κάποια αρχεία να γίνουν προσιτά μέσω του διαδικτύου, τότε το πιο σίγουρο είναι αυτά να τοποθετηθούν έξω από το firewall. Εναλλακτικά, απαιτούνται ισχυροί μηχανισμοί αυθεντικοποίησης (authentication) σε επίπεδο εφαρμογών για την παρεμπόδιση των μη- εξουσιοδοτημένων χρηστών.
- Να διαθέτει προηγμένα εργαλεία καταγραφής, επίβλεψης και πρόσκλησης συναγερμού (alarm generation), ικανά να αναλύουν τις πραγματοποιημένες συναλλαγές με σκοπό την εξαγωγή

συμπερασμάτων σχετικά με το είδος και τη φύση των επιθέσεων και τη συνακόλουθη προσαρμογή της υφιστάμενης πολιτικής ασφάλειας.

Συνοπτικά, ένα firewall πρέπει να είναι ικανό να προσφέρει υπηρεσίες ασφάλειας ελέγχου προσπέλασης (access control), συνδυάζοντας μηχανισμούς αυθεντικοποίησης (authentication), εξουσιοδότησης (authorization), επίβλεψης (auditing) και, όπου είναι δυνατόν, κρυπτογράφησης (encryption).



Σχ. 7. Διαβάθμιση ασφάλειας παρεχόμενης από firewall.

Ανάλογα με τα συστατικά που περιλαμβάνει ένα σύστημα firewall, παρέχει και διαφορετική βαθμίδα ασφαλείας. Ουσιαστικά πρόκειται για μια σχέση αντιστρόφως ανάλογη ανάμεσα στην παρεχόμενη ελευθερία σύνδεσης και στην ασφάλεια (connectivity against security). Πλήρης ελευθερία σύνδεσης σημαίνει καθόλου ασφάλεια, ενώ αντίθετα πλήρης ασφάλεια σημαίνει καθόλου ελευθερία σύνδεσης. Οι ενδιάμεσες βαθμίδες στη συνδεσιμότητα εξαρτώνται από τις υπηρεσίες και το βάθος ασφάλειας που υποστηρίζονται.

Η διαβάθμιση της παρεχόμενης ασφάλειας από ένα firewall εξαρτάται επιπλέον από το εάν αυτό παρέχει εμπιστευτικότητα και ακεραιότητα μέσω μηχανισμών κρυπτογράφησης. Η παρεχόμενη ασφάλεια καλείται Internet Layer Security γιατί η κρυπτογράφηση γίνεται μέσα στο (χαμηλού επιπέδου) IP κανάλι επικοινωνίας (IP Layer). Υποστηρίζει εμπιστευτικότητα και ακεραιότητα από οικοδεσπότη σε οικοδεσπότη

(host-to-host). Η δυνατότητα αυτή διακίνησης κρυπτογραφημένων δεδομένων μέσα στο πρωτόκολλο IP, καλείται και ασφαλές πρωτόκολλο IP (secure IP).Τα παραπάνω φαίνονται στο *Σχ. 7.*

ΒΙΒΛΙΟΓΡΑΦΙΑ

- NIST(National Institute of Standards and Technology)
- "Generally Accepted Principles and Practices for Securing information Technology Systems"
- Murrane Swanson- Barbara Gutman, September 1996.
- NIST (National Institute of Standards and Technology)
- "An Introduction To Computer Security: The List Hand Book"
- Special Publication 800-12
- Internet Firewalls Frequently Asked Questions
- Marcus S. Ranum and Matt Curtin, 26/05/1998.
- ICSA Firewall Polity Guide V2.00
- The World Wide Wed Security FAQ
- Lincoln D. Stein<1stein@cshl.orgs
- Version 2.00 December 1998
- OII Guide to Trust Services
- Information set by: Martin Bryan of the SGML Center and Man-S2e Li of IC Focus.
- OII Guide of information Security
- Martin Bryan- Man-S2e Li.
- OII- Information Security Standards
- Martin Bryan- Man S2e Li.
- "Internetworking with TCP/IP: Principles, Protocol J and Architecture" του Douglas E. Coumer, Prentice- Etall, Englewood (lifts. NJ.).
- "Internetworking with TCP/IP: Design, Imlevoentation and Internals" των Douglas E. Coumer και Dovid L. Stevens.
- "Unix Systems Security: A Guide for users, and System Administrations" του Addison- Wesley.
- "Computer Communications Security" του Warwick Ford.
- " TCP/IP Network Administration" του Craig Hunt.
- "Actually Use tool Internet Security Techniques" του Larry S. Hughes.